УТВЕРЖДЕН

МКЕЮ.00669-01 32 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «ЗАСТАВА-УПРАВЛЕНИЕ», ВЕРСИЯ 8 КС1» (ИСПОЛНЕНИЕ ZM8-EL64-FV-01)

РУКОВОДСТВО СИСТЕМНОГО ПРОГРАММИСТА

МКЕЮ.00669-01 32 01

Листов 298

Инв.№подл.	Подп. и дата	Взам. инв. №	Инв.№дубл.	Подп. и дата
9363				

2025

АННОТАЦИЯ

Документ МКЕЮ.00669-01 32 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01)». Руководство системного программиста» содержит сведения и инструкции, необходимые для работы с Программным комплексом «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01) МКЕЮ.00669-01 (далее - ПО ЗУ) пользователей с правами учётной записи администратора:

- локального/системного администратора;
- удаленного (сетевого) администратора;
- администратора безопасности средств криптографической защиты информации (СКЗИ).

Содержание

1 ВВЕДЕНИЕ ... 11
1.1 Общая информация ... 11
1.1.1 Назначение ... 11
1.1.2 Область применения ... 11
1.1.3 Ролевая модель ... 11
1.1.3.1 Функции удаленного администратора ... 12
1.1.3.2 Функции локального администратора ... 13
1.1.3.3 Функции администратора безопасности СКЗИ ... 13
2 ПОДГОТОВКА К ИСПОЛЬЗОВАНИЮ ПО ... 14
2.1 Системные требования к аппаратному обеспечению СВТ ... 14
2.2 Системные требования АРМ удаленного управления ПО ЗУ ... 14
2.3 Поддерживаемые версии управляемого программного обеспечения ... 14
2.4 Действия по приёмке ... 15
2.5 Проверка контрольной суммы образа ... 15
2.6 Проверка контрольной суммы ПО ЗУ ... 16
2.7 Действия по безопасной установке и настройке ... 16
2.7.1 Требования к персональным идентификаторам ... 17
2.8 Действия по реализации функций безопасности среды функционирования ... 17
2.9 Работа с сертификатами и ключами ... 18
2.9.1 Свойства сертификата и его проверка ... 18
2.9.2 Регистрация сертификата ... 19
2.9.3 Удаление сертификата ... 21
2.9.4 Создание запроса PKCS10 на выпуск сертификата ... 22
2.10 Способ извлечения запроса использования Secure Copy Protocol (SCP) ... 27
2.11 Компрометация ключей аутентификации ... 27
2.12 Рекомендации по безопасной настройке и конфигурированию ПО ЗУ ... 28
3 ПОДГОТОВКА К РАБОТЕ И БЫСТРЫЙ СТАРТ ... 32
3.1 Вход в ПО ЗУ локального/системного администратора ... 32
3.1.1 Смена пароля ... 32
3.2 Инициализация криптопровайдера «Элвис-Крипто» ... 33
3.3 Настройка сетевых параметров ... 33
3.3.1 Настройка адресации ... 33
3.3.2 Настройка маршрутизации ... 34
3.3.3 Настройка DNS ... 34
3.3.4 Применение настроек ... 34
3.3.5 Проверка корректности и завершение установки ... 34

3.3.6 Ввод файла с лицензией ... 35
3.3.7 Настройка «ЗАСТАВА-Офис» ... 36
4 ОБЗОР ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА ... 38
4.1 Общий вид веб-интерфейса ПО ЗУ ... 38
4.2 Элементы управления в веб-интерфейсе ... 38
4.2.1 Инструментальная линейка ... 38
4.2.1.1 Инструмент «Фильтр» ... 39
4.2.1.2 Инструмент «Показать топологию» ... 42
4.2.1.3 Инструмент «Показать лог» ... 43
4.2.1.4 Инструмент «Показать карту» ... 44
4.2.2 Общий вид окна со всеми активированными инструментами ... 44
4.2.3 Контекстные меню ... 45
5 ПАНЕЛЬ ВКЛАДОК МЕНЮ ... 48
5.1 Вкладка меню «Проект» ... 48
5.2 Вкладка меню «Настройки» ... 48
5.2.1 Настройка ролей и прав ... 49
5.2.2 Выбор языка интерфейса ... 51
5.3 Вкладка меню «Помощь» ... 52
6 БОКОВАЯ ПАНЕЛЬ ВКЛАДОК ... 53
6.1 Вкладка боковой панели «Правила» ... 53
6.1.1 Таблица правил ... 54
6.1.2 NAT правила ... 56
6.1.3 IKECFG динамические правила ... 58
6.1.4 IKECFG статические правила ... 60
6.1.5 Серверные правила ... 61
6.1.6 Прикладные правила ... 62
6.1.7 Работа с контекстным меню для элементов списка «Правила» ... 63
6.1.7.1 Общие команды контекстного меню для элементов списка «Правила»: ... 63
6.1.7.1.1 Дублировать ... 63
6.1.7.1.2 Изменить ... 64
6.1.7.1.3 Удалить ... 65
6.1.7.1.4 Показать в логе ... 66
6.1.7.2 Индивидуальные команды контекстного меню для элементов списка «Правила» ... 67
6.1.7.2.1 Добавить правило ... 67
6.1.7.2.2 Добавить дочернее правило ... 68
6.1.7.2.3 Добавить группу правил ... 69
6.1.7.2.4 Редактировать владельца ... 70
6.1.7.2.5 Редактировать сервер ... 71

6.1.7.2.6 Включить/отключить ... 72
6.1.7.2.7 Показать трассу ... 73
6.2 Вкладка боковой панели «Объекты политики» ... 74
6.2.1 Сетевые объекты ... 75
6.2.1.1 Работа с контекстным меню для элементов списка «Сетевые объекты» ... 76
6.2.2 Элемент списка «Пользователи» ... 76
6.2.2.1 Работа с контекстным меню для элементов списка «Пользователи» ... 78
6.2.3 Группы ... 79
6.2.3.1 Добавление группы ... 80
6.2.3.2 Создание иерархической структуры групп ... 81
6.2.3.3 Работа с контекстным меню для элементов списка «Группы» ... 83
6.2.4 Серверы ... 84
6.2.4.1 Добавления серверов ... 84
6.2.4.1.1 Общие настройки для всех типов серверов ... 86
6.2.4.2 Серверы-прогрузчики ... 87
6.2.4.2.1 Добавление и настройка загрузчика политики PMP ... 87
6.2.4.2.2 Объекты PMP Distribution Service. ... 87
6.2.4.2.3 Добавление и настройка загрузчика политики HTTP ... 89
6.2.4.3 Прокси-серверы ... 90
6.2.4.3.1 Настройки параметров соединений для прокси-серверов ... 91
6.2.4.3.2 Специфичные настройки авторизации для прокси-серверов ... 93
6.2.4.3.3 Специфичные настройки обработки для прокси-серверов ... 95
6.2.4.3.4 Объекты «Прокси FTP» ... 96
6.2.4.3.5 Объекты «Прокси HTTP» ... 99
6.2.4.3.6 Объекты «Прокси SMTP» ... 102
6.2.4.3.7 Объекты «Прокси SOCKS» ... 105
6.2.4.4 Прочие серверы ... 107
6.2.4.4.1 Объекты LDAP ... 107
6.2.4.4.2 Объекты SNMP ... 108
6.2.4.4.3 Объекты Syslog ... 110
6.2.4.4.4 Объект «Сервер обновления» ... 111
6.2.4.4.5 Объекты NetFlow ... 112
6.2.4.5 Серверы аутентификации ... 113
6.2.4.5.1 Аутентификация «Локальный» ... 114
6.2.4.5.2 Аутентификация RADIUS ... 114
6.2.4.6 Добавление сервера интеграции ... 115
6.2.4.7 Добавление объекта «Монитор» ... 117
6.2.5 Объединения ... 117

6.2.5.1 Работа с контекстным меню для элементов списка «Объединения» ... 119
6.3 Вкладка боковой панели «Настройки IKE/IPsec» ... 120
6.3.1 IKE ... 121
6.3.1.1 Объекты IKE и IKE предложения ... 121
6.3.1.2 Добавление IKE предложения ... 122
6.3.1.2.1 Примеры IKE предложений ... 124
6.3.1.3 Обмен сертификатами ... 125
6.3.2 IPsec ... 127
6.3.2.1 Добавление IPsec предложения ... 128
6.3.2.1.1 Примеры IPsec предложений ... 129
6.3.2.2 Добавление действия ... 129
6.3.3 Работа с контекстным меню для элементов списка «Настройки IKE/IPsec» ... 133
6.3.3.1 Дублировать ... 133
6.3.3.2 Изменить ... 134
6.3.3.3 Удалить ... 135
6.3.3.4 Показать в логе ... 136
6.4 Вкладка боковой панели «Монитор» ... 137
6.4.1 Объекты политики ... 137
6.4.1.1 Работа с контекстным меню элемента списка «Объекты политики» ... 138
6.4.1.1.1 Команда контекстного меню «Просмотр активной ЛПБ» ... 139
6.4.1.1.2 Команда контекстного меню «Редактировать политику» ... 139
6.4.1.1.3 Команда контекстного меню «Повторить активацию» ... 139
6.4.1.1.4 Команда контекстного меню «Установить обновление для агента» ... 140
6.4.1.1.5 Команда контекстного меню «Загрузить обновление для агента» ... 141
6.4.1.1.6 Команда контекстного меню «Установить URI для обновлений» ... 142
6.4.1.1.7 Команда контекстного меню «Соединения» ... 142
6.4.1.1.8 Команда контекстного меню «Загрузить список сертификатов» ... 142
6.4.1.1.9 Команда контекстного меню «Генерировать ключевую пару» ... 143
6.4.1.1.10 Команда контекстного меню «Отправить доверенный сертификат» ... 145
6.4.1.1.11 Команда контекстного меню «Интеграции» ... 145
6.4.1.1.12 Команда контекстного меню «Показать в логе» ... 145
6.4.2 Компьютеры ... 146
6.4.2.1 Контекстное меню элемента списка «Компьютеры» ... 146
6.4.3 Журнал ... 147
6.4.3.1 Настройка мониторинга для журнала «Обмен с агентами» ... 148
6.4.3.2 Фильтрация в журнале регистрации «Обмен с агентами» ... 149
6.4.3.3 Настройка мониторинга для журнала «Сторона сервера» ... 150
6.4.3.4 Фильтрация в журнале регистрации «Сторона сервера» ... 151

6.4.3.5 Настройка мониторинга для журнала «Последняя трансляция» ... 152
6.4.3.6 Фильтрация в журнале регистрации «Последняя трансляция» ... 152
6.4.3.7 Настройка мониторинга для журнала «Последний импорт» ... 154
6.4.3.8 Фильтрация в журнале регистрации «Последний импорт» ... 154
6.4.3.9 Настройка мониторинга для Журнала «Syslog» ... 155
6.4.3.10 Фильтрация результатов в журнале регистрации «Syslog» ... 158
6.4.3.11 Настройка и просмотр срабатываний журнала ... 160
6.4.4 Состояние сервера ... 161
6.4.5 Статистика ... 162
6.4.6 Валидность сертификатов ... 162
6.5 Вкладка боковой панели «Прочее» ... 163
6.5.1 Топология ... 164
6.5.1.1 Работа с контекстным меню элемента списка «Топология» ... 167
6.5.2 Карта ... 168
6.5.3 Зоны ... 169
6.5.4 Домены и учетные записи ... 170
6.5.4.1 Добавление и настройка параметров домена ... 171
6.5.4.2 Учетные записи доменов ... 172
6.5.5 Центры сертификации ... 173
6.5.5.1 Добавление центра сертификации ... 174
6.5.5.2 Добавление сертификата ... 175
6.5.5.3 Добавить дочерний ЦС ... 177
6.5.5.4 Добавление выпущенного сертификата ... 178
6.5.5.5 Импортировать сертификат или ЦС ... 178
6.5.5.6 Экспорт сертификата ... 179
6.5.6 Прокси-действия ... 180
6.5.7 Сетевые сервисы ... 181
6.5.7.1 Добавить сетевой сервис ... 182
6.5.7.2 Редактирование членов групп сетевых сервисов ... 183
6.5.7.3 Процедуры межсетевых экранов ... 184
6.5.8 Расписания ... 185
6.5.9 Текстовые данные ... 187
7 НАЧАЛО РАБОТЫ ... 189
7.1 Добавление объектов ГПБ ... 189
7.1.1 Добавление и настройка объекта типа «Подсеть» ... 189
7.1.1.1 Настройка параметров для элемента списка «Общее» ... 189
7.1.1.2 Настройка параметров для элемента списка «Топология» ... 190
7.1.1.3 Настройка параметров для элемента списка «Местоположение» ... 190

7.1.1.4 Настройка параметров для элемента списка «Входит в» ... 191
7.1.2 Добавление и настройка объекта типа «IP-диапазон» ... 192
7.1.2.1 Настройка параметров для элемента списка «Общее» ... 192
7.1.2.2 Настройка параметров для элемента списка «Топология» ... 192
7.1.2.3 Настройка параметров для элемента списка «Местоположение» ... 194
7.1.2.4 Настройка параметров для элемента списка «Входит в» ... 194
7.1.3 Добавление и настройка объекта типа «IP-хост» ... 195
7.1.3.1 Настройка параметров для элемента списка «Общее» ... 195
7.1.3.2 Настройка параметров для элемента списка «Сетевые параметры» ... 196
7.1.3.3 Настройка параметров для элемента списка «Местоположение» ... 197
7.1.3.4 Настройка параметров для элемента списка «Входит в» ... 198
7.1.4 Добавление и настройка объекта типа «Хост безопасности» ... 199
7.1.4.1 Настройка параметров для элемента списка «Общее» ... 200
7.1.4.2 Настройка параметров для элемента списка «Настройки IKE» ... 202
7.1.4.3 Настройка параметров для элемента списка «Firewall» ... 209
7.1.4.4 Настройка параметров для элемента списка «Управление» ... 211
7.1.4.5 Настройка параметров для элемента списка «Трансляция политики» ... 212
7.1.4.6 Настройка параметров для элемента списка «SNMP» ... 213
7.1.4.7 Настройка параметров для элемента списка «NetFlow» ... 214
7.1.4.8 Настройка параметров для элемента списка «SysLog» ... 215
7.1.4.9 Настройка параметров для элемента списка «Аутентификация пользователей» ... 216
7.1.4.10 Настройка параметров для элемента списка «Местоположение» ... 217
7.1.4.11 Настройка параметров для элемента списка «Входит в» ... 218
7.1.5 Добавление и настройка объекта типа «Шлюз безопасности» ... 220
7.1.5.1 Настройка параметров для элемента списка «Общее» ... 221
7.1.5.2 Настройка параметров для элемента списка «Сетевые параметры» ... 221
7.1.5.3 Настройка параметров для элемента списка «Настройки IKE» ... 223
7.1.5.4 Настройка параметров для элемента списка «Firewall» ... 229
7.1.5.5 Настройка параметров для элемента списка «Управление» ... 231
7.1.5.6 Настройка параметров для элемента списка «Трансляция политики» ... 232
7.1.5.7 Настройка параметров для элемента списка «SNMP» ... 232
7.1.5.8 Настройка параметров для элемента списка «NetFlow» ... 234
7.1.5.9 Настройка параметров для элемента списка «SysLog» ... 235
7.1.5.10 Настройка параметров для элемента списка «Аутентификация пользователей» ... 236
7.1.5.11 Настройка параметров для элемента списка «Местоположение» ... 237
7.1.5.12 Настройка параметров для элемента списка «Входит в» ... 238
7.1.6 Добавление и настройка объекта типа «Зона» ... 239
8 СОЗДАНИЕ ГЛОБАЛЬНОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ ... 241

8.1 Основные объекты ГПБ 241
8.2 Регистрация сертификатов 241
8.3 Определяемая пользователем ЛПБ 242
8.4 Построение ЛПБ для агентов 244
8.4.1 Блок «Структура ЛПБ» 246
8.5 Общие задачи 246
8.5.1 Форма для работы с сертификатами 246
8.5.1.1 Пример 1. Добавления сертификата 247
8.5.1.2 Пример 2. Импорт сертификата 248
8.5.1.3 Пример 3. Создание сертификатов 249
8.5.1.4 Пример 4. Загрузка списка сертификатов 253
8.5.2 Редактирование серверного правила 254
8.5.3 Создание и редактирование NAT-правил для шлюзов безопасности 257
8.5.4 Настройка получения обновлений агентов политики 257
8.5.5 Управляемые шлюзы безопасности (ЗАСТАВА-Офис) 258
8.5.6 Неуправляемые шлюзы безопасности 259
8.5.7 Объекты типа «Шлюз безопасности» в кластерном исполнении 259
8.5.8 Загрузка сертификатов для каждого узла кластера 261
8.5.9 Обновление шлюза безопасности в кластерном исполнении 261
8.5.10 Редактирование параметров шлюза безопасности 262
8.5.11 Работа с сообщениями SNMP 262
8.6 Объекты УЦ (ЦС) 263
8.6.1 Основные сведения 263
8.6.2 Дополнительные сведения 264
9 РАБОТА С ПРОЕКТАМИ И ГПБ 265
9.1 Работа с ГПБ и проектами 265
9.1.1 Создание нового проекта 266
9.1.1.1 Трансляция проекта 266
9.1.1.2 Активация проекта 267
9.1.2 Экспорт (сохранение) проекта 268
9.1.3 Импорт проекта 269
9.1.4 Обновление агентов 269
9.1.5 Управление дескрипторами 269
9.1.5.1 Дескрипторы агентов 269
9.1.5.2 Дескрипторы серверов 270
9.1.5.3 Прокси-дескрипторы 271
9.1.5.4 Добавление специального дескриптора 272
9.1.6 Просмотр и редактирование ЛПБ 272

9.1.6.1 Прямое редактирование ... 273
9.1.6.2 Редактирование структуры ЛПБ ... 274
9.2 Экспортирование ЛПБ ... 275
9.3 Активация ЛПБ на агентах ... 275
9.3.1 Управляемые агенты ... 276
9.3.2 Активация ... 276
9.3.3 Контроль статуса агента ... 277
10 МЕРЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ПО ЗУ ... 278
10.1 Краткий обзор проблем безопасности в ПО ЗУ ... 278
10.2 Безопасность сертификатов и ключей ... 278
10.3 Безопасность управления сетевыми соединениями ... 278
10.4 Защита данных ЛПБ ... 278
10.5 Рекомендации по политике безопасности ПО ЗУ ... 278
11 НАСТРОЙКА СЕРВЕРА ОБНОВЛЕНИЙ ... 280
11.1 Создание и настройка встроенного сервера обновления ... 280
11.1.1 Настройка обновления агента ... 283
12 ФАЙЛЫ ПАРАМЕТРОВ ... 284
12.1 Настройка лимитов времени ... 284
12.2 Опции лимитов времени ... 284
12.3 Параметры авторизации через пароль ... 284
12.4 Параметры методов аутентификации ... 285
12.5 Параметры трансляции ... 285
12.6 Другие параметры ... 285
13 УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ ... 286
ПРИЛОЖЕНИЕ 1. ПРИМЕР КОНФИГУРИРОВАНИЯ ГПБ В ПО ЗУ ДЛЯ ДВУХ АГЕНТОВ «ЗАСТАВА-ОФИС» ... 287
ПРИЛОЖЕНИЕ 2. СЕТЕВЫЕ СЕРВИСЫ И ГРУППЫ СЕТЕВЫХ СЕРВИСОВ ПО УМОЛЧАНИЮ ... 291
ПРИЛОЖЕНИЕ 3. «ПОДДЕРЖИВАЕМЫЕ ИЗДЕЛИЯ ЛИНЕЙКИ «ЗАСТАВА» ... 294
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ ... 296
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ ... 298

1 ВВЕДЕНИЕ

1.1 Общая информация

1.1.1 Назначение

ПО ЗУ выполняет функции центра управления политиками безопасности и представляет собой программу для унифицированного управления сетевой безопасностью в гетерогенных средах. Использование ПО ЗУ позволяет централизованно создавать, распределять и активировать политику сетевой безопасности для агентов в информационной (информационно-телекоммуникационной) сети, в которой установлено ПО ЗУ. Агентами для ПО ЗУ являются:

- средства вычислительной техники (СВТ) с установленными программными изделиями линейки «ЗАСТАВА-Офис», перечень которых приведён в приложении (см. Приложение 3);
- СВТ с установленными программными изделиями линейки «ЗАСТАВА-Клиент», перечень которых приведён в приложении (см. Приложение 3);
- аппаратно-программные комплексы (АПК) линейки «ЗАСТАВА», перечень которых приведён в приложении (см. Приложение 3).

ПО ЗУ 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. ПО ЗУ также определяет тип аутентификации пользователей и удаленных хостов в рамках стандартных опций IKE с использованием цифровых сертификатов или предварительно распределенных ключей.

1.1.2 Область применения

ПО ЗУ применяется для управления агентами в локальных, корпоративных и глобальных сетях, где в качестве протокола сетевого уровня используется протокол IP.

1.1.3 Ролевая модель

Ролевая модель ПО ЗУ включает в себя роли:

- удалённого (сетевого) администратора. Описание доступных для роли функций приведено в п. 1.1.3.1;
- локального (системного) администратора. Описание доступных для роли функций приведено в п. 1.1.3.2;
- администратора безопасности СКЗИ. Описание доступных для роли функций приведено в п. 1.1.3.3;

— оператора (локальный непривилегированный пользователь). Описание принципов работы пользователя с правами учётной записи оператора с ПО ЗУ приведено в документе МКЕЮ.00669-01 34 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Руководство оператора».

1.1.3.1 Функции удаленного администратора

ПО ЗУ позволяет удаленному (сетевому) администратору:

— создавать и редактировать глобальную политику безопасности (ГПБ);
— преобразовывать ГПБ в локальную политику безопасности (ЛПБ) для конкретных агентов;
— доставлять ЛПБ по защищенному каналу и активировать на агенте (по запросу или по команде ПО ЗУ) через протокол распределения политики (Policy Management Protocol - PMP), используя защищенное соединение ISAKMP/IKE SA;
— 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 ключевые носители) для того, чтобы хранить критическую информацию пользователя;
— вести файл журнала регистрации событий, контролировать события и проводить мониторинг событий системы;
— собирать Syslog-сообщения от управляемых агентов;
— хранить ГПБ и ЛПБ для агентов (т.е. наборы объектов политики и правила управления их взаимодействиями);
— экспортировать/импортировать проекты ГПБ из/в XML-файлов;
— управлять IKE CFG и расширенной аутентификацией на шлюзах безопасности;
— помещать ПО ЗУ и управляемые агенты за NAT-устройства;
— определять правила NAT, чтобы ПО ЗУ 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 ПО ЗУ через веб-протокол (HTTP/HTTPS);

— управлять политикой автоматического обновления для агентов;
— управлять качеством обслуживания (QoS) 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.).

1.1.3.2 Функции локального администратора

ПО ЗУ позволяет локальному/системному администратору:

— использовать специальные носители информации (PKCS#11-совместимые ключевые носители) для того, чтобы хранить критическую информацию пользователя;
— изменять сетевые настройки;
— создавать и задавать параметры доступа для локальных администраторов и пользователей;
— обновление ПО ЗУ;
— изменять и создавать ключевую информацию.

1.1.3.3 Функции администратора безопасности СКЗИ

ПО ЗУ позволяет администратору безопасности СКЗИ:

— использовать специальные носители информации (PKCS#11-совместимые ключевые носители) для того, чтобы хранить критическую информацию пользователя;
— изменять и создавать ключевую информацию.

2 ПОДГОТОВКА К ИСПОЛЬЗОВАНИЮ ПО

Для работы с ПО ЗУ требуется два СВТ, на которых будут работать администраторы:

— на первом СВТ - локальный (системный) администратор, осуществляющий настройки только через консоль ПО ЗУ, и администратор безопасности СКЗИ;
— на втором СВТ - удаленный (сетевой) администратор, осуществляющий настройки только через веб-интерфейс ПО ЗУ.

2.1 Системные требования к аппаратному обеспечению СВТ

Аппаратное обеспечение СВТ, на котором устанавливается ПО ЗУ, должно отвечать минимальным требованиям, представленным в таблице (см. Таблица 1).

Таблица 1 – Требования к аппаратному обеспечению для каждого исполнения ПО ЗУ

Исполнение	Требования к аппаратному обеспечению
ZM8-EL64-VF-01	– процессор эквивалентный Intel® Atom®C3758; – частота процессора 2,2 ГГц, не менее; – объем оперативной памяти 8 ГБ, не менее; – объем жесткого диска 240 ГБ, не менее; – не менее одного Ethernet-интерфейса; – наличие устройства для чтения компакт-дисков

2.2 Системные требования АРМ удаленного управления ПО ЗУ

АРМ, с которого удаленный администратор получает доступ к ПО ЗУ, должно отвечать следующим минимальным требованиям:

— процессор с архитектурой x86-64 (AMD, Intel);
— оперативная память 4 ГБ, не менее;
— объем свободного дискового пространства 32 ГБ, не менее;
— сетевой Ethernet интерфейс 100МБ/с, не менее;
— наличие веб-браузера (Microsoft Edge, Яндекс.Браузер, Google Chrome, Mozilla Firefox).

2.3 Поддерживаемые версии управляемого программного обеспечения

ПО ЗУ может управлять удалёнными маршрутизаторами, МЭ, шлюзами безопасности и VPN-клиентами различных производителей. Версии устройств/программ, которые были полностью проверены на совместимость с ПО ЗУ: агенты («ЗАСТАВА-Офис», «ЗАСТАВА-Клиент») версий 6.3 и выше см. Приложение 3.

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

2.4 Действия по приёмке

Описание действий по приёмке ПО ЗУ приведены в документе МКЕЮ.00669-01 30 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Формуляр».

2.5 Проверка контрольной суммы образа

При первом включении необходимо проверить контрольную сумму (КС) образа ПО ЗУ. Процедура проверки КС выполняется в следующей последовательности:

1) после включения ПО ЗУ дождаться появления меню загрузчика (см. Рисунок 1);

Рисунок 1 – Внешний вид меню загрузчика

2) выбрать в меню «Checksum test» и нажать клавишу <Enter>;
3) на экране появится сообщение о проверке КС образа ПО ЗУ. Дождаться окончания проверки;
4) по окончании проверки на экране появится сообщение с вычисленными КС, как представлено на рисунке (см. Рисунок 2).

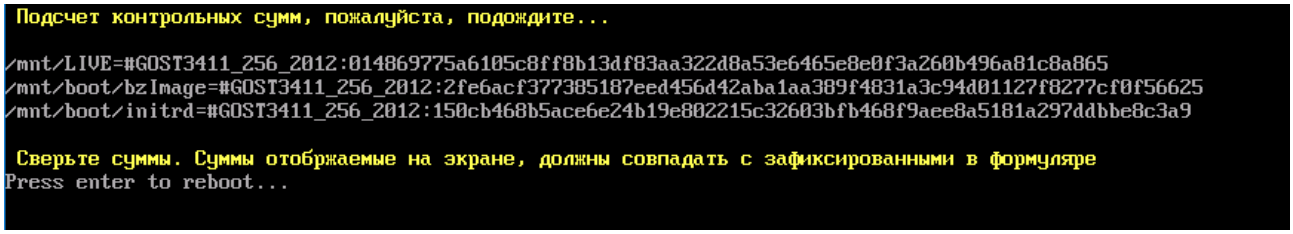


Рисунок 2 – Сообщение с вычисленными КС

2.6 Проверка контрольной суммы ПО ЗУ

Посчитать КС можно, запустив в эмуляторе терминала утилиту **icv_checker**. Далее выполнить команду:

```
icv_checker -f{полный путь к файлу дистрибутива}
```

Сверить КС, отображенную в окне эмулятора терминала, с КС дистрибутива, приведенной в документе МКЕЮ.00669-01 30 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Формуляр».

Для получения справки по работе утилиты в необходимо выполнить команду без параметров:

```
/opt/ZASTAVAmanagement/bin/icv_checker
```

2.7 Действия по безопасной установке и настройке

Действия по безопасной установке и настройке могут осуществлять администратор безопасности СКЗИ и/или локальный/системный администратор.

ПО ЗУ в исполнении ZM8-EL64-VF-01 поставляется вместе с МКЕЮ.00651-01 Программный комплекс «VPN/FW «ЗАСТАВА-Офис», версия 8 КС1» (функции которых защита СВТ с ПО ЗУ и распределение по ЛПБ агентам).

Использование ПО ЗУ должно осуществляться в соответствии с документами из комплекта поставки. Сведения о комплекте поставки приведены в документе МКЕЮ.00669-01 30 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Формуляр».

В ПО ЗУ реализованы два режима функции идентификации и аутентификации для локального/администратора и администратора безопасности СКЗИ:

— однофакторная идентификация и аутентификация (включена по умолчанию);

— двухфакторная идентификация и аутентификация.

При включенном режиме однофакторной идентификации и аутентификации локального/администратора ПО ЗУ (имя пользователя - admin) вход осуществляется на основании введенного логина и пароля.

При включенном режиме двухфакторной идентификации[1)] и аутентификации администратора ПО ЗУ вход осуществляется на основании цифрового сертификата, хранящегося на персональном идентификаторе, предъявленного ПИН-кода. Требования к персональным идентификаторам приведены в п. 2.7.1 данного документа.

Для включения режима двухфакторной идентификации и аутентификации необходимо выполнить команду:

```
enable

set 2nd_factor_authorization ESMART/RuToken
```

2.7.1 Требования к персональным идентификаторам

В ПО ЗУ в качестве персонального идентификатора используются функциональные ключевые носители (ФКН) в виде USB-токена: ESMART Token ГОСТ (форм-фактор USB) и Рутокен ЭЦП 3.0 (форм-фактор USB).

Имена пользователей зафиксированы в образе ПО ЗУ. Перед началом использования ПО ЗУ требуется сменить пароли предустановленных пользователей.

Персональный идентификатор пользователя должен содержать цифровой сертификат, имеющий следующие поля:

— Extended Key Usage (EKU), включающее в себя OID=Smart Card Logon;

— User Principal Name (UPN), равное admin@localhost (определяет роль администратора) или user@localhost (определяет роль оператора).

Перед использованием Рутокен ЭЦП 3.0 (форм-фактор USB) необходимо сменить заводской ПИН-код персонального идентификатора средствами производителя персонального идентификатора.

2.8 Действия по реализации функций безопасности среды функционирования

Для обеспечения выполнения функций безопасности в среде функционирования ПО ЗУ должны выполняться требования к внешним мерам безопасности, а именно:

[1)] Включение режима двухфакторной аутентификации является обязательным.

- должны быть обеспечены установка, конфигурирование и управление ПО ЗУ в соответствии с эксплуатационной документацией;
- персонал, ответственный за функционирование ПО ЗУ, должен обеспечивать функционирование ПО ЗУ, руководствуясь эксплуатационной документацией;
- должны быть обеспечены совместимость компонентов ПО ЗУ с компонентами СВТ информационной системы, а также необходимые ресурсы для выполнения функций безопасности ПО ЗУ (в том числе изоляция данных и процессов ПО ЗУ от иных данных и процессов СВТ, на котором он функционирует);
- должно быть обеспечено функционирование ПО ЗУ в среде, сертифицированной на соответствие требованиям безопасности информации по соответствующему классу защиты управляющего ПО или в среде, защищенной путем принятия мер для защиты информации, соответствующих классу защищенности информационной системы (автоматизированной системы управления), для использования в которой предназначается ПО ЗУ;
- должна быть исключена возможность использования не прошедших сертификацию компонентов программно-технического средства, в которое интегрировано ПО ЗУ, с иными видами средств защиты информации при его эксплуатации;
- доступ пользователя к функциям безопасности осуществляется двумя способами. Первый способ: локальный доступ через программу эмулятора терминала осуществляется администратором при личном физическом доступе к изделию. Второй способ: удалённый доступ по каналу, защищённому при помощи СКЗИ;
- локальный/системный администратор должен выполнить конфигурирование защищённого соединения с сервером управления согласно эксплуатационной документации;
- в состав ПО ЗУ входят средства контроля целостности (cspvpn_verify, stverify). Целостность критически важных файлов контролируется автоматически при помощи этих средств. Локальный/системный администратор может дополнить перечень контролируемых файлов. Администратору предписано выполнять периодический контроль целостности ПО ЗУ в соответствии с документацией из комплекта поставки.

2.9 Работа с сертификатами и ключами

2.9.1 Свойства сертификата и его проверка

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

```
vpnconfig –list cert
```

Затем выполнить команду:

```
vpnconfig –view cert <id>
```

В результате будет выведена полная информация о свойствах сертификата и его цепочке доверия, т.е. список удостоверяющих центров (УЦ), подтверждающих подлинность сертификата. Обычно нет необходимости проверять сертификат вручную, поскольку после получения сертификата от партнёра по связи через протокол IKE сертификат всегда проверяется автоматически. Однако ручная проверка сертификата полезна, когда возникают проблемы при создании защищенного соединения с данным партнёром связи. Описание всех свойств сертификата представлено в таблице (см. Таблица 2).

Таблица 2 – Свойства сертификата

Свойство	Описание
Version	Версия формата сертификата
Серийный номер	Серийный номер сертификата
Issuer	Кем выдан сертификат
Subject	Содержит отличительное имя субъекта, то есть владельца закрытого ключа, соответствующего открытому ключу данного сертификата
Sign Algorithm	Алгоритм цифровой подписи сертификата
Key Algorithm	Тип открытого ключа (алгоритм цифровой подписи и длина)
Public Key	Значение открытого ключа
Действителен с	Начальная дата действия сертификата
Действителен до	Конечная дата действия сертификата
Authority Key Identifier	Идентификатор ключа издателя, помогает определить правильный ключ для верификации подписи на сертификате
Subject Key Identifier	Идентификатор ключа субъекта, используется для того, чтобы различать ключи подписи в сертификатах одного и того же владельца
Key Usage	Назначение ключа
Ext. Key Usage	Расширенное назначение ключа
CRL Distribution Points	Точки распространения списков отозванных сертификатов (СОС), указанные в данном сертификате. Для каждой точки распространения отображается следующая информация: DP[N] "<DP Value>", CRLI[N] "<Issuer Value>", где: N – номер точки распространения; <DP Value>- месторасположение точки, где можно получить СОС; <Issuer Value>- имя организации, выпустившей СОС
Authority Info Access	Способ доступа к информации УЦ
Fingerprint (md5)	Хэш-сумма сертификата, вычисляемая по алгоритму md5
Fingerprint (sha1)	Хэш-сумма сертификата, вычисляемая по алгоритму sha1

Пример вывода цепочки доверия сертификата:

```
.-+- E=info@cryptopro.ru,C=RU,O=CRYPTO-PRO,CN=Test Center CRYPTO-PRO

   .--- C=RU,L=Moscow,O=ELVIS-PLUS,OU=TC,CN=CLIENT-LINUX
```

2.9.2 Регистрация сертификата

ПО ЗУ поддерживает возможность регистрации нескольких сертификатов типа X.509:

— доверенные сертификаты самоподписанные;

— доверенные сертификаты промежуточные;

— сертификаты с ключом (personal);

— сертификаты партнёров по связи (other).

Для работы с сертификатами требуется обеспечить доступ к контейнеру ключевой информации. Для этого необходимо:

1) выполнить команду:

```
vpnconfig list token
```

найти в появившемся списке ключевой носитель «ELVIS-PLUS CSP token» и запомнить его ID (по умолчанию 0);

2) выполнить команду:

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

где: <pin> – ПИН-код пользователя к ключевому носителю (по умолчанию 12345678), <token_id> - ID для «ELVIS-PLUS CSP token», ключ «save» нужен для автоматического доступа в ключевом носителе после перезапуска;

3) необходимо убедится, что вход в ключевой носитель «ELVIS-PLUS CSP token» осуществлён, ПИН-код сохранён и датчик случайных чисел проинициализирован (убедиться в наличии строк в отображаемом сообщении «Logged In: YES, PIN-code saved» и «RNG»: Initialized).

```
#vpnconfig –list token
Token
  Id: 0
  Label: ELVIS-PLUS CSP token
  Model: InternalCrypto
  Manufacturer: ELVIS-PLUS
  Serial Number: 18042017
  Logged In: YES, PIN-code saved
  Trusted: Yes
  Login required: Yes
  RNG: Initialized
  Algorithms:
```

```
    GOST R 34.10-2001
      Key Length: 512
      Hash Algorithms: GOST 34.11-94
    GOST R 34.10-2012 512
      Key Length: 1024
      Hash Algorithms: GOST 34.11-2012 512
    GOST R 34.10-2012 256
      Key Length: 512
      Hash Algorithms: GOST 34.11-2012 256
```

Чтобы зарегистрировать новый сертификат УЦ или промежуточный сертификат УЦ в ПО ЗУ, необходимо произвести следующие действия:

1) выполнить команду:

```
vpnconfig –add cert <file>
```

2) при импортировании сертификата необходимо ввести SO ПИН-код (ПИН-код администратора) ключевого носителя (по умолчанию 12345678). После ввода ПИН-кода нужно нажать клавишу <Enter>; в случае ввода корректных ПИН-кода и пароля появится сообщение, сигнализирующее об успешной регистрации сертификата:

```
Certificate is imported
```

Чтобы импортировать новый персональный сертификат, необходимо произвести следующие действия:

1) выполнить команду:

```
vpnconfig –add cert <path> password [<password>]
```

где: [<password>] – пароль доступа к PKCS#12 контейнеру;

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

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

2.9.3 Удаление сертификата

Для удаления выбранного сертификата необходимо узнать id сертификата, который необходимо удалить. Для этого нужно воспользоваться командой:

```
vpnconfig –list cert
```

После этого необходимо выполнить команду:

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

При удалении сертификата требуется ввод пользовательского ПИН-кода. Для удаления доверенных сертификатов потребуется ввод ПИН-кода администратора ключевого носителя.

2.9.4 Создание запроса PKCS10 на выпуск сертификата

Для создания запроса на выпуск сертификата используются встроенные возможности в ПО «ЗАСТАВА-Офис». Для создания запроса необходимо указать носитель, на котором будет создан ключевой контейнер.

Общий вид команды выглядит следующим образом:

```
vpnconfig -add request <token_id> <key_algorithm> <key_length> <hash_algorithm> <subject> [ip=<ip-address>] [dns=<dns>] [email=<e-mail>] [upn=<upn>] [eku=ipsec|sclogin] [noexport] [cms [signer=<dn>]]
```

Параметры, заключенные в прямоугольные скобки, кроме eku=ipsec, которой необходимо указывать всегда, не являются обязательными. Описание параметров представлено в таблице (см. Таблица 3).

Таблица 3 – Описание параметров команды «vpnconfig -add request»

Ключ	Описание действия
token_id	Указать используемый ключевой носитель
key_algorithm	Указать используемый алгоритм
key_length	Указать длину ключа
hash_algorithm	Указать используемый хэш алгоритм
subject	Указать информацию о владельце сертификата: C= Country Code, ST=State, L=Locality, O=Organization, OU=Organizational Unit, T=Title, CN=Common Name
<ip-address> <dns> <e-mail> <upn>	Опциональные поля AltSubjectName
eku	Указать область использования сертификата «IKE/IPsec» или «Smart Card Login»
noexport	Указать возможность экспорта сертификата
cms	Создать запрос на подпись в формате cms
signer	Указать субъект сертификата. Если параметр не указан, то будет использоваться значение из локальных настроек

Для просмотра доступных ключевых носителей (InternalCrypto, ESMARTToken GOST, Rutoken ECP) необходимо ввести команду:

```
vpnconfig list token
```

Поддерживаемые алгоритмы шифрования будут отображены в тексте сообщения в разделе «Algorithms»:

```
Token
  Id: 0
  Label: ELVIS-PLUS CSP token
  Model: InternalCrypto
  Manufacturer: ELVIS-PLUS
  Serial Number: 18042017
  Logged In: Yes, PIN-code saved
  Trusted: Yes
  Login required: Yes
  RNG: Initialized
  Algorithms:
    GOST R 34.10-2001
      Key Length: 512
      Hash Algorithms: GOST 34.11-94
    GOST R 34.10-2012 512
      Key Length: 1024
      Hash Algorithms: GOST 34.11-2012 512
    GOST R 34.10-2012 256
      Key Length: 512
      Hash Algorithms: GOST 34.11-2012 256


Token
  Id: 1
  Label: Internal
  Model: ESMARTToken GOST
  Manufacturer: ISBC
  Serial Number: 34600EE204084204
```

```
  Logged In: No
  Trusted: Yes
  Login required: Yes
  RNG: Initialized
  Algorithms:
    RSA
      Key Length: 1024
      Hash Algorithms: SHA1, MD5, SHA256, SHA224, SHA384, SHA512
    GOST R 34.10-2001
      Key Length: 512
      Hash Algorithms: GOST 34.11-94
    ECDSA
      Key Length: 192, 224, 256, 384, 521
      Hash Algorithms: SHA1, SHA256, SHA224, SHA384, SHA512
    GOST R 34.10-2012 256
      Key Length: 512
      Hash Algorithms: GOST 34.11-2012 256
Token
  Id: 2
  Label: Рутокен ЭЦП 3.0
  Model: Rutoken ECP
  Manufacturer: Aktiv Co.
  Serial Number: 424f84a2
  Logged In: No
  Trusted: Yes
  Login required: Yes
  RNG: Initialized
  Algorithms:
```

```
RSA
  Key Length: 1024, 2048, 4096
  Hash Algorithms: MD5, SHA1, SHA224, SHA256, SHA384, SHA512
GOST R 34.10-2001
  Key Length: 512
  Hash Algorithms: GOST 34.11-94
GOST R 34.10-2012 512
  Key Length: 1024
  Hash Algorithms: GOST 34.11-2012 512
ECDSA
  Key Length: 192, 224, 256, 384, 521
  Hash Algorithms: SHA1, SHA224, SHA256, SHA384, SHA512
GOST R 34.10-2012 256
  Key Length: 512
  Hash Algorithms: GOST 34.11-2012 256
```

Примеры команды создания ключей и запросов на издание сертификата с разной длиной ключа для защищённых соединений:

```
vpnconfig add request 0 "GOST R 34.10-2012 256" 512 "GOST 34.11-2012 256" "C=RU,OU=PO,CN=APK-150-key256" eku=ipsec

vpnconfig add request 0 "GOST R 34.10-2012 512" 1024 "GOST 34.11-2012 512" "C=RU,OU=PO,CN=APK-150-key512" eku=ipsec
```

Пример команды создания ключа и запроса на издание сертификата на отчуждаемом носителе Рутокен ЭЦП 3.0 для входа в ПО ЗУ:

```
vpnconfig add request 2 "GOST R 34.10-2012 256" 512 "GOST 34.11-2012 256" "C=RU,ST=77 Москва,L=Город или населённый пункт,O=ООО \\\"Имя организации\\\",OU=Подразделение,GN=Иванов,SN=Иван Иванович,CN=Администратор ПК,E=user@domain.net" eku=sclogin upn=admin@localhost
```

Пример выше дан с заполнением всех возможных полей «Subject». Количество полей «Subject» может быть сокращено. Для использования в полях кавычек требуется применять знаки

экранирования \\\ (три подряд обратные косые черты). При использовании eku=sclogin поле «upn» не должно быть пустым.

После создания ключевого контейнера на экране монитора будет отображен BASE64-запрос на выпуск сертификата. Для сохранения текста запроса в файл необходимо воспользоваться перенаправлением вывода после команды на создание запроса:

```
<текст запроса> > <адрес файла для сохранения>
```

Файл для сохранения запроса рекомендуется располагать в директории /home/admin. Ниже приведён пример текста сохранённого запроса.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICmTCCAkYCAQAwggFAMQswCQYDVQQGEwJSVTEYMBYGA1UECAwPNzcg0JzQvtGB
0LrQstCwMTowOAYDVQQHDDHQk9C+0YDQvtC0INC40LvQuCDQvdCw0YHQtdC70ZHQ
vdC90YvQuSDQv9GD0L3QutGCMS8wLQYDVQQKDCbQntCe0J4gItCY0LzRjyDQvtGA
0LPQsNC90LjQt9Cw0YbQuNC4IjEjMCEGA1UECwwa0J/QvtC00YDQsNC30LTQtdC7
0LXQvdC40LUxFTATBgNVBCoMDNCY0LLQsNC90L7QsjEiMCAGA1UEBAwZ0JjQstCw
0L0g0JjQstCw0L3QvtCy0LjRhzEqMCgGA1UEAwwh0JDQtNC80LjQvdC40YHRgtGA
0LDRgtC+0YAg0JDQn9CaMR4wHAYJKoZIhvcNAQkBFg91c2VyQGRvbWFpbi5uZXQw
ZjAfBggqhQMHAQEBATATBgcqhQMCAiMBBggqhQMHAQECAgNDAARAtUeSOECaj1+U
LNFUma0mJk340WOSOBjDeabeDFkkPu92Pp7EtdCuetvZgmEX5FCNscv6AoO7ewZH
XRY2cPA05qCBlDCBkQYJKoZIhvcNAQkOMYGDMIGAMA4GA1UdDwEB/wQEAwIFoDAV
BgNVHSUEDjAMBgorBgEEAYI3FAICMCoGA1UdEQQjMCGgHwYKKwYBBAGCNxQCA6AR
DA9hZG1pbkBsb2NhbGhvc3QwKwYDVR0QBCQwIoAPMjAyMzA4MzAxMzQxMDVagQ8y
MDI0MTEzMDEzNDEwNVowCgYIKoUDBwEBAwIDQQARQLAc52wTDwayStDSkDLdFEnO
R3sif3EcuCKU3TzhQ5frNQiyP2JYCiQDX5ZT7byC6KBE/ANa7kToQc32GrnE
-----END CERTIFICATE REQUEST-----
```

После создания запроса в базе сертификатов агента ПО ЗУ появится запись:

```
Certificate
  Id: 0/1
  Type: personal
  Subject: Key Pair without Certificate
```

```
  Issuer:
  Device Name: Рутокен ЭЦП 3.0
  Expiration Date: Error time
  Algorithm: GOST R 34.10-2012 256
        Possible Id Types: DN
```

2.10 Способ извлечения запроса использования Secure Copy Protocol (SCP)

После выпуска ключевым или УЦ сертификата необходимо импортировать его в ПО ЗУ и прикрепить к контейнеру ключевой пары, для этого ввести команду:

```
vpnconfig add cert <путь_к_сертификату> pin <pin_токена>  token <token id>
```

Пример сообщения на введённую команду:

```
Import certificate 'C=RU,ST=77 Москва,L=Город или населённый пункт,O=ООО \"Имя организации\",OU=Подразделение,CN=Администратор ПК,E=user@domain.net'
  to token 'Рутокен ЭЦП 3.0'...
Certificate is imported.
```

2.11 Компрометация ключей аутентификации

Скомпрометированные ключи подлежат замене с отзывом соответствующих им цифровых сертификатов путём включения сведений об отзываемых цифровых сертификатах в СОС УЦ.

В случае компрометации ключей аутентификации необходимо:

1) назначить ответственного за расследование инцидента;
2) в случае компрометации ключей для VPN необходимо выпустить новую ключевую информацию для VPN;
3) в случае компрометации ключей для входа в операционную систему (ОС) необходимо отправить ПО ЗУ предприятию-изготовителю на восстановление. Контактная информация предприятия-изготовителя приведена в документе МКЕЮ.00669-01 30 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Формуляр».

В случае утери ключевого носителя:

1) сообщить предприятию-изготовителю о факте утери. Контактная информация предприятия-изготовителя приведена в документе МКЕЮ.00669-01 30 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Формуляр»;
2) заказать новый ключевой носитель;
3) сменить все пароли, заданные на ПО ЗУ;
4) применить организационно-технические меры для обеспечения недоступности серверов для любых лиц;
5) если ключевой носитель найдется, его нужно отформатировать и сделать новый запрос на выпуск сертификата и передать его доверенным способом для процедуры подписи.

2.12 Рекомендации по безопасной настройке и конфигурированию ПО ЗУ

Рекомендации по безопасной настройке и конфигурированию ПО ЗУ:

1) установка, настройка и конфигурирование ПО ЗУ на аппаратную серверную платформу должны осуществляться исключительно Системным программистом - администратором безопасности СКЗИ в соответствии с требованиями документов МКЕЮ.00669-01 93 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Правила пользования» и МКЕЮ.00669-01 32 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Руководство системного программиста»;
2) на средствах СВТ, предназначенных для установки и эксплуатации ПО ЗУ, должно быть **ЗАПРЕЩЕНО** размещение и/или наличие средств разработки и отладки ПО;
3) установка ПО ЗУ на СВТ должна производиться только с дистрибутивов, полученных по доверенному каналу одним из способов, описанных в разделе 2 документа МКЕЮ.00669-01 93 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Правила пользования»;
4) установка интерфейса графического управления и интерфейса командной строки, входящих в состав программных модулей сервера управления ПО ЗУ, должна осуществляться на отдельные СВТ класса «Персональный компьютер». Порядок установки и настройки интерфейса графического управления и интерфейса командной строки на отдельном СВТ описан в настоящем документе. Эксплуатация указанного СВТ должна осуществляться с учетом выполнения требований п. 4.5.5 МКЕЮ.00669-01 93 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Правила пользования»;

5) линия связи между аппаратно-программной платформой ПОЗУ и удаленным отдельным СВТ, на котором установлены интерфейс графического управления и интерфейс командной строки, должна быть реализована в одном из следующих видов:

— находиться в пределах контролируемой зоны объекта информатизации, на котором указанные средства размещаются, и способ ее прокладки должен обеспечивать возможность визуального контроля и осмотра в целях защиты от несанкционированных подключений;

— информация, циркулирующая между серверной частью ПК и удаленным отдельным СВТ, должна защищаться криптографическими методами применением программных, программно-аппаратных или аппаратно-программных СКЗИ, производимых АО «ЭЛВИС-ПЛЮС», класса защищенности КС1 и выше;

6) в ПО ЗУ должен быть настроен механизм автоматического контроля целостности программных модулей путём запуска по расписанию утилиты ***icv_checker*** с файлом шаблона контроля целостности;

7) Для обеспечения защиты ПК от НСД при реализации ролевой модели должен быть настроен в соответствии с требованиями документа МКЕЮ.00669-01 32 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Руководство системного программиста» режим двухфакторной аутентификации, при котором доступ к загрузке ОС предоставляется на основании сертификата X.509, хранящегося на ключевом носителе и PIN-кода к этому носителю;

8) настройка параметров мониторинга, протоколирования, аудита и анализа системных событий в ПО ЗУ должны осуществляться в соответствии с требованиями и рекомендациями настоящего документа;

9) при настройке, конфигурировании и создании политики безопасности ПО ЗУ Системный программист - администратор безопасности СКЗИ должен руководствоваться следующими требованиями:

— атрибуту ***cipher*** в структуре ***proto_ike*** должно быть присвоено одно из следующих значений: ***«GR3412_2015_KD-H96-MGM»*** или ***«GR3412_2015_MD-H64-MGM»***;

— атрибуту ***group*** в структуре ***proto_ike*** должно быть присвоено значение «***GR34102012_256***» при использовании атрибуту ***cipher*** со значением ***«GR3412_2015_MD-H64-MGM»***;

— атрибуту ***group*** в структуре ***proto_ike*** должно быть присвоено значение «***GR34102012_256***» или «***GR34102012_512***» при использовании атрибуту ***cipher*** со значением ***«GR3412_2015_KD-H64-MGM»***;

— атрибуту ***prf*** в структуре ***proto_ike*** должно быть присвоено значение ***«GR34112012_512-HMAC»***;

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

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

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

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

10) при необходимости обеспечить совместимость ПО ЗУ с сертифицированными программными, программно-аппаратными и аппаратно-программными изделиями типа «VPN/FW «ЗАСТАВА», версия 6»[2)] производства АО «ЭЛВИС-ПЛЮС» при настройке, конфигурировании и создании политики безопасности администратор безопасности СКЗИ должен руководствоваться следующими требованиями:

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

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

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

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

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

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

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

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

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

Примечания.

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

11) при настройке, конфигурировании и создании политики безопасности средств межсетевого экранирования ПК **ЗАПРЕЩАЕТСЯ** использовать режим ***«Pass All»*** по умолчанию;

12) после установки ПО ЗУ на аппаратную серверную платформу, его настройки и проверки работоспособности должно быть проведено опечатывание системного блока СВТ, на котором установлено и функционирует ПК. Размещение печати должно позволять визуально контролировать вскрытие системного блока и исключать возможность бесконтрольного изменения аппаратной среды функционирования ПО ЗУ.

3 ПОДГОТОВКА К РАБОТЕ И БЫСТРЫЙ СТАРТ

3.1 Вход в ПО ЗУ локального/системного администратора

Для входа в терминал ПО ЗУ необходимо:

1) включить СВТ с установленным ПО ЗУ, нажав кнопку питания , дождаться появления меню выбора вариантов загрузки «ZASTAVA OS»;
2) выбрать в меню «ZASTAVA OS» и нажать клавишу <Enter>;
3) по окончании проверки будет отображено сообщение о вычисленных КС, а также о их соответствии или несоответствии эталонным значениям;
4) сверить вычисленные КС с указанными в документе МКЕЮ.00669-01 30 01 «Программный комплекс «ЗАСТАВА-Управление», версия 8 КС1» (исполнение ZM8-EL64-FV-01). Формуляр».

3.1.1 Смена пароля

Для смены пароля текущей учётной записи ввести команду:

```
> password
```

Запустится диалог:

```
Смена пароля для [user | admin].

Текущий пароль:

Новый пароль:

Повторите ввод нового пароля:
```

При успешной смене пароля выводится сообщение:

```
passwd: пароль успешно обновлён
```

При несовпадении паролей при задании нового пароля:

```
Извините, но пароли не совпадают.

passwd: Службе паролей не удалось выполнить предварительную проверку.

passwd: Пароль не изменён
```

При задании нового пароля, равного текущему, отобразится сообщение:

```
passwd: Пароль не изменён
```

3.2 Инициализация криптопровайдера «Элвис-Крипто»

Для инициализации криптопровайдера «Элвис-Крипто» необходимо выполнить команды:

```
enable

vpnconfig initrng elvis_token
```

Далее необходимо нажимать в случайном порядке клавиши на клавиатуре до тех пор, пока строка прогресса не заполнится полностью (см. Рисунок 3).

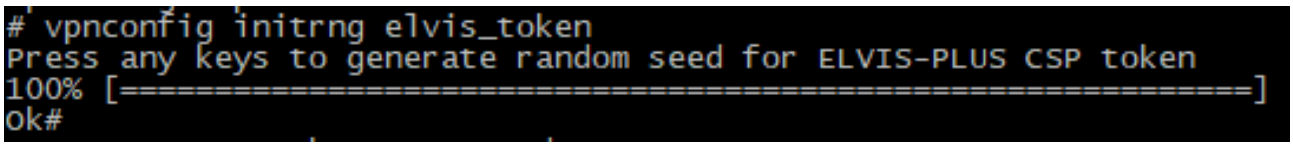


Рисунок 3 – Инициализация криптопровайдера «Элвис-Крипто»

3.3 Настройка сетевых параметров

Настройка сетевых параметров включает настройку IP-адреса, dns, ntp и, при необходимости, настройку таблицы маршрутизации.

Настройка сетевых параметров выполняется в командной оболочке KLISH. Для перехода в режим администрирования KLISH требуется войти с использованием данных учётной записи администратора (admin) и выполнить команду:

```
     > enable
```

3.3.1 Настройка адресации

Для настройки статического IP-адреса необходимо выполнить команды:

```
network connection add type ethernet con-name <название соединения> ifname <название физического интерфейса>

network connection modify <название соединения> ipv4.addresses <ip адрес/маска>

network connection modify <название соединения> ipv4.method manual

network connection modify <название соединения> autoconnect yes
```

Для настройки получения IP-адреса по DHCP необходимо выполнить команды:

```
network connection add type ethernet con-name <название соединения> ifname <название физического интерфейса>

network connection modify ipv4.addresses <ip адрес/маска>
```

```
network connection modify <название соединения> ipv4.method – auto
network connection modify <название соединения> autoconnect yes
```

3.3.2 Настройка маршрутизации

Для задания параметров маршрутизации необходимо выполнить:

```
network connection modify <название соединения> +ipv4.routes <ip-адрес/маска> <ip-адрес шлюза>
```

Для задания адреса шлюза необходимо выполнить:

```
network connection modify <название соединения> ipv4.gateway <ip-адрес>
```

3.3.3 Настройка DNS

Для добавления DNS-сервера необходимо выполнить:

```
network connection modify <название соединения> +ipv4.dns <IP адрес>
```

Для удаления DNS-сервера необходимо выполнить:

```
network connection modify <название соединения> -ipv4.dns <IP адрес>
```

3.3.4 Применение настроек

Для того чтобы заданные настройки успешно применились, необходимо выполнить:

```
network connection up <название соединения>
```

3.3.5 Проверка корректности и завершение установки

Проверить сетевую связность можно, выполнив команду в программе эмулятора терминала на АРМ удалённого администратора:

```
ping <IP-адрес СВТ с установленным ПО ЗУ>
```

После успешной проверки сетевого доступа командой «ping» необходимо открыть веб-браузер и в строке URI ввести:

```
http://<IP-адрес СВТ с установленным ПО ЗУ>:8088
```

В появившемся запросе на авторизацию ввести имя пользователя «admin», пароль «admin».

Для настройки своего IP-адреса для доступа необходимо:

1) в режиме «enable» ввести команду «network connection show», которая выведет на экран монитора список сетевых соединений, доступных для настройки (каждое из

сетевых соединений, кроме «managed», настроено на получение IP-адреса по DHCP);

2) для того чтобы настроить статический IP-адрес на выбранном сетевом соединении, необходимо ввести команду «network connection modify» eth0 ipv4.addresses «IP-адрес/маска» (Network connection modify «имя соединения», ipv4.addresses «IP-адрес/маска»);
3) изменить способ получения IP-адреса на статический при помощи команды «network connection modify» «имя соединения» ipv4.method manual;
4) соединить соответствующий настройке сетевой интерфейс и интерфейс имеющегося АРМ и настроить на нем IP-адрес из заданной ранее сети;
5) проверить сетевую связность, выполнив команду «ping» на АРМ управления, откуда планируется осуществлять доступ к веб-интерфейсу ПО ЗУ;
6) после успешного завершения команды «ping» необходимо открыть веб-браузер и в строке URI ввести http://"заданный_ранее_IP":8088;
7) в появившемся запросе на авторизацию ввести имя пользователя «admin» пароль «admin».

3.3.6 Ввод файла с лицензией

Для введения файла лицензии необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 4).

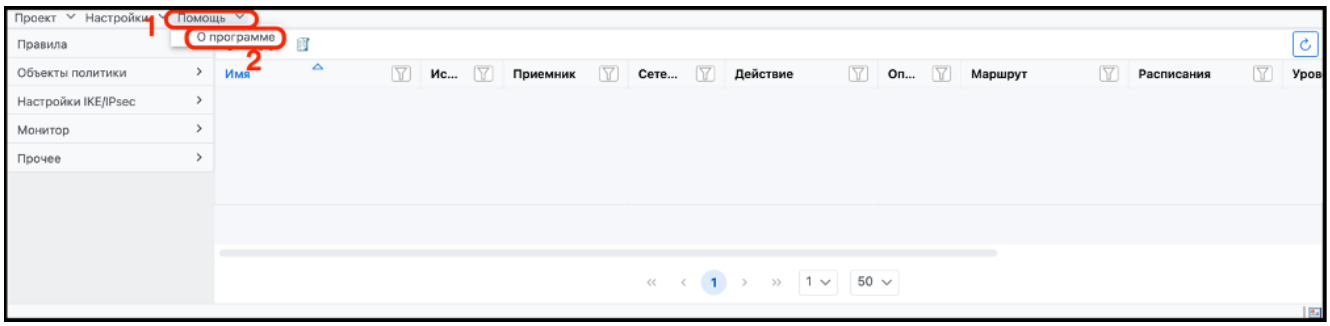


Рисунок 4 – Вкладка меню «Помощь»

Перейти во вкладку меню «Помощь» (цифра 1) и нажать команду «О программе» (цифра 2). В открывшемся окне отобразятся информация о программе и кнопка активации лицензии, изображенные на рисунке (см. Рисунок 5).

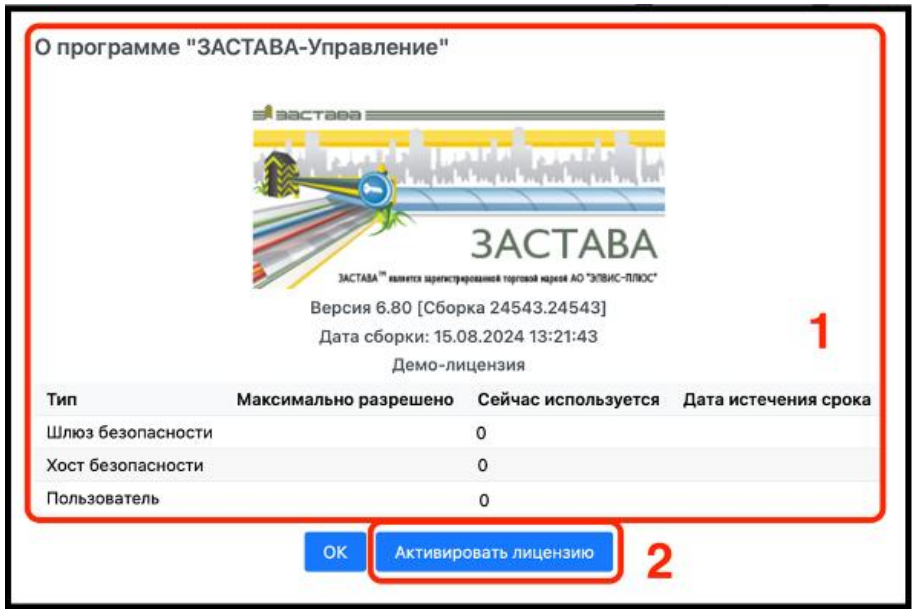


Рисунок 5 – Сведения о программе

Сведения о текущей версии ПО ЗУ и параметры зарегистрированной лицензии, включая её срок действия (цифра 1). Для активирования лицензии требуется нажать кнопку «Активировать лицензию» (цифра 2). В открывшемся окне выполнить шаги, изображенные на рисунке (Рисунок 6).

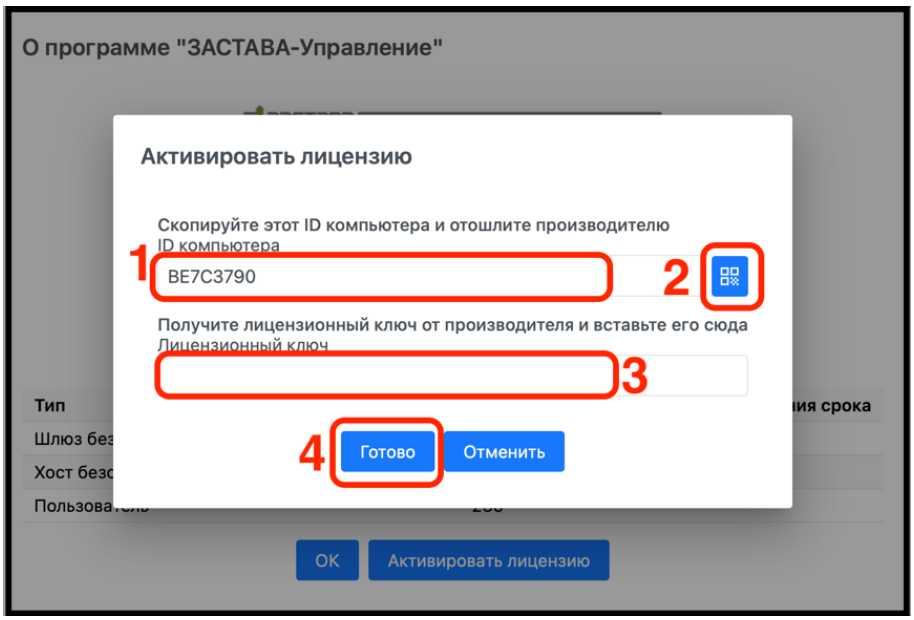


Рисунок 6 – Активация лицензии

Скопировать ID СВТ (цифра 1) или QR код (цифра 2), получить лицензионный ключ от предприятия-изготовителя ПО ЗУ и вставить его в строку (цифра 3). Нажать кнопку «Готово» (цифра 4).

3.3.7 Настройка «ЗАСТАВА-Офис»

На данном этапе будет предложено сконфигурировать «ЗАСТАВА-Офис», который был установлен вместе с ПО ЗУ. Этот процесс включает в себя указание идентификатора локального

сертификата, который будет использоваться в ПО ЗУ (данное действие имеет смысл в том случае, если в «ЗАСТАВА-Офис» импортировано более одного локального сертификата).

Если в хранилище сертификатов уже есть установленные сертификаты, то необходимо выбрать соответствующий для доступа к серверу политик. В случае если установленных сертификатов нет, список будет пустым. Добавить сертификаты можно будет позже вручную.

Без конфигурирования «ЗАСТАВА-Офис» активация ГПБ в ПО ЗУ будет невозможна. Регламентный контроль целостности не реже, чем раз в месяц.

4 ОБЗОР ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА

4.1 Общий вид веб-интерфейса ПО ЗУ

ПО ЗУ представляет собой пользовательский веб-интерфейс, реализующий следующие функции:

— работы с проектами и ГПБ;
— манипуляции с объектами ГПБ;
— просмотр журналов;
— мониторинг состояния объектов информационно-телекоммуникационной системы.

Вид окна веб-интерфейса ПО ЗУ представлен на рисунке (см. Рисунок 7).

Рисунок 7 – Внешний вид веб-интерфейса ПО ЗУ

Панель вкладок меню (цифра 1). Боковая панель вкладок (цифра 2). Инструментальная линейка (цифра 3). Рабочая область таблицы (цифра 4).

4.2 Элементы управления в веб-интерфейсе

4.2.1 Инструментальная линейка

В окне веб-интерфейса ПО ЗУ отображается инструментальная линейка с быстрым доступом к часто используемым инструментам. Для каждой вкладки будет отображаться свой набор инструментов, представленный на рисунке (см. Рисунок 8).

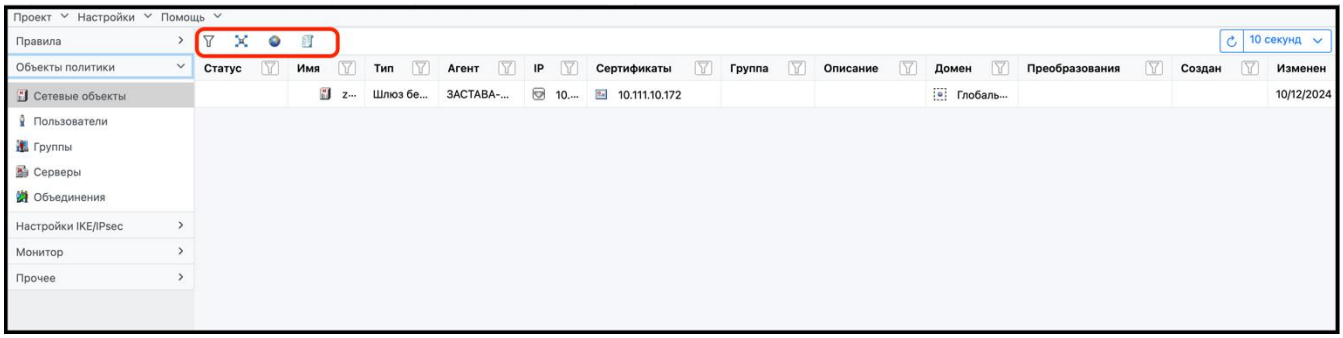


Рисунок 8 – Инструментальная линейка

Доступные опции, отображаемые в контекстных меню, представлены в таблице (см. Таблица 4).

Таблица 4 – Описание доступных элементов контекстных меню

Элемент	Характеристика
	Фильтр (состояние «Нет заданных фильтров»)
	Фильтр (состояние «Осуществляется фильтрация»)
	Фильтр (состояние «Не найдено»)
	Показать топологию
	Показать лог
	Показать карту
	Показать иерархический список
	Валидность сертификатов

4.2.1.1 Инструмент «Фильтр»

Инструмент «Фильтр» используется для настройки поиска сетевых объектов, групп, связанных с конкретным объектом. Для каждой вкладки предлагается свой набор фильтрации. Настройки инструмента «Фильтр» представлены на рисунке (см. Рисунок 9).

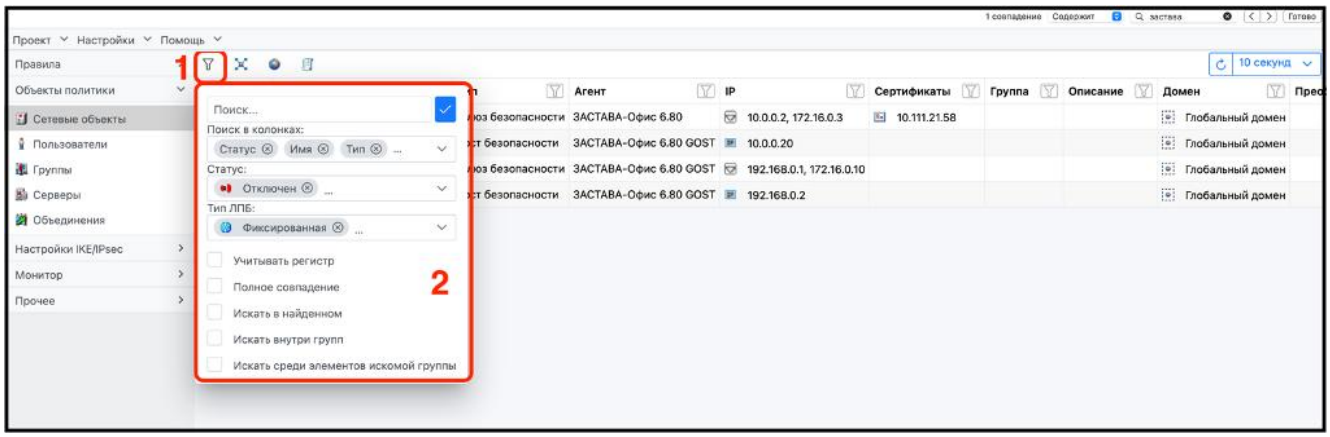


Рисунок 9 – Инструмент «Фильтр»

Для настройки поиска требуется перейти в фильтр, нажав на элемент « » (цифра 1), в открывшемся блоке настроек (цифра 2) выбрать требуемые атрибуты поиска.

Для удобной и быстрой фильтрации можно настроить рабочую область таблицы, выполнив шаги, указанные на рисунке (см. Рисунок 10).

Рисунок 10 – Фильтр «Поиск»

В строке «Поиск» задать значение фильтрации (цифра 1) и нажать на элемент «» (цифра 2). На панели инструментов элемент « » «Нет заданных фильтров» перейдет в режим «Осуществляется фильтрация» и изменит свой вид на « » (цифра 3), в строке поиска появится элемент «» «Очистить фильтр» (цифра 4), на панели инструментов также отобразится элемент « » «Не найдено» (цифра 5). Далее требуется настроить поиск в колонках, выполнив шаги, указанные на рисунке (см. Рисунок 11).

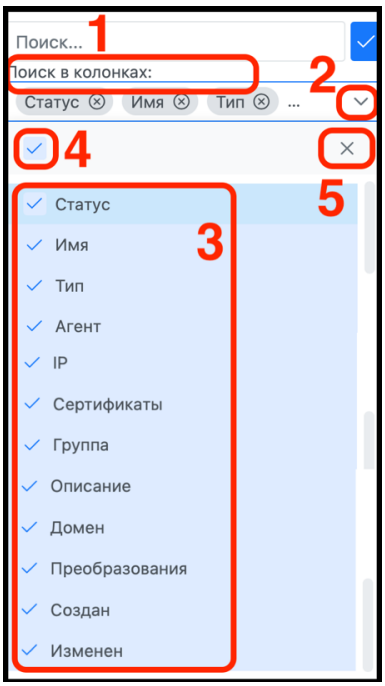


Рисунок 11 – Фильтр «Поиск в колонках»

В выпадающем списке «Поиск в колонках» (цифра 1) открыть список доступных атрибутов фильтрации с помощью элемента «» (цифра 2), установив или сняв напротив выбранных атрибутов флажок (наличие флажка делает атрибут выбранным) (цифра 3).

Одновременно активировать или деактивировать все атрибуты списка параметров можно, установив флажок (цифра 4). Выйти из режима «Поиск в колонках» можно с помощью

элемента «×» (цифра 5). Назначить статус фильтрации, выполнив шаги, указанные на рисунке (см. Рисунок 12).

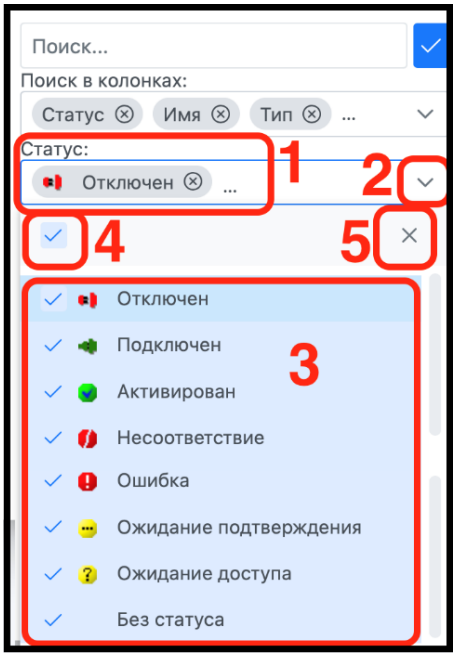


Рисунок 12 – Фильтр «Статус»

В выпадающем списке «Статус» (цифра 1) открыть список доступных атрибутов фильтрации с помощью элемента «✓» (цифра 2), установив или сняв напротив выбранных атрибутов флажок (наличие флажка делает атрибут выбранным) (цифра 3).

Возможные значения статусов пиктограмм объектов политики:

— « » – «Активирован»;

— « » – «Ожидание подтверждения»;

— « » – «Ожидание доступа»;

— « » – «Ошибка»;

— « » – «Подключен»;

— « » – «Несоответствие»;

— « » – «Без статуса»;

— « » – «Отключен».

Одновременно активировать или деактивировать все атрибуты списка можно, установив флажок (цифра 4). Выйти из режима «Статус» можно с помощью элемента «✕» (цифра 5).

Выбрать требуемый вариант фильтрации «Тип ЛПБ», выполнив шаги, указанные на рисунке (см. Рисунок 13).

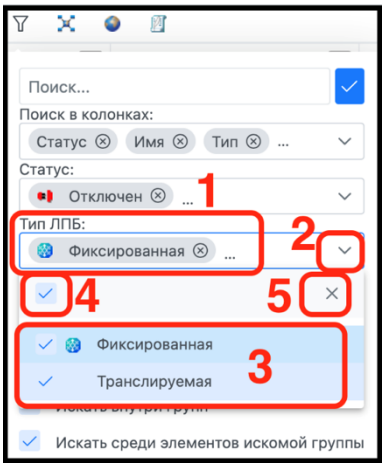


Рисунок 13 – Фильтр «Тип ЛПБ»

В выпадающем списке «Статус» (цифра 1) открыть список доступных атрибутов фильтрации с помощью элемента «⌄» (цифра 2), установив или сняв напротив выбранных атрибутов флажок (наличие флажка делает атрибут выбранным) (цифра 3). Одновременно активировать или деактивировать все атрибуты списка дополнительных фильтров можно, установив флажок (цифра 4). Выйти из режима «Статус» можно с помощью элемента «×» (цифра 5).

Выбрать дополнительные фильтры в списке доступных атрибутов фильтрации (см. Рисунок 14), установив или сняв флажок (наличие флажка делает атрибут выбранным).

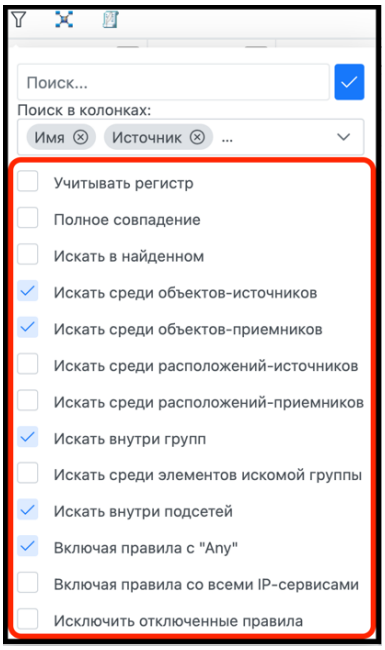


Рисунок 14 – Дополнительные фильтры

4.2.1.2 Инструмент «Показать топологию»

Инструмент «Показать топологию» применяется для быстрого перехода в режим «Топология» и просмотра в нем сетевых объектов. Для перехода в режим «Топология» необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 15).

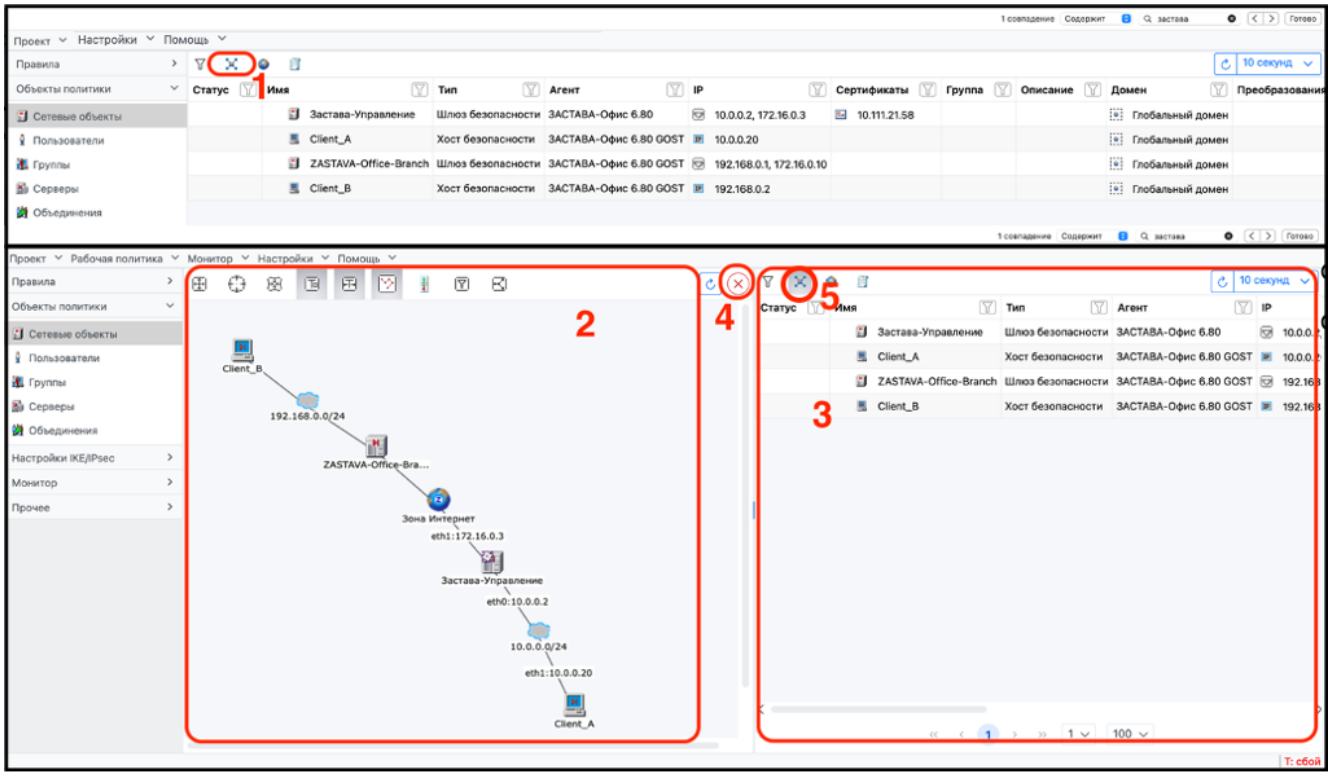


Рисунок 15 – Инструмент «Показать топологию»

Нажать на элемент « » (цифра 1). В результате рабочая область текущей вкладки разделится на две части: в левой части отобразится окно «Топология» (цифра 2), а текущая вкладка переместится вправо (цифра 3). Для выхода из режима работы «Топология» необходимо нажать на элемент «» (цифра 4) или на элемент « » (цифра 5).

4.2.1.3 Инструмент «Показать лог»

Инструмент «Показать лог» применяется для быстрого перехода в журнал регистрации событий. Для перехода в режим «Показать лог» необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 16).

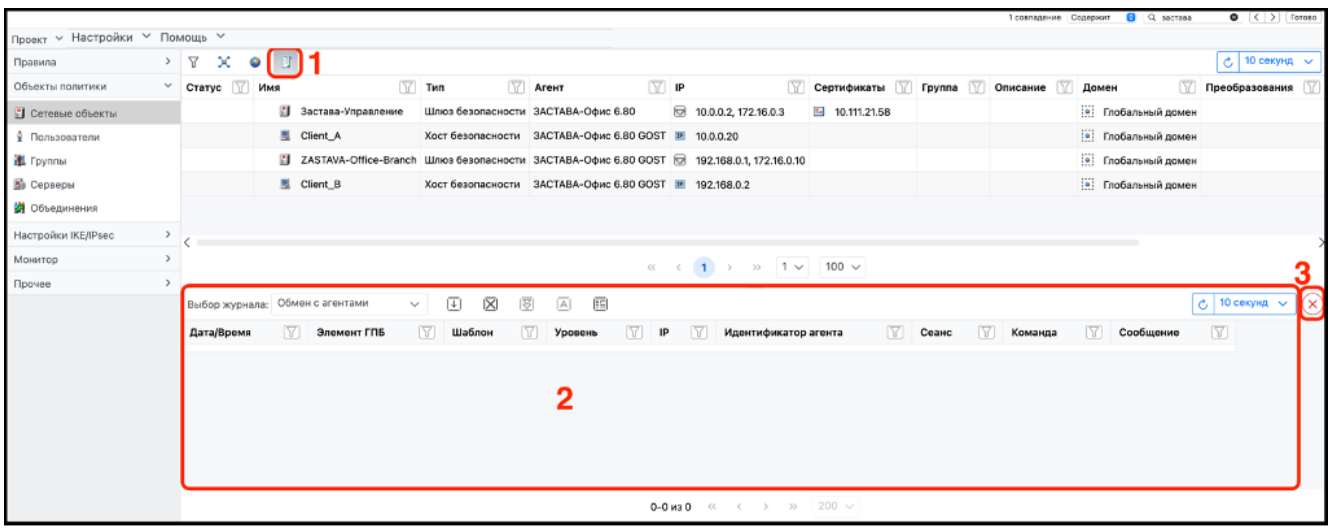


Рисунок 16 – Инструмент «Показать лог»

Нажать на элемент « » (цифра 1). В результате рабочая область текущей вкладки разделится на две части, где в нижней части отобразится окно журнала регистрации событий (цифра 2). Для выхода из режима работы «Показать лог» необходимо нажать на элемент « » (цифра 3) или снова на элемент « » (цифра 1).

4.2.1.4 Инструмент «Показать карту»

Инструмент «Показать карту» применяется для быстрого перехода в режим «Карта» и просмотра на ней расположения сетевых объектов. Для перехода в режим «Карта» необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 17).

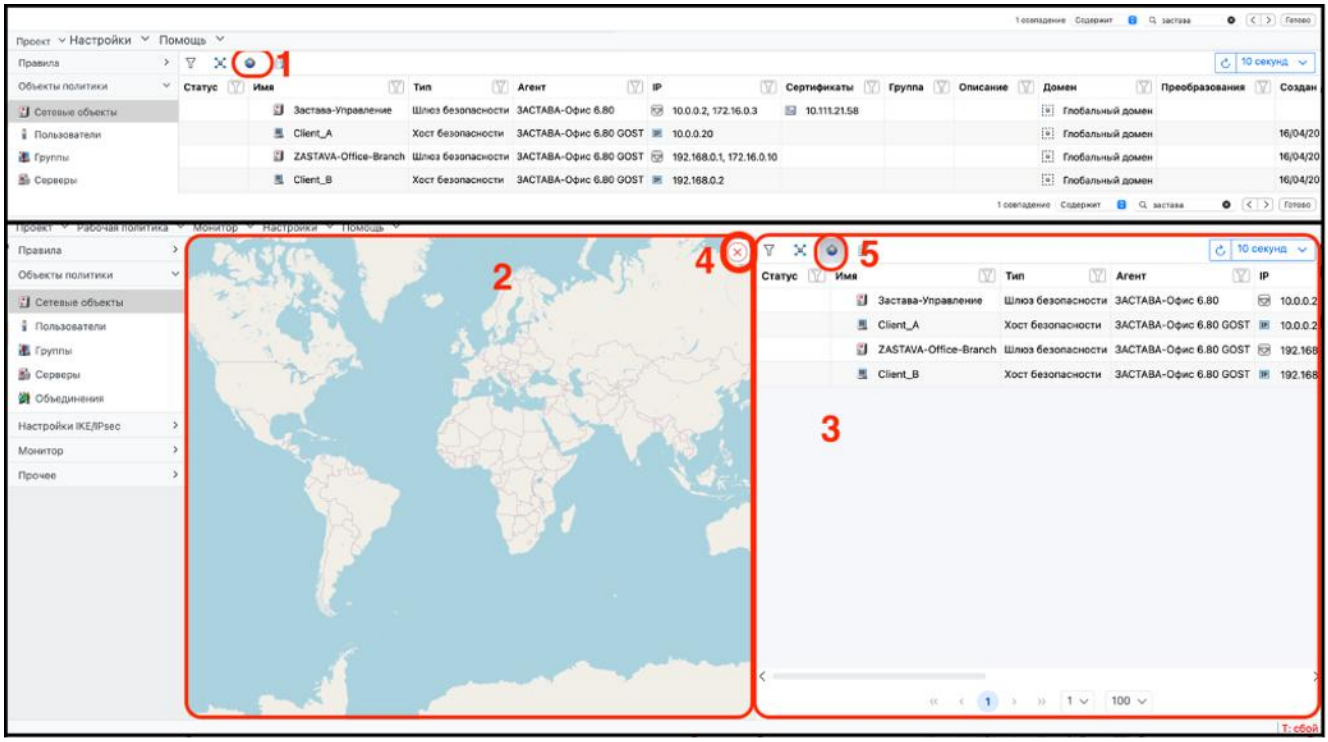


Рисунок 17 – Инструмент «Показать карту»

Нажать на элемент « » (цифра 1). В результате рабочая область текущей вкладки разделится на две части: в левой части отобразится окно с картой (цифра 2), а текущая вкладка переместится вправо (цифра 3). Для выхода из режима работы «Карта» необходимо нажать на элемент « » (цифра 4) или на элемент « » (цифра 5).

4.2.2 Общий вид окна со всеми активированными инструментами

Также в одном окне, например, «Сетевые объекты», можно активировать все его инструменты. На рисунке (см. Рисунок 18) изображен интерфейс с окнами активированных инструментов.

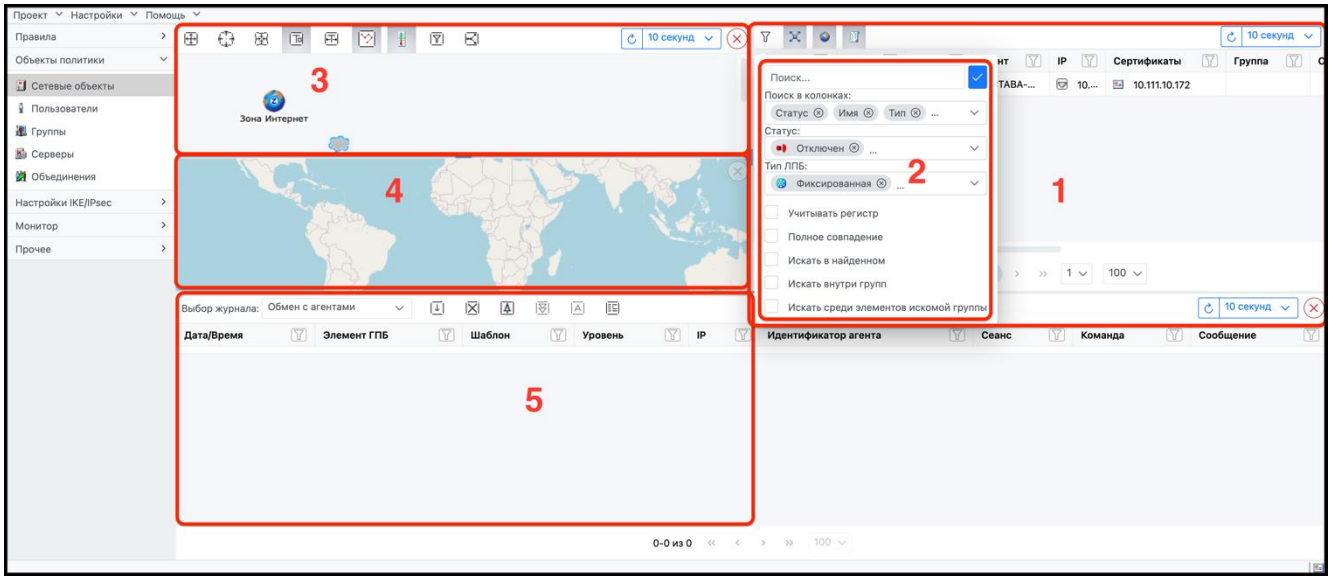


Рисунок 18 – Вид окна с активированными инструментами

При использовании инструментов основное окно «Сетевые объекты» сместится вправо (цифра 1). Использован инструмент «Фильтр» (цифра 2), «Показать топологию» (цифра 3), «Показать карту» (цифра 4), «Показать лог» (цифра 5).

4.2.3 Контекстные меню

Управлять объектами во вкладках можно, используя контекстные меню, которые отображаются при нажатии правой клавишей мыши на свободном месте рабочей области таблицы, на выбранном объекте или одном из его атрибутов. Доступные опции, отображаемые в контекстных меню, представлены в таблице (см. Таблица 5).

Таблица 5 – Описание доступных элементов контекстных меню

Пиктограмма	Характеристика
	Добавить подсеть. Создать новый объект ГПБ
	Преобразовать в подсеть
	Добавить IP диапазон
	Добавить IP-хост
	Добавить хост безопасности
	Добавить шлюз безопасности
	Дублировать. Создать копию объекта ГПБ. Открывает окно для задания параметров нового объекта с использованием параметров выделенного объекта
	Добавить зону
	Преобразовать в постоянную зону

Пиктограмма	Характеристика
	Изменить. Открывает окно для изменения параметров выделенного объекта
	Изменить тип агента. Позволяет изменить дескриптор для выбранного объекта, доступно только для объектов с определенным дескриптором, для объектов без дескриптора не доступно
	Редактировать владельца
	Скрыть все конечные элементы. Перемещает все крайние объекты в список скрытых элементов
	Скрыть. Перемещает все объекты в список скрытых элементов
	Скрыть все связанные элементы. Перемещает все связанные элементы в список скрытых элементов
	Скрыть все невыделенные элементы. Перемещает все объекты, кроме выбранного, в список скрытых элементов
	Скрыть все выделенные элементы. Перемещает все объекты, кроме невыбранного, в список скрытых элементов
	Удалить. Удалить объект ГПБ[1)]
	Удалить из группы
	Включить/отключить
	Сбросить трассу
	Показать трассу
	Транслировать. Выполняет трансляцию ЛПБ для выделенного объекта, доступно только для объектов, у которых может быть политика (установлен параметр «Автоматическое создание» в свойствах «Трансляции ЛПБ» и настроены параметры соединения с PMP-прогрузчиком)
	Добавить домен
	Добавить сервер
	Добавить пользовательскую ЛПБ
	Добавить IKE-предложение
	Добавить действие или IPsec-предложение
	Добавить агента «ЗАСТАВА-Клиент»
	Добавить группу

Пиктограмма	Характеристика
	Добавить группу агентов «ЗАСТАВА-Клиент»
	Добавить правило
	Добавить группу правил
	Добавить центр сертификации (ЦС)
	Добавить сертификат
	Импортировать сертификат/ЦС
	Экспорт
	Добавить прокси-действия
	Добавить расписание
	Добавить сетевой сервис
	Добавить текстовые данные
	Показать в логе
[1)]Нельзя удалить объекты: «Зона Интернет»	

5 ПАНЕЛЬ ВКЛАДОК МЕНЮ

В данном разделе представлено описание опций и настроек для вкладок: «Проект», «Настройки», «Помощь», содержащихся в панели вкладок меню.

5.1 Вкладка меню «Проект»

Вкладка меню «Проект» содержит опции и команды управления ГПБ, изображенные на рисунке (см. Рисунок 19).

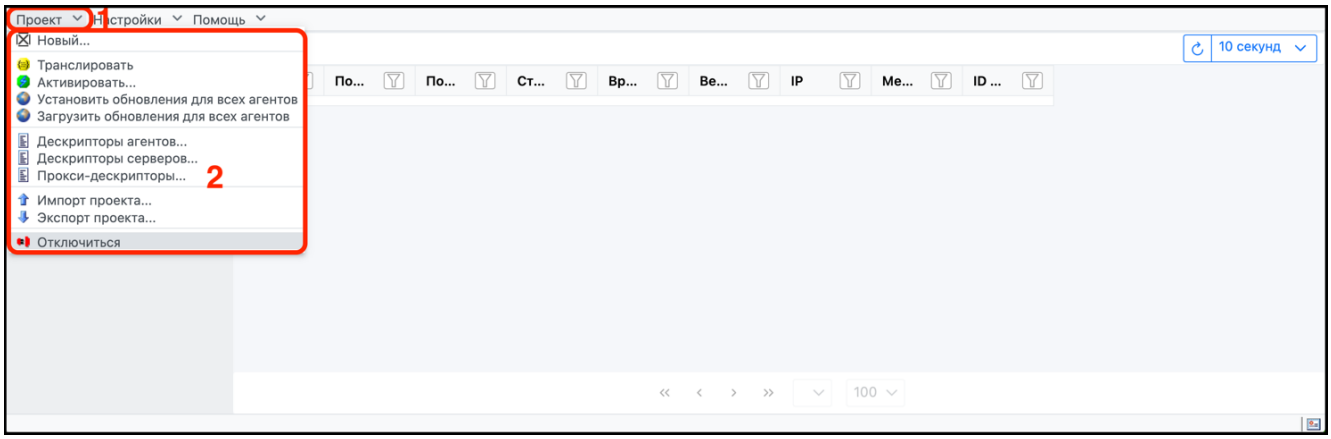


Рисунок 19 – Вкладка меню «Проект»

Во вкладке меню «Проект» (цифра 1) объединены опции и команды (цифра 2), с помощью которых можно произвести глобальные действия для создания ГПБ или её изменения. Описание опций и команд панели вкладок меню «Проект» представлено в таблице (см. Таблица 6).

Таблица 6 – Описание опций и команд вкладки меню «Проект»

Элемент	Характеристика
	Создание нового проекта
	Транслировать текущую ГПБ в ЛПБ для всех управляемых агентов
	Активация ГПБ для всех объектов политики
	Установка и загрузка агентами обновлений с сервера обновлений
	Дескрипторы агентов. Управление XML-файлами, содержащими описание параметров для каждого агента
	Дескрипторы серверов. Управление XML-файлами, содержащими описание параметров для каждого сервера
	Прокси-дескрипторы. Управление XML-файлами, содержащими описание параметров для каждого прокси
	Управление импортом
	Управление экспортом
	Выйти из авторизованной учетной записи пользователя

5.2 Вкладка меню «Настройки»

Во вкладке меню «Настройки» содержатся опции и команды, изображенные на рисунке (см. Рисунок 20).

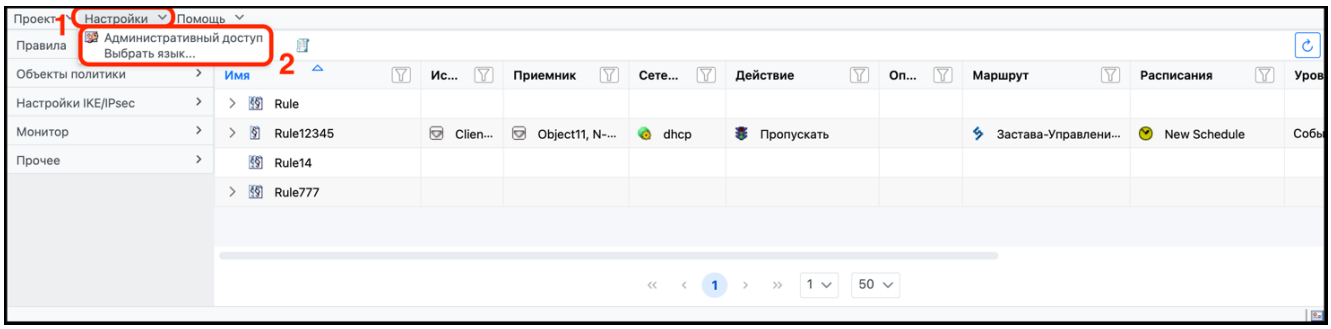


Рисунок 20 – Вкладка меню «Настройки»

Во вкладке меню «Настройки» (цифра 1) в выпадающем списке содержатся опция «Административный доступ», используемая для создания ролей и назначения прав пользователей, и команда «Выбрать язык» для выбора языка веб-интерфейса (доступны русский и английский языки) (цифра 2).

5.2.1 Настройка ролей и прав

Выбрать команду «Административный доступ». В результате откроется окно «Административный доступ», представленное на рисунке (см. Рисунок 21).

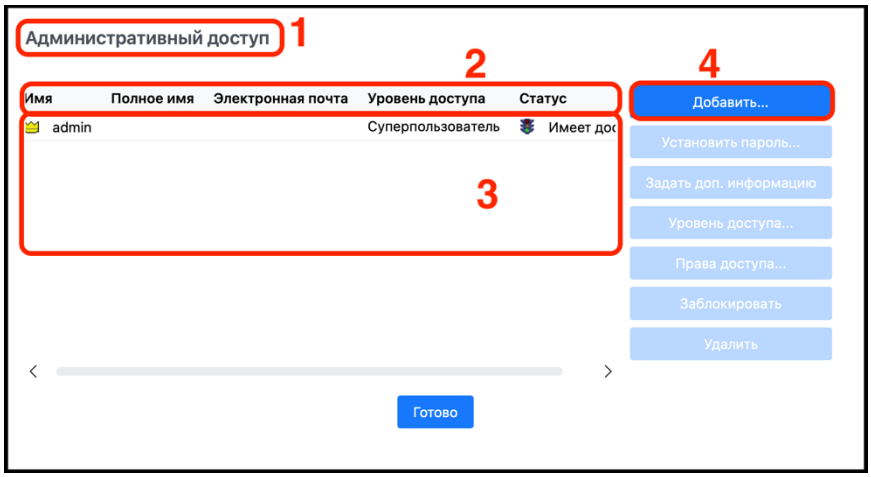


Рисунок 21 – Административный доступ

В окне «Административный доступ» (цифра 1) отобразится список учётных записей и их параметров в виде таблицы (цифра 2). Рабочая область окна, в которой при первоначальном входе в ПО ЗУ отобразится учётная запись «admin» с уровнем доступа «Суперпользователь» (цифра 3). Права на создание учётных записей, определение их уровня доступа и настройку прав принадлежат пользователю с уровнем доступа «Суперпользователь». Удалить учётную запись, имеющую уровень доступа «Суперпользователь», нельзя. Для добавления учётной записи и настройки её уровня доступа нужно нажать кнопку «Добавить» (цифра 4).

В окне «Добавить пользователя» требуется выполнить шаги, изображенные на рисунке (см. Рисунок 22).

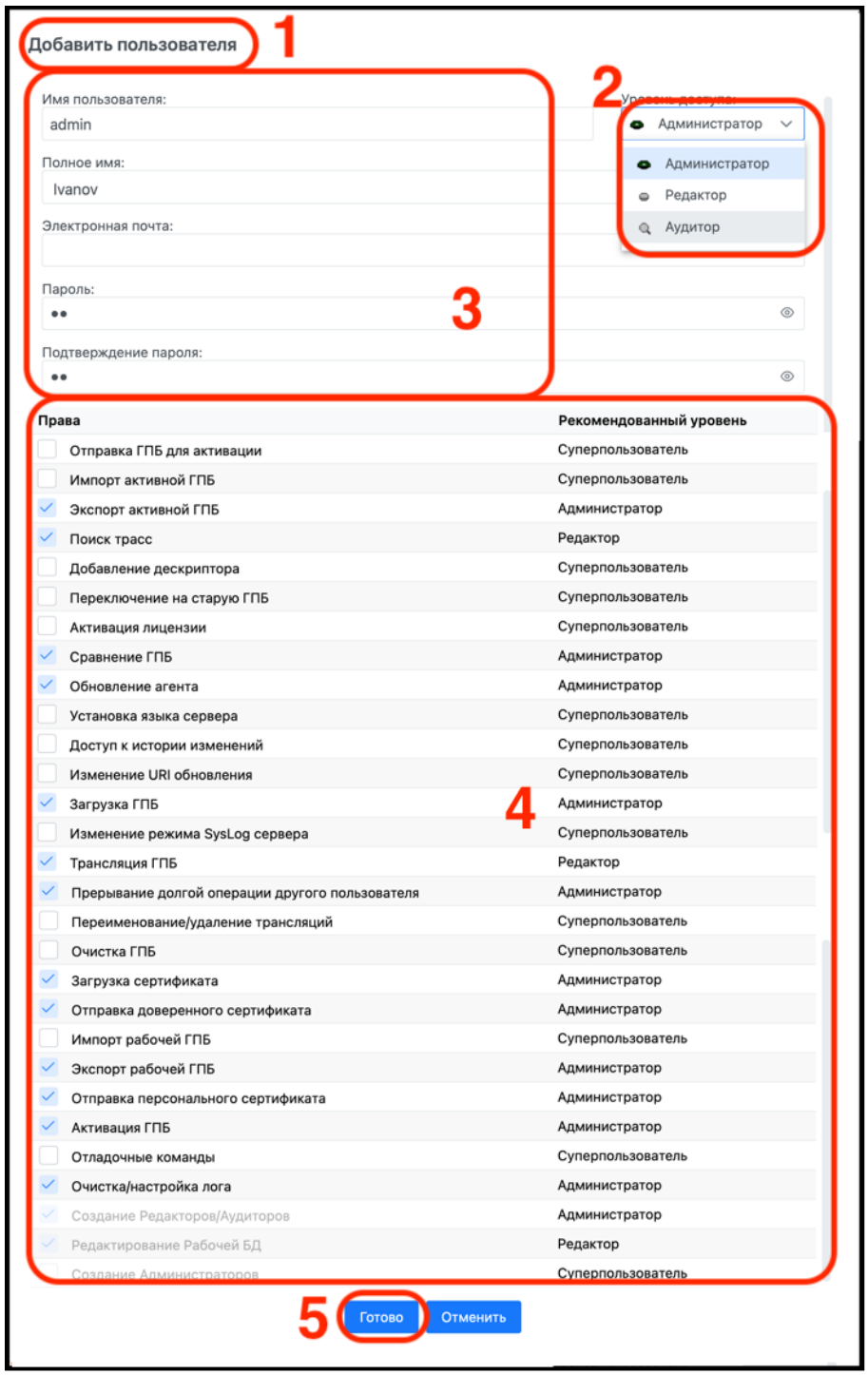


Рисунок 22 – Настройка пользователя

В окне «Добавить пользователя» (цифра 1) выполнить шаги:

1) определить уровень доступа (цифра 2) учётной записи:

— администратор;

— редактор (по умолчанию с ограниченными правами);

— аудитор (по умолчанию с правами наблюдателя);

2) в блоке «Имя пользователя»[3)] (цифра 3) ввести имя, электронную почту и пароль;
3) назначить требуемые для учётной записи права, установив флажок напротив рекомендованного уровня (цифра 4);
4) нажать кнопку «Готово» (цифра 5).

В результате выполненных действий откроется диалоговое окно, представленное на рисунке (см. Рисунок 23).

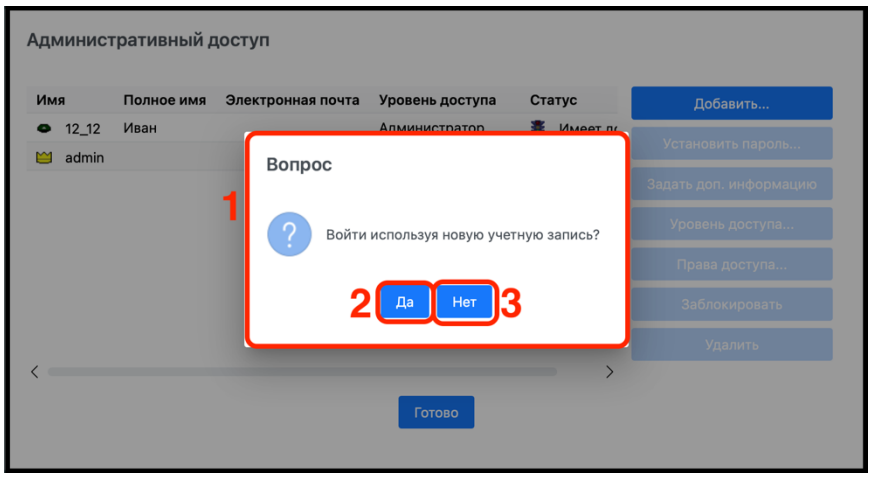


Рисунок 23 – Диалоговое окно перехода в учетную запись

В открывшемся диалоговом окне (цифра 1) для перехода в созданную учетную запись необходимо нажать кнопку «Да» (цифра 2). Чтобы остаться в текущей учетной записи, нажать кнопку «Нет» (цифра 3).

5.2.2 Выбор языка интерфейса

Для выбора языка интерфейса требуется выполнить шаги, изображенные на рисунке (см. Рисунок 24).

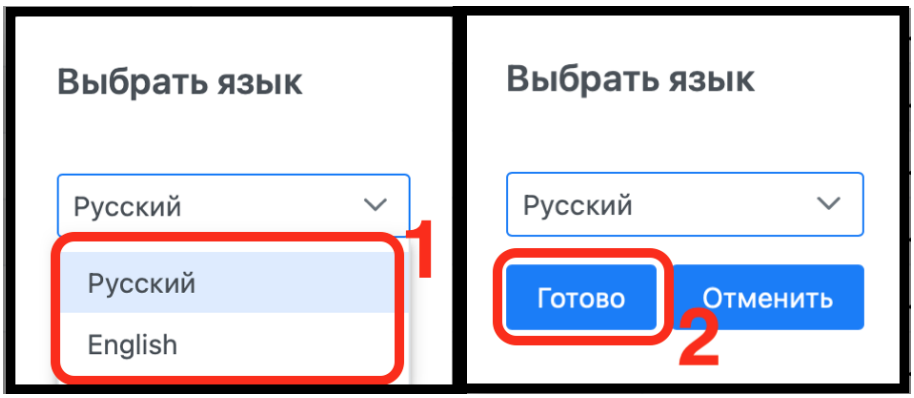


Рисунок 24 – Административный доступ, выбор языка

[3)] Может содержать только следующие символы: подчеркивание, дефис, точка, латинские буквы, цифры. Первым символом могут быть только подчеркивание, дефис, точка, латинская буква, цифра.

Во вкладке меню «Настройки» выбрать команду «Выбрать язык». В открывшемся окне «Выбрать язык» выбрать элемент выпадающего списка (цифра 1) и нажать кнопку «Готово» (цифра 2).

5.3 Вкладка меню «Помощь»

Во вкладке меню «Помощь» содержится информация о ПО ЗУ и производится активация лицензии. Для просмотра информации о ПО ЗУ или введения файла лицензии необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 25).

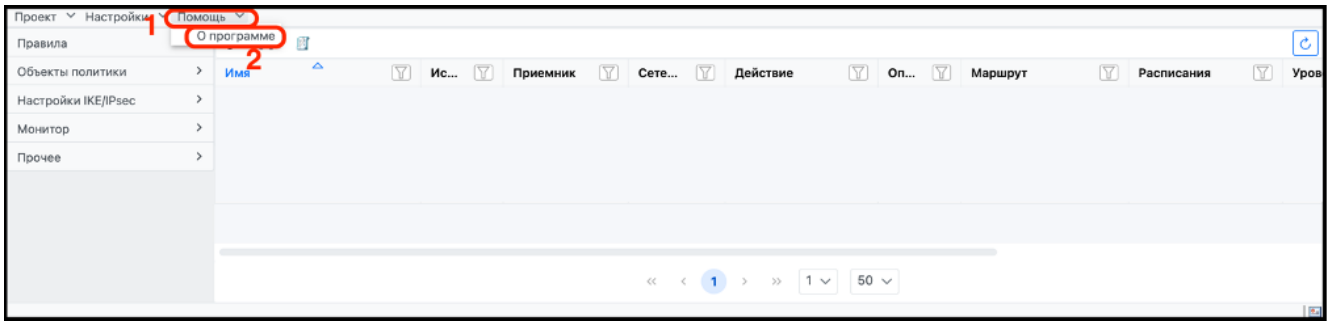


Рисунок 25 – Вкладка меню «Помощь»

Перейти во вкладку меню «Помощь» (цифра 1) и нажать опцию «О программе» (цифра 2). В открывшемся окне отобразятся информация о ПО ЗУ и кнопка активации лицензии, изображенные на рисунке (см. Рисунок 26).

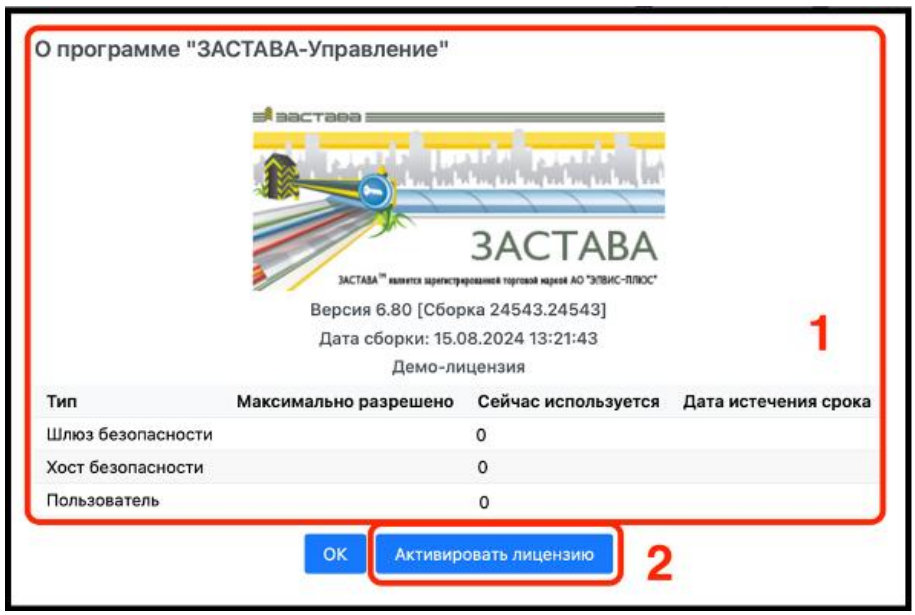


Рисунок 26 – Сведения о программе

В окне «О программе» отобразятся сведения о текущей версии ПО ЗУ и параметры зарегистрированной лицензии, включая её срок действия (цифра 1). Описание активации лицензии (цифра 2) приведено в п. 3.3.6.

6 БОКОВАЯ ПАНЕЛЬ ВКЛАДОК

Во вкладках боковой панели настраивается и отображается вся информация об объектах ГПБ. Добавление, настройка и редактирование объектов ГПБ производятся при помощи контекстного меню, вызываемого правой клавишей мыши отдельно для каждого элемента списка боковой панели вкладок. Вид боковой панели вкладок изображен на рисунке (см. Рисунок 27).

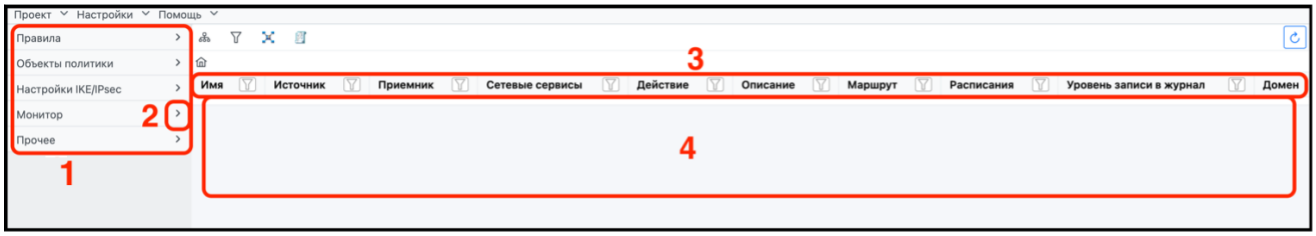


Рисунок 27 – Боковая панель вкладок

В окне вкладок боковой панели отобразятся вкладки (цифра 1) с вложенными списками элементов настройки. Открыть списки можно нажав на элемент «›» (цифра 2). Также для каждого выбранного элемента списка или вкладки будет отображаться таблица его параметров (цифра 3). По каждому из параметров возможна сортировка списка. В рабочей области таблицы параметров (цифра 4) будут отображены созданные ранее и зарегистрированные в ПО ЗУ объекты ГПБ.

6.1 Вкладка боковой панели «Правила»

Правила определяют допустимые взаимодействия для компонентов среды безопасности, которые участвуют в информационном обмене. Для каждого взаимодействия, требующего шифрования сетевого трафика, нужно создавать отдельные правила. Также рекомендуется группировать объекты с одинаковым уровнем доступа и применять одно правило ко всей группе, если эта группа определена как «Группа».

Определенные объекты не могут участвовать в правилах, которые используют действие «encrypt and Pass traffic» («зашифровать и пропустить трафик»), поскольку они не содержат механизмов, чтобы устанавливать защищенное соединение с другими объектами политики. Данные объекты, которые не защищены шлюзом безопасности, могут участвовать только в обычных (нешифрованных) действиях «Пропустить» (Pass) или «Блокировать» (Drop): «Подсеть», «IP-Хост» и «IP-Диапазон», а также объекты «Шлюз Безопасности» и «Хост Безопасности», у которых в настройках поля «Включить IKE/IPsec-обработку» нет отметок.

Вид вкладки боковой панели «Правила» изображен на рисунке (см. Рисунок 28).

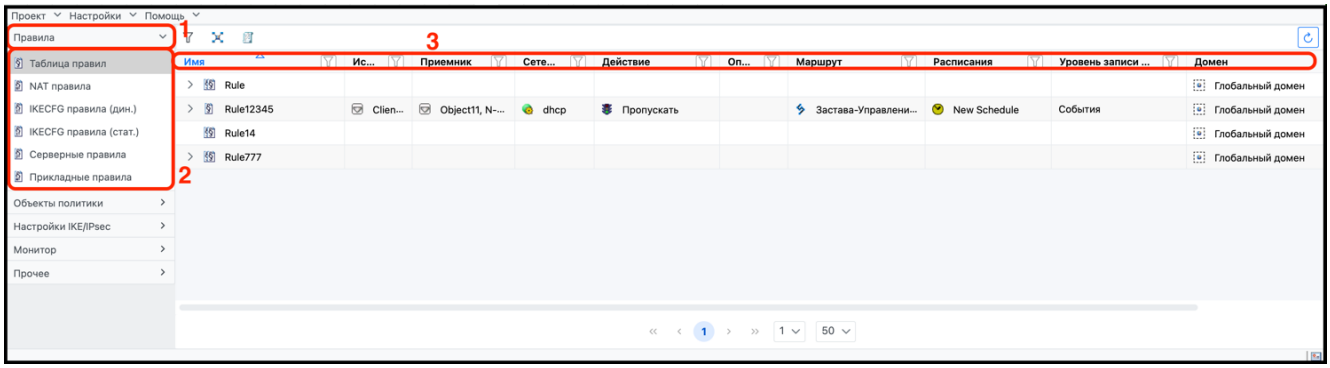


Рисунок 28 – Вид вкладки боковой панели «Правила»

На вкладке боковой панели «Правила» требуется нажать на элемент « › » (цифра 1) для перехода к списку элементов (цифра 2):

— «Таблица правил»;
— «NAT правила»;
— «IKECFG динамические правила»;
— «IKECFG статические правила»;
— «Серверные правила»;
— «Прикладные правила».

Параметры правил отображаются в виде таблицы (цифра 3).

6.1.1 Таблица правил

Вид окна элемента списка «Таблица правил» изображен на рисунке (см. Рисунок 29).

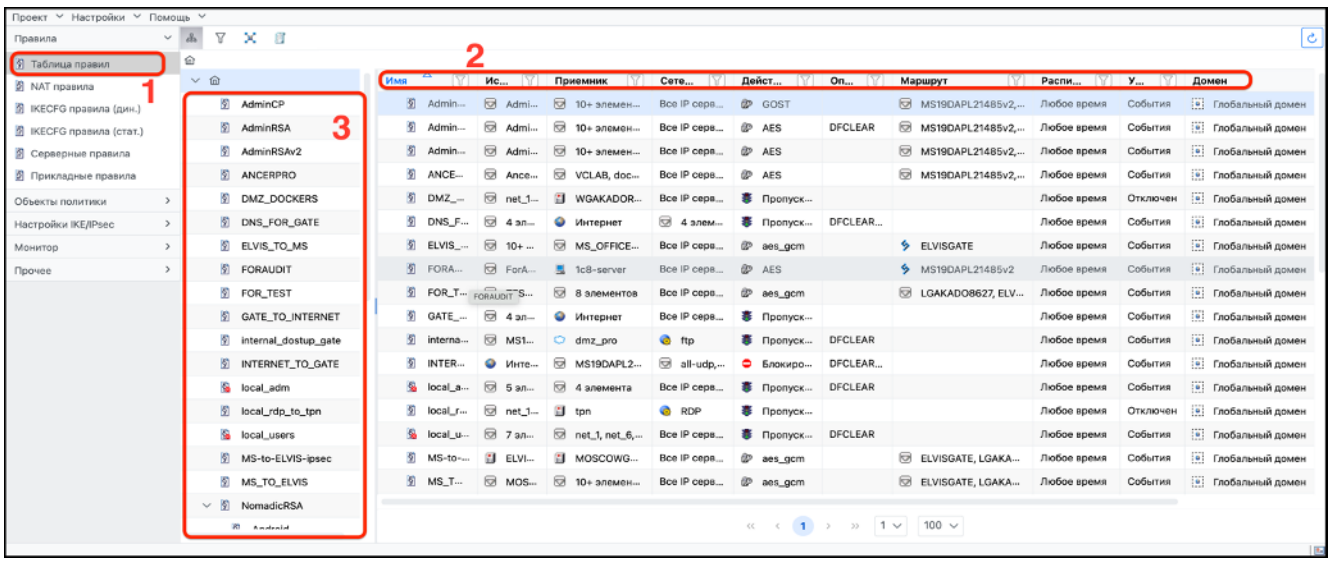


Рисунок 29 – Таблица правил

При переходе на элемент списка «Таблица правил» (цифра 1) откроется окно, в котором будут отображены все правила в ГПБ в виде таблицы, которая содержит следующие параметры (цифра 2):

— «Имя» – наименование правила;

— «Источник» – объект ГПБ, инициирующий сетевое соединение;

— «Приемник» – объект ГПБ, с которым устанавливается сетевое соединение;

— «Сетевые сервисы» – протоколы сетевого обслуживания (или их группы) см. Приложение 2);

— «Действие» – варианты пропустить (Pass), блокировать (Drop), зашифровать по одному из предложенных вариантов, описанных в разделе «IPsec» (см. п. 6.3.2);

— «Описание» – дополнительная информация;

— «Маршрут» – шлюзы, через которые обязательно должен пройти трафик;

— «Расписание» – временные интервалы работы правила;

— «Уровень» записи событий в журнал;

— «Домен» – домен, в отношении которого действует правило.

По каждому из параметров возможна сортировка списка.

В колонке (цифра 3) отобразится список правил объектов. Некоторые из них могут содержать дочерние компоненты. Для просмотра параметров дочерних компонентов необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 30).

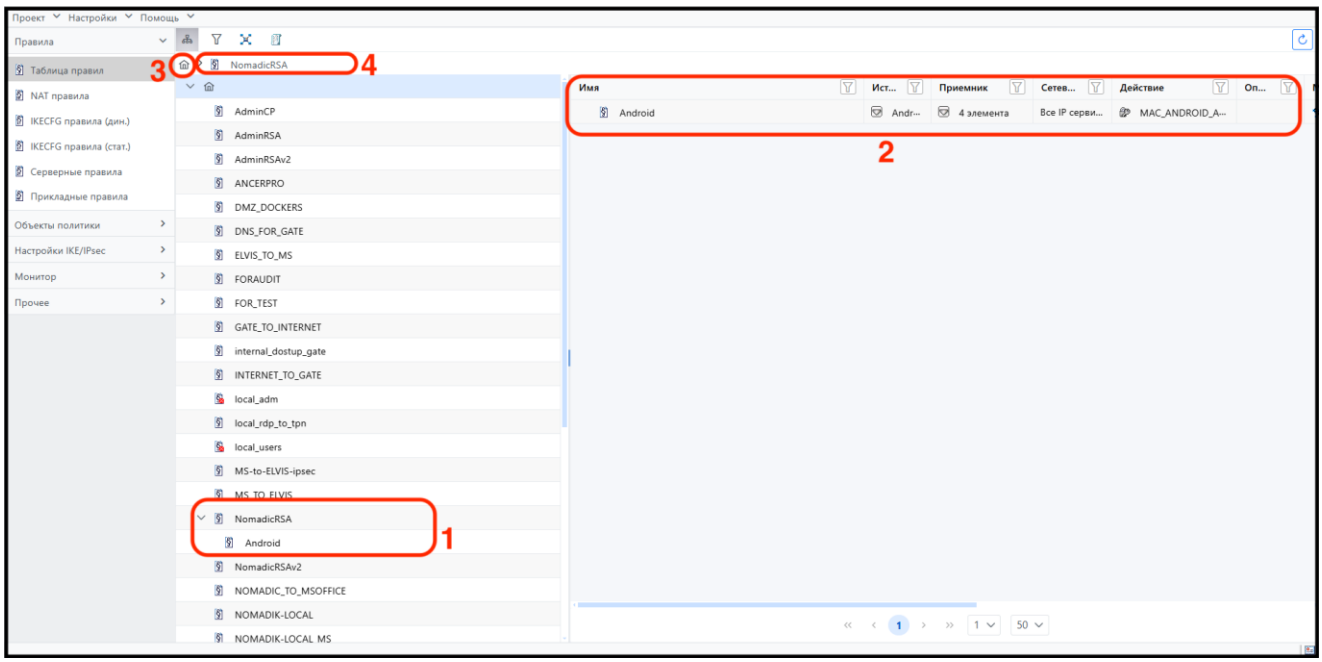


Рисунок 30 – Окно компонентов правила

Выбрать в списке родительский компонент (цифра 1). Всё, что в него входит, отобразится в рабочей области таблицы (цифра 2). Выбранное правило будет дополнительно указано в строке (цифра 3). Вернутся к просмотру таблицы правил можно, нажав на элемент «⌂» (цифра 4). Если у выбранного правила нет дочернего компонента, то рабочая область таблицы будет пустой.

Подробное описание добавления и редактирования правил приведено в п. 6.1.7.

6.1.2 NAT правила

Центр управления политикой безопасности поддерживает работу с сетями, где используется трансляция сетевых адресов (NAT) типа:

— статическая трансляция адресов;

— динамическая трансляция адресов.

NAT настраивается на пограничных устройствах, отделяющих локальные сети от сети Интернет. Пограничными устройствами могут быть небольшие специализированные аппаратные устройства или полноценные VPN-шлюзы/МЭ. В обоих случаях для описания данного устройства (агента) в ПО ЗУ создается объект «Шлюз безопасности». Для некоторых типов агентов возможно активное управление политикой NAT (путем включения команд NAT в ЛПБ агента), для остальных агентов ПО ЗУ просто учитывает информацию о NAT-преобразованиях на данном объекте, чтобы отслеживать возможные изменения IP-адресов при прохождении трафика через сеть (через специальный алгоритм трассировки на этапе трансляции ГПБ).

В рабочей области окна «NAT правила» будет отображен список всех NAT правил и существующих в ГПБ объектов политики, созданных ранее. Вид окна элемента списка «NAT правила» представлен на рисунке (см. Рисунок 31).

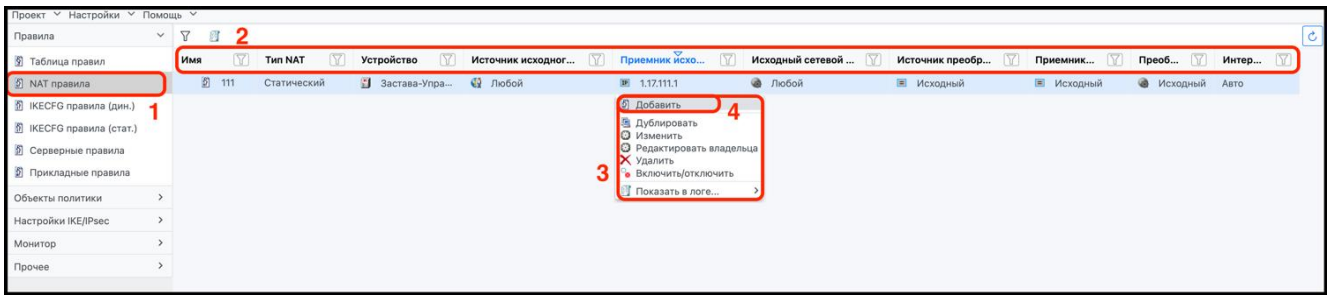


Рисунок 31 – NAT правила

В окне элемента списка «NAT правило» (цифра 1) отображается таблица с параметрами о каждом NAT правиле в ГПБ (цифра 2):

— «Имя правила» (выключенные правила помечаются пиктограммой «Красный крест»);

— «Тип NAT» (динамический или статический);

— «Устройство» (устройство, на котором задано правило);

— «Источник исходного пакета»;

— «Приемник исходного пакета»;

— «Исходный сетевой сервис»;

— «Источник преобразованного пакета»;

— «Приемник преобразованного пакета»;

— «Преобразованный сетевой сервис»;

— «Интерфейс применения правила».

По каждому из параметров возможна сортировка списка.

Создать новое правило можно, нажав правой клавишей мыши в свободное место рабочей области таблицы, вызвав контекстное меню (цифра 3) и выбрав элемент «Добавить» (цифра 4).

В результате откроется окно «Добавить NAT правило», в котором необходимо произвести настройку NAT правила, выполнив шаги, представленные на рисунке (см. Рисунок 32).

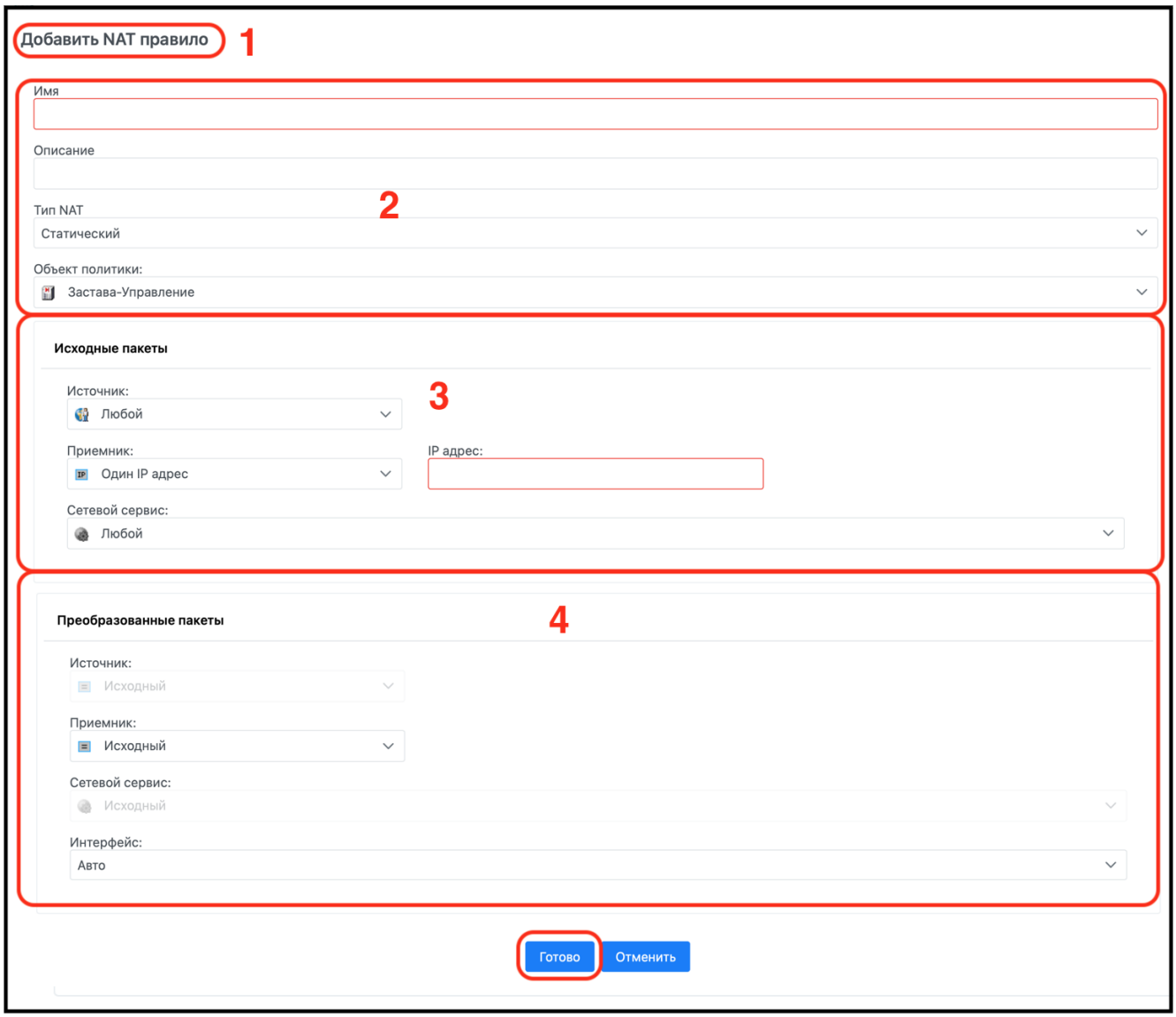


Рисунок 32 – NAT правила

1) В окне настроек «Добавить NAT правило» (цифра 1) в общем блоке настроек (цифра 2):

— ввести «Имя»;

— ввести «Описание»;

— выбрать «Тип NAT» (статический/динамический);

— выбрать «Объект политики»;

2) в блоке настроек «Исходные пакеты» (цифра 3):

— выбрать «Источник». При выборе в качестве источника существующего объекта из выпадающего списка правило будет привязано к адресу объекта политики;

— выбрать «Приемник»;

— выбрать «Сетевой сервис»;

— в поле «IP-адрес» указать IP-адрес приемника исходных пакетов;

3) в блоке «Преобразованные пакеты» (цифра 3) в выпадающем списке выбрать:

— «Источник». При выборе в качестве источника существующего объекта из выпадающего списка правило будет привязано к адресу объекта политики;

— «Приемник»;

— «Сетевой сервис»;

— «Интерфейс».

Нажать кнопку «Готово». В таблице появится новое NAT правило.

Если необходимо, чтобы NAT правило применялось только к некоторым типам трафика, то в блоке настроек «Исходные пакеты» в строке «Сетевой сервис» надо указать нужный сетевой сервис. При этом необходимо убедиться в том, что в блоке настроек «Преобразованные пакеты» строка «Сетевой сервис» имеет значение «Исходный», либо выбрать в качестве значения конкретный сетевой сервис. В результате будет включена трансляция сетевых сервисов (например, таким образом можно транслировать HTTP-трафик с порта TCP:80 на порт TCP:8080). Список доступных для выбора сетевых сервисов редактируется в соответствующем окне ПО ЗУ.

Если необходимо определить интерфейс, через который будет осуществляться трансляция, необходимо выбрать этот интерфейс в поле «Интерфейс» в блоке настроек «Преобразованные пакеты».

Если в блоке настроек «Исходные пакеты» в качестве значения для «Приемник», «Источник» или «Сетевой сервис» указано «Любой», то значение 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.

6.1.3 IKECFG динамические правила

В рабочей области окна «IKECFG правила (дин.)» будет отображен список всех динамических IKECFG правил, созданных ранее для объектов политики ГПБ. Вид окна элемента списка «IKECFG правила (дин.)» представлен на рисунке (см. Рисунок 33).

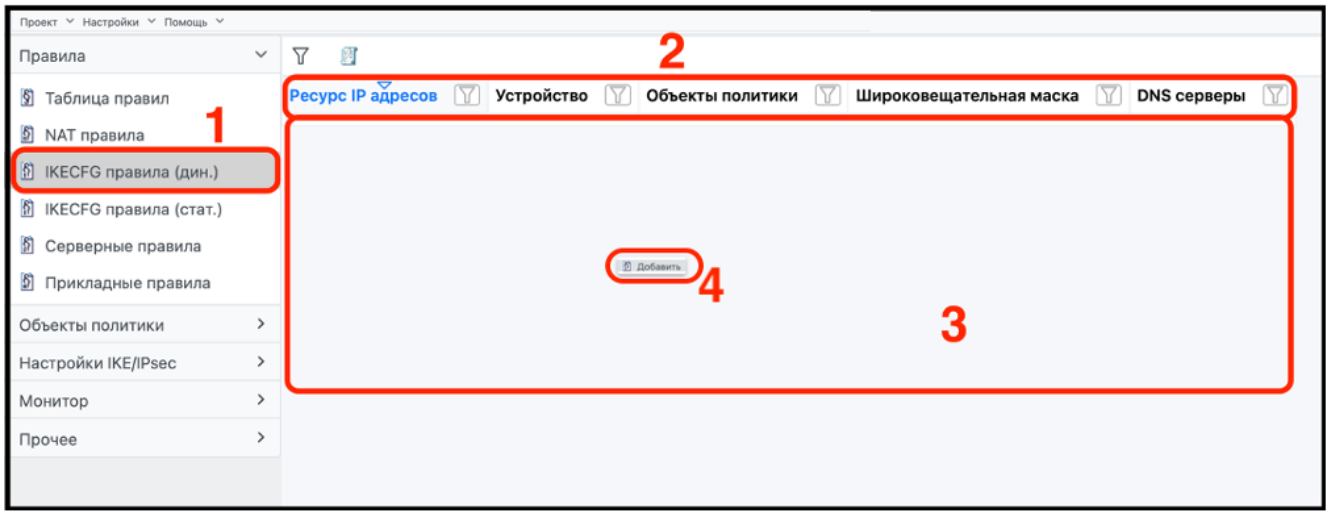


Рисунок 33 – IKECFG динамические правила

В окне элемента списка «IKECFG правила. (дин)» (цифра 1) отображается таблица с параметрами о каждом динамическом IKECFG правиле в ГПБ (цифра 2):

— «Ресурс IP-адресов»;
— «Устройство» (устройство, на котором создано правило);
— «Объект политики»;
— «Широковещательная маска»;
— «DNS серверы».

По каждому из параметров возможна сортировка списка.

Создать новое правило можно, нажав правой клавишей мыши в свободное место рабочей области таблицы (цифра 3), после чего нажать появившуюся кнопку «Добавить» (цифра 4).

В результате откроется окно «Добавить IKECFG правило», в котором требуется выполнить шаги, изображенные на рисунке (см. Рисунок 34).

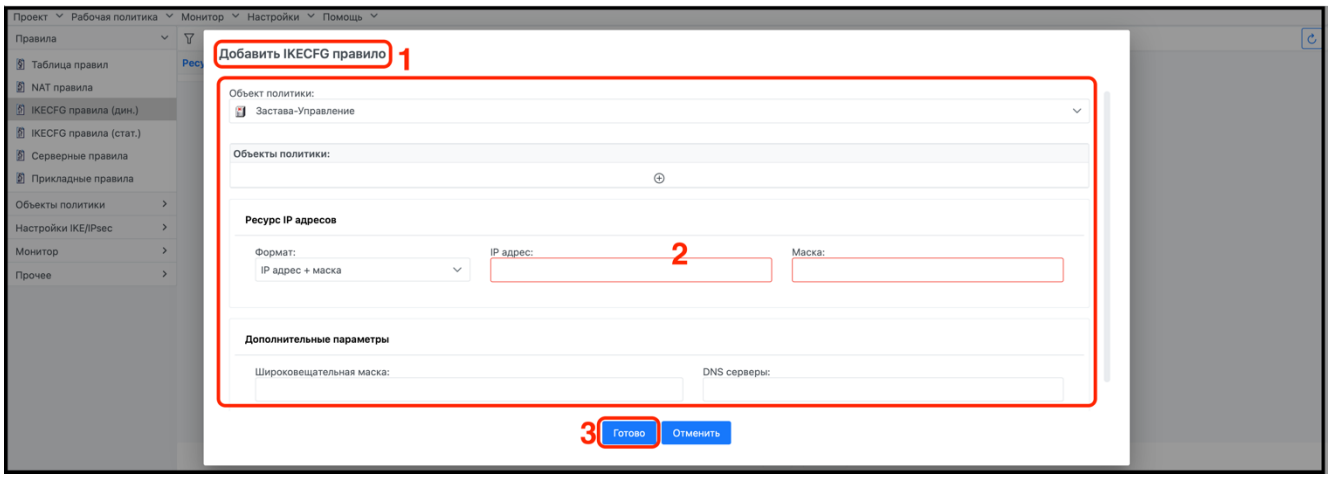


Рисунок 34 – Форма для добавления динамического IKECFG правила

В окне «Добавить IKECFG правило» (цифра 1) необходимо заполнить форму (цифра 2) для добавления IKECFG динамического правила, нажать кнопку «Готово» (цифра 3). В результате будет создано IKECFG динамическое правило.

6.1.4 IKECFG статические правила

В окне «IKECFG правила (стат.)» отображается список всех статических IKECFG правил, созданных ранее для объектов политики ГПБ. Вид окна элемента списка «IKECFG правила (стат.)» представлен на рисунке (см. Рисунок 35).

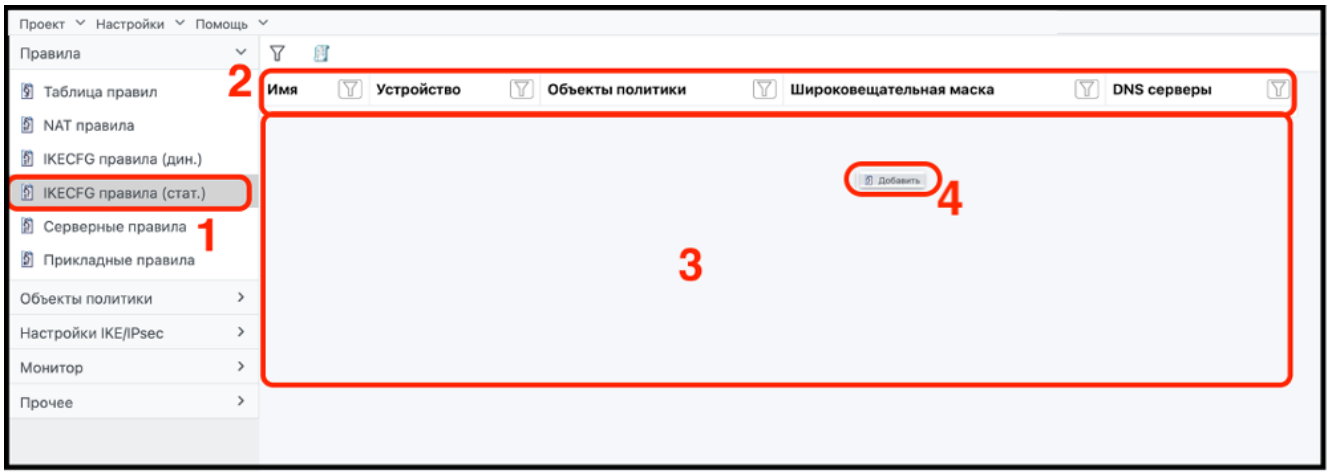


Рисунок 35 – Вид окна «IKECFG правила (стат.)»

В окне элемента списка «IKECFG правила (стат.)» (цифра 1) отображается таблица с информацией о каждом IKECFG статическом правиле в ГПБ (цифра, 2):

— «Имя»;
— «Устройство» (устройство, на котором создано правило);
— «Объекты политики»;
— «Широковещательная маска»;
— «DNS серверы».

По каждому из параметров возможна сортировка списка.

Создать новое IKECFG статическое правило можно, нажав правой клавишей мыши в свободное место рабочей области таблицы (цифра 3), далее нажать появившуюся кнопку «Добавить» (цифра 4).

В результате откроется окно «Добавить IKECFG правило», в котором требуется выполнить шаги, изображенные на рисунке (см. Рисунок 36).

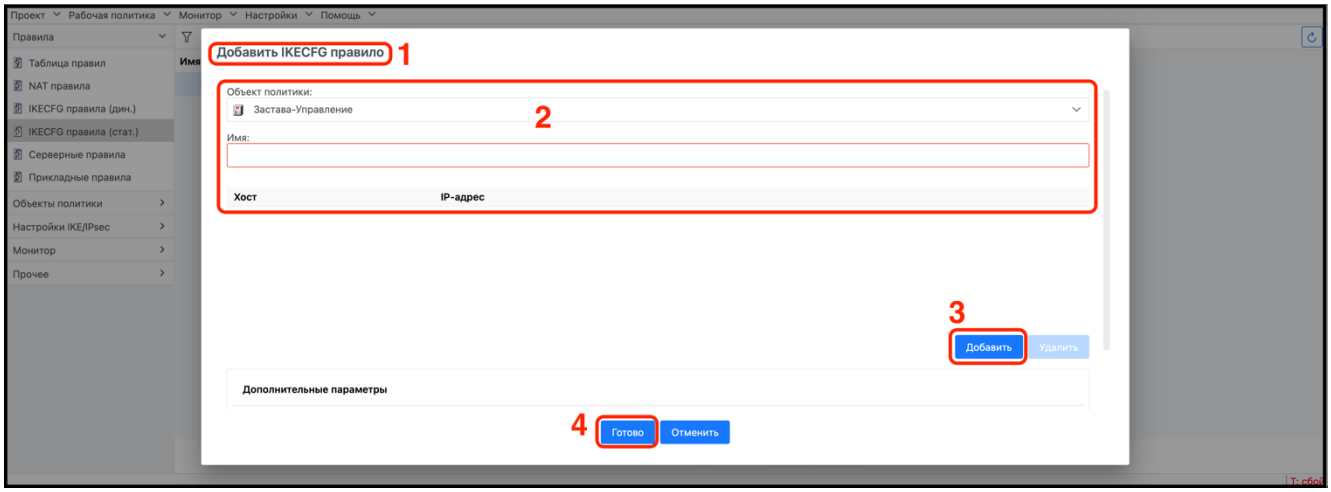


Рисунок 36 – добавление IKECFG статического правила

В окне «Добавить IKECFG правило» (цифра 1) необходимо заполнить форму (цифра 2), при необходимости добавить хост, нажав кнопку «Добавить» (цифра 3). Для добавления IKECFG статического правила нажать кнопку «Готово» (цифра 4). В результате будет создано IKECFG статическое правило.

6.1.5 Серверные правила

Вид окна элемента списка «Серверные правила» отображается список всех созданных ранее серверных правил для объектов политики ГПБ. Вид окна «Серверные правила» представлен на рисунке (см. Рисунок 37).

Рисунок 37 – Серверные правила

В окне «Серверные правила» (цифра 1) в таблице показана информация о каждом серверном правиле в ГПБ (цифра 2):

— «Применение»;
— «Клиент»;
— «Сервер»;
— «Владелец сервера»;
— «Клиент -> сервер»;
— «Клиент <- сервер»;

— «Режимы»;

— «Действие»;

— «Уровень записи в журнал».

По каждому из параметров возможна сортировка списка. В рабочей области таблицы будут отображаться все серверные правила (цифра 3).

6.1.6 Прикладные правила

В окне элемента списка «Прикладные правила» отображается список всех созданных ранее прикладных правил в ГПБ. Вид окна «Прикладные правила» представлен на рисунке (см. Рисунок 38).

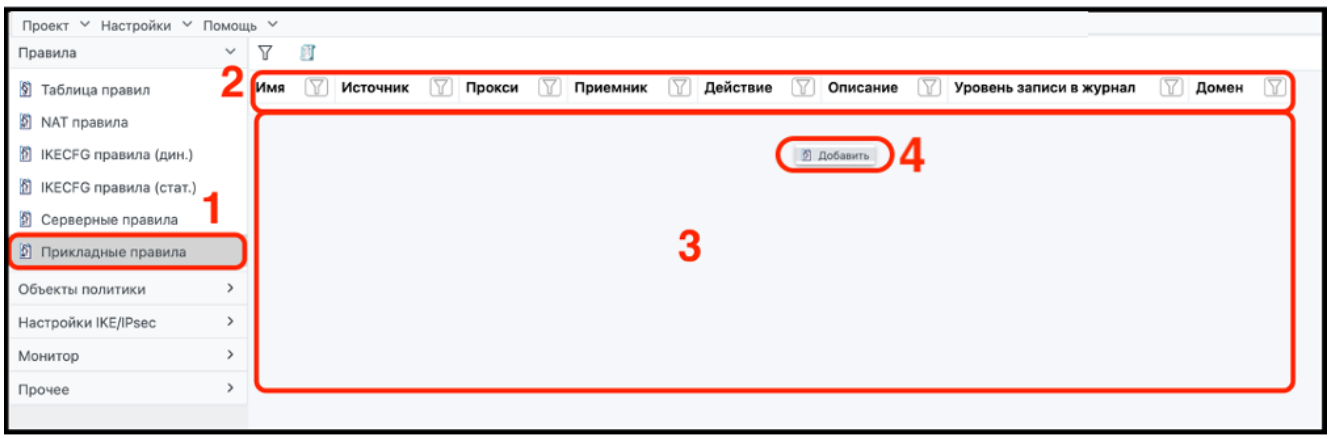


Рисунок 38 – Прикладные правила

В окне «Прикладные правила» (цифра 1) в виде таблицы показана информация о каждом прикладном правиле в ГПБ (цифра 2):

— «Имя»;

— «Источник»;

— «Прокси»;

— «Приемник»;

— «Действие»;

— «Описание»;

— «Уровень записи в журнал»;

— «Домен».

По каждому из параметров возможна сортировка списка.

Создать новое прикладное правило можно, нажав правой клавишей мыши в свободное место рабочей области таблицы (цифра 3), далее нажать появившуюся кнопку «Добавить» (цифра 4).

В результате откроется окно «Добавить Прикладное правило», в котором требуется выполнить шаги, изображенные на рисунке (см. Рисунок 39).

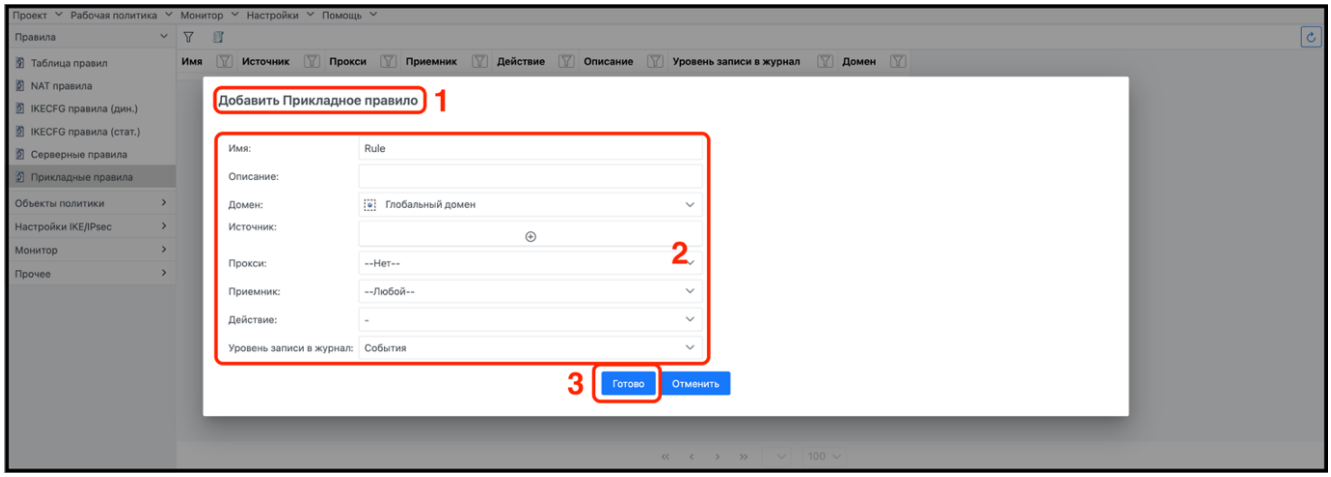


Рисунок 39 – Добавить Прикладные правила

В окне «Добавить Прикладное правило» (цифра 1) необходимо заполнить форму (цифра 2), нажать кнопку «Готово» (цифра 3). В результате будет создано прикладное правило.

6.1.7 Работа с контекстным меню для элементов списка «Правила»

Добавление настройка и редактирование объектов производятся с помощью контекстного меню. Для каждого элемента списка боковой панели вкладок контекстное меню имеет как общий список команд, так и свой индивидуальный список.

Для вызова контекстного меню нужно выбрать требуемый элемент списка, в открывшемся окне нажать правой клавишей мыши в свободное место рабочей области таблицы или на требуемый в списке объект.

6.1.7.1 Общие команды контекстного меню для элементов списка «Правила»:

— «Дублировать»;
— «Изменить»;
— «Удалить»;
— «Показать в логе».

6.1.7.1.1 Дублировать

Для дублирования правила нужно выбрать требуемое правило, затем в контекстном меню выбрать команду «Дублировать», как представлено на рисунке (см. Рисунок 40).

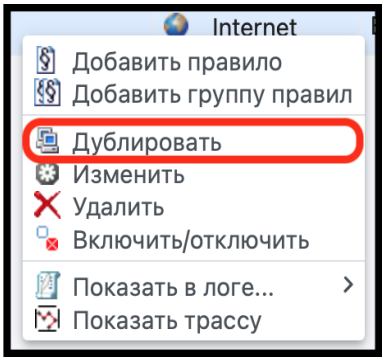


Рисунок 40 – Команда «Дублировать»

В результате откроется окно «Дублировать», в котором необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 41).

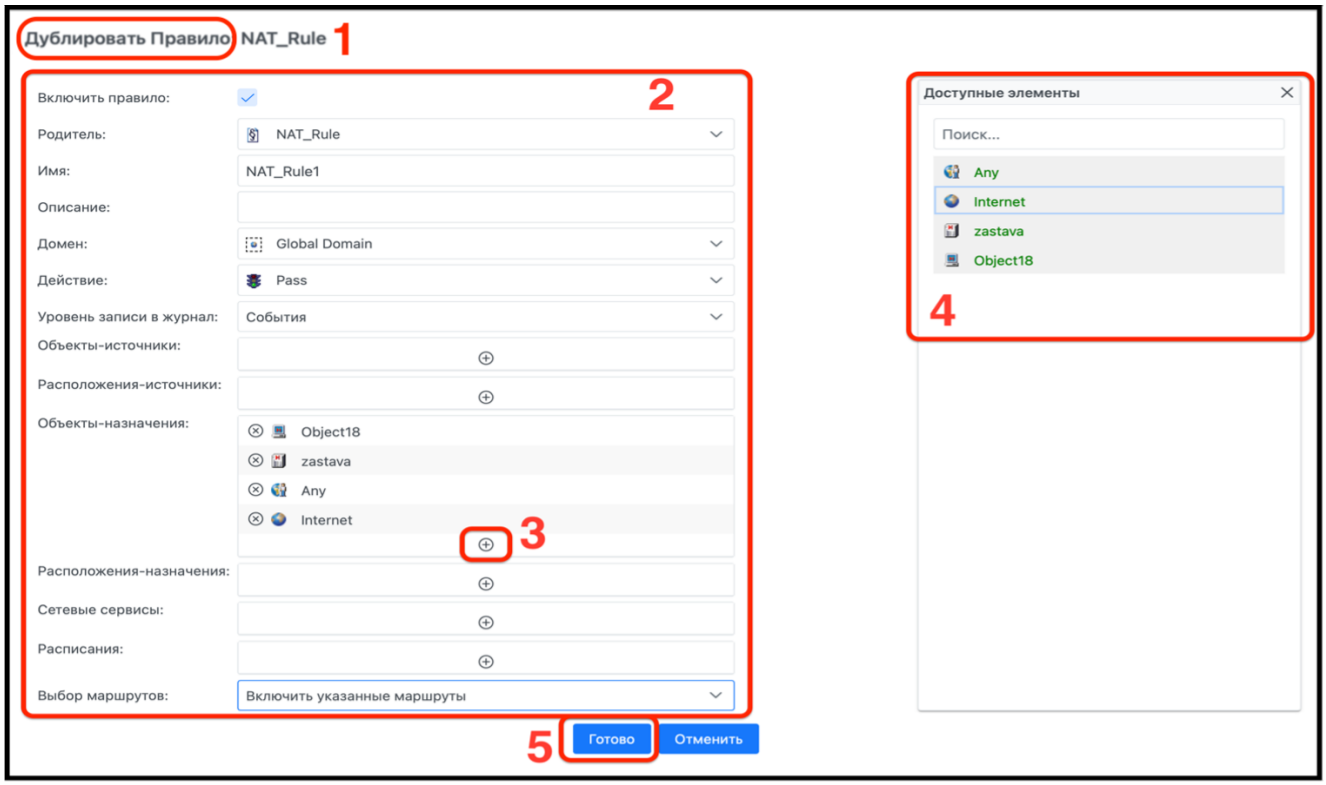


Рисунок 41 – Окно настроек «Дублировать»

В окне «Дублировать» (цифра 1) заполнить форму для выбранного объекта (цифра 2), используя выпадающие списки и элемент «⊕» (цифра 3) для вызова бокового меню «Доступные элементы» (цифра 4) (в примере показано дублирование объекта NAT правила). После завершения действий нажать кнопку «Готово» (цифра 5).

6.1.7.1.2 Изменить

Для редактирования правила нужно выбрать требуемое правило, затем в контекстном меню выбрать команду «Изменить», как представлено на рисунке (см. Рисунок 42).

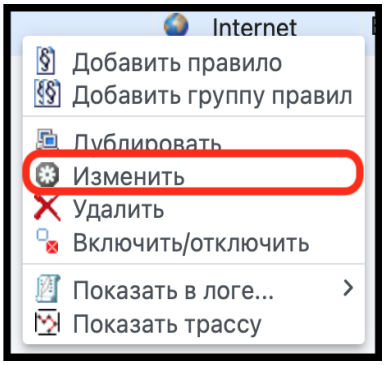


Рисунок 42 – Команда «Изменить»

В результате откроется окно «Изменить», в котором необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 43).

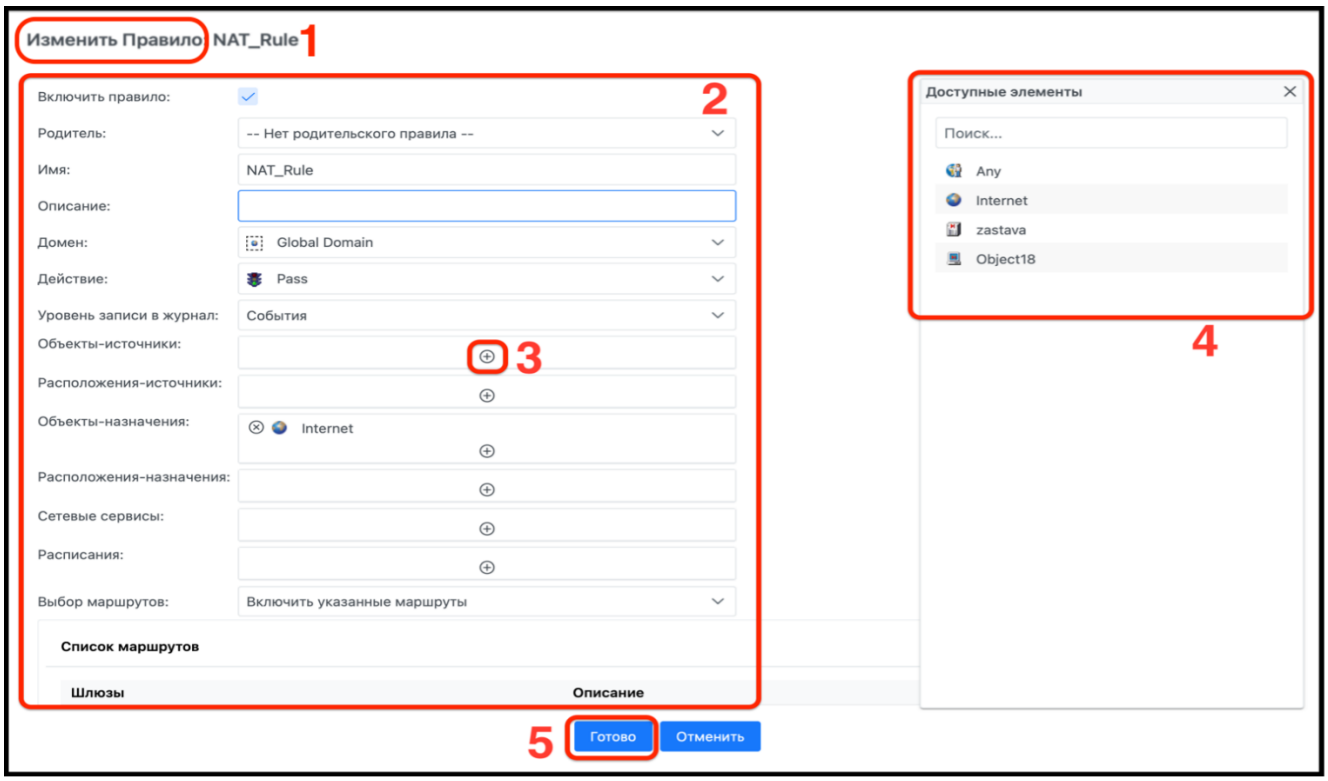


Рисунок 43 – Окно настроек «Изменить»

В окне «Изменить» (цифра 1) редактировать параметры выбранного объекта (цифра 2), используя выпадающие списки и элемент «⊕» (цифра 3) для вызова бокового меню «Доступные элементы» (цифра 4) (в примере показано дублирование объекта NAT правила). После завершения всех действий нажать кнопку «Готово» (цифра 5).

6.1.7.1.3 Удалить

Для удаления правила необходимо выделить требуемые объекты, затем выбрать команду контекстного меню «Удалить», как представлено на рисунке (см. Рисунок 44).

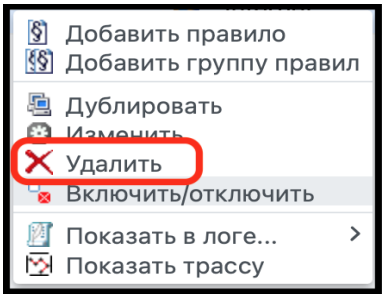


Рисунок 44 – Команда «Удалить»

В открывшемся диалоговом окне выполнить команды, представленные на рисунке (см. Рисунок 45).

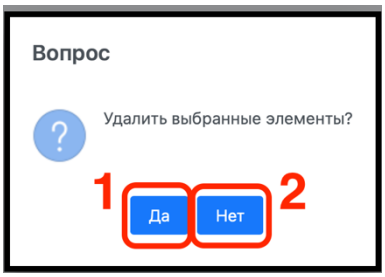


Рисунок 45 – Удаление выбранных элементов

Для удаления правила нажать кнопку «Да» (цифра 1). В случае, если удаление не нужно, нажать кнопку «Нет» (цифра 2). Одной командой можно удалить сразу несколько элементов.

6.1.7.1.4Показать в логе

Команда «Показать в логе» используется для сортировки и отображения выбранных правил в журнале. Для перехода в журнал необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 46).

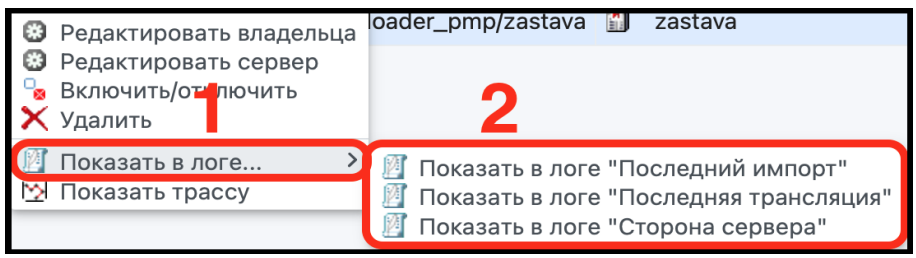


Рисунок 46 – Показать в логе

В контекстном меню выбранного правила нажать команду «Показать в логе» (цифра 1), в дополнительном выпадающем списке выбрать требуемый журнал (цифра 2):

— «Последний импорт»;

— «Последняя трансляция»;

— «Сторона сервера».

В результате откроется окно выбранного журнала, изображенного на рисунке (см. Рисунок 47).

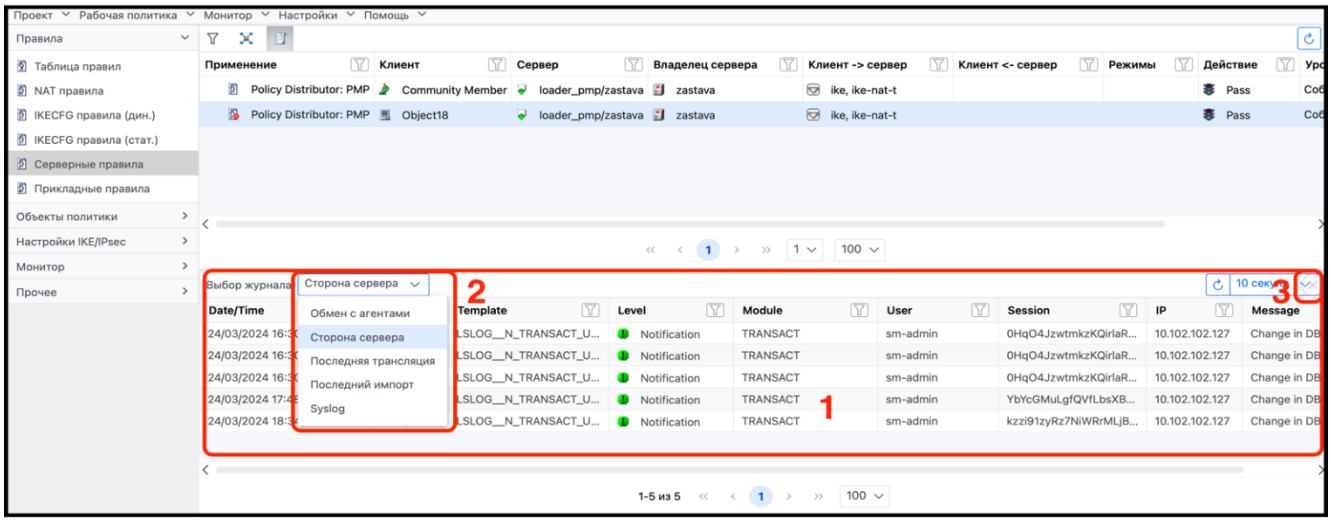


Рисунок 47 – Переход в другие журналы

Список сообщений выбранного журнала (цифра 1). Для перехода в другой журнал, нужно открыть выпадающий список (цифра 2). Выйти из режима просмотра журналов можно, нажав всплывающий элемент «⊗» (цифра 3).

6.1.7.2 Индивидуальные команды контекстного меню для элементов списка «Правила»

Индивидуальные команды контекстного меню для элементов списка «Правила»:

— «Добавить правило»;

— «Добавить дочернее правило»;

— «Добавить группу правил»;

— «Редактировать владельца»;

— «Редактировать сервер»;

— «Включить/отключить»;

— «Показать трассу».

6.1.7.2.1 Добавить правило

Для добавления правила нужно выбрать команду контекстного меню «Добавить правило», как представлено на рисунке (см. Рисунок 48).

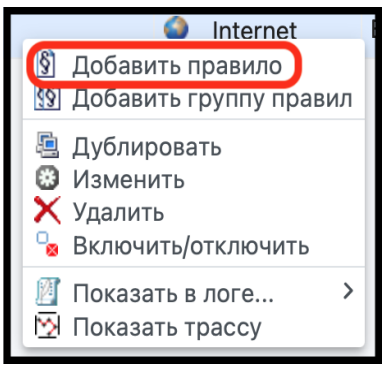


Рисунок 48 – Команда «Добавить правило»

В результате откроется окно настроек «Добавить Правило», в котором необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 49).

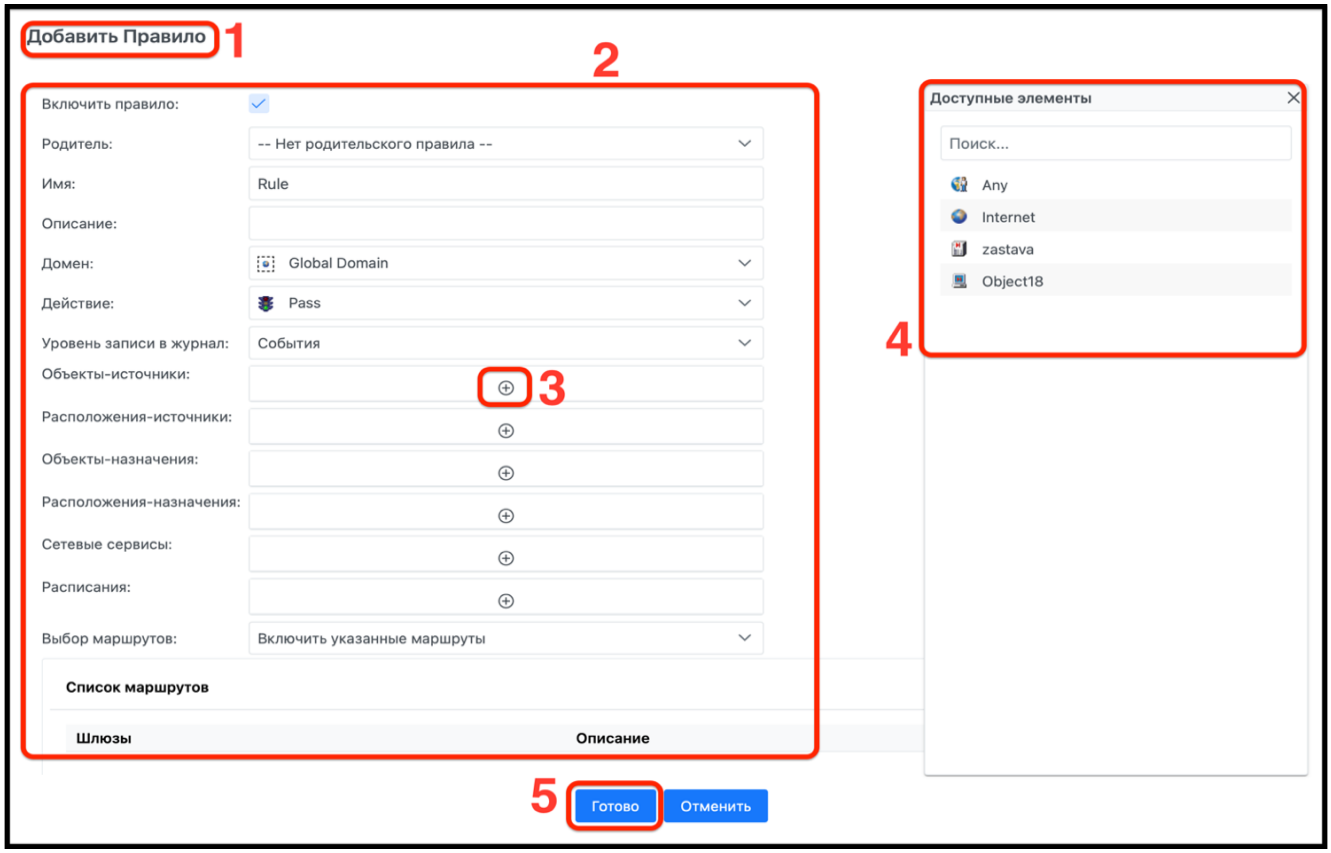


Рисунок 49 – Окно настроек «Добавить Правило»

В окне «Добавить Правило» (цифра 1) нужно заполнить форму (цифра 2), используя выпадающие списки и элемент «⊕» (цифра 3) для вызова бокового меню «Доступные элементы» (цифра 4). После завершения действий нажать кнопку «Готово» (цифра 5).

6.1.7.2.2 Добавить дочернее правило

Для добавления дочернего правила нужно выбрать команду контекстного меню «Добавить дочернее правило», как представлено на рисунке (см. Рисунок 50). Данная команда доступна только в окне элемента списка «Таблица правил».

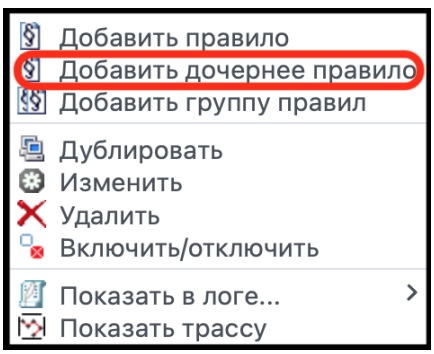


Рисунок 50 – Команда «Добавить дочернее правило»

В результате откроется окно настроек «Добавить правило», в котором необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 51).

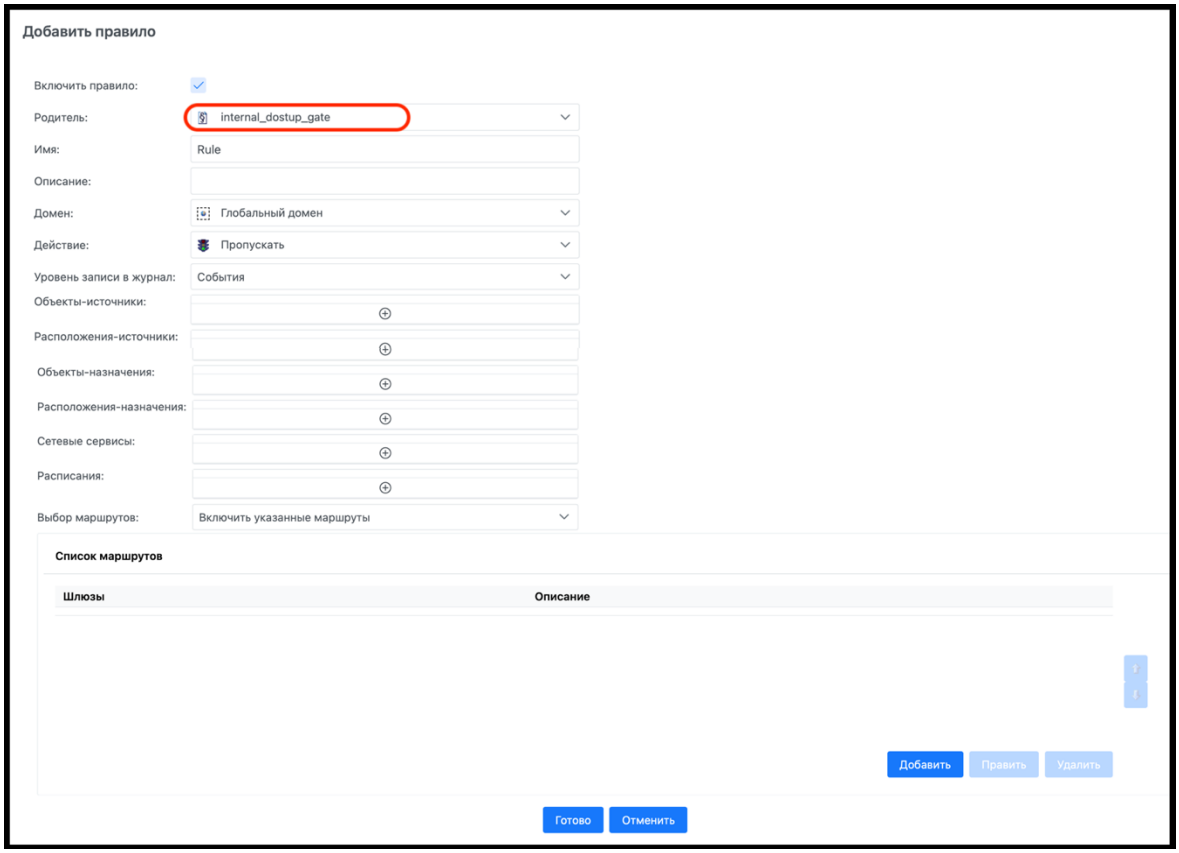


Рисунок 51 – Окно настроек «Добавить правило»

В окне «Добавить правило» необходимо заполнить форму, выбрав в выпадающем списке «Родителя», далее произвести настройку аналогично 6.1.7.2.1.

6.1.7.2.3Добавить группу правил

Для добавления правила нужно выбрать команду контекстного меню «Добавить группу правил», как представлено на рисунке (см. Рисунок 52). Данная команда доступна только в окне элемента списка «Таблица правил».

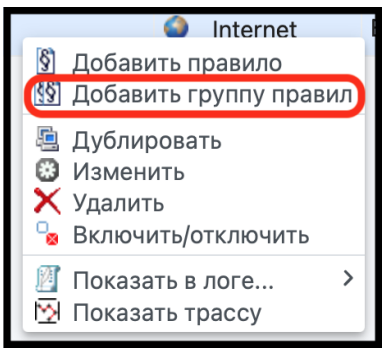


Рисунок 52 – Команда «Добавить группу правил»

В результате откроется окно «Добавить группу правил», в котором необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 53).

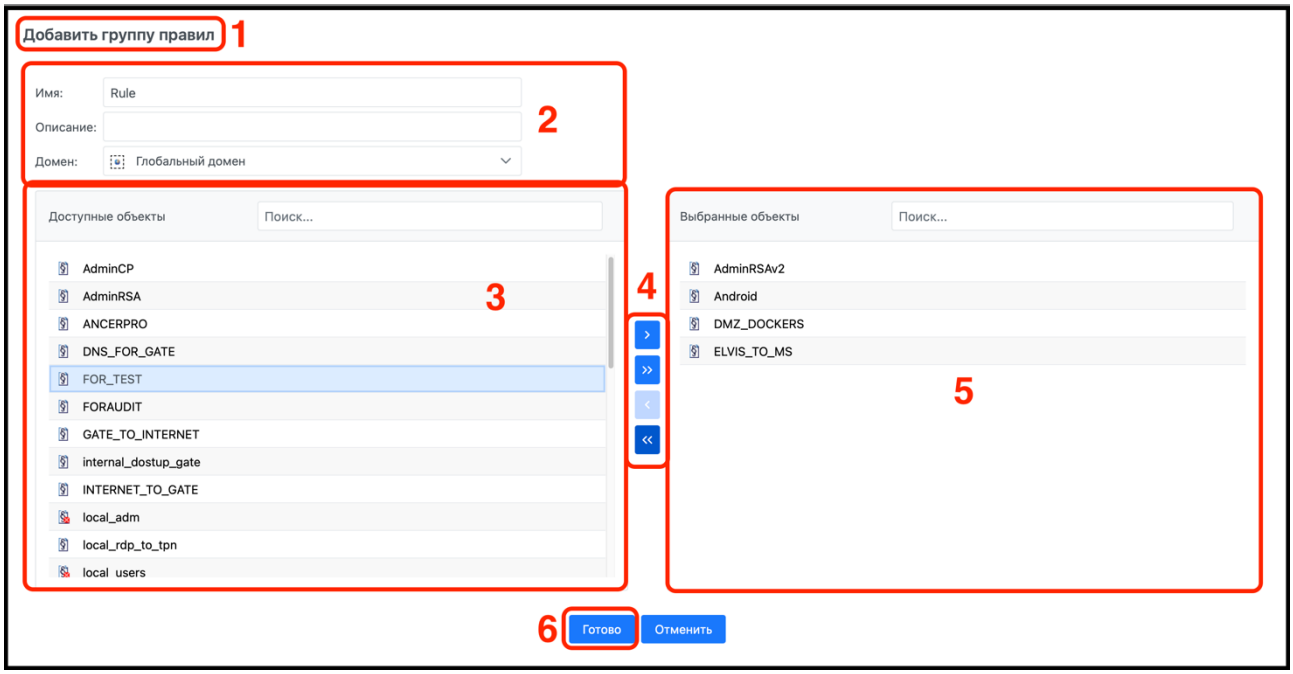


Рисунок 53 – Окно настроек «Добавить группу правил»

В окне «Добавить группу правил» (цифра 1) необходимо заполнить общий блок настроек (цифра 2), выбрать в секции «Доступные объекты» требуемое правило (цифра 3), с помощью элементов перемещения (цифра 4) переместить его в секцию «Выбранные объекты» (цифра 5). После завершения действий нажать кнопку «Готово» (цифра 6). В результате выбранные объекты объединятся в одну группу.

6.1.7.2.4 Редактировать владельца

Для редактирования владельца объекта нужно выбрать команду контекстного меню «Редактировать владельца», как представлено на рисунке (см. Рисунок 54). Данная команда доступна только в окне элемента списка «Серверные правила».

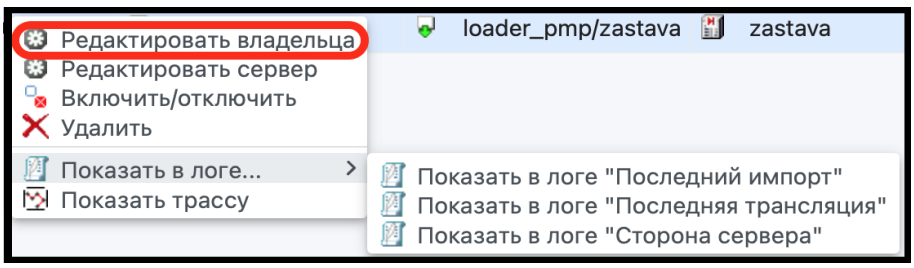


Рисунок 54 – Команда «Редактировать владельца»

В результате откроется окно «Изменить пользователя», в котором необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 55).

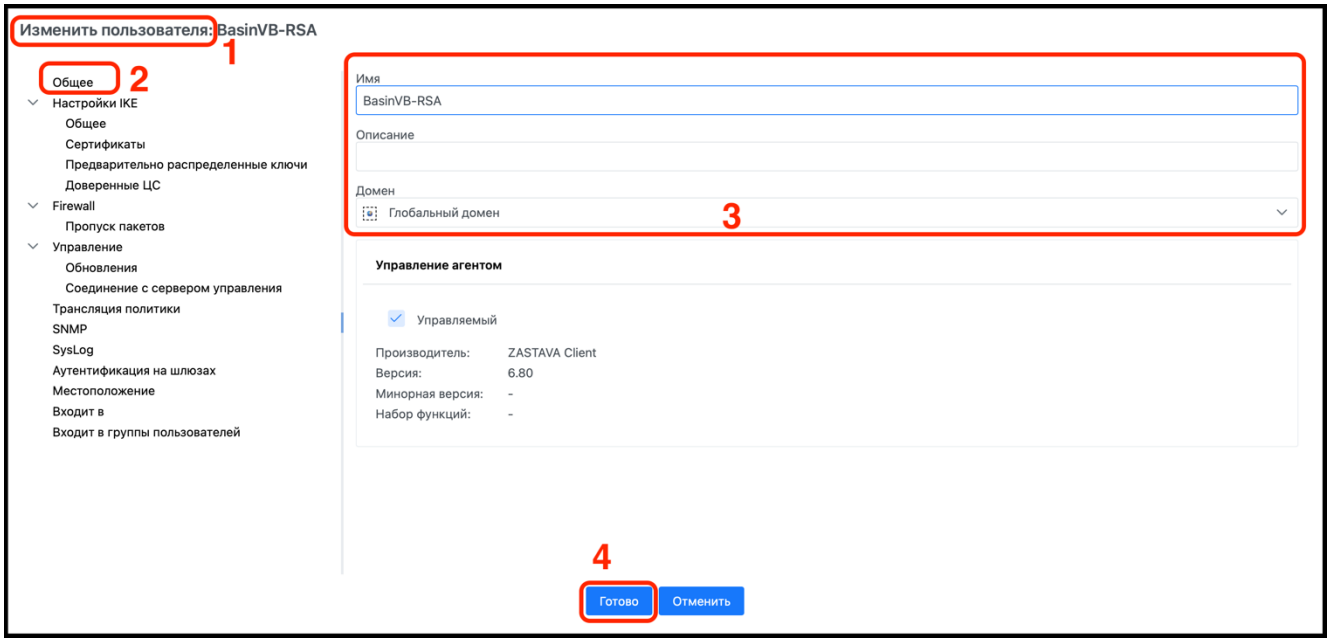


Рисунок 55 – Окно настроек «Изменить пользователя»

В окне «Изменить пользователя» (цифра 1) в элементе списка «Общее» (цифра 3) применить требуемые изменения (цифра 3) и нажать кнопку «Готово» (цифра 4).

6.1.7.2.5 Редактировать сервер

Для редактирования параметров сервера нужно выбрать команду контекстного меню «Редактировать сервер», как представлено на рисунке (см. Рисунок 56). Данная команда доступна только в окне элемента списка «Серверные правила».

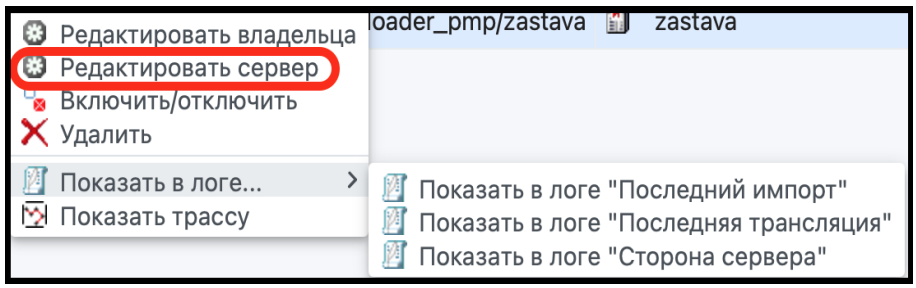


Рисунок 56 – Команда «Редактировать сервер»

В результате откроется окно «Изменить Загрузчик политики», в котором необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 57).

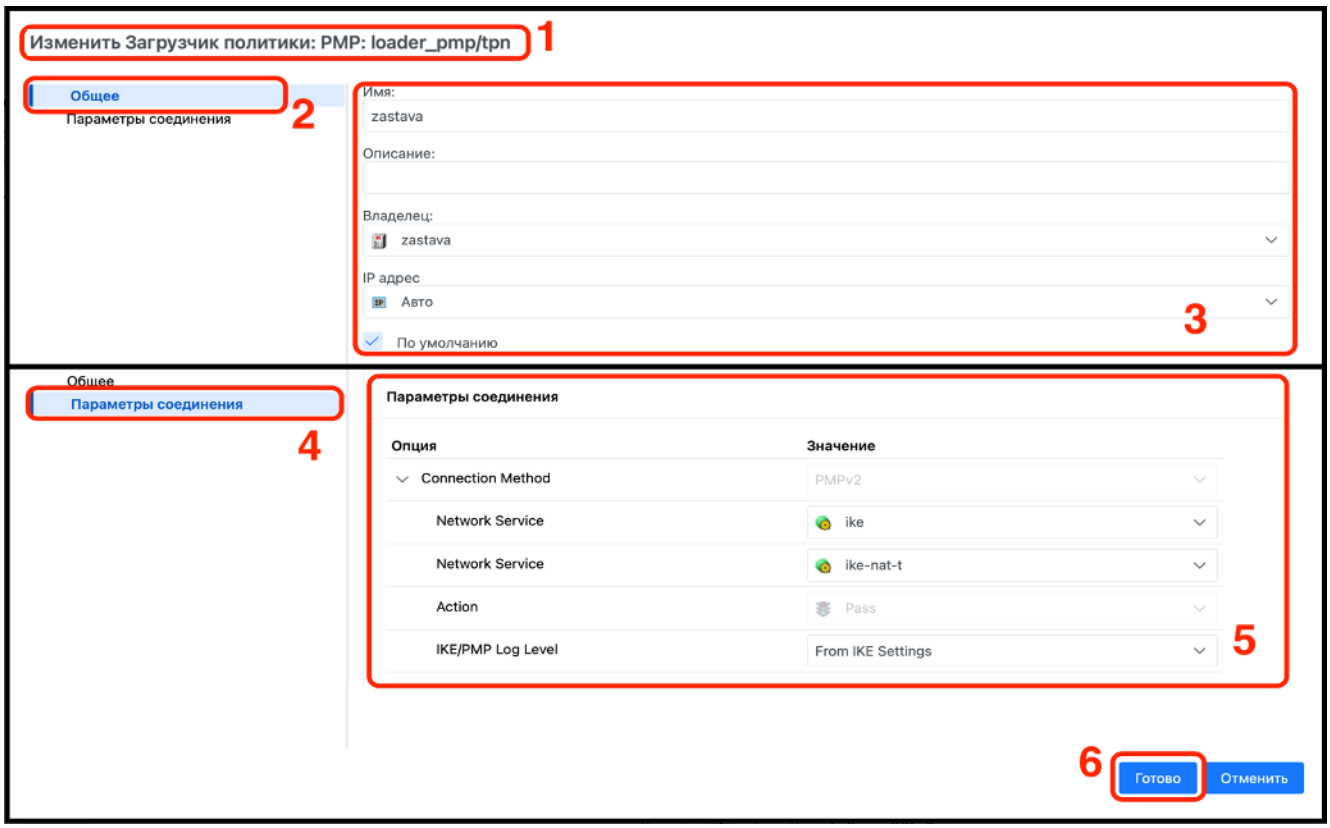


Рисунок 57 – Окно редактирования сервера

В открывшемся окне «Изменить» (цифра 1) необходимо изменить настройки выбранного объекта. В элементе списка «Общее» (цифра 2) редактировать параметры объекта (цифра 3). В элементе списка «Параметры соединения» (цифра 4) произвести необходимые изменения в настройках соединения (цифра 5) (в примере представлено окно для редактирования загрузчика политики). После завершения действий нажать кнопку «Готово» (цифра 6).

6.1.7.2.6 Включить/отключить

Способность к включению/отключению отдельных правил является одним из основных аспектов процесса создания и тестирования ГПБ. Также это может пригодиться для введения временных изменений в рабочую среду безопасности. Отключенное правило не будет транслироваться, и, таким образом, отключение правил может использоваться для определения неисправностей.

Для отключения правила необходимо выбрать требуемое правило или группу правил, вызвать контекстное меню и выбрать команду «Включить/отключить», как представлено на рисунке (см. Рисунок 58).

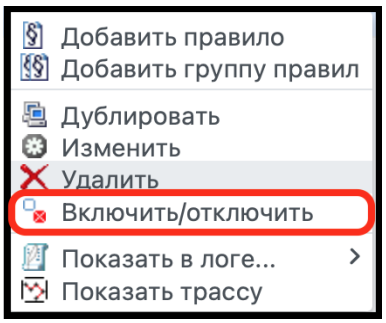


Рисунок 58 – Команда «Включить/отключить»

В результате в строке выбранного правила элемент « » поменяет свой вид на «». Если родительское правило будет заблокировано, то вместе с ним будут заблокированы все его «дочерние» правила. Для включения правила необходимо снова выбрать команду «Включить/отключить».

Можно выключать и включать несколько правил с помощью одной команды. Для этого необходимо выделить правила, которые требуется выключить или включить, затем использовать в контекстном меню команду «Выключить/отключить».

6.1.7.2.7 Показать трассу

Использовать для наглядности трассу взаимодействия между объектами можно, выбрав в контекстном меню команду «Показать трассу», как показано на рисунке (см. Рисунок 59).

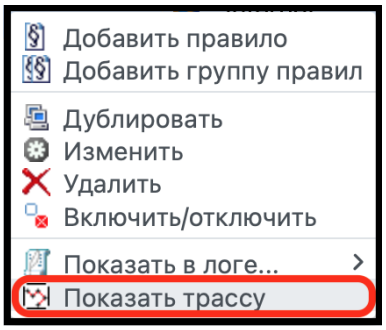


Рисунок 59 – Показать трассу

В результате откроется дополнительное окно «Топология». Вид окна с отображением топологии представлен на рисунке (см. Рисунок 60).

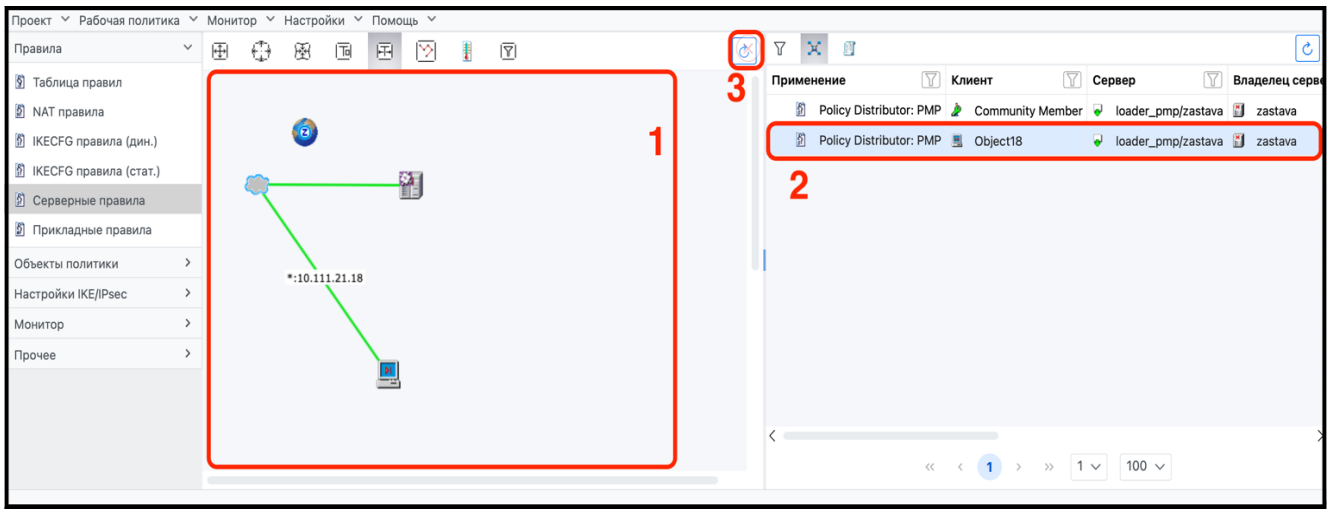


Рисунок 60 – Трасса взаимодействия

Окно топологии (цифра 1) с отображением взаимодействия выбранного объекта (цифра 2) с другими. Закрыть окно «Топология» можно, нажав элемент «⊗ » (цифра 3).

6.2 Вкладка боковой панели «Объекты политики»

Вкладка боковой панели «Объекты политики» позволяет добавлять объекты политики и управлять ими. Вид вкладки боковой панели «Объекты политики» изображен на рисунке (см. Рисунок 61).

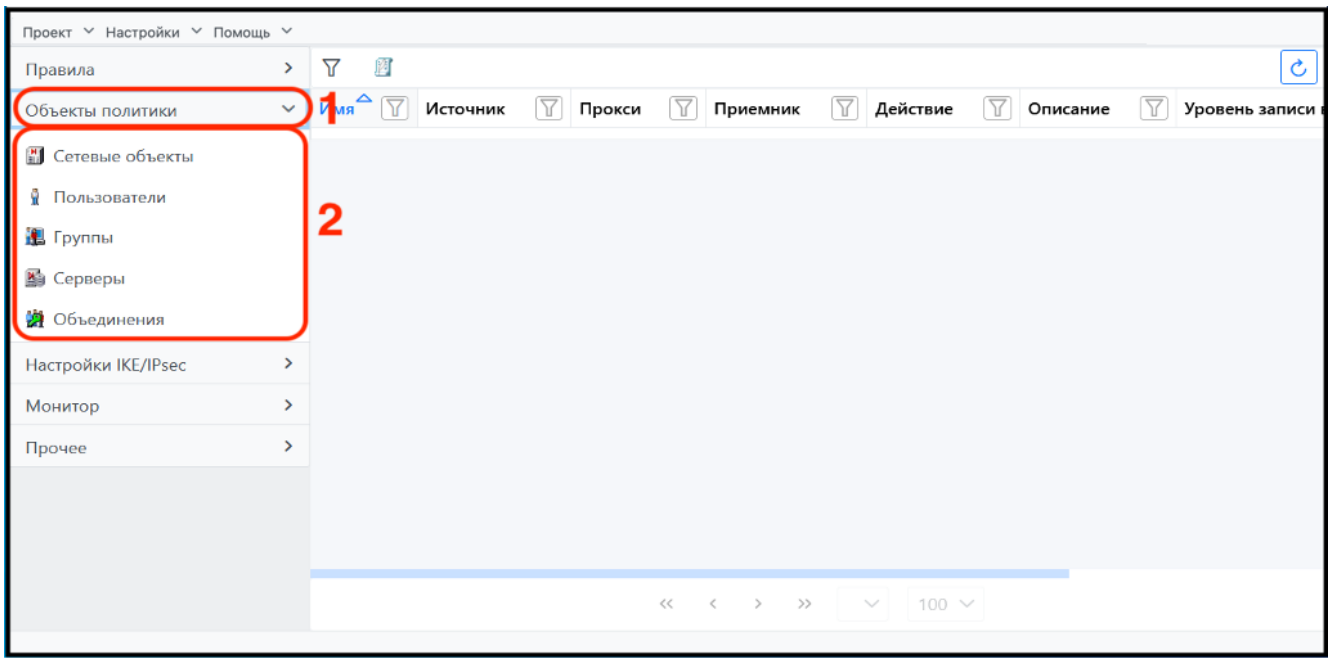


Рисунок 61 – Вкладка «Объекты политики»

На вкладке боковой панели «Объекты политики» требуется нажать на элемент « › » (цифра 1) для перехода к элементам списка (цифра 2):

— «Сетевые объекты»;

— «Пользователи»;

— «Группы»;

— «Серверы»;

— «Объединения».

6.2.1 Сетевые объекты

Вид окна элемента списка «Сетевые объекты» изображен на рисунке (см. Рисунок 62).

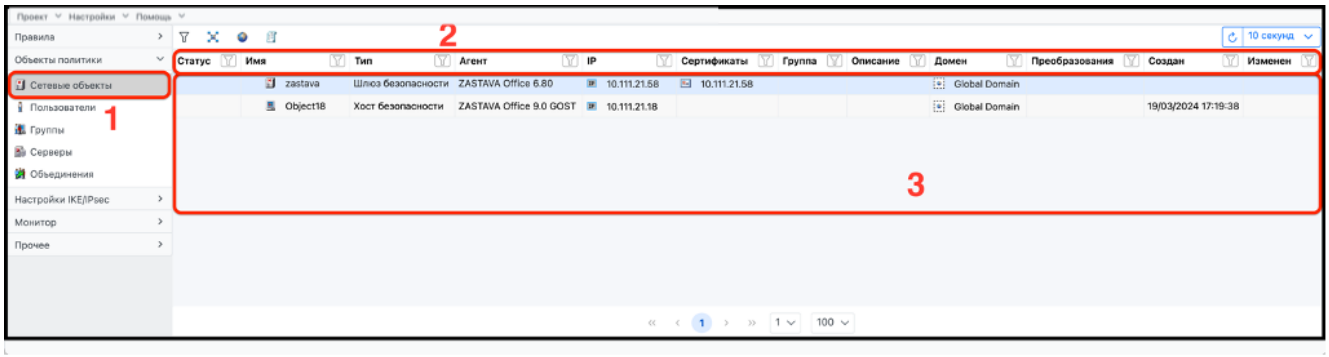


Рисунок 62 – Элемент списка «Сетевые объекты»

В окне элемента списка «Сетевые объекты» (цифра 1) отобразится таблица со следующими параметрами (цифра 2):

— «Статус»;

— «Имя». Имя сетевого объекта;

— «Тип». Тип агента сетевого объекта;

— «Агент». Отдельный персональный компьютер, на котором установлены «ЗАСТАВА-Клиент» или шлюз с «ЗАСТАВА-Офис» или АПК «ЗАСТАВА» см. Приложение 3;

— «IP». IP-адрес, под которым происходило подключение сетевого объекта;

— «Сертификаты». Персональный сертификат сетевого объекта;

— «Группа». Перечень групп, в которые включен сетевой объект;

— «Описание». Краткое описание, указанное при создании объекта;

— «Домен». Домен, которому принадлежит сетевой объект;

— «Преобразование». Добавленные к ЛПБ объекта текстовые данные;

— «Создан». Дата и время создания объекта;

— «Изменен». Дата и время изменения объекта.

По каждому из параметров возможна сортировка списка.

В рабочей области таблицы параметров сетевых объектов (цифра 3) будут отображены физические устройства, созданные ранее, и зарегистрированные в ПО ЗУ объекты ГПБ, такие как:

— «Шлюзы безопасности» (управляемые, неуправляемые);

— «Хосты безопасности»;

— «Подсети»;

— «IP-диапазоны»;

— «IP-хосты».

6.2.1.1 Работа с контекстным меню для элементов списка «Сетевые объекты»

Для добавления объектов следует вызвать контекстное меню, нажав правой клавишей мыши на выбранный объект в списке, или на свободное место в рабочей области таблицы.

Контекстное меню элемента списка «Сетевые объекты» для добавления или редактирования представлено на рисунке (см. Рисунок 63).

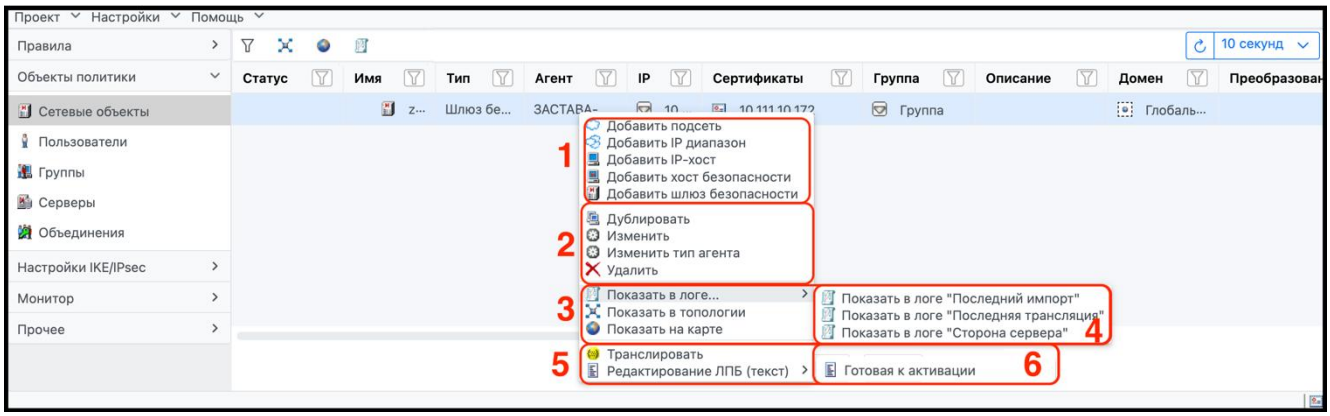


Рисунок 63 – Контекстное меню элемента списка «Сетевые объекты»

В блоке контекстного меню (цифра 1) отображается список команд для добавления объектов политики. Этот блок контекстного меню вызывается со свободного места рабочей области таблицы. Добавление объектов политики подробно описано в разделе 7.

Команды для редактирования объектов политики отображаются в блоке контекстного меню (цифра 2). Команды для просмотра состояний и размещения, а также удаления объектов политики отображаются в блоке (цифра 3), а также быстрого доступа в просмотр журналов (цифра 4).

Команды: «Дублировать», «Изменить», «Удалить», «Показать в логе» являются общими для всех объектов ПО ЗУ. Эти команды выполняются аналогично описанию, приведённому в п. 6.1.7.1.

Команды для запуска трансляции и редактирования текста ЛПБ отображаются в блоке (цифра 5), в выпадающем списке отобразится статус ЛПБ с переходом в текстовый редактор (цифра 6).

6.2.2 Элемент списка «Пользователи»

В элементе списка «Пользователи» содержится информация о подключенных к ПО ЗУ СВТ с установленными агентами «ЗАСТАВА-Клиент» (перечень поддерживаемых программных

изделий линейки «ЗАСТАВА-Клиент» приведён в приложении см. Приложение 3). Агенты «ЗАСТАВА-Клиент» не имеют фиксированного IP-адреса, назначаемого DHCP-сервером, и обладают собственной системой шифрования, позволяющей осуществлять безопасное соединение с узлом, который находится вне среды безопасности.

Вид окна элемента списка «Пользователи» изображен на рисунке (см. Рисунок 64).

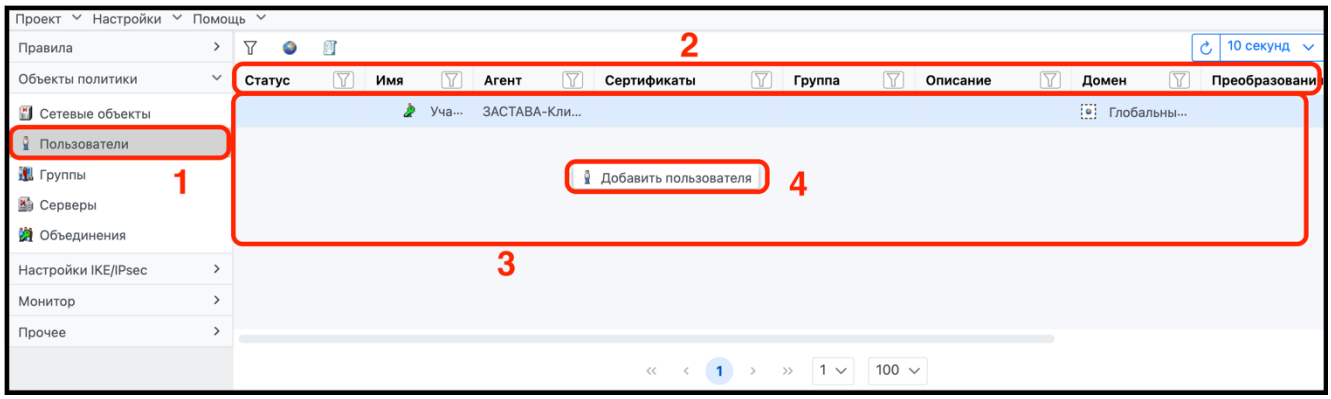


Рисунок 64 – Команда «Пользователи»

В окне элемента списка «Пользователи» (цифра 1) отобразится таблица со следующими параметрами (цифра 2):

— «Статус»;
— «Имя». Имя сетевого объекта;
— «Агент». Отдельный персональный компьютер, на котором установлены «ЗАСТАВА-Клиент» или шлюз с «ЗАСТАВА-Офис» или АПК «ЗАСТАВА» см. Приложение 3;
— «Сертификаты». Персональный сертификат сетевого объекта;
— «Группа». Перечень групп, в которые включен сетевой объект;
— «Описание». Краткое описание, указанное при создании объекта;
— «Домен». Домен, которому принадлежит сетевой объект;
— «Преобразование». Добавленные к ЛПБ объекта текстовые данные;
— «Создан»;
— «Изменен».

По каждому из параметров возможна сортировка списка.

Для добавления первого объекта в элемент списка «Пользователи» нажать правую клавишу мыши в свободном месте рабочей области таблицы, затем выбрать появившуюся команду контекстного меню «Добавить пользователя» (цифра 4).

В открывшемся окне «Выберите версию агента» требуется выполнить шаги, изображенные на рисунке (см. Рисунок 65).

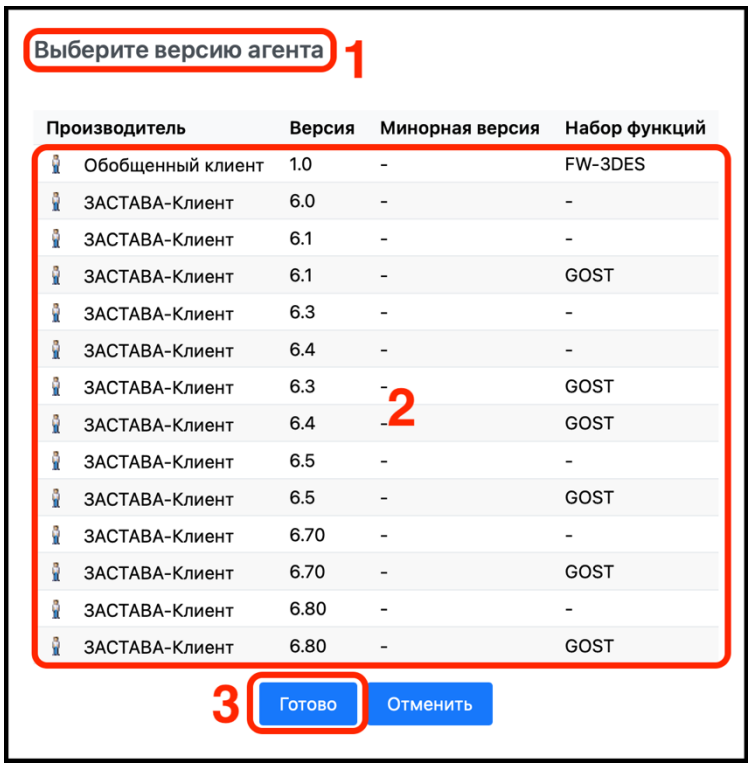


Рисунок 65 – Окно выбора агента

В окне «Выберите версию агента» (цифра 1) выбрать в списке требуемую версию (цифра 2) и нажать кнопку «Готово» (цифра 3).

6.2.2.1 Работа с контекстным меню для элементов списка «Пользователи»

Вызвать контекстное меню можно, нажав правой клавишей мыши на выбранный объект в списке или на свободное место в рабочей области таблицы.

Команды контекстного меню элемента списка «Пользователи» представлены на рисунке (см. Рисунок 66).

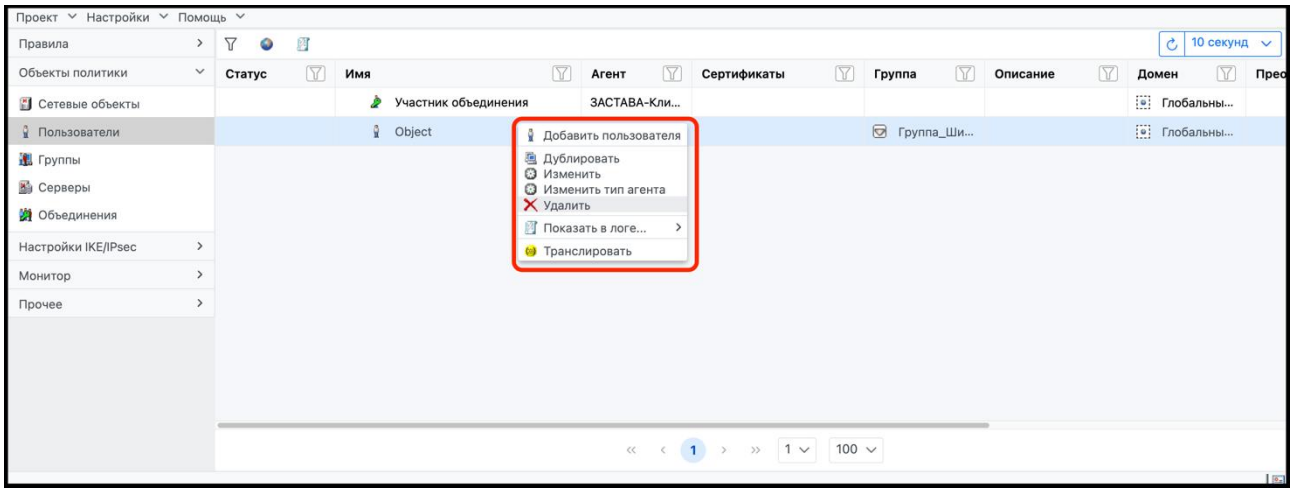


Рисунок 66 – Команда «Пользователи»

В контекстном меню отобразятся следующие команды:

— «Добавить пользователя»;

— «Дублировать»;
— «Изменить»;
— «Изменить тип агента»;
— «Удалить»;
— «Показать в логе»;
— «Транслировать».

6.2.3 Группы

Объекты политики можно 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. Приоритетно создание группы при любой возможности, это поможет снизить количество используемых правил.

Перед тем, как применить какое-либо правило к группе, необходимо 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.

Вид окна элемента списка «Группы» изображен на рисунке (см. Рисунок 67).

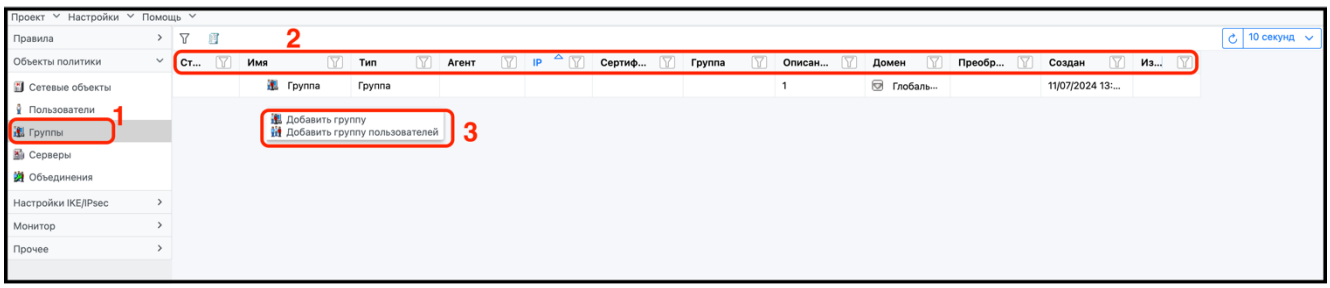


Рисунок 67 – Окно «Группы»

В окне «Группы» (цифра 1) отобразится таблица параметров (цифра 2). Список параметров содержит:

— «Статус»;
— «Имя». Имя группы;
— «Тип». Типы пользователей, входящих в группу. В группу могут включаться другие группы;
— «Агент». Тип агента каждого пользователя группы;

— «IP». IP-адреса всех пользователей группы, под которыми происходило подключение пользователей;

— «Сертификаты». Персональные сертификаты пользователей группы;

— «Группа». Перечень групп, в которые включены пользователи группы;

— «Описание». Краткое описание группы;

— «Домен». Домен, которому принадлежат пользователи группы;

— «Преобразования текстов». Добавленные к ЛПБ объекта текстовые данные;

— «Создан». Время создания объекта;

— «Изменен». Время изменения объекта.

По каждому из параметров возможна сортировка списка.

Для добавления новой группы или группы пользователей требуется вызвать контекстное меню правой клавишей мыши (цифра 3).

6.2.3.1 Добавление группы

В открывшемся окне настроек «Добавить группу» выполнить шаги, изображённые на рисунке (см. Рисунок 68).

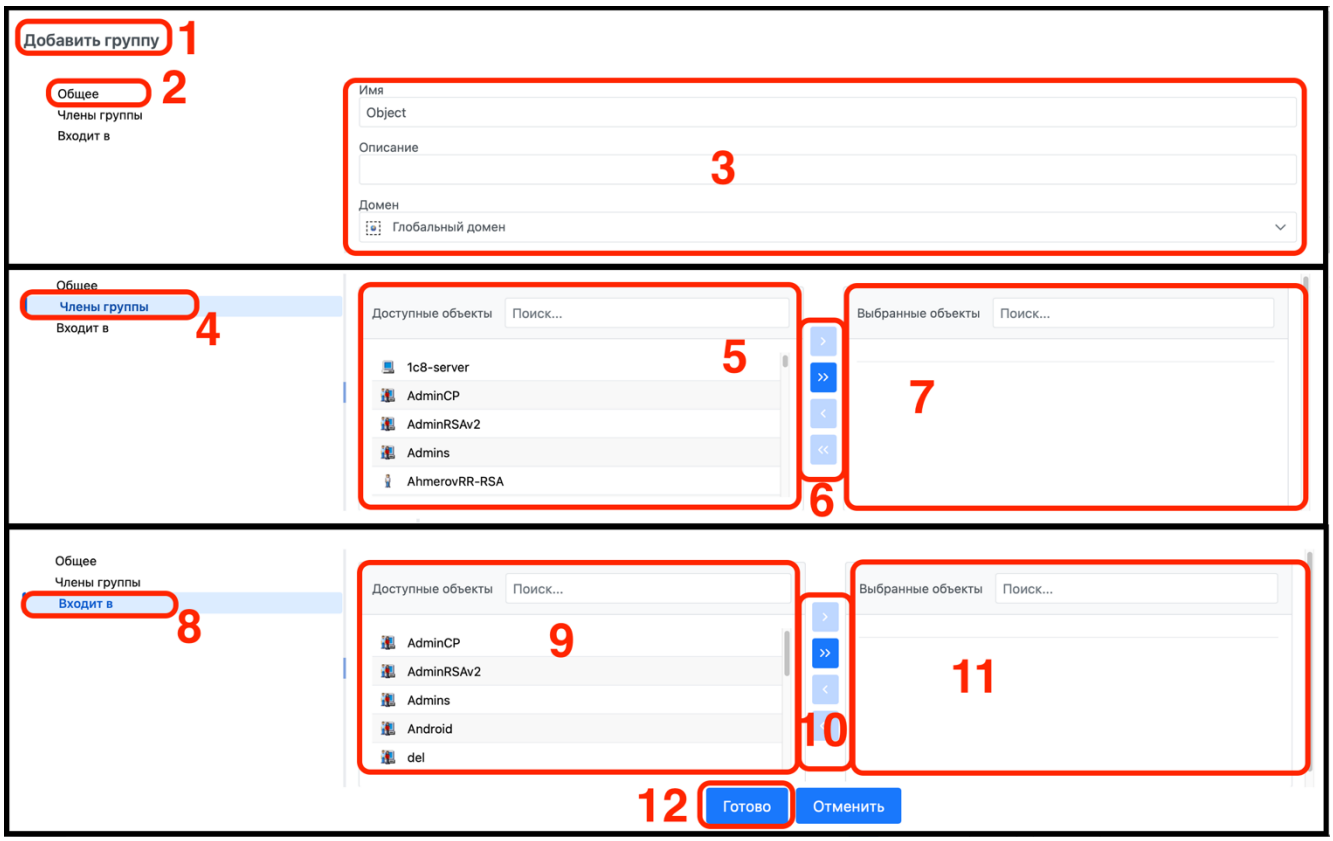


Рисунок 68 – Окно добавления группы

1) В окне настроек «Добавить группу» (цифра 1) в элементе списка «Общее» (цифра 2) заполнить параметры блока настроек (цифра 3):

— ввести уникальное имя для данного объекта группы;

— выбрать домен, в который будет входить данный объект группа;

— при необходимости можно ввести текстовое описание объекта;

2) в элементе списка «Члены группы» (цифра 4) выбрать объекты политики из области «Доступные объекты» (цифра 5) и, используя элементы перемещения (цифра 6), переместить их в область «Выбранные объекты» (цифра 7);

3) в элементе списка «Входит в» (цифра 8) в области «Доступные объекты» (цифра 9) будет отображен перечень созданных ранее групп, в котором, при необходимости, можно выбрать группы для перемещения их из одного списка в другой и с помощью элементов перемещения (цифра 10) переместить их в область «Выбранные объекты» (цифра 11);

Нажать кнопку «Готово» (цифра 12).

Вид окна элемента списка «Группы» с добавленными объектами изображен на рисунке (см. Рисунок 69).

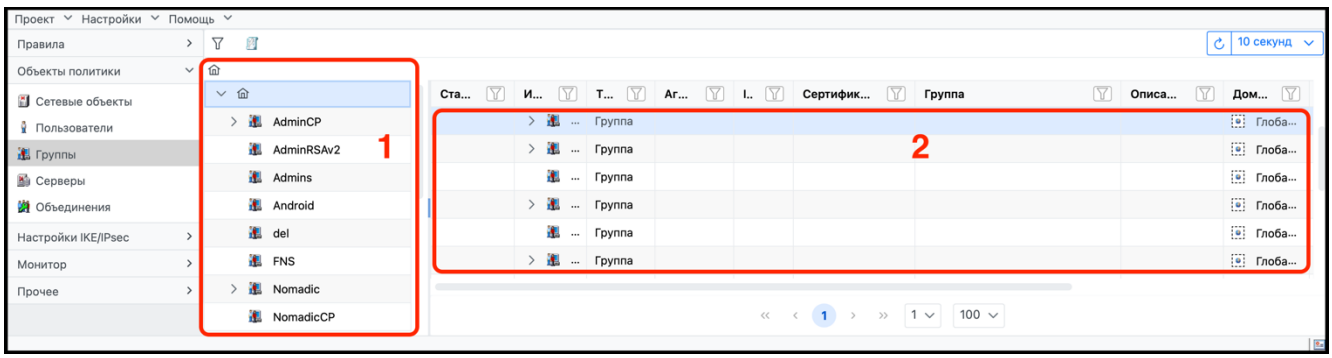


Рисунок 69 – Результат добавления в группу объектов политики

Добавленные группы будут отображаться в списке созданных групп (цифра 1). В случае, если ни одна из них не выбрана, добавленные группы также будут отображаться в рабочей области таблицы (цифра 2). Далее, при необходимости, можно создать иерархическую структуру вложенных групп.

6.2.3.2 Создание иерархической структуры групп

Для создания иерархической структуры групп необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 70).

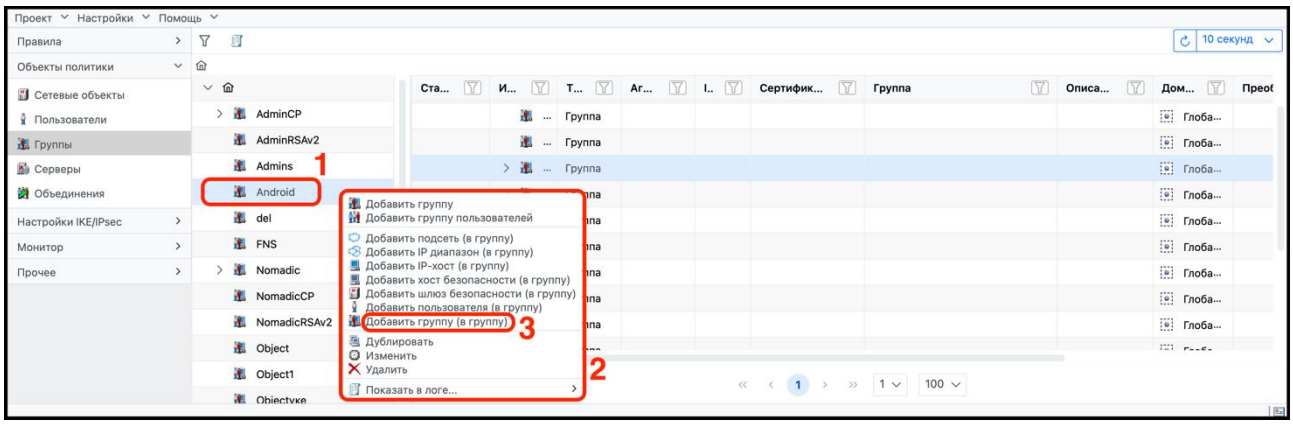


Рисунок 70 – Создание иерархической структуры дочерних групп

Выбрать созданную ранее группу (цифра 1), вызвать правой клавишей мыши ее контекстное меню (цифра 2), выбрать команду «Добавить группу (в группу)».

В открывшемся окне настроек «Добавить группу» выполнить шаги, аналогичные описанным в 6.2.3.1.

После выполнения настроек посмотреть добавленные в группу вложения можно, выполнив шаги, изображённые на рисунке (см. Рисунок 71).

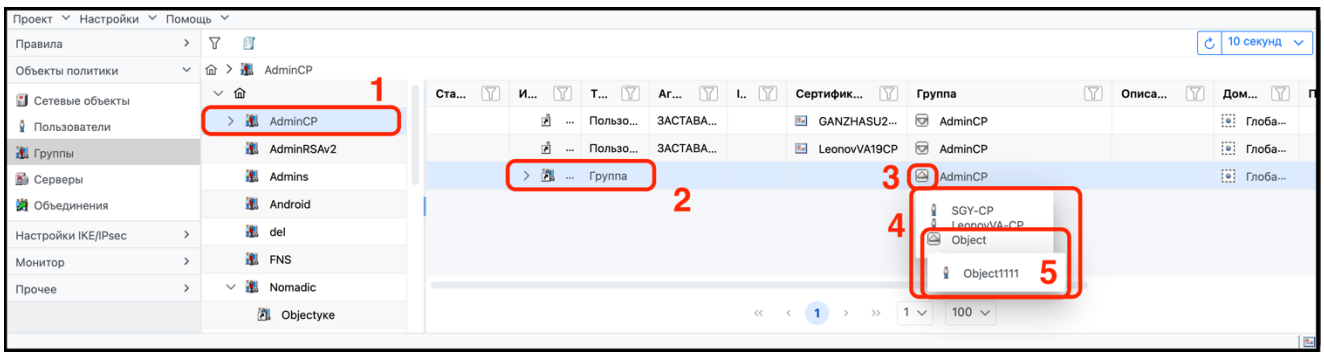


Рисунок 71 – Содержания вложений группы

Для просмотра вложений нажать левой клавишей мыши на требуемую родительскую группу (цифра 1), в рабочей области таблицы в списке вложенных объектов отобразится добавленная дочерняя группа (цифра 2). Посмотреть содержимое добавленной группы можно с помощью элемента «» (цифра 3), при нажатии на который откроется список вложений (цифра 4). Переход к просмотру последующих вложений иерархического списка (цифра 5) (если таковой имеется), осуществляется нажатием на элемент «» (цифра 4) соответствующего иерархического уровня.

Открыть добавленные вложения можно также в списке групп, выполнив шаги, изображённые на рисунке (см. Рисунок 72).

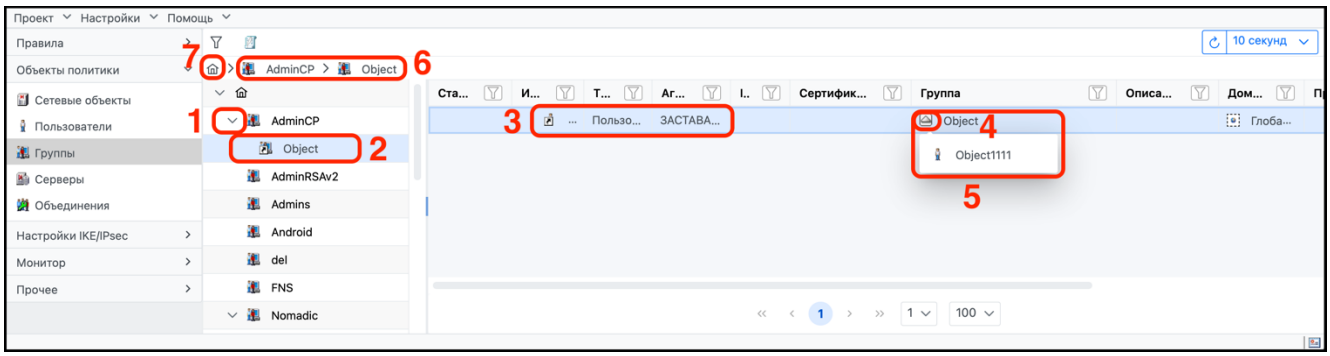


Рисунок 72 – Содержания вложений в списке группы

Для просмотра вложения из списка групп необходимо выбрать требуемую родительскую группу и открыть список вложенных элементов при помощи элемента «⌄» (цифра 1), далее выбрать вложенную дочернюю группу (цифра 2). В рабочей области таблицы отобразится только выбранная дочерняя группа (цифра 3). При помощи элемента «✉» (цифра 4) можно посмотреть содержимое дочерней группы (цифра 5). Для удобства восприятия будет отображен иерархический путь вложений (цифра 6). Отменить выбор группы можно, нажав кнопку «⌂» (цифра 6).

6.2.3.3 Работа с контекстным меню для элементов списка «Группы»

Контекстное меню элемента списка «Группы» представлено на рисунке (см. Рисунок 73).

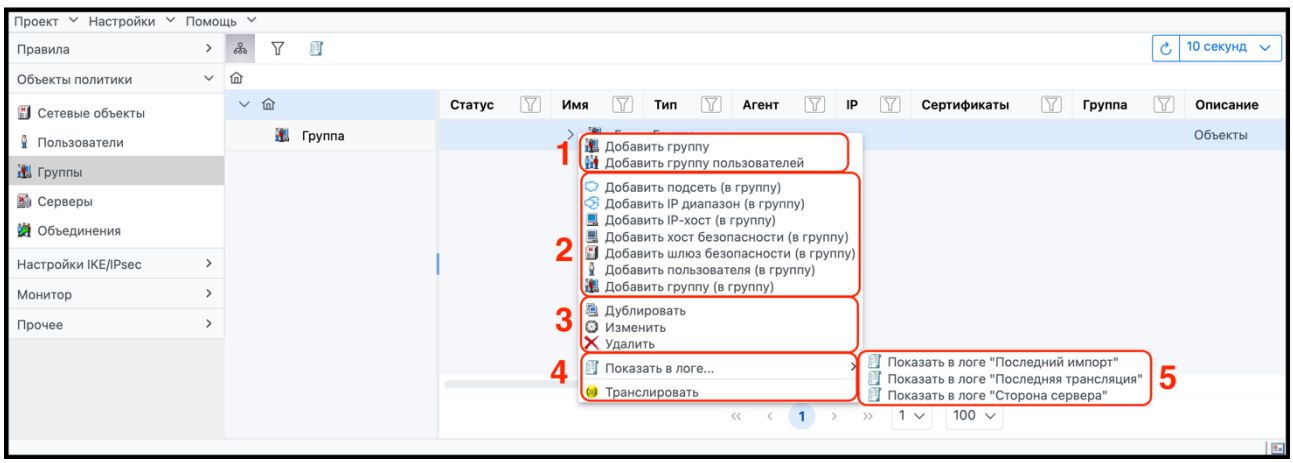


Рисунок 73 – Контекстное меню элемента списка «Группы»

В блоке (цифра 1) контекстного меню отображается список команд для добавления групп и создания групп пользователей. Этот блок контекстного меню вызывается со свободного места рабочей области таблицы.

Команды для добавления в группы объектов политики отображаются в блоке контекстного меню (цифра 2). Команды для дублирования, редактирования, удаления объектов политики отображаются в блоке (цифра 3).

Команды для запуска трансляции, просмотра журнала отображаются в блоке (цифра 4), а также для быстрого доступа к журналам в выпадающем списке (цифра 5).

6.2.4 Серверы

Элемент списка «Серверы» позволяет создавать и редактировать объекты политики безопасности, выполняющие сервисные функции (серверы), необходимые для работы защищенной сети. Также существует возможность добавления интеграций сторонних ПО и серверов обновления.

Вид окна элемента списка «Серверы» изображен на рисунке (см. Рисунок 74).

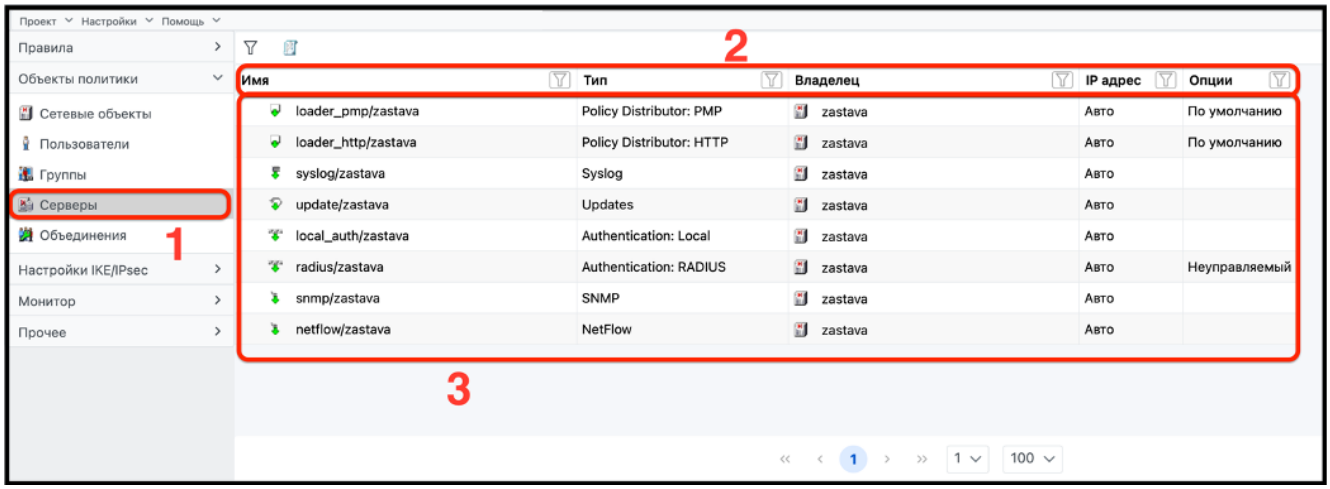


Рисунок 74 – Элемент списка «Серверы»

Окно «Серверы» (цифра 1) отображает параметры серверов в виде таблицы с указанием следующей информации (цифра 2):

— «Имя»;
— «Тип»;
— «Владелец» (объект политики, который выполняет функции сервера);
— «IP-адрес»;
— «Опции».

По каждому из параметров возможна сортировка списка.

В рабочей области таблицы отображается список серверов (цифра 3).

6.2.4.1 Добавления серверов

Для добавления требуемого сервера необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 75).

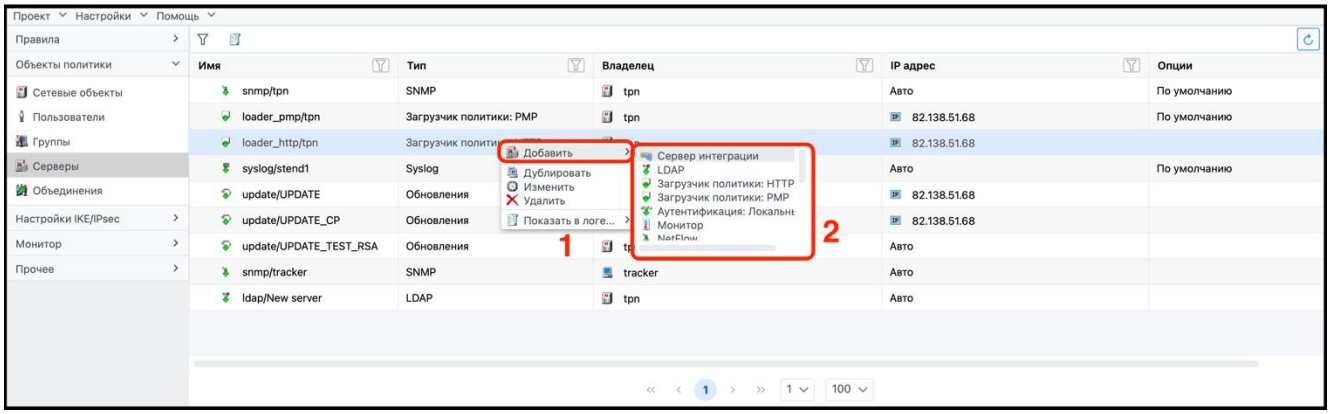


Рисунок 75 – Контекстное меню элемента списка «Серверы»

Вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем нажать на появившуюся команду «Добавить» (цифра 1). Выбрать из списка требуемый сервер (цифра 2). Типы серверов представлены в таблице (см. Таблица 7).

Таблица 7 – Типы серверов

Тип сервера	Назначение объектов, содержащихся в списке
PMP Distribution Service	Описания сервисов-прогрузчиков, которые используются для доставки и активации ЛПБ на объекты с агентами через протокол PMP
FTP Proxy Server	Описания прокси-серверов для протокола FTP, которые могут быть установлены на объектах с агентами
SMTP Proxy Server	То же, но для протокола SMTP
HTTP Proxy Server	То же, но для протокола HTTP
SOCKS Proxy Server	То же, но для протокола SOCKS
NetFlow	Используется для включения в политику сервера, собирающего от агентов информацию о трафике по протоколу NetFlow
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 клиентов защищенног удаленного доступа по протоколу XAUTH. Данный протокол поддерживается некоторыми типами шлюзов защищенного удаленного доступа и конфигурируется в их свойствах в окне «Пропуск пакетов ->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 от управляемых агентов по протоколу Syslog
Update Server	Описания веб-серверов, которые используются агентами для проверки и скачивания автоматических обновлений
Policy Distr HTTP	Описания сервисов-прогрузчиков, которые используются для доставки и активации ЛПБ на объекты с агентами через протокол HTTP

Тип сервера	Назначение объектов, содержащихся в списке
Authentication Local	Сервер для локальной аутентификации пользователей, например, при аутентификации в рамках работы HTTP-прокси. Сервер этого типа добавляется при создании учетной записи для локальной аутентификации в настройках пользователя
Monitor	Интеграция с ПО БДМ
Integration	Объект для интеграции с внешними веб-приложениями

6.2.4.1.1 Общие настройки для всех типов серверов

В окне добавления и настройки серверов «Общее» перечислены все общие параметры настройки для всех типов серверов, изображенные на рисунке (см. Рисунок 76).

Рисунок 76 – Окно настроек «Общее»

Перейти в окно общих настроек «Общее» (цифра 1), заполнить форму настроек (цифра 2). Все общие параметры настроек для всех типов серверов представлены в таблице (см. Таблица 8).

Таблица 8 – Общие настройки объектов типа сервер

Параметр	Значение
Имя	Название сервера (произвольное). Данное название используется внутри ПО ЗУ 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: – выбрать один из интерфейсов хоста; – 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.)
Управляемый	Если флажок установлен, то для вновь создаваемых объектов политики данный сервер будет управляемый
Установить, как сервер по умолчанию	Если флажок установлен, то для вновь создаваемых объектов политики данный сервер будет автоматически привязываться как удаленный сервер

Перед добавлением объекта сервера, в элементе списка «Топология» или во вкладке боковой панели «Объекты политики» необходимо создать объект политики, на котором будет установлен сервер.

6.2.4.2 Серверы-прогрузчики

Любой объект с установленным агентом «ЗАСТАВА-Офис» (см. Приложение З) может быть использован как сервер-прогрузчик. В большинстве случаев в роли сервиса прогрузки выступает данный экземпляр ПО ЗУ (а именно, сервер TPNDistributor).

Использование удаленных серверов-прогрузчиков позволяет разгрузить основной сервер-прогрузчик при большом количестве управляемых объектов.

6.2.4.2.1 Добавление и настройка загрузчика политики PMP

Этот сервер представляет собой сервис-прогрузчик для агентов, который передает ЛПБ на управляемые агенты по протоколу PMP (Policy Management Protocol).

6.2.4.2.2 Объекты PMP Distribution Service.

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.

Для добавления прогрузчика политики PMP требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Далее выбрать из дополнительного списка требуемый сервер. Для добавления и настройки сервера прогрузчика политики PMP требуется выполнить шаги, представленные на рисунке (см. Рисунок 77).

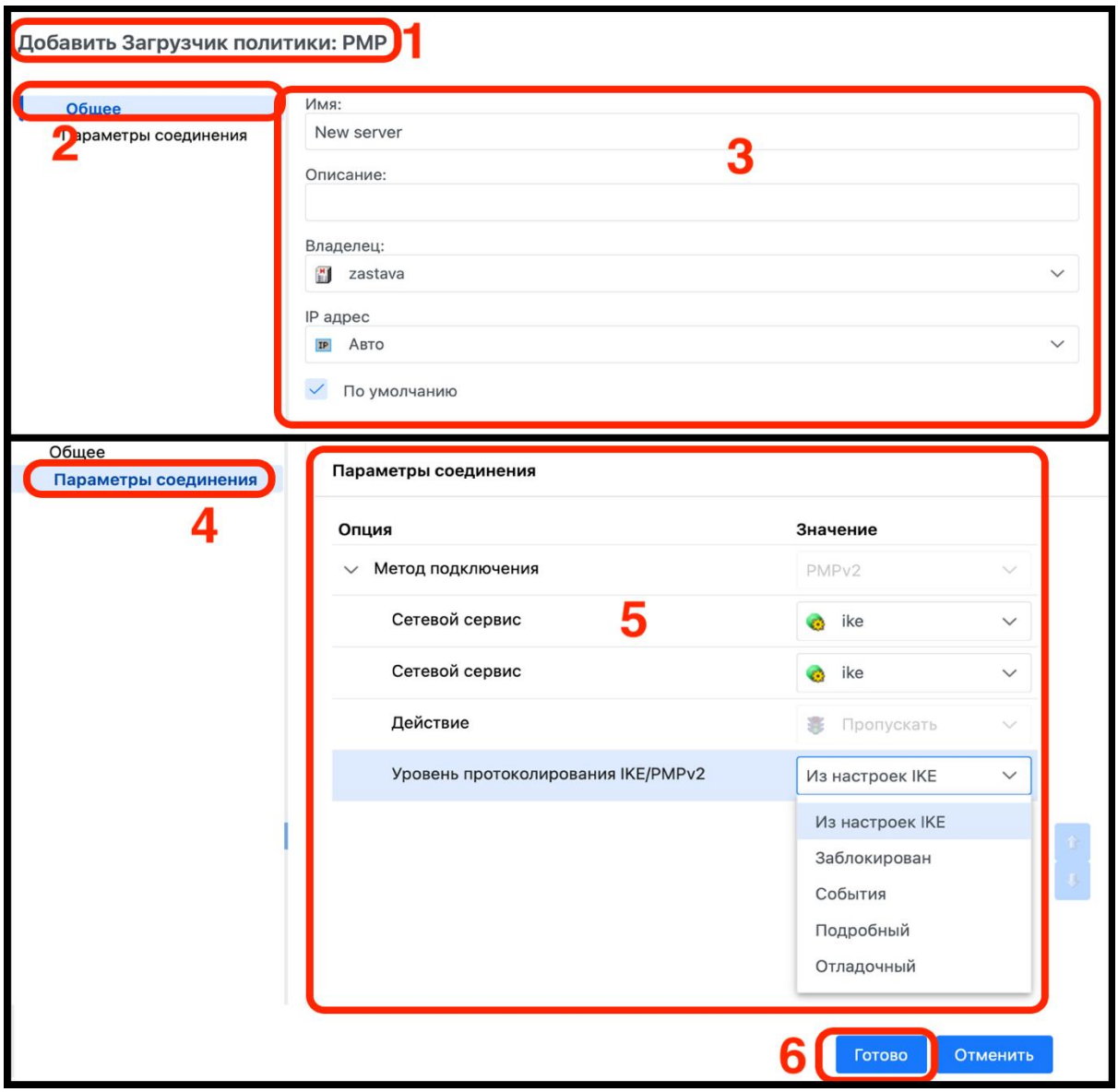


Рисунок 77 – Окно настройки загрузчика политики PMP

1) Перейти в окно настроек «Добавить Загрузчик политики: PMP» (цифра 1);
2) в элементе списка «Общие» (цифра 2) выполнить настройки блока (цифра 3). Подробное описание настроек представлено в таблице (см. Таблица 8);
3) в элементе списка «Параметры соединения» (цифра 4) заполнить требуемые параметры в блоке настроек (цифра 5):

— «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. 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;

— «Действие». 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». Задает уровень протоколирования событий. Возможны следующие значения, в порядке возрастания количества потенциальных протоколируемых сообщений:
  – «Заблокирован»;
  – «События»;
  – «Детальный»;
  – «Отладочный»;
  – «Из настроек IKE»;

4) чтобы сервер прогрузчик ЛПБ выполнял свои функции, необходимо на агентах, которые будут загружать с него политику, правильно указать удаленный сервер в параметрах соединения:
— на хосте, на котором реализован сервер прогрузчик ЛПБ, нужно указать параметр vpnconfig –set jk HTTP UIR http://<tpn ip>:3118/distributor/, где <tpn ip> - IP-адрес ПО ЗУ;
— корректно указать параметры загрузки политики на агентах, которые будут загружать политику с сервера прогрузчика ЛПБ;
5) после выполненных настроек нажать кнопку «Готово» (цифра 6).

6.2.4.2.3 Добавление и настройка загрузчика политики HTTP

Для добавления загрузчика политики HTTP требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем выбрать в отобразившемся контекстном меню команду «Добавить». Выбрать из дополнительного списка требуемый сервер. Окно добавления и настройки сервера загрузчика политики HTTP представлено на рисунке (см. Рисунок 77).

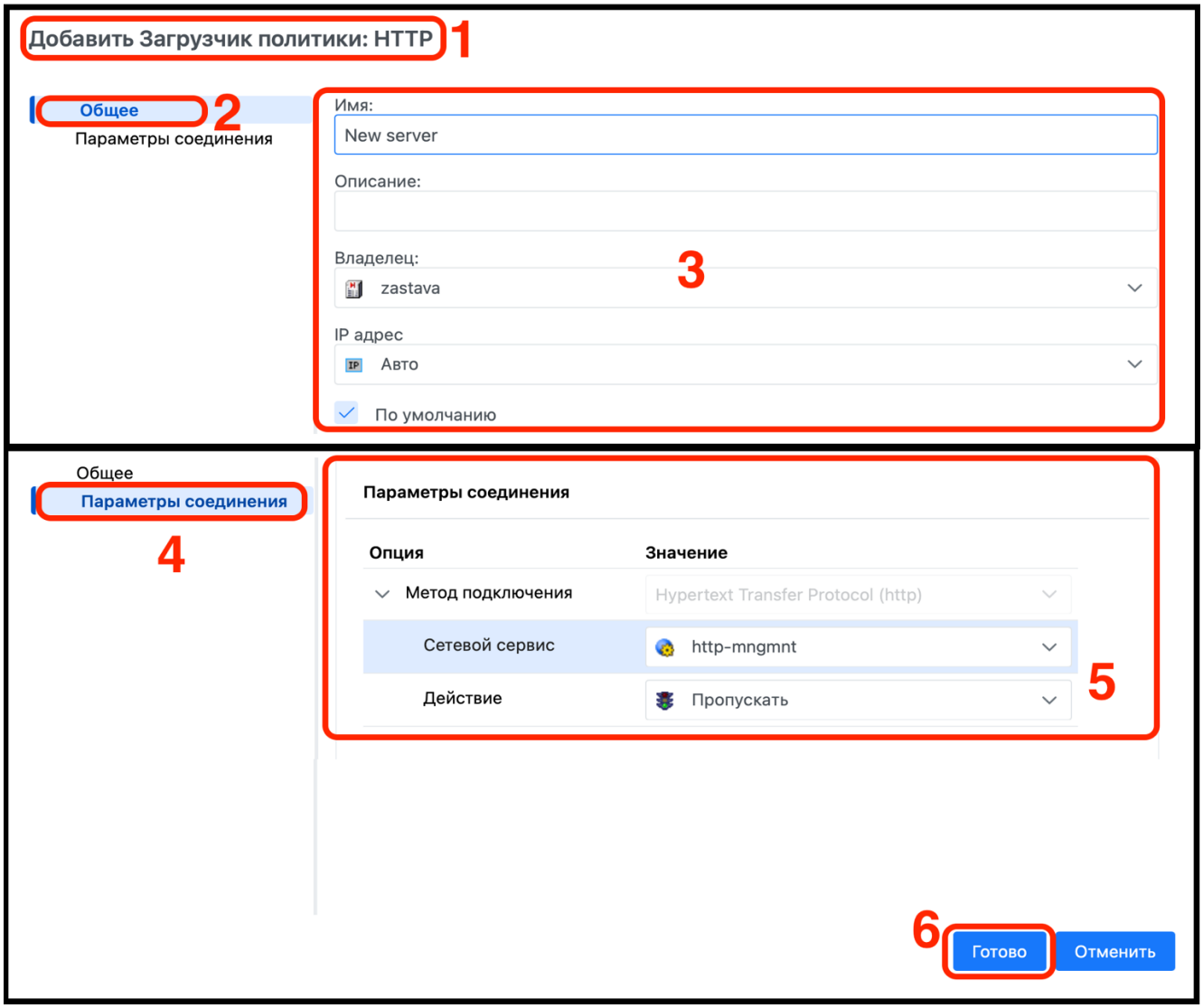


Рисунок 78 – Добавление и настройки загрузчика политики HTTP

1) Перейти в окно настроек «Добавить Загрузчик политики: HTTP» (цифра 1);
2) В элементе списка «Общее» (цифра 2) выполнить настройки блока (цифра 3). Подробное описание настроек представлено в таблице (см. Таблица 8);
3) В элементе списка «Параметры соединения» (цифра 4) заполнить требуемые параметры в блоке настроек (цифра 5):

— «Метод подключения»;
— «Сетевой сервис»;
— «Действие».

После выполненных настроек нажать кнопку «Готово» (цифра 6).

6.2.4.3 Прокси-серверы

Тип прокси-серверов содержит описания прокси-серверов для разных протоколов (HTTP, FTP и т.п.). Эти прокси-серверы входят в состав «VPN/FW «ЗАСТАВА-Офис», версия 8 и при необходимости, могут использоваться для дополнительной интеллектуальной обработки трафика. Конфигурирование прокси-серверов производится централизованно через ПО ЗУ.

Для конфигурирования определенного прокси-сервера необходимо создать соответствующее описание в нужной папке и указать:

— информацию для ПО ЗУ (объект политики, на котором установлен прокси-сервер, параметры служебного соединения между ПО ЗУ и прокси-сервером: протокол, имя и пароль);
— параметры для конфигурирования самого прокси-сервера (используемый порт, время жизни сессии, аутентификация и т.п.).

6.2.4.3.1 Настройки параметров соединений для прокси-серверов

Тип прокси содержит описания прокси-серверов для разных протоколов (HTTP, FTP и т.п.). Все протоколы имеют как общие параметры, так и дополнительные параметры.

В окне настройки серверов «Параметры соединения» перечислены все параметры настроек для всех типов прокси-серверов, изображенные на рисунке (см. Рисунок 79).

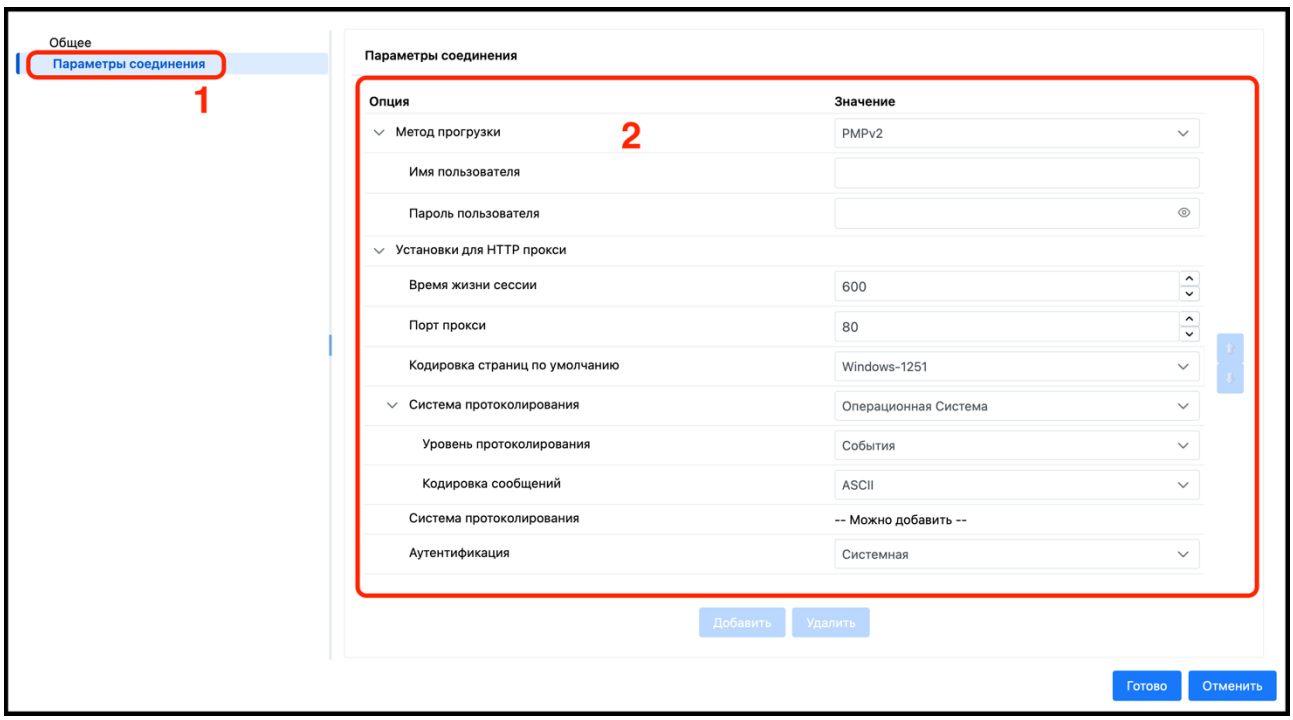


Рисунок 79 – Окно настроек «Параметры соединения»

Перейти в окно настроек «Параметры соединения» (цифра 1), заполнить форму настроек (цифра 2). Опции настроек для всех типов прокси-серверов представлены в таблице (см. Таблица 9).

Таблица 9 – Опции настроек «Параметры соединения» для прокси-серверов

Опция	Параметры	Значение
Метод прогрузки	В качестве методов прогрузки можно выбирать: PMPv2; SSH; Telnet. Настройка данных методов подключения со стороны прокси-сервера должна быть выполнена штатными средствами ОС	

Опция	Параметры	Значение
	Имя пользователя Пароль пользователя	Параметры для установления соединений между ПО ЗУ и данным прокси-сервером при активации ГПБ
Установки для прокси-сервера	Время жизни сессии	При отсутствии активности со стороны клиента (клиент-серверная архитектура) в течение данного времени текущая сессия с клиентом будет закрыта прокси-сервером (т.е. при повторном обращении клиенту придется проходить повторную аутентификацию). Время задается в секундах
	Порт прокси	TCP/UDP-порт, на котором прокси-сервер будет обслуживать поступающие запросы клиентов (клиент-серверная архитектура). Данный параметр будет также использоваться ПО ЗУ для создания необходимых технологических правил (подробнее см. п. 8.5.2)
	Кодировка страниц по умолчанию	Выбрать требуемое: Windows-1251; KOI8-R; UTF-8
Система протоколирования (их может быть несколько или не быть вообще)	Прокси-сервер позволяет регистрировать происходящие на нем события с использованием следующих методов: – Операционная система (ОС): сообщения записываются в стандартный журнал протокола ОС СВТ, на котором запущен прокси-сервер (в случае ОС Windows это будет Application Log); – SNMP: по каждому событию отсылается SNMP-трап на внешний SNMP-сервер; – программа эмулятора терминала: сообщения выводятся в окно консоли, из которой запущен данный прокси-сервер. Данный вариант возможен только при запуске прокси-сервера вручную в «консольном режиме» (с ключом –d). 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». 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); – Windows 1251;

Опция	Параметры	Значение
		– CP866 (рекомендуется при запуске прокси-сервера под ОС Windows в консольном режиме)
Система протоколирования	Вкладка в колонке «Значение» «--Можно добавить--»	
Пароль SNMP сервера (только для системы протоколирования SNMP)		Имя сообщества (Community name), которое будет указано в отсылаемых SNMP-трапах
Аутентификация		Метод аутентификации клиентов, который будет использоваться прокси-сервером. Возможные значения: – системная: средствами ОС СВТ, на котором запущен данный прокси-сервер. Т.е., при обращении клиента к прокси-серверу присланная информация (логин/пароль) будет отправлена на проверку ОС; – Radius: при обращении клиента к прокси-серверу присланная информация (логин/пароль) будет отправлена на проверку внешнему RADIUS-серверу; – локальная: при помощи текстового файла (на СВТ с запущенным прокси-сервером), содержащего пары вида «<логин>=<MD5-хеш пароля>»

6.2.4.3.2 Специфичные настройки авторизации для прокси-серверов

Авторизация содержит набор настроек правил для авторизации клиентов прокси-серверов. Переход к окну настроек правил для авторизации представлен на рисунке (см. Рисунок 80).

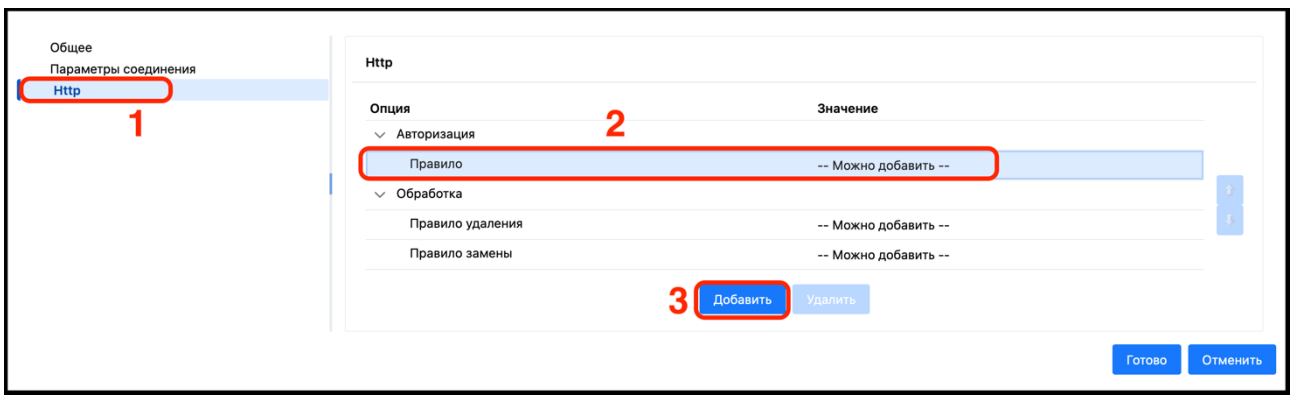


Рисунок 80 – Переход к окну настроек правил для авторизации

Открыть окно «Http» (цифра 1), в окне настроек «Http» выбрать строку «Правило» (цифра 2) и нажать кнопку «Добавить» (цифра 3).

Откроется окно настроек правил для авторизации клиентов прокси-серверов, представленное на рисунке (см. Рисунок 80).

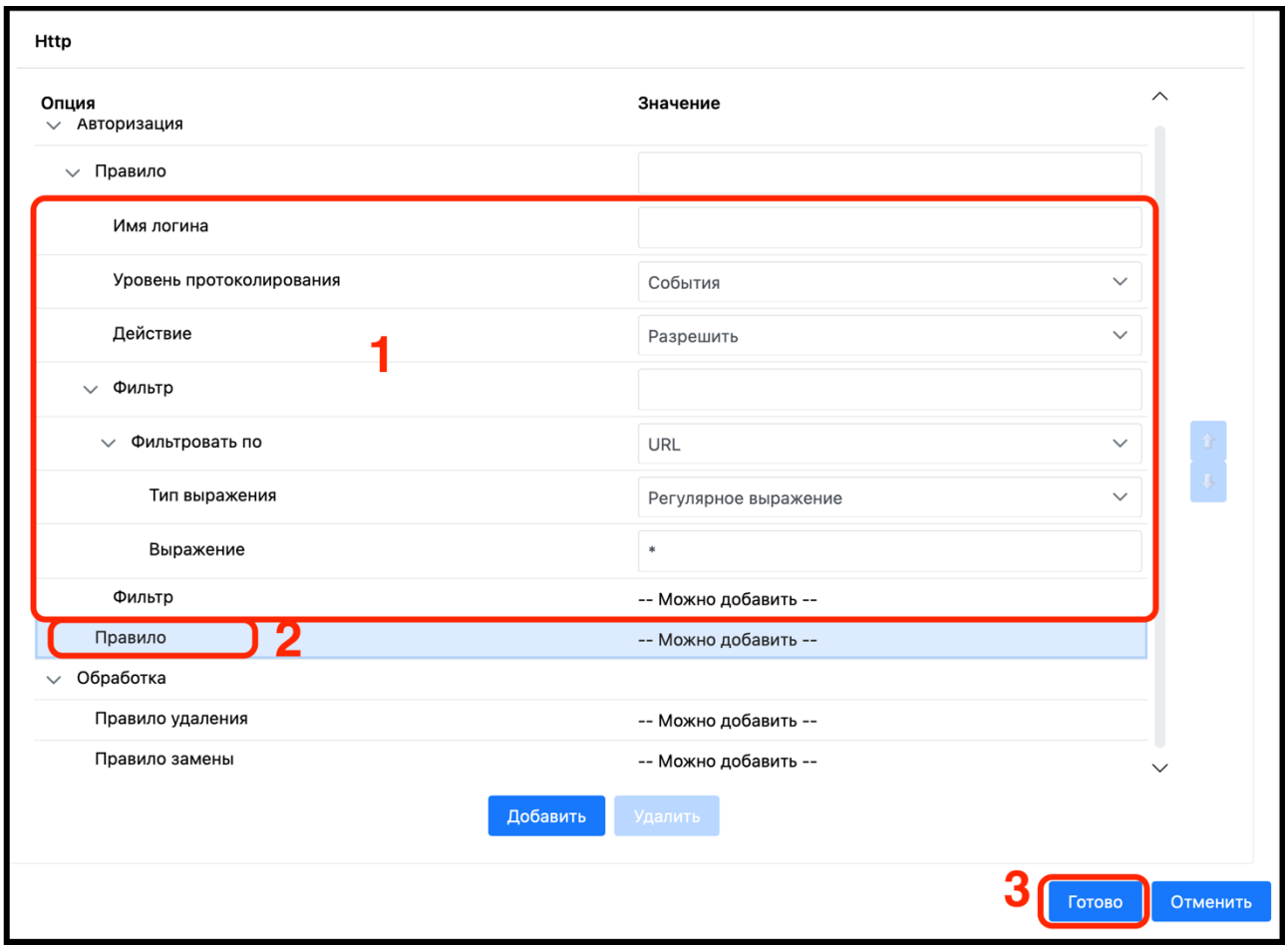


Рисунок 81 – Окно настроек правил для авторизации клиентов прокси-серверов

Заполнить форму открывшихся настроек (цифра 1). В случае необходимости можно добавить и аналогично предыдущему настроить следующее правило, нажав на «Правило» (цифра 2). После выполненных настроек нажать кнопку «Готово» (цифра 3). Опции, описания параметров и значений для настройки правил авторизации клиентов представлены в таблице (см. Таблица 10).

Таблица 10 – Описание параметров правил авторизации клиентских запросов

Опция	Параметр	Значение
Правило	Правило – это контейнер, содержащий фильтры, по которым проводится принятие решения об авторизации клиентов прокси-сервера	
	Имя логина	Логин, для которого будет срабатывать данное правило. Ввести при необходимости имя правила можно в колонке «Значение»
	Уровень протоколирования	Степень подробности сообщений, записываемых в лог прокси-сервера при срабатывании данного правила: – «Заблокирован»; – «События»; – «Детальный»; – «Отладочный»
	Действие	Возможные значения: – «Разрешить» – разрешить клиенту доступ к запрашиваемому ресурсу; – «Сбросить» – запретить клиенту доступ и сбросить текущее состояние авторизации для данного клиента;

Опция	Параметр	Значение
		– «Отказать» – запретить клиенту доступ к запрашиваемому ресурсу
Фильтр	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
	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

6.2.4.3.3 Специфичные настройки обработки для прокси-серверов

Настройка обработки подразумевает создание набора правил для обработки клиентских запросов, проходящих через прокси-сервер, прошедших этап авторизации. Под обработкой понимается удаление и/или замена определенных полей в запросе. Переход к настройкам обработки прокси-серверов представлен на рисунке (см. Рисунок 82).

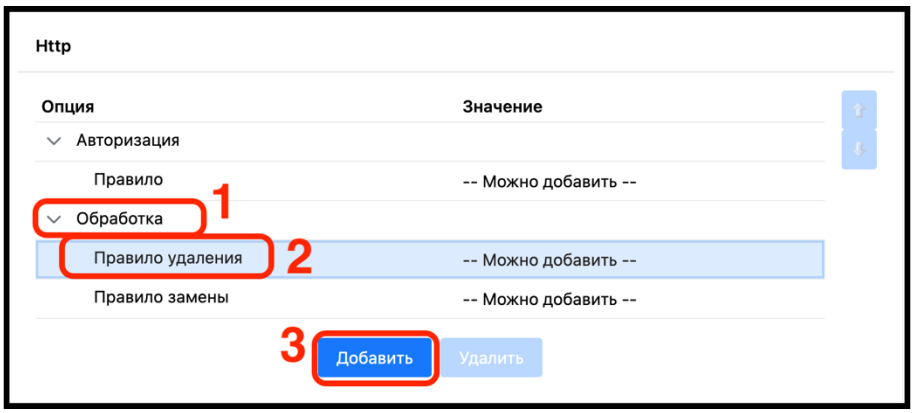


Рисунок 82 – Окно настроек обработки для прокси-серверов

В колонке «Опция» в списке настроек «Обработка» (цифра 1) выбрать настройку «Правила удаления» (цифра 2). Нажать кнопку «Добавить» (цифра 3). В открывшемся списке дополнительных настроек выполнить шаги, изображенные на рисунке (см. Рисунок 83).

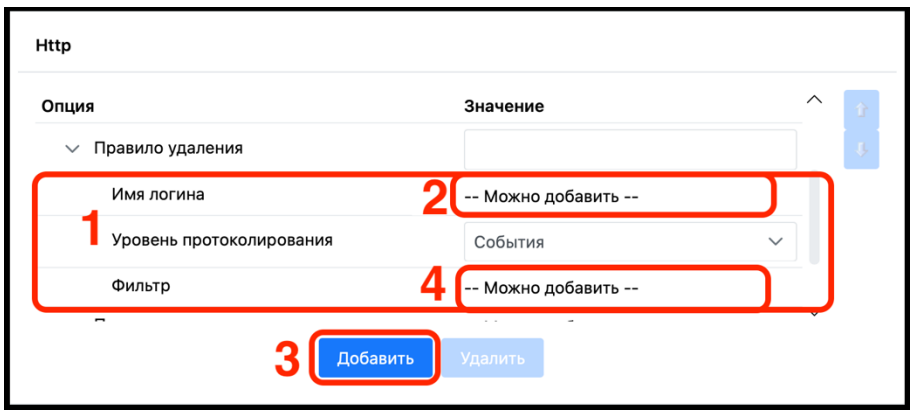


Рисунок 83 – Окно настроек «Правила удаления»

В блоке настроек (цифра 1) напротив строки «Имя логина» открыть дополнительные настройки, нажав вкладку в колонке «Значение» «--Можно добавить--» (цифра 2), затем нажать кнопку «Добавить» (цифра 3). Аналогично открыть дополнительные настройки напротив строки «Фильтр», нажав вкладку в колонке «Значение» «--Можно добавить--» (цифра 4), затем нажать кнопку «Добавить» (цифра 3). Заполнить параметры открывшихся настроек, представленных на рисунке (см. Рисунок 84).

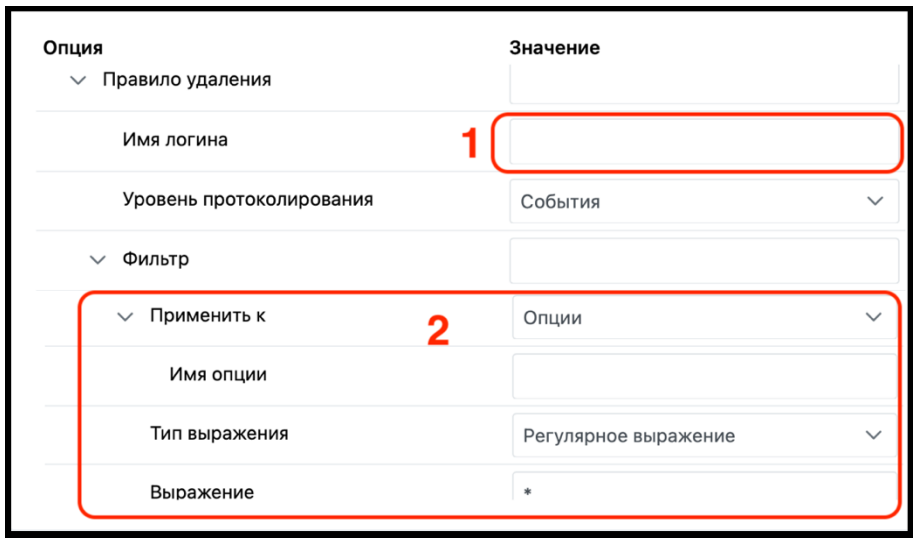


Рисунок 84 – Окно дополнительных настроек «Правила удаления»

Ввести имя логина (цифра 1), в блоке дополнительных настроек (цифра 2) заполнить параметры. Настройка опции «Правило замены» производится аналогично.

Специфичные настройки параметров обработки для прокси-серверов разнятся и представлены отдельно для каждого прокси сервера.

6.2.4.3.4 Объекты «Прокси FTP»

Тип объекта «Прокси FTP» содержит описания прокси-серверов для протокола FTP, который является стандартным протоколом передачи файлов в сети Интернет. Ниже перечислены некоторые задачи, которые может выполнять FTP прокси-сервер:

— дополнительная аутентификация пользователей на основании следующих механизмов аутентификации: RADIUS, системная (средствами ОС СВТ), 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.

Для добавления объекта «Прокси FTP» требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из дополнительного списка требуемый сервер. Окно добавления и настройки объекта «Прокси FTP» представлено на рисунке (см. Рисунок 85).

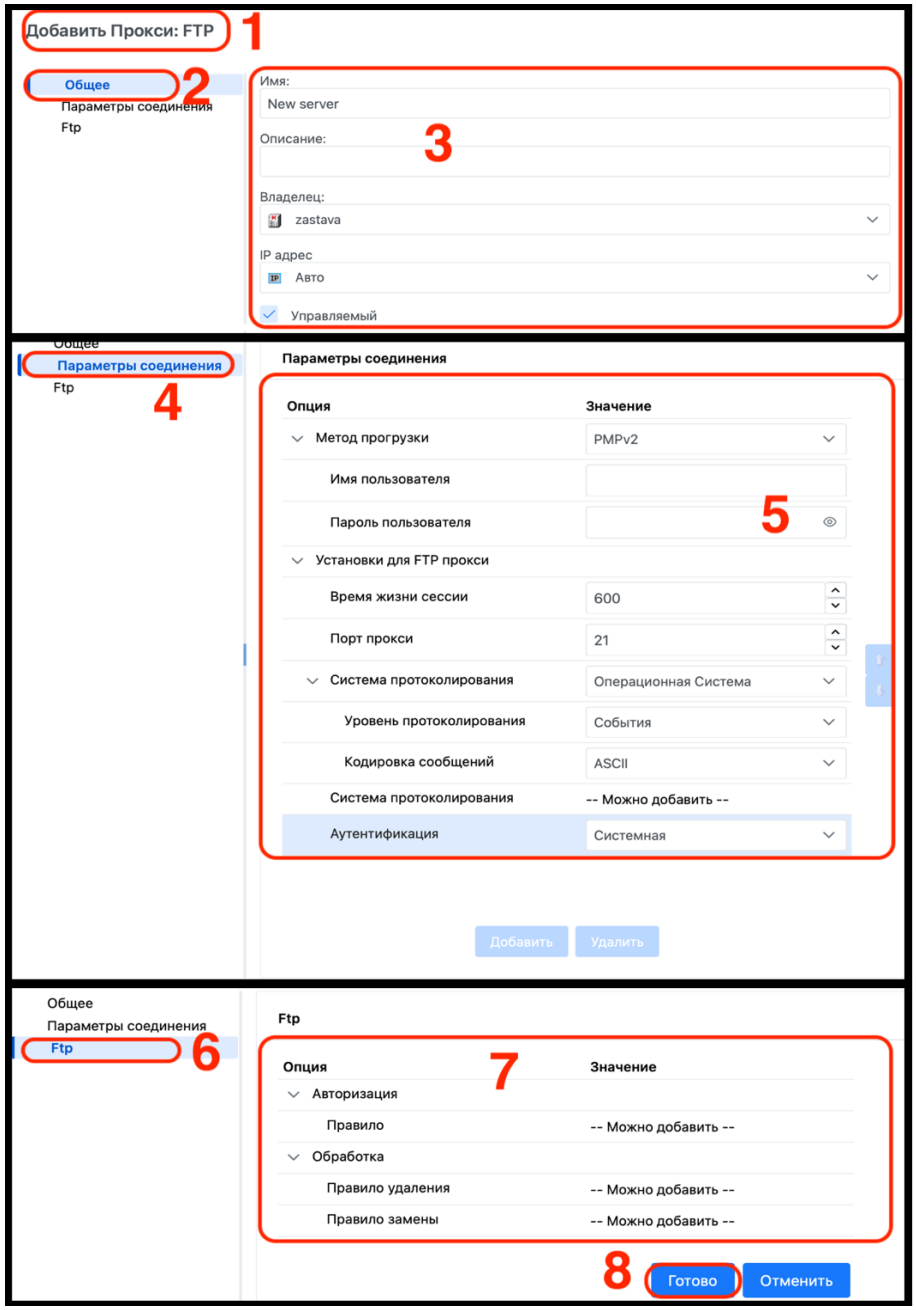


Рисунок 85 – Объекты «Прокси FTP»

Для добавления и настройки сервера прокси FTP необходимо перейти в его окно настроек (цифра 1) и заполнить:

1) в списке элементов «Общее» (цифра 2) заполнить требуемые параметры в блоке настроек (цифра 3). Описание общих параметров для прокси-серверов представлено в таблице (см. Таблица 8);

2) в списке элементов «Параметры соединения» (цифра 4) ввести требуемые параметры в блоке настроек (цифра 5). Описание параметров представлено в таблице (см. Таблица 9);
3) настроить специфичные параметры для FTP (цифра 6) в блоке настроек (цифра 7). В таблицах (см. Таблица 10 и Таблица 11) перечислены опции и описание дополнительных параметров обработки клиентских запросов прокси.

После выполненных настроек нажать кнопку «Готово» (цифра 8).

Таблица 11 – Описание дополнительных параметров обработки клиентских запросов прокси FTP

Опция	**Параметр**	**Значение**
Правило удаления	Контейнер, содержащий фильтры, по которым будет удаляться информация из запросов клиентов. 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 прокси-сервера при срабатывании данного правила: – «Заблокирован»; – «События»; – «Детальный»; – «Отладочный»
	Фильтр	Создает запросы, которые могут быть удалены: – «Применить к» – тип анализируемого элемента в значениях: «Опции» и «Тело»; – «Имя опции» – имя элемента, в котором может быть проведена замена; – «Тип выражения» – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны «Регулярное выражение» или, при необходимости, «Регулярное выражение чувствительное к регистру»; «Шаблон»; «Шаблон чувствительный к регистру»); – «Выражение» – значение строки поиска. Если указанное выражение найдено в указанной опции, то данная опция будет удалена
Правило замены	Контейнер, содержащий фильтры, по которым будет проводиться замена информации в запросах клиентов. 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 прокси-сервера при срабатывании данного правила: – «Заблокирован»; – «События»; – «Детальный»; – «Отладочный»
	Фильтр (для строки «Правила замены»)	Создает запросы, в которых может быть проведена замена в строке: – «Применить к» – тип анализируемого элемента в значениях: «Опции» и «Тело»; – «Имя опции» – имя элемента, в котором может быть проведена замена; – «Тип выражения» – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны «Регулярное выражение» или,

Опция	Параметр	Значение
		при необходимости, «Регулярное выражение чувствительное к регистру» «Шаблон»; «Шаблон чувствительный к регистру»); – «Из» – значение строки поиска; – «В» – значение, на которое будет заменен найденный блок текста

6.2.4.3.5 Объекты «Прокси HTTP»

Тип объекта «Прокси HTTP» содержит описания прокси-серверов для протокола HTTP, который является стандартным протоколом передачи файлов в сети Интернет. Ниже перечислены некоторые задачи, которые может выполнять HTTP прокси-сервер:

- дополнительная аутентификация пользователей на основании следующих механизмов аутентификации: RADIUS, системная (средствами ОС СВТ), локальная (при помощи файла с хешами паролей);
- фильтрация запросов пользователей на основании IP-адреса или имени HTTP - 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.

Для добавления объекта «Прокси HTTP» требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из дополнительного списка требуемый сервер. Окно добавления и настройки объекта «Прокси HTTP» представлено на рисунке (см. Рисунок 86).

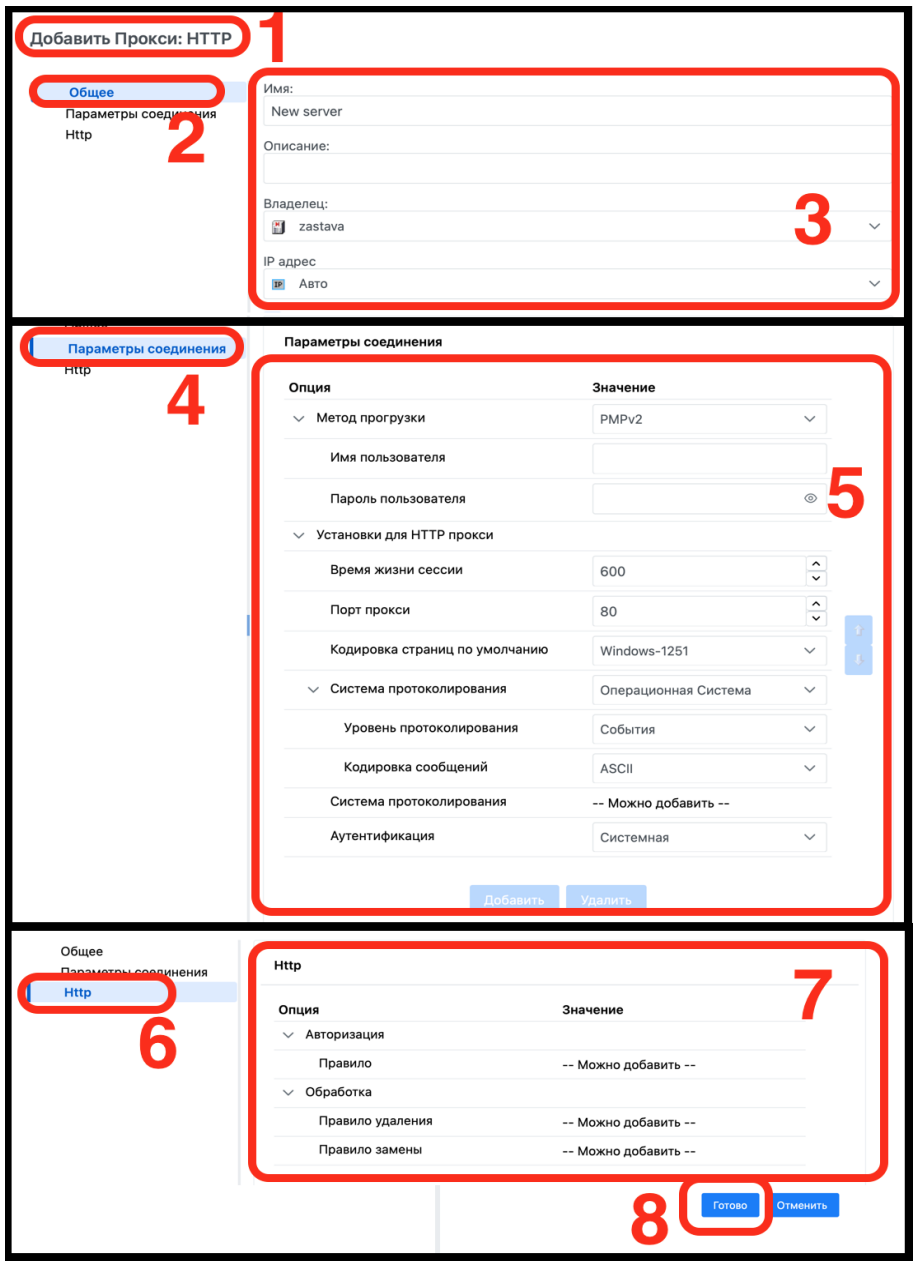


Рисунок 86 – Объекты «Прокси HTTP»

В окне настроек «Добавить Прокси: HTTP» (цифра 1) необходимо заполнить:

1) в элементе списка «Общее» (цифра 2) заполнить требуемые параметры в блоке настроек (цифра 3). Описание общих параметров для прокси-серверов представлено в таблице (см. Таблица 8);
2) в элементе списка «Параметры соединения» (цифра 4) ввести требуемые параметры в блоке настроек (цифра 5). Описание параметров представлено в таблице (см. Таблица 9);
3) настроить специфичные параметры для прокси-серверов (цифра 6) в блоке настроек (цифра 7). Описание параметров представлено в таблицах (см. Таблица 10 и Таблица 12).

После выполненных настроек нажать кнопку «Готово» (цифра 8).

Таблица 12 – Описание дополнительных параметров обработки клиентских запросов прокси HTTP

Опция	Параметр	Значение
Правило удаления	Контейнер, содержащий фильтры, по которым будет удаляться информация из запросов клиентов. 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 прокси-сервера при срабатывании данного правила: – «Заблокирован»; – «События»; – «Детальный»; – «Отладочный»
	Фильтр	Создает запросы, которые могут быть удалены: – «Применить к» – тип анализируемого элемента в значениях: «Опции» и «Тело»; – «Имя опции» – имя элемента, в котором может быть проведена замена; – «Тип выражения» – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны «Регулярное выражение» или, при необходимости, «Регулярное выражение чувствительное к регистру»); – «Выражение» – значение строки поиска. Если указанное выражение найдено в указанной опции, то данная опция будет удалена
Правило замены	Контейнер, содержащий фильтры, по которым будет проводиться замена информации в запросах клиентов. 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 прокси-сервера при срабатывании данного правила: – «Заблокирован»; – «События»; – «Детальный»; – «Отладочный»
	Фильтр	Создает запросы, в которых может быть проведена замена в строке: – «Применить к» – тип анализируемого элемента в значениях: «Опции» и «Тело»; – «Имя опции» – имя элемента, в котором может быть проведена замена; – «Тип выражения» – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны «Регулярное выражение» или, при необходимости, «Регулярное выражение чувствительное к регистру»); – «Из» – значение строки поиска; – «В» – значение, на которое будет заменен найденный блок текста

6.2.4.3.6 Объекты «Прокси SMTP»

Тип «Прокси SMTP» содержит описания прокси-серверов для протокола SMTP, который является стандартным протоколом передачи электронной почты в сети Интернет. Ниже перечислены некоторые задачи, которые может выполнять SMTP прокси-сервер:

- дополнительная аутентификация пользователей на основании следующих механизмов аутентификации: RADIUS, системная (средствами ОС СВТ), локальная (при помощи файла с хешами паролей);
- удаление или замена произвольных полей в заголовках писем;
- удаление или замена произвольных блоков текста в телах писем.

Для добавления объекта «Прокси SMTP» требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из дополнительного списка требуемый сервер. Окно добавления и настройки объекта прокси SMTP представлено на рисунке (см. Рисунок 87).

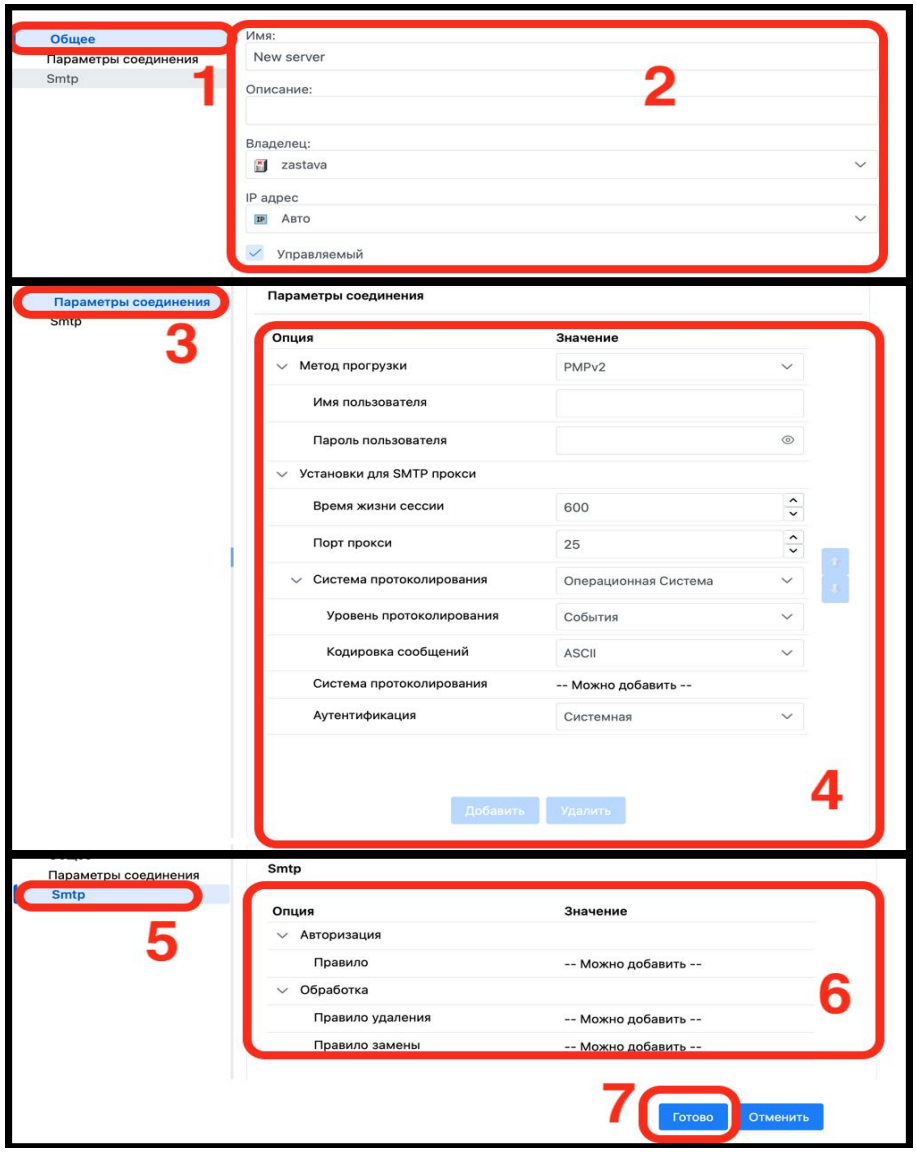


Рисунок 87 – Объекты «Прокси SMTP»

В окне настроек прокси SMTP необходимо заполнить:

1) в элементе списка «Общее» (цифра 1) заполнить требуемые параметры в блоке настроек (цифра 2). Описание общих параметров для прокси-серверов представлено в таблице (см. Таблица 8);
2) в элементе списка «Параметры соединения» (цифра 3) ввести требуемые параметры в блоке настроек (цифра 4). Описание параметров представлено в таблице (см. Таблица 9);
3) настроить специфичные параметры для прокси-серверов (цифра 5) в блоке настроек (цифра 6). Описание параметров представлено в таблицы (см. Таблица 10 и Таблица 13).

После выполненных настроек нажать кнопку «Готово» (цифра 7).

Таблица 13 – Описание дополнительных параметров обработки клиентских запросов прокси SMTP

Опция	Параметр	Значение
Правило удаления	Контейнер, содержащий фильтры, по которым будет удаляться информация из запросов клиентов. 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 прокси-сервера при срабатывании данного правила: – «Заблокирован»; – «События»; – «Детальный»; – «Отладочный»
	Фильтр	Создает запросы, которые могут быть удалены: – «Применить к» – тип анализируемого элемента в значениях: «Опции» и «Тело»; – «Имя опции» – имя элемента, в котором может быть проведена замена; – «Тип выражения» – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны «Регулярное выражение» или, при необходимости, «Регулярное выражение чувствительное к регистру»; «Шаблон»; «Шаблон чувствительный к регистру»); – «Выражение» – значение строки поиска. Если указанное выражение найдено в указанной опции, то данная опция будет удалена
Правило замены	Контейнер, содержащий фильтры, по которым будет проводиться замена информации в запросах клиентов. 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 прокси-сервера при срабатывании данного правила: – «Заблокирован»; – «События»; – «Детальный»; – «Отладочный»
	Фильтр	Создает запросы, в которых может быть проведена замена в строке: – «Применить к» – тип анализируемого элемента– в значениях: «Опции» и «Тело»; – «Имя опции» – имя элемента, в котором может быть проведена замена; – «Тип выражения» – формат, в котором будет вводиться строка поиска (можно использовать простые шаблоны «Регулярное выражение» или, при необходимости – «Регулярное выражение чувствительное к регистру»; «Шаблон»; «Шаблон чувствительный к регистру»); – «Из» – значение строки поиска; – «В» – значение, на которое будет заменен найденный блок текста

6.2.4.3.7 Объекты «Прокси SOCKS»

Тип «Прокси SOCKS» содержит описания прокси-серверов на основе протокола SOCKS. Ниже перечислены некоторые задачи, которые может выполнять SOCKS прокси-сервер:

- дополнительная аутентификация пользователей на основании следующих механизмов аутентификации: RADIUS, системная (средствами ОС СВТ), 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.

Для добавления объекта «Прокси SOCKS» требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из дополнительного списка требуемый сервер. Окно добавления и настройки объекта «Прокси SOCKS» представлено на рисунке (см. Рисунок 88).

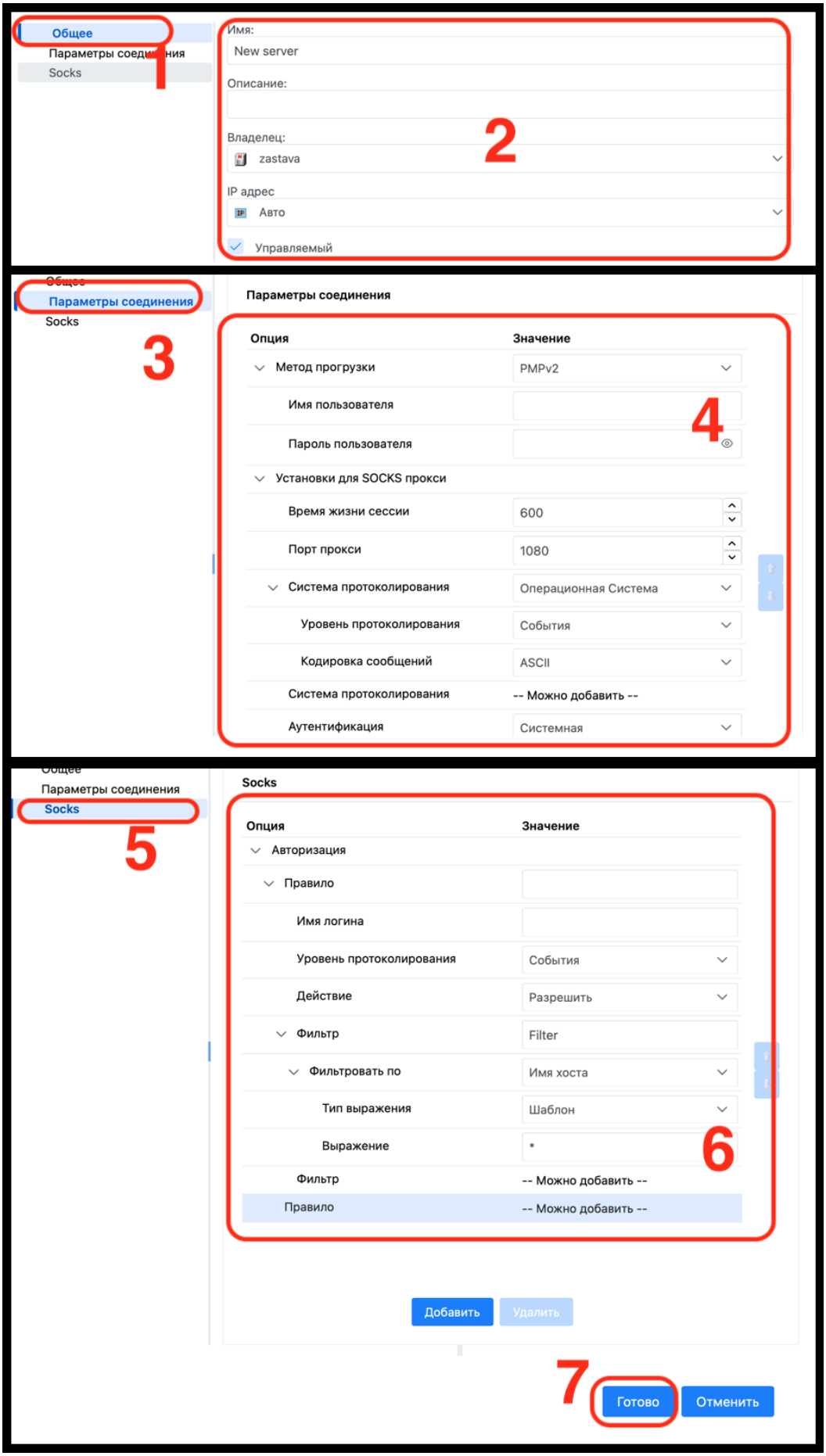


Рисунок 88 – Объекты «Прокси SOCKS»

В окне настроек «Прокси SOCKS» необходимо заполнить:

1) в окне «Общее» (цифра 1) заполнить требуемые параметры в блоке настроек (цифра 2). Описание общих параметров для прокси-серверов представлено в таблице (см. Таблица 8);
2) в окне «Параметры соединения» (цифра 3) ввести требуемые параметры в блоке настроек (цифра 4). Описание параметров представлено в таблице (см. Таблица 9);
3) настроить специфичные параметры для прокси-серверов (цифра 5) в блоке настроек (цифра 6). Описание параметров представлено в таблице (см. Таблица 10).

После выполненных настроек нажать кнопку «Готово» (цифра 7).

6.2.4.4 Прочие серверы

6.2.4.4.1 Объекты LDAP

Тип объекта LDAP содержит описания LDAP-серверов, присутствующих в сети и содержащих каталоги с сертификатами и COC. При создании объекта политики, представляющего управляемый агент, в его свойствах, в окне «Сертификаты» можно указать объект «LDAP-сервер» как удаленный каталог, куда может обратиться агент для получения сертификата партнера или актуального COC. Флажок «LDAP autopass» (обработка COC) всегда в состоянии «Disabled», поскольку данная функция поддерживается через привязку LDAP-сервера в окне «Пропуск пакетов».

Для добавления объекта LDAP требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню команду «Добавить». Выбрать из дополнительного списка требуемый сервер. Окно добавления и настройки объекта LDAP представлено на рисунке (см. Рисунок 89).

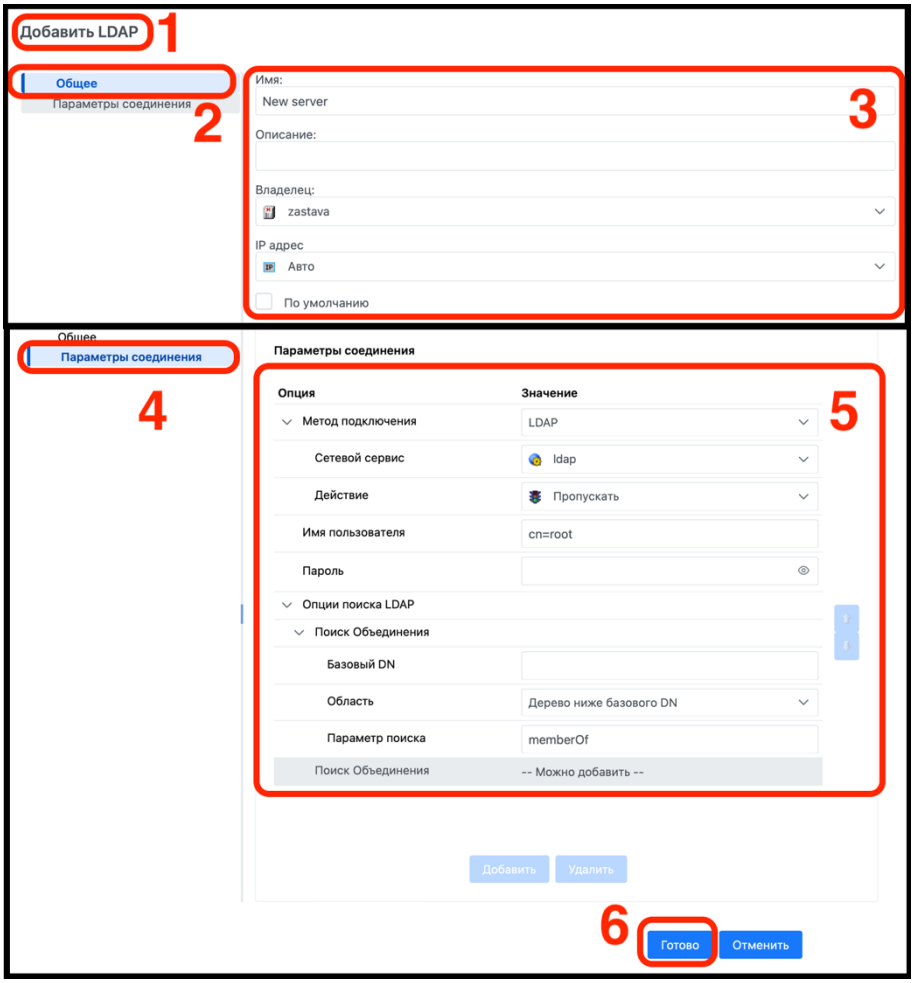


Рисунок 89 – Объекты LDAP

В окне настроек «Добавить LDAP» (цифра 1) необходимо заполнить:

1) в элементе списка «Общее» (цифра 2) заполнить требуемые параметры в блоке настроек (цифра 3). Описание общих параметров представлено в таблице (см. Таблица 8);
2) в элементе списка «Параметры соединения» (цифра 4) ввести требуемые параметры в блоке настроек (цифра 5). Описание параметров представлено в таблице (см. Таблица 9).

После выполненных настроек нажать кнопку «Готово» (цифра 6).

6.2.4.4.2 Объекты SNMP

Тип объекта SNMP содержит описания присутствующих в сети SNMP-серверов, которые могут отправлять SNMP-запросы к объектам политики, а также принимать от этих объектов политики сообщения о происходящих на объекте событиях (SNMP-трапы).

К каждому объекту политики можно привязать один или несколько подобных SNMP-серверов.

В состав ПО ЗУ входит собственный SNMP-сервер (представленный сервером TPNSnmpServer), описывающий его объект создается автоматически.

Для добавления объекта SNMP требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из дополнительного списка требуемый сервер. Окно добавления и настройки объекта SNMP представлено на рисунке (см. Рисунок 90).

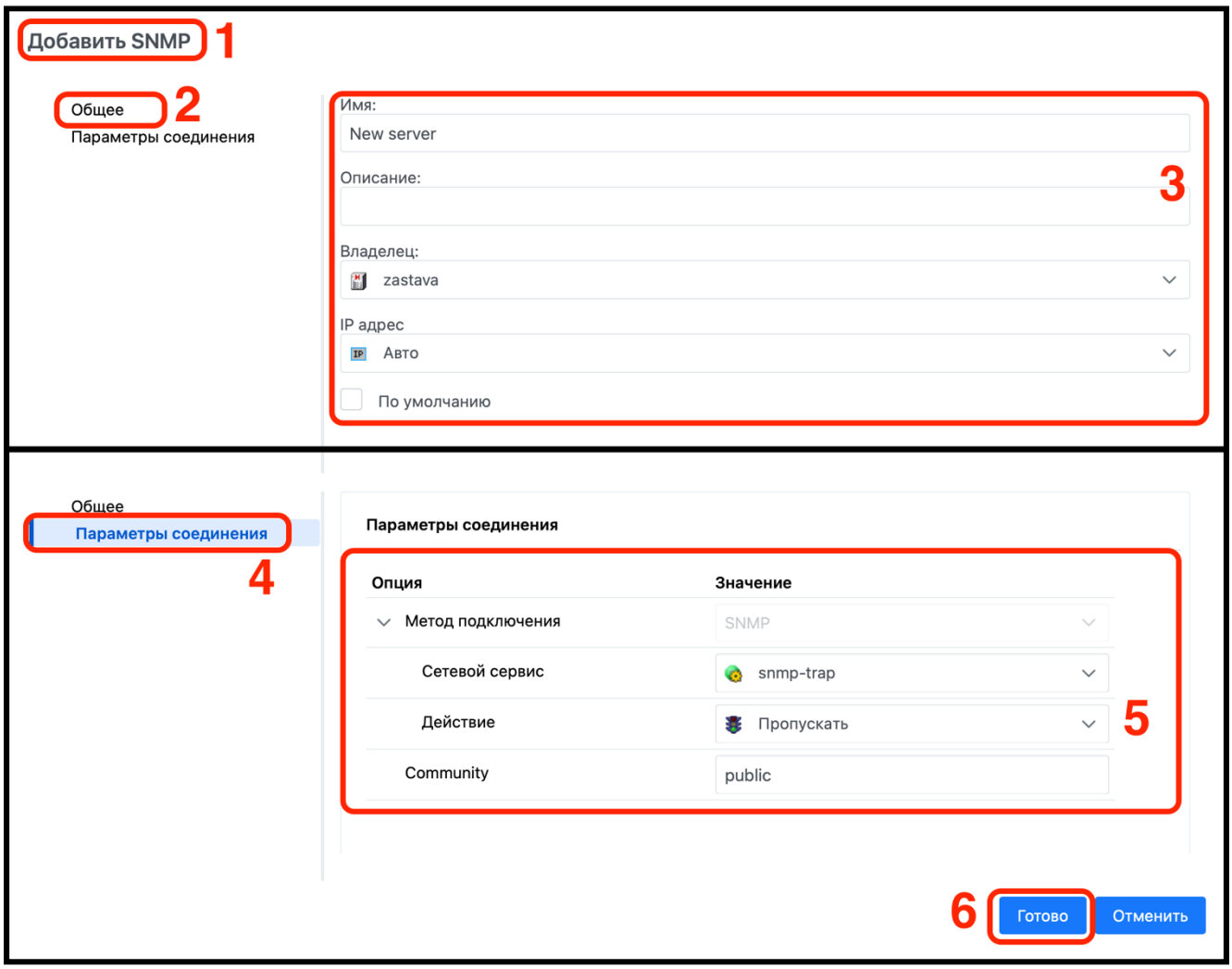


Рисунок 90 – Объект SNMP

В окне добавления и настройки объекта SNMP необходимо заполнить:

1) в элементе списка «Общее» (цифра 2) заполнить требуемые параметры в блоке настроек (цифра 3). Описание общих параметров представлено в таблице (см. Таблица 8);
2) в элементе списка «Параметры соединения» (цифра 4) ввести требуемые параметры в блоке настроек (цифра 5). Описание параметров представлено в таблице (см. Таблица 9).

После выполненных настроек нажать кнопку «Готово» (цифра 6).

6.2.4.4.3Объекты Syslog

Тип объекта Syslog содержит описания присутствующих в сети Syslog-серверов, которые могут использоваться для сбора информации от управляемых агентов по протоколу Syslog. К каждому объекту политики, который поддерживает этот протокол, можно привязать один или несколько подобных Syslog-серверов.

В состав ПО ЗУ входит собственный Syslog-сервер (представленный сервером TPNSyslog) описывающий его объект, он создается автоматически и дополнительного конфигурирования в большинстве случаев не требуется.

Для добавления объекта Syslog требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из дополнительного списка требуемый сервер. Окно добавления и настройки объекта SNMP представлено на рисунке (см. Рисунок 91).

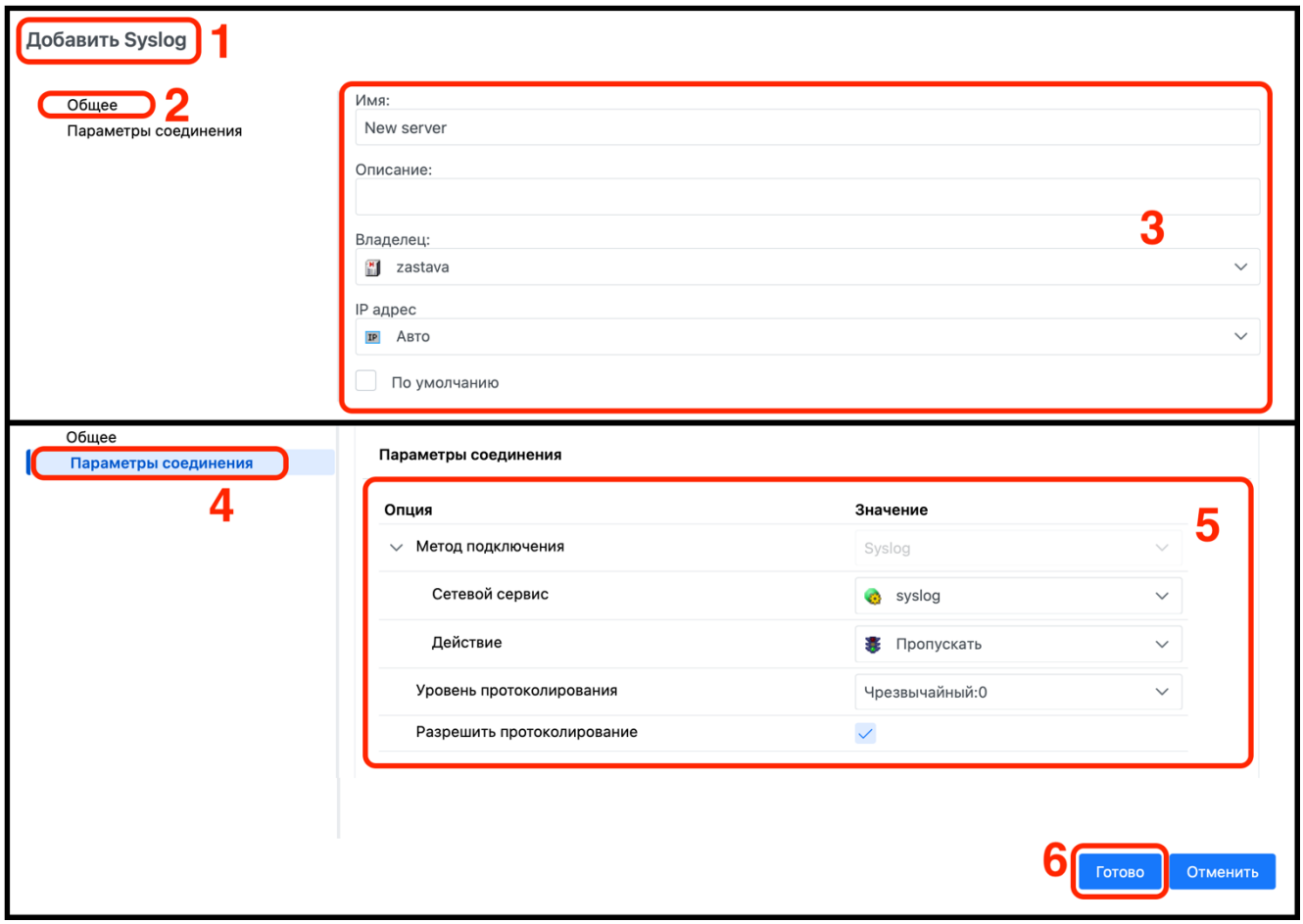


Рисунок 91 – Объекты Syslog

В окне добавления и настройки объекта Syslog необходимо заполнить:

1) в элементе списка «Общее» (цифра 2) заполнить требуемые параметры в блоке настроек (цифра 3). Описание общих параметров представлено в таблице (см. Таблица 8);
2) в элементе списка «Параметры соединения» (цифра 4) ввести требуемые параметры в блоке настроек (цифра 5). Описание специфичных параметров представлено в таблице (см. Таблица 9).

После выполненных настроек нажать кнопку «Готово» (цифра 6).

6.2.4.4.4 Объект «Сервер обновления»

Тип объекта «Сервер обновления» содержит описания серверов обновления, присутствующих в сети (или в сети Интернет) и содержащих обновления, которые позволяют скачивать и устанавливать актуальные версии ПО ЗУ.

Если на сервере обновления выложена актуальная версия ПО ЗУ, то будет запущен процесс обновления, включающий скачивание файла обновления, деинсталляцию текущей версии ПО ЗУ и инсталляцию новой с сохранением всей информации о настройках, сертификатах и т.п.

Обращение к серверу обновлений производится по открытому протоколу HTTP. В данной версии ПО ЗУ есть опции «не обновлять», «обновлять по командам с сервера управлений» и проверять обновление при подключении.

Для добавления объекта «Сервер обновления» требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из дополнительного списка требуемый сервер. Окно добавления и настройки объекта «Сервер обновления» представлено на рисунке (см. Рисунок 92).

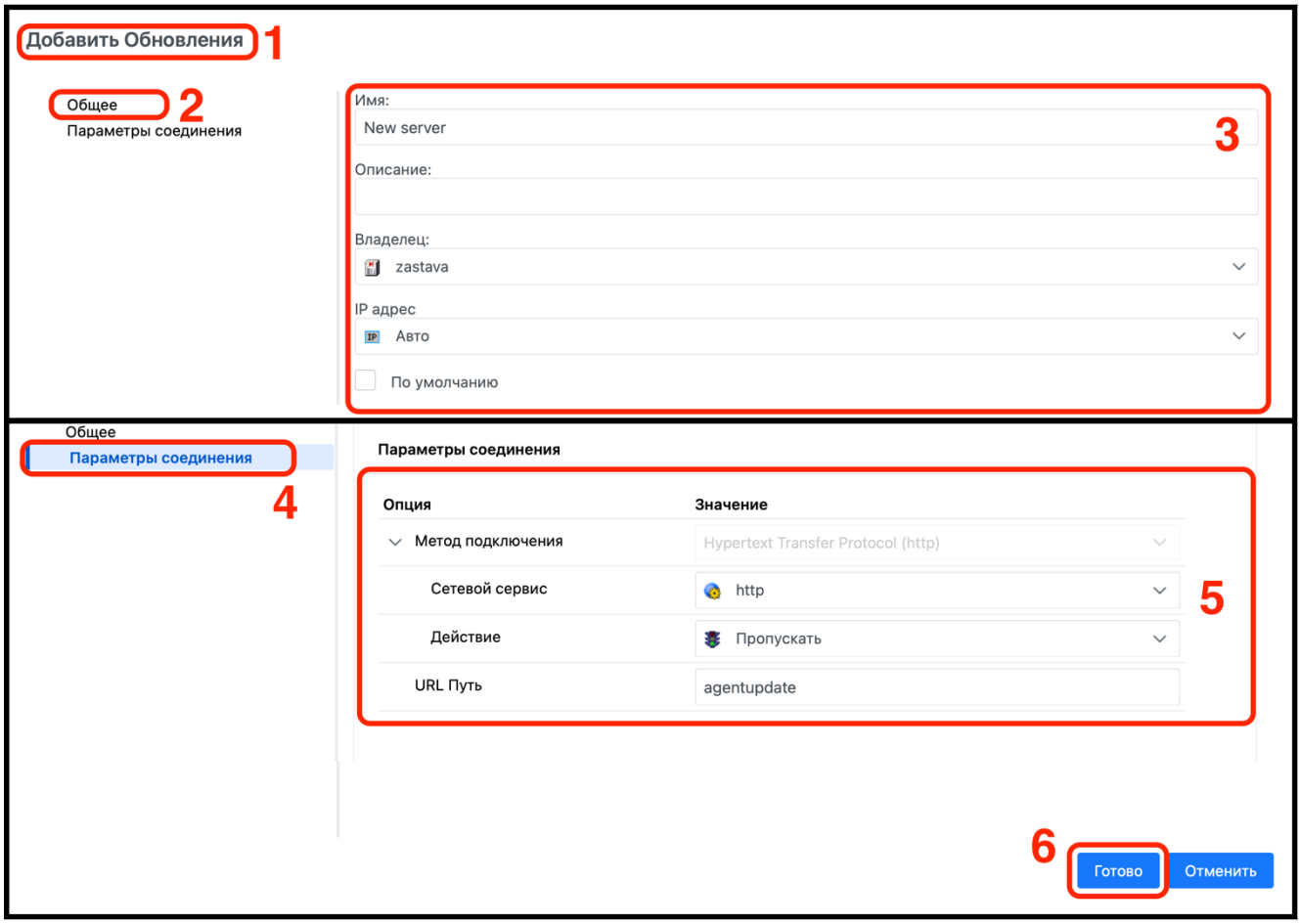


Рисунок 92 – Окно настроек «Добавить Обновления»

В окне «Добавить Обновления» необходимо заполнить:

1) в элементе списка «Общее» (цифра 2) заполнить требуемые параметры в блоке настроек (цифра 3). Описание общих параметров представлено в таблице (см. Таблица 8);
2) в элементе списка «Параметры соединения» (цифра 4) ввести требуемые параметры в блоке настроек (цифра 5). URL путь – веб-адрес сервера обновления, содержащего обновления, с которым будет периодически связываться агент при проверке обновлений. Описание параметров представлено в таблице (см. Таблица 10).

После выполненных настроек нажать кнопку «Готово» (цифра 6).

6.2.4.4.5 Объекты NetFlow

Для добавления объекта NetFlow требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из дополнительного списка требуемый сервер. Окно добавления и настройки объекта NetFlow представлено на рисунке (см. Рисунок 93).

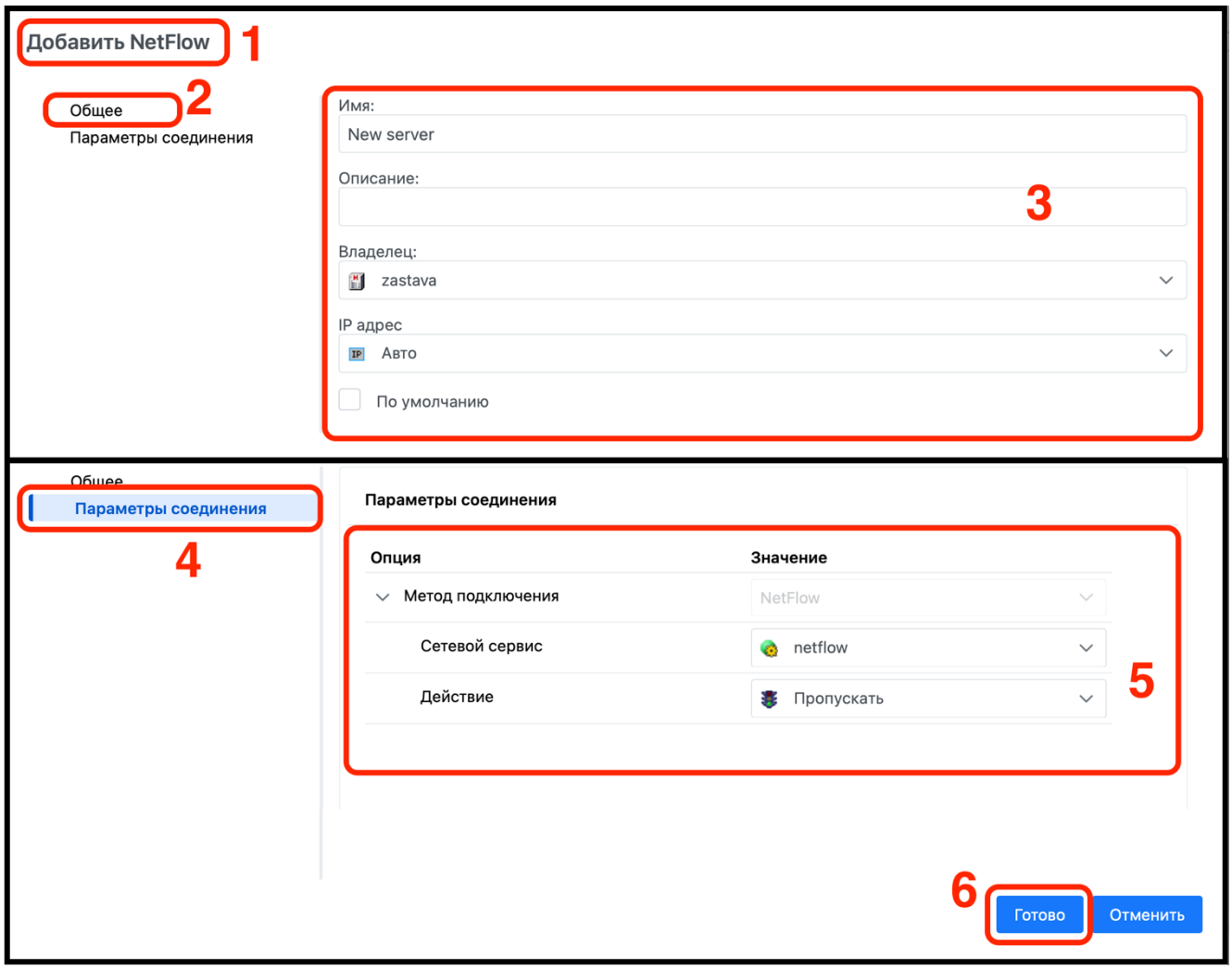


Рисунок 93 – Объекты NetFlow

В окне «Добавить NetFlow» (цифра 1) необходимо заполнить:

1) в элементе списка «Общее» (цифра 2) заполнить требуемые параметры в блоке настроек (цифра 3). Описание общих параметров представлено в таблице (см. Таблица 8);
2) в элементе списка «Параметры соединения» (цифра 4) ввести требуемые параметры в блоке настроек (цифра 5). Описание параметров представлено в таблице (см. Таблица 9).

После выполненных настроек нажать кнопку «Готово» (цифра 6).

6.2.4.5 Серверы аутентификации

Серверы аутентификации позволяет создавать и редактировать вспомогательные объекты (серверы аутентификации), которые не являются объектами политики безопасности, тем не менее выполняют разнообразные важные функции, необходимые для работы защищенной сети.

Серверы аутентификации - виртуальные сущности (объекты Certification Authority (CA), выполняющие функции сертификатов УЦ), которые напрямую не связаны с хостами в сети.

Многие серверы аутентификации создаются автоматически. Обычно это приложения (системные сервисы), которые входят в состав ПО ЗУ и взаимодействуют с внешними хостами.

6.2.4.5.1 Аутентификация «Локальный»

Для добавления аутентификации «Локальный» требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из дополнительного списка требуемый сервер. Окно добавления и настройки сервера аутоинтефикации «Локальный» представлено на рисунке (см. Рисунок 94).

Рисунок 94 – Добавление аутентификации «Локальный»

В окне настроек «Добавить Аутентификация: Локальный» (цифра 1) заполнить в элементе списка «Общее» (цифра 2) требуемые параметры в блоке настроек (цифра 3). Описание общих параметров представлено в таблице (см. Таблица 8). После выполненных настроек нажать кнопку «Готово» (цифра 4).

6.2.4.5.2 Аутентификация RADIUS

Тип объекта «Сервер аутентификации RADIUS» 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.

В состав ПО ЗУ входит собственный RADIUS-сервер (представленный сервером FreeRadius Server). Описывающий его объект создается автоматически.

Для добавления сервера аутентификации «RADIUS» требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из

дополнительного списка требуемый сервер. Окно добавления и настройки сервера аутентификации RADIUS представлено на рисунке (см. Рисунок 95).

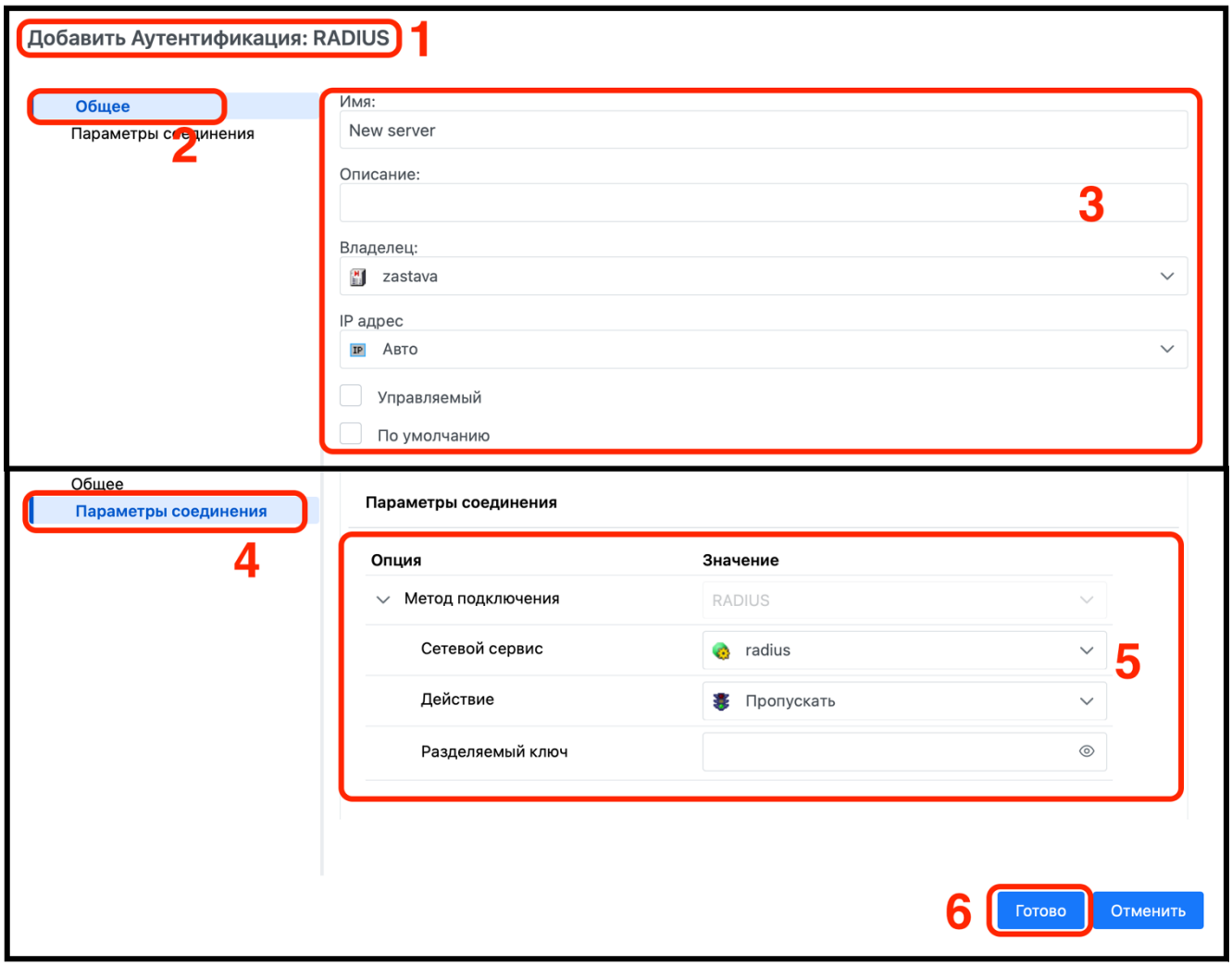


Рисунок 95 – Объекты RADIUS

В окне добавления и настройки объекта аутентификации RADIUS (цифра 1) необходимо заполнить:

1) в элементе списка «Общее» (цифра 2) заполнить требуемые параметры в блоке настроек (цифра 3). Описание общих параметров представлено в таблице (см. Таблица 8);
2) в элементе списка «Параметры соединения» (цифра 4) ввести требуемые параметры в блоке настроек (цифра 5). Описание параметров представлено в таблице (см. Таблица 9).

После выполненных настроек нажать кнопку «Готово» (цифра 6).

6.2.4.6 Добавление сервера интеграции

Для добавления объекта сервера интеграции требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из

дополнительного списка требуемый сервер. Окно добавления сервера интеграции представлено на рисунке (см. Рисунок 96).

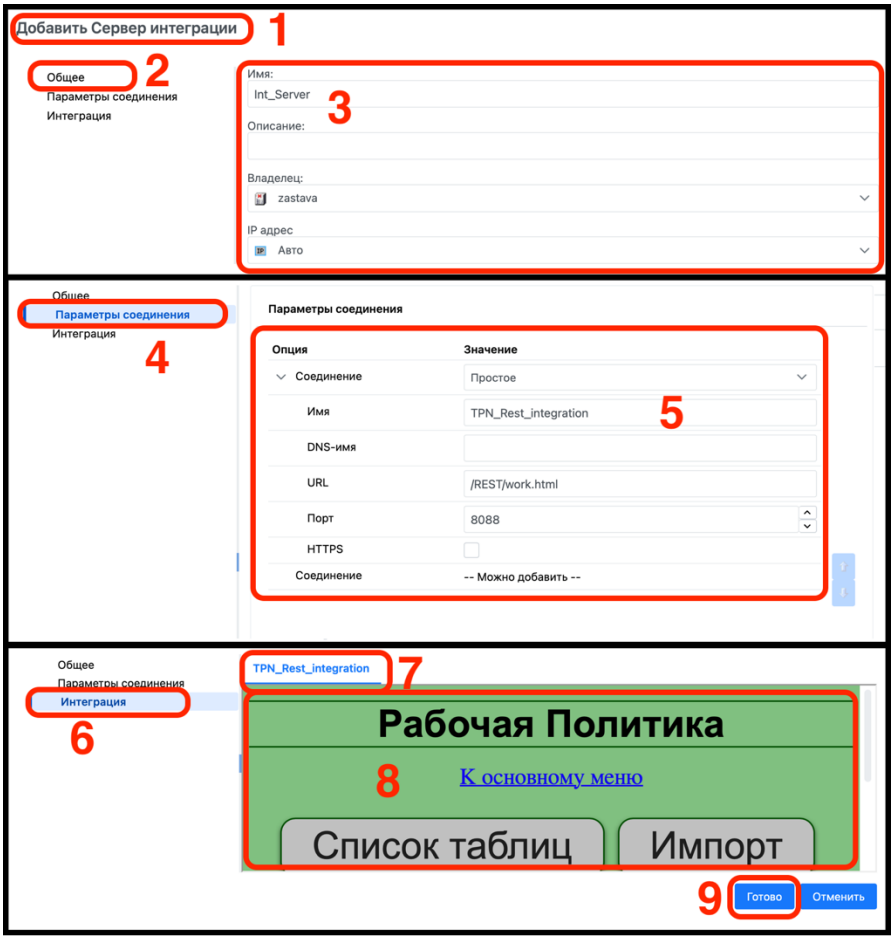


Рисунок 96 – Добавление сервера интеграции

В окне «Добавить Сервер интеграции» (цифра 1) необходимо заполнить:

1) в окне «Общее» (цифра 2) заполнить требуемые параметры в блоке настроек (цифра 3). Описание общих параметров представлено в таблице (см. Таблица 8);
2) в окне «Параметры соединения» (цифра 4) ввести требуемые параметры соединения в блоке настроек (цифра 5);
3) в окне «Интеграция» (цифра 6) во вкладке «TPN_Rest_integration» (цифра 7) (это имя задано вручную на этапе настроек параметров соединения) отобразится вид окна интерфейса интеграции (цифра 8). После выполненных настроек нажать кнопку «Готово» (цифра 9).

В результате выполненных действий в боковой панели вкладок появится вкладка «Интеграции». Вид интерфейса ПО ЗУ с добавленной интеграцией представлен на рисунке (см. Рисунок 97).

Рисунок 97 – Вид интерфейса ПО ЗУ с добавленной интеграцией

В боковой панели вкладок «Интеграции» (цифра 1) в списке ее элементов будут отображаться все настроенные интеграции (цифра 2), в рабочей области отобразится вид интегрируемого объекта (цифра 3).

В случае удаления интеграции, вкладка «Интеграция» пропадет с боковой панели.

6.2.4.7 Добавление объекта «Монитор»

Для добавления объекта «Монитор» требуется вызвать контекстное меню, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем в отобразившемся контекстном меню выбрать команду «Добавить». Выбрать из дополнительного списка команду «Монитор». Окно добавления «Добавить Монитор» представлено на рисунке (см. Рисунок 98).

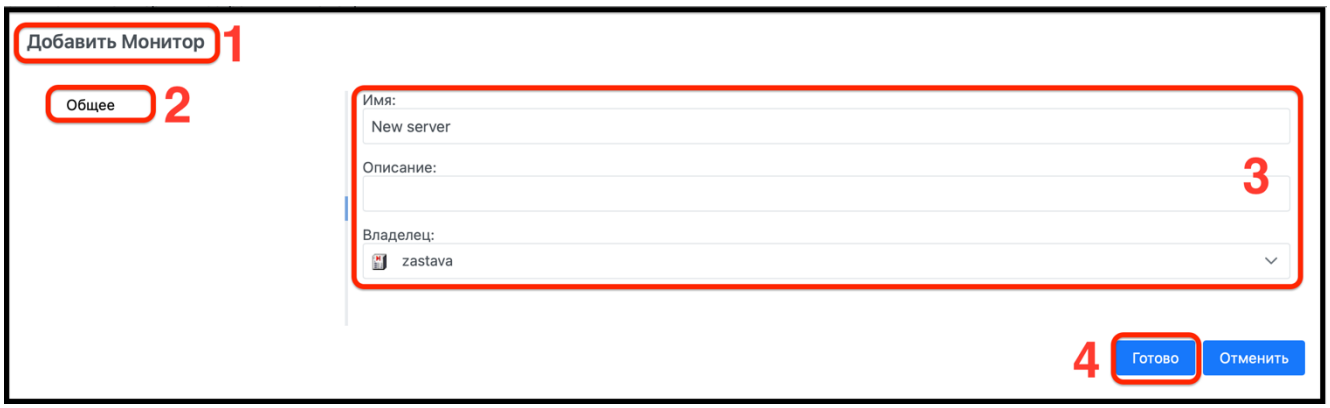


Рисунок 98 – Добавление объекта «Монитор»

В окне «Добавить Монитор» (цифра 1) в блоке «Общее» (цифра 2) заполнить требуемые параметры настроек (цифра 3). Описание общих параметров представлено в таблице (см. Таблица 8).

6.2.5 Объединения

В элементе списка «Объединения» отображаются объекты типа «Объединение». Вид окна элемента списка «Объединения» изображен на рисунке (см. Рисунок 99).

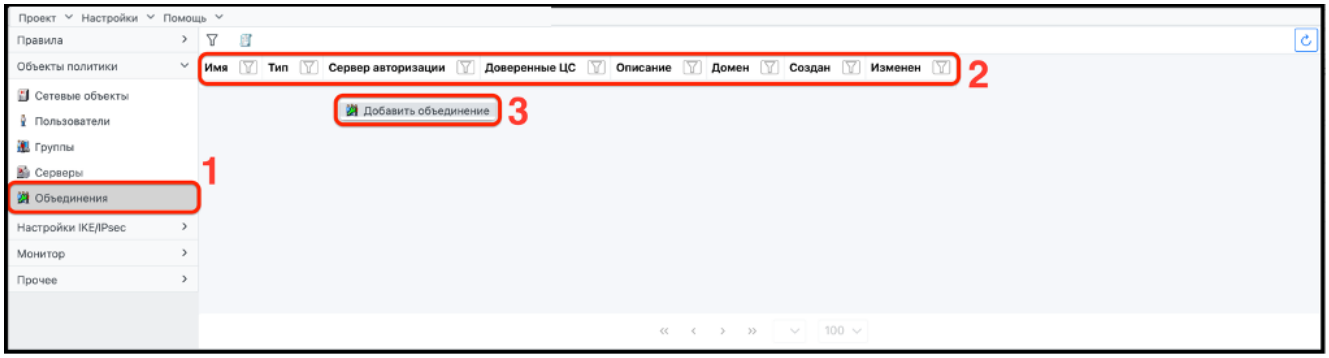


Рисунок 99 – Элемент списка «Объединения»

Окно элемента списка «Объединения» (цифра 1) отображает таблицу параметров объектов типа «Объединение» (цифра 2):

— «Имя»;
— «Тип»;
— «Сервер авторизации»;
— «Доверенные ЦС» (цент сертификации);
— «Описание»;
— «Домен»;
— «Создан»;
— «Изменен».

По каждому из параметров доступна фильтрация.

Для добавления и настройки объединения необходимо нажать правой клавишей мыши в рабочую область таблицы, выбрать команду «Добавить объединение» (цифра 3). В открывшемся окне «Добавить Объединения» выполнить шаги, изображенные на рисунке (см. Рисунок 100).

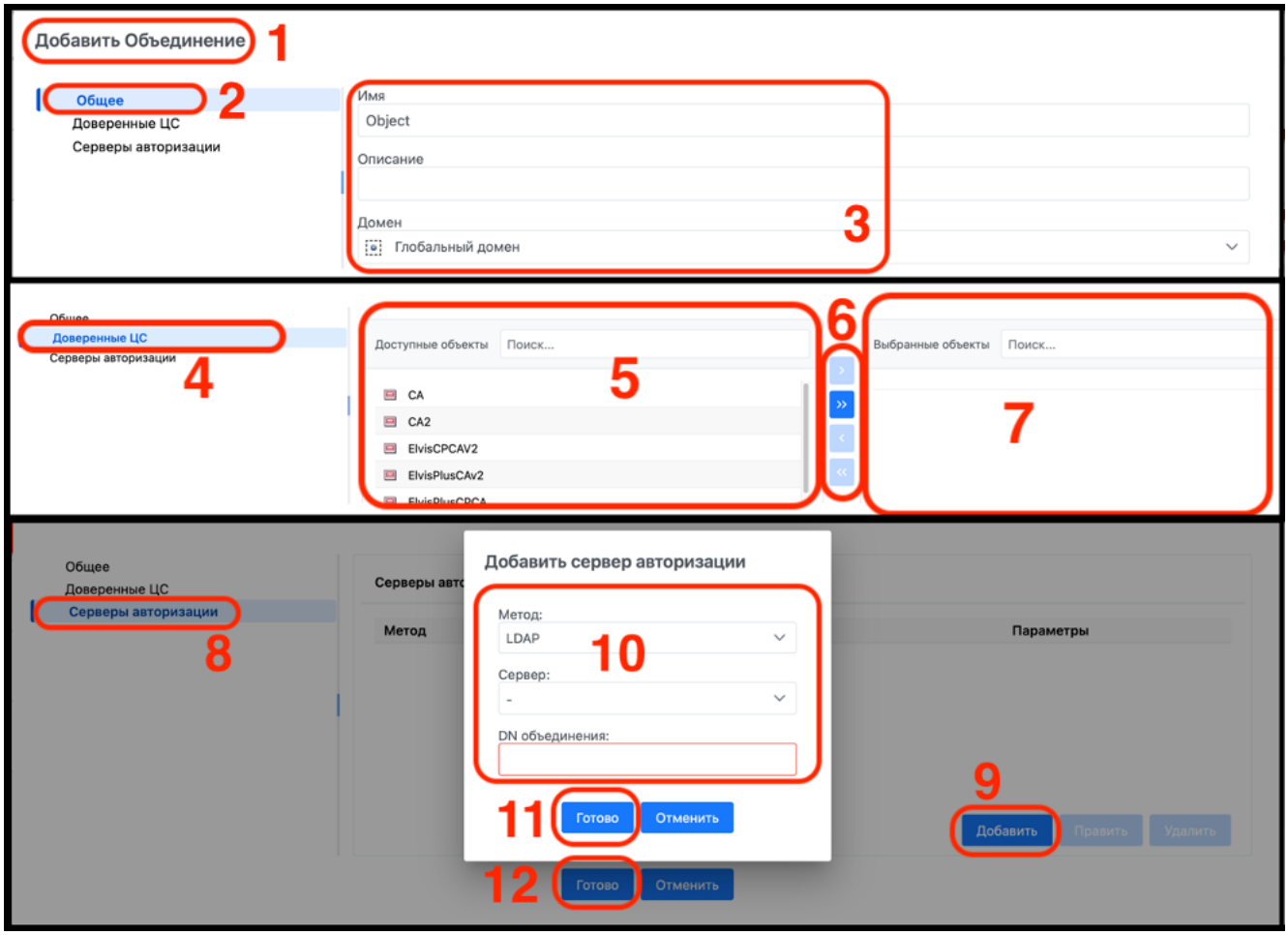


Рисунок 100 – Добавление объединения объектов

В открывшемся окне настроек «Добавить Объединение» (цифра 1) необходимо:

1) в элементе списка «Общие» (цифра 2) ввести в блоке настроек (цифра 3) требуемые параметры;
2) в элементе списка «Доверенные ЦС» (цифра 4) в блоке «Доступные объекты» (цифра 5) выбрать нужный объект и при помощи инструментов переноса (цифра 6) переместить его в блок «Выбранные объекты» (цифра 7);
3) в элементе списка «Серверы авторизации» (цифра 8) нажать кнопку «Добавить» (цифра 9);
4) в открывшемся окне заполнить параметры для добавления сервера авторизации (цифра 10), нажать кнопку «Готово» (цифра 11).

Завершить настройки с помощью кнопки «Готово» (цифра 12).

6.2.5.1 Работа с контекстным меню для элементов списка «Объединения»

Контекстное меню элемента списка «Объединения» представлено на рисунке (см. Рисунок 101).

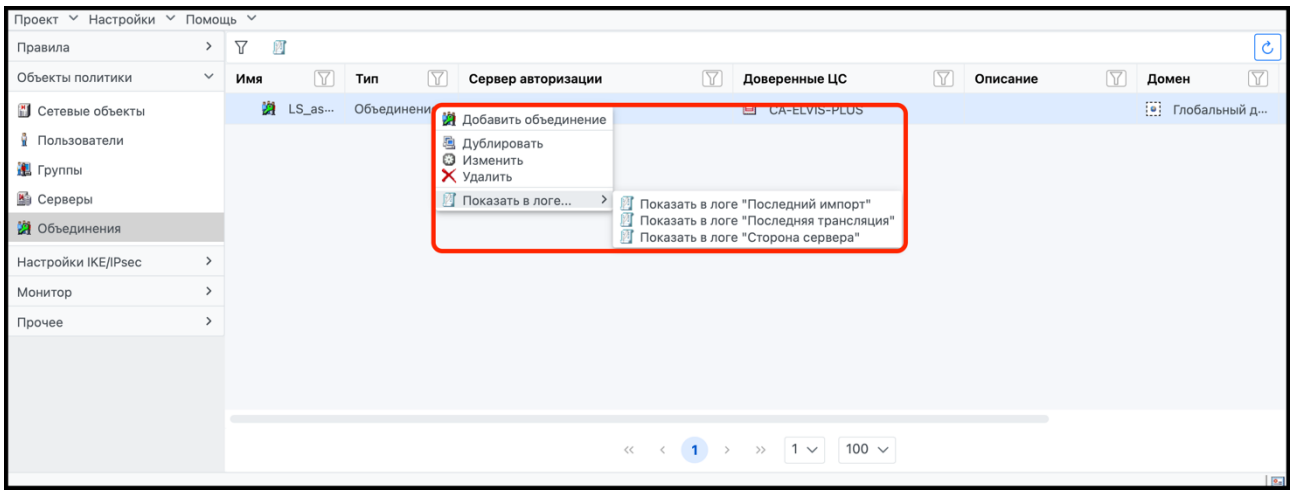


Рисунок 101 – Контекстное меню элемента списка «Объединения»

В контекстном меню отображается список общих команд: «Добавить объединение», «Дублировать», «Изменить», «Удалить», «Показать в логе», а также быстрый доступ к журналам в выпадающем списке.

6.3 Вкладка боковой панели «Настройки IKE/IPsec»

Вкладка боковой панели «Настройки IKE/IPsec» изображена на рисунке (см. Рисунок 102).

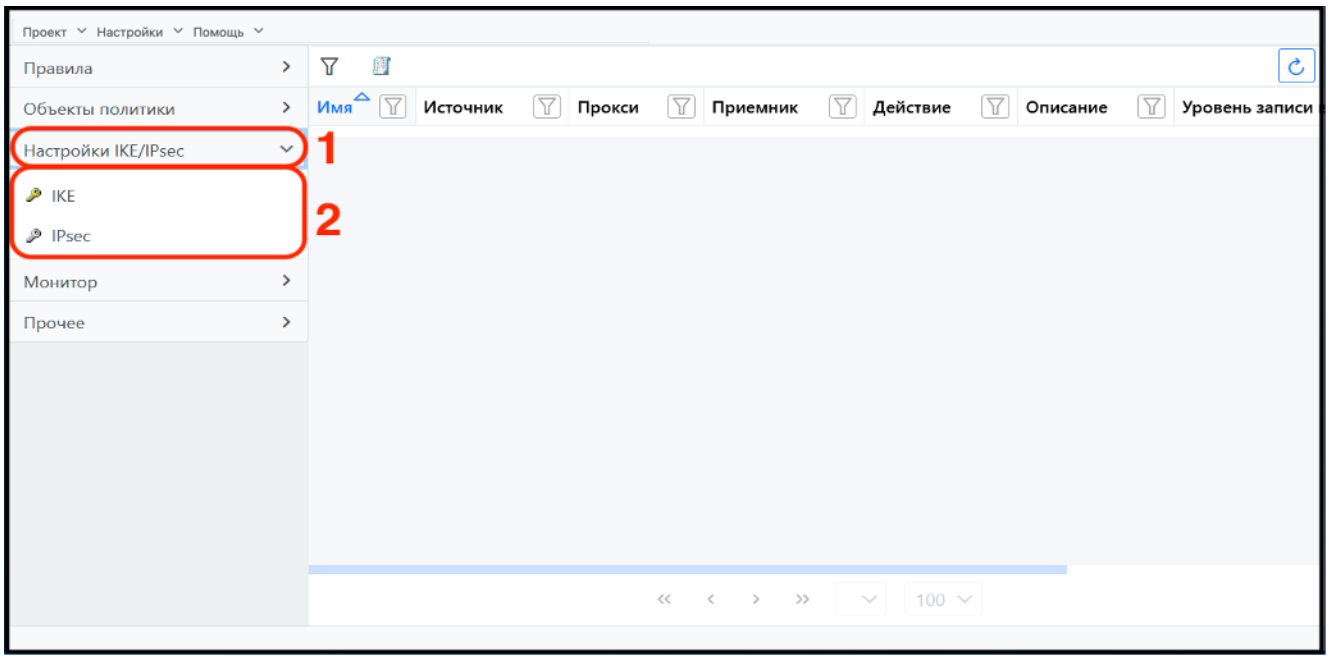


Рисунок 102 – Вкладка «Настройки IKE/IPsec»

Вкладка боковой панели «Настройки IKE/IPsec» (цифра 1) содержит следующие элементы списка (цифра 2):

— «IKE» для определения параметров протокола IKE;

— «IPsec» – содержит список IPsec-действий и IPsec-предложений.

6.3.1 IKE

Элемент списка IKE используется для определения параметров протокола IKE (Internet Key Exchange), которые будут использоваться в процессе установления первичного защищенного соединения (IKE/ISAKMP SA).

6.3.1.1 Объекты IKE и IKE предложения

Объекты IKE и IKE предложения – это набор параметров IKE, предлагаемых партнеру по связи для согласования защищенного соединения ISAKMP во время первой фазы IKE. Параметры первой фазы IKE и набор алгоритмов для шифрования – это два независимых набора параметров и алгоритмов, которые требуют настройки в разных элементах списка (IKE и IPsec соответственно). Эти параметры являются глобальными и затрагивают все объекты ГПБ, которые участвуют в правилах.

Криптоплагины на агентах должны содержать те же алгоритмы шифрования, которые поддерживаются всеми агентами в данном правиле, которые применяют настройку «Действие», в том числе и устройствами третьей стороны. Так же агенты должны содержать хотя бы один из настроенных IKE предложений, используемых в правилах с этими агентами IPsec предложений.

При создании нового проекта ГПБ IKE предложения будут представлены по умолчанию. IKE-предложения, связанные с алгоритмами аутентификации и шифрования, создаются пользователями: можно создать любое необходимое количество, в зависимости от того, какие алгоритмы шифрования доступны.

Если есть несколько IKE-предложений, то их параметры отображаются последовательно, согласно их положению в иерархической структуре (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.

Вид элемента списка «IKE» представлен на рисунке (см. Рисунок 103).

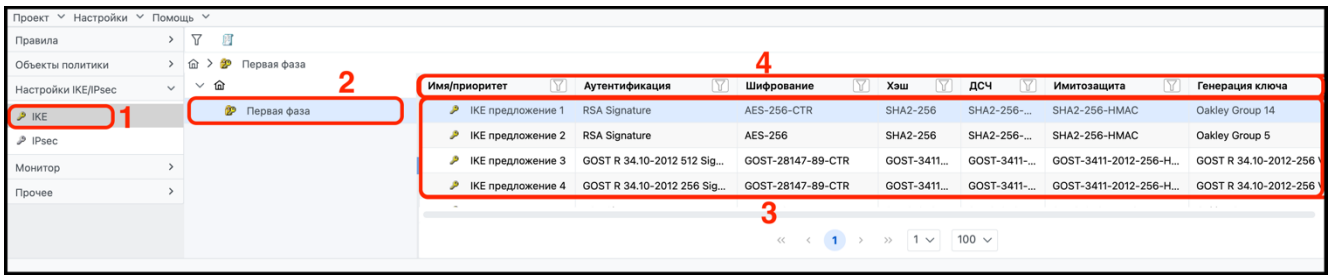


Рисунок 103 – Вкладка «Настройки IKE»

В окне элемента списка «IKE» (цифра 1) будет отображен список первой фазы (цифра 2) IKE-предложений (цифра 3) в виде таблицы с указанием следующей информации (цифра 4):

— «Имя/приоритет»;

— «Аутентификация»;

— «Шифрование»;

— «Хэш»;

— «ДСЧ» (датчик случайных чисел);

— «Имитозащита»;

— «Генерация ключа».

По каждому из параметров возможна сортировка списка.

В случае необходимости можно редактировать объекты IKE. Для этого необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 104).

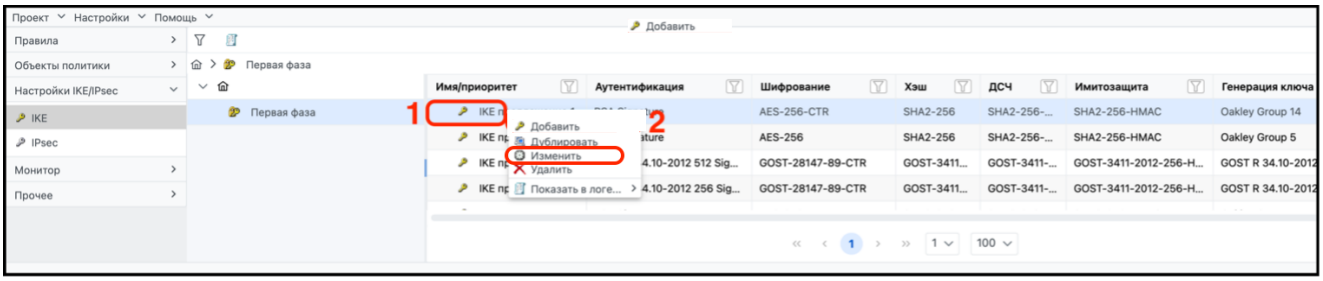


Рисунок 104 – Редактирование объектов IKE

Выделить левой клавишей мыши требуемый объект в списке (цифра 1), вызвать его контекстное меню правой клавишей мыши и выбрать команду «Изменить» (цифра 2).

6.3.1.2 Добавление IKE предложения

Окно элемента списка «Добавить IKE предложение» представлено на рисунке (см. Рисунок 105).

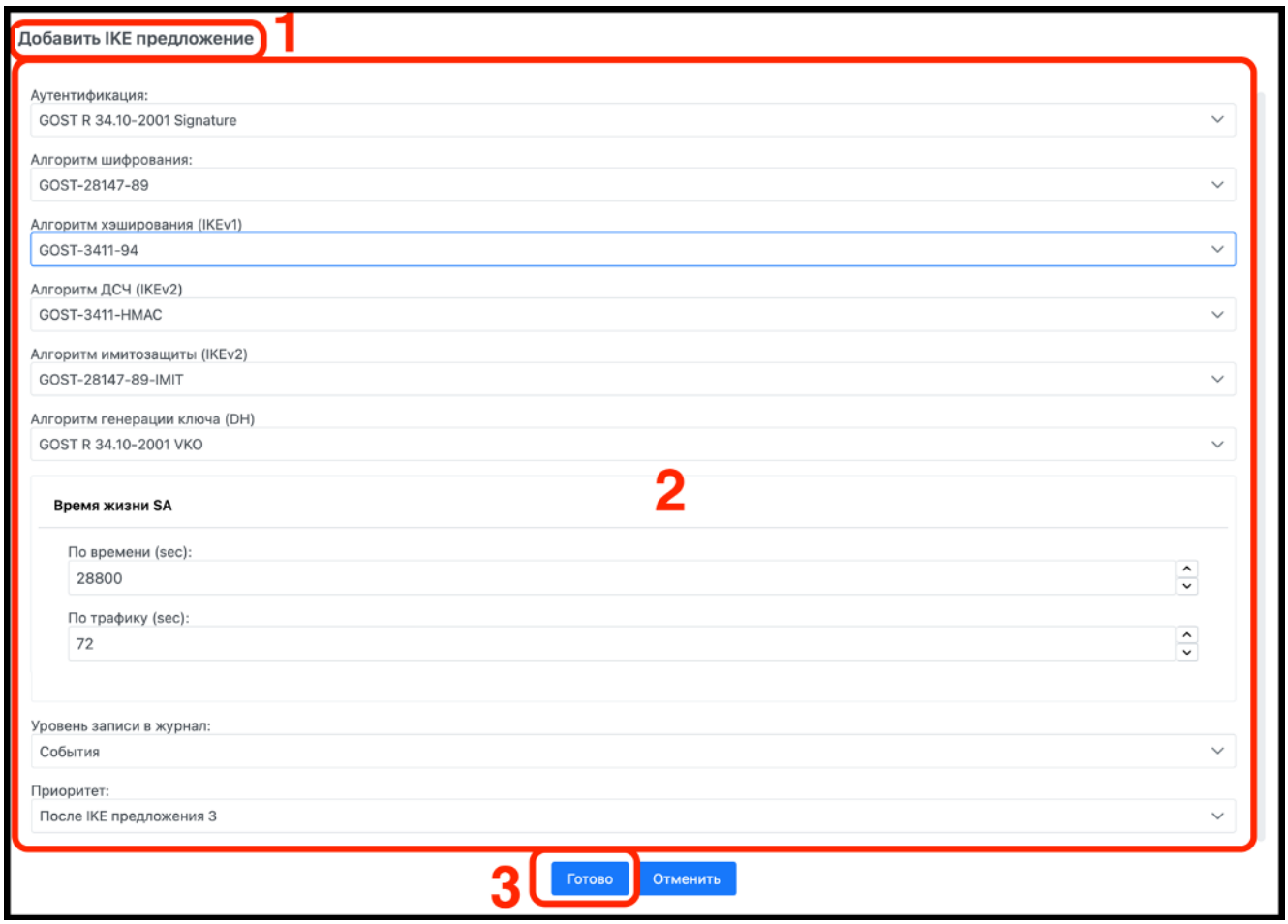


Рисунок 105 – Окно создания IKE-предложения

В окне элемента списка «Добавить IKE предложение» (цифра 1) указать значения параметров IKE предложения в блоке настроек (цифра 2). Описание параметров настройки представлено в таблице (см. Таблица 14).

Таблица 14 – Параметры настройки IKE предложения

Параметр	Описание
Аутентификация	Алгоритм аутентификации IKE
Алгоритм шифрования	Алгоритм шифрования IKE
Алгоритм хеширования (IKEv2)	Алгоритм реализации хеш-функции IKE
Алгоритм ДСЧ (IKEv2)	Алгоритм датчика случайных чисел
Алгоритм имитозащиты (IKEv2)	Алгоритм имитозащиты
Алгортм создания ключа (DH)	Алгортм создания ключа
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 событий в журнале	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 иерархической структуре, - сверху вниз. Приоритет может быть от 1 до 4. Самые приоритетные IKE предложения должны находиться выше всех остальных в структуре

Если участники среды безопасности будут использовать разные опции аутентификации и шифрования, тогда потребуется более одного набора IKE параметров. Если партнерам по связи в ГПБ потребуются предварительно распределенные ключи, тогда необходимо создать особое IKE предложение, в котором будет определяться порядок аутентификации предварительно распределенных ключей. Если существует более одного набора IKE параметров, необходимо указать порядок объектов в дереве с помощью выпадающего списка «Приоритет» в блоке настроек IKE.

Если будет использоваться только один набор IKE параметров, тогда не обязательно создавать новый предлагаемый набор параметров. Если необходимо изменить параметры, установленные по умолчанию, для уже существующего набора, нужно отредактировать объект «IKE предложение», установленный по умолчанию. Для этого требуется выбрать объект «IKE предложение» и отредактировать его параметры в выпадающих списках и числовых полях, которые появятся в блоке настроек IKE.

Некоторые типы алгоритмов аутентификации и шифрования, представленные по умолчанию в ПО ЗУ.

Чтобы изменить какой-либо параметр аутентификации, необходимо выбрать одно из IKE-предложений, которое необходимо редактировать, и изменить нужный параметр. Если другие субъекты среды безопасности используют сертификаты с разными алгоритмами цифровой подписи, тогда нужно создать IKE предложение (командой «Добавить» из контекстного меню) 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, необходимо создать отдельные IKE предложения для каждого возможного варианта.

6.3.1.2.1 Примеры IKE предложений

IKE предложения для алгоритма шифрования МАГМА представлены в таблице (см. Таблица 15).

Таблица 15 – IKE предложения для алгоритма шифрования МАГМА

Параметр	Значение
Аутентификация:	GOST R 34.10-2012 512 Signature
Алгоритм шифрования	GOST-3412-2015-M-MGM
Алгоритм имитозащиты	None
Алгоритм хэширования (IKEv1)	GOST-3411-2012-256
Алгоритм ДСЧ (IKEv2)	GOST-3411-2012-512-HMAC
Алгоритм генерации ключа (DH)	GOST R 34.10-2012-512

IKE предложения для алгоритма шифрования КУЗНЕЧИК представлены в таблице (см. Таблица 16).

Таблица 16 – IKE предложения для алгоритма шифрования КУЗНЕЧИК

Параметр	Значение
Аутентификация:	GOST R 34.10-2012 512 Signature
Алгоритм шифрования	GOST-3412-2015-K-MGM
Алгоритм имитозащиты	None
Алгоритм хэширования (IKEv1)	GOST-3411-2012-256
Алгоритм ДСЧ (IKEv2)	GOST-3411-2012-512-HMAC
Алгоритм генерации ключа (DH)	GOST R 34.10-2012-512

Для агента не поддерживающего алгоритмы шифрования МАГМА или КУЗНЕЧИК возможно использование IKE предложения, представленного в таблице (см. Таблица 17).

Таблица 17 – IKE предложения для алгоритма шифрования ГОСТ 28147-89

Параметр	Значение
Аутентификация:	GOST R 34.10-2012 256 Signature
Алгоритм шифрования	GOST-28147-89-CTR
Алгоритм имитозащиты (IKEv2)	GOST-3411-2012-256-HMAC
Алгоритм хэширования (IKEv1)	GOST-3411-2012-256
Алгоритм ДСЧ (IKEv2)	GOST-3411-2012-256-HMAC
Алгоритм генерации ключа (DH)	GOST R 34.10-2012-256 VKO

6.3.1.3 Обмен сертификатами

Функция «Обмен сертификатами» позволяет выбрать один из трех вариантов, определяющих обмен сертификатами во время переговоров ISAKMP SA (см. Таблица 18). Для перехода к настройкам обмена сертификатами требуется выполнить шаги, изображенные на рисунке (см. Рисунок 106).

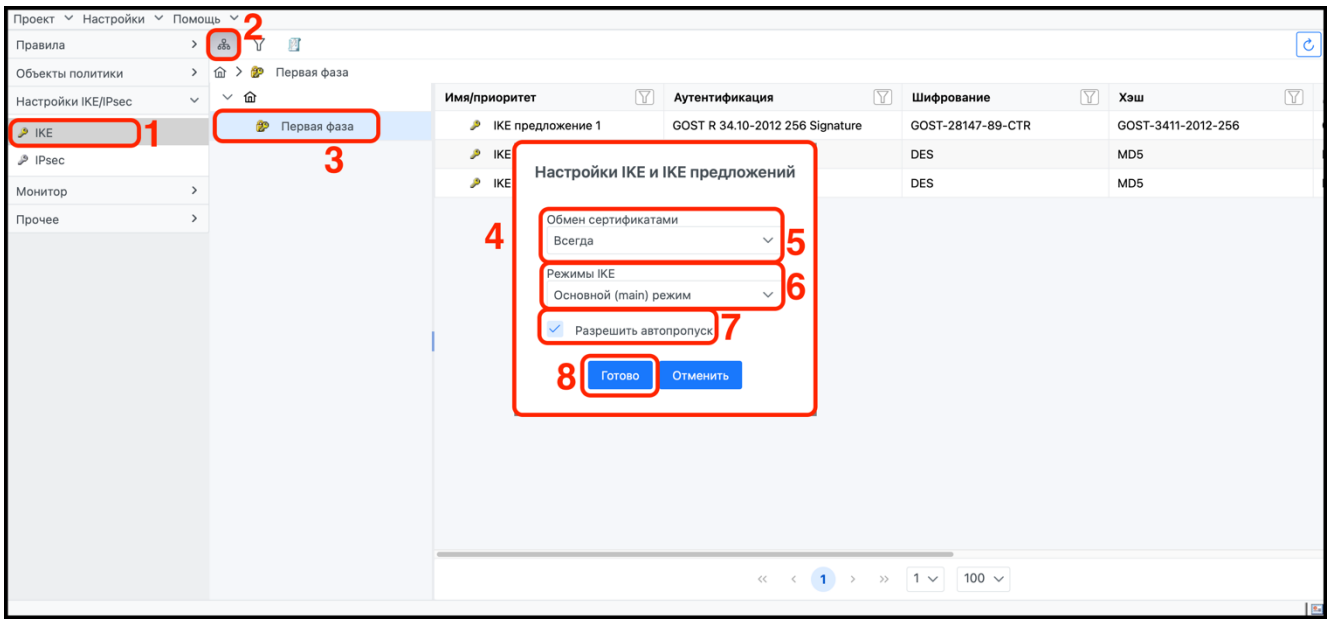


Рисунок 106 – Окно настройки IKE и IKE-предложений

В окне элемента списка «IKE» (цифра 1) перейти с помощью элемента «⁂» (цифра 2) в структурный список, дважды нажать левой клавишей мыши на строку «Первая фаза» (цифра 3). В результате откроется окно настроек «Настройки IKE и IKE предложений» (цифра 4).

В поле «Обмен сертификатами» (цифра 5) с помощью элемента «⌄» раскрыть выпадающий список и выбрать требуемый параметр. Описание параметров обмена сертификатами представлено в таблице (см. Таблица 18). По умолчанию будет установлено значение «Всегда».

В поле «Режимы IKE» (цифра 6) с помощью элемента «⌄» раскрыть выпадающий список и выбрать требуемый режим соединения, который будет использоваться для защищенного обмена:

— основной режим предоставляет полную защиту, однако требует больше времени, включая минимум шесть информационных обменов;

— агрессивный режим не гарантирует полную защиту, однако включает в себя менее шести информационных обменов.

Описание параметров режимов представлено в таблице (см. Таблица 19). По умолчанию будет установлено значение «Основной (main) режим».

Установить при необходимости флажок «Разрешить автопропуск» (цифра 7). Если флажок установлен, трафик протокола ISAKMP/IKE между двумя партнерами по связи будет пропускаться вне зависимости от индивидуальных настроек партнеров по связи. Например, если настройки отдельно взятого объекта хоста безопасности, шлюза безопасности, пользователя («ЗАСТАВА-Клиент») 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. Также, 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 флажок «Разрешить автопропуск» не установлен, это будет означать, что пропуск ISAKMP/IKE-трафика между объектами политики запрещен. Таким образом, невозможно будет установить защищенное соединение IKE между объектами политики (необходимо вручную создать правила для пропуска IKE-трафика). В обычных условиях рекомендуется проставлять флажок «Разрешить автопропуск».

После завершения настроек нажать кнопку «Готово» (цифра 8).

Таблица 18 – Описание параметров обмена сертификатами

Параметр	Описание
Всегда	Обмен сертификатами между партнерами по связи будет производиться всегда при переговорах в защищенном соединении

Параметр	Описание
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

Таблица 19 – 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, Агрессивный режим	Если 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)

6.3.2 IPsec

Вид элемента списка «IPsec» представлен на рисунке (см. Рисунок 107).

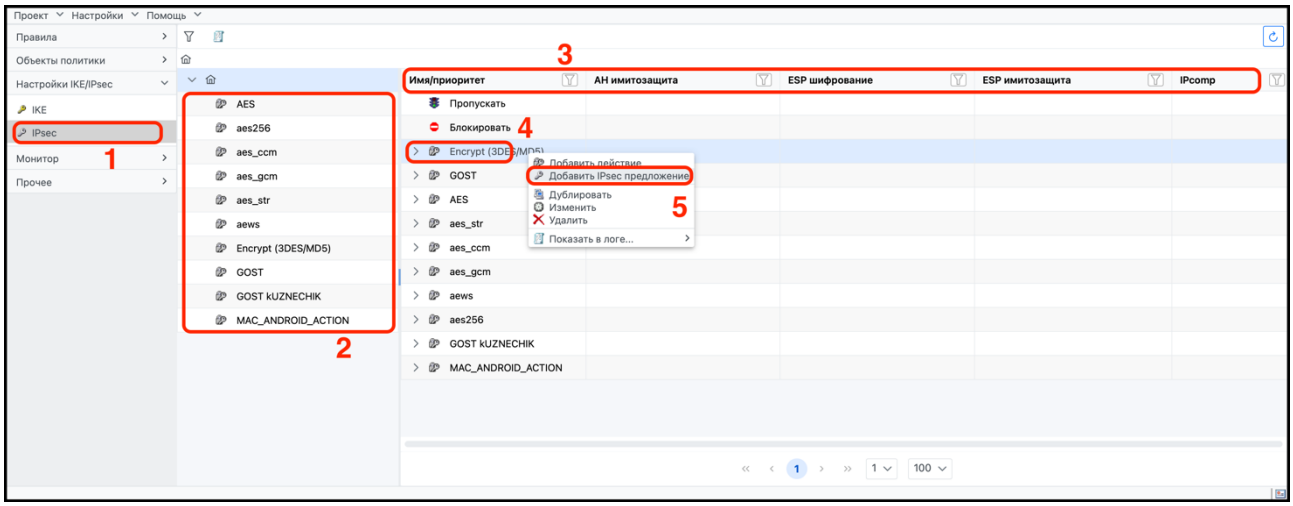


Рисунок 107 – Элемент списка IPsec

В окне элемента списка «IPsec» (цифра 1) отобразится список IPsec-действий (цифра 2). В рабочей области таблицы будут отображаться IPsec предложения (цифра 4) с указанием следующей информации (цифра 3):

— «Имя/приоритет»;
— «АН имитозащита»;
— «ESP шифрование»;
— «ESP имитозащита»;
— «IPcomp».

По каждому из параметров возможна сортировка списка.

В случае необходимости добавления IPsec предложений и других функций (создания или редактирования действия) необходимо перейти в контекстное меню. Для этого в пустом месте рабочей области таблицы или в строке с требуемым объектом (цифра 4) вызвать его контекстное меню правой клавишей мыши и выбрать команду «Добавить IPsec предложение» (цифра 5).

6.3.2.1 Добавление IPsec предложения

Для добавления IPsec предложения необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 108).

Рисунок 108 – Окно «Добавить IPsec предложение»

В окне «Добавить IPsec предложение» (цифра 1) настроить:

1) в блоке «АН протокол» (цифра 2) при необходимости использования протокола АН установить флажок «Включить АН» и выбрать алгоритм аутентификации, который будет использоваться протоколом АН;
2) в блоке «ESP протокол»[4)] (цифра 3) (флажок установлен по умолчанию);

[4)] Должны использоваться только те алгоритмы шифрования, которые поддерживаются всеми агентами в данном правиле, которое применяет IPsec-действие, в том числе устройствами третьей стороны.

3) алгоритм шифрования и имитозащиты, которые будет использоваться протоколом ESP см. п. 6.3.2.1.1;
4) в блоке «IPComp» (цифра 4) установить, при необходимости, флажок для применения протокола IPComp. Затем выбрать алгоритм сжатия, который будет использоваться протоколом IPComp;
5) в блоке «Время жизни SA»[5)] (цифра 5) задать в поле «Время жизни SA» предельное время (сек) и установить максимальное значение поля «По трафику» (Кбайт). В поле «Приоритет» выбрать требуемое значение.

После выполненных настроек нажать кнопку «Готово» (цифра 6). В результате в рабочей области таблицы будет добавлено новое IPsec предложение.

6.3.2.1.1 Примеры IPsec предложений

IPsec предложения для алгоритма шифрования МАГМА представлены в таблице (см. Таблица 20).

Таблица 20 – IPsec предложения для алгоритма шифрования МАГМА

Параметр	Значение
Алгоритм шифрования	GOST-3412-2015-M-MGM
Алгоритм имитозащиты	None

IPsec предложения для алгоритма шифрования КУЗНЕЧИК представлены в таблице (см. Таблица 21).

Таблица 21 – IPsec предложения для алгоритма шифрования КУЗНЕЧИК

Параметр	Значение
Алгоритм шифрования	GOST-3412-2015-K-MGM
Алгоритм имитозащиты	None

Для агента не поддерживающего алгоритмы шифрования МАГМА или КУЗНЕЧИК возможно использование IKE предложения, представленного в таблице (см. Таблица 22).

Таблица 22 – IPsec предложения для алгоритма шифрования ГОСТ 28147-89

Параметр	Значение
Алгоритм шифрования	GOST-28147-89-CTR-DIVERS
Алгоритм имитозащиты	GOST-28147-89-IMIT

6.3.2.2 Добавление действия

«Действия» определяют, как входящий/исходящий трафик, будет обрабатываться на данном устройстве защиты. Объект действия представляет собой комбинации опций аутентификации и шифрования, которые используются правилами ГПБ для того, чтобы определять, как агенты в данной среде безопасности будут обрабатывать различные типы

[5)] Для параметров «Предельное время (сек)» и «Предельный трафик (Кбайт)», значение «ноль» (0) подразумевает «неограниченно». Не рекомендуется использовать ограничение «Предельный трафик» (Кбайт), когда ГПБ включает в себя правила, распространяющиеся на пользователей.

трафика, установленные в сетевых сервисах. По умолчанию установлено действие «Encrypt (GOST/GOST)», которое зашифровывает трафик с помощью алгоритма ГОСТ, затем пропускает его.

Для добавления действия необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 109).

Рисунок 109 – Добавление действия

Нажать правой клавишей мыши на выбранный объект в списке IPsec-предложений (цифра 1) и в контекстном меню выбрать команду «Добавить действие» (цифра 2).

Вид окна «Добавить действие» представлено на рисунке (см. Рисунок 110).

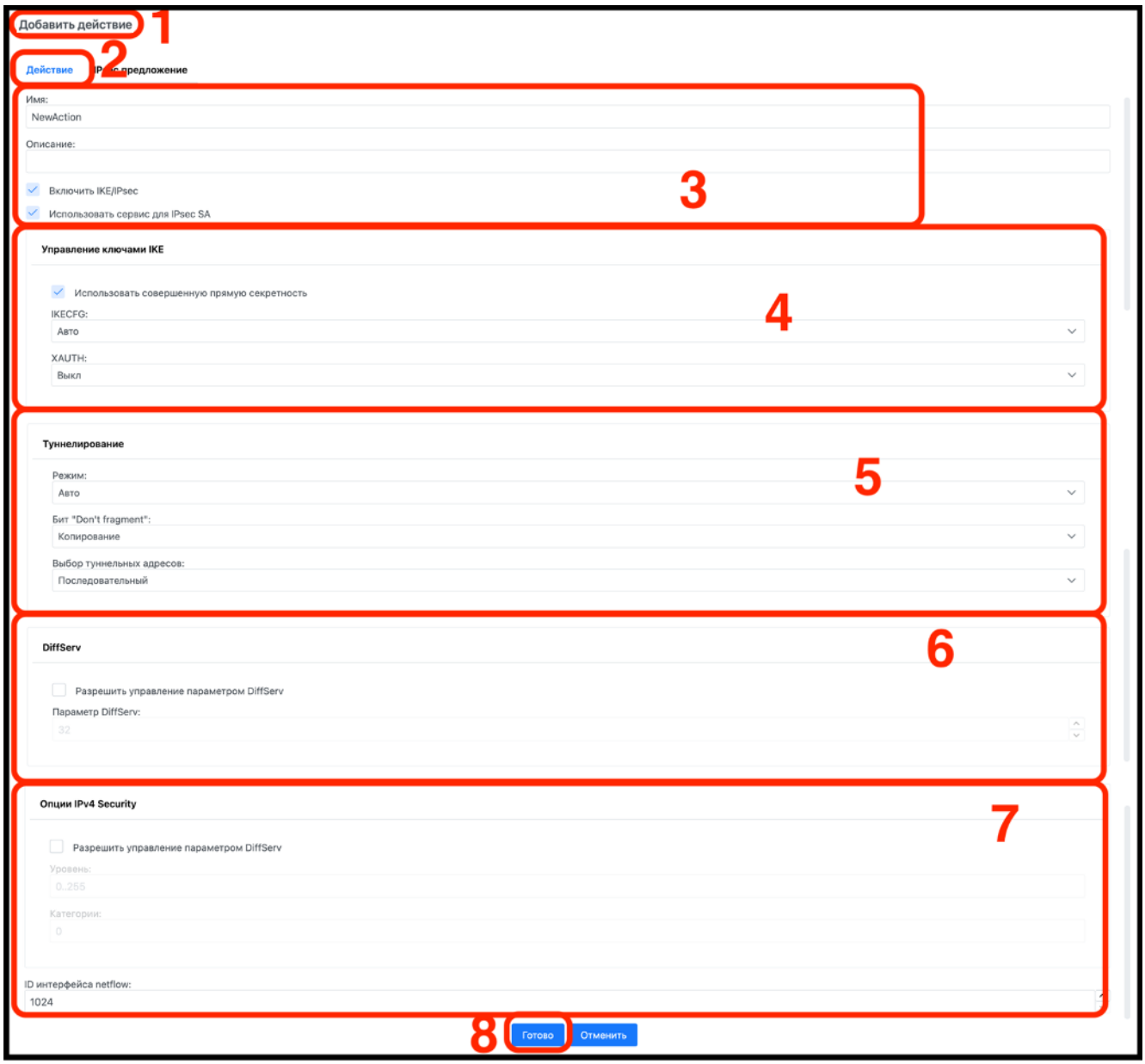


Рисунок 110 – Окно «Добавить действие»

В открывшемся окне «Добавить действие» (цифра 1) перейти во вкладку «Действие» (цифра 2), далее:

1) ввести в блоке (цифра 3) уникальное имя для нового действия. При необходимости можно ввести текстовое описание действия. Если требуется установить флажок «Включить IKE/IPsec». При установке флажка «Использовать сервис для IPsec SA» создаются узкие правила с FW-процедурами с указанием порта и протокола, если флажок снят, то используются широкие правила;
2) в блоке «Управление ключами IKE» (цифра 4) установить флажок «Использовать совершенную прямую секретность», если требуется использовать криптосистему, где шифрованный текст не дает никакой информации об открытом тексте, за исключением его длины, которая будет создавать новую пару ключей для каждого сеанса защищенного соединения IPsec. 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;

3) выбрать одно из значений из выпадающего списка IKECFG, чтобы настроить работу алгоритма трассировки топологии ПО ЗУ. 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;

— значение, выбранное в выпадающем списке XAUTH, повлияет на алгоритм трассировки ПО ЗУ. Значения те же, что и для IKECFG;

4) выбрать в блоке «Туннелирование» (цифра 5):

— «Режим». Доступные значения:

  – «Авто»;
  – «Туннельный»;
  – «Транспортный»;

— параметры для «Бит «Don`t fragment» 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 невыполнения фрагментации) в новом внешнем IP-заголовке. Доступны следующие установки:

  – «Копирование» - копировать значение «Don`t fragment bit» из исходного IP-пакета;
  – «Установка» - для «Don`t fragment bit» устанавливается значение «1»;
  – «Очистка» - для «Don`t fragment bit» устанавливается значение «0» (по умолчанию);

— выбрать туннельный адрес:

  – «Последовательный»;
  – «Случайный»;

5) в блоке «DiffServ» (цифра 6) установить флажок «Разрешить управление параметром DiffServ» и установить нужное значение в поле «Параметр DiffServ» из диапазона от 0 до 63;
6) в блоке «Опции IPv4 Security» (цифра 7) установить флажок «Разрешить опции IPv4 Security» и выполнить настройки полей «Уровень» и «Категории».

После завершения настроек нажать кнопку «Готово» (цифра 8).

6.3.3 Работа с контекстным меню для элементов списка «Настройки IKE/IPsec»

Добавление, настройка и редактирование объектов производится с помощью контекстного меню. Вызвать контекстное меню можно, нажав правой клавишей мыши в свободном месте рабочей области таблицы выбранного элемента списка боковой панели вкладок или на требуемый в списке объект.

Вид контекстного меню, вызванного путём нажатия в свободном месте области таблицы, отображен на рисунке (см. Рисунок 111).

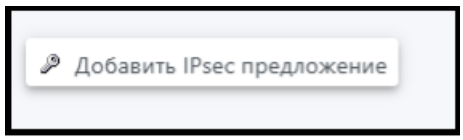


Рисунок 111 – Вид контекстного меню, вызванного со свободного места

Вид контекстного меню, вызванного путём нажатия на выбранный объект, отображен на рисунке (см. Рисунок 112).

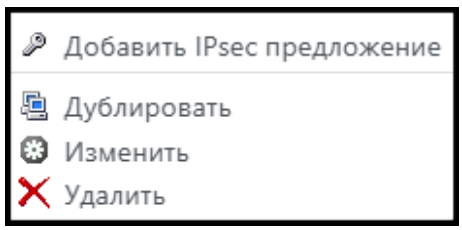


Рисунок 112 – Вид контекстного меню, вызванного с выбранного объекта

Вид контекстного меню «Добавить IPsec предложение» содержит:

— «Добавить IPsec предложение»;
— «Дублировать»;
— «Изменить»;
— «Удалить».

6.3.3.1 Дублировать

Для дублирования правила нужно выбрать требуемое правило, затем в контекстном меню выбрать команду «Дублировать» как представлено на рисунке (см. Рисунок 113).

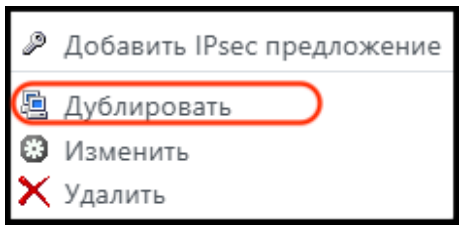


Рисунок 113 – Команда «Дублировать»

В результате откроется окно «Дублировать», в котором необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 114).

Рисунок 114 – Окно настроек «Дублировать»

В окне «Дублировать» (цифра 1) заполнить форму. После завершения действий нажать кнопку «Готово» (цифра 2).

6.3.3.2 Изменить

Для редактирования правила нужно выбрать требуемый объект, затем в контекстном меню нажать команду «Изменить», как представлено на рисунке (см. Рисунок 115).

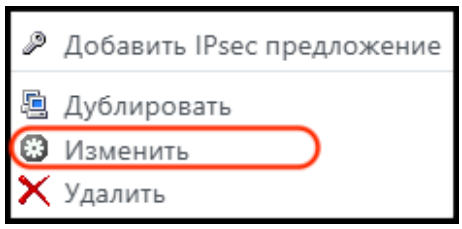


Рисунок 115 – Команда «Изменить»

В результате откроется окно «Изменить», в котором необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 116).

Рисунок 116 – Окно настроек «Изменить»

В окне «Изменить» (цифра 1) редактировать параметры выбранного объекта. После завершения всех действий нажать кнопку «Готово» (цифра 2).

6.3.3.3 Удалить

Для удаления правила необходимо выделить требуемые объекты (один или несколько), затем выбрать команду контекстного меню «Удалить», как представлено на рисунке (см. Рисунок 117).

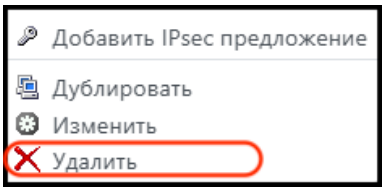


Рисунок 117 – Команда «Удалить»

В открывшемся диалоговом окне выполнить команды, представленные на рисунке (см. Рисунок 118).

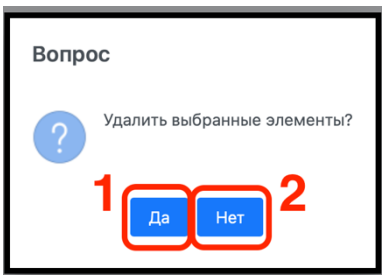


Рисунок 118 – Удаление выбранных элементов

Для удаления нажать кнопку «Да» (цифра 1). В случае если удаление не нужно, нажать кнопку «Нет» (цифра 2).

6.3.3.4 Показать в логе

Команда «Показать в логе» используется для сортировки и отображения выбранных объектов в журнале. Для перехода в журнал необходимо с помощью элемента «» перейти в иерархическую структуру, выбрать требуемый объект и нажать на него дважды левой клавишей мыши. Далее выполнить шаги, изображенные на рисунке (см. Рисунок 119).

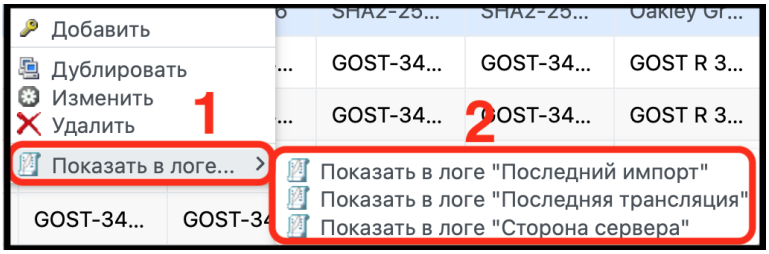


Рисунок 119 – Команда «Показать в логе»

В контекстном меню выбранного правила нажать команду «Показать в логе» (цифра 1), в дополнительном выпадающем списке выбрать требуемый журнал (цифра 2):

— «Последний импорт»;

— «Последняя трансляция»;

— «Сторона сервера».

В результате откроется окно выбранного журнала, как показано на рисунке (см. Рисунок 120).

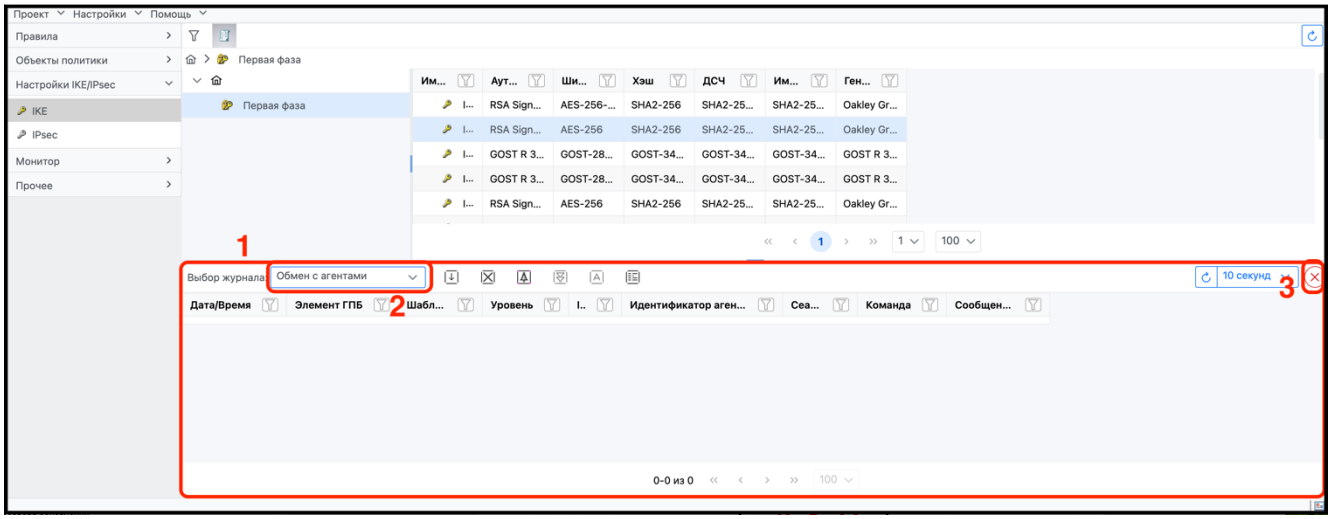


Рисунок 120 – Переход в другие журналы

В открывшемся окне (цифра 1) можно перейти в другой журнал, открыв выпадающий список (цифра 2). Выйти из режима просмотра журналов можно, нажав всплывающий элемент «» (цифра 3).

6.4 Вкладка боковой панели «Монитор»

Окно во вкладке боковой панели «Монитор» остается пустым до начала активации ГПБ. Далее после активации созданного и настроенного проекта в нем будут отображены результаты активации ГПБ: управляемые объекты политики, а также управляемые серверы, у которых есть собственная ЛПБ.

Окно вкладки боковой панели «Монитор» представлено на рисунке (см. Рисунок 121).

Рисунок 121 – Вкладка «Монитор»

Окно вкладки боковой панели «Монитор» (цифра 1) содержит следующие элементы списка (цифра 2):

— «Объекты политики»;
— «Компьютеры»;
— «Журнал»;
— «Состояние сервера»;
— «Статистика»;
— «Валидность сертификатов».

6.4.1 Объекты политики

Окно элемента списка «Объекты политики» представлено на рисунке (см. Рисунок 122).

Рисунок 122 – Элемент списка «Объекты политики»

В элементе списка «Объекты политики» (цифра 1) можно посмотреть список существующих объектов активной ГПБ в рабочей области таблицы (цифра 3). Таблица параметров объектов политики содержит следующую информацию (цифра 2):

— «Пользователь/Сетевой объект»;
— «Предупреждения»;
— «Тип»;
— «Компьютер»;
— «Последний контакт»;
— «Статус активации»;
— «Статус команды»;
— «Время изменения статуса»;
— «Метод загрузки»;
— «Версия»;
— «IP»;
— «Место»;
— «IP агента».

По каждому из параметров возможна сортировка списка.

В элементе списка «Объекты политики» доступна команда «Обновить статус монитора» (цифра 4), которая позволяет обновлять «Монитор» по заданному времени или вручную. Для удобства поиска можно использовать элементы пролистывания страниц (цифра 5).

6.4.1.1 Работа с контекстным меню элемента списка «Объекты политики»

Вызвать контекстное меню можно, нажав правой клавишей мыши на любой объект или на свободное место в рабочей области таблицы, затем выбрать требуемую команду. Контекстное меню элемента списка «Объекты политики» для добавления или редактирования объектов представлено на рисунке (см. Рисунок 123).

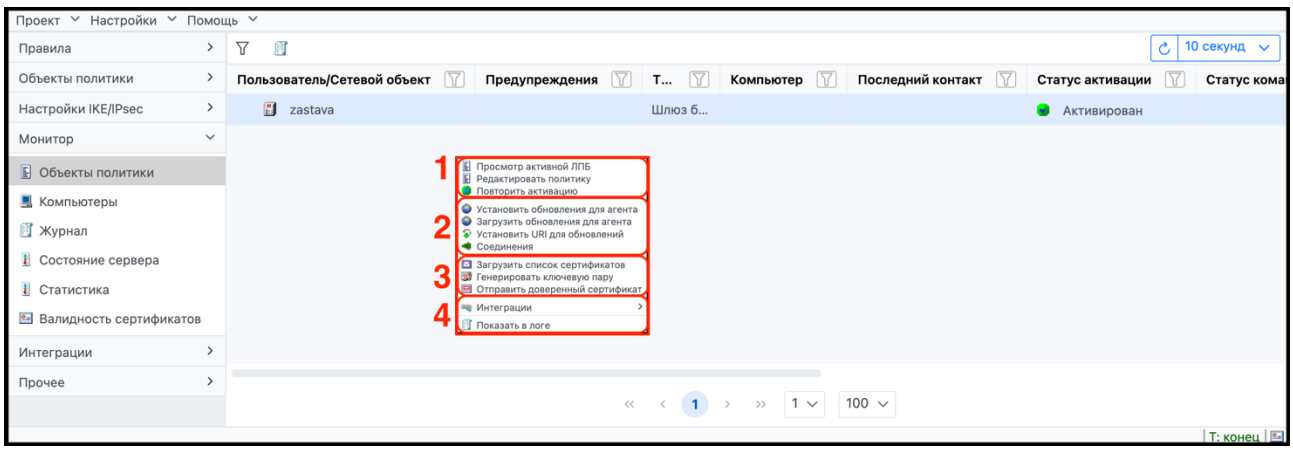


Рисунок 123 – Контекстное меню «Объекты политики»

В блоке (цифра 1) контекстного меню отображается список команд: «Просмотр активной ЛПБ», «Редактировать политику»; «Повторить активацию».

В блоке (цифра 2) контекстного меню отображается список команд: «Установить обновления для агента», «Загрузить обновления для агента»; «Установить URI для обновлений», «Соединения».

В блоке (цифра 3) контекстного меню отображается список команд: «Загрузить список сертификатов», «Генерировать ключевую пару», «Отправить доверенный сертификат».

В блоке (цифра 4) контекстного меню отображается список команд: «Интеграции» (команда отобразится если добавлены интеграции) и «Показать в логе».

6.4.1.1.1 Команда контекстного меню «Просмотр активной ЛПБ»

В контекстном меню выбрать команду «Просмотр активной ЛПБ», в результате откроется окно текстового редактора, представленное на рисунке (см. Рисунок 124).

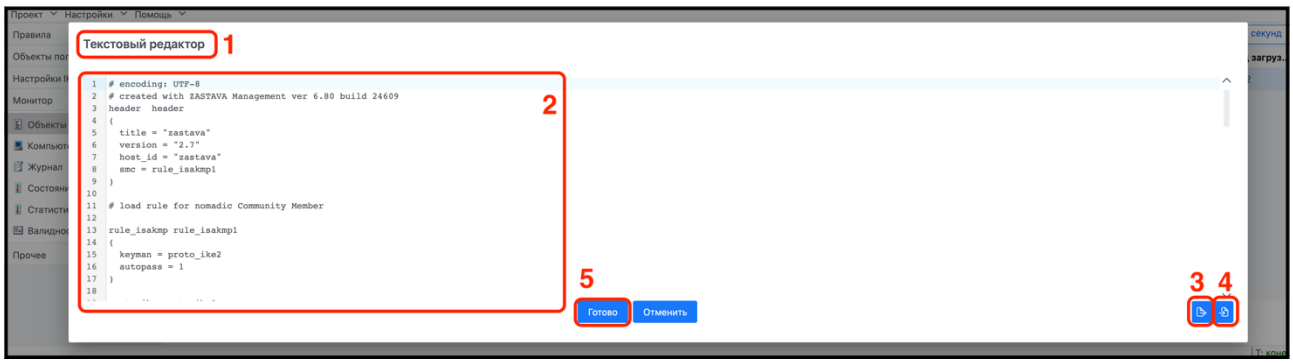


Рисунок 124 – Окно «Текстовый редактор»

В окне текстового редактора (цифра 1) при необходимости внести изменения в тексте (цифра 2). Дополнительно можно выгрузить или загрузить файл используя элементы «» – загрузить (цифра 3) или «» – выгрузить (цифра 4). Нажать кнопку «Готово» (цифра 5).

6.4.1.1.2 Команда контекстного меню «Редактировать политику»

Для выбранного объекта политики в его контекстном меню выбрать команду «Редактировать политику», в результате откроется соответствующее окно настроек выбранного объекта, в котором требуется выполнить редактирование. После редактирования требуется транслировать и затем активировать ГПБ.

6.4.1.1.3 Команда контекстного меню «Повторить активацию»

В случае проведенных изменений в настройках требуется повторить активацию, выбрав в контекстном меню «Повторить активацию».

6.4.1.1.4Команда контекстного меню «Установить обновление для агента»

В контекстном меню выбрать команду «Установить обновление для агента», в результате откроется окно, представленное на рисунке (см. Рисунок 125).

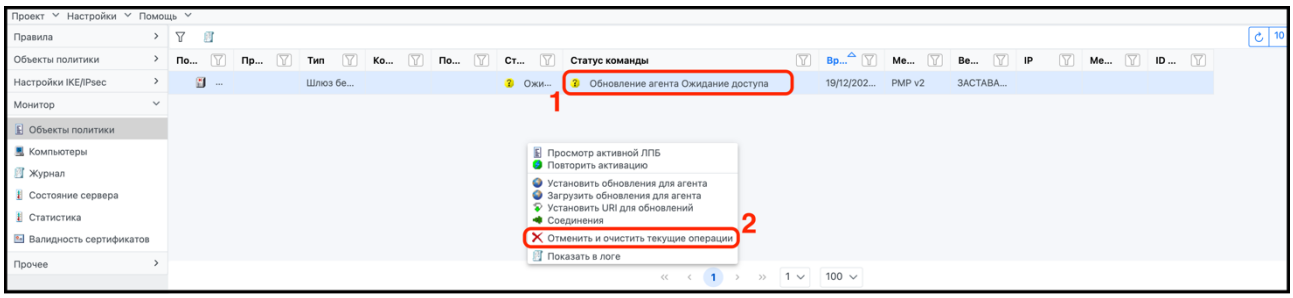


Рисунок 125 – Статус «Обновление агента. Ожидание доступа» команды «Установить обновление для агента»

В результате выполненных действий параметр «Статус команды» изменит свой вид и перейдёт в режим «Обновление агента. Ожидания доступа» (цифра 1). В случае необходимости отмены запроса требуется вызвать контекстное меню и нажать команду «Отменить и очистить текущие операции» (цифра 2).

Окно «Установить обновление для агента» после запуска удалённого обновления отображает процесс обновления (см. Рисунок 125).

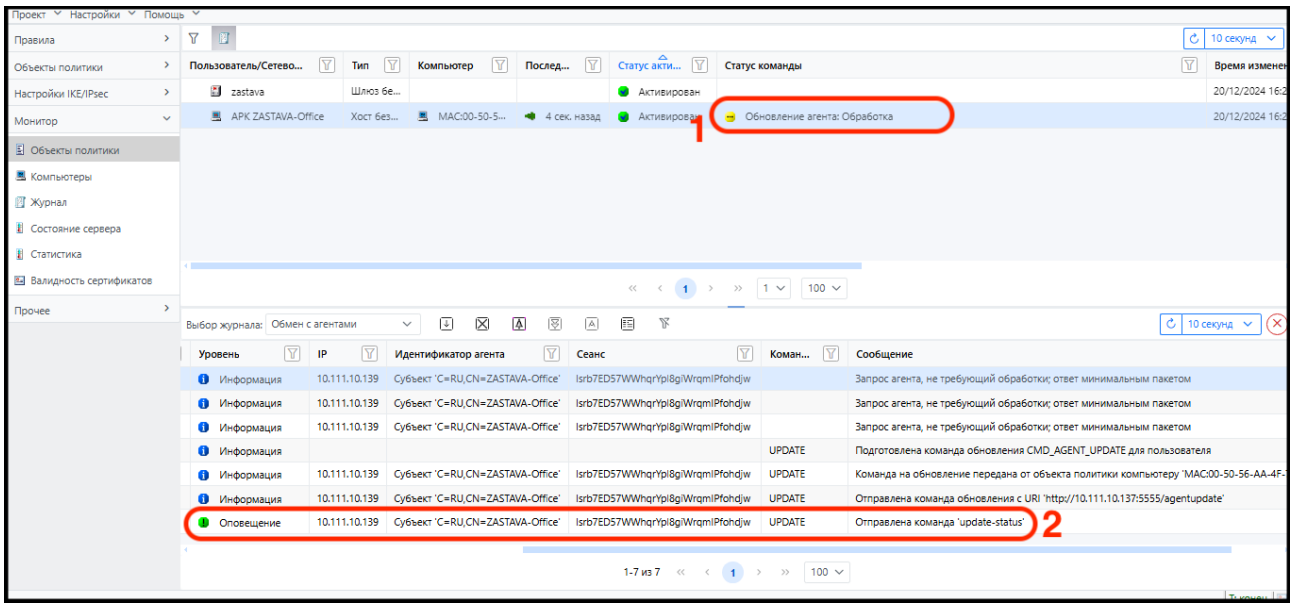


Рисунок 126 – Статус «Обновление агента: Обработка» команды «Установить обновление для агента»

После запуска удалённого обновления статус команды для выбранного объекта меняется на «Обновление агента: Обработка» (цифра 1), в журнале сообщений отобразится оповещение о процессе обновления (цифра 2).

Окно «Установить обновление для агента» после завершения процесса удалённого обновления представлено на рисунке (см. Рисунок 125).

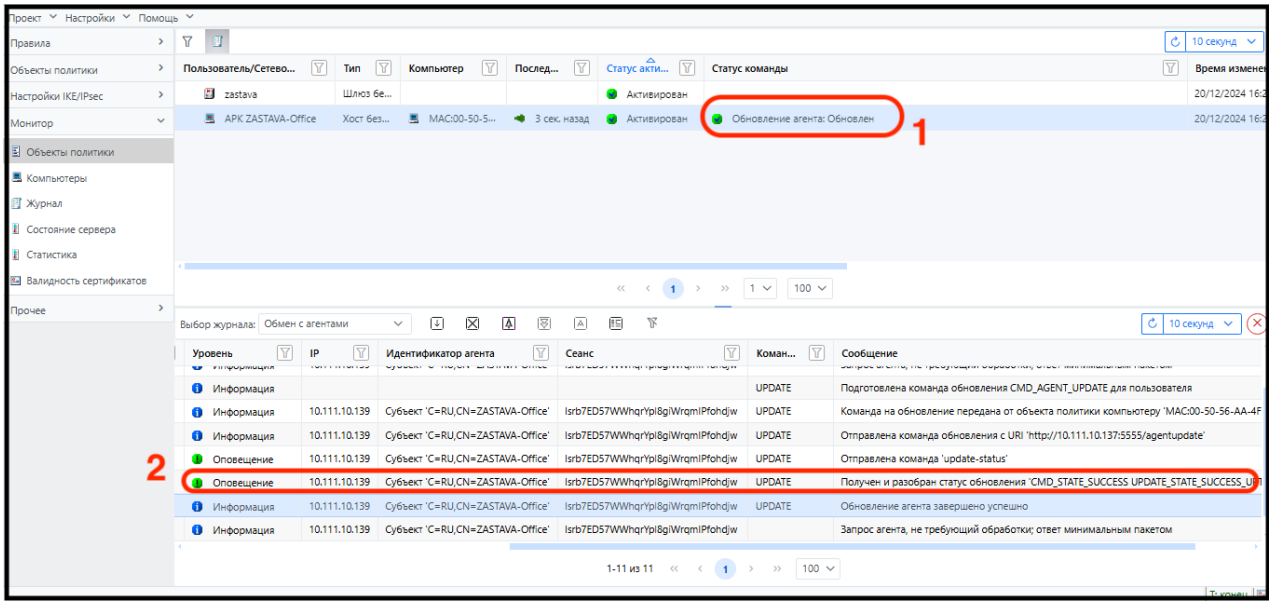


Рисунок 127 – Статус «Обновление агента: Обновлён» команды «Установить обновление для агента»

После завершения удалённого обновления статус команды для выбранного объекта меняется на «Обновление агента: Обновлён» (цифра 1), в журнале сообщений отобразится оповещение «UPDATE» об окончании процесса обновления (цифра 2).

6.4.1.1.5 Команда контекстного меню «Загрузить обновление для агента»

В контекстном меню выбрать команду «Загрузить обновление для агента», в результате откроется окно, представленное на рисунке (см. Рисунок 128).

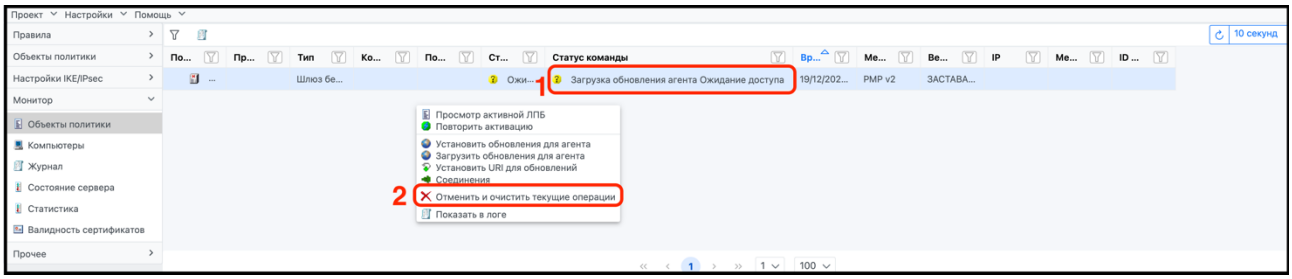


Рисунок 128 – Статус команды «Загрузить обновление для агента»

После запуска загрузки обновления параметр «Статус команды» изменит свой вид и перейдёт в режим «Загрузка обновления агента: Ожидания доступа» (цифра 1). В случае необходимости отмены запроса требуется вызвать контекстное меню и нажать команду «Отменить и очистить текущие операции» (цифра 2).

Далее будет отображаться процесс загрузки файлов обновления, и параметр «Статус команды» для выбранного объекта изменится на «Загрузка обновления агента: Обработка», в журнале сообщений отобразится оповещение о процессе загрузки файлов обновления.

После завершения процесса загрузки файлов обновления статус команды для выбранного объекта изменится на «Загрузка обновления агента: Обновлён», в журнале

сообщений отобразится оповещение «UPDATE» об окончании процесса загрузки файлов обновления.

6.4.1.1.6 Команда контекстного меню «Установить URI для обновлений»

В контекстном меню выбрать команду «Установить URI для обновлений», в результате откроется окно, представленное на рисунке (см. Рисунок 129).

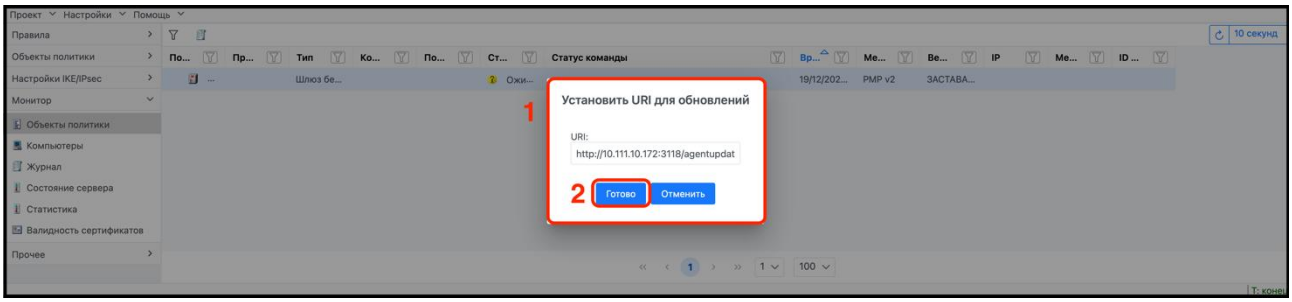


Рисунок 129 – Окно «Установить URI для обновлений»

В окне «Установить URI для обновлений» (цифра 1) ввести адрес URI и нажать кнопку «Готово» (цифра 2).

6.4.1.1.7 Команда контекстного меню «Соединения»

В контекстном меню выбрать команду «Соединения», в результате откроется окно, представленное на рисунке (см. Рисунок 130).

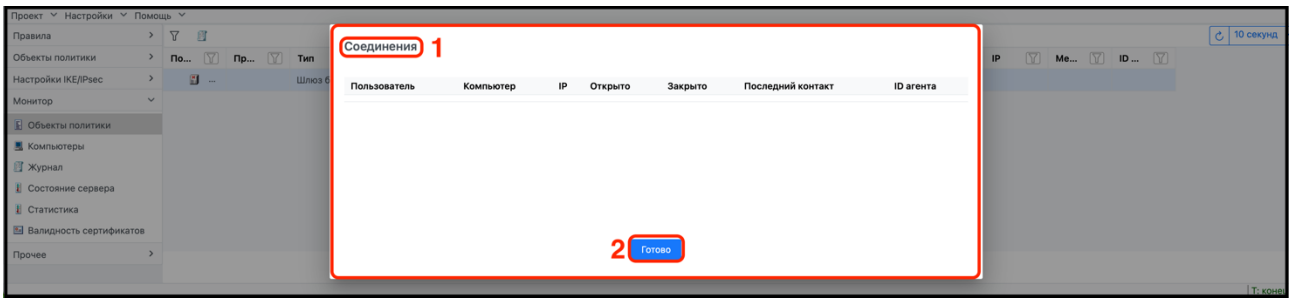


Рисунок 130 – Окно «Соединения»

В окне «Соединения» (цифра 1) выводится список текущих соединений. Для выхода из окна Соединения» требуется нажать кнопку «Готово» (цифра 2).

6.4.1.1.8 Команда контекстного меню «Загрузить список сертификатов»

В контекстном меню выбрать команду «Загрузить список сертификатов», в результате откроется окно текстового редактора, представленное на рисунке (см. Рисунок 131).

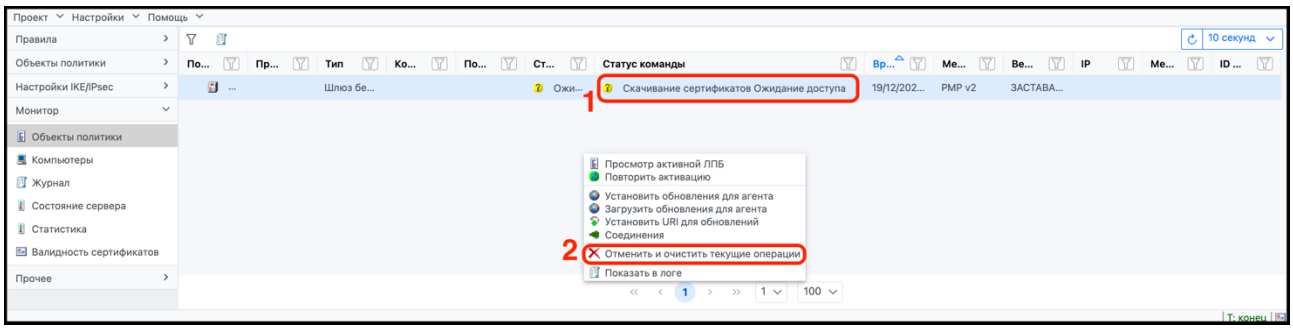


Рисунок 131 – Статус «Скачивание сертификатов: Ожидание доступа» команды «Загрузить список сертификатов»

В результате выполненных действий параметр «Статус команды» изменит свой вид и перейдёт в режим «Скачивание сертификата. Ожидания доступа» (цифра 1). В случае необходимости отмены запроса требуется вызвать контекстное меню и нажать команду «Отменить и очистить текущие операции» (цифра 2).

6.4.1.1.9 Команда контекстного меню «Генерировать ключевую пару»

В контекстном меню выбрать команду «Генерировать ключевую пару», в результате откроется окно «Создать запрос сертификата», для настройки которого необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 132).

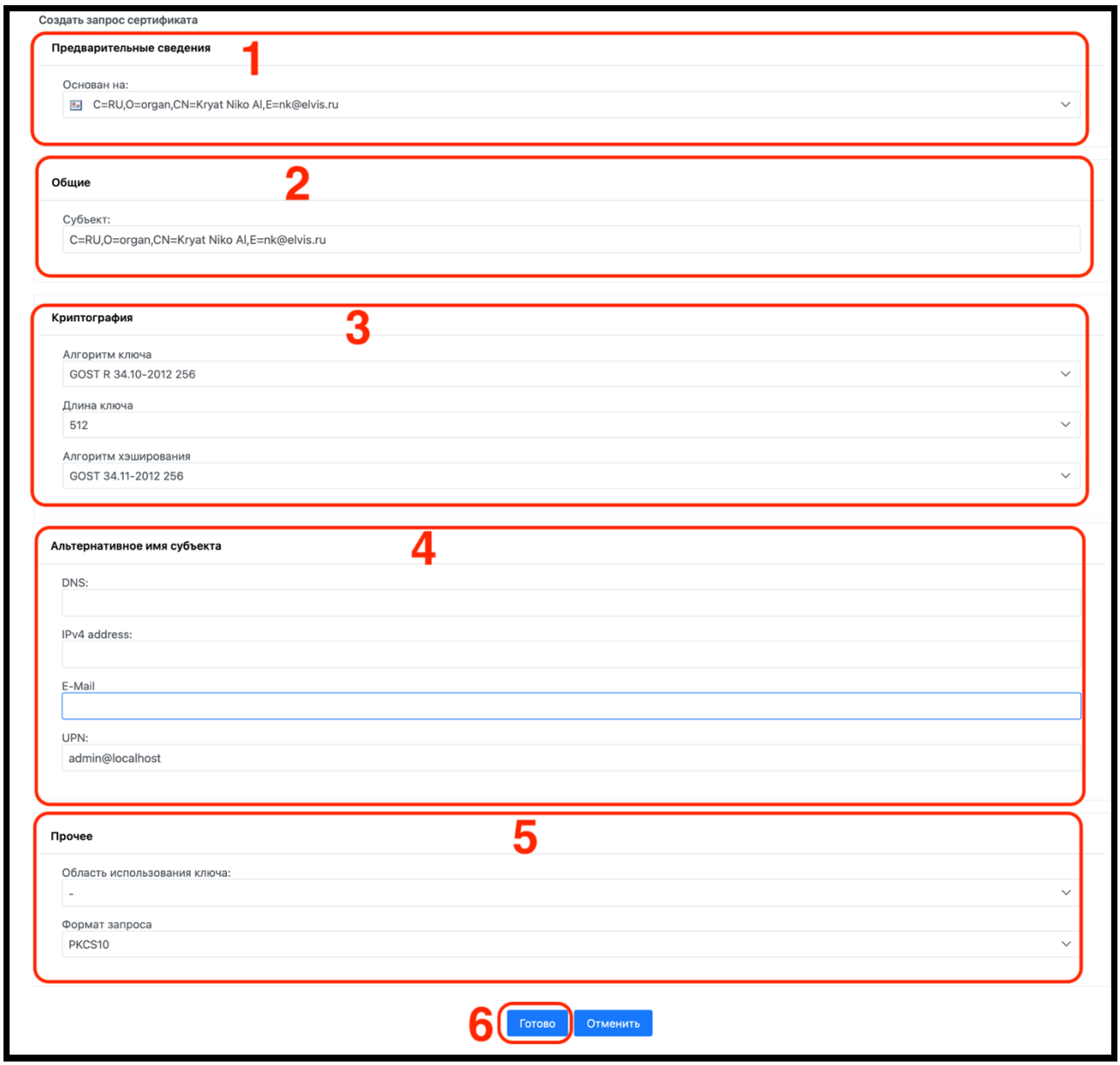


Рисунок 132 – Окно «Создать запрос сертификата»

В окне «Создать запрос сертификата» настроить требуемые параметры:

1) заполнить блок «Предварительные сведения» (цифра 1);
2) заполнить блок параметров «Общие» (цифра 2);
3) в блоке «Криптография» (цифра 3) выбрать из выпадающих списков параметры ключа;
4) задать альтернативное имя субъекта в блоке (цифра 4);
5) выполнить настройки в блоке «Прочее» (цифра 5);
6) Нажать кнопку «Готово» (цифра 6).

Подробное описание добавления сертификатов представлено в п. 6.5.5.2.

6.4.1.1.10 Команда контекстного меню «Отправить доверенный сертификат»

В контекстном меню выбрать команду «Отправить доверенный сертификат», в результате откроется, представленное на рисунке (см. Рисунок 133).

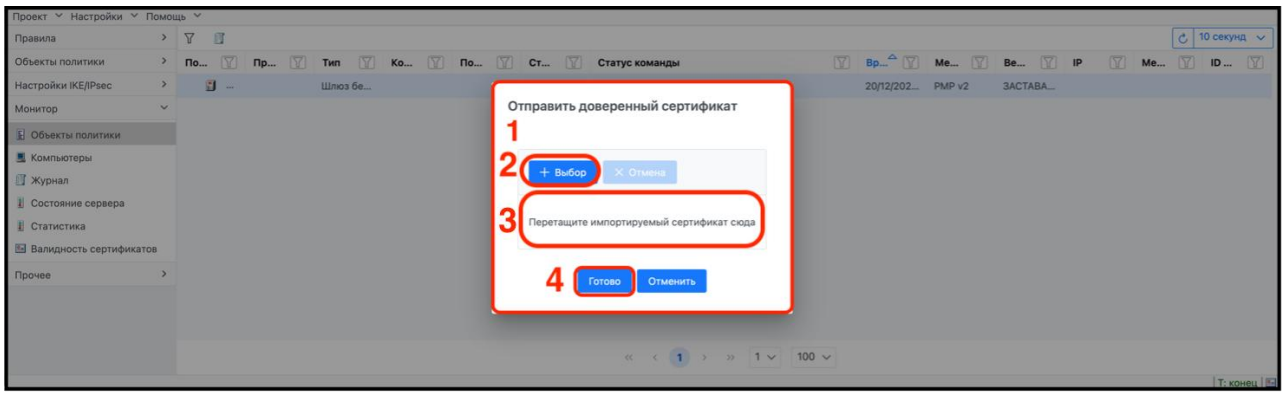


Рисунок 133 – Окно «Отправить доверенный сертификат»

В окне настроек «Отправить доверенный сертификат» (цифра 1) нажать кнопку «+Выбор» (цифра 2), в списке ранее полученных сертификатов выбрать требуемый, либо переместить файл в область «Перетащите импортируемый сертификат сюда» (цифра 3). Нажать кнопку «Готово» (цифра 4).

6.4.1.1.11 Команда контекстного меню «Интеграции»

В контекстном меню выбрать команду «Интеграции», в выпадающем списке интеграций выбрать требуемую интеграцию и открыть ее в окне текстового редактора.

6.4.1.1.12 Команда контекстного меню «Показать в логе»

В контекстном меню выбрать команду «Показать в логе», в результате откроется окно журнала, представленное на рисунке (см. Рисунок 134).

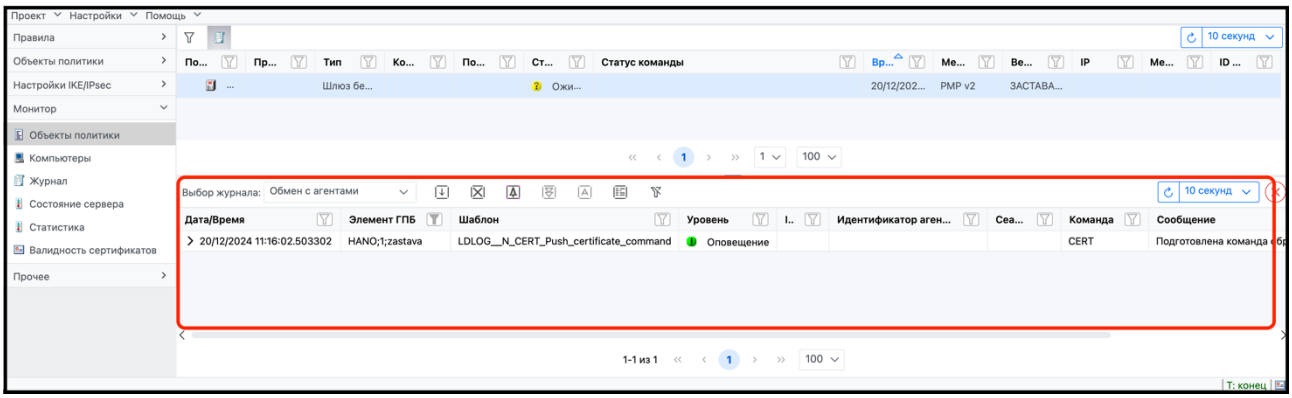


Рисунок 134 – Окно «Показать в логе»

6.4.2 Компьютеры

Элемент списка «Компьютеры» отображает информацию обо всех СВТ, хотя бы единожды получивших политику в топологии. Окно элемента списка «Компьютеры» изображено на рисунке (см. Рисунок 135).

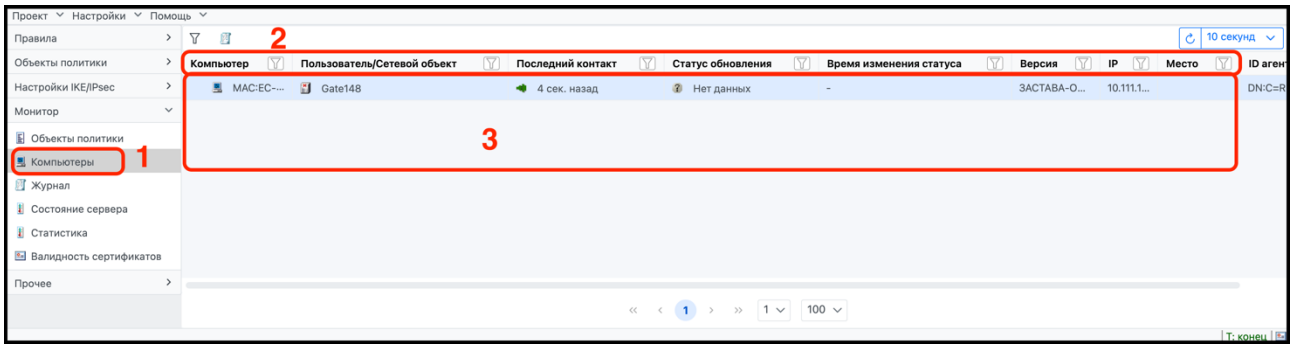


Рисунок 135 – Элемент списка «Компьютеры»

В окне элемента списка «Компьютеры» (цифра 1) будет отображен список компьютеров (цифра 3) в виде таблицы, которая содержит следующие параметры (цифра 2):

— «Компьютер»;
— «Пользователь/Сетевой объект»;
— «Последний контакт»;
— «Статус обновления»;
— «Время изменения статуса»;
— «Версия»;
— «IP»;
— «Место»;
— «ID агента».

6.4.2.1 Контекстное меню элемента списка «Компьютеры»

Вызвать контекстное меню можно, нажав правой клавишей мыши на любой объект в списке рабочей области таблицы, затем выбрать требуемую команду. Контекстное меню элемента списка «Компьютеры» для добавления или редактирования представлено на рисунке (см. Рисунок 136).

Рисунок 136 – Контекстное меню «Компьютеры»

В блоке (цифра 1) контекстного меню отображается команда «Просмотр активной ЛПБ».

В блоке (цифра 2) контекстного меню отображается список команд: «Установить обновления для агента», «Загрузить обновления для агента»; «Обновлённые файлы», «Соединения».

В блоке (цифра 3) контекстного меню отображается команда «Забыть».

В блоке (цифра 4) контекстного меню отображается список команд: «Интеграции», «Показать в логе».

6.4.3 Журнал

В ПО ЗУ имеется возможность отслеживания возникающих событий в автоматическом режиме. Элемент списка «Журнал» используется для просмотра зарегистрированных ошибок, предупреждений, событий и информационных сообщений, собранных в процессе работы с ПО ЗУ. Настройка мониторинга осуществляется отдельно для каждого журнала с доступными в нем инструментами. Вид окна элемента вкладки «Журнал» представлен на рисунке (см. Рисунок 137).

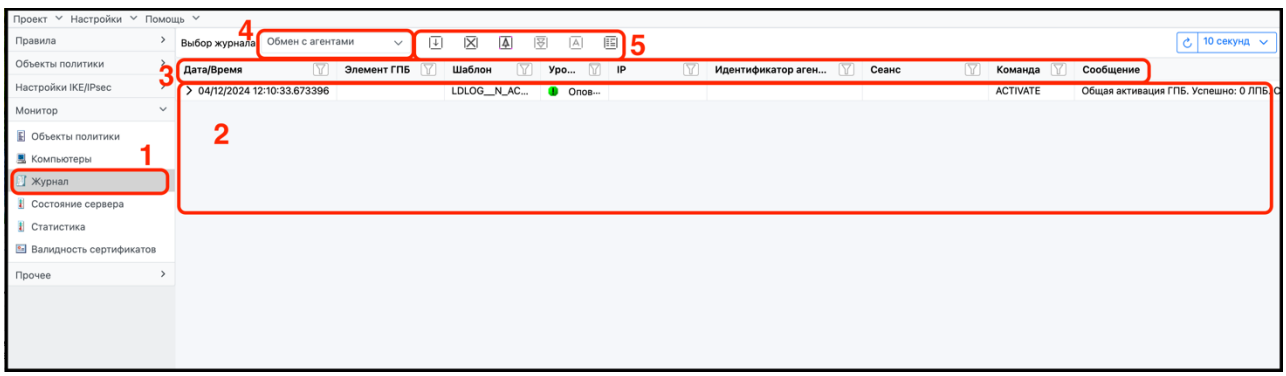


Рисунок 137 – Элемент списка «Журнал»

В окне элемента списка «Журнал» (цифра 1) будет отображен список зарегистрированных событий (цифра 2) в виде таблицы (цифра 3).

Для удобства поиска можно настроить и использовать выпадающие списки фильтрации журналов (цифра 4):

— «Обмен с агентами»;

— «Сторона сервера»;

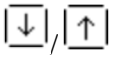
— «Последняя трансляция»;

— «Последний импорт»;

— «Syslog».

Панель инструментов для настройки фильтров выбранного журнала (цифра 5). Описание характеристик инструментов представлено в таблице (см. Таблица 23).

Таблица 23 – Описание панели инструментов элемента списка «Журнал»

Кнопка	Характеристика
	Сортировать от новых/от старых
	Очистить журнал
	Смотреть срабатывания
	Фильтры записи
	Добавить псевдоним
	Настройки параметров журнала

6.4.3.1 Настройка мониторинга для журнала «Обмен с агентами»

Для настройки работы мониторинга в журнале «Обмен с агентами» необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 138).

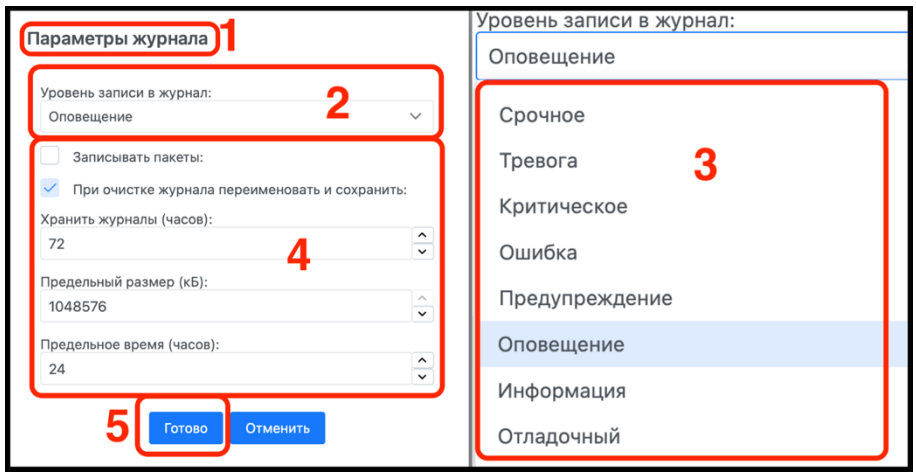


Рисунок 138 – Окно настроек для журнала «Обмен с агентами»

Выбрать в выпадающем списке фильтрации журнал «Обмен с агентами». Открыть диалоговое окно «Параметры журнала» (цифра 1), нажав на панели инструментов элемент «  », и задать требуемые параметры:

1) выбрать уровень записи в журнал. Для этого требуется нажать на элемент « » (цифра 2) и выбрать в выпадающем списке требуемый уровень записи в журнал (цифра 3);
2) настроить параметры в блоке (цифра 4);
3) нажать кнопку «Готово» (цифра 5).

6.4.3.2 Фильтрация в журнале регистрации «Обмен с агентами»

Для фильтрации журнала зарегистрированных событий необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 139).

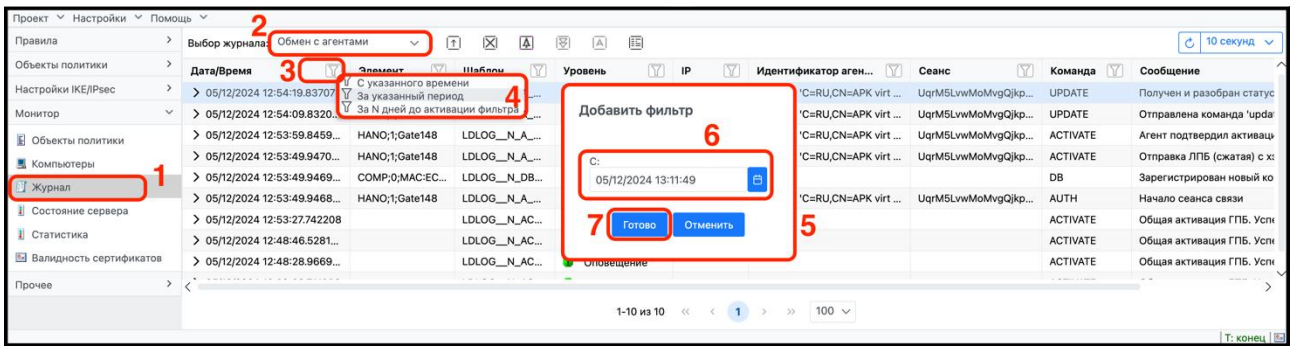


Рисунок 139 – Фильтрация в журнале «Обмен с агентами»

Для получения отфильтрованной информации из журнала «Обмен с агентами» необходимо:

1) в окне элемента списка «Журнал» (цифра 1) выбрать из выпадающего списка требуемый журнал (цифра 2);
2) выбрать параметр фильтрации из колонок таблицы и нажать на его элемент « » (цифра 3);
3) в выпадающем списке фильтра выбрать требуемый подфильтр (цифра 4);
4) настроить в открывшемся окне (цифра 5) (для каждого подфильтра открывается свое окно) требуемые параметры (цифра 6);
5) нажать кнопку «Готово» (цифра 7).

В результате произведенных настроек в рабочей области таблицы отобразится список отфильтрованных объектов, а элемент « » фильтра колонки параметра объектов изменит свой вид на «». Описание доступной фильтрации в журнале «Обмен с агентами» представлено в таблице (см. Таблица 24).

Таблица 24 – Описание доступных фильтров и подфильтров в журнале «Обмен с агентами»

Фильтры	Подфильтры
«Дата/Время»	С указанного времени За указанный период За N дней до активации фильтра

Фильтры	Подфильтры
«Элемент ГПБ»	Для указанных объектов ГПБ Для указанной полной строки
«Шаблон»	Для указанного шаблона сообщения
«Уровень»	По уровню
«IP»	Для указанного IP-адреса
«Идентификатор агента»	Для указанной подстроки Для указанной полной строки
«Сеанс»	Для указанного сеанса
«Команда»	Для указанной строки
«Сообщение»	Для указанной подстроки Для указанной полной строки

6.4.3.3 Настройка мониторинга для журнала «Сторона сервера»

Для настройки работы мониторинга в журнале «Сторона сервера» необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 140).

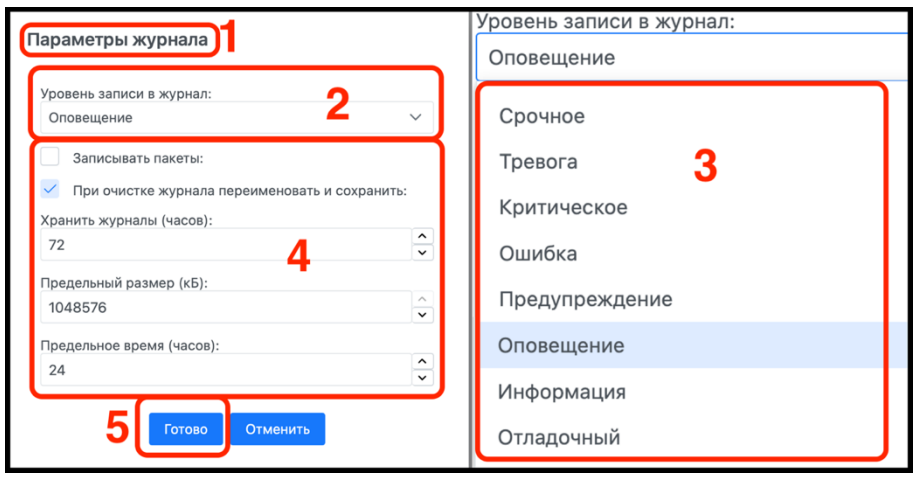


Рисунок 140 – Окно настроек для журнала «Сторона сервера»

Выбрать в выпадающем списке фильтрации журнал «Сторона сервера». Открыть диалоговое окно «Параметры журнала» (цифра 1), нажав на панели инструментов элемент «», и задать требуемые параметры настроек для журнала «Сторона сервера»:

1) выбрать уровень записи в журнал. Для этого требуется нажать на элемент « » (цифра 2) и выбрать в выпадающем списке требуемый уровень записи в журнал (цифра 3);
2) настроить требуемые параметры в блоке (цифра 4);
3) нажать кнопку «Готово» (цифра 5).

6.4.3.4 Фильтрация в журнале регистрации «Сторона сервера»

Для фильтрации журнала зарегистрированных событий необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 141).

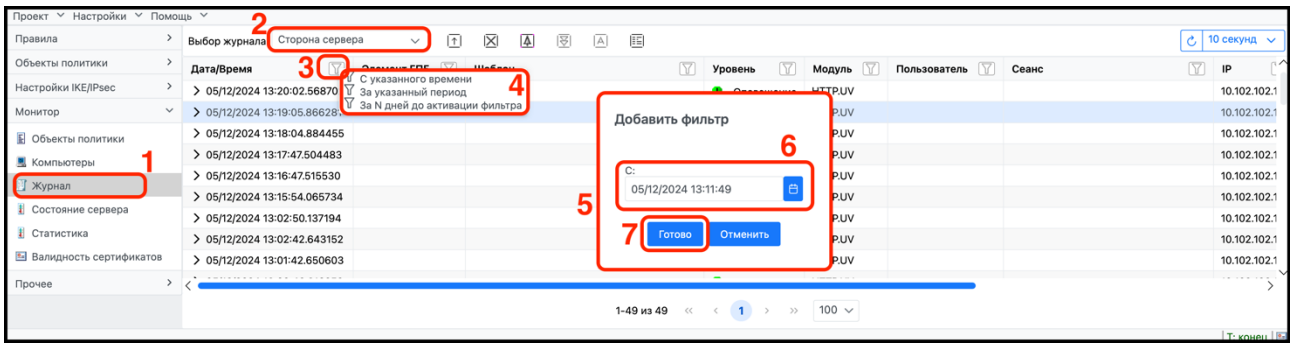


Рисунок 141 – Фильтрация в журнале «Сторона сервера»

Для получения отфильтрованной информации из журнала «Сторона сервера» необходимо:

1) в окне элемента списка «Журнал» (цифра 1) выбрать из выпадающего списка требуемый журнал (цифра 2);
2) выбрать параметр фильтрации из колонок таблицы и нажать на его элемент «» (цифра 3);
3) в выпадающем списке фильтра выбрать (если их несколько) требуемый подфильтр (цифра 4);
4) настроить в открывшемся окне (цифра 5) (для каждого подфильтра открывается свое окно) требуемые параметры (цифра 6);
5) нажать кнопку «Готово» (цифра 7).

В результате произведенных настроек в рабочей области таблицы отобразится список отфильтрованных объектов, а элемент «» фильтра колонки параметра объектов изменит свой вид на «». Описание доступной фильтрации в журнале «Сторона сервера» представлено в таблице (см. Таблица 25).

Таблица 25 – Описание доступных фильтров и подфильтров в журнале «Сторона сервера»

Фильтры	Подфильтры
«Дата/Время»	С указанного времени За указанный период За N дней до активации фильтра
«Элемент ГПБ»	Для указанных объектов ГПБ Для указанной полной строки
«Шаблон»	Для указанного шаблона сообщения
«Уровень»	По уровню
«Модуль»	Для указанной строки

Фильтры	Подфильтры
«Пользователь»	Для указанного учетной записи пользователя ПО ЗУ
«Сеанс»	Для указанного сеанса
«IP»	Для указанного IP-адреса
«Сообщение»	Для указанной подстроки Для указанной полной строки

6.4.3.5 Настройка мониторинга для журнала «Последняя трансляция»

Для настройки работы мониторинга в журнале «Последняя трансляция» необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 142).

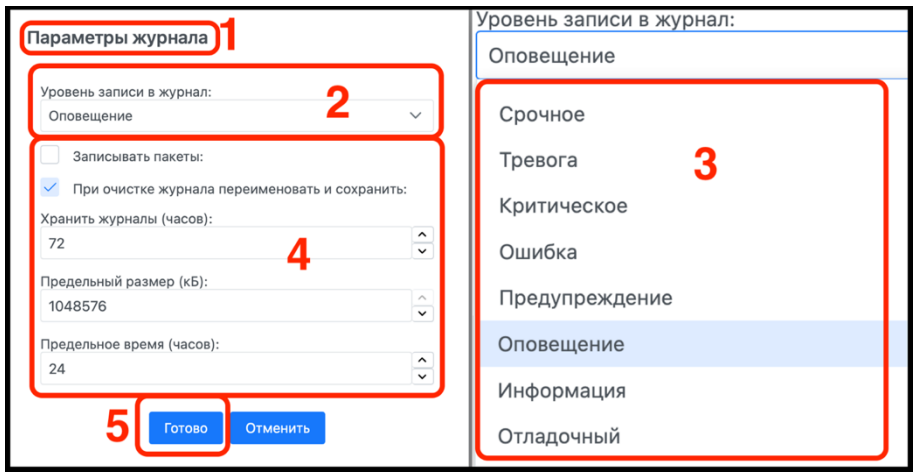


Рисунок 142 – Окно настроек для журнала «Последняя трансляция»

Выбрать в выпадающем списке фильтрации журнал «Последняя трансляция». Открыть диалоговое окно «Параметры журнала» (цифра 1), нажав на панели инструментов элемент «», и задать требуемые параметры настроек для журнала «Последняя трансляция»:

1) выбрать уровень записи в журнал. Для этого требуется нажать на элемент « » (цифра 2) и выбрать в выпадающем списке требуемый уровень записи в журнал (цифра 3);
2) настроить требуемые параметры в блоке (цифра 4);
3) нажать кнопку «Готово» (цифра 5).

6.4.3.6 Фильтрация в журнале регистрации «Последняя трансляция»

Для фильтрации журнала зарегистрированных событий необходимо выполнить шаги, описанные на рисунке (см. Рисунок 143).

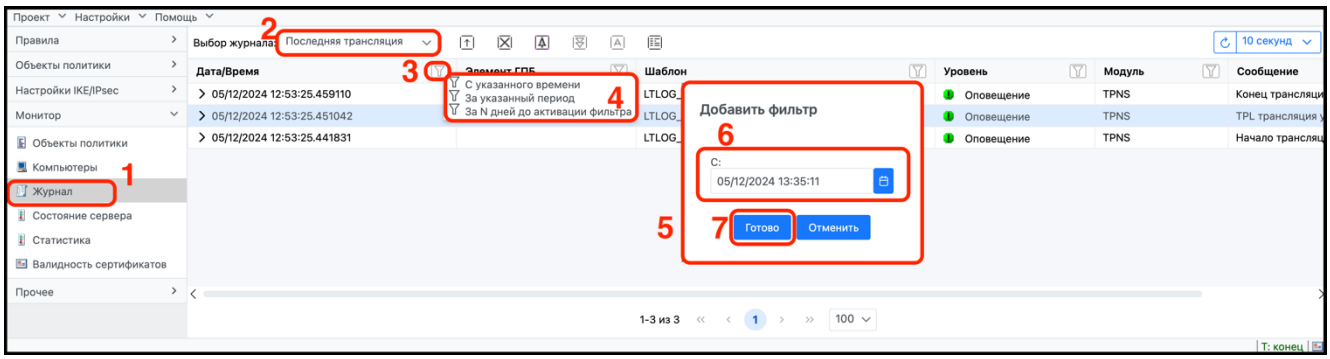


Рисунок 143 – Фильтрация в журнале «Последняя трансляция»

Для получения отфильтрованной информации из журнала «Последняя трансляция» необходимо:

1) в окне элемента списка «Журнал» (цифра 1) выбрать из выпадающего списка требуемый журнал (цифра 2);
2) выбрать параметр фильтрации из колонок таблицы и нажать на его элемент «» (цифра 3);
3) в выпадающем списке фильтра выбрать (если их несколько) требуемый подфильтр (цифра 4);
4) настроить в открывшемся окне (цифра 5) (для каждого подфильтра открывается свое окно) требуемые параметры (цифра 6);
5) нажать кнопку «Готово» (цифра 7).

В результате произведенных настроек в рабочей области таблицы отобразится список отфильтрованных объектов, а элемент «» фильтра колонки параметра объектов изменит свой вид на «». Описание доступной фильтрации в журнале «Последняя трансляция» представлено в таблице (см. Таблица 26).

Таблица 26 – Описание доступной фильтрации и подфильтров в журнале «Последняя трансляция»

Фильтры	Подфильтры
«Дата/Время»	С указанного времени За указанный период За N дней до активации фильтра
«Элемент ГПБ»	Для указанных объектов ГПБ Для указанной полной строки
«Шаблон»	Для указанного шаблона сообщения
«Уровень»	По уровню
«Модуль»	Для указанной строки
«Сообщение»	Для указанной подстроки Для указанной полной строки

6.4.3.7 Настройка мониторинга для журнала «Последний импорт»

Для настройки работы мониторинга в журнале «Последний импорт» необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 144).

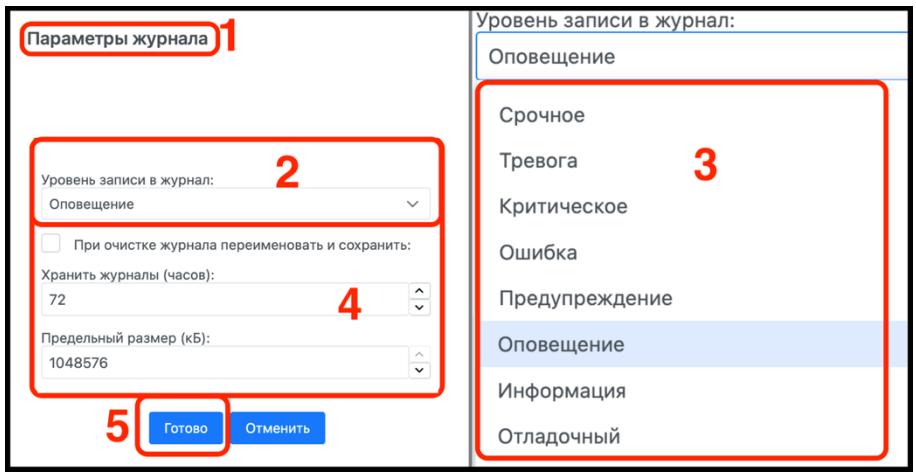


Рисунок 144 – Окно настроек для журнала «Последний импорт»

Выбрать в выпадающем списке фильтрации журнал «Последний импорт». Открыть диалоговое окно «Параметры журнала» (цифра 1), нажав на панели инструментов элемент «», и задать требуемые параметры настроек для журнала «Последний импорт»:

1) выбрать уровень записи в журнал. Для этого требуется нажать на элемент « » (цифра 2) и выбрать в открывшемся выпадающем списке требуемый уровень записи в журнал (цифра 3);
2) настроить требуемые параметры в блоке (цифра 4);
3) нажать кнопку «Готово» (цифра 5).

6.4.3.8 Фильтрация в журнале регистрации «Последний импорт»

Для фильтрации журнала зарегистрированных событий необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 143).

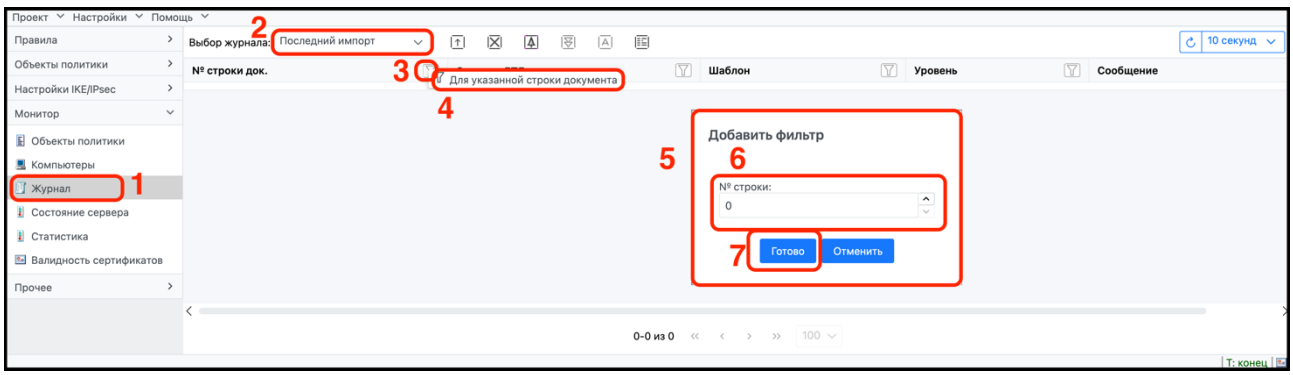


Рисунок 145 – Фильтрация в журнале «Последний импорт»

Для получения отфильтрованной информации из журнала «Последний импорт» необходимо:

1) в окне элемента списка «Журнал» (цифра 1) выбрать из выпадающего списка требуемый журнал (цифра 2);
2) выбрать параметр фильтрации из колонок таблицы и нажать на его элемент «» (цифра 3);
3) в выпадающем списке фильтра выбрать (если их несколько) требуемый подфильтр (цифра 4);
4) настроить в открывшемся окне (цифра 5) (для каждого подфильтра открывается свое окно) требуемые параметры (цифра 6);
5) нажать кнопку «Готово» (цифра 7).

В результате произведенных настроек в рабочей области таблицы отобразится список отфильтрованных объектов, а элемент «» фильтра колонки параметра объектов изменит свой вид на «». Описание доступной фильтрации в журнале «Последний импорт» представлено в таблице (см. Таблица 27).

Таблица 27 – Описание доступной фильтрации и подфильтров в журнале «Последний импорт»

Фильтры	**Подфильтры**
«№ строки док.»	Для указанной строки документа
«Элемент ГПБ»	Для указанных объектов ГПБ Для указанной полной строки
«Шаблон»	Для указанного шаблона сообщения
«Уровень»	По уровню
«Сообщение»	Для указанной подстроки Для указанной полной строки

6.4.3.9 Настройка мониторинга для Журнала «Syslog»

Процедура работы с настройками для журнала «Syslog» состоит из этапов:

— добавления фильтра;
— создания псевдонима;
— настройки параметров журнала.

Для добавления фильтра «Syslog» необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 146).

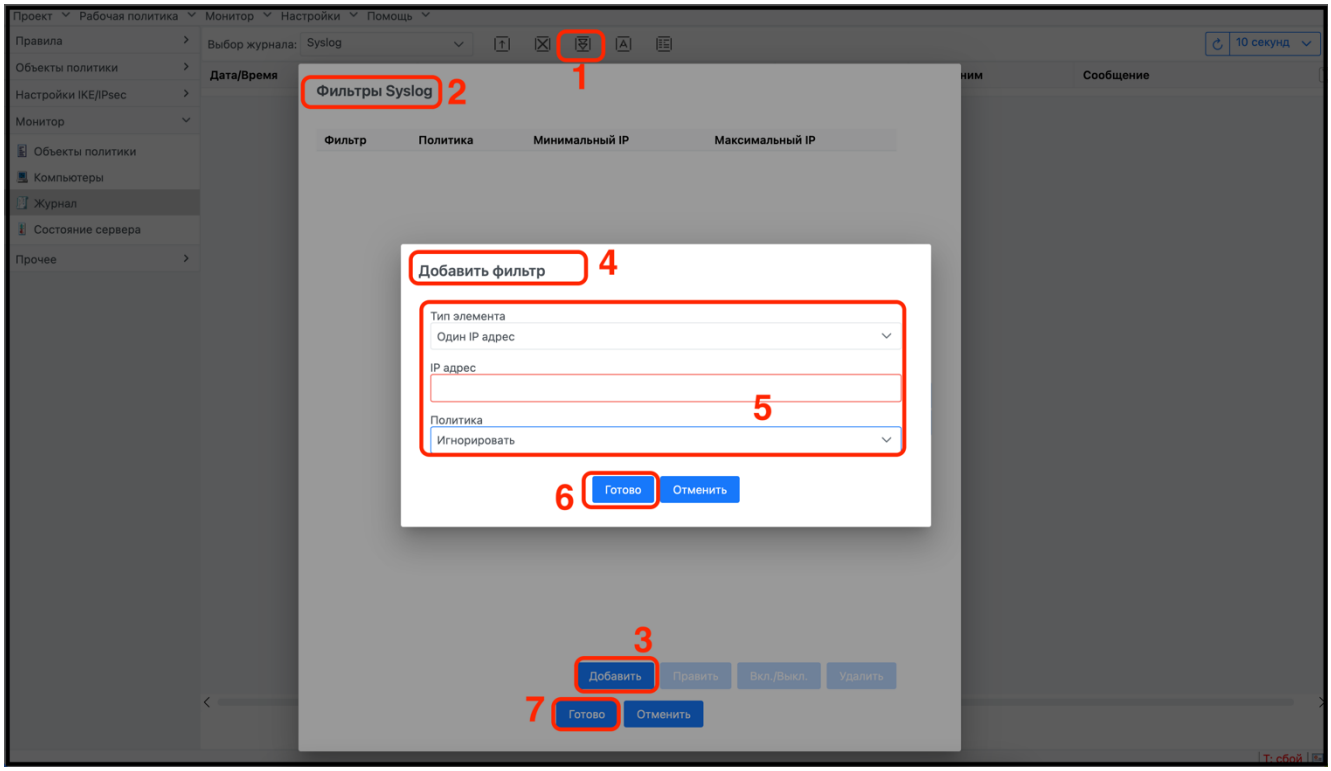


Рисунок 146 – Окно настроек «Фильтры Syslog»

Выбрать в выпадающем списке фильтрации журнал «Syslog». Нажать на панели инструментов элемент «» (цифра 1). В открывшемся диалоговом окне «Фильтры Syslog» (цифра 2) нажать кнопку «Добавить» (цифра 3). Ввести в блоке настроек «Добавить фильтр» (цифра 4) требуемые параметры (цифра 5), нажать кнопку «Готово» (цифра 6). Нажать кнопку «Готово» (цифра 7) в окне «Фильтры Syslog».

При необходимости добавления псевдонима «Syslog» необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 147).

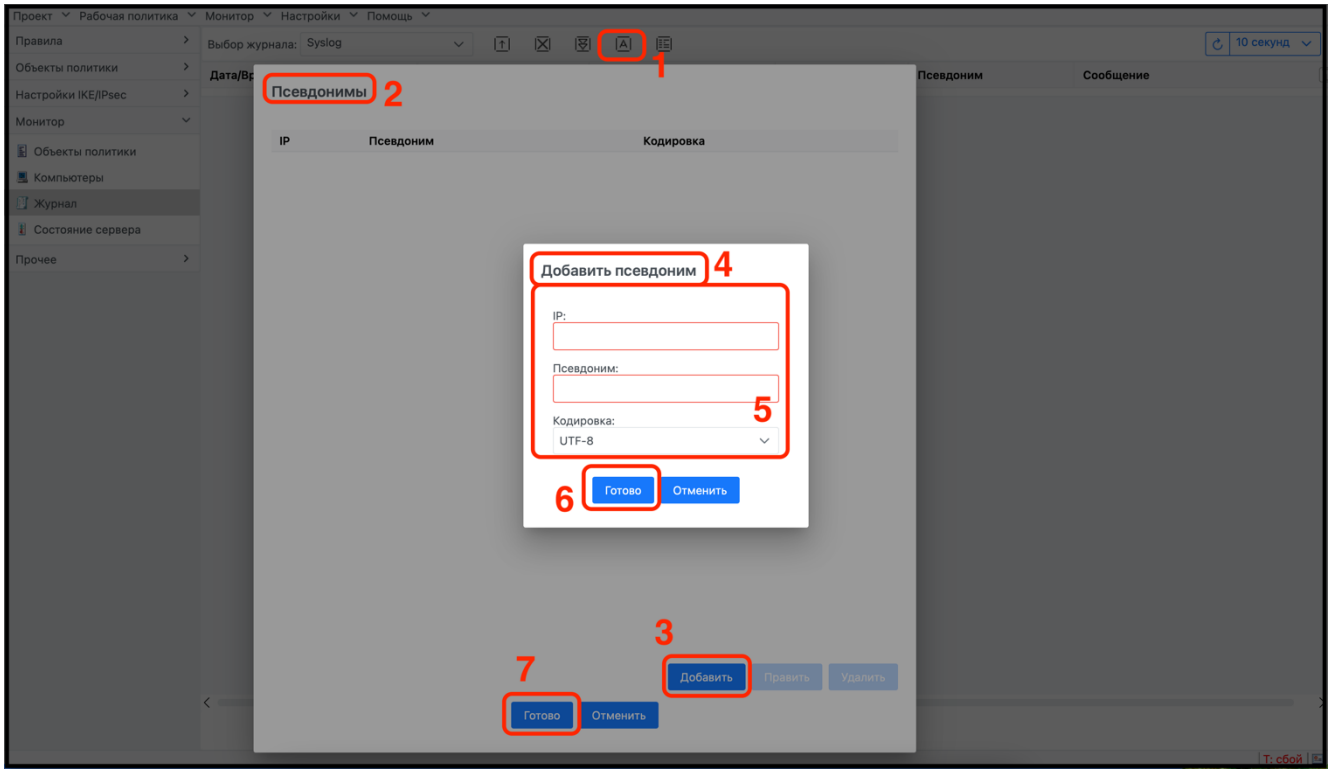


Рисунок 147 – Окно настроек «Псевдоним»

Нажать на панели инструментов элемент «  » (цифра 1). В открывшемся диалоговом окне «Псевдонимы» (цифра 2) нажать кнопку «Добавить» (цифра 3). Ввести в блоке настроек «Добавить псевдоним» (цифра 4) требуемые параметры (цифра 5). 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 сохраняются. 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». Нажать кнопку «Готово» (цифра 6). Нажать кнопку «Готово» (цифра 7) в окне «Псевдонимы».

Для настройки работы мониторинга в журнале «Последний импорт» необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 148).

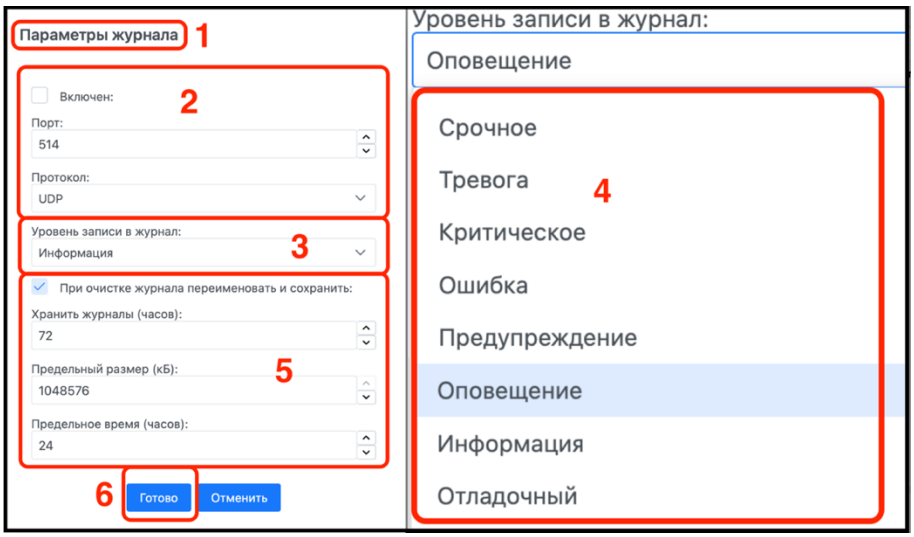


Рисунок 148 – Окно настроек для журнала «Syslog»

Открыть диалоговое окно «Параметры журнала» (цифра 1), нажав на панели инструментов элемент «», и задать требуемые параметры настроек для журнала «Syslog»:

1) в настроечном блоке (цифра 2) установить флажок напротив строки «Включен», выбрать требуемый порт. В выпадающем списке, используя элемент « », выбрать требуемый протокол;
2) выбрать уровень записи в журнал. Для этого требуется нажать на элемент « » (цифра 2) и выбрать в выпадающем списке требуемый уровень записи в журнал (цифра 3);
3) выбрать требуемые параметры в открывшемся блоке (цифра 4);
4) в настроечном блоке (цифра 5) при очистке журнала переименовать и сохранить параметры (флажок установлен по умолчанию):

— количество часов хранения журнала;
— предельный размер (кБ);
— предельное время часов.

5) нажать кнопку «Готово» (цифра 6).

6.4.3.10 Фильтрация результатов в журнале регистрации «Syslog»

Для фильтрации журнала зарегистрированных событий необходимо выполнить шаги, описанные на рисунке (см. Рисунок 149).

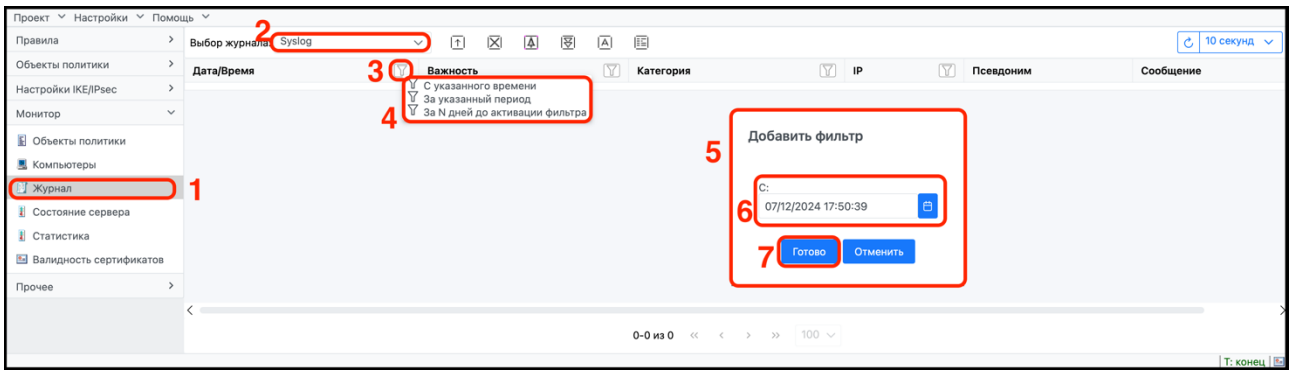


Рисунок 149 – Фильтрация в журнале «Syslog»

Для получения отфильтрованной информации из журнала «Syslog» необходимо:

1) в окне элемента списка «Журнал» (цифра 1) выбрать из выпадающего списка требуемый журнал (цифра 2);
2) выбрать параметр фильтрации из колонок таблицы и нажать на его элемент «» (цифра 3);
3) в выпадающем списке фильтра выбрать (если их несколько) требуемый подфильтр (цифра 4);
4) настроить в открывшемся окне (цифра 5) (для каждого подфильтра открывается свое окно) требуемые параметры (цифра 6);
5) нажать кнопку «Готово» (цифра 7).

В результате произведенных настроек в рабочей области таблицы отобразится список отфильтрованных объектов, а элемент «» фильтра колонки параметра объектов изменит свой вид на «». Описание доступной фильтрации в журнале «Syslog» представлены в таблице (см. Таблица 28).

Таблица 28 – Описание доступной фильтрации и подфильтров в журнале «Syslog»

Фильтры	**Подфильтры**
«Дата/Время»	С указанного времени За указанный период За N дней до активации фильтра
«Важность»	По уровню
«Категория»	По категории
«IP»	Для указанного IP-адреса
«Псевдоним»	Для псевдонима
«Сообщение»	Для указанной подстроки Для указанной полной строки

6.4.3.11 Настройка и просмотр срабатываний журнала

Посмотреть срабатывание журнала можно, выполнив шаги, изображенные на рисунке (см. Рисунок 150).

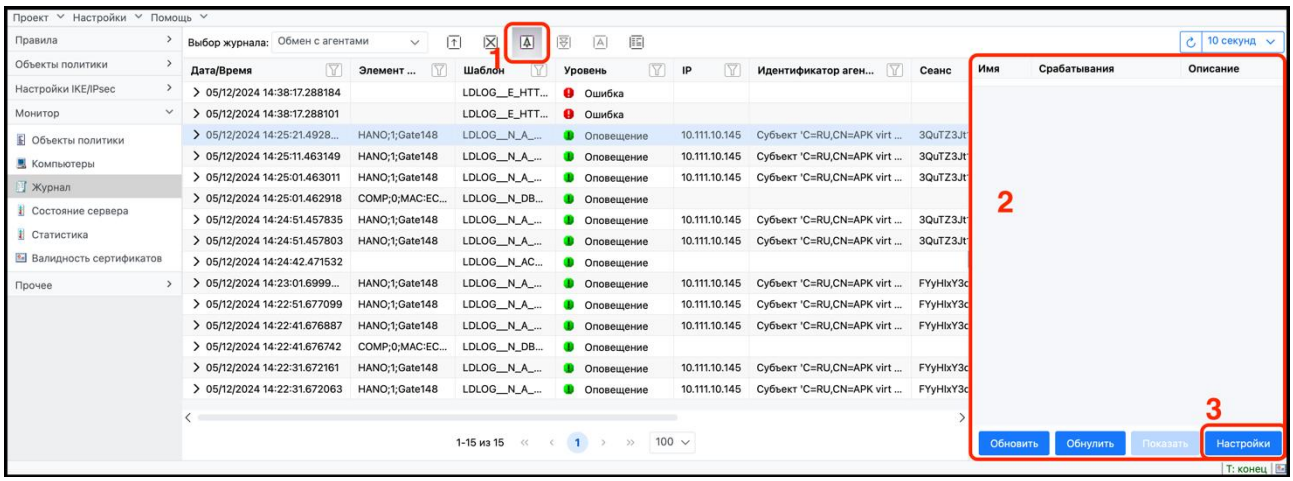


Рисунок 150 – Инструмент «Срабатывание журнала»

Для просмотра срабатываний журнала необходимо нажать на панели инструментов элемент «» (цифра 1). Справа откроется окно просмотра срабатываний журнала (цифра 2). Перейти к настройкам срабатываний, нажав кнопку «Настройки» (цифра 3). В результате откроется окно «Список индикаторов», представленное на рисунке (см. Рисунок 151), в котором необходимо нажать кнопку «Добавить».

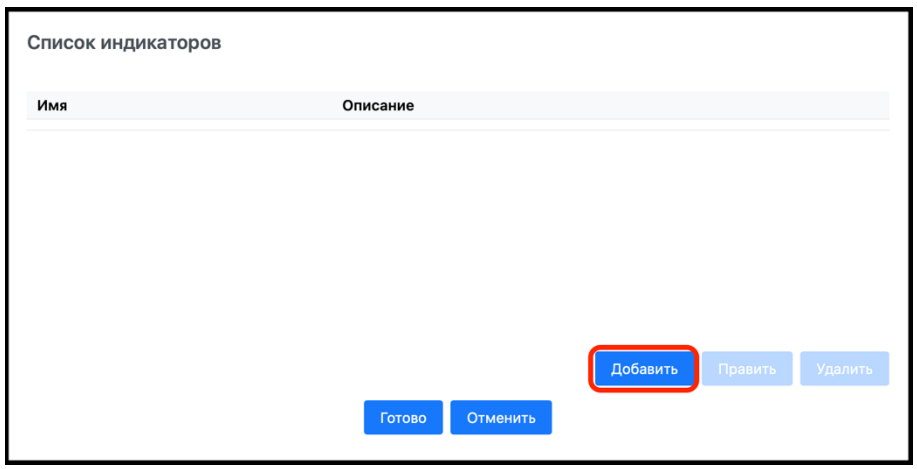


Рисунок 151 – Окно «Список индикаторов»

Для добавления индикаторов необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 152).

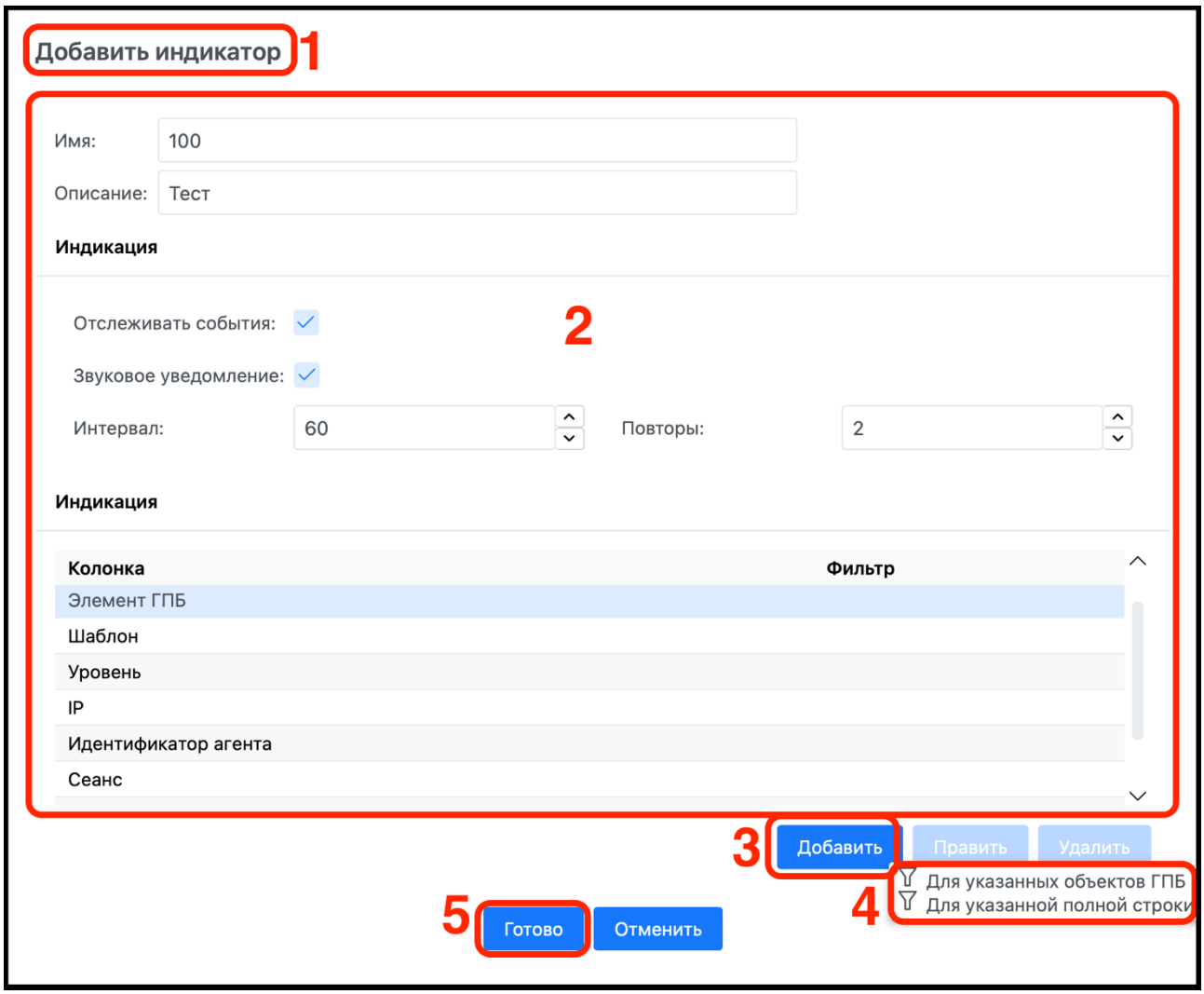


Рисунок 152 – Окно «Добавить индикатор»

В открывшемся окне настроек «Добавить индикатор» (цифра 1) выполнить необходимые настройки (цифра 2), нажать кнопку «Добавить» (цифра 3), выбрать в выпадающем списке требуемый подфильтр (цифра 4), нажать кнопку «Готово» (цифра 5).

6.4.4 Состояние сервера

Посмотреть состояние сервера можно в элементе списка «Состояние сервера», представленном на рисунке (см. Рисунок 153).

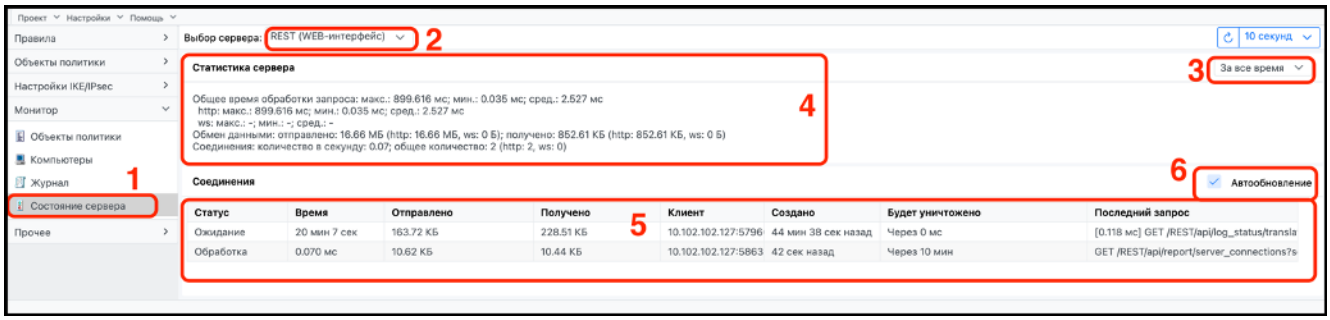


Рисунок 153 – Элемент списка «Состояние сервера»

Для просмотра состояния сервера необходимо в окне элемента списка «Состояние сервера» (цифра 1) выбрать из выпадающего списка требуемый сервер (цифра 2). Установить интересующий временной диапазон (цифра 3). В результате в блоке «Статистика сервера» (цифра 4) отобразится вся информация о состоянии сервера. В рабочей области таблицы параметров (цифра 5) будет отображен список параметров по выбранному серверу. При необходимости автообновления информации по состоянию сервера установить флажок (цифра 6).

6.4.5 Статистика

Посмотреть статистику можно в элементе списка «Статистика», представленном на рисунке (см. Рисунок 153).

Рисунок 154 – Окно «Статистика»

В окне элемента списка «Статистика» будет отображаться состояние (цифра 2) и количество (цифра 3) объектов.

6.4.6 Валидность сертификатов

Элемент списка «Валидность сертификатов» используется для отслеживания сертификатов с истёкшим или истекающим в ближайшее время сроком действия у объектов активной ГПБ. Вид окна «Валидность сертификатов» представлен на рисунке (см. Рисунок 155).

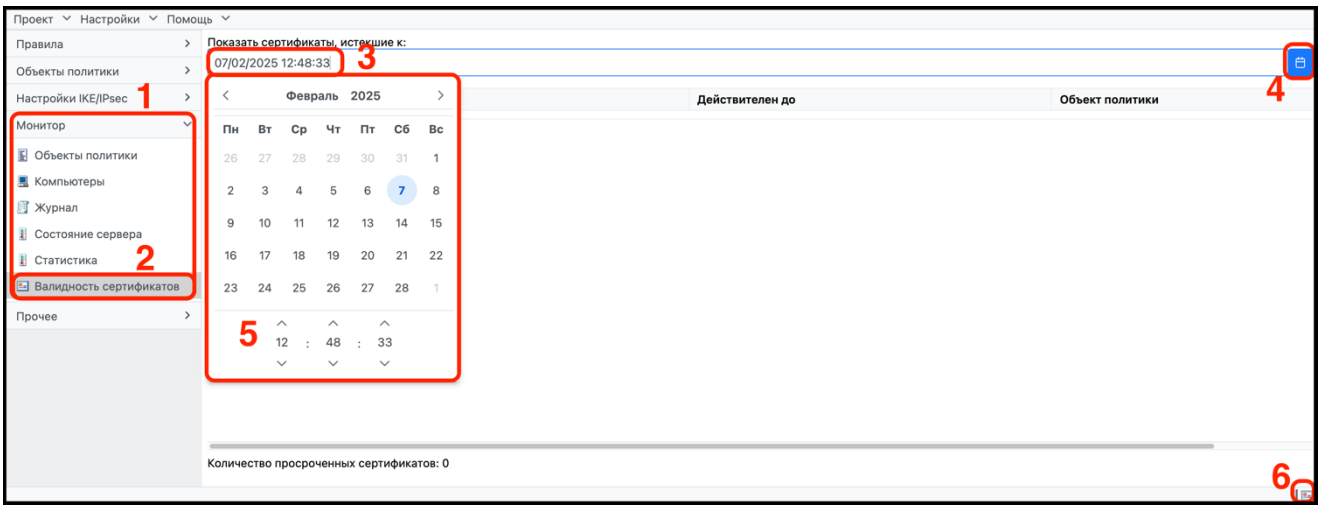


Рисунок 155 – Окно «Валидность сертификатов»

Во вкладке боковой панели «Монитор» (цифра 1) в окне элемента списка «Валидность сертификатов» (цифра 2) в рабочей области таблицы будут отображаться сертификаты с истёкшим или истекающим в ближайшее время сроком действия. Настроить контроль времени действительности сертификата можно, выбрав требуемый сертификат в списке, далее перейти в строку (цифра 3) или нажать левой клавишей мыши на элемент «» (цифра 4) и в открывшемся календаре назначить контрольное время (цифра 5).

ПО ЗУ автоматически отслеживает сертификаты с истёкшим сроком действия при включенной функции слежения «Проверять просроченные сертификаты». В случае обнаружения таких сертификатов в строке статуса основного окна ПО ЗУ появляется мигающая пиктограмма «» (цифра 6). Нажатие на эту пиктограмму открывает окно со списком сертификатов с истёкшим или истекающим сроком действия. Пиктограмма мигает до тех пор, пока окно «Валидность сертификатов» не будет закрыто. Перейти в окно валидности сертификатов можно из других директорий, используя пиктограмму « ».

6.5 Вкладка боковой панели «Прочее»

Окно вкладки боковой панели «Прочее» представлено на рисунке (см. Рисунок 156).

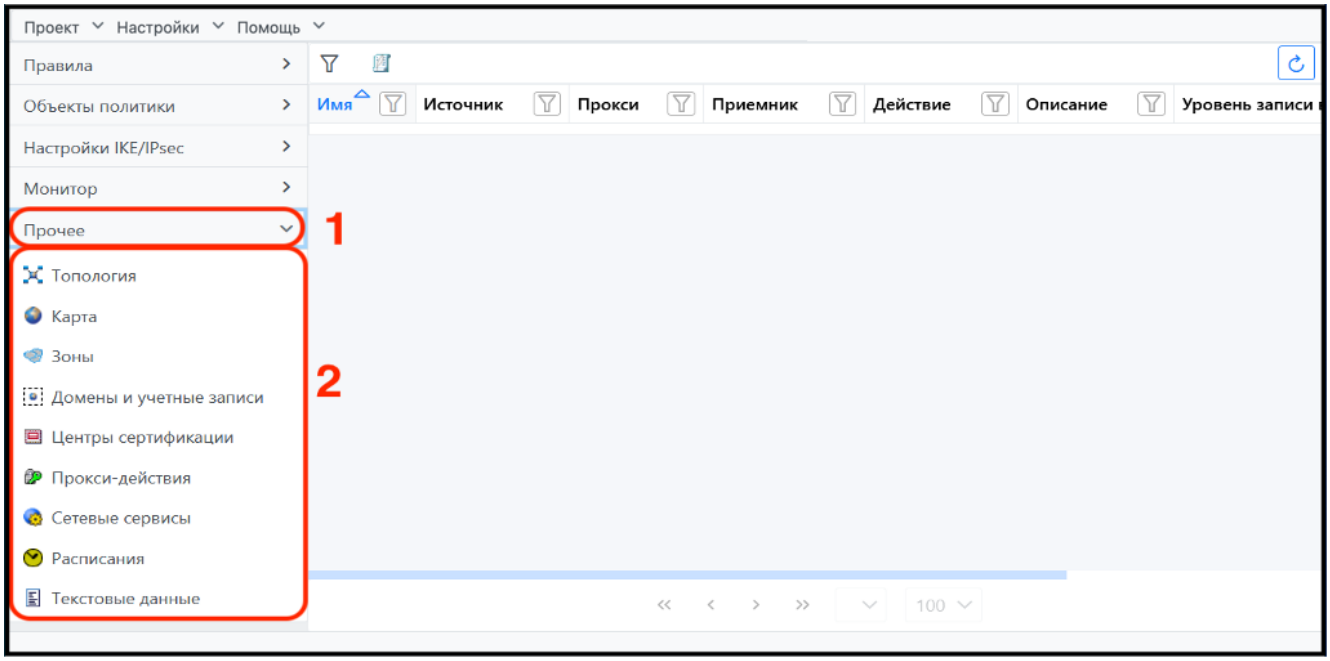


Рисунок 156 – Вкладка «Прочее»

Окно вкладки боковой панели «Прочее» (цифра 1) содержит следующие элементы списка (цифра 2):

— «Топология»;
— «Карты»;
— «Зоны»;
— «Домены и учетные записи»;
— «Центры сертификации»;
— «Прокси-действия»;
— «Сетевые сервисы»;
— «Расписания»;
— «Текстовые данные».

6.5.1 Топология

Элемент списка «Топология» предназначен для представления топологии сети в графическом виде, где отображаются объекты политики с известными IP-адресами, а также вспомогательные узлы защищённой сети предприятия, созданные в ПО ЗУ в виде пиктограмм.

Объекты в окне топологии соединены линиями между адресными пространствами сетевых объектов и объектов типа «Зона», указывающих на связи объектов друг с другом. Эти линии создаются автоматически на основе данных, которые содержатся в свойствах объектов.

Связь задается при описании топологии объекта в соответствии с интерфейсами объекта. Если у объекта несколько интерфейсов, то он может соединяться с несколькими зонами

одновременно. Если у объекта сети несколько интерфейсов, чьи IP-адреса принадлежат одной зоне, связь в окне «Топология» будет представлена одной линией.

При первом запуске веб-интерфейса ПО ЗУ в окне элемента списка «Топология» будут отображаться автоматически созданные три объекта:

— «Зона Интернет»;
— объект, соответствующий ПО ЗУ, которым осуществляется управление. Название будет соответствовать имени СВТ с установленным ПО ЗУ. Сертификат безопасности создастся автоматически, является технологическим, самоподписанным и не должен использоваться при построении защищенных соединений;
— объект «Зона» (облако серого цвета) создается автоматически и служит для отображения логической связи между объектами топологии соответствующей сети, которой принадлежит IP-адрес сетевого интерфейса ПО ЗУ.

Вид окна при первом запуске элемента списка «Топология» представлен на рисунке (см. Рисунок 157).

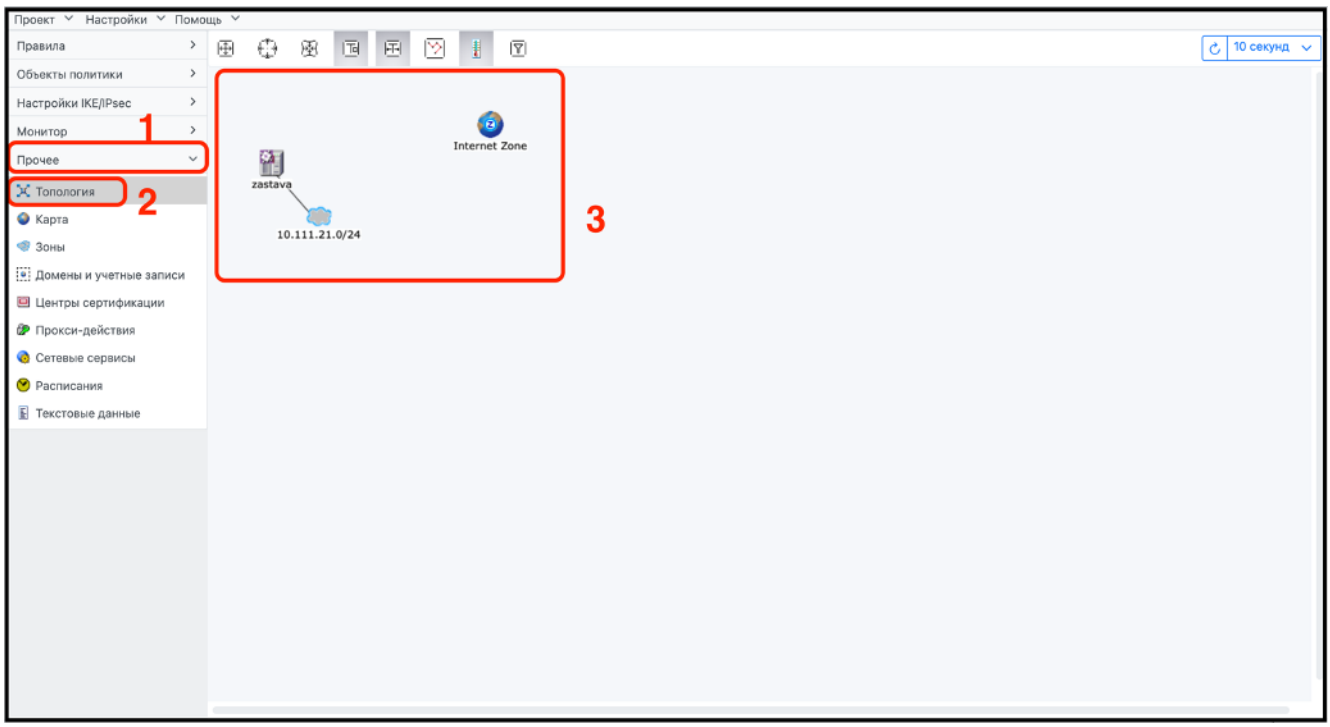


Рисунок 157 – Вкладка «Прочее», начало работы

В вкладке боковой панели «Прочее» (цифра 1) выбрать элемент списка «Топология» (цифра 2). Автоматически созданные при первом запуске три объекта (цифра 3).

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 «Зона Интернет».

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 одной линией, как представлено на рисунке (см. Рисунок 158).

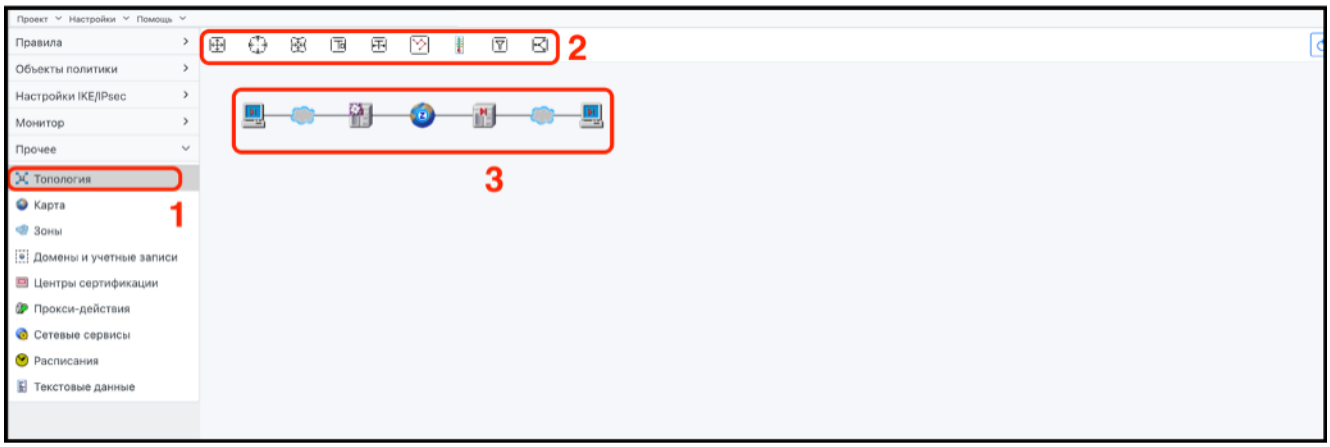


Рисунок 158 – Окно элемент списка «Топология»

В окне «Топология» (цифра 1) доступна своя панель инструментов (цифра 2). Описание панели инструментов представлено в таблице (см. Таблица 29). Все объекты политики, созданные в данном проекте (за исключением пользователей (агент «ЗАСТАВА-Клиент») и групп), будут отображаться в рабочей области элемента списка «Топология» (цифра 3).

Таблица 29 – Описание доступных инструментов окна «Топология»

Кнопка	Характеристика
	Уместить в окно
	Уменьшить масштаб
	Увеличить масштаб
	Показать имена объектов
	Скрыть все кроме маршрута
	Фильтр
	Показывать статус
	Показать надписи для связей

Кнопка	Характеристика
	Варианты расстановки (Автоматическая расстановка, Круговая расстановка, Оптимальная расстановка, Циркулирующая расстановка, Эффективная расстановка)

В окне «Топология» будут отображаются не все объекты. Перечень отображаемых объектов:

— Шлюзы безопасности;
— Хосты безопасности;
— IP хосты;
— Подсети;
— IP диапазоны;
— Зоны.

Перечень неотображаемых объектов:

— Пользователи (агенты «ЗАСТАВА-Клиент»);
— Группы;
— Группы компьютеров;
— Серверы.

6.5.1.1 Работа с контекстным меню элемента списка «Топология»

Вызвать контекстное меню, можно нажав правой клавишей мыши на любой объект или на свободное место в рабочей области окна топологии, затем выбрать требуемую команду. Окно с вызванными разным способом контекстными меню элемента списка «Топология» представлено на рисунке (см. Рисунок 159).

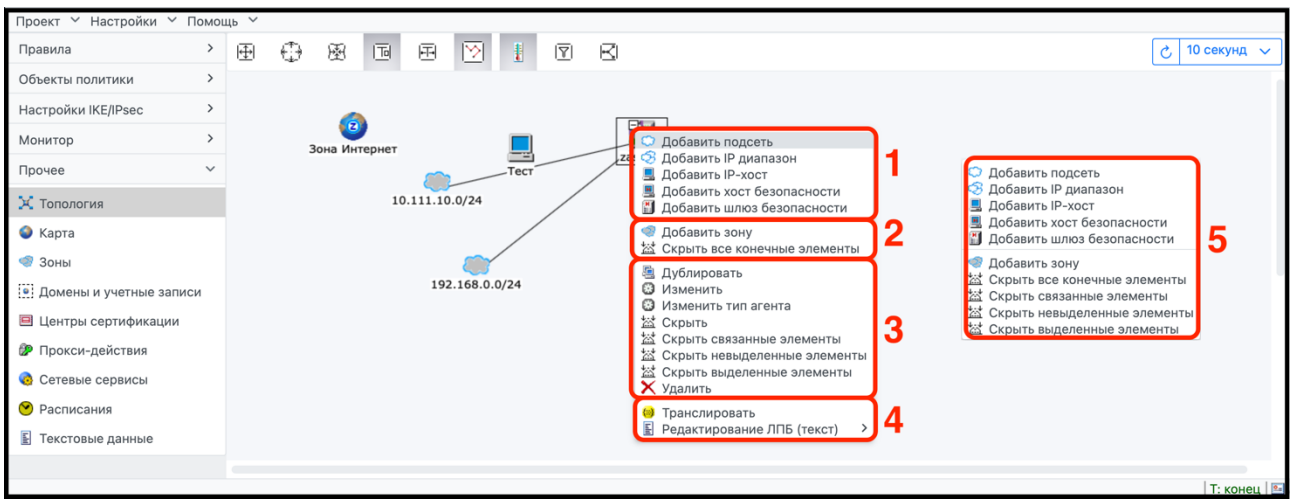


Рисунок 159 – Контекстное меню «Объекты политики»

На рисунке изображены блоки команд, вызываемые при нажатии правой клавишей мыши по выбранному объекту:

— в блоке (цифра 1) контекстного меню отображается список команд для добавления объектов политики. Добавление объектов политики подробно описано в разделе 7;

— в блоке (цифра 2) контекстного меню отображается список команд: «Добавить зону» и «Скрыть все конечные элементы»;

— в блоке (цифра 3) контекстного меню отображается список команд для редактирования объектов: «Дублировать», «Изменить», «Изменить тип агента», «Удалить» и команды для управления видом топологии «Скрыть» «Скрыть связанные элементы», «Скрыть невыделенные элементы», «Скрыть выделенные элементы»;

— команды для запуска трансляции и редактирования текста ЛПБ отображаются в блоке (цифра 4). В выпадающем списке отобразится статус ЛПБ с переходом в текстовый редактор.

Блок команд контекстного меню, вызываемый при нажатии правой клавишей мыши по свободному месту рабочей области таблицы (цифра 5).

6.5.2 Карта

Элемент списка «Карта» используется для отображения расположения объектов политики на карте земного шара с учетом их географических координат. Вид окна элемента списка «Карта» представлен на рисунке (см. Рисунок 160).

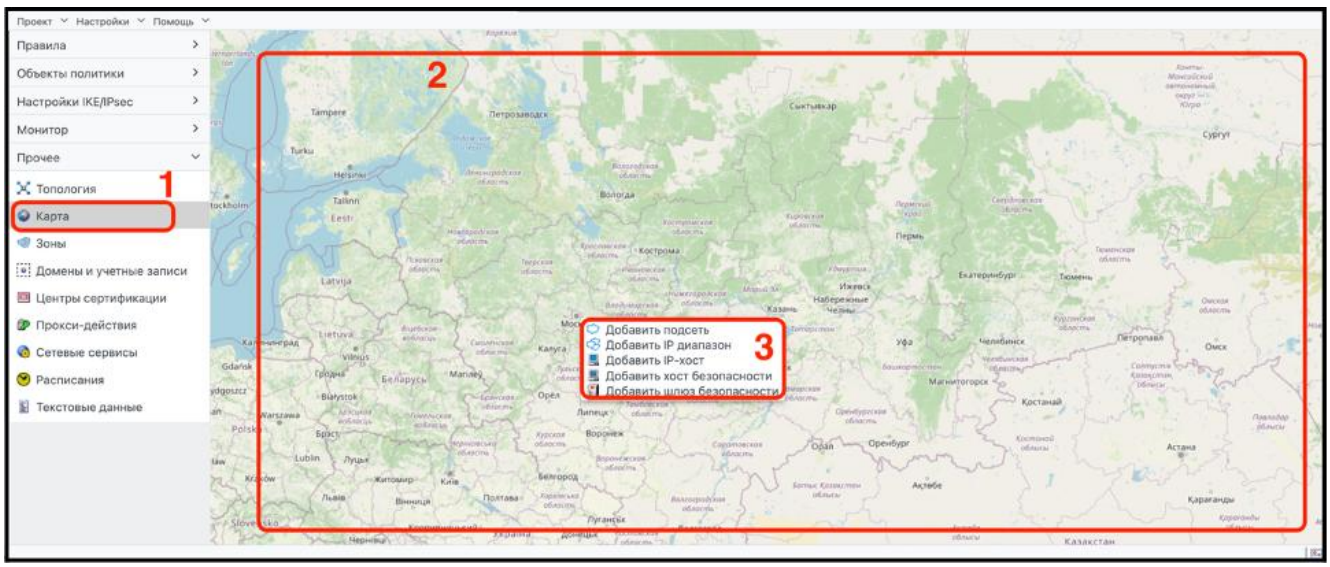


Рисунок 160 – Элемент списка «Карта»

В окне элемента списка «Карта» (цифра 1) отображается географическая карта местности (цифра 2), на которой, при наличии соответствующих настроек, будут отображены объекты ГПБ.

Для элемента списка «Карта» доступно свое контекстное меню (цифра 3), в котором отображается список команд для добавления объектов политики. Добавление объектов политики подробно описано в разделе 7.

6.5.3 Зоны

Зона – это пространство IP-адресов, защищаемое шлюзом безопасности. ПО ЗУ использует зоны для того, чтобы проводить трассировку топологии во время трансляции ГПБ, а также, чтобы определять, какие диапазоны IP-адресов защищены каждым шлюзом безопасности. 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.

Зоны могут быть созданы только в топологии, они не являются объектами политики. Входящий трафик для любого из агентов зоны будет 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.

Вид окна элемента списка «Зоны» отображен на рисунке (см. Рисунок 161).

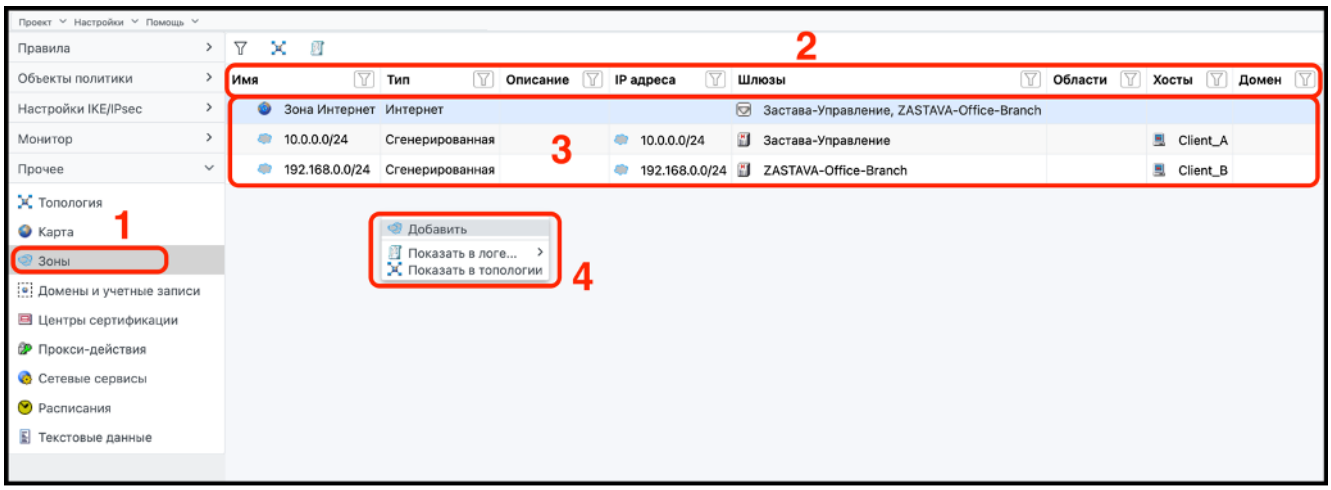


Рисунок 161 – Элемент списка «Зоны»

В окне элемента списка «Зоны» (цифра 1) отобразится информация о параметрах каждой зоне в виде таблицы (цифра 2):

— «Имя»;
— «Тип»;
— «Описание»;
— «IP-адреса»;
— «Шлюзы»;
— «Области» (сети и диапазоны IP-адресов);
— «Хосты»;

— «Домен».

По каждому параметру возможна сортировка. В рабочей области таблицы будет отображаться список зон (цифра 3).

Для элемента списка «Зоны» доступно свое контекстное меню (цифра 4), в котором отображается список команд.

6.5.4 Домены и учетные записи

В ПО ЗУ предусмотрена доменная модель (в рамках ПО ЗУ, не относится к Active Directory). Эта модель реализует разграничение прав доступа к ПО ЗУ по принципу авторизации.

Домены образуют иерархический список, по умолчанию в ГПБ создается домен[6)] с именем «Глобальный». Каждый домен связан с набором учетных записей. При входе в ПО ЗУ пользователь указывает имя учетной записи и ее пароль. В случае успешной аутентификации учетная запись, данные которой вводил пользователь, становится текущей. Домен, который связан с текущей учетной записью, также становится текущим доменом. Окно элемента списка «Домены и учетные записи» представлено на рисунке (см. Рисунок 162).

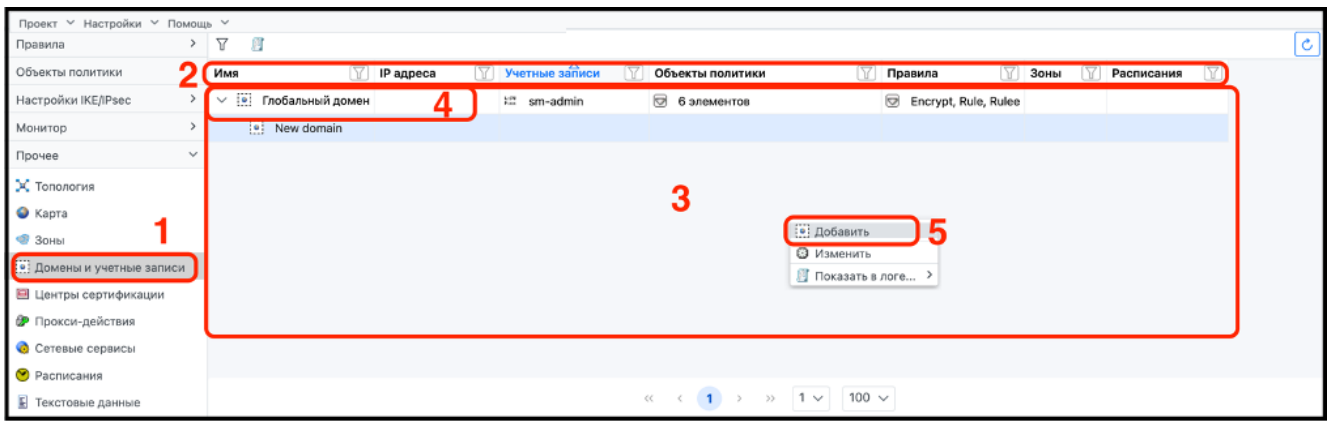


Рисунок 162 – Элемент списка «Домены и учетные записи»

В окне элемента списка «Домены и учетные записи» (цифра 1) отображаются параметры существующих доменов в виде таблицы (цифра 2):

— «Имя»;
— «IP-адреса»;
— «Учетные записи»;
— «Объекты политики»
— «Правила»;
— «Зоны»;

---

6) Глобальный домен невозможно удалить. Невозможно удалить домен, которому принадлежат объекты политики.

— «Расписания».

В рабочей области таблицы отобразится иерархический список доменов (цифра 3) с глобальным доменом (цифра 4).

Для элемента списка «Домены и учетные записи» доступно свое контекстное меню, в котором отображается список команд. Для добавления домена необходимо правой клавишей мыши нажать на свободное место в рабочей области таблицы. В открывшемся контекстном меню и выбрать команду «Добавить» (цифра 5). В открывшемся окне перейти к настройке параметров нового домена.

6.5.4.1 Добавление и настройка параметров домена

Окно «Добавить домен» представлено на рисунке (см. Рисунок 163).

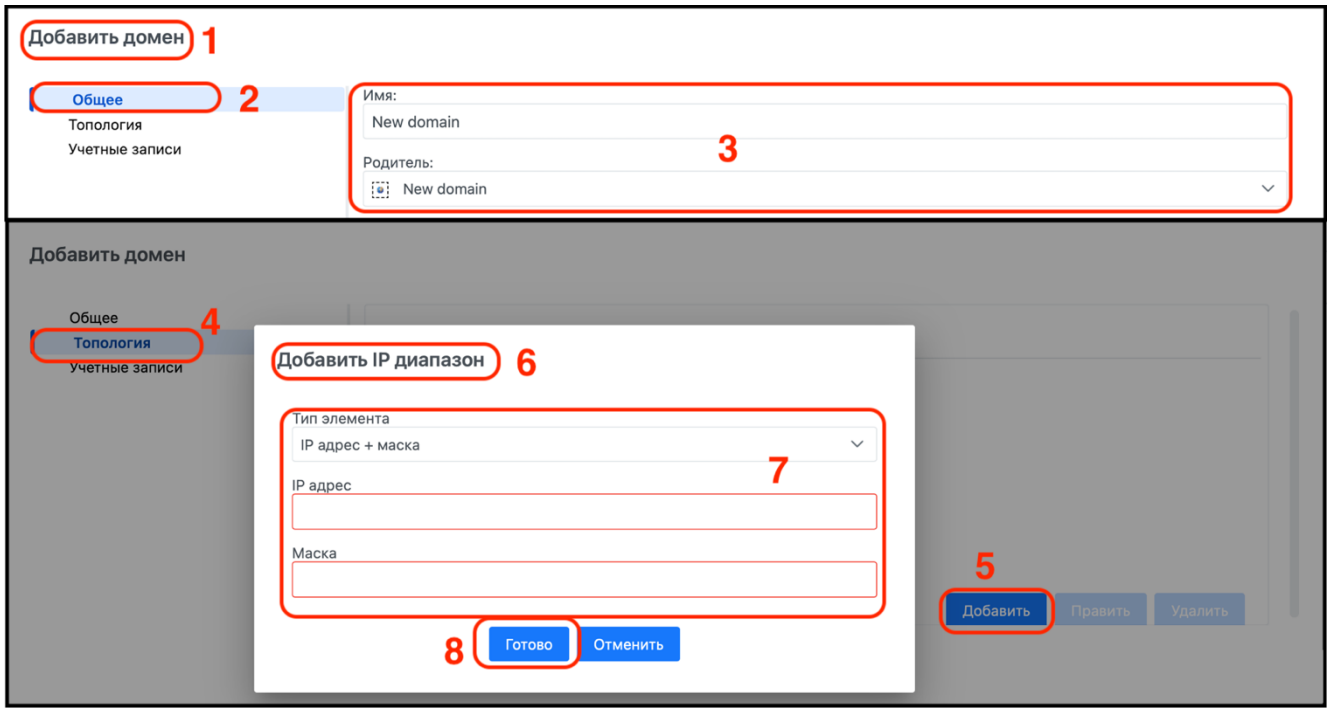


Рисунок 163 – Добавление домена

В окне настроек «Добавить домен» (цифра 1) в блоке «Общие» (цифра 2) создается иерархическая связь создаваемого домена с родительским, где необходимо ввести имя домена и выбрать иерархическую связь при помощи выпадающего списка «Родитель» (цифра 3). Для описания принадлежности сетевых объектов домену необходимо в блоке «Топология» (цифра 4) нажать кнопку «Добавить» (цифра 5), в открывшемся окне «Добавить IP-диапазон» (цифра 6) настроить в блоке (цифра 7) требуемые параметры:

1) Тип элемента:

— «IP-адрес + маска» (выбирается по умолчанию) – IP-адрес подсети может быть указан только в десятичной системе исчисления, маска подсети может быть задана как в сокращенной форме (например, /24), так и в десятичной системе исчисления;

- «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).

2) «IP-адрес»;

3) «Маска».

Если у сетевых объектов отсутствуют IP-адреса, то их принадлежность домену можно описать при условии, что в топологии домена отсутствует описание IP-диапазонов. Список IP-диапазонов домена задается в элементе списка «Топология» в окне настроек «Добавить домен» или «Изменить домен».

Доменная модель позволяет описать принадлежность домену следующих объектов политики:

- «Подсеть»;
- «IP-диапазон»;
- «IP-хост»;
- «Хост безопасности»;
- «Шлюз безопасности»;
- «Группа»;
- «Пользователь» (агент «ЗАСТАВА-Клиент»);
- «Расписание».
- «Правило»;
- «Группа правил».

Ни один из вышеперечисленных объектов не может одновременно принадлежать разным доменам.

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.

6.5.4.2 Учетные записи доменов

Управление учетными записями создаваемого/существующего домена осуществляется в окне настроек «Добавить домен» в элементе списка «Учетные записи». Окно настроек «Добавить домен» с элементом списка «Учетные записи» представлено на рисунке (см. Рисунок 164).

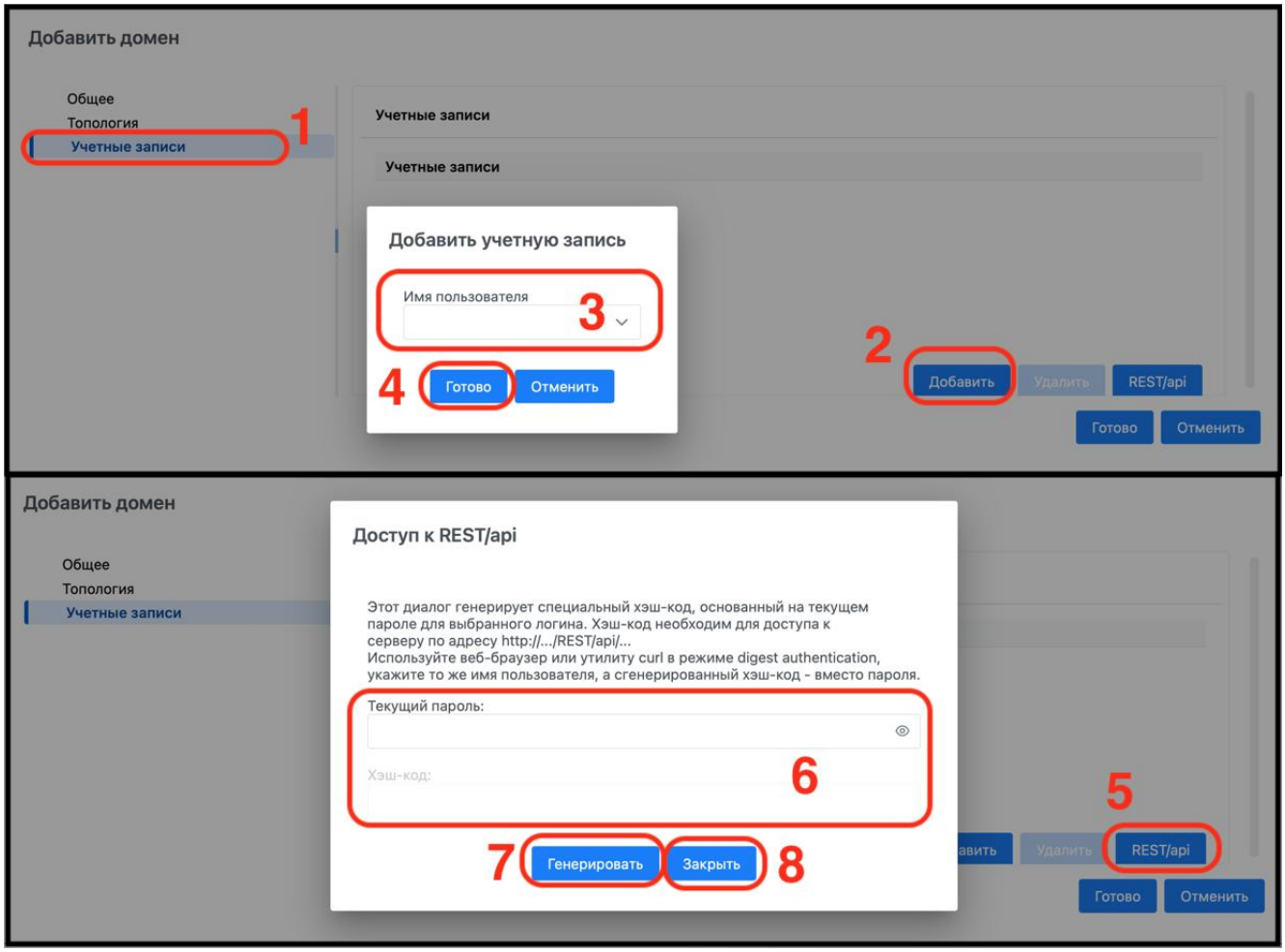


Рисунок 164 – Добавление учетной записи

Перейти в элемент списка «Учетные записи» (цифра 1), нажать кнопку «Добавить» (цифра 2), в открывшемся окне «Добавить учетную запись» ввести название учетной записи в поле «Имя пользователя» (цифра 3) и нажать кнопку «Готово» (цифра 4). Для получения доступа к веб-ресурсу с описанием API http://.../REST/api/ нажать кнопку «REST/api» (цифра 5), в открывшемся окне «Доступ к REST/api» ввести текущий пароль (цифра 6). Для просмотра введенного пароля можно воспользоваться элементом «» «Показать пароль» и обратно, тогда элемент поменяет вид на «». Ограничение на количество символов в пароле отсутствует. Нажать кнопку «Генерировать» (цифра 7). Нажать кнопку «Закрыть» (цифра 8).

6.5.5 Центры сертификации

Элемент списка «Центры сертификации» содержит описание УЦ, где издаются сертификаты, информацию о сертификатах, использованных для описания объектов ГПБ, а также сертификатах УЦ, выпустивших эти сертификаты[7)]. Окно элемента списка «Центры сертификации» представлено на рисунке (см. Рисунок 165).

[7)] В качестве сертификатов УЦ будут размещены подписанные ими сертификаты.

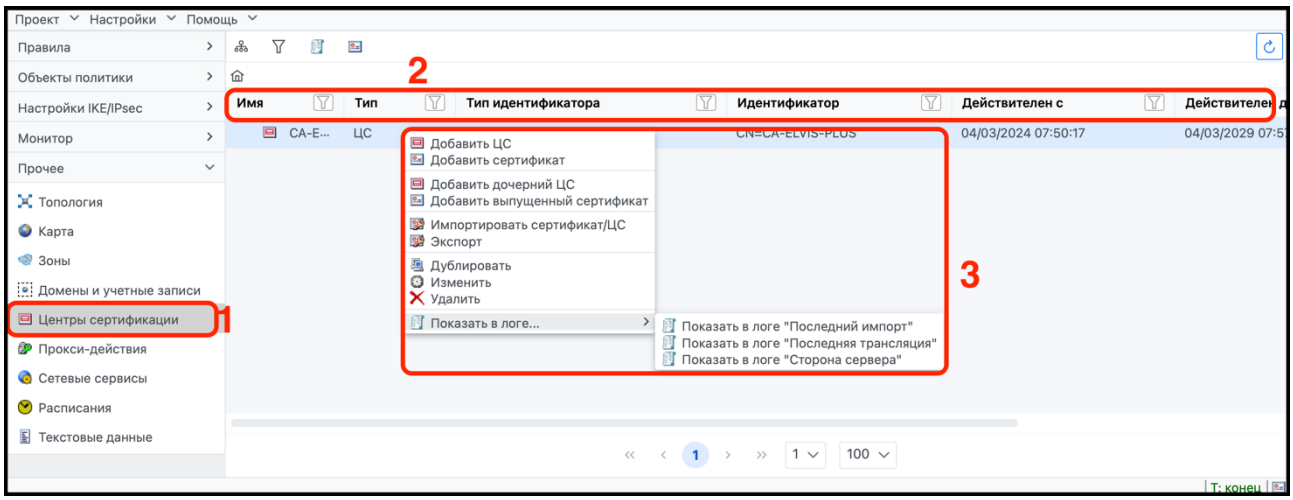


Рисунок 165 – Элемент списка «Центр сертификации»

В окне элемента списка «Центры сертификации» (цифра 1) отображены сертификаты в виде таблицы со следующими параметрами (цифра 2):

— «Имя»;
— «Тип»;
— «Тип идентификатора»;
— «Идентификатор»;
— «Действителен с»;
— «Действителен до»;
— «Объект».

По каждому параметру возможна сортировка.

Вызвать контекстное меню можно, нажав правой клавишей мыши на выбранный объект в списке или на свободное место в рабочей области таблицы (цифра 3).

6.5.5.1 Добавление центра сертификации

Для добавления ЦС нужно нажать на свободное место или на требуемый в списке объект правой клавишей мыши, вызвав контекстное меню. Нажать команду «Добавить ЦС», как представлено на рисунке (см. Рисунок 166).

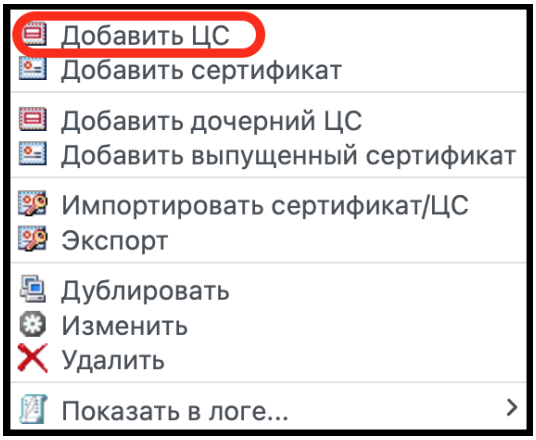


Рисунок 166 – Команда «Добавить ЦС»

В открывшемся окне «Добавить ЦС» необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 167).

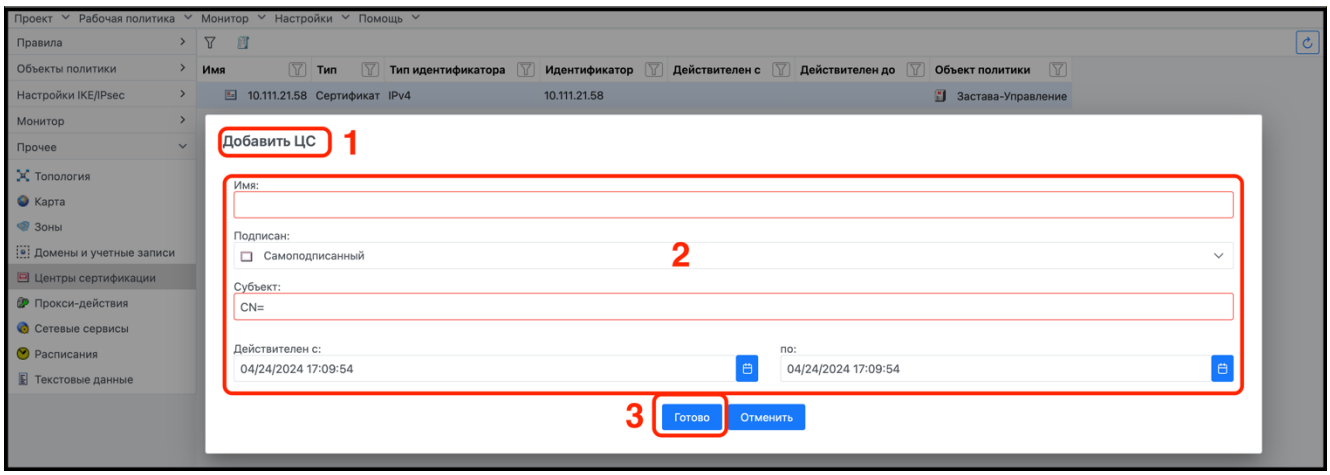


Рисунок 167 – Добавление центра сертификации

В окне настроек «Добавить ЦС» (цифра 1) в блоке (цифра 2) настроить требуемые параметры и нажать кнопку «Готово» (цифра 3).

6.5.5.2 Добавление сертификата

Для добавления сертификата нужно нажать на свободное место или на требуемый в списке объект правой клавишей мыши, вызвав контекстное меню. Нажать команду «Добавить сертификат», как представлено на рисунке (см. Рисунок 168).

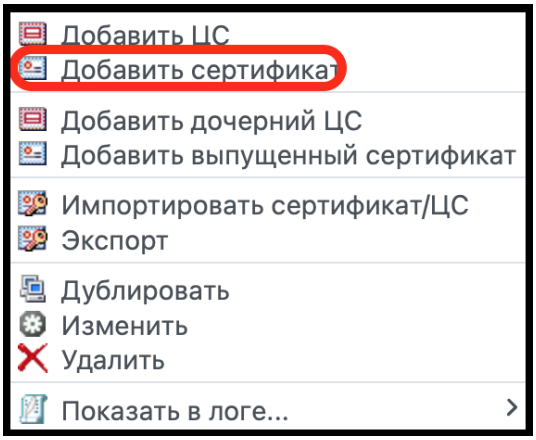


Рисунок 168 – Команда «Добавить сертификат»

Для добавления сертификата необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 169).

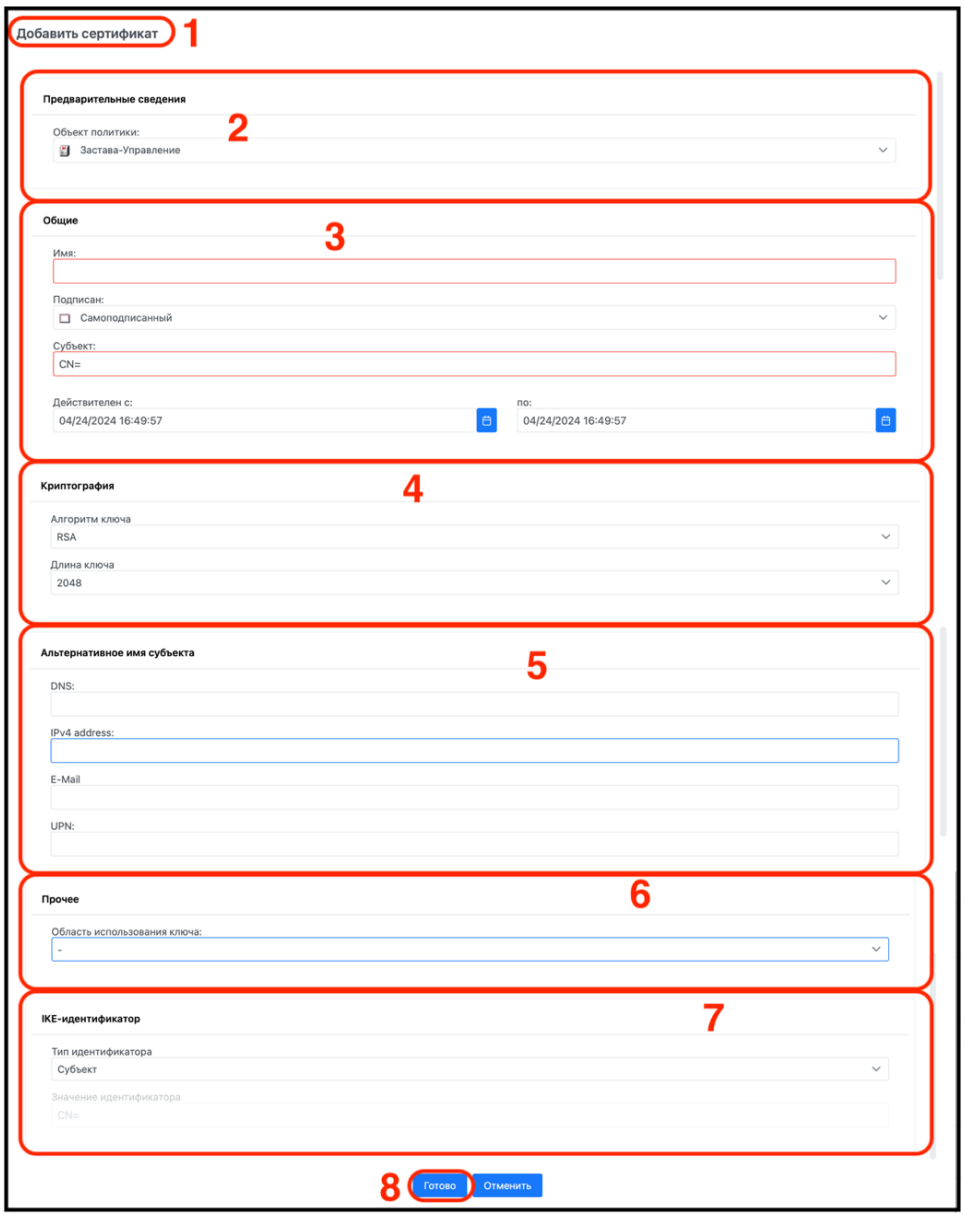


Рисунок 169 – Добавление сертификата

В контекстном меню нажать кнопку «Добавление сертификата», в открывшемся окне настроек «Добавить сертификат» (цифра 1) настроить требуемые параметры:

1) заполнить блок «Предварительные сведения» (цифра 2);
2) заполнить блок параметров «Общие» (цифра 3);
3) в блоке «Криптография» (цифра 4) выбрать из выпадающих списков параметры ключа;
4) задать альтернативное имя субъекта в блоке (цифра 5);
5) выполнить настройки в блоке «Прочее» (цифра 6);
6) выполнить настройки в блоке «IKE-идентификатор» (цифра 7);
7) нажать кнопку «Готово» в блоке (цифра 8).

Описание параметров, используемых при добавлении сертификата, представлено в таблице (см. Таблица 30).

Таблица 30 – Описание параметров, используемых при добавлении сертификата

Опция	Параметр	Описание
Предварительные сведения	Объект политики	Объект политики из списка предложенных
Общие	Имя	Distinguished Name (DN) сертификата
	Подписан	Сертификат УЦ, которым подписан данный сертификат
	Субъект	Поле, содержащее информацию о владельце сертификата в формате Distinguished Name (DN) (например, CN=Alice, OU=Management, O=MyCompany)
	Действителен с	Начало срока действия сертификата
	Действителен по	Окончание срока действия сертификата
Криптография	Алгоритм ключа	Тип открытого ключа, содержащегося в сертификате
	Длина ключа	Длина ключа, содержащегося в сертификате
Альтернативное имя субъекта	Поле, содержащее дополнительную информацию о владельце сертификата	
	DNS	Имя хоста
	IPv4 address	IP-адрес хоста
	E-mail	Адрес электронной почты владельца
	UPN	Атрибут имени
Прочее	Область использования ключа	IRE/IPSEC, Вход со смарт-картой
IKE-идентификатор		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
	Тип идентификатора	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	Значение «IKE Identity». Заполняется автоматически в зависимости от параметра «Identity type» и параметров с информацией о владельце сертификата

6.5.5.3 Добавить дочерний ЦС

Для импорта сертификата ЦС нужно нажать на свободное место или на требуемый в списке объект правой клавишей мыши, вызвав контекстное меню. Выбрать команду «Добавить дочерний ЦС», как представлено на рисунке (см. Рисунок 170).

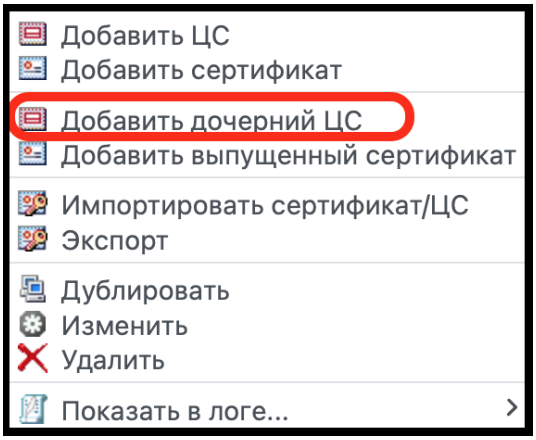


Рисунок 170 – Команда «Добавить дочерний ЦС»

Процедура добавления дочернего ЦС выполняется аналогично добавлению сертификата, подробное описание представлено в п. 6.5.5.1.

6.5.5.4 Добавление выпущенного сертификата

Для импортирования сертификата ЦС нужно нажать на свободное место или на требуемый в списке объект правой клавишей мыши, вызвав контекстное меню. Выбрать команду «Добавить выпущенный сертификат», как представлено на рисунке (см. Рисунок 171).

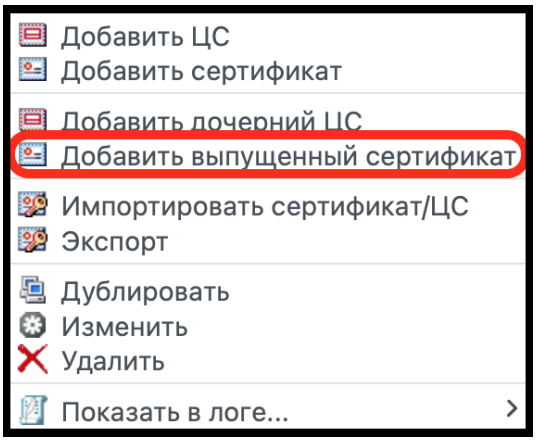


Рисунок 171 – Команда «Добавить выпущенный сертификат»

Процедура добавления выпущенного сертификата выполняется аналогично добавлению ЦС, подробное описание представлено в п. 6.5.5.2.

6.5.5.5 Импортировать сертификат или ЦС

Для импортирования сертификата ЦС нужно нажать на свободное место или на требуемый в списке объект правой клавишей мыши, вызвав контекстное меню. Выбрать команду «Импортировать сертификат/ЦС», как представлено на рисунке (см. Рисунок 172).

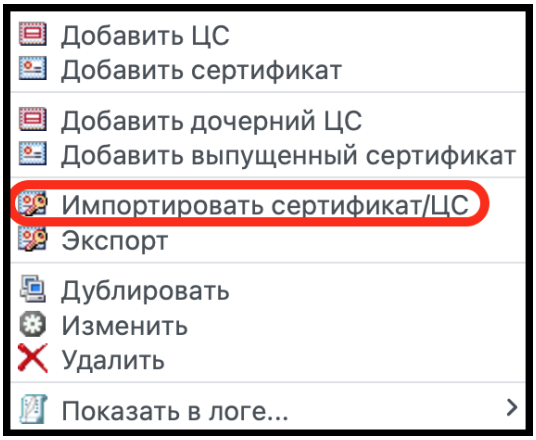


Рисунок 172 – Команда «Импортировать сертификат/ЦС»

Для импортирования сертификата ЦС необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 173).

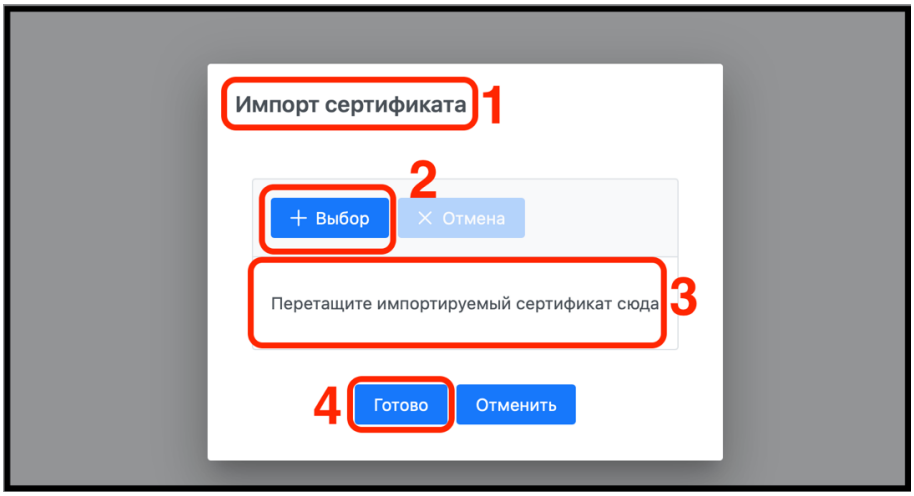


Рисунок 173 – Добавление центра сертификации

В окне настроек «Импорт сертификата» (цифра 1) нажать кнопку «+Выбор» (цифра 2), в списке ранее полученных сертификатов выбрать требуемый, либо переместить файл в окно «Перетащите импортируемый сертификат сюда» (цифра 3). Нажать кнопку «Готово» (цифра 4).

6.5.5.6 Экспорт сертификата

Для экспорта сертификата нужно нажать на свободное место или на требуемый в списке объект правой клавишей мыши, вызвав контекстное меню. Выбрать команду «Экспорт», как представлено на рисунке (см. Рисунок 174).

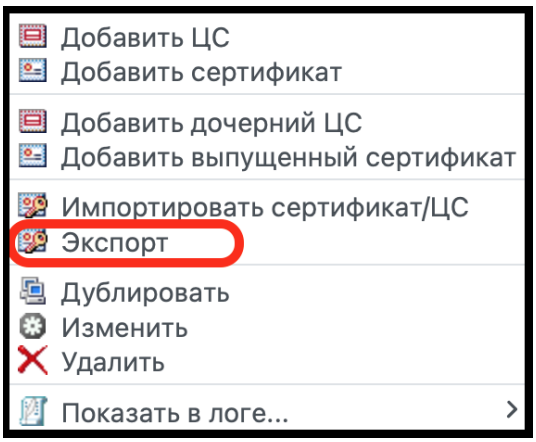


Рисунок 174 – Команда «Экспорт»

В результате сертификат будет экспортирован в выбранную для хранения файла директорию.

6.5.6 Прокси-действия

Для добавления и настройки прокси-действия необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 175).

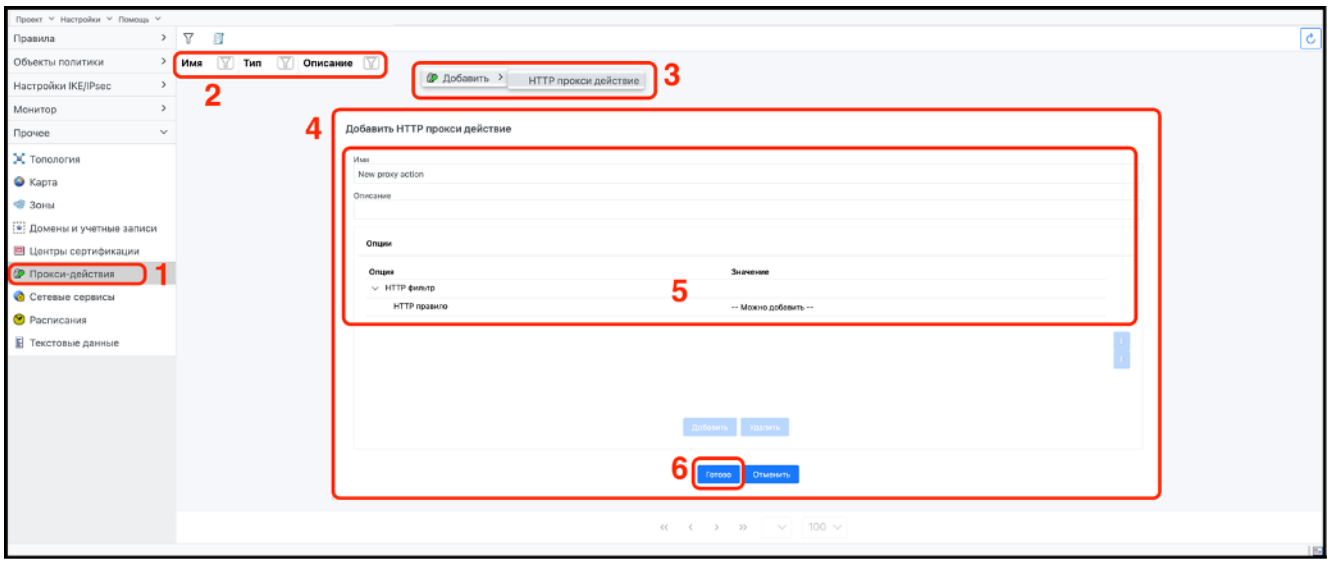


Рисунок 175 – Элемент списка «Прокси-действия»

В окне элемента списка «Прокси-действия» (цифра 1) отображается список прокси-действий в виде таблицы с параметрами (цифра 2):

— «Имя»;

— «Тип»;

— «Описание».

По каждому параметру доступна сортировка.

Для добавления прокси-действия необходимо вызвать контекстное меню, выбрать дополнительную команду «HTTP прокси-действие» (цифра 3). В результате откроется окно настроек «Добавить HTTP прокси-действие» (цифра 4). Ввести требуемые параметры (цифра 5).

При необходимости создания нескольких прокси-действий необходимо нажать кнопку «Добавить». Для завершения настроек нажать кнопку «Готово» (цифра 6).

Контекстное окно элемента списка «Прокси-действия» с доступными в нем общими командами изображено на рисунке (см. Рисунок 176).

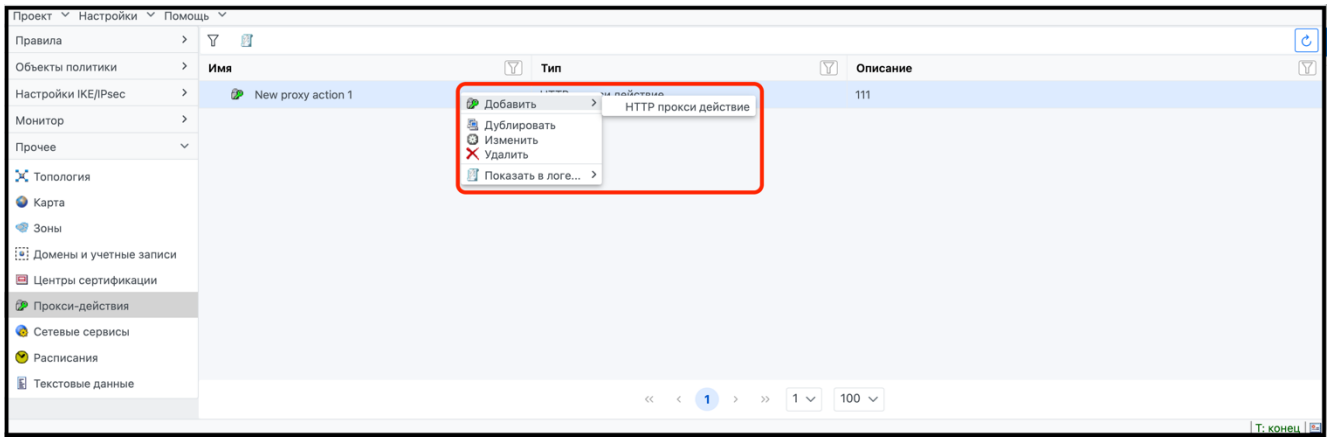


Рисунок 176 – Контекстное окно элемента списка «Прокси-действия»

6.5.7 Сетевые сервисы

Объекты сетевых сервисов представляют протоколы сетевого обслуживания (или их группы), используемые для установления типов трафика, которые будут обрабатываться правилом (по умолчанию около 100 объектов сетевых сервисов присутствуют в ПО ЗУ). Правила применяются ко всем типам IP-пакетов. Протоколы TCP, UDP и ICMP, группы этих протоколов, а также протоколы AH и ESP заранее установлены в ПО ЗУ. Вид окна «Сетевые сервисы представлен на рисунке (см. Рисунок 177).

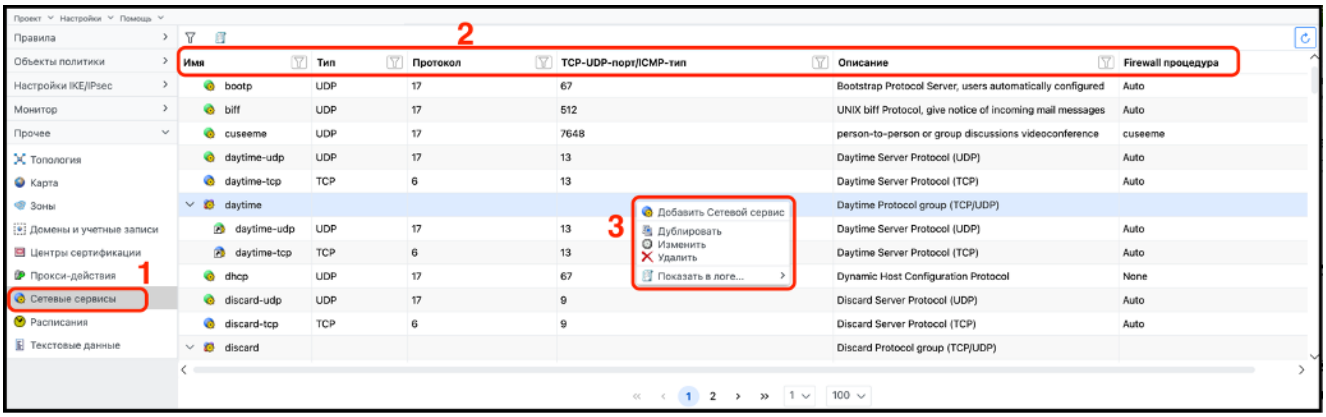


Рисунок 177 – Окно элемента списка «Сетевые сервисы»

Объекты сетевых сервисов создаются и редактируются в элементе списка «Сетевые сервисы» (цифра 1), где они отображаются в виде таблицы (цифра, 2), с указанием следующих параметров:

— «Имя»;

— «Тип»;

— «Протокол»;

— «TCP/UDP-порт/ICMP-тип»;

— «Описание»;

— «Firewall-процедура».

По каждому из параметров возможна сортировка списка. Порядок, в котором сетевые сервисы отображаются в таблице, может быть изменен. По умолчанию объекты отсортированы по имени в алфавитном порядке. Чтобы отсортировать сервисы по необходимому параметру, нужно нажать на соответствующий параметр вверху таблицы сетевых сервисов. Для элемента списка «Сетевые сервисы» доступны общие команды контекстного меню (цифра 3).

6.5.7.1 Добавить сетевой сервис

Для добавления сетевого сервиса необходимо вызвать контекстное меню, выбрать команду «Добавить сетевой сервис», далее выполнить шаги, изображенные на рисунке (см. Рисунок 178).

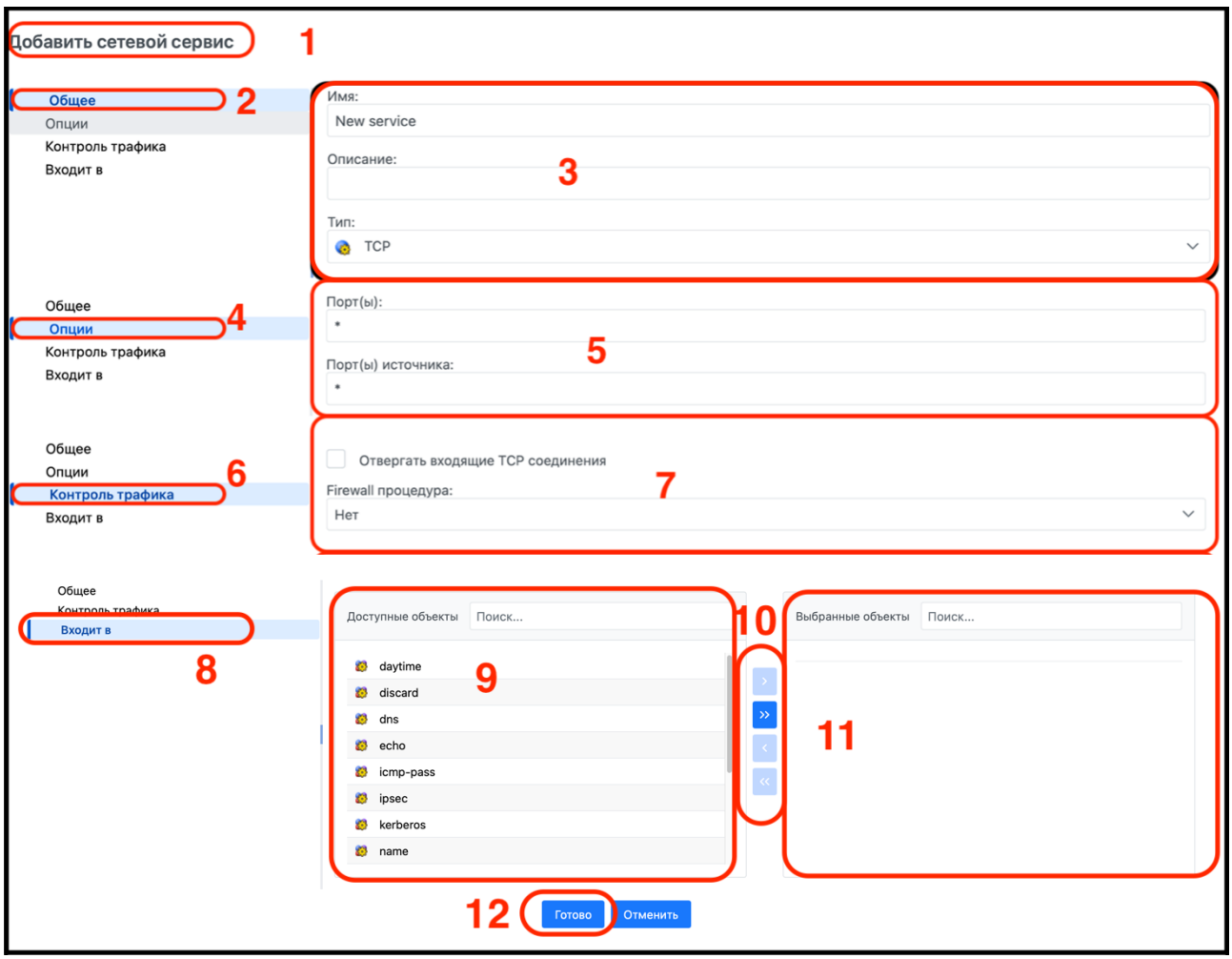


Рисунок 178 – Окно «Добавить сетевой сервис»

В окне настроек «Добавить сетевой сервис» (цифра 1) настроить:

1) в блоке настроек «Общее» (цифра 2) заполнить требуемые параметры (цифра 3):

— ввести уникальное имя;

— при необходимости добавить описание;

— выбрать тип сервиса. Графическое представление сетевых сервисов представлено в таблице (см. Таблица 31);

2) в блоке настроек «Опции» (цифра 4) задать требуемые параметры (цифра 5). В зависимости от выбранного типа сервиса в блоке настроек «Опции» (цифра 4) будут отображаются разные группы настраиваемых параметров. В случае выбора:

— сервисов ICMP необходимо задать параметры «ICMP тип(ы)» и «ICMP код(ы)»;

— сервисов UDP или TCP необходимо задать параметры для «Порт(ы)» и «Порт(ы) источника»;

3) в блоке настроек «Контроль трафика» (цифра 6) выбрать из выпадающего списка процедуры межсетевого экранирования (Firewall-процедура) (цифра 7);

4) в блоке настроек «Входит в» (цифра 8) в области «Доступные объекты» (цифра 9) будет отображен перечень созданных ранее групп, в котором, при необходимости, можно выбрать группы для перемещения их из одного списка в другой, используя для этого элементы управления (цифра 10), переместить их в область «Выбранные объекты» (цифра 11).

Нажать кнопку «Готово» (цифра 12).

Таблица 31 – Графическое представление сетевых сервисов

Элемент	Описание	Элемент	Описание
	IP/Все протоколы IP		Группа сетевых сервисов
	Сервисы ICMP		Сервисы TCP
	Сервисы UDP		Импорт сервисов TCP

6.5.7.2 Редактирование членов групп сетевых сервисов

Для редактирования членов групп сетевых сервисов требуется выполнить шаги, изображенные на рисунке (см. Рисунок 179).

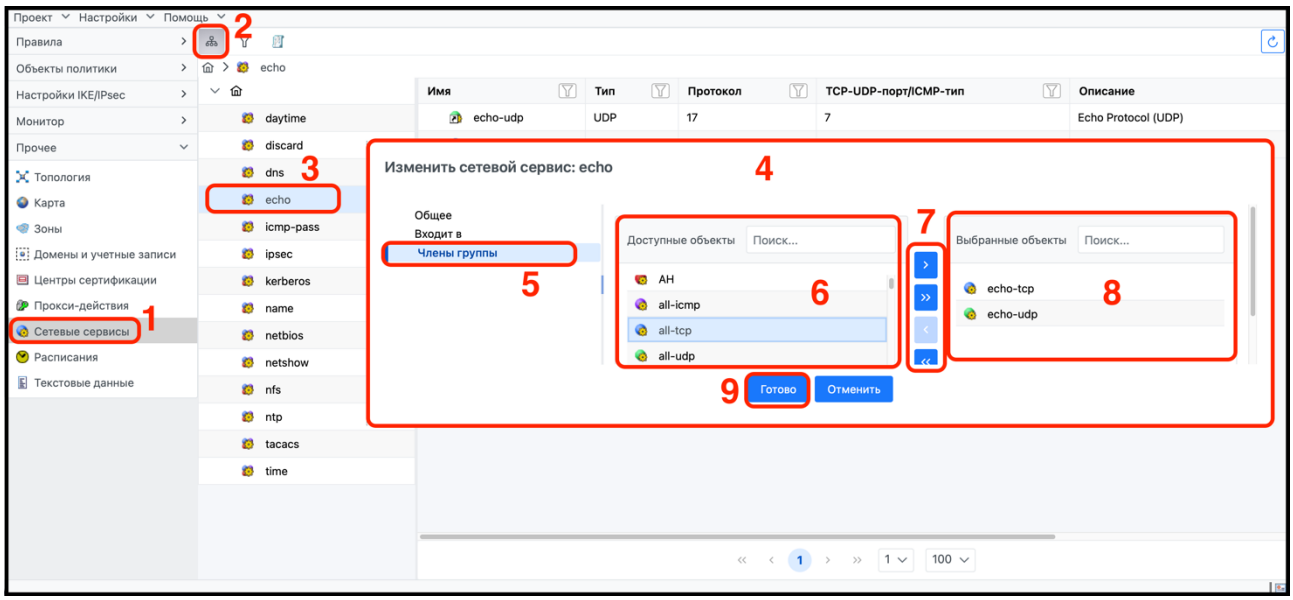


Рисунок 179 – Редактирование членов групп сетевых сервисов

В окне элемента списка «Сетевые сервисы» (цифра 1) с помощью элемента «⁂» (цифра 2) выбрать в иерархическом списке требуемую группу (цифра 3), дважды нажав на нее левой клавишей мыши. В результате откроется окно «Изменить сетевой сервис» (цифра 4), в котором требуется открыть блок настроек «Члены группы» (цифра 5) и произвести требуемые изменения. Из области «Доступные объекты» (цифра 6), где будет отображен перечень созданных ранее групп, выбрать группы для перемещения из одного списка в другой, используя для этого элементы (цифра 7), переместить их в область «Выбранные объекты» (цифра 8). Нажать кнопку «Готово» (цифра 9).

6.5.7.3 Процедуры межсетевых экранов

Firewall-процедуры (далее - 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 ПО ЗУ содержит набор процедур МЭ, которые фильтруют трафик, используя несколько типов протоколов.

При настройке сетевого сервиса в процедуре МЭ в поле «Контроль трафика» можно выбрать одно из трёх значений: «None», «Auto» или «FTP». None означает, что данный сетевой сервис не будет использовать никаких процедур МЭ. Значение «Auto» подразумевает, что ПО ЗУ автоматически включит процедуры, являющиеся стандартными для указанного протокола. Эта процедура МЭ будет принимать параметры напрямую из сетевых сервисов.

Процедуры МЭ обеспечивают безопасность внутренних систем и сетей, которые фильтруют входящий и исходящий трафик. Любые заказные процедуры МЭ должны быть добавлены к соответствующему файлу описания до того, как они будут использованы в ПО ЗУ. Список процедур МЭ:

— «Icmp»;
— «Ip»;
— «Tcp»;
— «Udp»;
— «ftp»;
— «tos_modify»;
— «ipopt_sec»;
— «nat»;
— «napt»;
— «nat_redirect».

Если ЛПБ содержит процедуру МЭ, которой нет на компьютере агента, в файле регистрации событий агента появится сообщение об ошибке, и ЛПБ не будет загружена.

6.5.8 Расписания

Элемент списка «Расписание» используется для настройки определенного интервала времени 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.

Окно элемента списка «Расписания» представлено на рисунке (см. Рисунок 180).

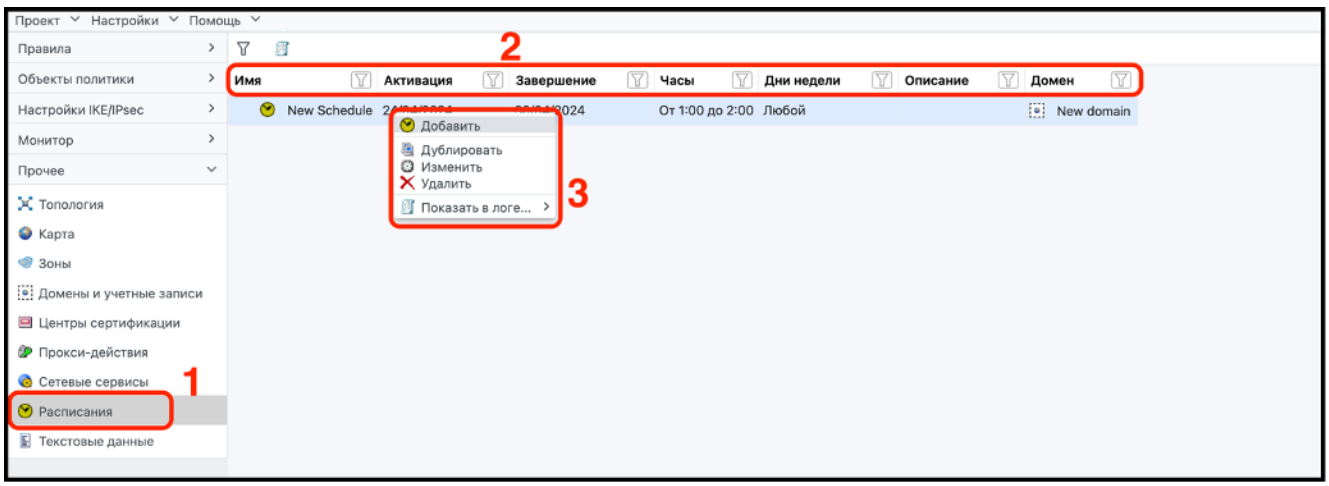


Рисунок 180 – Элемент списка «Расписание»

В окне «Расписания» (цифра 1) отображается список расписания правил в виде таблицы со следующими параметрами (цифра 2):

— «Имя»;
— «Активация»;
— «Завершение»;
— «Часы»;
— «Дни недели»;
— «Описание»;
— «Домен».

Для элемента списка «Расписание» доступно контекстное меню (цифра 3) с общими командами. Для добавления расписания необходимо в свободном месте таблицы вызвать контекстное меню правой клавишей мыши, где выбрать команду «Добавить» и выполнить шаги, изображенные на рисунке (см. Рисунок 181).

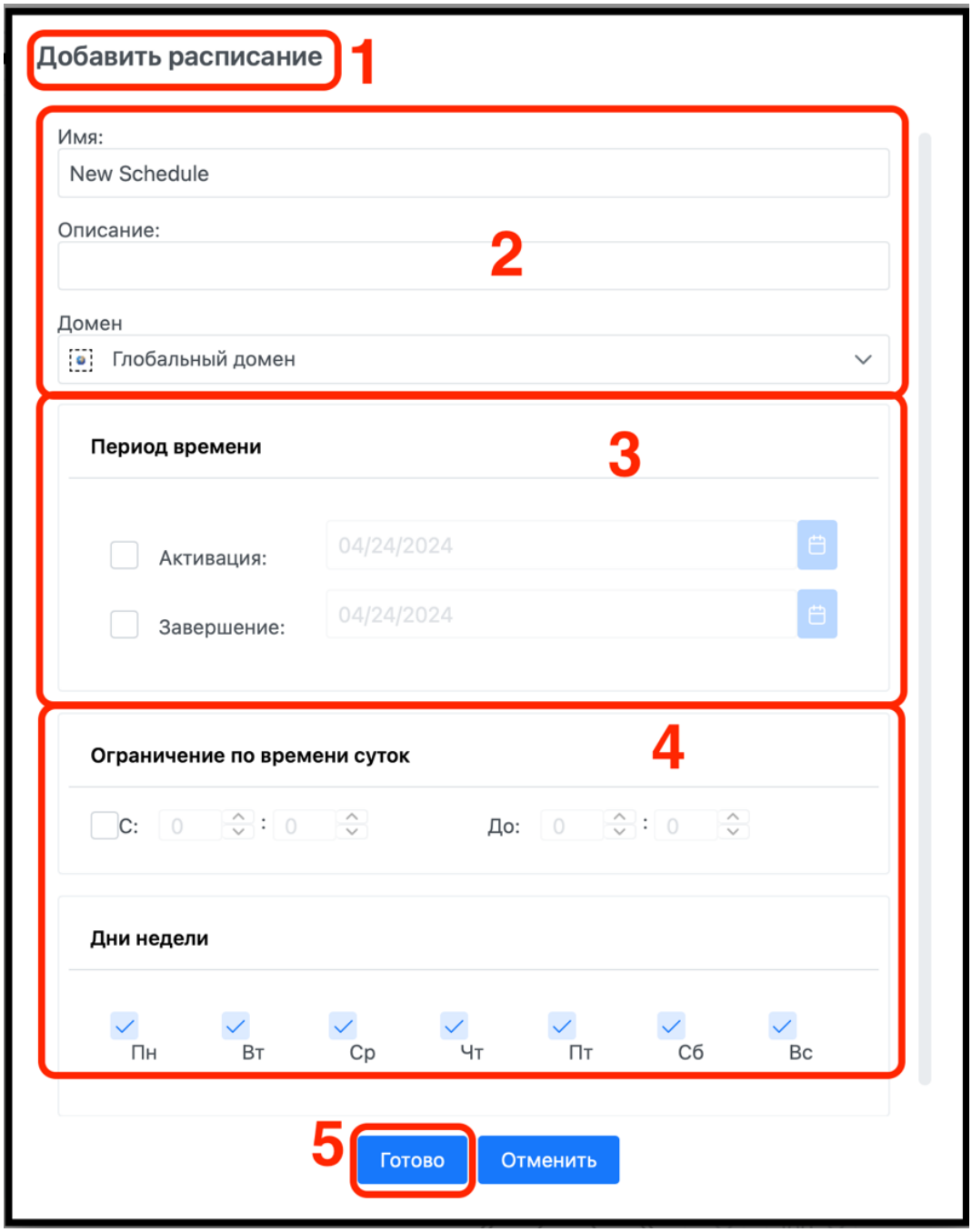


Рисунок 181 – Окно настроек «Добавить расписание»

В открывшемся окне «Добавить расписание» (цифра 1) заполнить:

1) блок общих настроек (цифра 2);
2) определить период времени в блоке (цифра 3);
3) настроить ограничение по времени суток и назначить дни недели работы расписания (цифра 4);
4) нажать кнопку «Готово» (цифра 5).

6.5.9 Текстовые данные

Окно элемента списка «Текстовые данные» представлено на рисунке (см. Рисунок 182).

Рисунок 182 – Элемент списка «Текстовые данные»

В окне элемента списка «Текстовые данные» (цифра 1) отображается список определяемых пользователем ЛПБ в текстовом виде с указанием следующей информации (цифра 2):

— «Имя»;

— «Описание»;

— «Где используется».

Для элемента списка доступно контекстное меню (цифра 3) с общими командами. Для добавления текстового файла необходимо выбрать в контекстном меню команду «Добавить» и выполнить шаги, изображенные на рисунке (см. Рисунок 183).

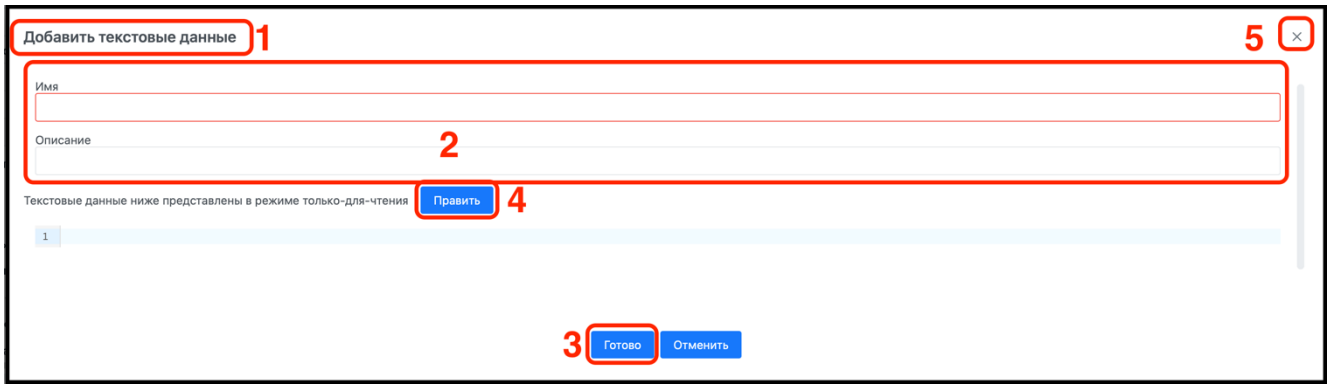


Рисунок 183 – Окно настроек «Добавить текстовые данные»

В открывшемся окне «Добавить текстовые данные» (цифра 1) заполнить:

1) блок общих настроек (цифра 2);
2) нажать кнопку «Готово» (цифра 3);
3) при необходимости править текст, используя кнопку «Править» (цифра 4);
4) выйти из окна настроек «Добавить текстовые данные», используя элемент «×» (цифра 5).

7 НАЧАЛО РАБОТЫ

Для построения ГПБ требуется выполнить ряд мероприятий, связанных с добавлением и настройкой объектов политики, регистрацией сертификатов с последующей трансляцией созданных настроек и дальнейшей активацией ГПБ для отображения ее в интерфейсе ПО ЗУ.

В этой части описываются все типы объектов, их назначение, параметры и характеристики, инструкции по созданию и управлению этими объектами.

7.1 Добавление объектов ГПБ

Создавать объекты ГПБ можно в боковой панели вкладок «Объекты политики» или в любом другом окне, где в контекстном меню есть команды добавления объектов. Для удобства работы и восприятия можно создавать объекты в элементе списка «Топология» и перемещать их в рабочей области топологии.

Для каждого объекта имя должно быть уникальным[8)].

7.1.1 Добавление и настройка объекта типа «Подсеть»

Для добавления объекта типа «Подсеть» необходимо перейти в контекстное меню, как представлено в подразделе 7.1 выбрать команду «Добавить подсеть» и перейти к настройкам.

7.1.1.1 Настройка параметров для элемента списка «Общее»

В открывшемся окне «Добавить подсеть», выполнить шаги, изображенные на рисунке (см. Рисунок 184).

Рисунок 184 – Настройка объекта типа «Подсеть»

В окне настроек «Добавить подсеть» (цифра 1) в элементе списка «Общее» (цифра 2) необходимо заполнить форму (цифра 3):

— имя объекта;

[8)] В имени объекта можно использовать только символы таблицы ASCII из диапазона индексов от 0 до 125 включительно.

— описание (при необходимости);

— выбрать домен из выпадающего списка.

7.1.1.2 Настройка параметров для элемента списка «Топология»

Перейти в элемент списка «Топология», в открывшемся окне выполнить шаги, изображенные на рисунке (см. Рисунок 185).

Рисунок 185 – Настройка топологии объекта типа «Подсеть»

В окне элемента списка «Топология» (цифра 1) выполнить настройки (цифра 2):

— «Адрес» (указать IP-адрес);

— «Маска»;

— «Зона» (выбрать требуемую зону из выпадающего списка).

7.1.1.3 Настройка параметров для элемента списка «Местоположение»

Перейти в элемент списка «Местоположение», в открывшемся окне выполнить шаги, изображенные на рисунке (см. Рисунок 186).

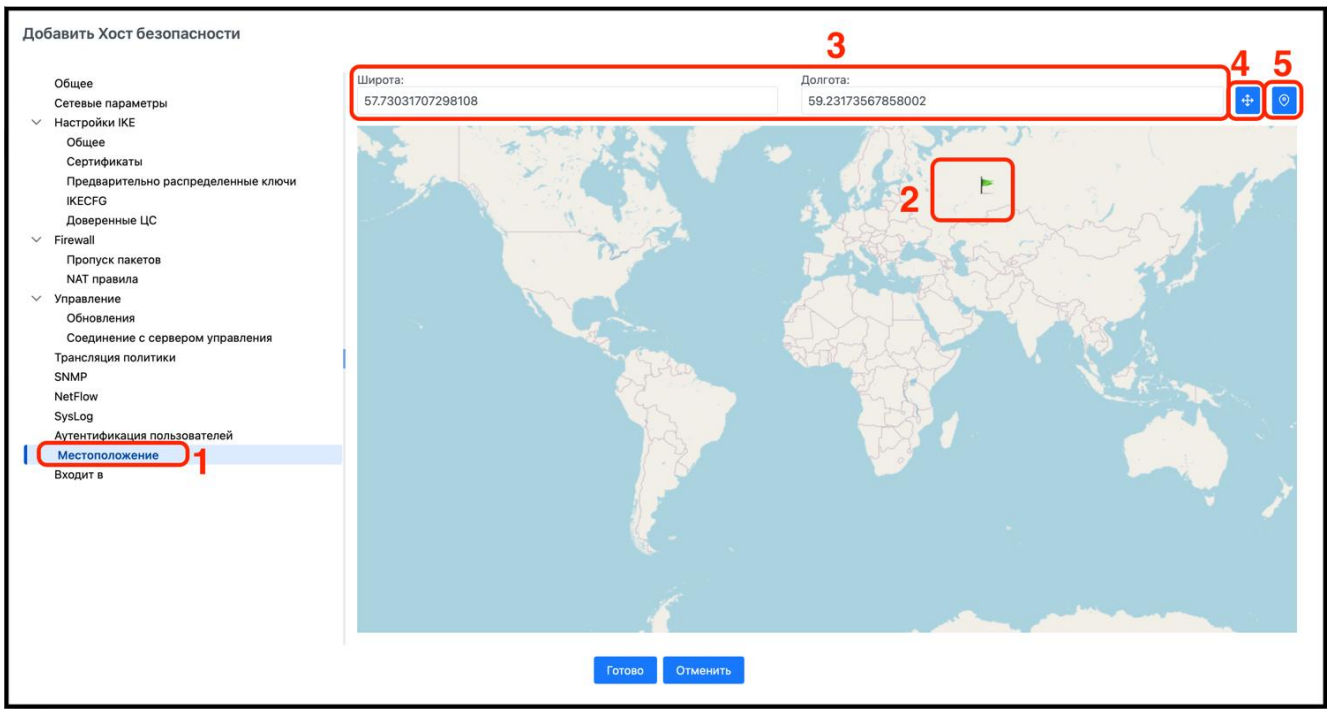


Рисунок 186 – Настройка местоположения объекта типа «Подсеть»

В окне элемента списка «Местоположение» (цифра 1) на карте разместить указатель мыши в требуемом месте и нажать левой клавишей мыши, установив флажок объекта (цифра 2). Также разместить объект на карте можно, указав широту и долготу нужного местоположения в строке координат (цифра 3). В результате выполненных действий флажок переместится в заданную точку. С помощью элемента «» «Показать на карте» (цифра 4) карта расположится по центру относительно установленного флажка. С помощью элемента «» можно найти географические координаты местоположения объекта, если в его настройках включена передача геолокации (цифра 5).

7.1.1.4 Настройка параметров для элемента списка «Входит в»

Перейти в элемент списка «Входит в», в открывшемся окне выполнить шаги, изображенные на рисунке (см. Рисунок 187).

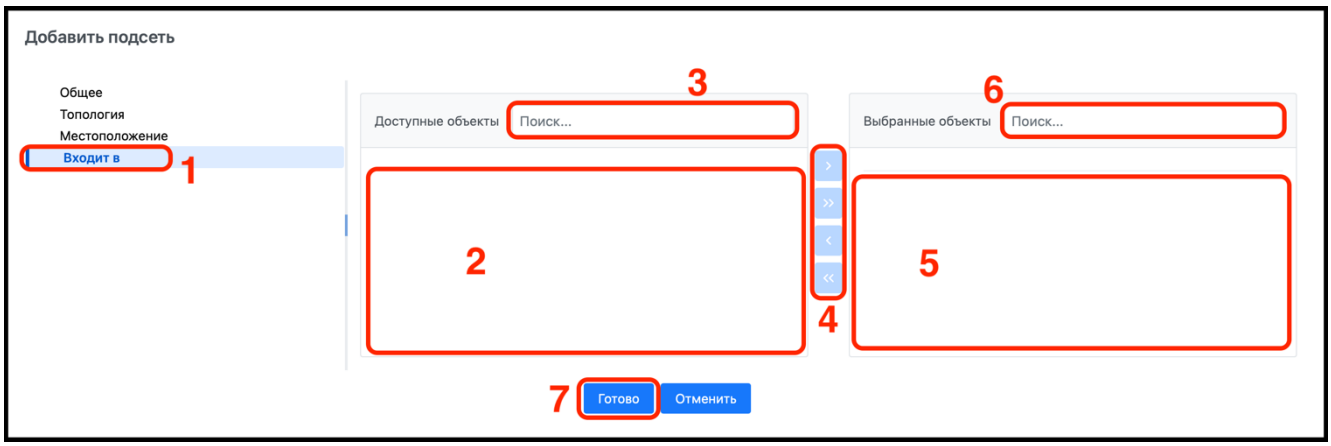


Рисунок 187 – Настройка окна «Входит в» объекта типа «Подсеть»

В окне элемента списка «Входит в» (цифра 1) выбрать требуемый для вхождения в группу объект в поле «Доступные объекты» (цифра 2) или найти его, используя поисковую строку (цифра 3). Выбрать требуемый объект для создания группы в поле «Выбранные объекты» (цифра 5) или найти его, используя поисковую строку (цифра 6). Переместить требуемый объект в необходимые группы или разгруппировать объекты можно с помощью инструментов перемещения (цифра 4). Выполнив все требуемые настройки, необходимо нажать кнопку «Готово» (цифра 7).

В результате в рабочей области элемента списка «Топология» будет добавлен и настроен объект типа «Подсеть», как изображено на рисунке (см. Рисунок 188).

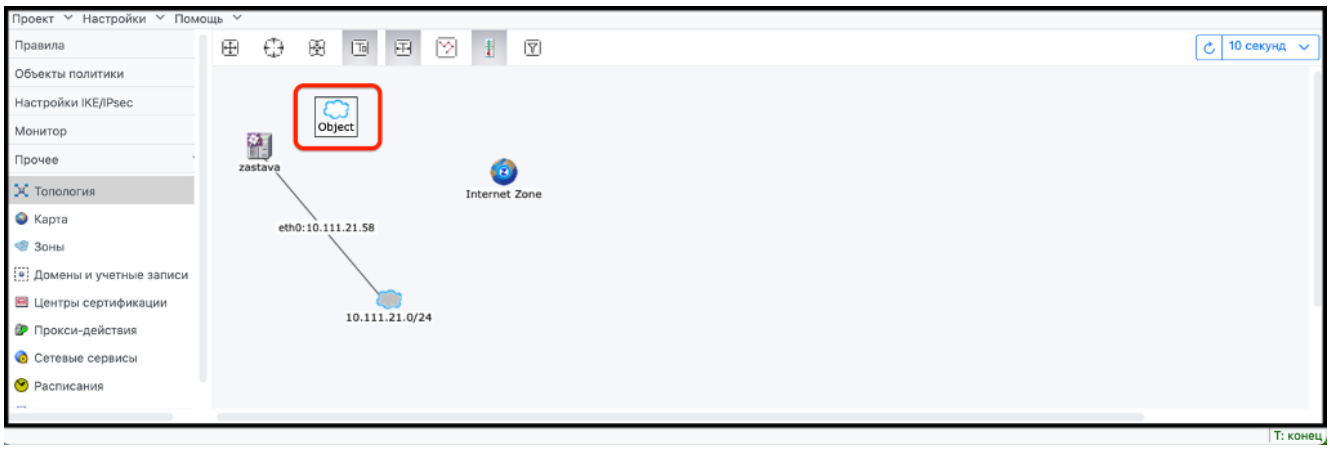


Рисунок 188 – Вид окна элемента списка «Топология» с добавленным объектом типа «Подсеть»

7.1.2 Добавление и настройка объекта типа «IP-диапазон»

Для добавления объекта типа «IP диапазон» необходимо перейти в контекстное меню, как представлено в подразделе 7.1, и выбрать команду «Добавить IP-диапазон» и перейти к настройкам.

7.1.2.1 Настройка параметров для элемента списка «Общее»

В открывшемся окне «Добавить IP диапазон», выполнить шаги, изображенные на рисунке (см. Рисунок 189).

Рисунок 189 – Настройка объекта типа «IP-диапазон»

В окне настроек «Добавить IP-диапазон» (цифра 1) в элементе списка «Общее» (цифра 2) необходимо заполнить форму (цифра 3):

— имя объекта;

— описание (при необходимости);

— выбрать домен из выпадающего списка.

7.1.2.2 Настройка параметров для элемента списка «Топология»

В открывшемся окне элемента списка «Топология» выполнить шаги, изображенные на рисунке (см. Рисунок 190).

Рисунок 190 – Настройка топологии для объекта типа «IP-диапазон»

В окне элемента списка «Топология» (цифра 1) нажать кнопку «Добавить» (цифра 2).

В открывшемся блоке настроек выполнить шаги, изображенные на рисунке (см. Рисунок 191).

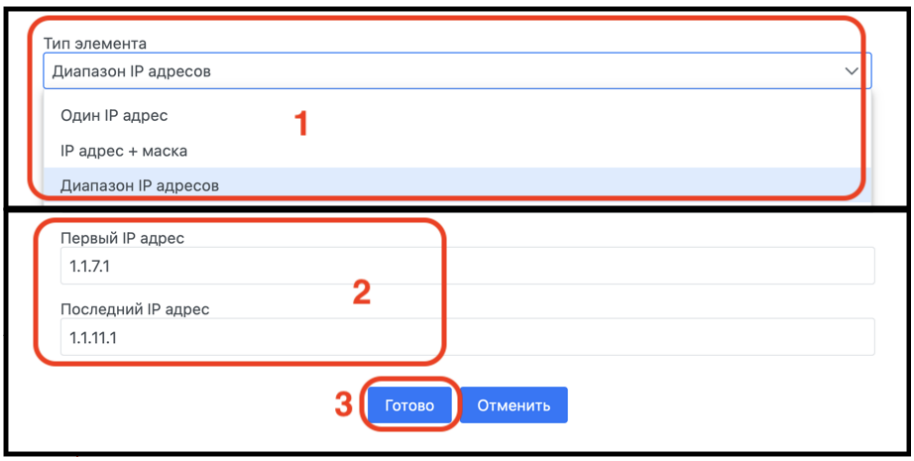


Рисунок 191 – Настройка объекта типа «IP-диапазон»

Выбрать тип элемента (цифра 1) из выпадающего списка, ввести диапазоны IP-адресов (цифра 2), нажать кнопку «Готово» (цифра 3).

В случае неверно введенных данных откроется окно, изображенное на рисунке (см. Рисунок 192), с предупреждением об ошибке.

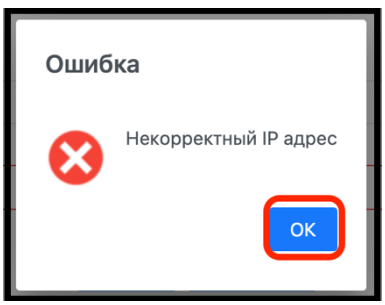


Рисунок 192 – Предупреждение об ошибке.

7.1.2.3 Настройка параметров для элемента списка «Местоположение»

Перейти в элемент списка «Местоположение» и выполнить шаги, изображенные на рисунке (см. Рисунок 193).

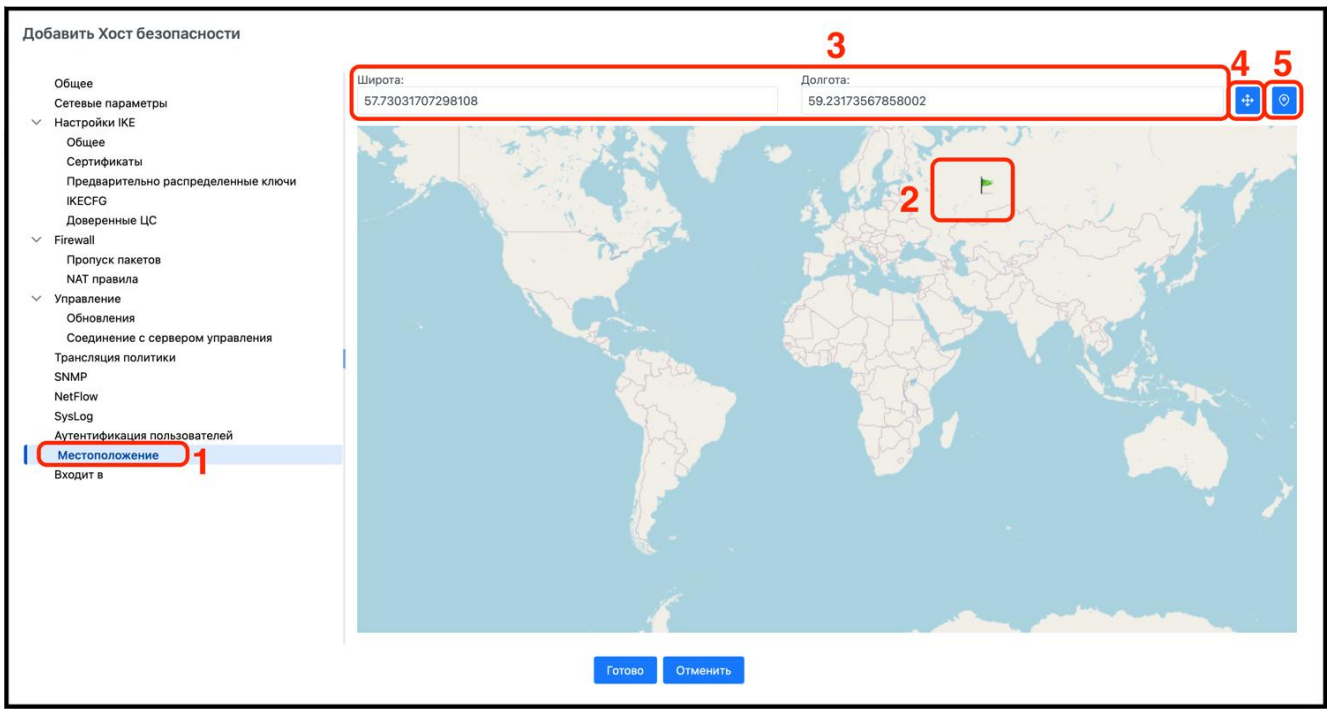


Рисунок 193 – Настройка местоположения объекта типа «IP-диапазон»

В окне элемента списка «Местоположение» (цифра 1) на карте разместить указатель мыши в требуемом месте и нажать левой клавишей мыши, установив флажок объекта (цифра 2). Также разместить объект на карте можно, указав широту и долготу нужного местоположения в строке координат (цифра 3). В результате выполненных действий флажок переместится в заданную точку. С помощью элемента «» «Показать на карте» (цифра 4) флажок окажется в центре карты. С помощью элемента «» можно найти географические координаты местоположения объекта, если в его настройках включена передача геолокации (цифра 5).

7.1.2.4 Настройка параметров для элемента списка «Входит в»

Перейти в элемент списка «Входит в» и выполнить шаги, изображенные на рисунке (см. Рисунок 194).

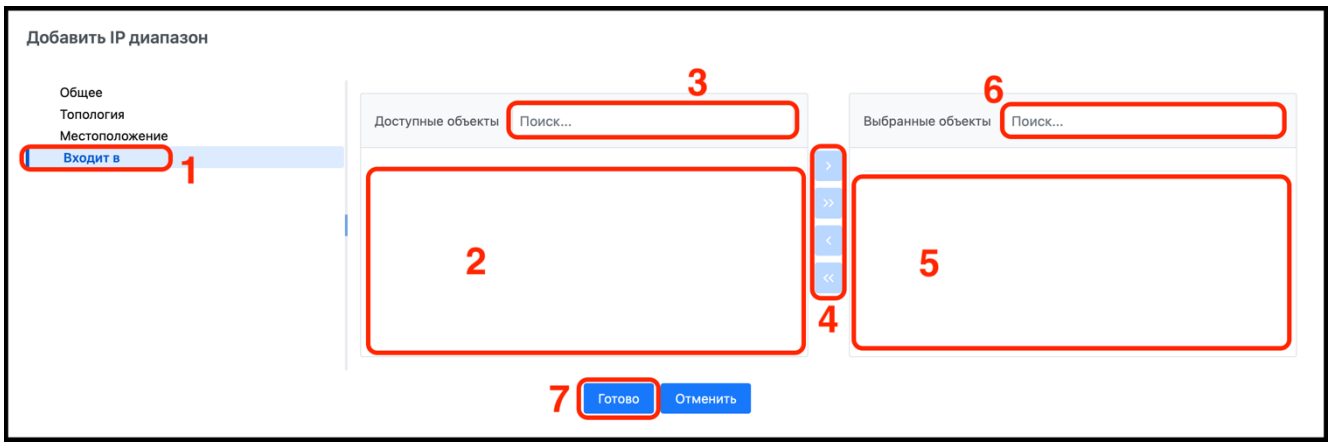


Рисунок 194 – Настройка окна «Входит в» объекта типа «IP-диапазон»

В окне элемента списка «Входит в» (цифра 1) выбрать требуемый для вхождения в группу объект в поле «Доступные объекты» (цифра 2) или найти его, используя поисковую строку (цифра 3). Выбрать требуемый объект для создания группы в поле «Выбранные объекты» (цифра 5) или найти его, используя поисковую строку (цифра 6). Переместить требуемый объект в необходимые группы или разгруппировать объекты можно с помощью инструментов перемещения (цифра 4). Выполнив все требуемые настройки, необходимо нажать кнопку «Готово» (цифра 7).

В результате в рабочей области топологии будет добавлен и настроен объект типа «IP-диапазон», как изображено на рисунке (см. Рисунок 195).

Рисунок 195 – Вид окна топологи с добавленным объектом типа «IP-диапазон»

7.1.3 Добавление и настройка объекта типа «IP-хост»

Для добавления объекта типа «IP-хост» необходимо перейти в контекстное меню, как представлено в подразделе 7.1, и выбрать команду «Добавить IP-хост» и начать настройку.

7.1.3.1 Настройка параметров для элемента списка «Общее»

В открывшемся окне «Добавить IP-хост», выполнить шаги, изображенные на рисунке (см. Рисунок 196).

Рисунок 196 – Настройка объекта типа «IP-хост»

В окне настроек «Добавить IP-хост» (цифра 1) в элементе списка «Общее» (цифра 2) необходимо заполнить форму (цифра 3):

— имя объекта;

— описание (при необходимости);

— выбрать домен из выпадающего списка.

7.1.3.2 Настройка параметров для элемента списка «Сетевые параметры»

В окне элемента списка «Сетевые параметры» выполнить шаги, изображенные на рисунке (см. Рисунок 197).

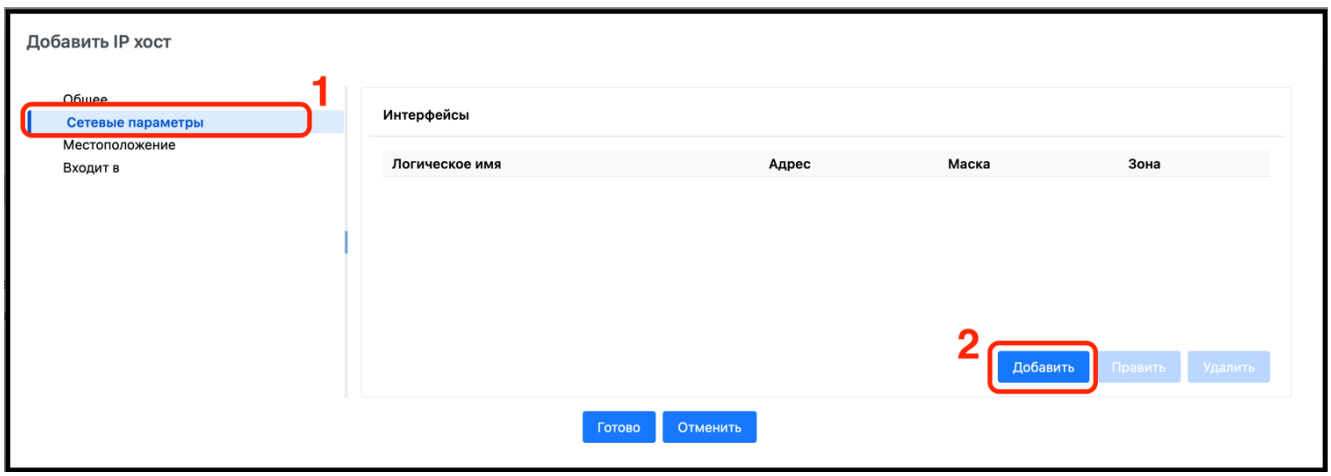


Рисунок 197 – Настройка топологии объекта типа «IP-хост»

В окне «Сетевые параметры» (цифра 1) нажать кнопку «Добавить» (цифра 2).

В открывшемся окне настроек выполнить шаги, изображенные на рисунке (см. Рисунок 198).

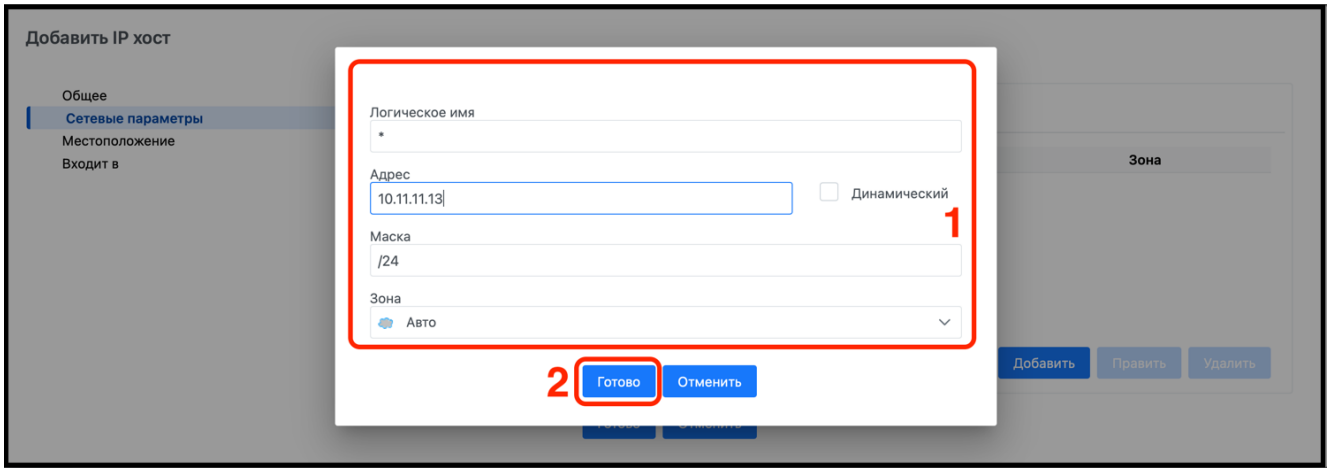


Рисунок 198 – Настройка объекта типа «IP-хост»

Заполнить данные настроечного блока (цифра 1) и нажать кнопку «Готово» (цифра 2).

В случае неверно введенных данных откроется окно, изображенное на рисунке (см. Рисунок 199), с предупреждением об ошибке.

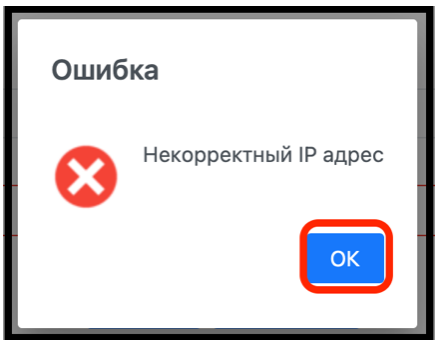


Рисунок 199 – Предупреждение об ошибке

7.1.3.3 Настройка параметров для элемента списка «Местоположение»

Перейти в элемент списка «Местоположение» в открывшемся окне выполнить шаги, изображенные на рисунке (см. Рисунок 200).

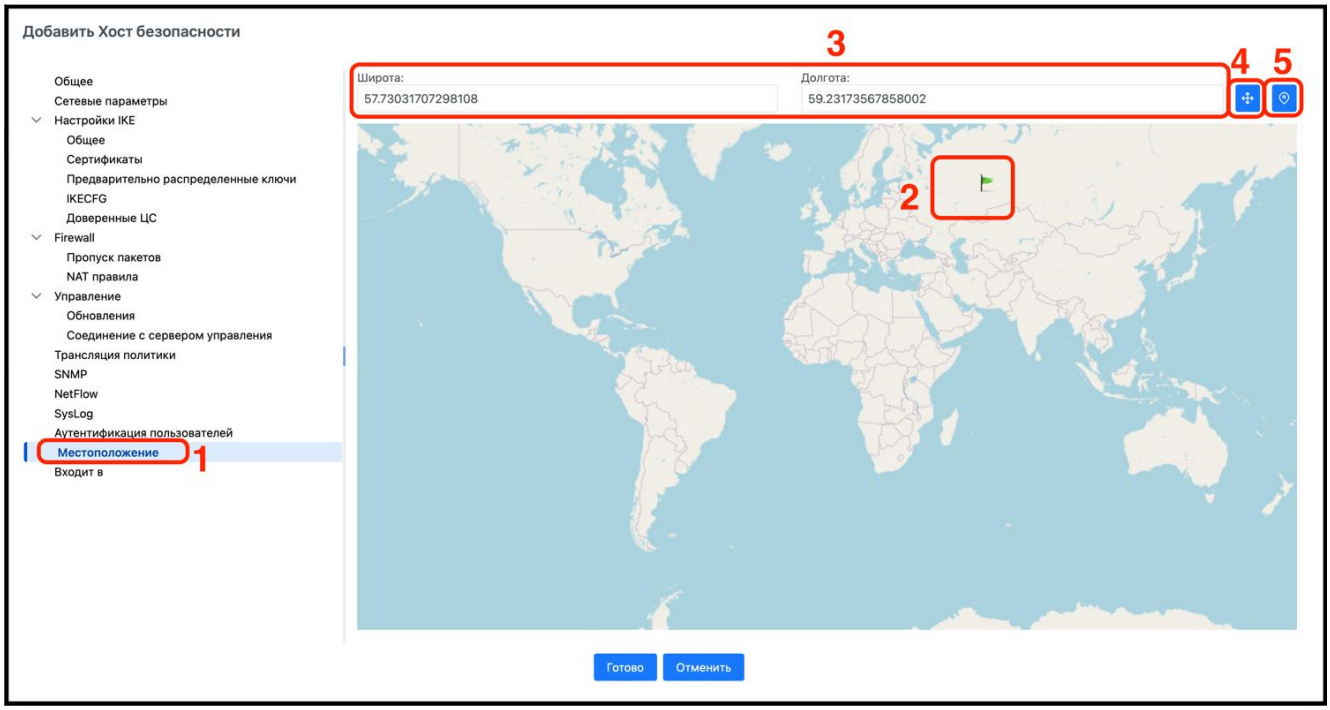


Рисунок 200 – Настройка местоположения объекта типа «IP-хост»

В окне элемента списка «Местоположение» (цифра 1) на карте разместить указатель мыши в требуемом месте и нажать левой клавишей мыши, установив флажок объекта (цифра 2). Также разместить объект на карте можно, указав широту и долготу нужного местоположения в строке координат (цифра 3). В результате выполненных действий флажок переместится в заданную точку. С помощью элемента «» «Показать на карте» (цифра 4) флажок окажется в центре карты. С помощью элемента «» можно найти географические координаты местоположения объекта, если в его настройках включена передача геолокации (цифра 5).

7.1.3.4 Настройка параметров для элемента списка «Входит в»

Перейти в элемент списка «Входит в», в открывшемся окне выполнить шаги, изображенные на рисунке (см. Рисунок 194).

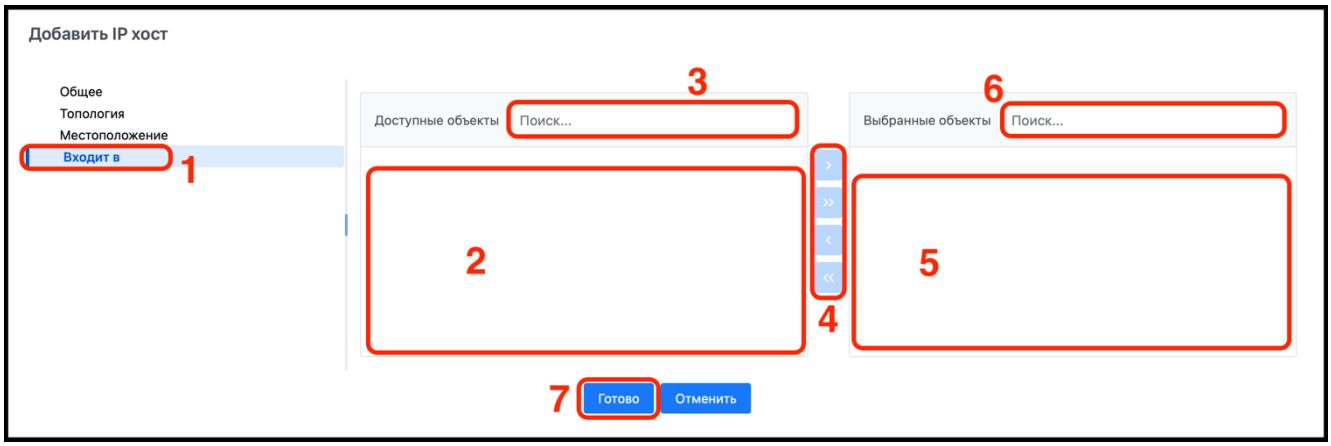


Рисунок 201 – Настройка окна «Входит в» объекта типа «IP-хост»

В окне элемента списка «Входит в» (цифра 1) выбрать требуемый для вхождения в группу объект в поле «Доступные объекты» (цифра 2) или найти его, используя поисковую строку (цифра 3). Выбрать требуемый объект для создания группы в поле «Выбранные объекты» (цифра 5) или найти его, используя поисковую строку (цифра 6). Переместить требуемый объект в необходимые группы или разгруппировать объекты можно с помощью инструментов перемещения (цифра 4). Выполнив все требуемые настройки, необходимо нажать кнопку «Готово» (цифра 7).

В результате в рабочей области элемента списка «Топология» будет добавлен объект типа «IP-хост» как изображено на рисунке (см. Рисунок 202).

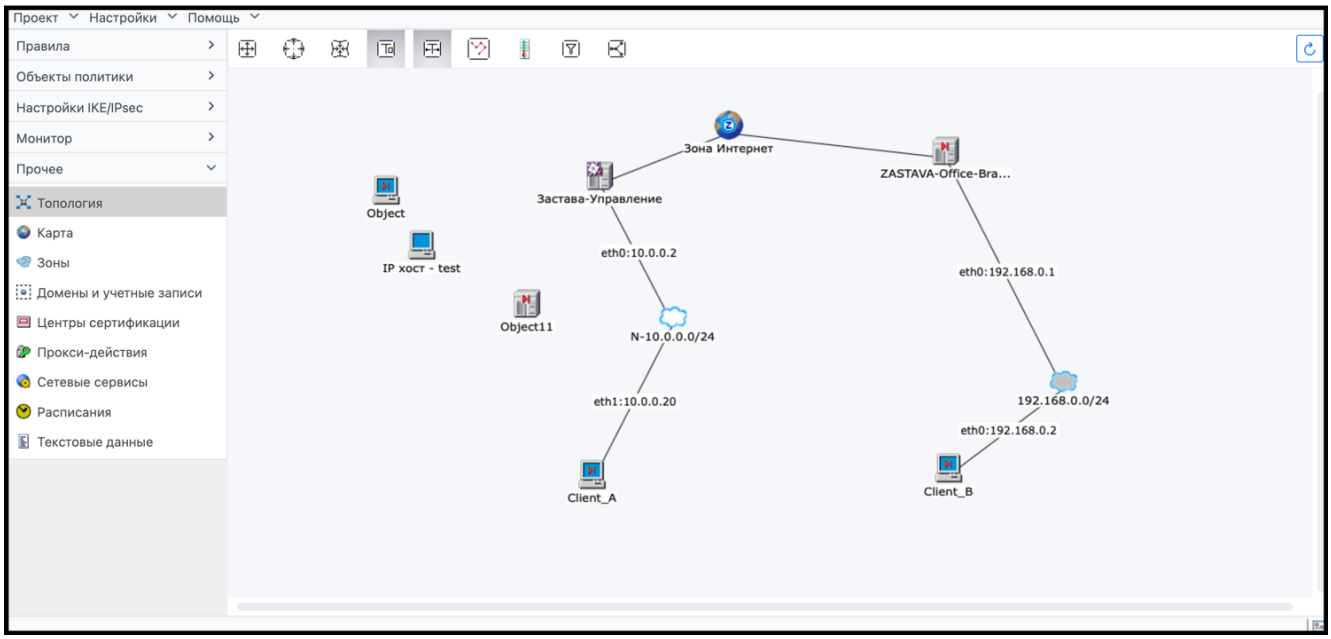


Рисунок 202 – Вид рабочей области элемента списка «Топология» с добавленным объектом типа «IP-хост»

7.1.4 Добавление и настройка объекта типа «Хост безопасности»

Хост безопасности — это компьютер с установленным агентом и фиксированным IP-адресом, с которого можно установить защищенное соединение с сетевыми узлами.

Хосты безопасности могут быть управляемыми « », в этом случае их ЛПБ создается ПО ЗУ, или неуправляемыми « ».

Для добавления объекта типа «Хост безопасности» необходимо перейти в контекстное меню, как представлено в подразделе 7.1, и выбрать команду «Добавить хост безопасности». В результате откроется окно «Выберите версию агента», где необходимо выбрать требуемую версию агента. Вид окна «Выберите версию агента» изображен на рисунке (см. Рисунок 203).

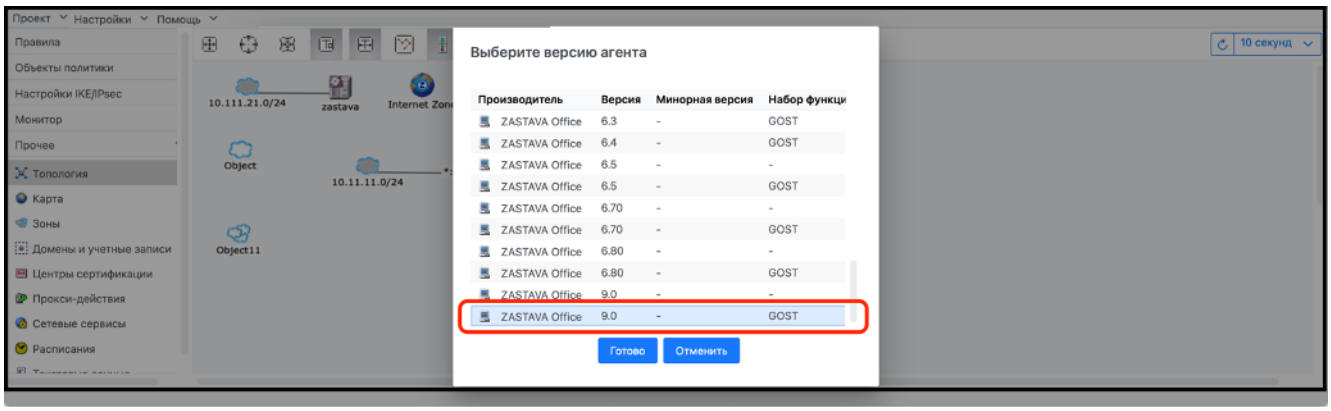


Рисунок 203 – Выбор версии агента

7.1.4.1 Настройка параметров для элемента списка «Общее»

В открывшемся окне настроек «Добавить Хост безопасности», в элементе списка «Общее», требуется выполнить шаги, изображенные на рисунке (см. Рисунок 204).

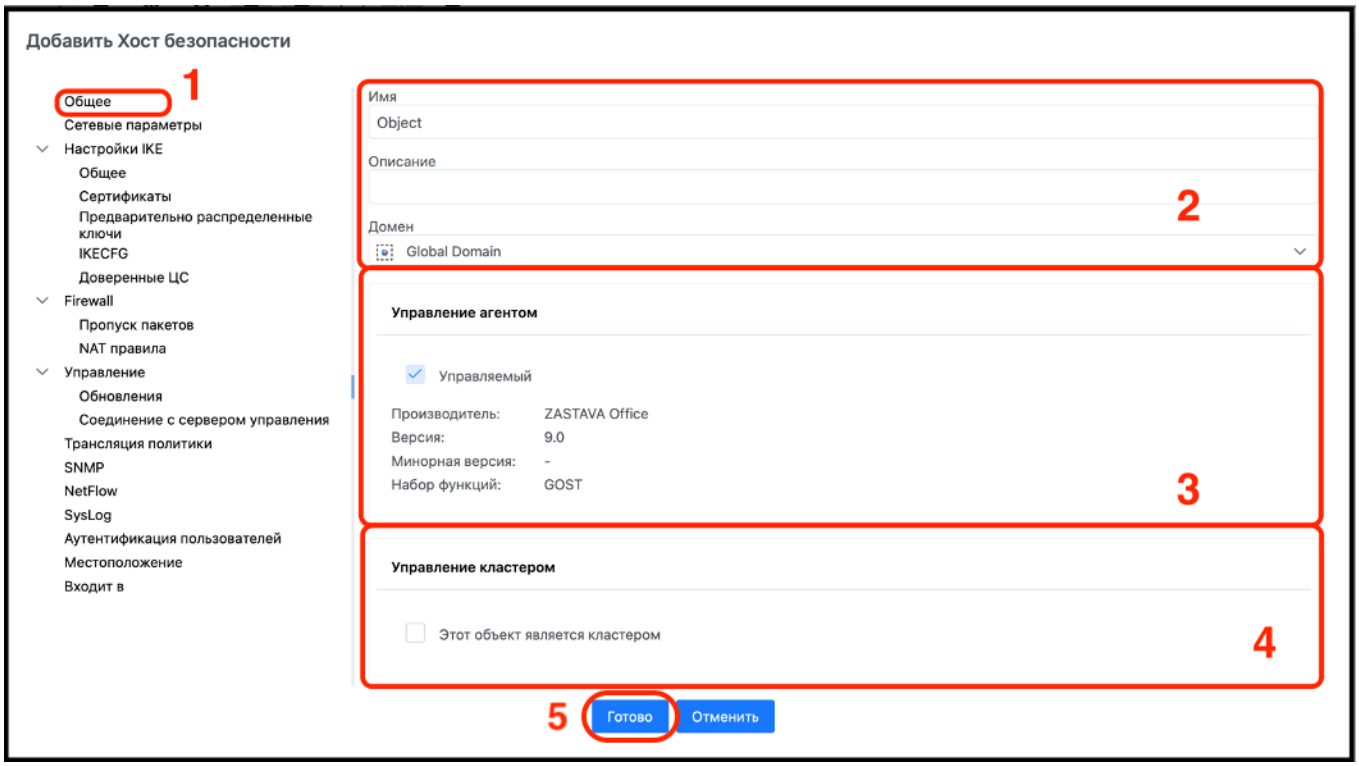


Рисунок 204 – Настройка объекта типа «Хост безопасности»

1) в окне элемента списка «Общее» (цифра 1) необходимо заполнить форму (цифра 2):
   - имя объекта;
   - описание (при необходимости);
   - выбрать домен из выпадающего списка;
2) выбрать вариант управления агентом (цифра 3). В случае прямого управления агентом необходимо установить флажок «Управляемый». В случае встречной работы с агентом, не находящимся под управлением, флажок снять (по умолчанию он снят);

3) определить управление кластером (цифра 4). В случае, если хост является кластером, необходимо установить флажок подтверждения;

4) нажать кнопку «Готово» (цифра 5).

В окне элемента списка «Сетевые параметры» выполнить шаги, изображенные на рисунке (см. Рисунок 205).

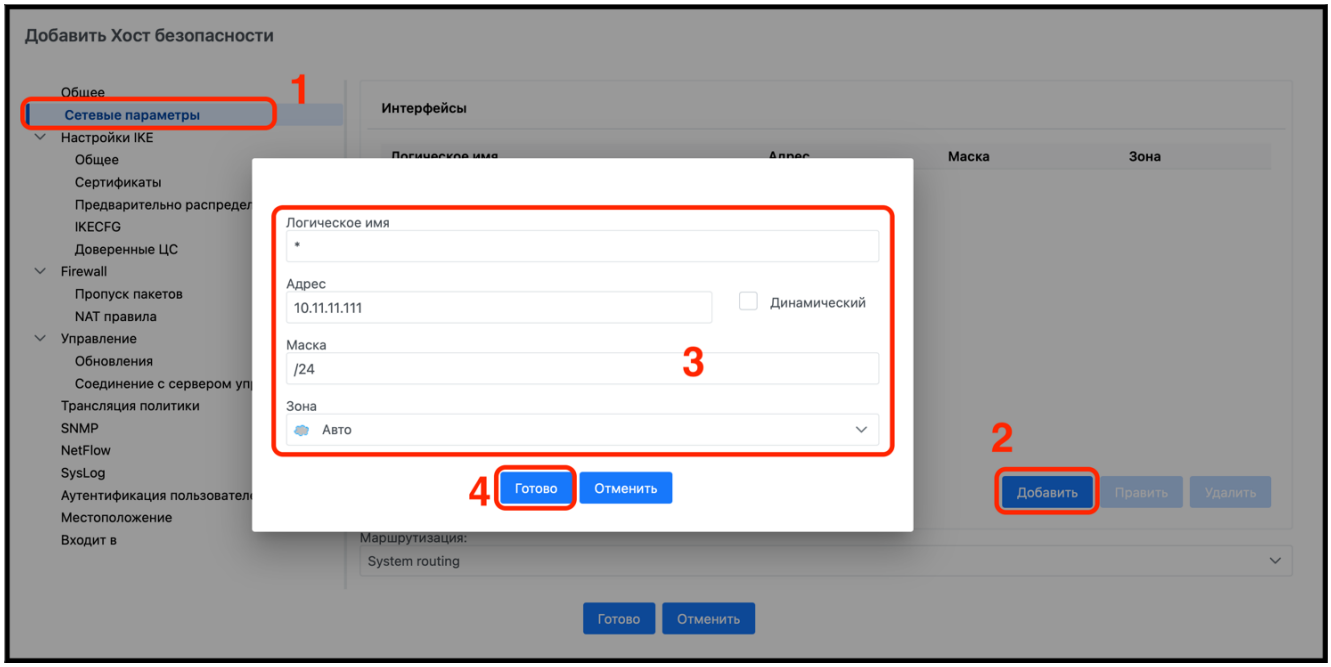


Рисунок 205 – Настройка объекта типа «Хост безопасности»

Перейти в элемент списка «Сетевые параметры» (цифра 1) и нажать кнопку «Добавить» (цифра 2). В открывшемся блоке настроек (цифра 3) заполнить данные:

— «Логическое имя»;

— «Адрес»;

— если требуется, установить флажок «Динамический»;

— внести параметры маски;

— выбрать из выпадающего списка требуемую зону.

Нажать кнопку «Готово» (цифра 4).

Повторить данную процедуру для всех используемых сетевых интерфейсов.

В случае неверно введенных данных откроется окно, изображенное на рисунке (см. Рисунок 206), с предупреждением об ошибке.

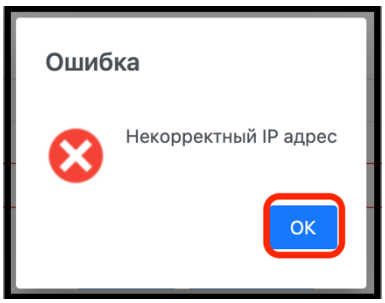


Рисунок 206 – Предупреждение об ошибке

7.1.4.2 Настройка параметров для элемента списка «Настройки IKE»

Перейти в элемент списка «Настройки IKE» и выполнить шаги, изображенные на рисунке (см. Рисунок 207).

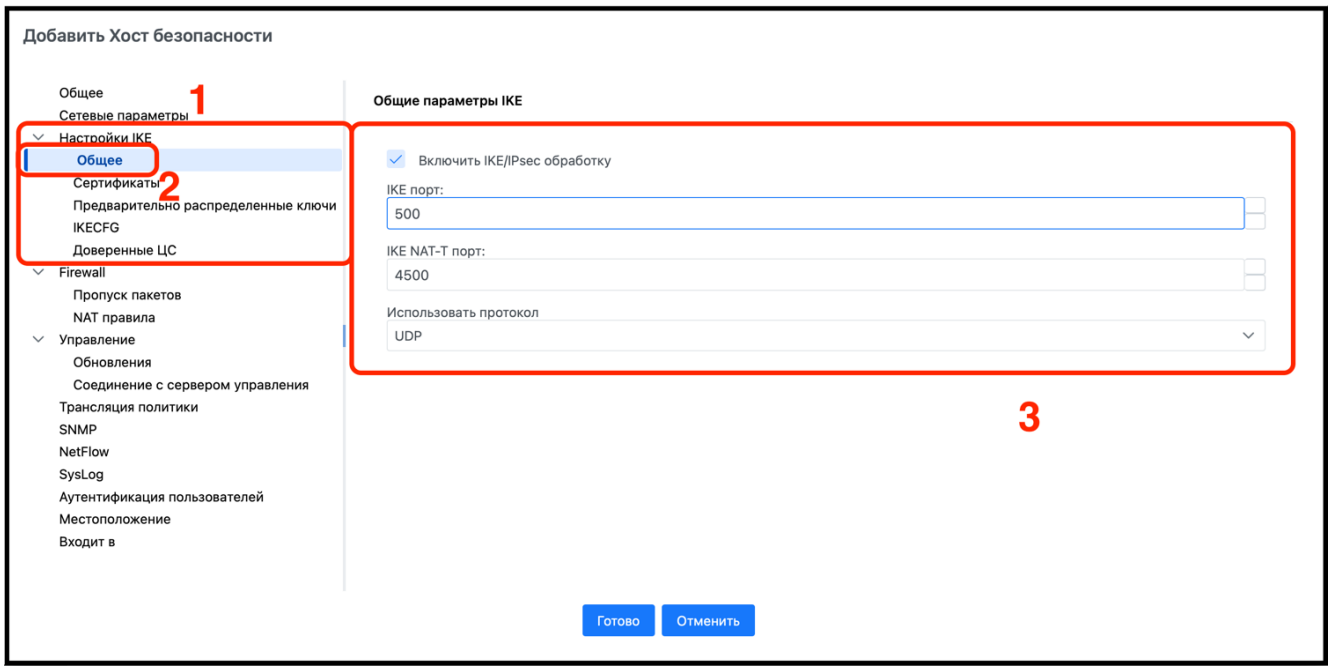


Рисунок 207 – Настройка общих параметров IKE

Перейти в элемент списка «Настройки IKE» (цифра 1) и в окне «Общее» (цифра 2) ввести требуемые параметры IKE (цифра 3):

- если нет необходимости, чтобы шлюз безопасности использовал протоколы IKE и IPsec, необходимо убрать отметку в поле «Включить IKE/IPsec обработку», которая установлена по умолчанию;
- в поле «IKE порт» указать порт, который будет использоваться шлюзом безопнасти;
- в поле «IKE NAT-T порт» указать порт, используемый шлюзом для работы протокола IKE-NAT-Traversal;
- выбрать в списке «Использовать протокол» вариант протокола.

В окне «Сертификаты» выполнить шаги, изображенные на рисунке (см. Рисунок 208).

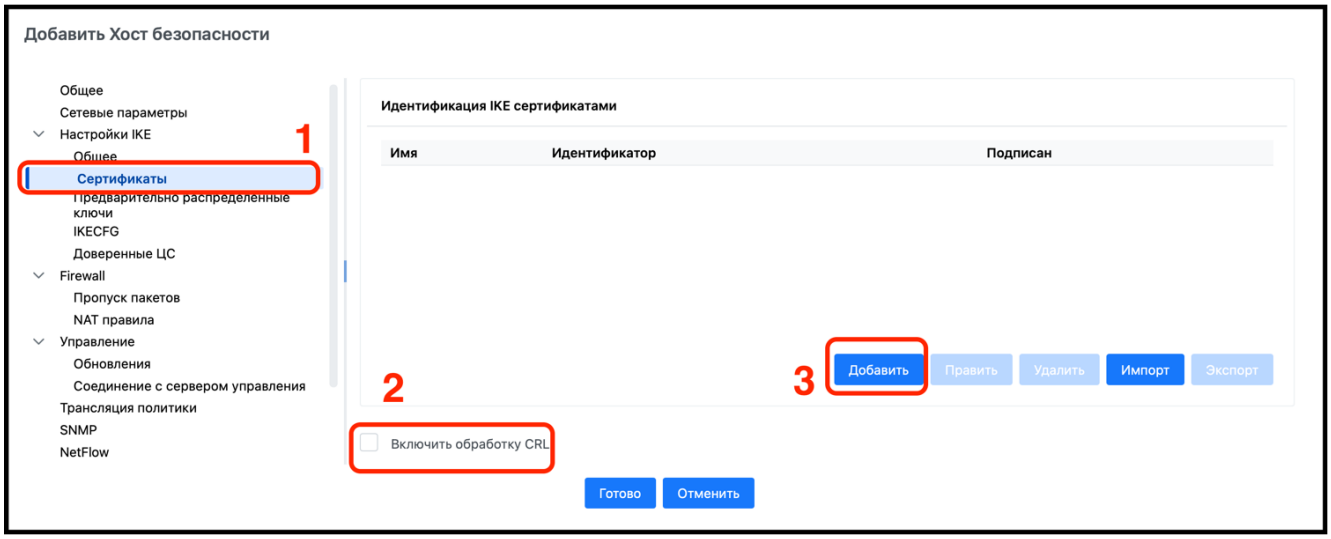


Рисунок 208 – Настройка IKE сертификатов

В окне «Сертификаты» (цифра 1) при необходимости включения обработки COC (CRL) (цифра 2) установить соответствующий флажок. Для добавления сертификата безопасности использовать кнопку «Добавить» (цифра 3).

В открывшемся окне настроек «Создать IKE сертификат» ввести описание сертификата, выполнив шаги, изображенные на рисунке (см. Рисунок 209). Подробное описание создания сертификатов представлено в п. 6.5.5.2.

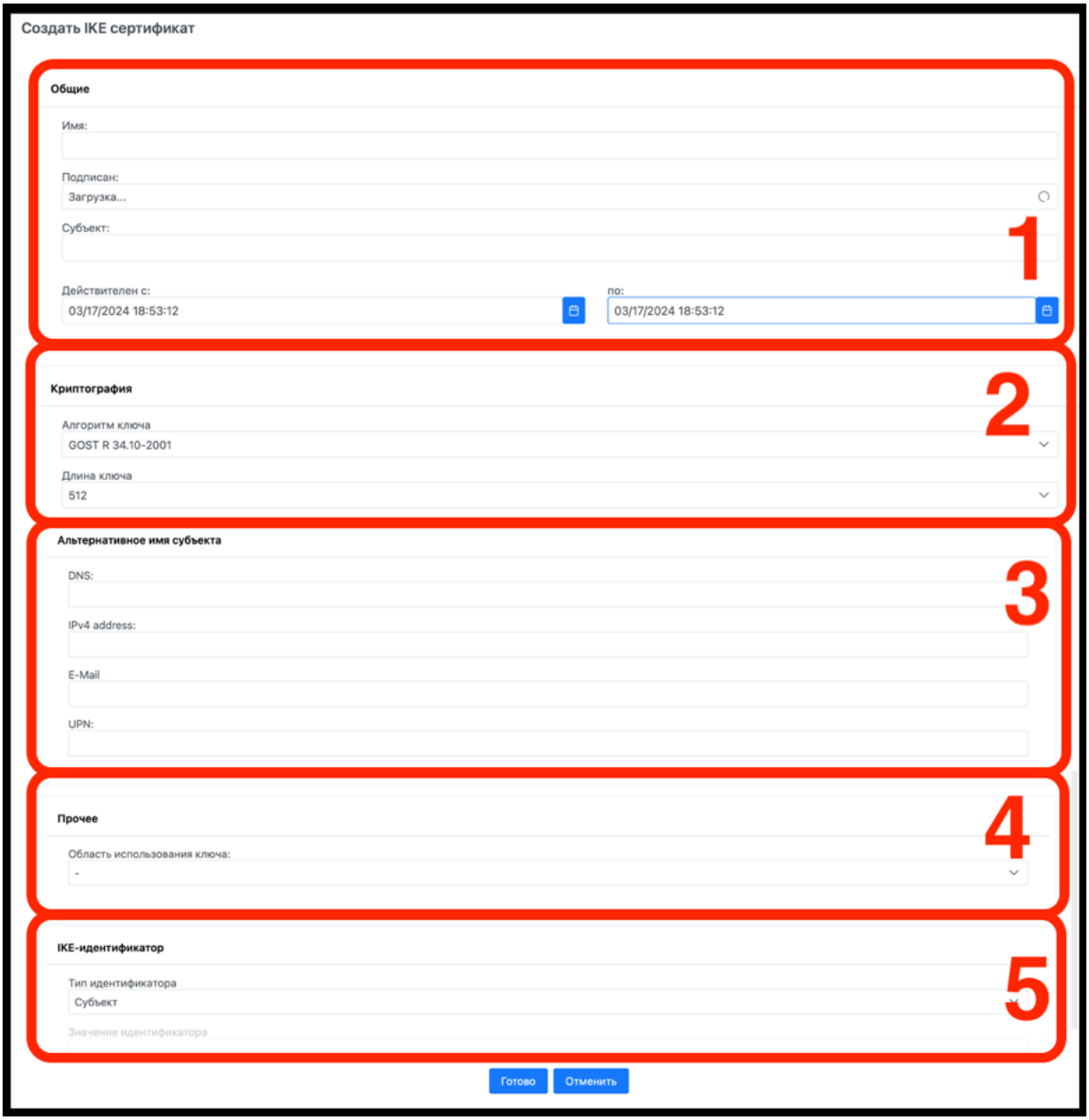


Рисунок 209 – Настройка IKE сертификатов

Заполнить требуемые поля в следующих блоках:

1) «Общие» (цифра 1): «Имя», «Подписан», «Субъект» «Действителен с» и «по»;
2) «Криптография» (цифра 2): «Алгоритм ключа», «Длина ключа»;
3) «Альтернативное имя субъекта» (цифра, 3): «DNS», «IPv4 address», «E-mail», «UPN»;
4) «Прочее» (цифра, 4): «Область использования ключа»;
5) «IKE идентификатор» (цифра 5): «Тип идентификатора», «Значение идентификатора»;

Нажать кнопку «Готово» (цифра 6).

В случае использования предварительно распределённых ключей требуется выполнить шаги, изображенные на рисунке (см. Рисунок 210).

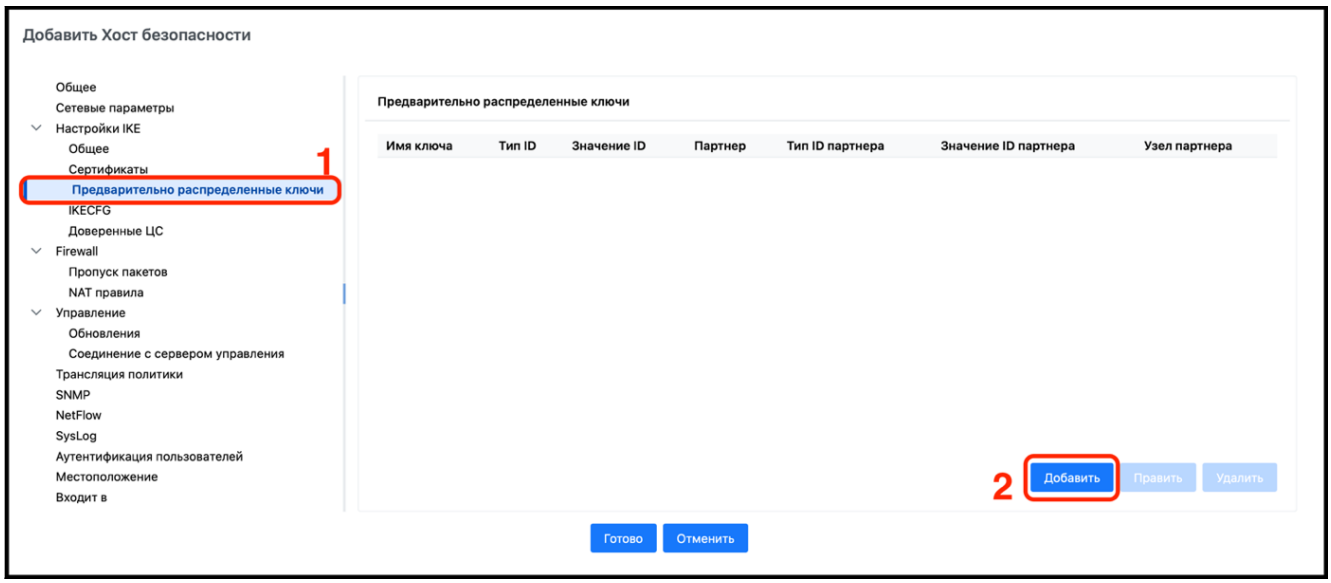


Рисунок 210 – Добавление предварительных распределенных ключей

В окне «Предварительно распределенные ключи» (цифра 1) нажать кнопку «Добавить» (цифра 2). В открывшемся окне настроек ввести требуемые параметры и добавить предраспределённый ключ. Окно настроек «Добавить предраспределённый ключ» представлено на рисунке (см. Рисунок 211).

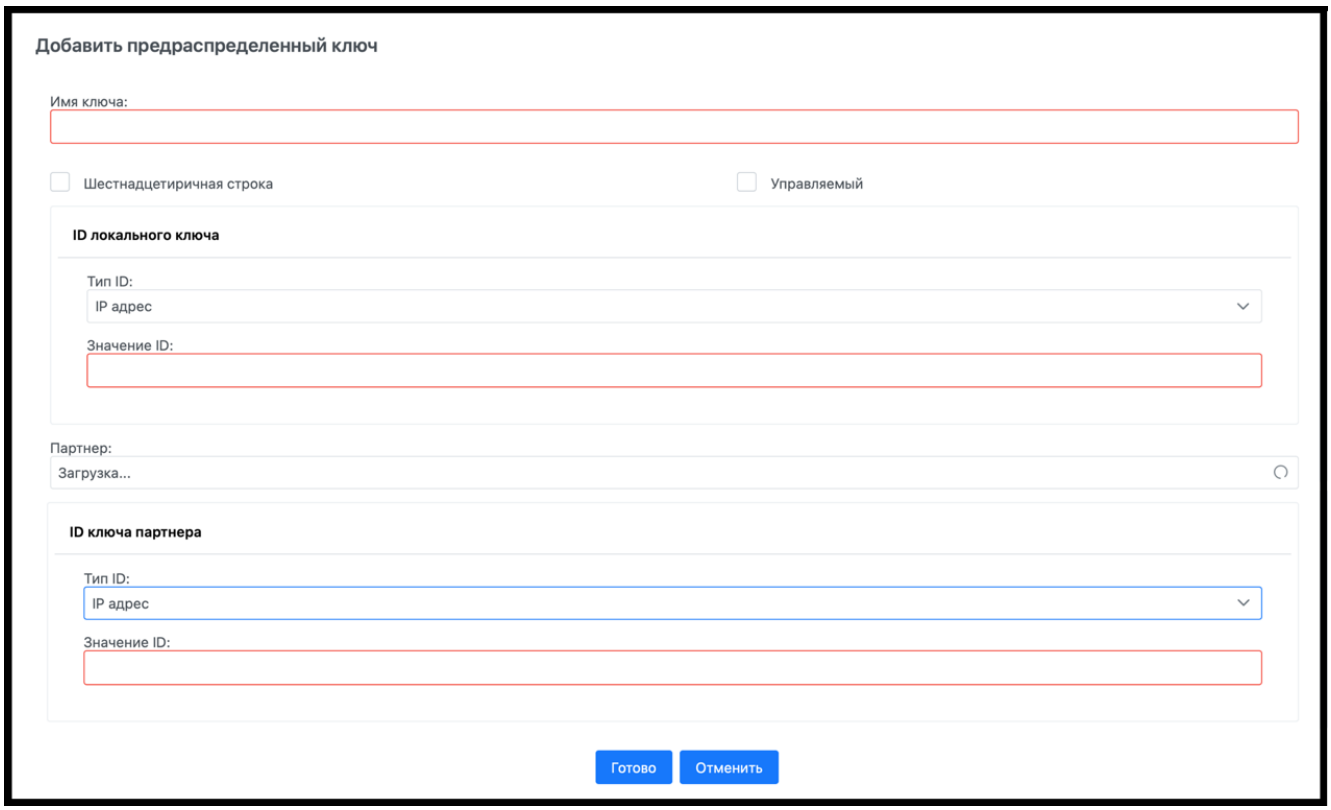


Рисунок 211 – Настройка параметров предраспределённого ключа

В окне настроек «Добавить предраспределённый ключ» выполнить настройки:

— в поле «Имя ключа» ввести имя. Это имя должно соответствовать имени предварительно распределенного ключа в «ЗАСТАВА-Офис» (см. Приложение 3), который представляет данный хост 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 настраиваемый 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 предварительно 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 поле «Значение ID».

В случае использования функций IKECFG перейти в настройки «IKECFG» и выполнить шаги, изображенные рисунке (см. Рисунок 212).

Рисунок 212 – Выбор варианта IKECFG

В окне «IKECFG» (цифра 1) выбрать вариант использования IKECFG (динамический или статический) (цифра 2) и нажать кнопку «Добавить» (цифра 3).

В случае выбора варианта «Динамический IKECFG» откроется окно настроек, изображенное на рисунке (см. Рисунок 213).

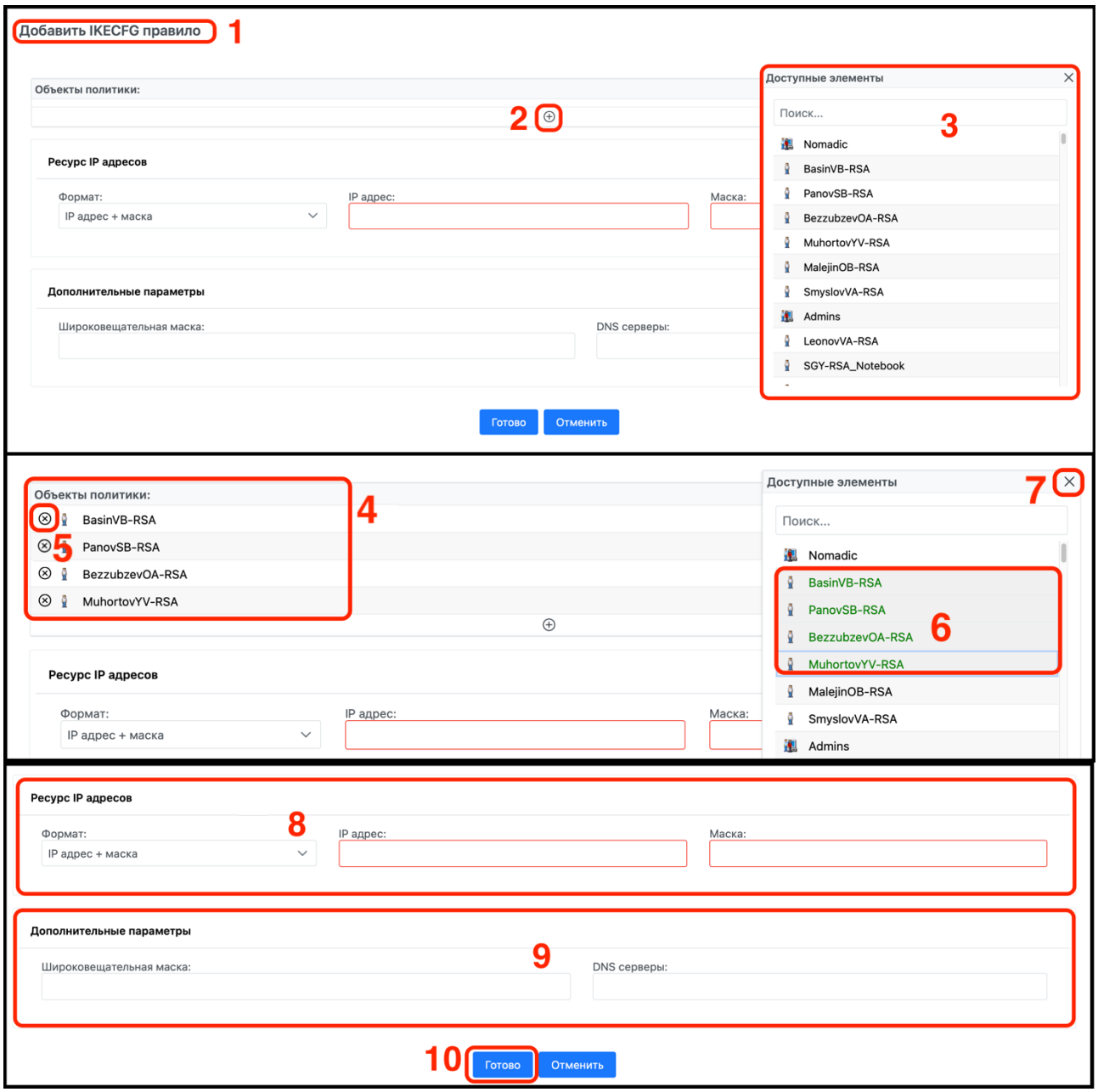


Рисунок 213 – Настройка варианта «Динамический IKECFG»

В окне «Добавить IKECFG правило» (цифра 1) необходимо произвести требуемые настройки:

1) нажать на элемент «⊕» (цифра 2), в открывшемся окне «Доступные элементы» (цифра 3) выбрать из списка требуемые объекты политики, к которым будет применяться протокол IKECFGЮ. Для выбора объекта требуется нажать на его строку, и он переместится в список «Объекты политики» (цифра 4). Удалить перемещенный объект из списка «Объекты политики» можно, нажав на элемент «⊗ ». В списке «Доступные элементы» перемещенные объекты окрасятся в зеленый цвет (цифра 6). Закрыть список «Доступные элементы» можно, нажав на элемент « ×» (цифра 7);

2) в блоке настроек (цифр 8) указать «Ресурс IP-адресов», находящийся за шлюзом безопасности, из которого будут браться IP-адреса для удаленных хостов безопасности / пользователей (агенты «ЗАСТАВА-Клиент»).

— из выпадающего списка «Формат» выбрать метод указания ресурса IP-адресов («IP-диапазон», «IP-адрес + маска» или «DHCP»). При выборе метода «DHCP» в качестве идентификатора агента «ЗАСТАВА-Клиент» будет направлен IP-адрес, выбранный DHCP-сервером, который первым ответит на запрос (DHCP REQUEST) шлюза безопасности. При обмене информацией с DHCP-сервером, с которым работает шлюз безопасности, запрашиваются следующие параметры: IP-адрес, subnet mask и broadcast addr, DNS;

— ввести в поле «IP-адрес»;

— указать маску;

3) в блоке настроек (цифр 9) «Дополнительные параметры» указать широковещательную маску и IP-адрес DNS-сервера;

4) нажать кнопку «Готово» (цифра 10).

В случае выбора варианта «Статический IKECFG» откроется окно настроек, изображенное на рисунке (см. Рисунок 214).

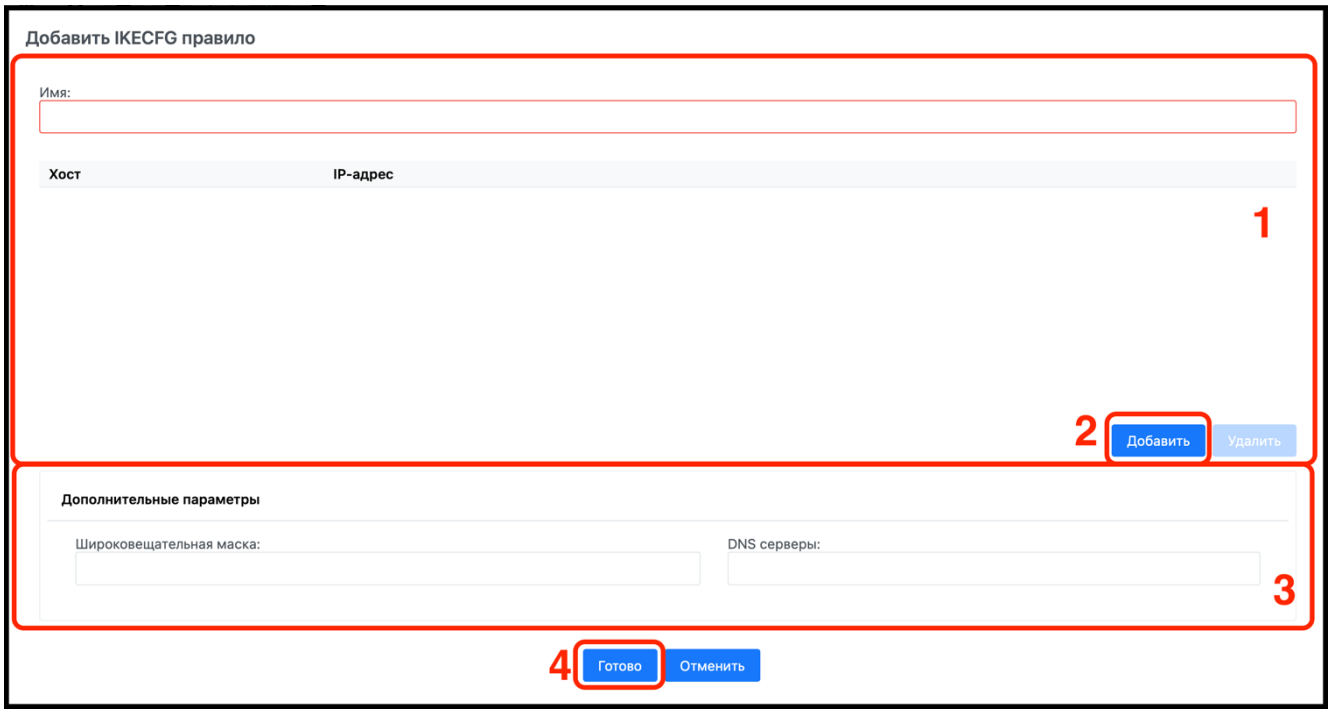


Рисунок 214 – Настройка варианта «Статический IKECFG»

В окне настроек «Добавить IKECFG правило» (цифра 1) необходимо назначить имя IKECFG правила, затем нажать кнопку «Добавить» (цифра 2) и ввести требуемые параметры хоста в блоке настроек «Дополнительные параметры» (цифра 3), затем нажать кнопку «Готово» (цифра, 4).

Для указания информации о ЦС необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 215).

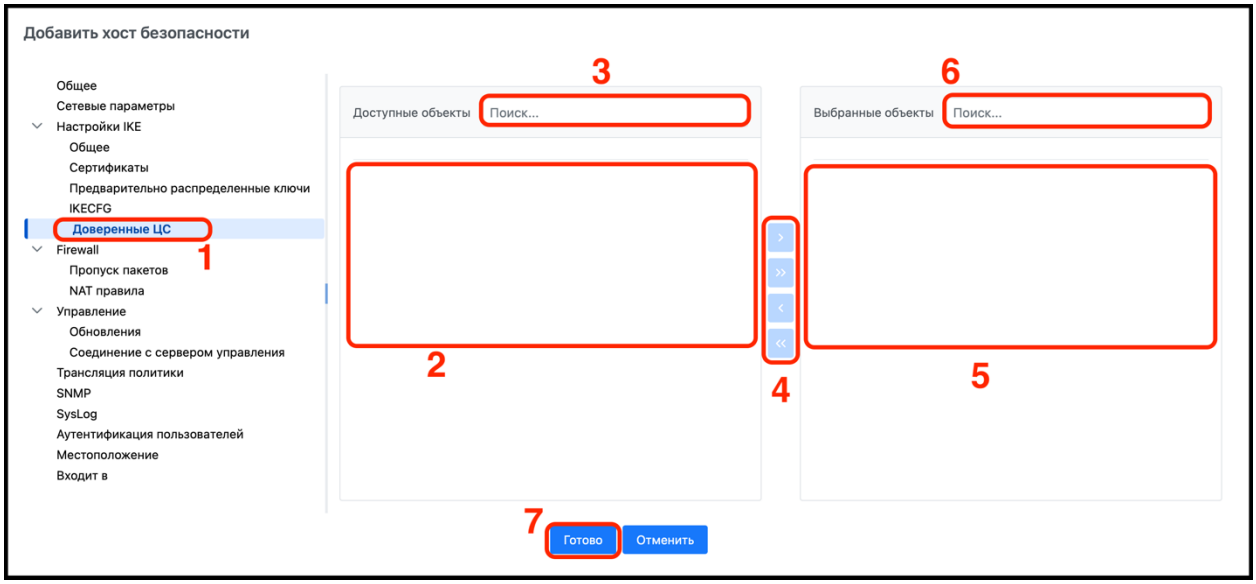


Рисунок 215 – Вид окна «Доверенные ЦС»

В окне «Доверенные ЦС» (цифра 1) выбрать требуемый для перемещения объект в поле «Доступные объекты» (цифра 2) или найти его, используя поисковую строку (цифра 3). Выбрать требуемый объект в поле «Выбранные объекты» (цифра 5) или найти его, используя поисковую строку (цифра 6). Переместить требуемый объект в необходимое поле можно с помощью инструментов перемещения (цифра 4). Выполнив все требуемые настройки, нажать кнопку «Готово» (цифра 7).

В результате всех выполненных действий будет произведена настройка для элемента списка «Настройки IKE».

7.1.4.3 Настройка параметров для элемента списка «Firewall»

Перейти в элемент списка «Firewall» (МЭ) в открывшемся окне выполнить шаги, изображенные на рисунке (см. Рисунок 216).

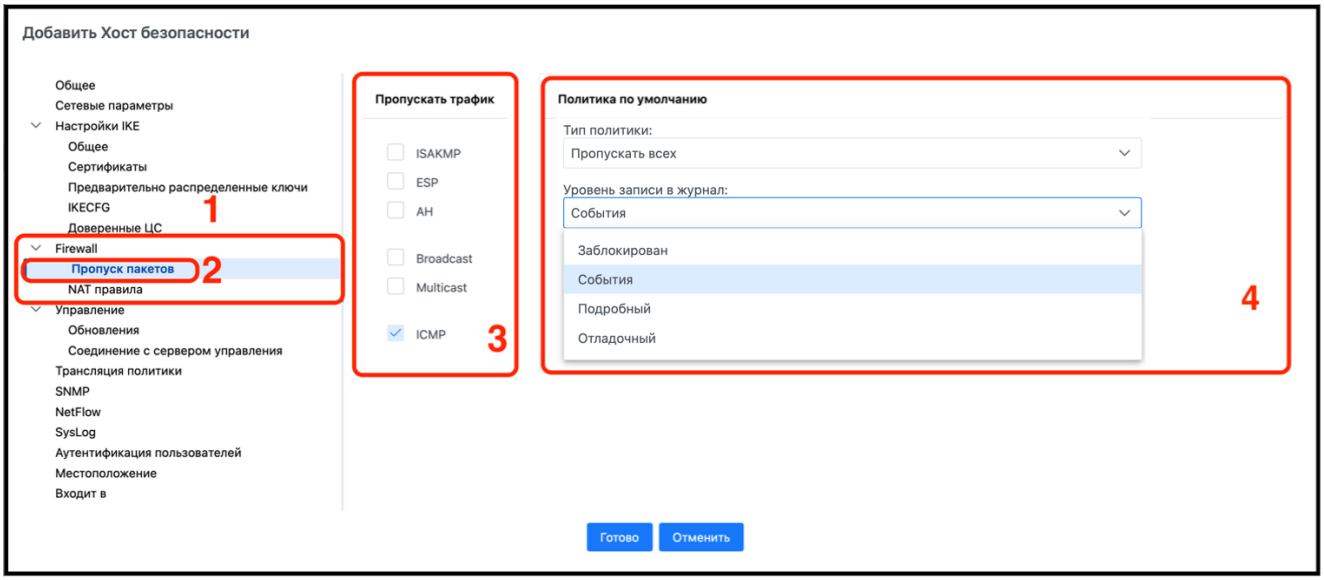


Рисунок 216 – Настройка «Пропуск пакетов»

Перейти в элемент списка «Firewall» (цифра 1), в окне «Пропуск пакетов» (цифра 2) в блоке «Пропускать трафик» установить флажок напротив требуемого значения (цифра 3). В блоке «Политика по умолчанию» выбрать в выпадающем списке тип политики и уровень записи в журнал (цифра 4).

При необходимости использования трансляции IP-адресов необходимо в элементе списка «NAT правила» выполнить шаги, изображенные на рисунке (см. Рисунок 217).

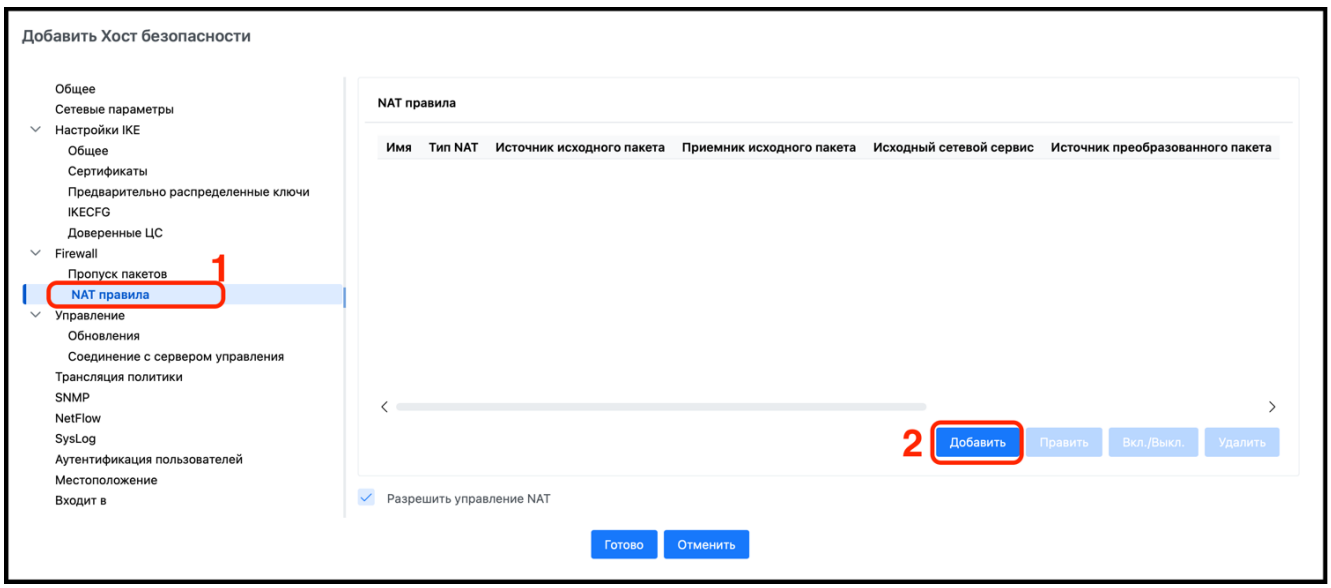


Рисунок 217 – Настройка «NAT правила»

В окне «NAT правила» (цифра 1) нажать кнопку «Добавить» (цифра 2).

В открывшемся окне настроек «Создать NAT правило» выполнить шаги, изображенные на рисунке (см. Рисунок 218).

Рисунок 218 – Настройка «NAT правила»

Заполнить общие данные (цифра 1), в блоке «Исходные пакеты» выбрать источник, приемник и сетевой сервис (цифра 2), в блоке «Преобразованные пакеты» также выбрать источник, приемник, сетевой сервис и интерфейс (цифра 3). Нажать кнопку «Готово» (цифра 4). Подробное описание создания NAT-правил представлено в п. 6.1.2.

В случае управляемого агента необходимо ввести соответствующие настройки в элементе списка «Управление»,

7.1.4.4 Настройка параметров для элемента списка «Управление»

В открывшемся окне «Управление» выполнив шаги, изображенные на рисунке (см. Рисунок 219).

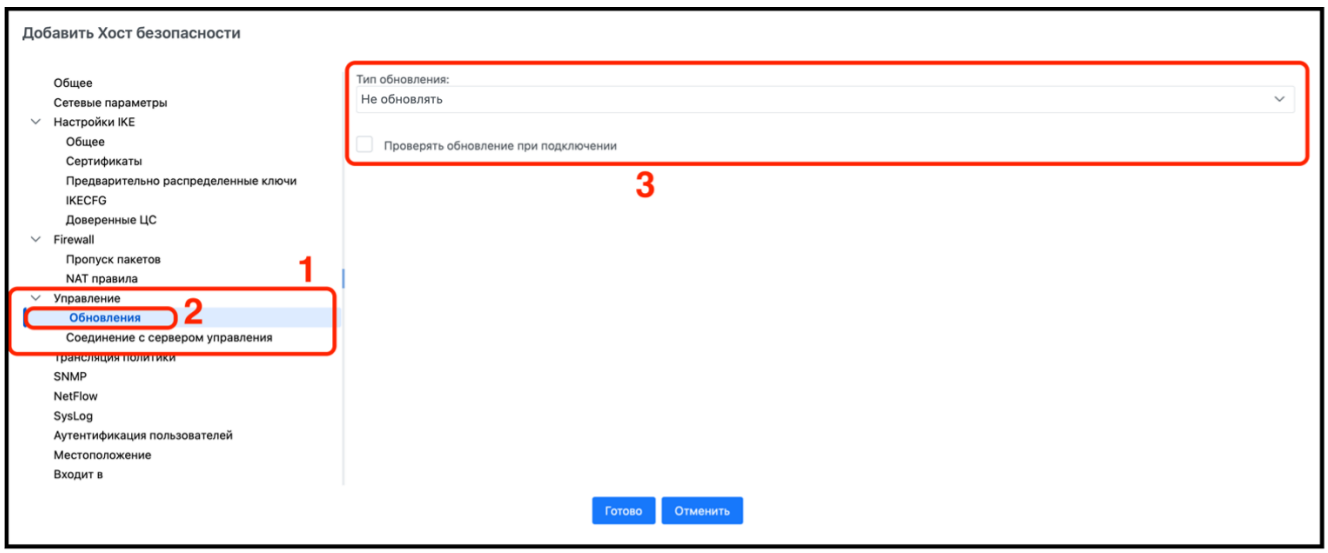


Рисунок 219 – Настройка окна «Обновление»

Перейти в элемент списка «Управление» (цифра 1), в окне «Обновление» (цифра 2) настроить параметры обновления агента (цифра 3).

Для настроек соединения с сервером управления необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 220).

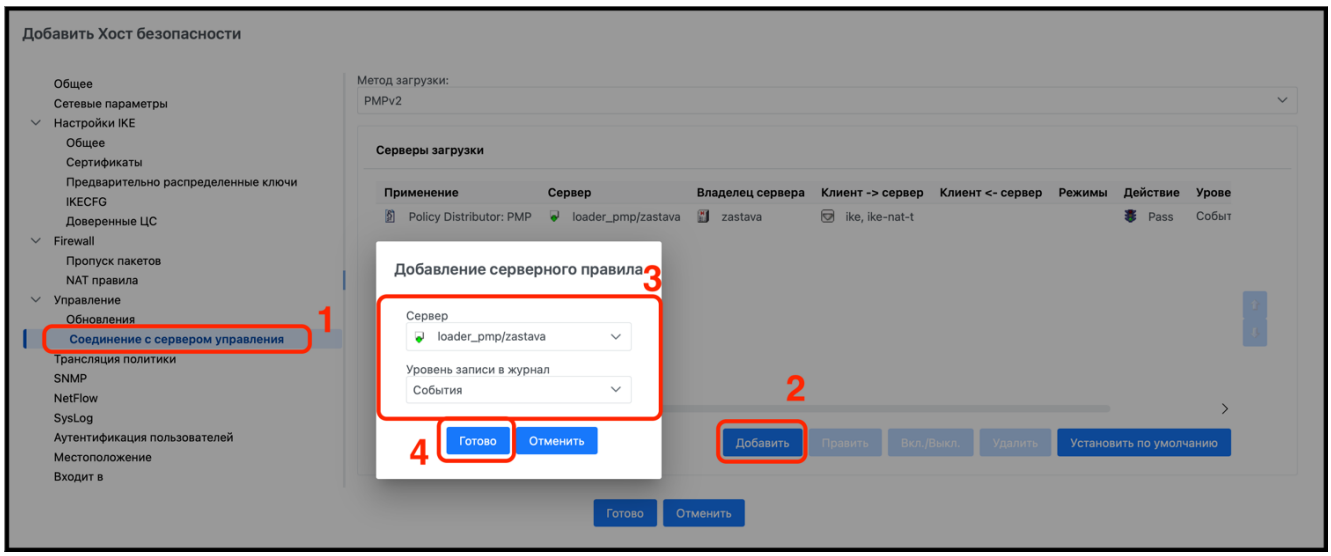


Рисунок 220 – Настройка «Соединение с сервером управления»

В окне «Соединение с сервером управления» (цифра 1) нажать кнопку «Добавить» (цифра 2). В открывшемся окне «Добавление серверного правила» выполнить настройки (цифра 3), затем нажать кнопку «Готово» (цифра 4).

7.1.4.5 Настройка параметров для элемента списка «Трансляция политики»

В случае необходимости добавления дополнительных параметров к автоматически создаваемой ЛПБ необходимо перейти в элемент списка «Трансляция политики» и выполнить шаги, изображенные на рисунке (см. Рисунок 221).

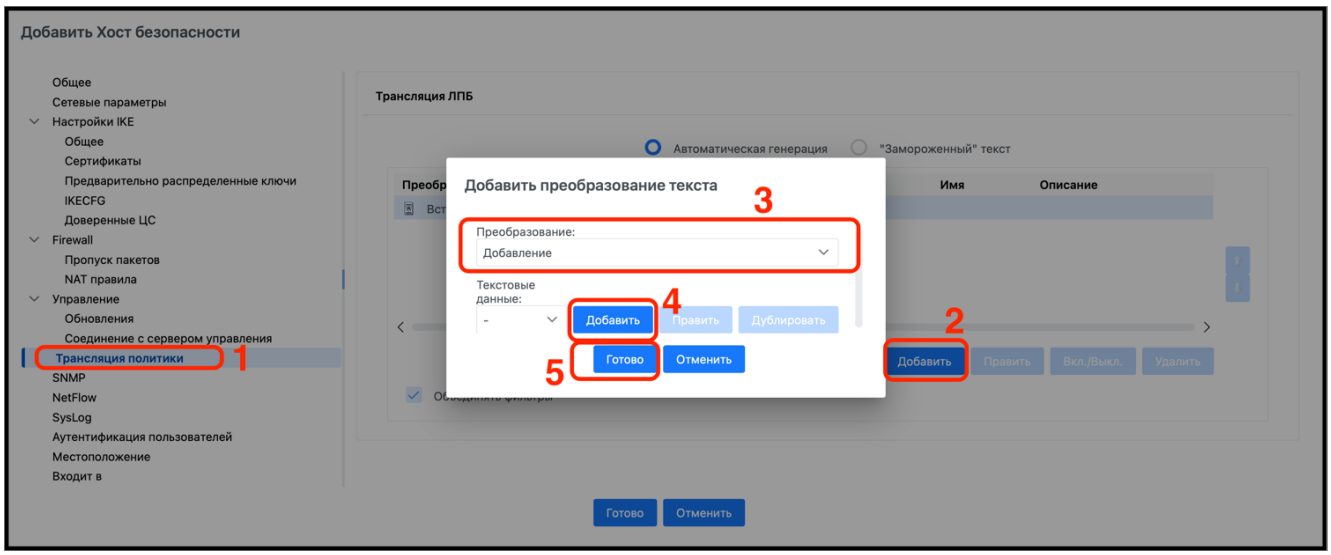


Рисунок 221 – Настройка «Трансляция политики»

Перейти в элемент списка «Трансляция политики» (цифра 1), нажать кнопку «Добавить» (цифра 2). В открывшемся окне «Добавить преобразование текста» в выпадающем списке выбрать вариант добавления (цифра 3), при необходимости с помощью кнопки «Добавить» (цифра 4) открыть дополнительное окно для ввода текстовых данных, затем нажать кнопку «Готово» (цифра 5).

7.1.4.6 Настройка параметров для элемента списка «SNMP»

В случае необходимости использования протокола SNMP для сбора статистики, необходимо перейти в элемент списка «SNMP» и выполнить шаги, изображенные на рисунке (см. Рисунок 222).

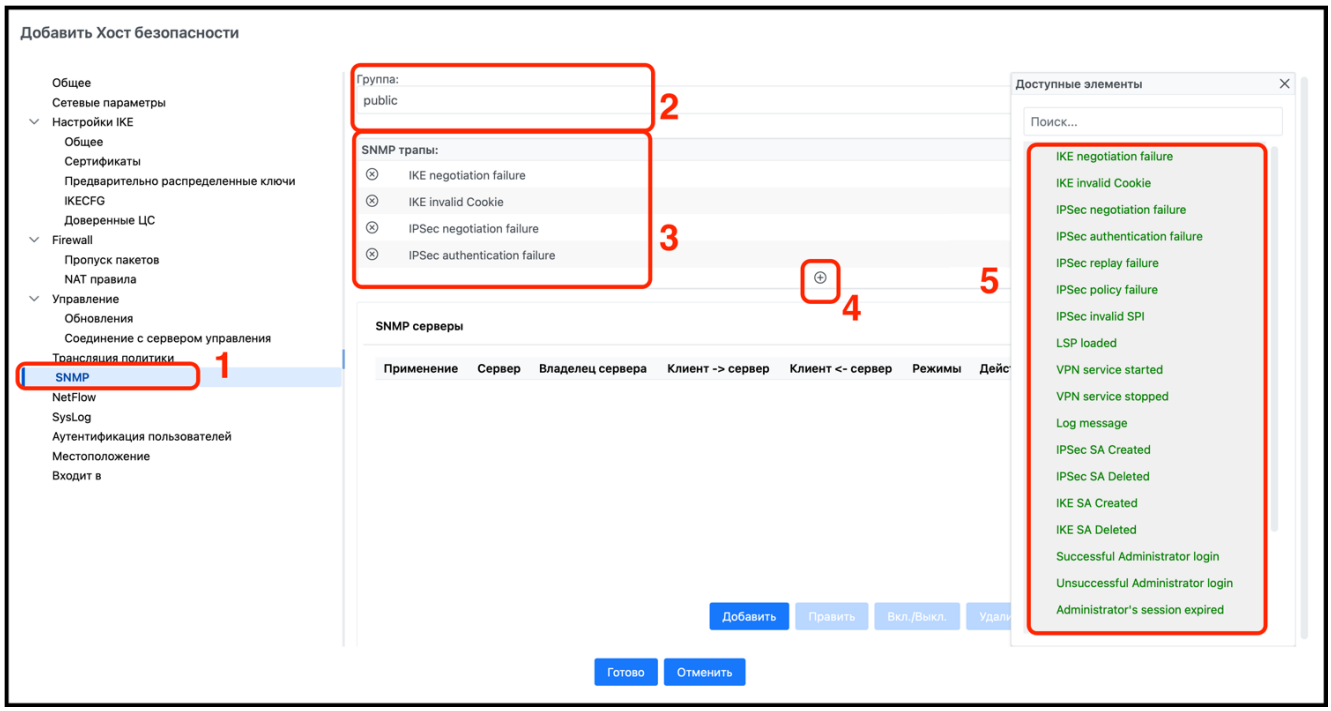


Рисунок 222 – Элемент списка «SNMP»

Перейти в элемент списка «SNMP» (цифра 1) и выбрать группу (цифра 2). По умолчанию используется порт SNMP-клиента 3454, а значение среды SNMP – public. При необходимости эти значения могут быть изменены в соответствующих полях. Все SNMP-сообщения должны содержать имя сообщества (community name), которое используется для аутентификации. Сообщения, содержащие имя сообщества, которое не установлено на «SNMP-клиент», не будут приняты. С помощью кнопки «+» (цифра 4) перенести сообщение из списка «Доступные элементы» (цифра 5) в SNMP-трапы (цифра 3). После перемещения элемент меняет цвет на зеленый (цифра 5). Весь список SNMP-сообщений представлен в п. 8.5.11.

Если необходимо, чтобы шлюз безопасности всегда пропускал SNMP-трафик без предварительной проверки правил ЛПБ, надо создать правило для пропуска SNMP-трафика, поступающего от шлюза безопасности на SNMP-сервер. Добавить для «SNMP» серверное правило можно, выполнив шаги, изображенные на рисунке (см. Рисунок 223).

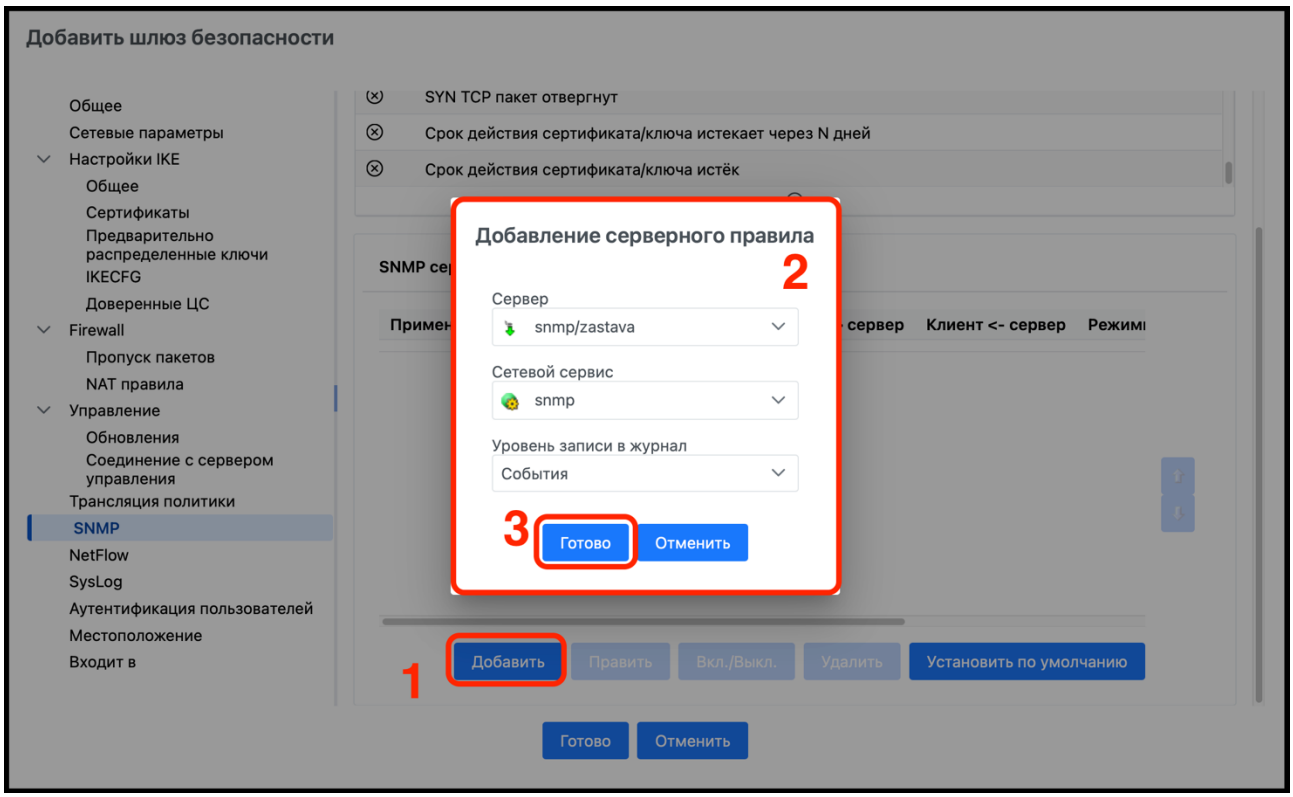


Рисунок 223 – Добавление серверного правила для «SNMP»

Нажать кнопку «Добавить» (цифра 1) и в открывшемся окне «Добавление серверного правила» выполнить настройки (цифра 2):

1) в выпадающем списке «Сервер» выбрать SNMP-сервер[9)], на который «ЗАСТАВА-Офис» (см. Приложение 3) будет отправлять SNMP-сообщения,
2) выбрать в списке сетевой сервис и уровень записи в журнал (доступны значения: «Отключен», «События», «Подробный», «Отладочный»),
3) затем нажать кнопку «Готово» (цифра 3).

7.1.4.7 Настройка параметров для элемента списка «NetFlow»

В случае необходимости использования протокола NetFlow необходимо перейти в элемент списка «NetFlow» в открывшемся окне выполнить шаги, изображенные на рисунке (см. Рисунок 224).

[9)] В списке будут отображаться те серверы, которые были предварительно зарегистрированы в окне «Серверы».

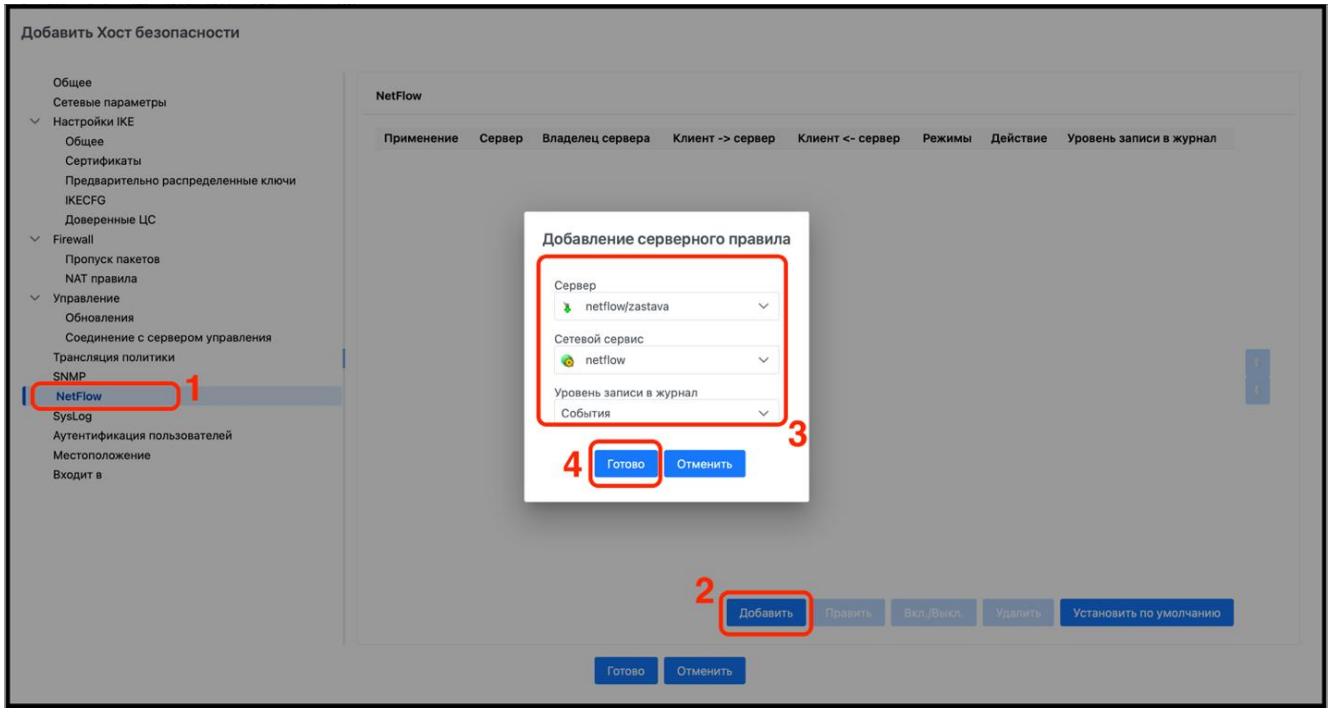


Рисунок 224 – Настройка элемента списка «NetFlow»

Перейти в элемент списка «NetFlow» (цифра 1), нажать кнопку «Добавить» (цифра 2), в открывшемся окне «Добавление серверного правила»:

1) выбрать NetFlow-сервер, на который «ЗАСТАВА-Офис» (см. Приложение 3) будет отправлять SNMP-сообщения. В списке будут отображаться те серверы, которые были предварительно зарегистрированы в окне «Серверы»;
2) выбрать сетевой сервис и уровень записи в журнал (доступны варианты: «Отключен», «События», «Подробный», «Отладочный») (цифра 3);
3) нажать кнопку «Готово» (цифра 4).

7.1.4.8 Настройка параметров для элемента списка «SysLog»

В случае необходимости использования внешнего SysLog-сервера необходимо перейти в элемент списка «SysLog» в открывшемся окне выполнить шаги, изображенные на рисунке (см. Рисунок 225).

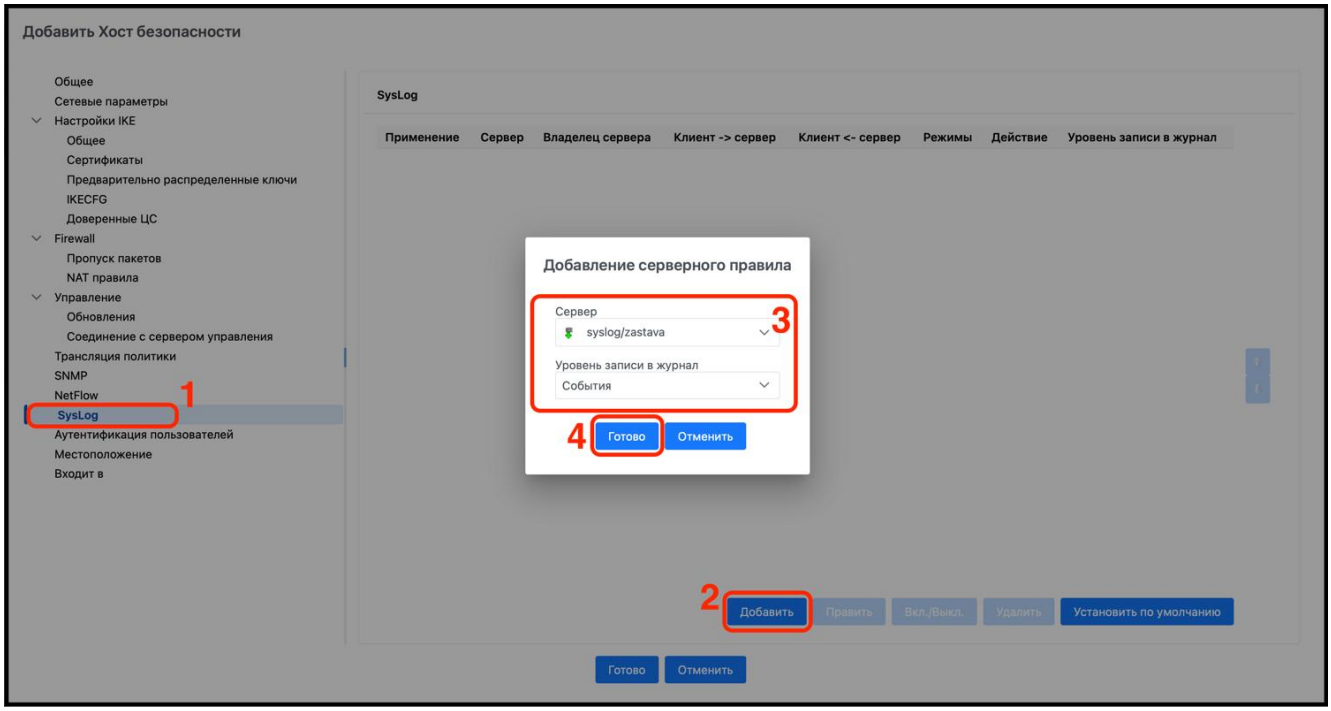


Рисунок 225 – Настройка элемента списка «SysLog»

Перейти в элемент списка «SysLog» (цифра 1), нажать кнопку «Добавить» (цифра 2), в открывшемся окне «Добавление серверного правила»:

1) выбрать SNMP-сервер, на которые «ЗАСТАВА-Офис» (см. Приложение 3) будет отправлять SNMP-сообщения. В списке будут отображаться те серверы, которые были предварительно зарегистрированы в окне «Серверы»;
2) выбрать уровень записи в журнал (доступны варианты: «Отключен», «События», «Подробный», «Отладочный») (цифра 3);
3) нажать кнопку «Готово» (цифра 4).

7.1.4.9 Настройка параметров для элемента списка «Аутентификация пользователей»

В элементе списка «Аутентификация пользователей» требуется выполнить шаги, изображенные на рисунке (см. Рисунок 226).

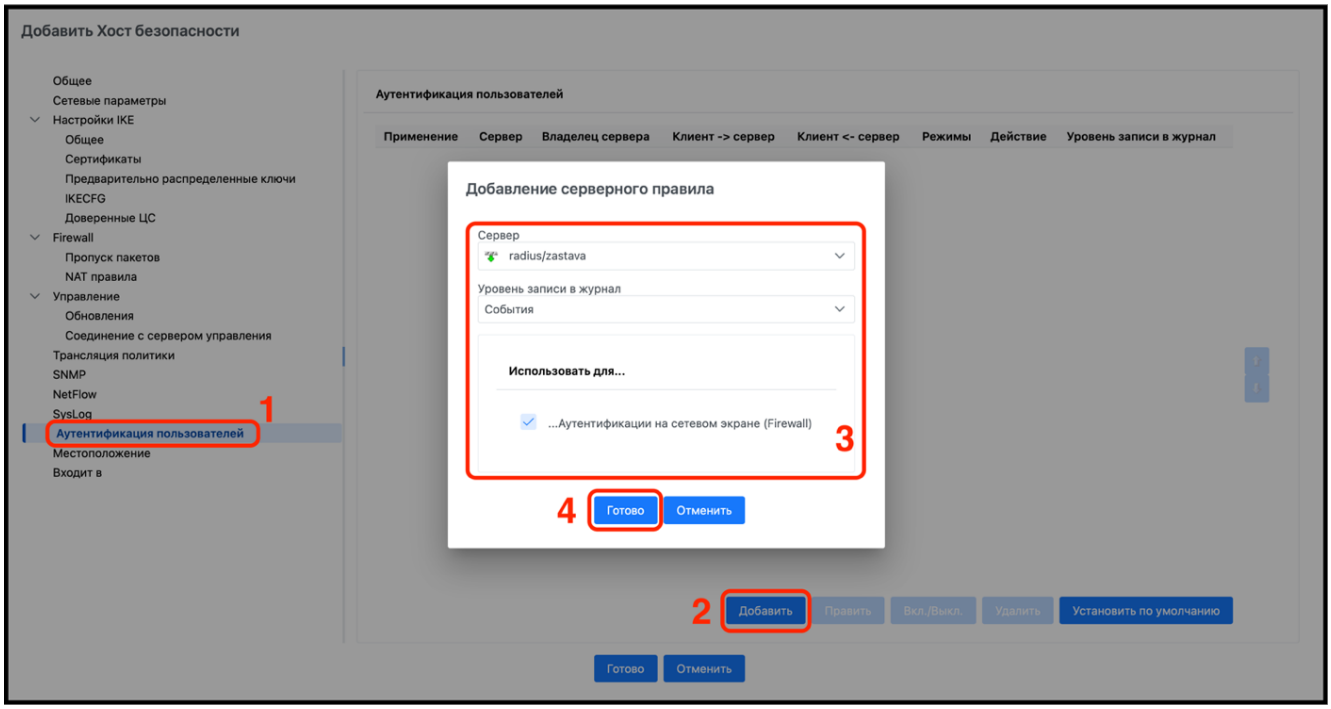


Рисунок 226 – Настройка элемента списка «Аутентификация пользователей»

Перейти в элемент списка «Аутентификация пользователей» (цифра 1), нажать кнопку «Добавить» (цифра 2), в открывшемся окне настроить параметры серверного правила[10)] (цифра 3), нажать кнопку «Готово» (цифра 4).

7.1.4.10 Настройка параметров для элемента списка «Местоположение»

Перейти в элемент списка «Местоположение» и выполнить шаги, изображенные на рисунке (см. Рисунок 227).

[10)] Перед настройкой параметров серверного правила удостоверится в наличии сервера аутентификации.

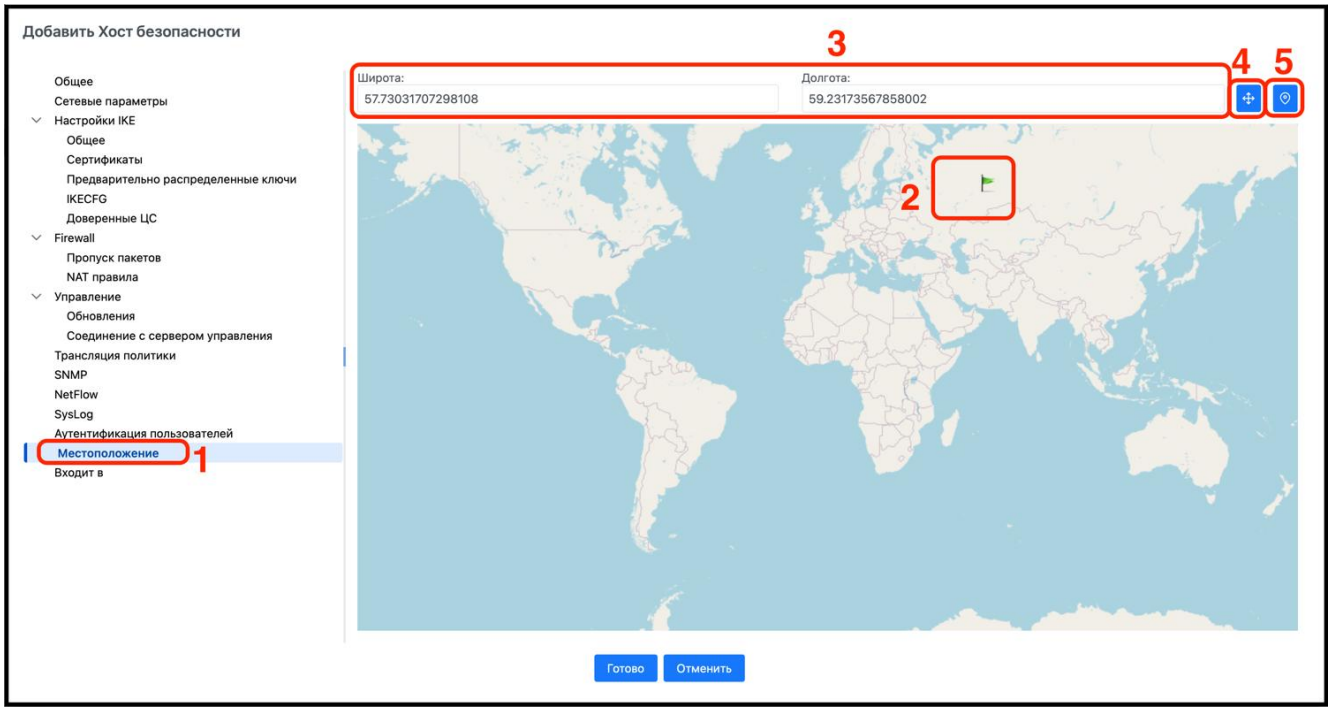


Рисунок 227 – Настройка элемента списка «Местоположение»

В окне элемента списка «Местоположение» (цифра 1) на карте разместить указатель мыши в требуемом месте и нажать левой клавишей мыши, установив флажок объекта (цифра 2). Также разместить объект на карте можно, указав широту и долготу нужного местоположения в строке координат (цифра 3). В результате выполненных действий флажок переместится в заданную точку. С помощью элемента «» «Показать на карте» (цифра 4) флажок окажется в центре карты. С помощью элемента «» можно найти географические координаты местоположения объекта, если в его настройках включена передача геолокации (цифра 5).

7.1.4.11 Настройка параметров для элемента списка «Входит в»

Перейти в элемент списка «Входит в» в открывшемся окне выполнить шаги, изображенные на рисунке (см. Рисунок 228).

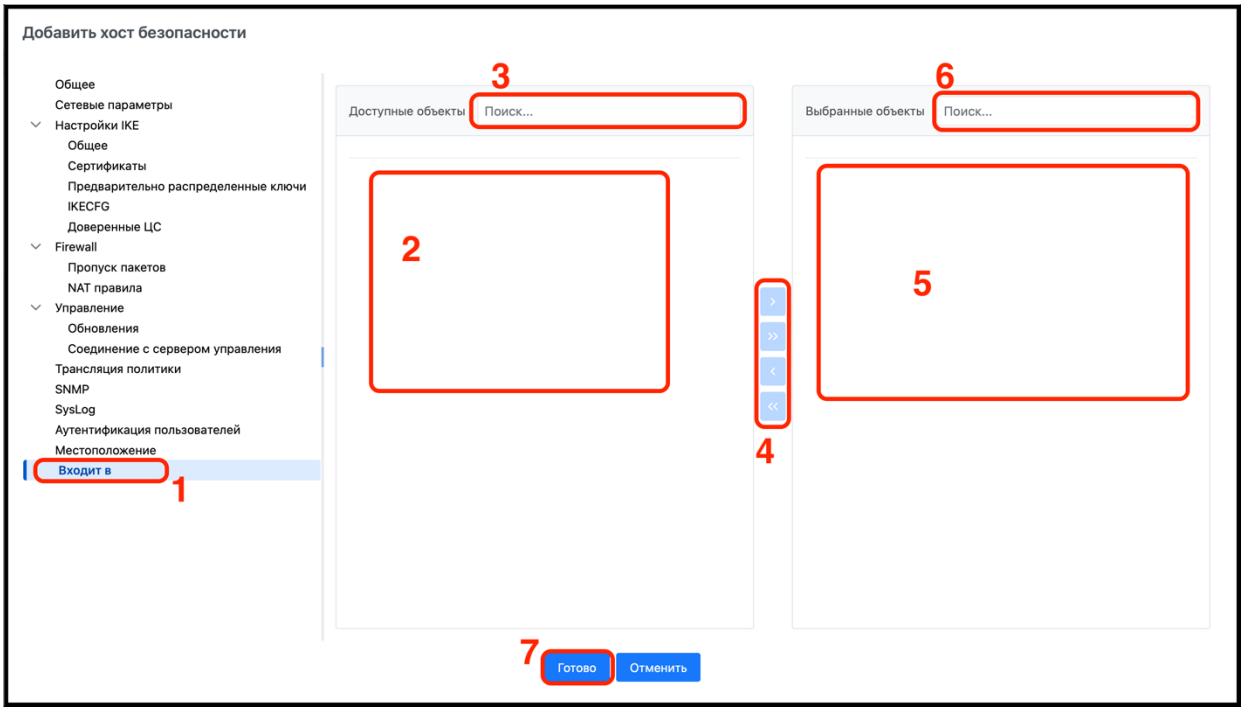


Рисунок 228 – Настройка «Входит в»

В окне элемента списка «Входит в» (цифра 1) выбрать требуемый для вхождения в группу объект в поле «Доступные объекты» (цифра 2) или найти его, используя поисковую строку (цифра 3). Выбрать требуемый объект для создания группы в поле «Выбранные объекты» (цифра 5) или найти его, используя поисковую строку (цифра 6). Переместить требуемый объект в необходимые группы или разгруппировать объекты можно с помощью инструментов перемещения (цифра 4). Выполнив все требуемые настройки, нажать кнопку «Готово» (цифра 7).

В результате в рабочей области элемента списка «Топология» добавится объект типа «Хост безопасности», изображенный на рисунке (см. Рисунок 229).

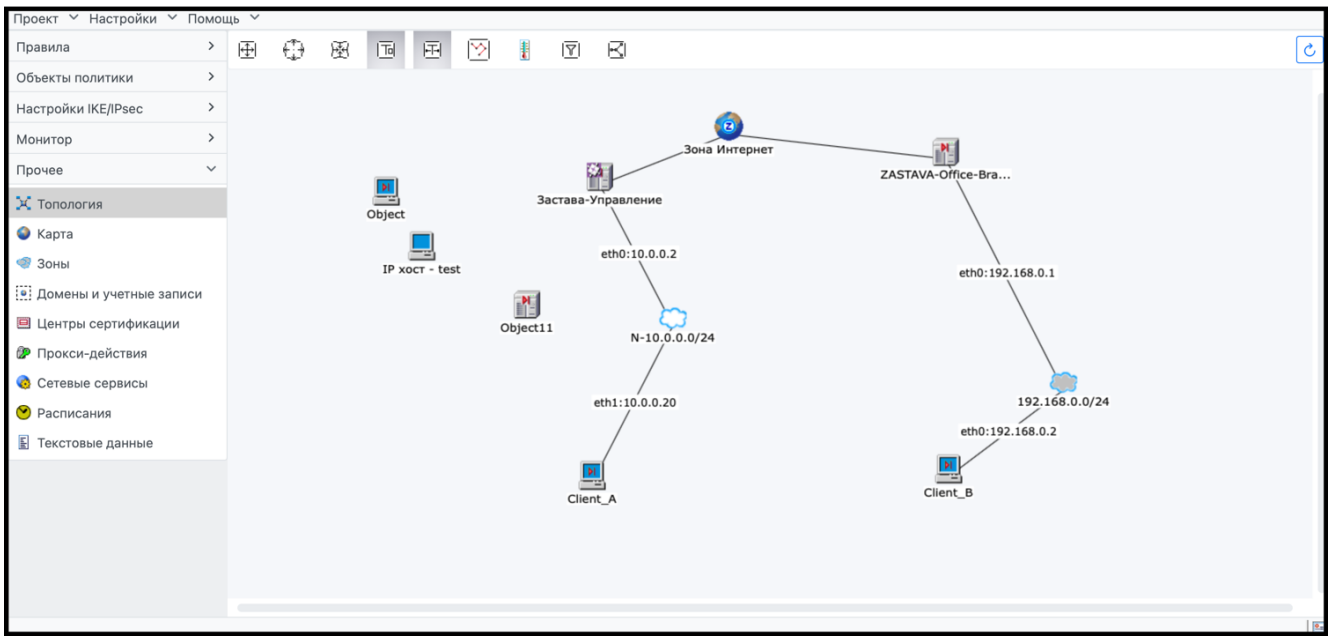


Рисунок 229 – Вид окна элемента списка «Топология» с добавленным объектом типа «Хост безопасности»

7.1.5 Добавление и настройка объекта типа «Шлюз безопасности»

Объекты типа «Шлюз безопасности» представляют собой физическое устройство локальной вычислительной сети (ЛВС) с фиксированной топологией, на котором установлен «VPN/FW «ЗАСТАВА-Офис», версия 8, которое однозначно идентифицируется с именем (в ГПБ) и сертификатом (при прогрузке ЛПБ и установке соединения). Объекты такого типа предназначены для защиты сегмента ЛВС. Весь входящий и исходящий трафик, проходя через шлюз безопасности, обрабатывается в соответствии со сформированной ЛПБ. В соответствии с ЛПБ пакеты могут быть пропущены, отброшены, преобразованы, зашифрованы или расшифрованы. Шлюзы безопасности могут быть управляемыми «» или неуправляемыми «». Для управляемых шлюзов безопасности ЛПБ формируется путем её трансляции с дальнейшей активацией на агенте (см. Приложение 3). Для неуправляемых шлюзов ЛПБ не формируется.

Для добавления объекта типа «Шлюз безопасности» необходимо перейти в боковую панель вкладок «Объекты политики» или в любом другом окне, где в контекстном меню есть команды добавления объектов. Для удобства работы и восприятия можно добавлять объекты в элементе списка «Топология» и выбрать команду «Добавить шлюз безопасности». В результате откроется окно «Выберите версию агента», в котором необходимо выбрать требуемую версию агента. Вид окна «Выберите версию агента» изображен на рисунке (см. Рисунок 230).

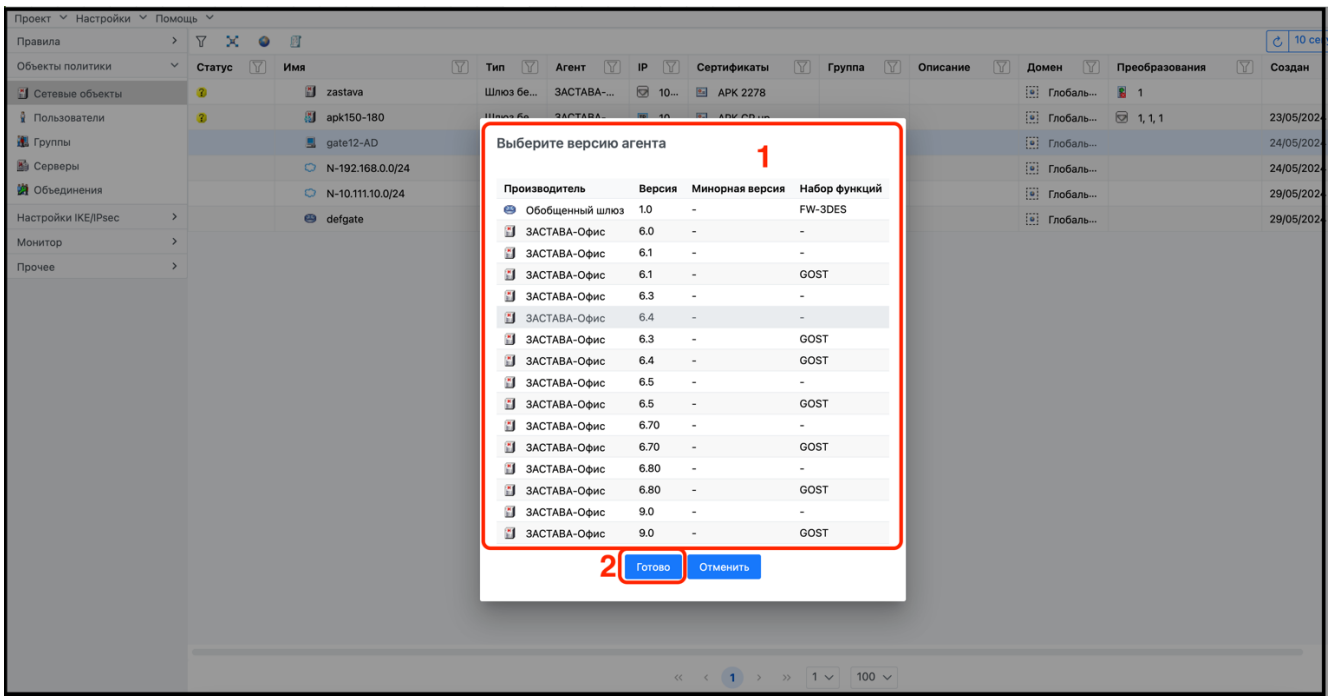


Рисунок 230 – Выбор версии агента

В окне «Выберите версию агента» (цифра 1) необходимо выбрать версию агента и нажать кнопку «Готово» (цифра 2). В результате выполненных действий откроется окно настроек «Добавить шлюз безопасности».

7.1.5.1 Настройка параметров для элемента списка «Общее»

Для настройки элемента списка «Общее» требуется выполнить шаги, изображенные на рисунке (см. Рисунок 231).

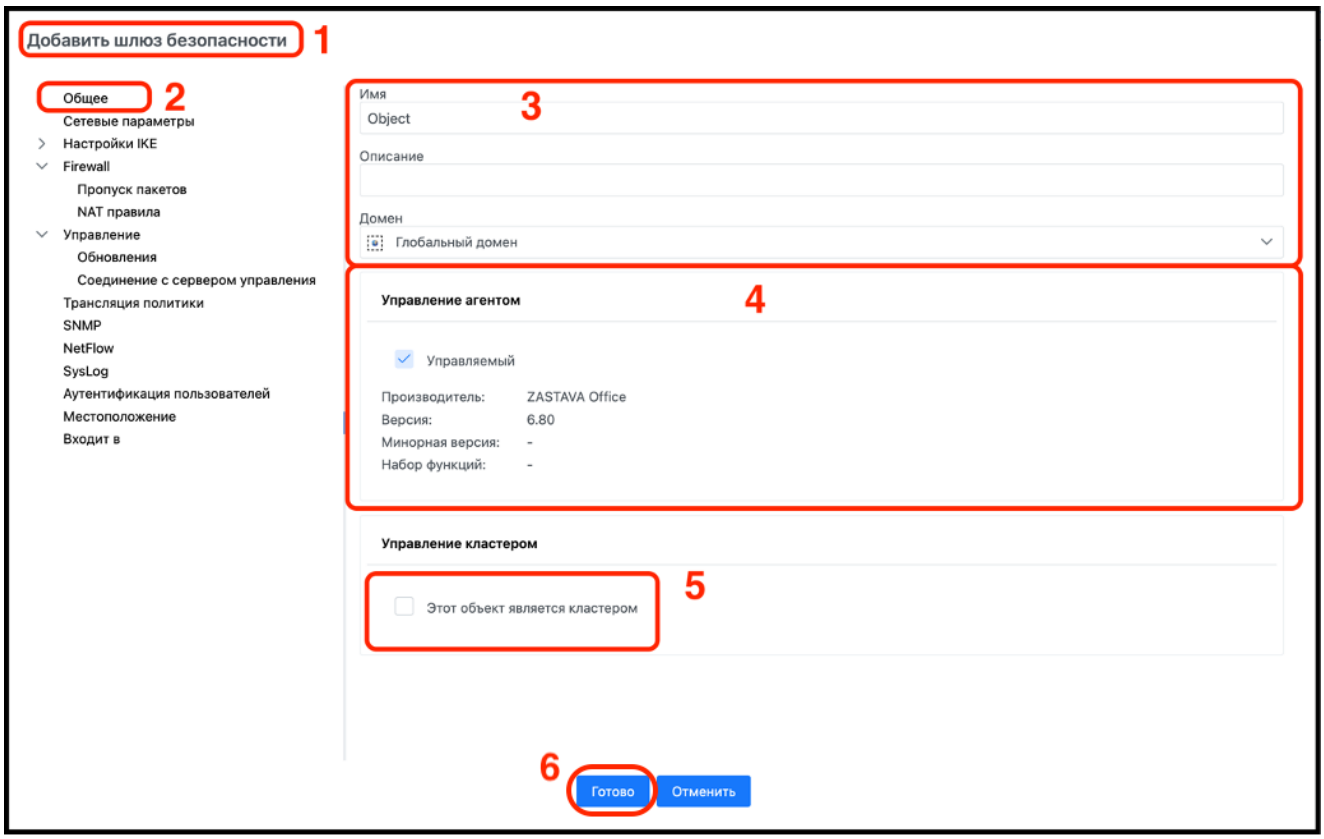


Рисунок 231 – Настройка объекта типа «Шлюз безопасности».

В окне «Добавить шлюз безопасности» (цифра 1) в элементе списка настроек «Общие» (цифра 2) указать общие характеристики шлюза безопасности (цифра 3):

— имя объекта шлюза безопасности;

— описание (при необходимости);

— выбрать домен, в который будет входить данный шлюз безопасности.

Если необходимо создать неуправляемый шлюз безопасности, надо убрать отметку в поле «Управляемый» (цифра 4). Для прямого управления агентом флажок «Управляемый» установлен по умолчанию.

Если создаваемый шлюз безопасности является кластером, то необходимо установить флажок напротив «Этот объект является кластером» (цифра 5). Подробное описание настройки шлюза безопасности в кластерном исполнении представлено в п. 8.5.7. Нажать кнопку «Готово» (цифра 6).

7.1.5.2 Настройка параметров для элемента списка «Сетевые параметры»

В элементе списка «Сетевые параметры» выполнить шаги, изображенные на рисунке (см. Рисунок 232).

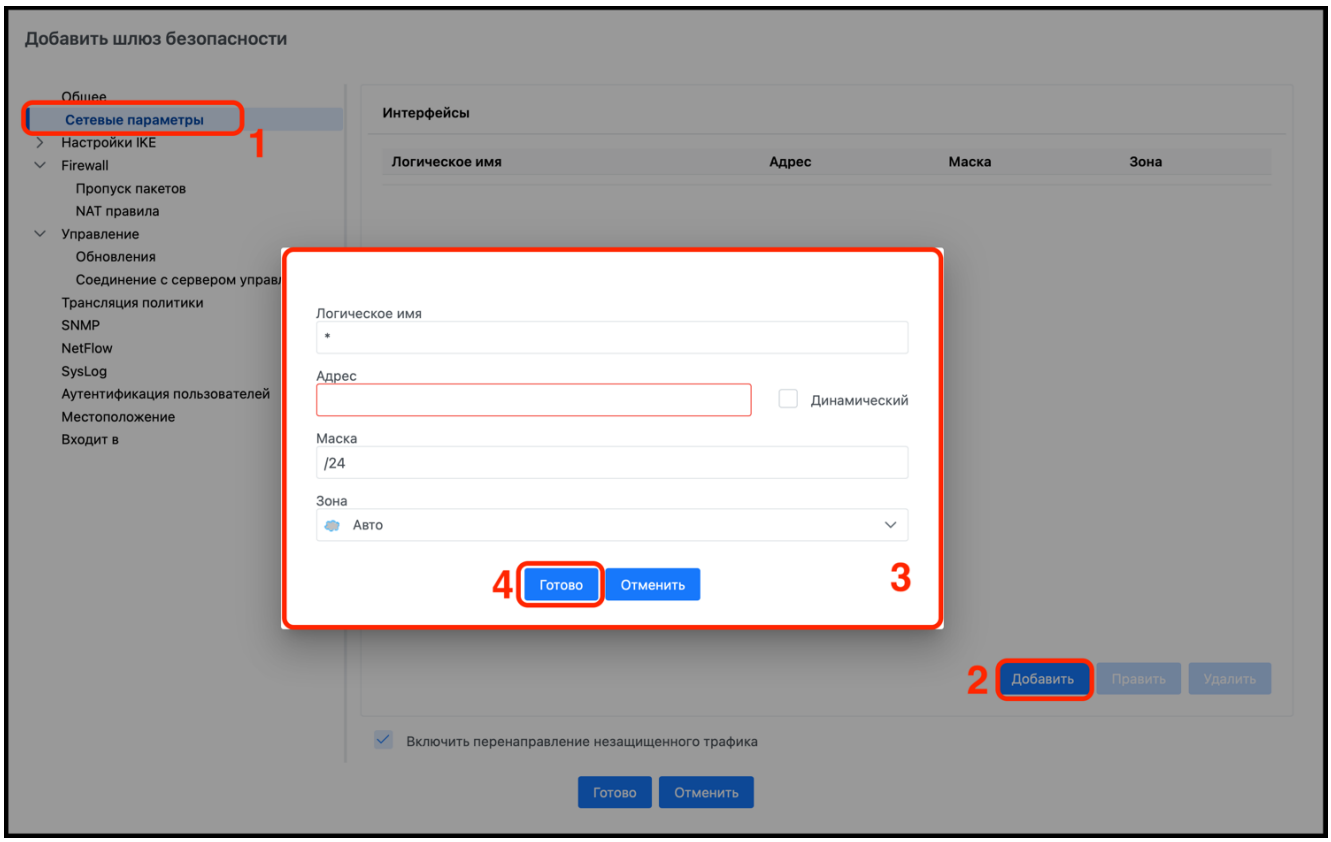


Рисунок 232 – Настройка сетевых параметров для объекта «Шлюз безопасности»

Перейти в элемент списка «Сетевые параметры» (цифра 1), после чего выполнить действия:

1) нажать кнопку «Добавить» (цифра 2);
2) в открывшемся окне настроек (цифра 3) заполнить:

— поле «Логическое имя»;
— в поле «Адрес» ввести 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;
— поле «Маска»;
— выпадающий список «Зона». Где при выборе значение «Авто» зона будет создана автоматически. При добавлении IP-интерфейса, находящегося в зоне Интернет, необходимо выбрать нужный параметр «Зона Интернет»;

3) нажать кнопку «Готово» (цифра 4).

В случае неверно введенных данных откроется окно, изображенное на рисунке (см. Рисунок 233), с предупреждением об ошибке.

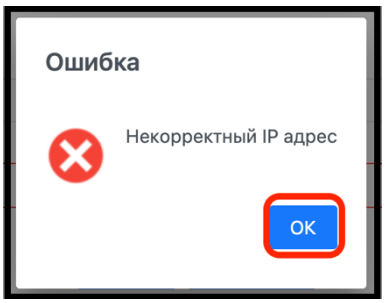


Рисунок 233 – Предупреждение об ошибке

7.1.5.3 Настройка параметров для элемента списка «Настройки IKE»

В элементе списка «Настройки IKE» выполнить шаги, изображенные на рисунке (см. Рисунок 234).

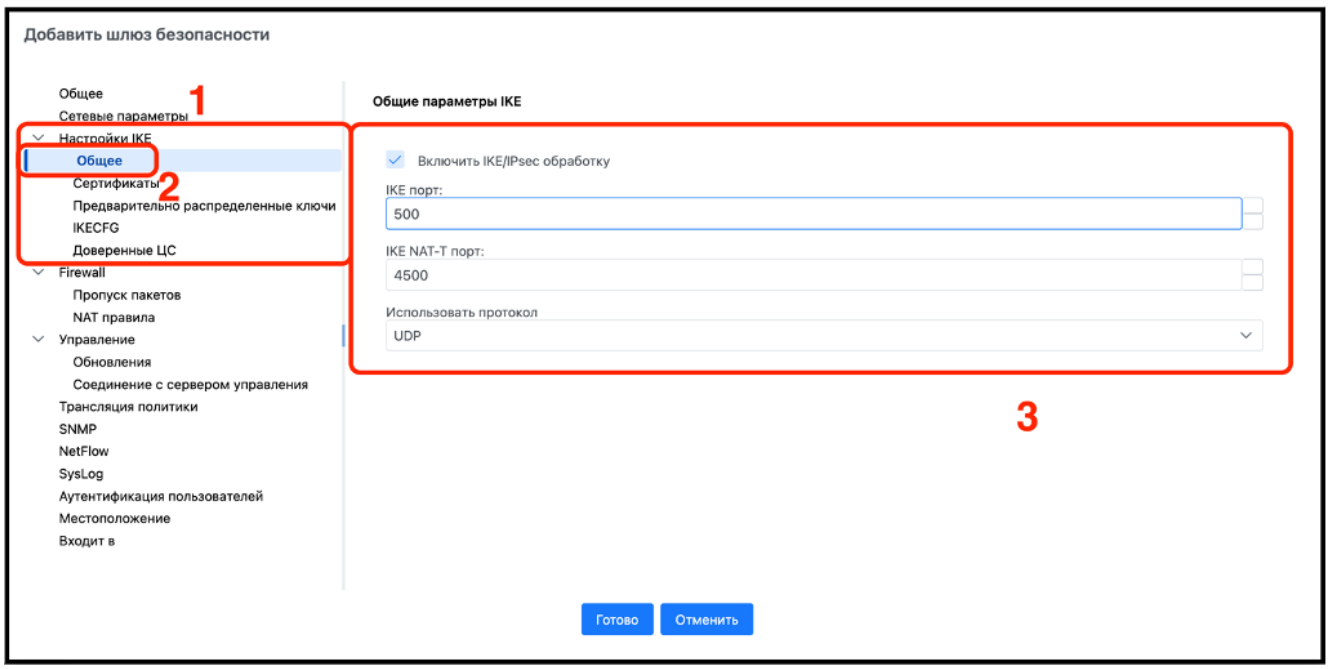


Рисунок 234 – Настройка общих параметров IKE

Перейти в элемент списка «Настройки IKE» (цифра 1), в окне «Общее» (цифра 2) ввести требуемые параметры IKE (цифра 3):

— если нет необходимости, чтобы шлюз безопасности использовал протоколы IKE и IPsec, необходимо убрать отметку в поле «Включить IKE/IPsec обработку», которая установлена по умолчанию;
— в поле «IKE порт» можно указать порт, который будет использоваться шлюзом безопасности;
— в поле «IKE NAT-T порт» можно указать порт, используемый шлюзом безопасности для работы протокола IKE-NAT-Traversal;
— выбрать в списке «Использовать протокол» вариант протокола.

В окне «Сертификаты» и выполнить шаги, изображенные на рисунке (см. Рисунок 235).

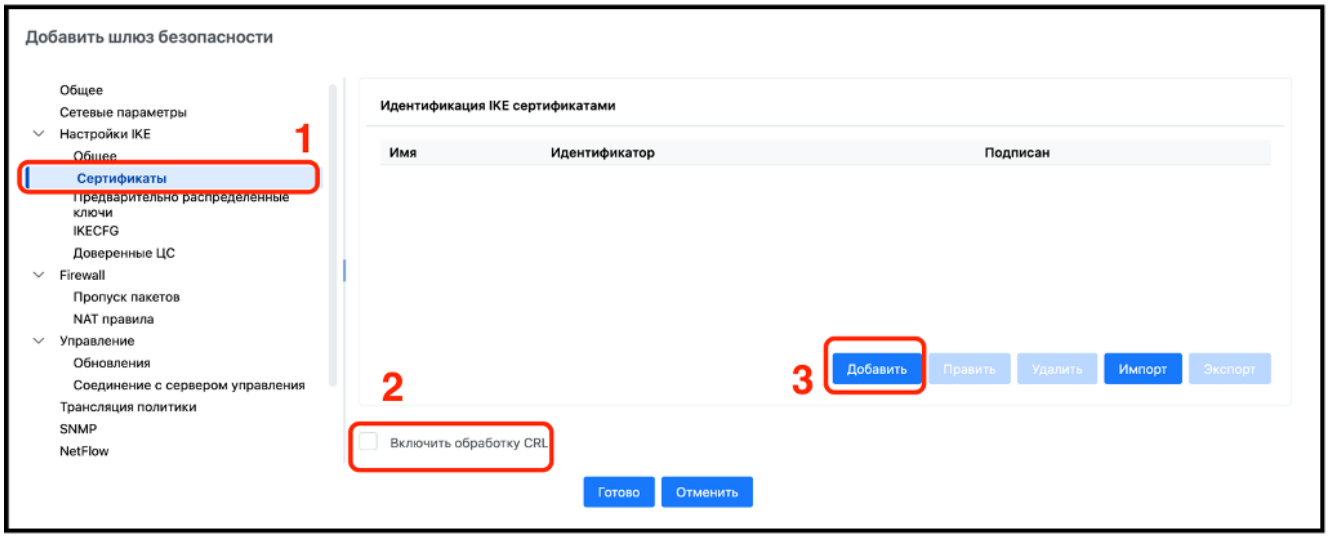


Рисунок 235 – Настройка IKE сертификатов

В окне «Сертификаты» (цифра 1) для включения обработки COC (CRL) установить соответствующий флажок (цифра 2). Для добавления сертификата безопасности использовать кнопку «Добавить» (цифра 3).

В открывшемся окне настроек «Добавить сертификат» ввести описание сертификата, выполнив шаги, изображенные на рисунке (см. Рисунок 236). Введенные данные должны полностью соответствовать данным фактического сертификата, и этот сертификат должен быть зарегистрирован в «ЗАСТАВА-Офис» (см. Приложение 3), используемом шлюзом безопасности. Подробное описание создания сертификатов представлено в п. 6.5.5.2.

Рисунок 236 – Настройка IKE сертификатов

Если шлюз безопасности будет использовать предварительно распределенные ключи, то их необходимо зарегистрировать. Для этого перейти во вкладку «Предварительно распределенные ключи». Вид окна «Предварительно распределенные ключи» изображен на рисунке (см. Рисунок 237).

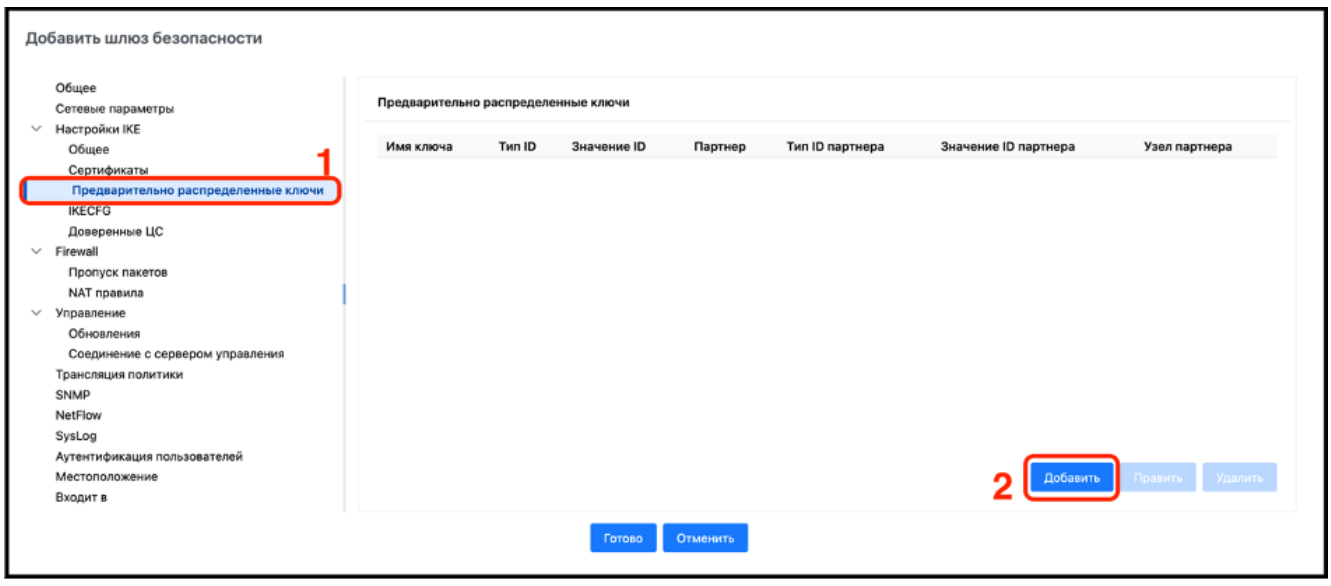


Рисунок 237 – Добавление предварительных распределенных ключей

В окне «Предварительно распределенные ключи» (цифра 1) нажать кнопку «Добавить» (цифра 2).

В открывшемся окне ввести требуемые параметры и добавить предраспределённый ключ. Вид окна представлен на рисунке (см. Рисунок 238).

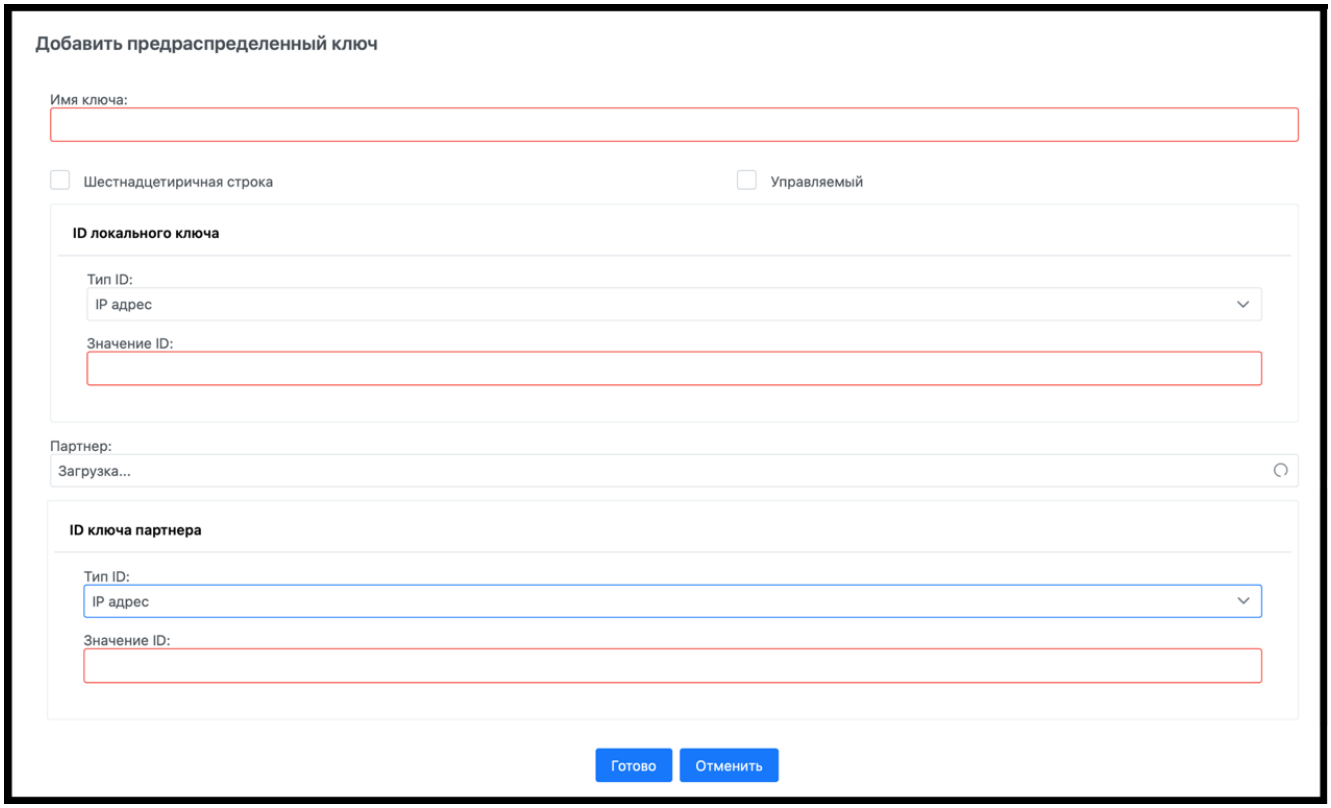


Рисунок 238 – Настройка параметров предраспределённого ключа

В открывшемся окне ввести требуемые параметры:

— в поле «Имя ключа» ввести имя. Это имя должно соответствовать имени предварительно распределенного ключа в «ЗАСТАВА-Офис» (см. Приложение 3), используемом шлюзом безопасности;

— поставить отметку в поле «Управляемый» (если агенты поддерживают управление значением предварительно распределенных ключей);

— из выбрать партнера по связи в строке «Партнер», совместно с которым данный объект политики будет использовать этот ключ;

— выбрать способ идентификации локального ключа из выпадающего списка «Тип ID» в блоке «ID локального ключа». Таким образом партнер по связи сможет убедиться в том, что данный ключ является правильным. По умолчанию для идентификации предварительно распределенного ключа будет использован первичный IP-адрес «ЗАСТАВА-Офис» 8. В этом случае не требуется предоставлять дополнительных сведений. Локальный ключ также может быть идентифицирован с помощью другого IP-адреса, сервиса DNS, ID ключа или шестнадцатеричного идентификатора ключа. В таком случае выбрать тип идентификации ключа из выпадающего списка и ввести значение идентификатора в поле «Значение ID» в блоке «ID локального ключа».

Если данный шлюз безопасности требует конфигурирования удаленных хостов безопасности/пользователей (агент ЗАСТАВА-Клиент) через IKECFG, присваивая им IP-адреса в пространстве IP-адресов, расположенном за шлюзом безопасности, можно отразить это в конфигурации ПО ЗУ, создавая правила IKECFG.

Для создания правила IKECFG необходимо перейти в настройки «IKECFG» и выполнить шаги, изображенные рисунке (см. Рисунок 239).

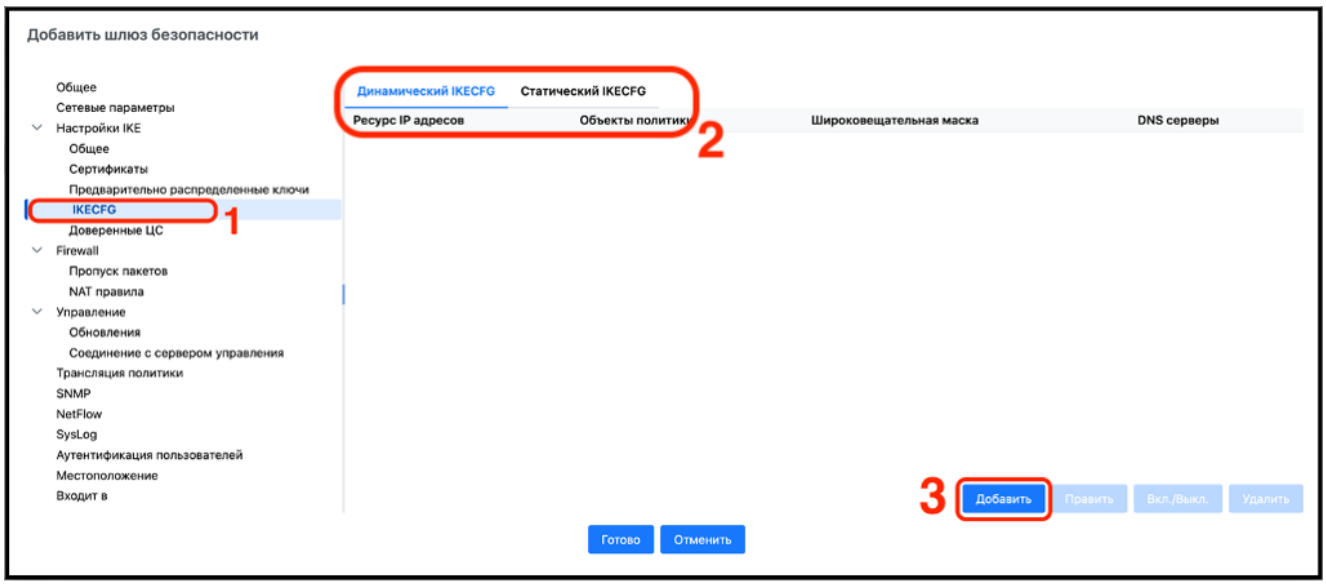


Рисунок 239 – Выбор варианта IKECFG

В окне «IKECFG» (цифра 1) выбрать вариант использования IKECFG (динамический или статический) (цифра 2) и нажать кнопку «Добавить» (цифра 3).

В случае выбора варианта «Динамический IKECFG» откроется окно настроек, изображенное на рисунке (см. Рисунок 240).

Рисунок 240 – Настройка варианта «Динамический IKECFG»

В окно настроек «Добавить IKECFG правило» (цифра 1) необходимо ввести требуемые параметры для динамического IKECFG:

1) выбрать объекты политики, к которым будет применяться протокол IKECFG;
2) указать «Ресурс IP-адресов»:

— «Формат». Выбрать метод указания IP-адресов (доступны варианты: «IP-диапазон», «IP-адрес + маска» или «DHCP»). При выборе метода «DHCP» в качестве идентификатора на агента «ЗАСТАВА-Клиент» будет направлен IP-адрес, выбранный DHCP-сервером, который первым ответит на запрос (DHCP REQUEST) шлюза безопасности.

— «IP-адрес». В поле ввести IP-адрес;

— «Дополнительные параметры». Указать широковещательную маску и адрес DNS-сервера;

3) нажать кнопку «Готово» (цифра 2).

В случае необходимости ввести информацию о ЦС необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 241).

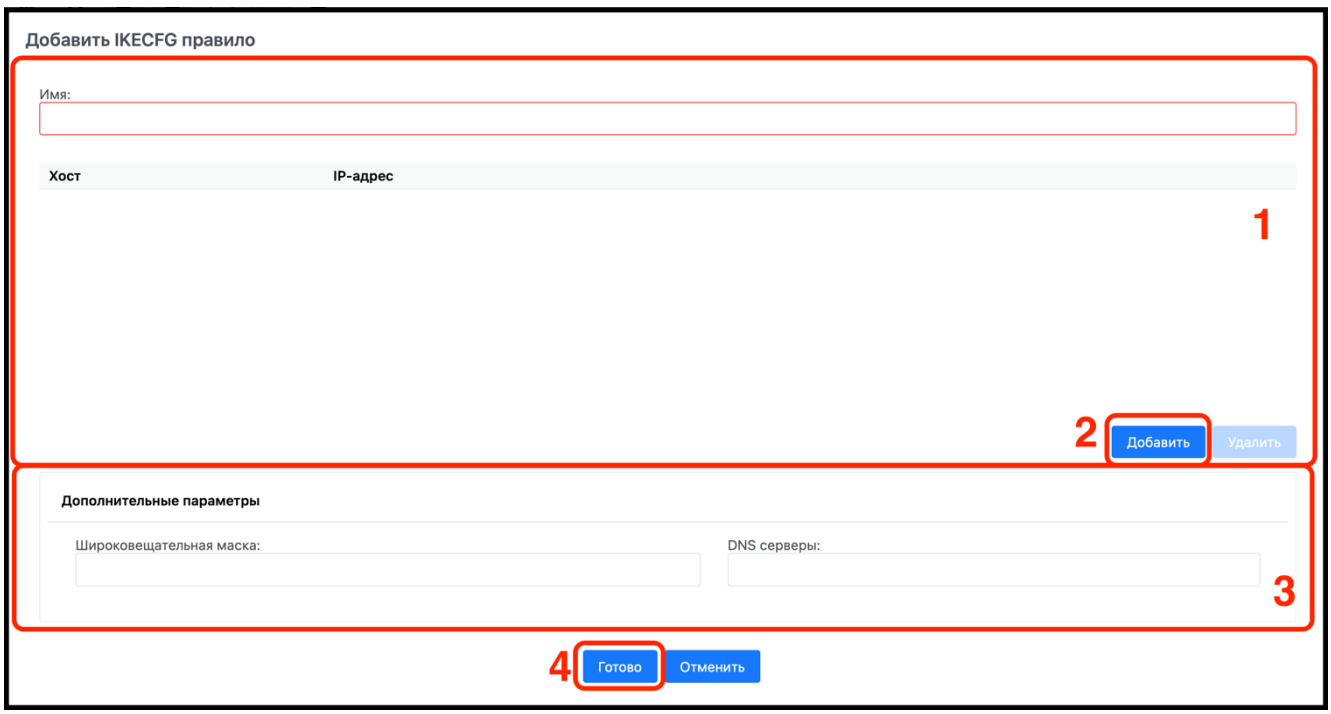


Рисунок 241 – Настройка варианта «Статический IKECFG»

В окне настроек «Добавить IKECFG правило» (цифра 1) необходимо назначить имя IKECFG-правила, затем нажать кнопку «Добавить» (цифра 2) и ввести требуемые параметры для шлюза безопасности в блоке настроек «Дополнительные параметры» (цифра 3), затем нажать кнопку «Готово» (цифра 4).

В случае необходимости ввести информацию о ЦС необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 242).

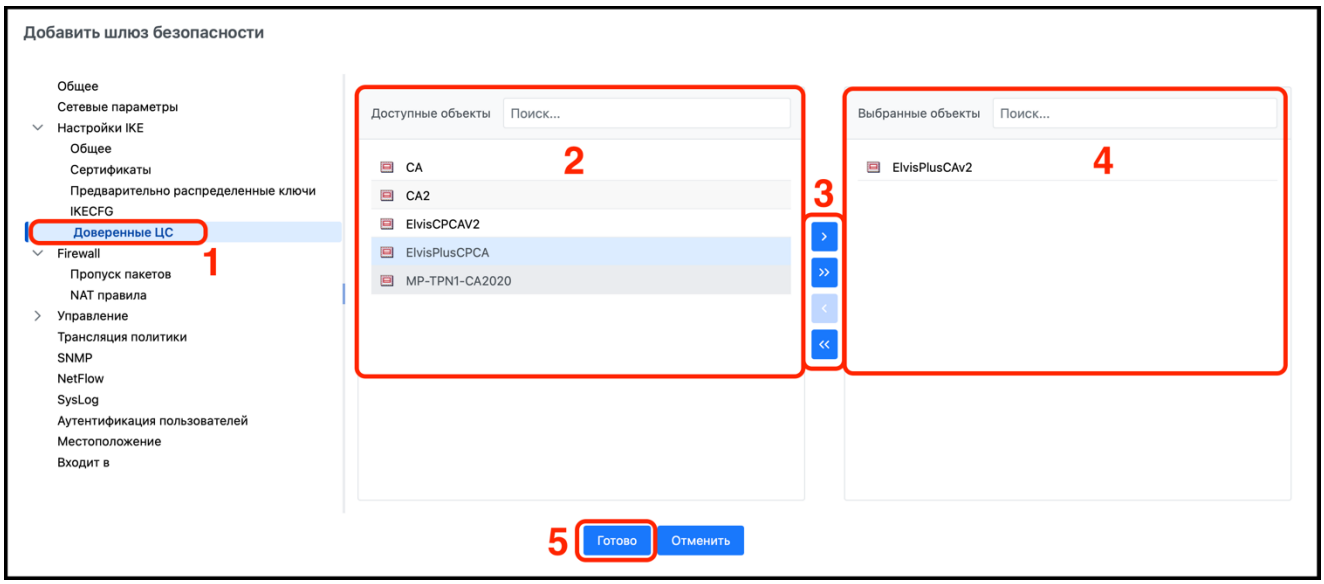


Рисунок 242 – Вид окна «Доверенные ЦС»

В окне «Доверенные ЦС» (цифра 1) выбрать требуемый для перемещения объект в поле «Доступные объекты» (цифра 2) или найти его, используя элементы управления (цифра 3). переместить требуемый объект в поле «Выбранные объекты» (цифра 4). Выполнив все требуемые настройки, нажать кнопку «Готово» (цифра 5).

В результате всех выполненных действий будет произведена настройка для элемента списка «Настройки IKE».

7.1.5.4 Настройка параметров для элемента списка «Firewall»

Перейти в элемент списка «Firewall» (МЭ) и выполнить шаги, изображенные на рисунке (см. Рисунок 243).

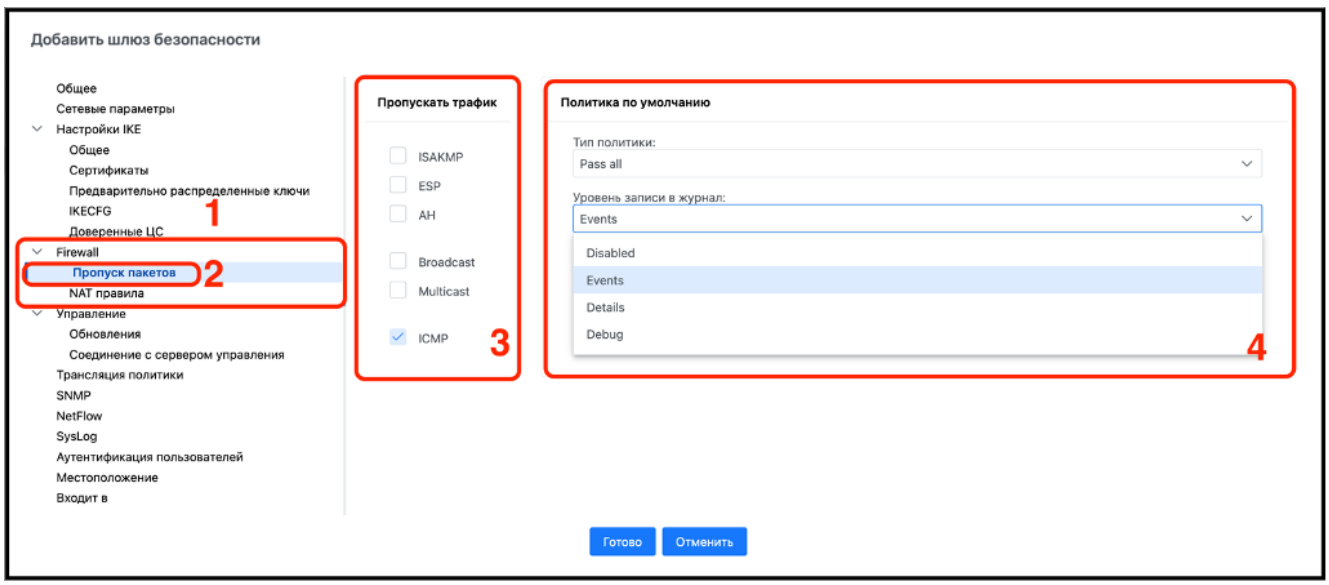


Рисунок 243 – Настройка вкладки «Пропуск пакетов»

Перейти в элемент списка «Firewall» (цифра 1), в окне «Пропуск пакетов» (цифра 2) в блоке «Пропускать трафик» установить флажок напротив требуемого значения (цифра 3). В

блоке «Политика по умолчанию» выбрать в выпадающем списке тип политики и уровень записи в журнал (цифра 4).

При необходимости использования трансляции IP-адресов необходимо в элементе списка «NAT правила» выполнить шаги, изображенные на рисунке (см. Рисунок 244).

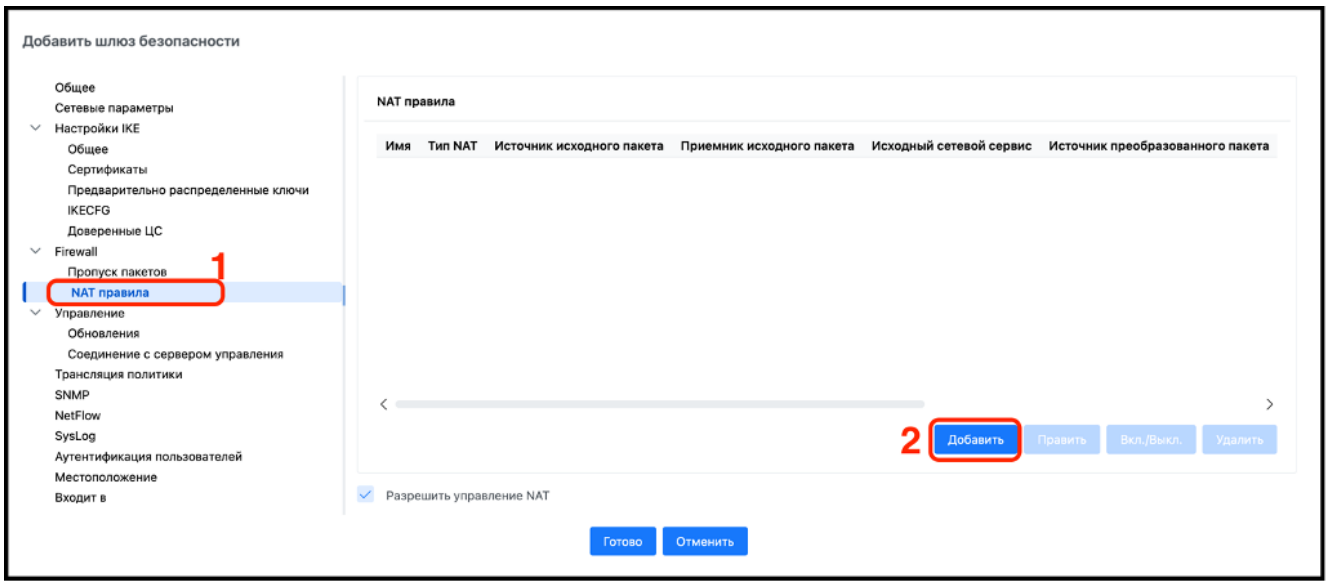


Рисунок 244 – Настройка вкладки «NAT правила»

В окне «NAT правила» (цифра 1) нажать кнопку «Добавить» (цифра 2).

В открывшемся окне настроек «Создать NAT правило» выполнить шаги, изображенные на рисунке (см. Рисунок 245).

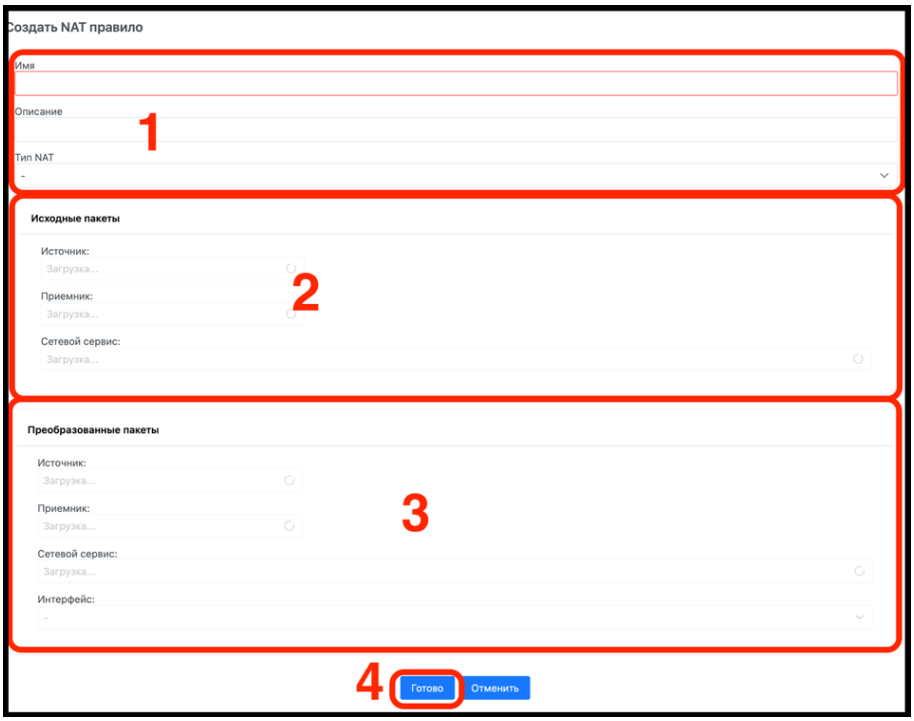


Рисунок 245 – Настройка «NAT правила»

Заполнить общие данные (цифра 1), в блоке «Исходные пакеты» выбрать источник, приемник и сетевой сервис (цифра 2), в блоке «Преобразованные пакеты» также выбрать

источник, приемник, сетевой сервис и интерфейс (цифра 3). Нажать кнопку «Готово» (цифра 4). Подробное описание создания NAT-правил для шлюза безопасности представлено в п. 8.5.3.

7.1.5.5 Настройка параметров для элемента списка «Управление»

В случае управляемого шлюза безопасности необходимо ввести соответствующие настройки в элементе списка «Управление», выполнив шаги, изображенные на рисунке (см. Рисунок 246).

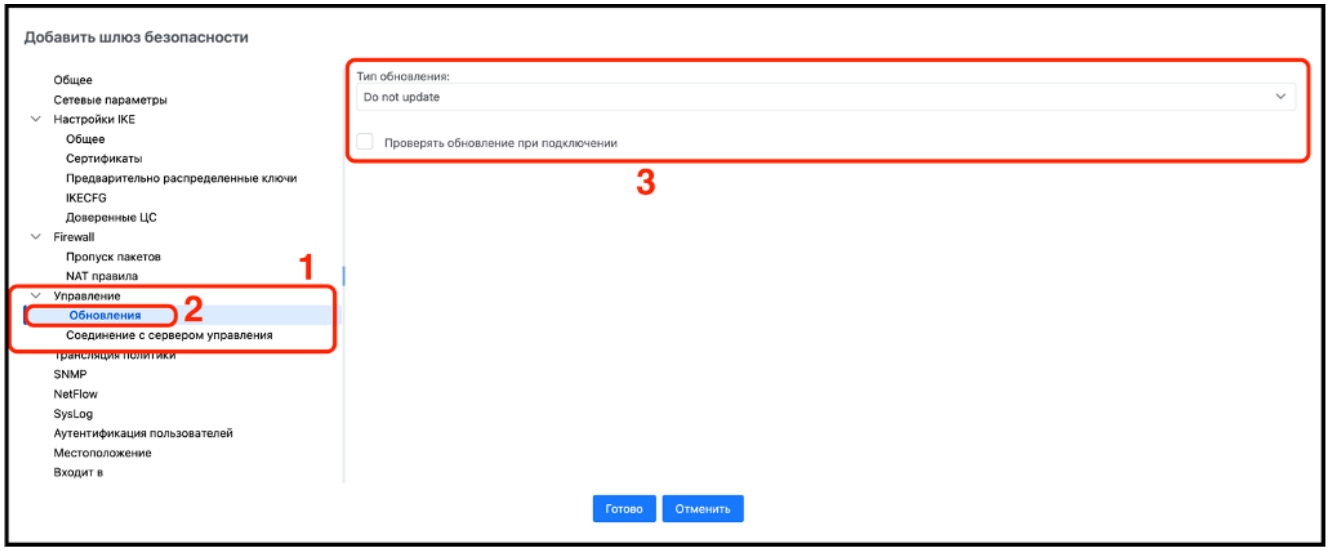


Рисунок 246 – Настройка вкладки «Обновление»

Перейти в элемент списка «Управление» (цифра 1), в окне «Обновление» (цифра 2) настроить параметры обновления агента (цифра 3). Для настроек соединения с сервером управления необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 247).

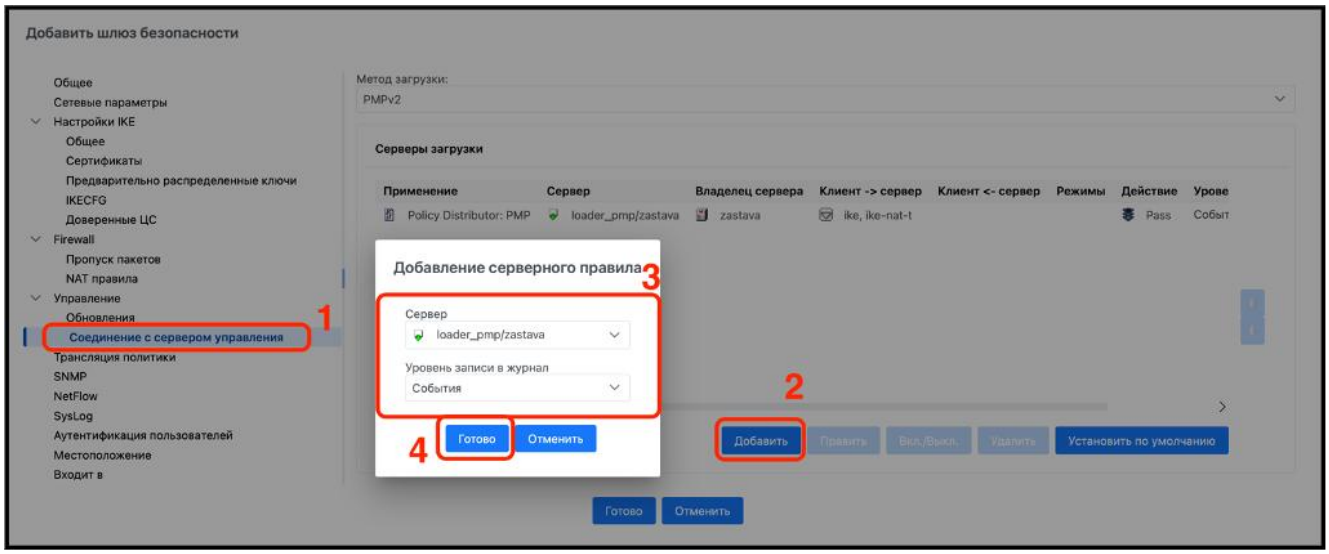


Рисунок 247 – Настройка вкладки «Соединение с сервером управления»

В окне «Соединение с сервером управления» (цифра 1) нажать кнопку «Добавить» (цифра 2). В открывшемся окне «Добавление серверного правила» выполнить настройки (цифра 3), затем нажать кнопку «Готово» (цифра 4).

7.1.5.6 Настройка параметров для элемента списка «Трансляция политики»

В случае необходимости добавления дополнительных параметров к автоматически создаваемой ЛПБ необходимо перейти в элемент списка «Трансляция политики» и выполнить шаги, изображенные на рисунке (см. Рисунок 248).

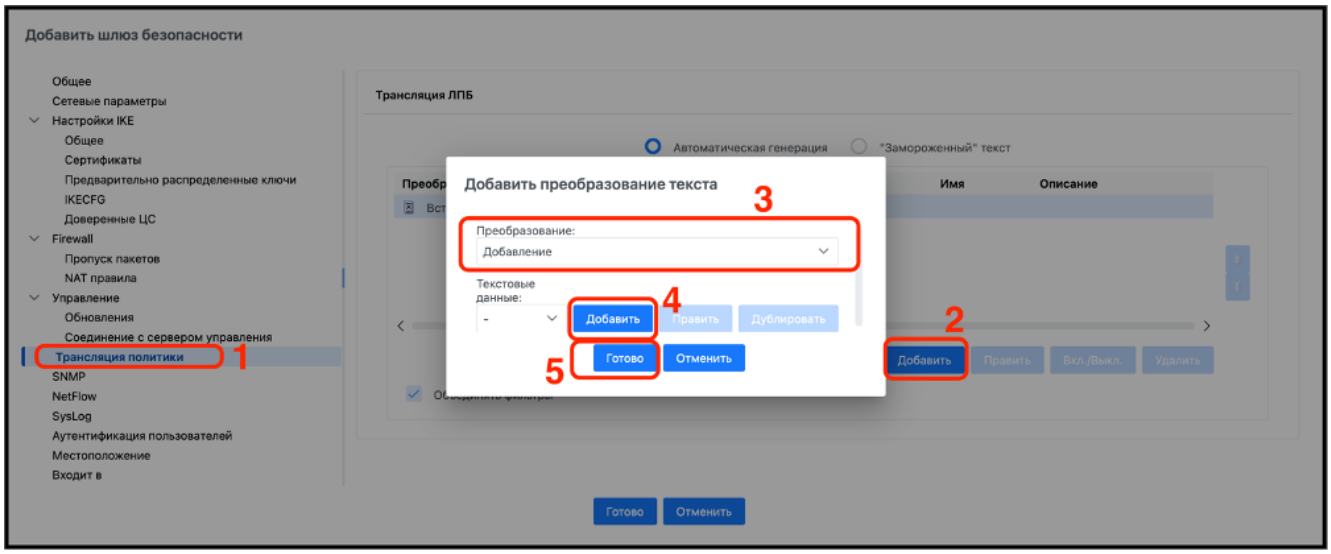


Рисунок 248 – Настройка элемента списка «Трансляция политики»

Перейти в элемент списка «Трансляция политики» (цифра 1), нажать кнопку «Добавить» (цифра 2). В открывшемся окне «Добавить преобразование текста» в выпадающем списке выбрать вариант добавления (цифра 3), при необходимости с помощью кнопки «Добавить» (цифра 4) открыть дополнительное окно для ввода текстовых данных, затем нажать кнопку «Готово» (цифра 5).

7.1.5.7 Настройка параметров для элемента списка «SNMP»

В случае необходимости использования протокола «SNMP» для сбора статистики необходимо перейти в элемент списка «SNMP» и выполнить шаги, изображенные на рисунке (см. Рисунок 249).

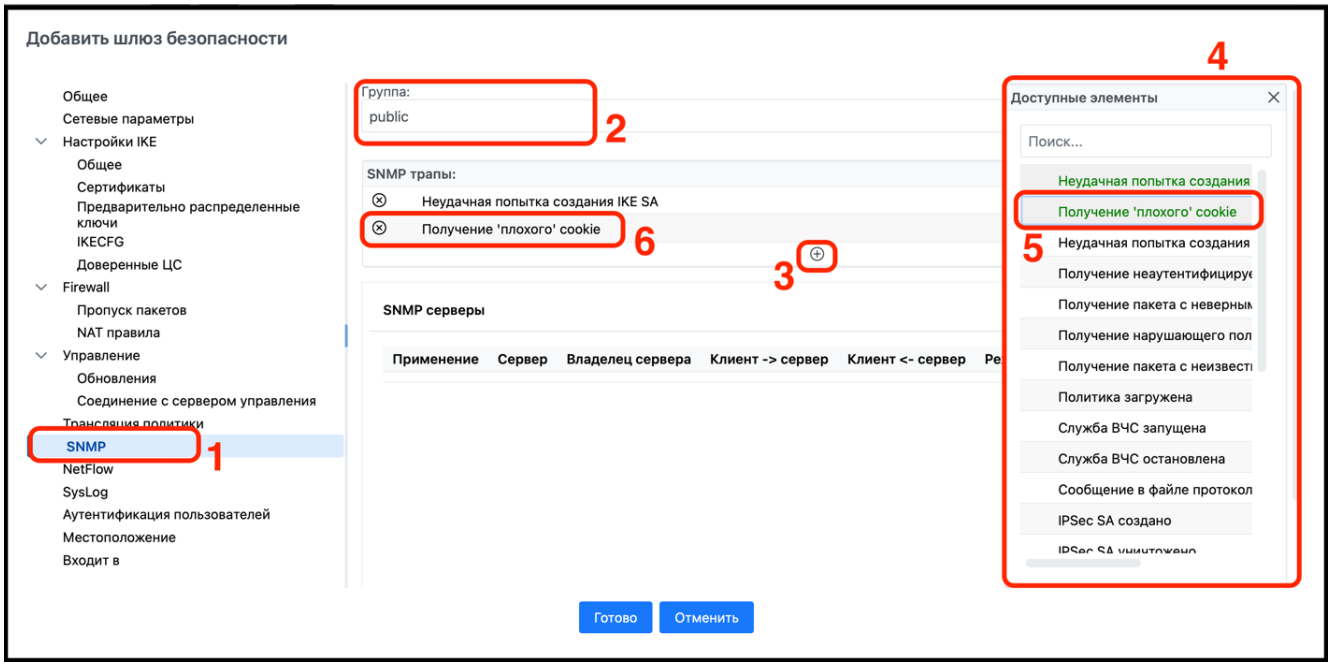


Рисунок 249 – Элемент списка «SNMP»

Перейти в элемент списка «SNMP» (цифра 1) и выбрать группу (цифра 2). По умолчанию порт SNMP клиента - 3454, а значение среды SNMP – public. При необходимости эти значения могут быть изменены в соответствующих полях. Все SNMP-сообщения должны содержать имя сообщества (community name), используемое для аутентификации. Сообщения, содержащие имя сообщества, которое не установлено на хосте, не будут приняты. С помощью кнопки «+» (цифра 3) перенести сообщение из списка «Доступные элементы» (цифра 4) в SNMP-трапы (цифра 6). После перемещения элемент меняет цвет на зеленый (цифра 5). В п. 8.5.10 приведён полный список SNMP-сообщений.

Если необходимо, чтобы шлюз безопасности всегда пропускал SNMP-трафик без предварительной проверки правил ЛПБ, надо создать правило для пропуска SNMP-трафика, поступающего от шлюза безопасности на SNMP-сервер. Добавить для «SNMP» серверное правило можно, выполнив шаги, изображенные на рисунке (см. Рисунок 250).

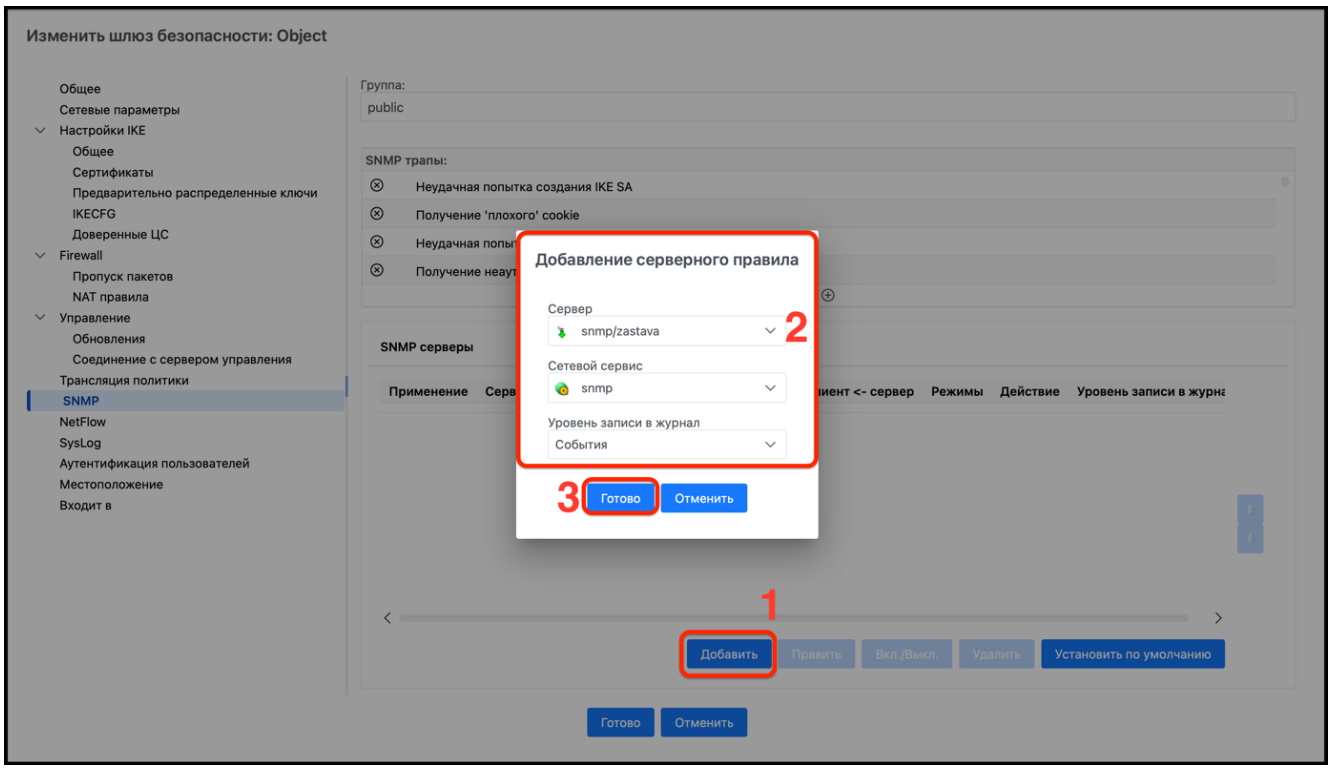


Рисунок 250 – Добавление серверного правила для «SNMP»

Нажать кнопку «Добавить» (цифра 1), в открывшемся окне «Добавление серверного правила» (цифра 2) выбрать требуемый SNMP-сервер, на которые «ЗАСТАВА-Офис» (см. Приложение 3) будет отправлять SNMP-сообщения. В списке будут отображаться те серверы, которые были предварительно зарегистрированы в окне «Серверы». Выбрать уровень записи в журнал (доступны варианты: «Отключен», «События», «Подробный», «Отладочный»), затем нажать кнопку «Готово» (цифра 3).

7.1.5.8 Настройка параметров для элемента списка «NetFlow»

В случае необходимости использования протокола «NetFlow» необходимо перейти в элемент списка «NetFlow» и выполнить шаги, изображенные на рисунке (см. Рисунок 251).

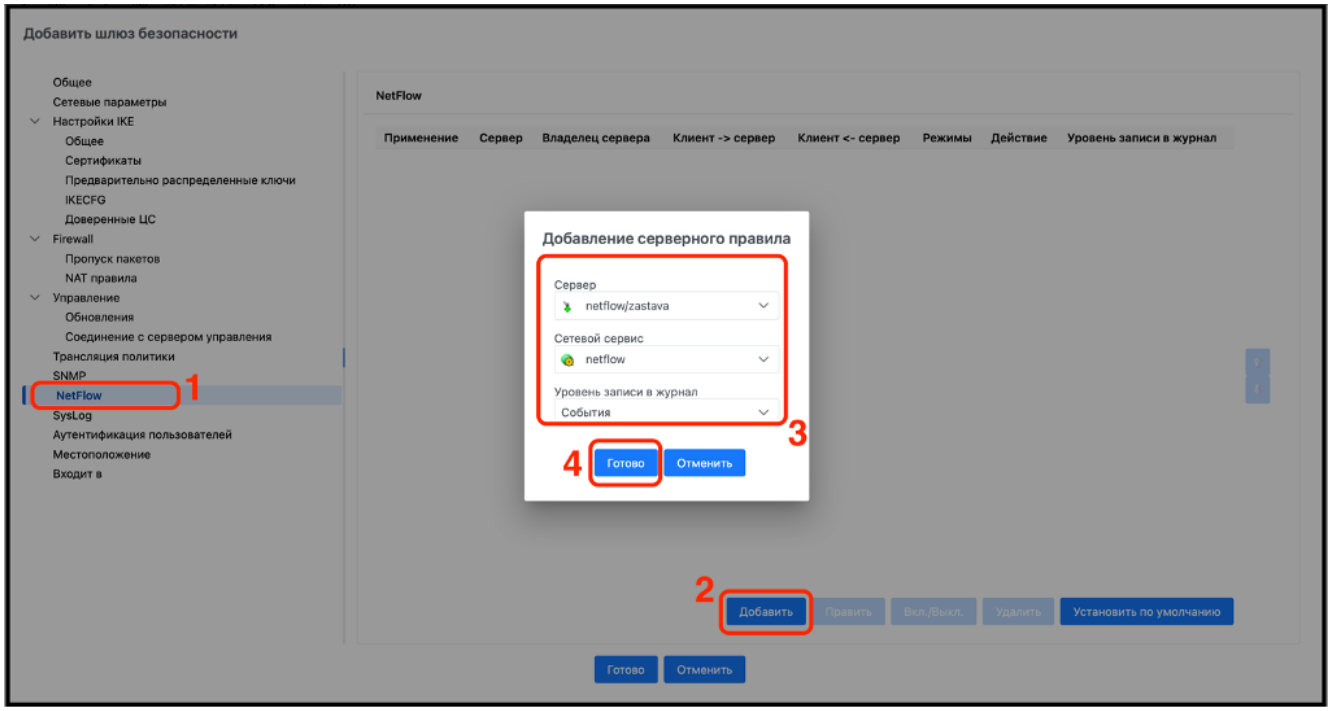


Рисунок 251 – Настройка «NetFlow»

Перейти в элемент списка «NetFlow» (цифра 1), нажать кнопку «Добавить» (цифра 2), в открывшемся окне «Добавление серверного правила» выполнить шаги:

1) выбрать NetFlow-сервер, на который «ЗАСТАВА-Офис» (см. Приложение 3) будет отправлять SNMP-сообщения. В списке будут отображаться те серверы, которые были предварительно зарегистрированы в окне «Серверы»;
2) выбрать сетевой сервис и уровень записи в журнал (доступны варианты: «Отключен», «События», «Подробный», «Отладочный») (цифра 3);
3) нажать кнопку «Готово» (цифра 4).

7.1.5.9 Настройка параметров для элемента списка «SysLog»

В случае необходимости использования внешнего SysLog-сервера необходимо перейти в элемент списка «SysLog» и выполнить шаги, изображенные на рисунке (см. Рисунок 252).

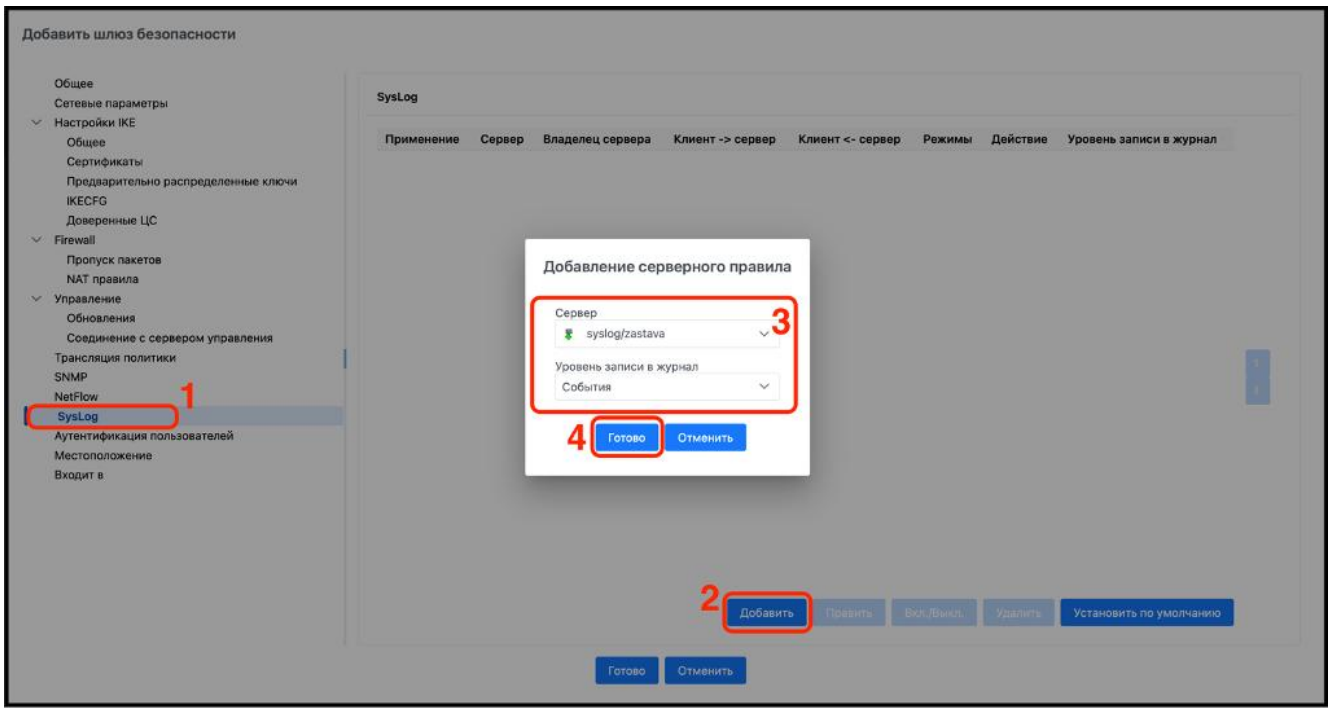


Рисунок 252 – Настройка «SysLog»

Перейти в элемент списка «SysLog» (цифра 1), нажать кнопку «Добавить» (цифра 2), далее в открывшемся окне «Добавление серверного правила» выполнить шаги:

1) в выпадающем списке «Сервер» выбрать один или несколько SNMP-серверов, на которые «ЗАСТАВА-Офис» (см. Приложение 3) будет отправлять SNMP-сообщения. В списке будут отображаться те серверы, которые были предварительно зарегистрированы в окне «Серверы»;
2) выбрать уровень записи в журнал (доступны варианты: «Отключен», «События», «Подробный», «Отладочный») (цифра 2);
3) нажать кнопку «Готово» (цифра 4).

7.1.5.10 Настройка параметров для элемента списка «Аутентификация пользователей»

В элементе списка «Аутентификация пользователей» требуется выполнить шаги, изображенные на рисунке (см. Рисунок 253).

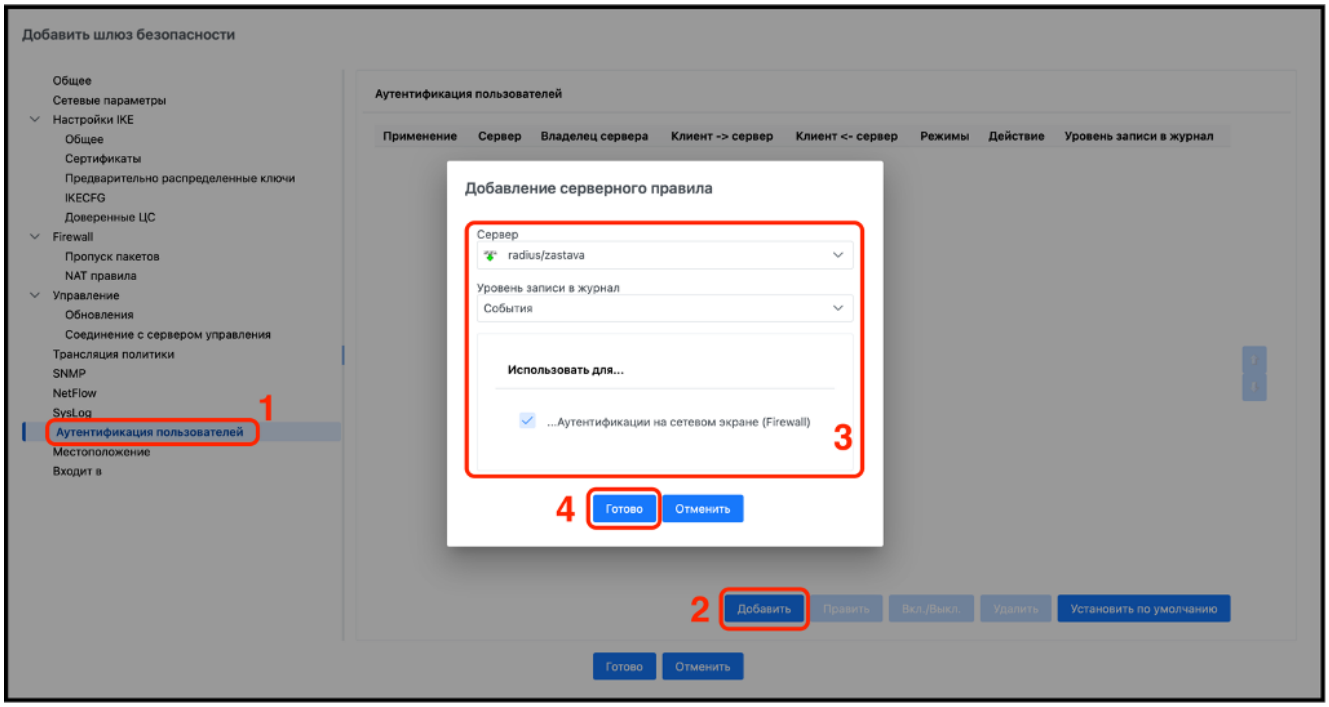


Рисунок 253 – Настройка «Аутентификация пользователей»

Перейти в элемент списка «Аутентификация пользователей» (цифра 1), нажать кнопку «Добавить» (цифра 2), в открывшемся окне настроить параметры серверного правила (цифра 3), нажать кнопку «Готово» (цифра 4).

7.1.5.11 Настройка параметров для элемента списка «Местоположение»

Перейти в элемент списка «Местоположение» и выполнить шаги, изображенные на рисунке (см. Рисунок 254).

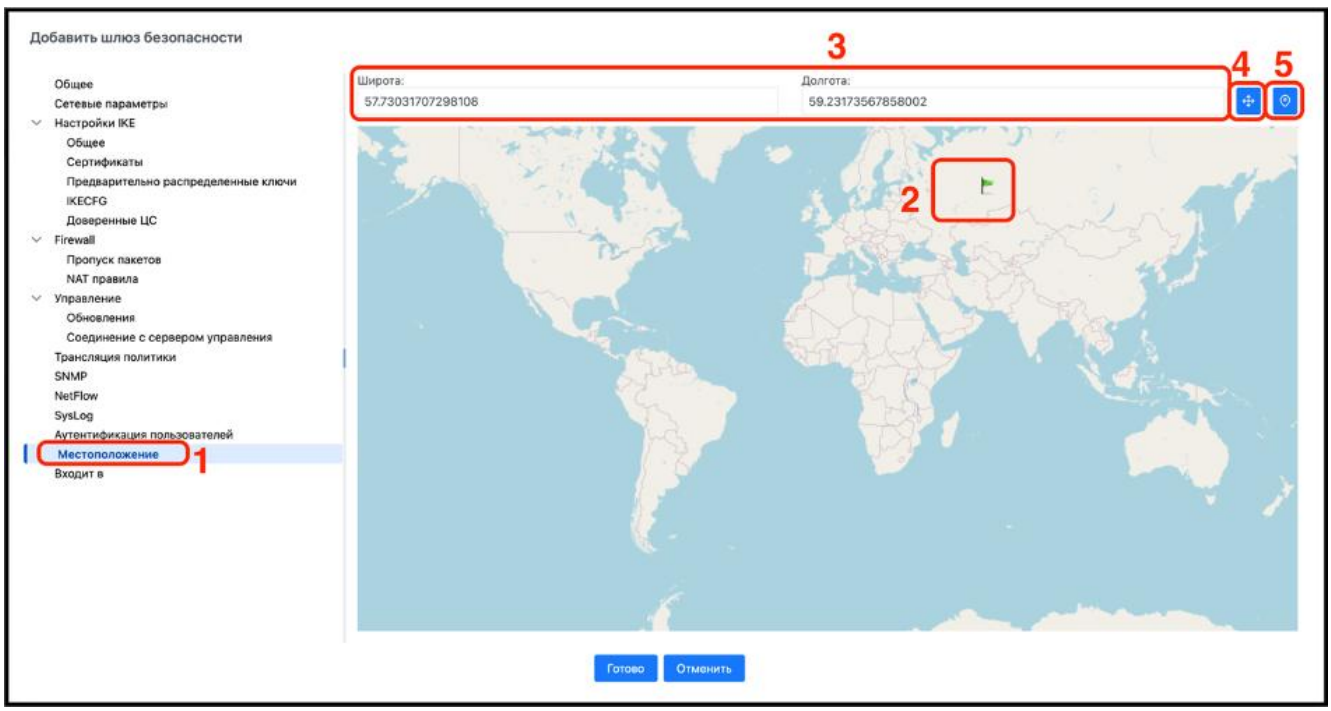


Рисунок 254 – Настройка «Местоположение»

В окне элемента списка «Местоположение» (цифра 1) разместить указатель мыши в требуемом месте карты и нажать левой клавишей мыши, установив флажок объекта (цифра 2). Также разместить объект на карте можно, указав широту и долготу нужного местоположения в строке координат (цифра 3). В результате выполненных действий флажок переместится в заданную точку. С помощью элемента «» «Показать на карте» (цифра 4) флажок окажется в центре карты. С помощью элемента «» можно найти географические координаты местоположения объекта, если в его настройках включена передача геолокации (цифра 5).

7.1.5.12 Настройка параметров для элемента списка «Входит в»

Перейти в элемент списка «Входит в» и выполнить шаги, изображенные на рисунке (см. Рисунок 255).

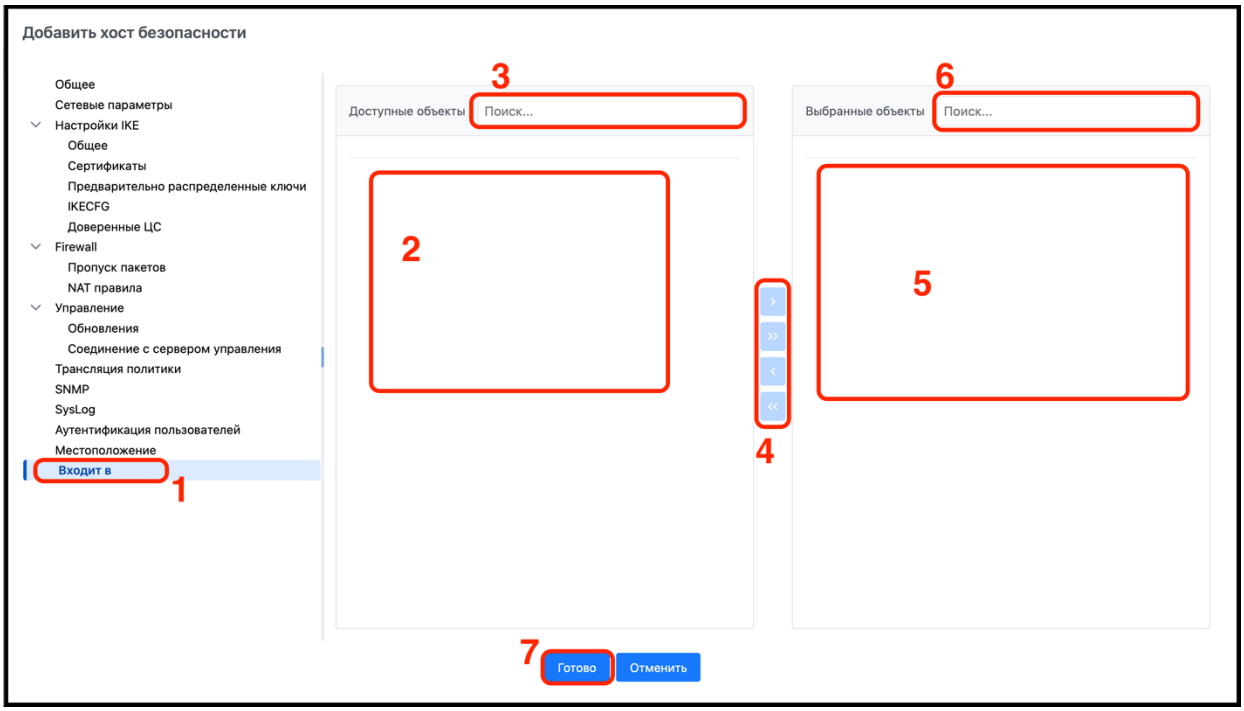


Рисунок 255 – Настройка «Входит в»

В окне элемента списка «Входит в» (цифра 1) выбрать требуемый для вхождения в группу объект в поле «Доступные объекты» (цифра 2) или найти его, используя поисковую строку (цифра 3). Выбрать требуемый объект для создания группы в поле «Выбранные объекты» (цифра 5) или найти его, используя поисковую строку (цифра 6). Переместить требуемый объект в необходимые группы или разгруппировать объекты можно с помощью инструментов перемещения (цифра 4). Выполнив все требуемые настройки, нажать кнопку «Готово» (цифра 7).

В результате в рабочей области элемента списка «Топология» добавится объект типа «Шлюз безопасности», изображенный на рисунке (см. Рисунок 256).

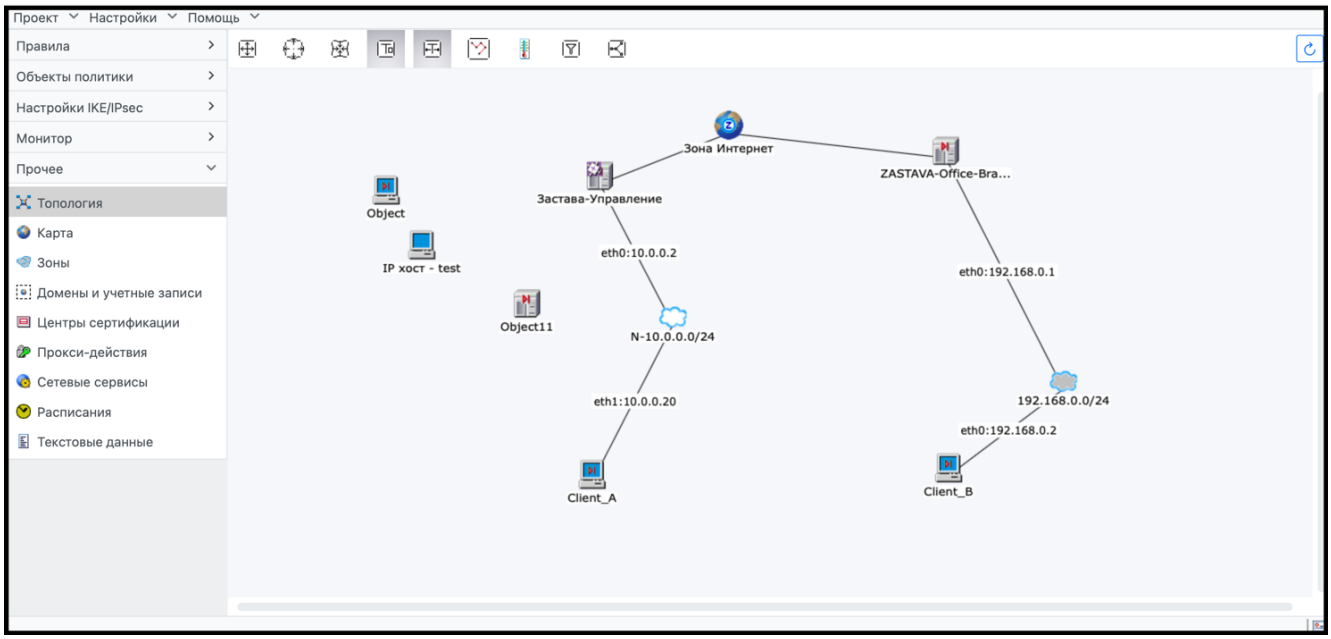


Рисунок 256 – Вид элемента списка «Топология» с добавленным объектом типа «Шлюз безопасности»

7.1.6 Добавление и настройка объекта типа «Зона»

Объект «Зона» может создаваться автоматически при создании объекта «Шлюз безопасности», исходя из значений его IP-адресов и их масок и состояния настроек (установка флажка «Интернет»), выбранного при создании топологии шлюза безопасности. Если настройка установлена, то данный интерфейс объекта «Зона» автоматически входит в зону Интернет, если настройка не установлена на интерфейсе шлюза безопасности, 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 безопасности.

Для добавления объекта типа «Зона» необходимо перейти в контекстное меню, как представлено в подразделе 7.1, и выбрать команду «Добавить зону». В результате откроется окно «Добавить зону», вид которого изображен на рисунке (см. Рисунок 257).

Рисунок 257 – Добавление и общая настройка объекта «Зона»

В окне настроек «Общее» (цифра 1) выполнить настройки блока (цифра 2).

Перейти в окно настроек «Топология», выполнив шаги, изображенные на рисунке (см. Рисунок 258).

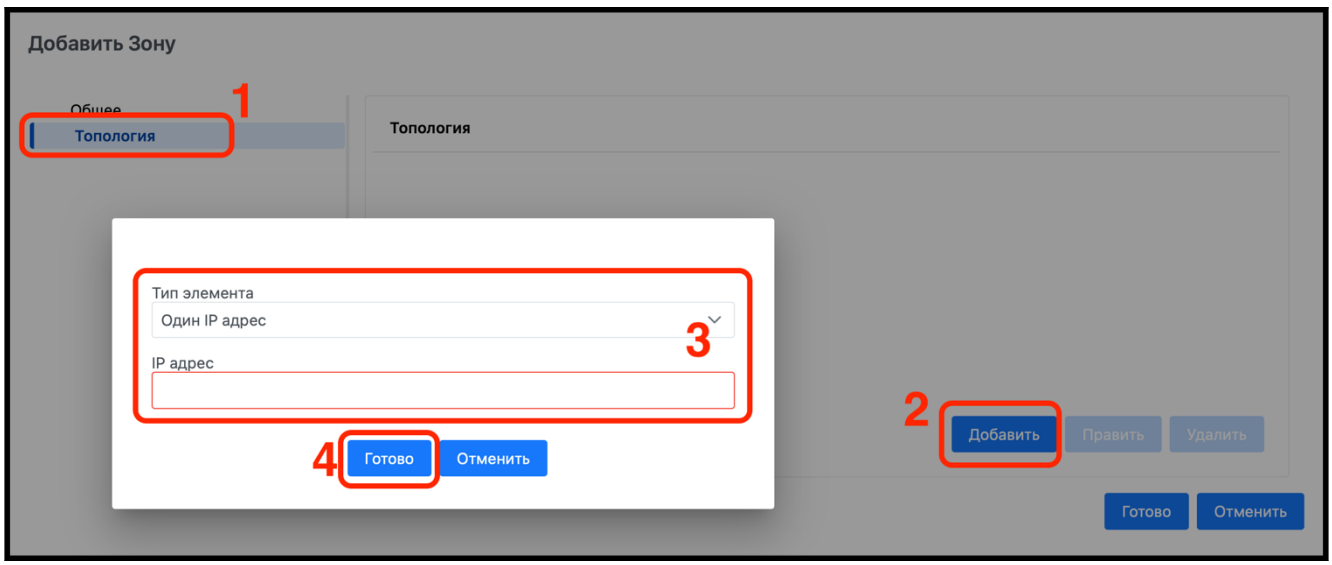


Рисунок 258 – Добавление и настройка топологии для объекта «Зона»

В окне настроек «Топология» (цифра 1) нажать кнопку «Добавить» (цифра 2), в открывшемся окне (цифра 3) выбрать тип элемента и ввести IP-адрес. Необходимо 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 IP-адресов данной подсети и диапазона IP-адресов тоже находится в этой зоне. Нажать кнопку «Готово» (цифра 4).

8 СОЗДАНИЕ ГЛОБАЛЬНОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ

8.1 Основные объекты ГПБ

Для создания самой простой ГПБ необходимо определить два типа компонентов:

— объекты политики (в том числе зоны);

— правила.

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

Правила ГПБ определяют, как объекты политики могут обмениваться информацией в защищенной сети. Создание правил безопасности - наиболее важный шаг при работе с ПО ЗУ, поскольку правила являются основой ГПБ: все привязано к правилам в той или иной степени.

В процессе конфигурирования ГПБ настоятельно рекомендуется либо делать заметки, либо выполнять действия по плану (см. Приложение 1).

Другие объекты ГПБ представлены в таблице (см. Таблица 32).

Таблица 32 – Другие объекты ГПБ

Другие объекты ГПБ	Описание
Серверы	Серверы представляют собой особые виды хостов (не обязательно защищенных), к которым различные участники защищенной системы будут иметь доступ.
Сетевые сервисы	Сетевые сервисы используются для уточнения правил: если в правиле указан сетевой сервис, то это правило будет действовать только для соответствующего типа трафика
Настройки IKE	Настройки IKE определяют параметры протокола IKE, которые будут использоваться в процессе установления первичного защищенного соединения (IKE/ISAKMP SA).
Действия	Действия указываются в правилах и определяют метод обработки трафика: пропускать, сбрасывать или зашифровывать/расшифровывать.
ЛПБ, определяемые пользователем	ЛПБ, определяемые пользователем, позволяют администратору составлять типовые не изменяющиеся фрагменты ЛПБ и вставлять их в произвольное место итоговой ЛПБ, которая создается при трансляции ГПБ.
Домены	Домены позволяют реализовать модель разграничения прав доступа ПО ЗУ по принципу авторизации.

8.2 Регистрация сертификатов

Регистрация сертификата выполняется следующим образом:

1) запустить «ЗАСТАВА-Офис» (см. Приложение 3) и импортировать корневой сертификат УЦ с пометкой «Доверенный»;
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»;
4) зарегистрировать идентификатор локального сертификата «ЗАСТАВА-Офис» в объекте политики, представляющем ПО ЗУ Сервер.

Зарегистрировать сертификат можно также путем экспорта в агент созданного ПО ЗУ сертификата. Для того чтобы создать ключевую пару, необходимо нажать кнопку «Генерировать» и заполнить все поля в окне «Генерировать ключевую пару». Описание процесса работы с контекстным меню представлено в п. 6.4.1.1.9. Отправить созданный запрос в УЦ (в зависимости от требований УЦ использовать электронную почту, веб-браузер или другие средства). После получения сертификата из УЦ импортировать его в объект политики, для этого необходимо в контекстном меню окна ЦС выбрать команду «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 агента в окне «Токены» надо поставить наивысший приоритет тому ключевому носителю, который соответствует криптоалгоритму ключевой информации.

Если объект является кластером, то для него допустимо изменение алгоритма создания и обработки запроса на создание ключевой пары. Допускается создание параллельных запросов на создание ключевой пары для разных узлов кластера. Т.е. после создания ключевой пары для первого узла кластера эта функция будет оставаться доступной для остальных узлов. Создать еще один запрос для первого узла в этот момент невозможно.

8.3 Определяемая пользователем ЛПБ

Определяемая пользователем ЛПБ — это фрагмент ЛПБ в текстовом формате, содержащий установки устройства, которые не управляются непосредственно ПО ЗУ. ЛПБ можно создавать для любых видов объектов политики, кроме объекта «IP-хост» или любого неуправляемого объекта, доставка ЛПБ для которых невозможна.

Для перехода к просмотру и настройкам ЛПБ необходимо перейти во вкладку «Объекты политики» и выполнить шаги, изображенные на рисунке (см. Рисунок 259).

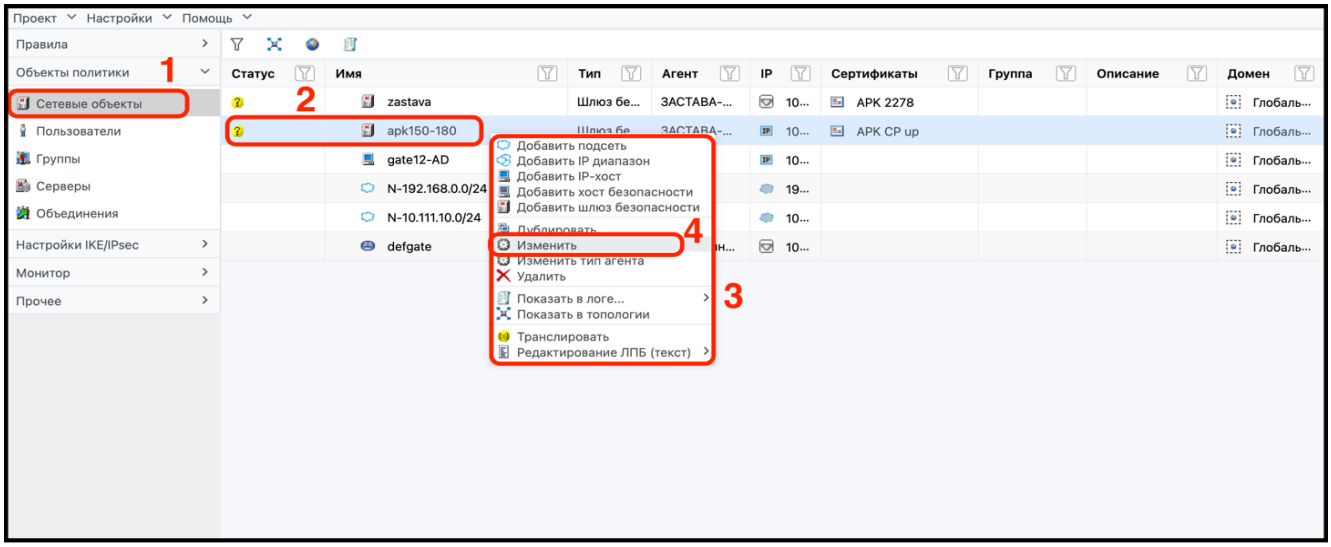


Рисунок 259 –Переход в ЛПБ

В окне элемента списка «Сетевые объекты» (цифра 1) выбрать требуемый объект (цифра 2), правой клавишей мыши вызвать его контекстное меню (цифра 3), где выбрать команду «Изменить» (цифра 4).

Далее перейти в окно «Трансляция политики» и выполнить шаги, изображенные на рисунке (рис. Рисунок 175).

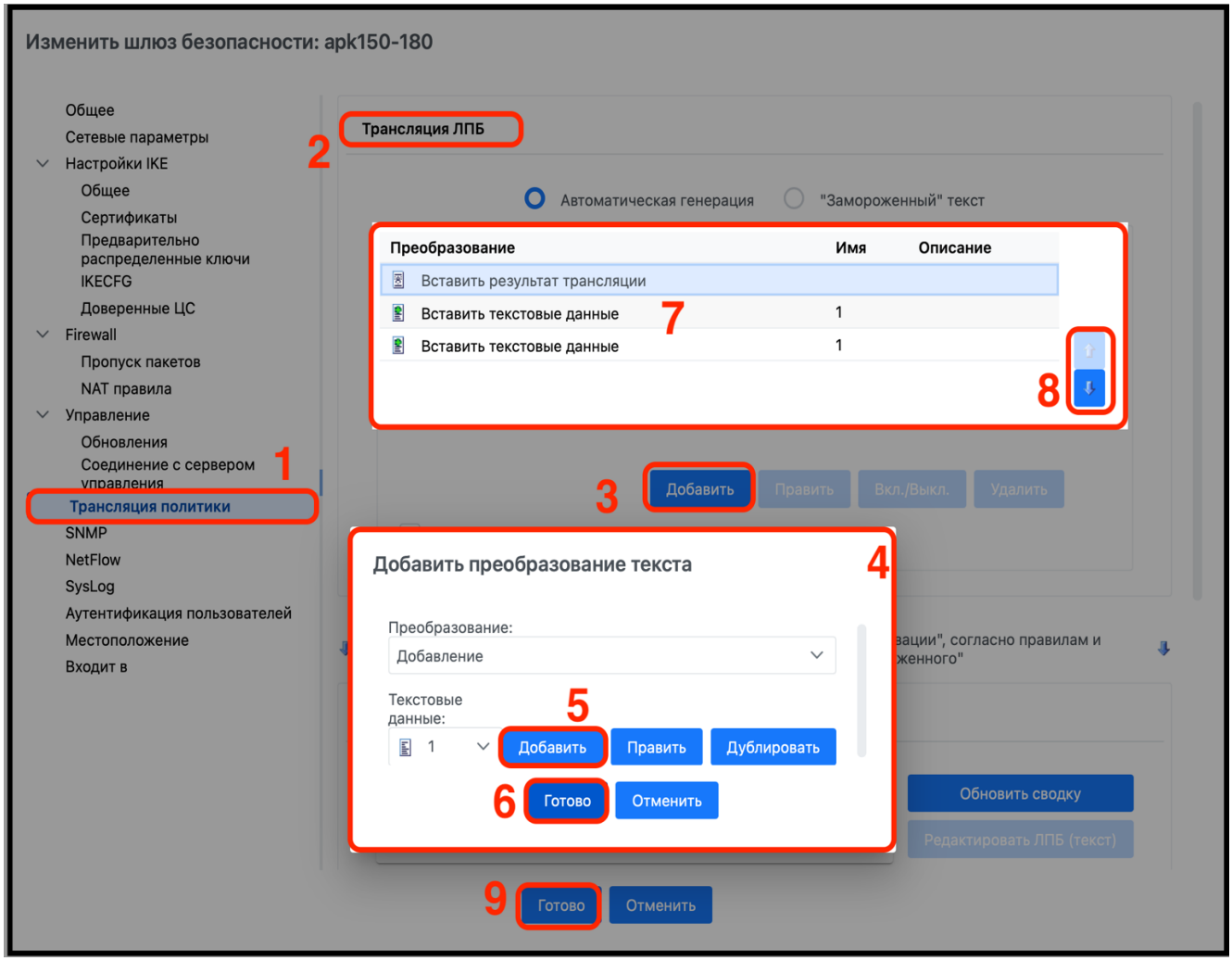


Рисунок 260 –Трансляция ЛПБ

Перейти в окно «Трансляция политики» (цифра 1). В открывшемся окне настроек «Трансляция ЛПБ» (цифра 2) нажать кнопку «Добавить» (цифра 3). Далее:

1) в открывшемся окне настроек «Добавить преобразование текста» (цифра 4) выполнить настройки и нажать кнопку «Добавить» (цифра 5);
2) в открывшемся окне написать фрагмент ЛПБ с помощью встроенного редактора или импортировать его из файла и нажать кнопку «Готово» (цифра 6);
3) в результате выполненных настроек в окне «Трансляция ЛПБ» (цифра 2) в списке «Преобразование» (цифра 7) отобразится список фрагментов ЛПБ. Изменить, если требуется, иерархию заданных ЛПБ (по умолчанию создается автоматически), используя элементы перемещения (цифра 8), вверх или вниз списка. Окончательная ЛПБ будет собрана из этих частей в указанном порядке в направлении сверху вниз.

8.4 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 в 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. Определяемые пользователем ЛПБ, помещенные над атрибутом «Автоматически созданная ЛПБ» будут добавлены в порядке сверху вниз, к началу «автоматически созданной» ЛПБ. Подобным образом определяемые пользователем ЛПБ, помещенные под атрибутом, будут добавлены в порядке снизу вверх к концу автоматически созданной ЛПБ.

Если необходимо определить одну неизменную ЛПБ для отдельного защищённого агента (на которую не будут влиять изменения в ГПБ), требуется выполнить шаги, изображенные на рисунке (см. Рисунок 261).

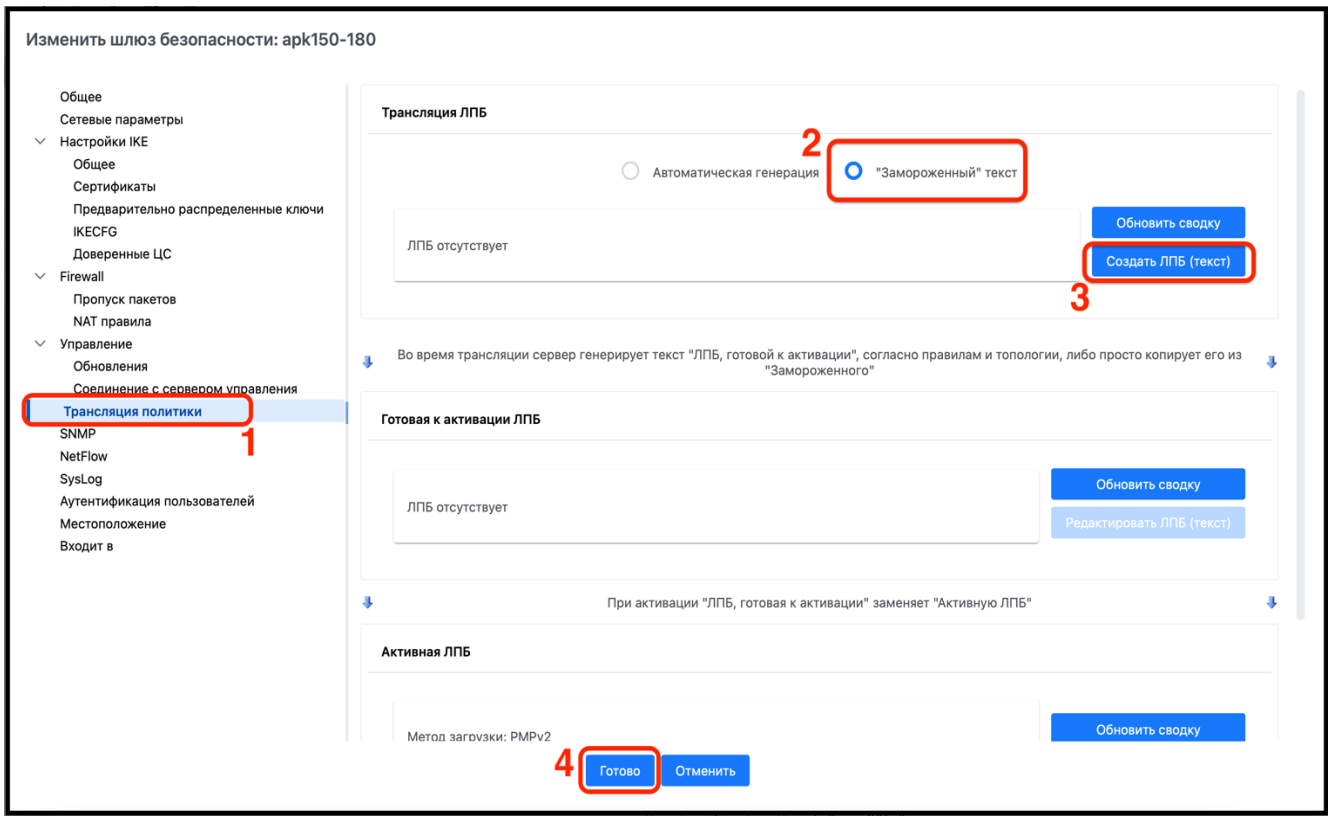


Рисунок 261 – Настройка неизменной ЛПБ

Перейти в окно «Трансляция политики» (цифра 1) и установить флажок в положение «Замороженный текст» (цифра 2). Нажать кнопку «Создать ЛПБ (текст)» (цифра 3), в открывшемся текстовом редакторе написать требуемый текст. Нажать кнопку «Готово» (цифра 4).

В результате 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 не будет убрана отметка из соответствующего поля, и пока снова не будет преобразована и активирована ГПБ. Пиктограмма объекта везде будет отмечена как замороженная «  ». ЛПБ должна быть создана или импортирована для этого объекта политики.

8.4.1 Блок «Структура ЛПБ»

Определяемые пользователем ЛПБ в текстовом формате могут быть добавлены в начало и/или конец ЛПБ агента, оттранслированной из полученной агентом ГПБ. Добавляемые фрагменты могут быть созданы вручную или импортированы из файла (о том, как создавать определяемые пользователем ЛПБ, см. п. 8.3).

Блок «Структура ЛПБ» содержит атрибут «Автоматически созданная ЛПБ». Этот атрибут указывает на местонахождение ЛПБ, оттранслированной из ГПБ в общей ЛПБ. То есть, если определяемая пользователем ЛПБ (фрагмент ЛПБ) помещена 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 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» можно, 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 её с помощью кнопок со стрелками <вверх> и <вниз>.

8.5 Общие задачи

8.5.1 Форма для работы с сертификатами

Работа с сертификатами включает в себя:

— добавление (пример добавления сертификата представлен в п. 8.5.1.1);
— импорт (пример импорта сертификата представлен в п. 8.5.1.2);
— создание (пример создания сертификата представлен в п. 8.5.1.3);

— загрузку списка сертификатов (пример загрузки сертификата представлен в п. 8.5.1.4).

Для работы с сертификатами необходимо перейти в элемент списка «Сетевые объекты» и выполнить шаги, изображенные на рисунке (см. Рисунок 262).

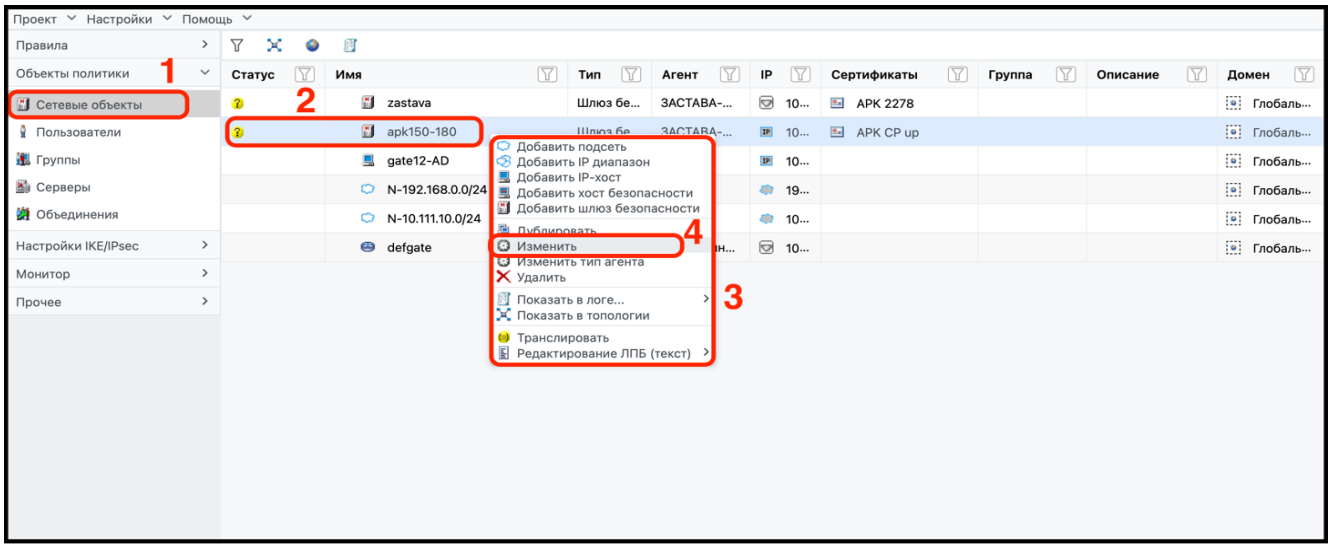


Рисунок 262 – Переход в окно настроек выбранного объекта

В окне «Сетевые объекты» (цифра 1) выбрать требуемый объект, для которого требуется сертификат (цифра 2), дважды нажать на него или вызвать правой клавишей мыши его контекстное меню (цифра 3), затем выбрать команду «Изменить» (цифра 4).

8.5.1.1 Пример 1. Добавления сертификата

Если файла с сертификатом нет, то необходимо его добавить и заполнить поля формы вручную. Для этого в открывшемся окне настроек выбранного объекта необходимо перейти в окно «Сертификаты» и выполнить шаги, изображенные на рисунке (см. Рисунок 263).

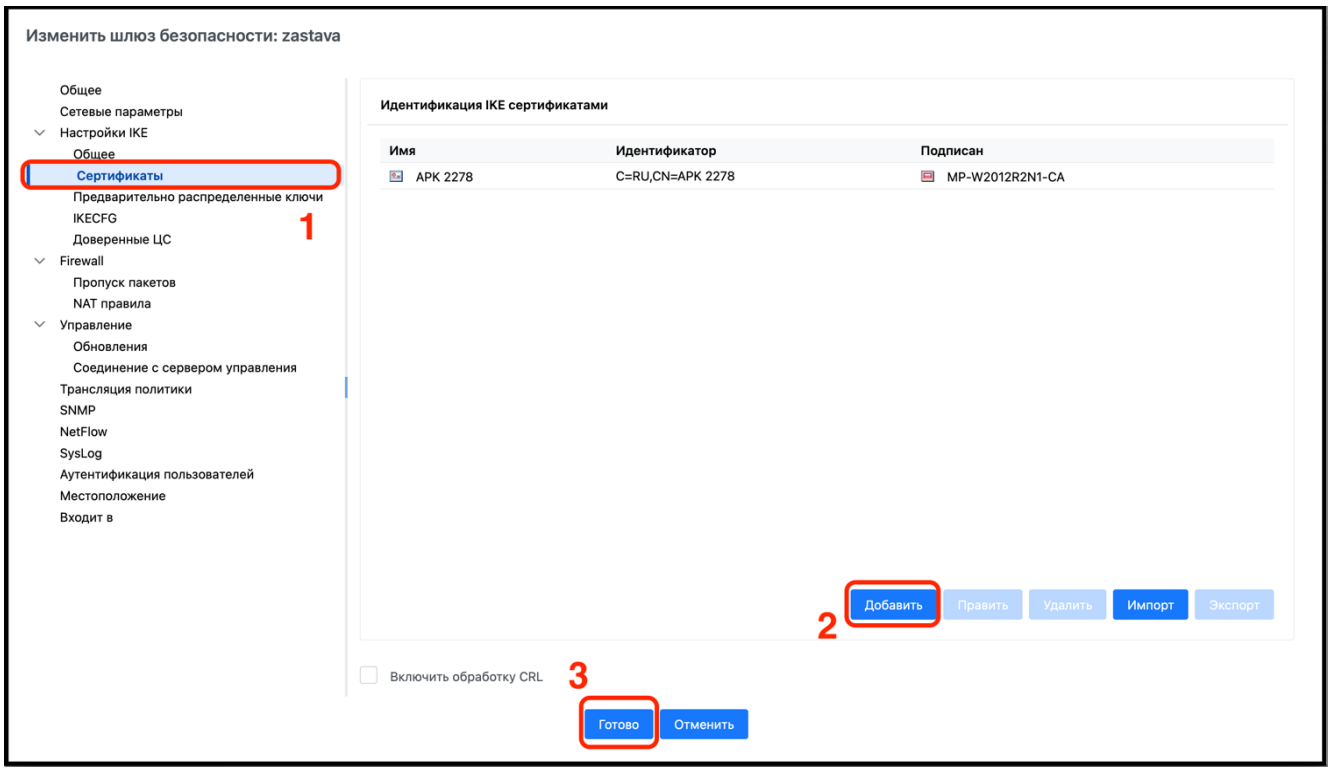


Рисунок 263 – Окно настроек объекта

Перейти в окно «Сертификаты» (цифра 1) и нажать кнопку «Добавить» (цифра 2). Информацию о сертификате ввести вручную (сам сертификат в ПО ЗУ не импортирован). Выполнить настройку сертификата, описание которой приведено в п. 6.5.5.2.

8.5.1.2 Пример 2. Импорт сертификата

Если есть файл с выпущенным для выбранного объекта сертификатом (и, возможно, с секретным ключом), то импортировать его можно, выполнив шаги, изображенные на рисунке (см. Рисунок 264).

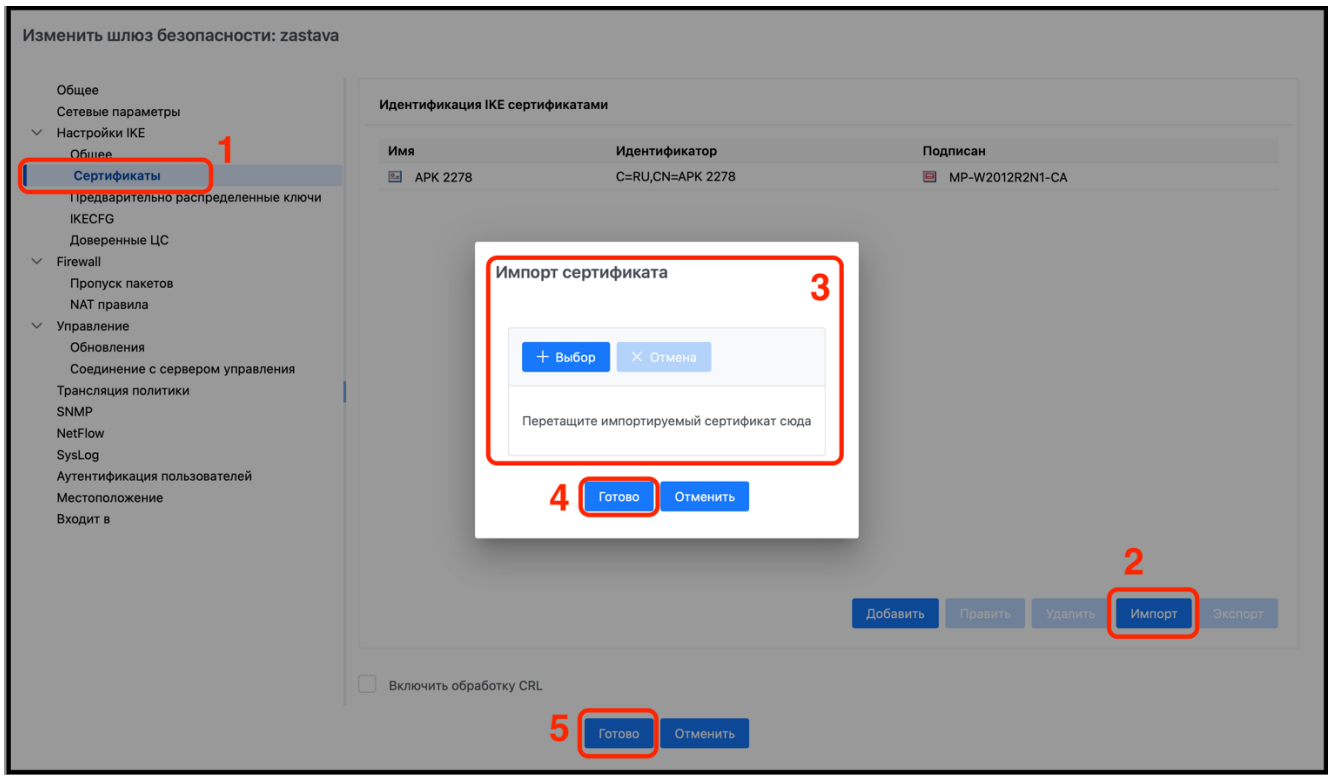


Рисунок 264 – Импорт сертификата (пример 2)

В окне «Сертификаты» (цифра 1) необходимо нажать кнопку «Импорт» (цифра 2). Переместить импортируемый сертификат в открывшееся окно «Импорт сертификата» (цифра 3) или добавить его, нажав кнопку «+Выбор», далее нажать кнопку «Готово» (цифра 4). Сертификат и закрытый ключ (при наличии) будут импортированы в ПО ЗУ.

8.5.1.3 Пример 3. Создание сертификатов

В ПО ЗУ предусмотрены дополнительные возможности для работы с агентами:

— создавать в ПО ЗУ сертификаты и экспортировать их в агент и ГПБ (Пример 3);

— импортировать в ПО ЗУ сертификаты, зарегистрированные в агенте (Пример 4).

Для того чтобы создать сертификат и добавить его для выбранного объекта политики, необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 265).

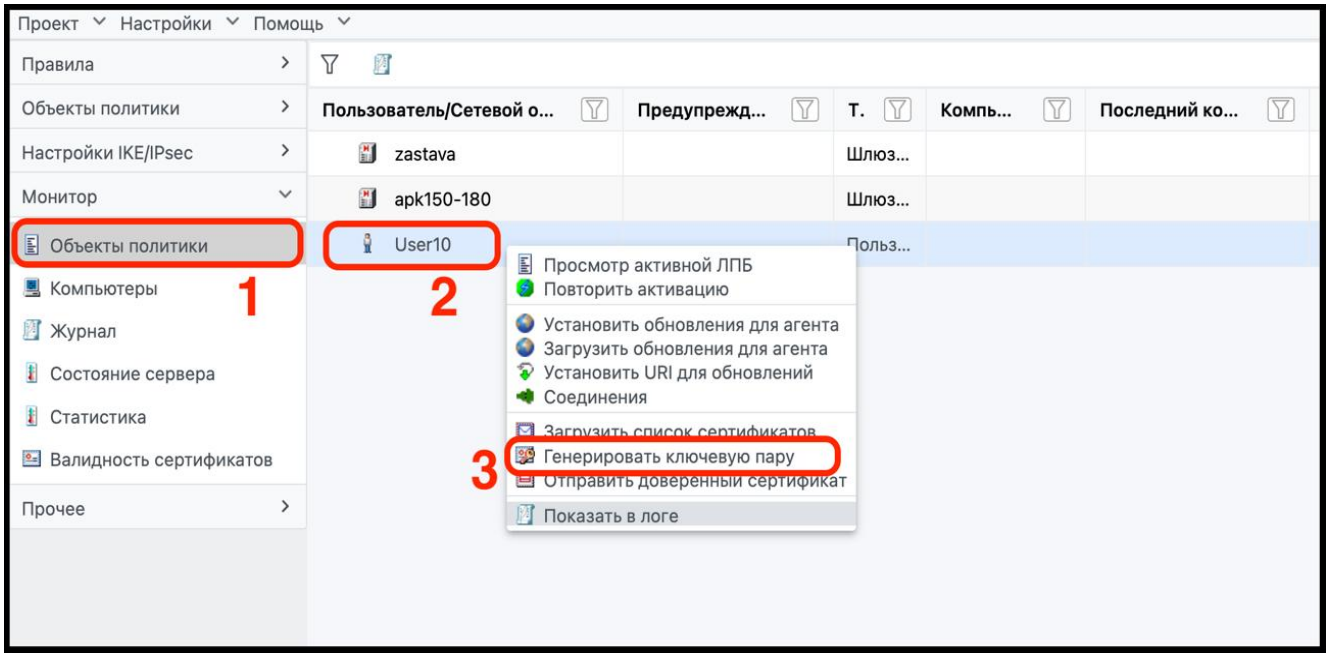


Рисунок 265 – Создание сертификатов

Перейти в элемент списка «Объекты политики» (цифра 1), выбрать требуемый объект (цифра 2) и в его контекстном меню выбрать команду «Генерировать ключевую пару» (цифра 3).

В результате откроется окно «Создать запрос сертификата», в котором требуется выполнить шаги, изображенные на рисунке (см. Рисунок 266).

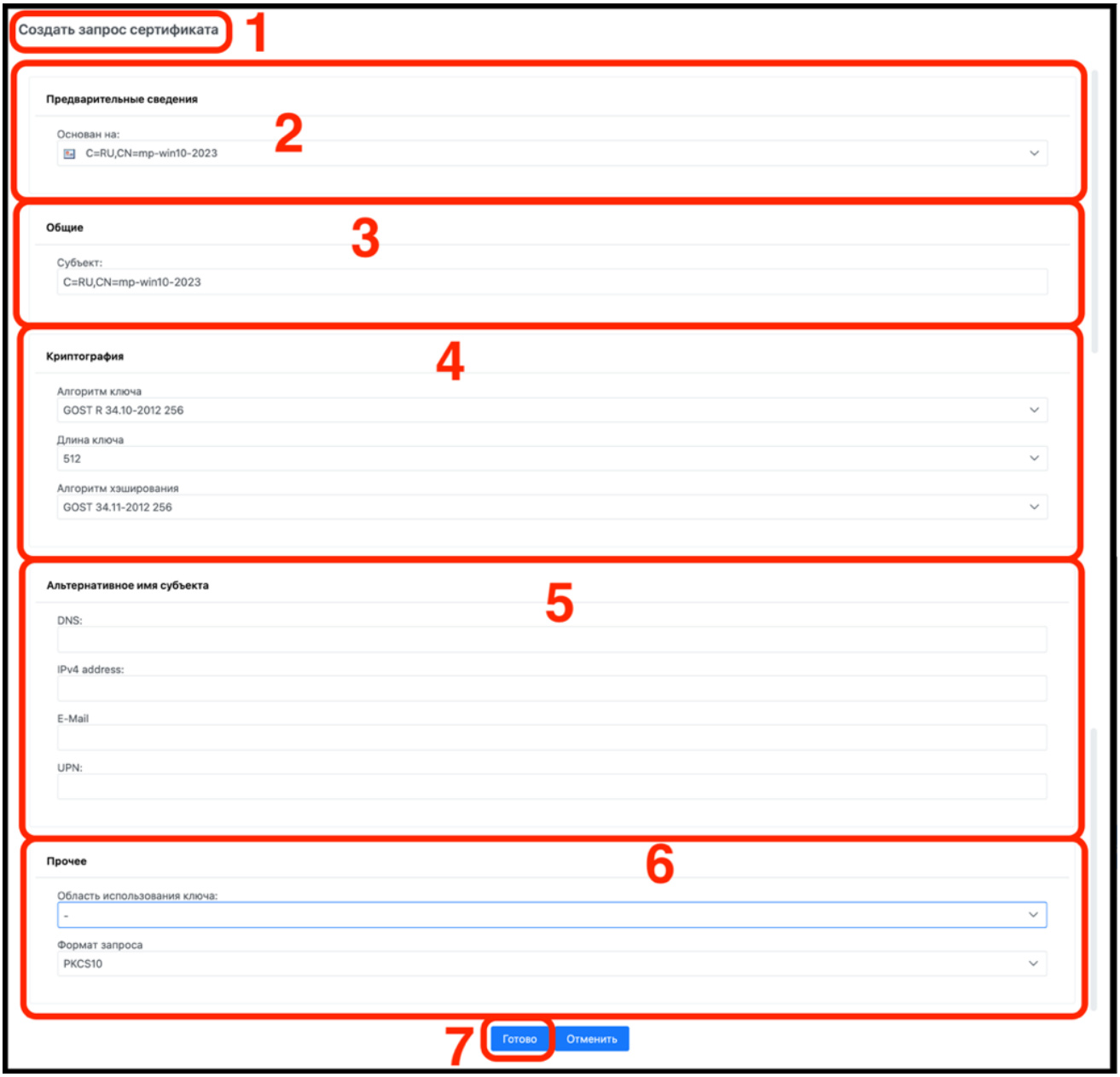


Рисунок 266 – Окно запроса сертификата

В окне «Создать запрос сертификата» (цифра 1) ввести информацию о сертификате:

1) в блоке «Предварительные сведения» (цифра 2) выбрать параметры «Основан на»
2) в блоке «Общие» (цифра 3) ввести информацию о субъекте;
3) в блоке «Криптография» (цифра 4) выбрать алгоритм и длину ключа, а также алгоритм хэширования;
4) заполнить, если требуется, параметры блока «Альтернативное имя субъекта» (цифра 5);
5) определить, если требуется, в блоке «Прочее» (цифра 6) область использования ключа и формат запроса;
6) нажать кнопку «Готово» (цифра 7).

Вид окна элемента списка «Объекты политики» в результате выполненных действий изображен на рисунке (см. Рисунок 267).

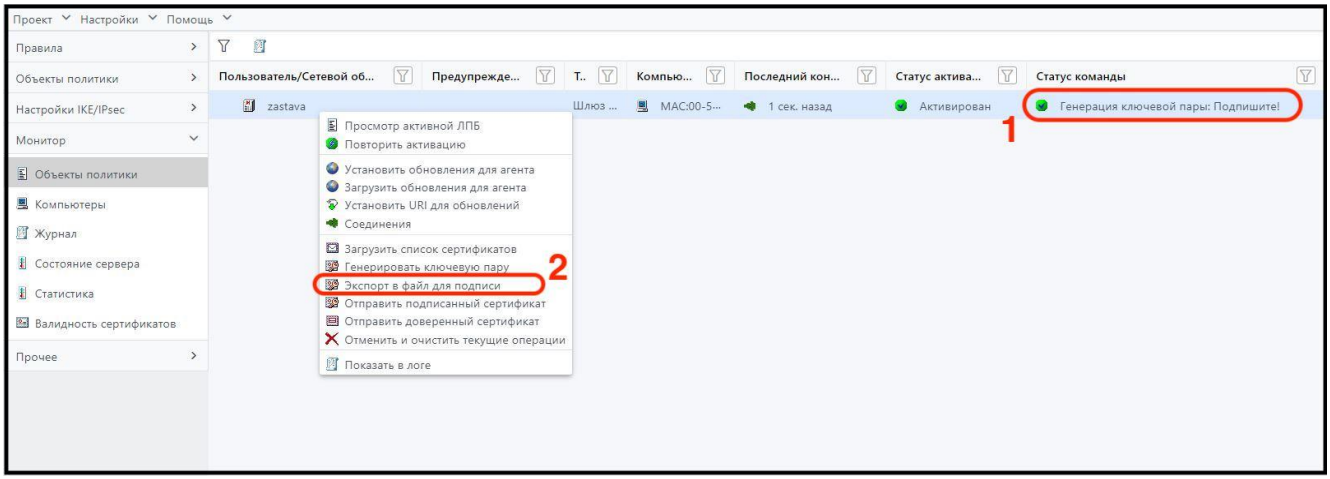


Рисунок 267 – Экспорт сертификатов

Параметр «Статус команды» изменится на «Генерация ключевой пары: Подпишите!» (цифра 1). Вызвать правой клавишей мыши контекстное меню объекта и выбрать команду «Экспорт в файл для подписи» (цифра 2).

Вид окна элемента списка «Объекты политики» в результате выполненных действий изображен на рисунке (см. Рисунок 268).

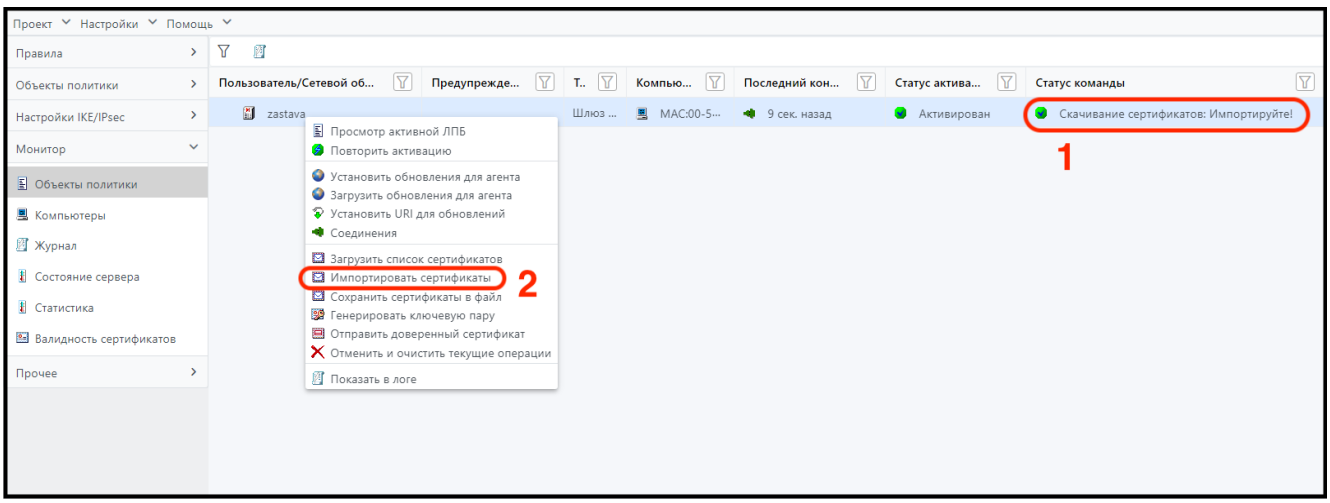


Рисунок 268 – Импорт сертификатов

В результате выполненных действий статус команды изменится на «Скачивание сертификатов: Импортируйте!» (цифра 1). Вызвать правой клавишей мыши контекстное меню объекта и выбрать команду «Импортировать сертификаты» (цифра 2). Сертификат будет добавлен в ГПБ и отправлен агенту.

При несоответствии параметров сертификата в контейнере и параметров в запросе на создание ключевой пары в ПО ЗУ возникнет предупреждение в момент экспорта запроса в буфер обмена или в файл.

Для удаления запроса на создание ключевой пары, необходимо выбрать команду контекстного меню «Отменить и очистить текущие операции».

8.5.1.4 Пример 4. Загрузка списка сертификатов

Можно загрузить список сертификатов из агента, для этого необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 269).

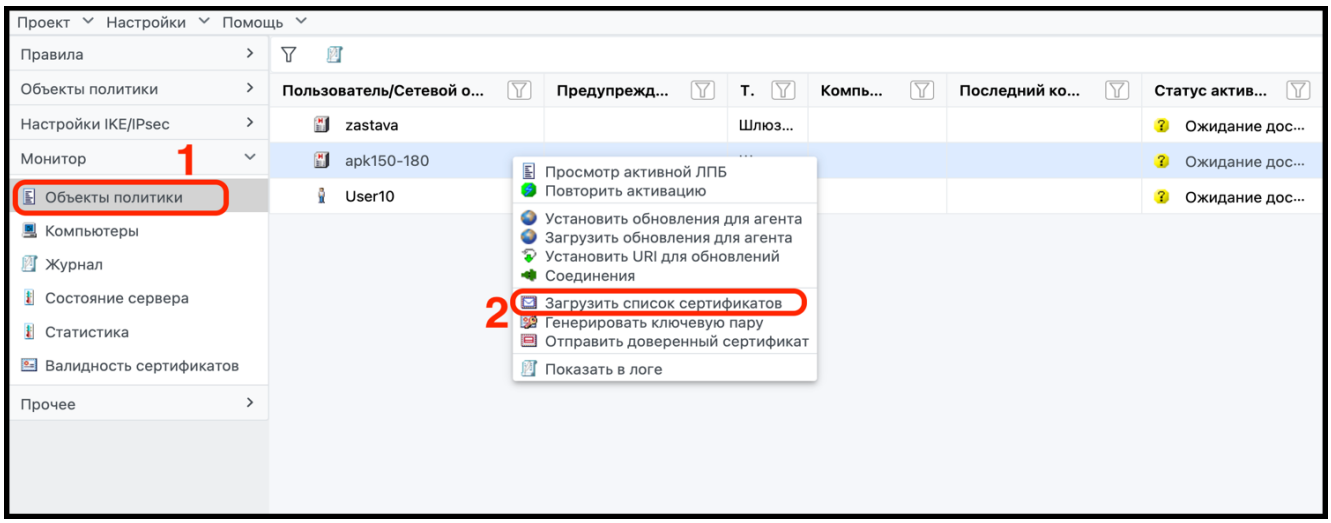


Рисунок 269 – Загрузить список сертификатов

Перейти в элемент списка «Объекты политики» (цифра 1), вызвать правой клавишей мыши контекстное меню объекта и выбрать команду «Загрузить список сертификатов» (цифра 2).

Вид окна элемента списка «Объекты политики» в результате выполненных действий изображен на рисунке (см. Рисунок 270).

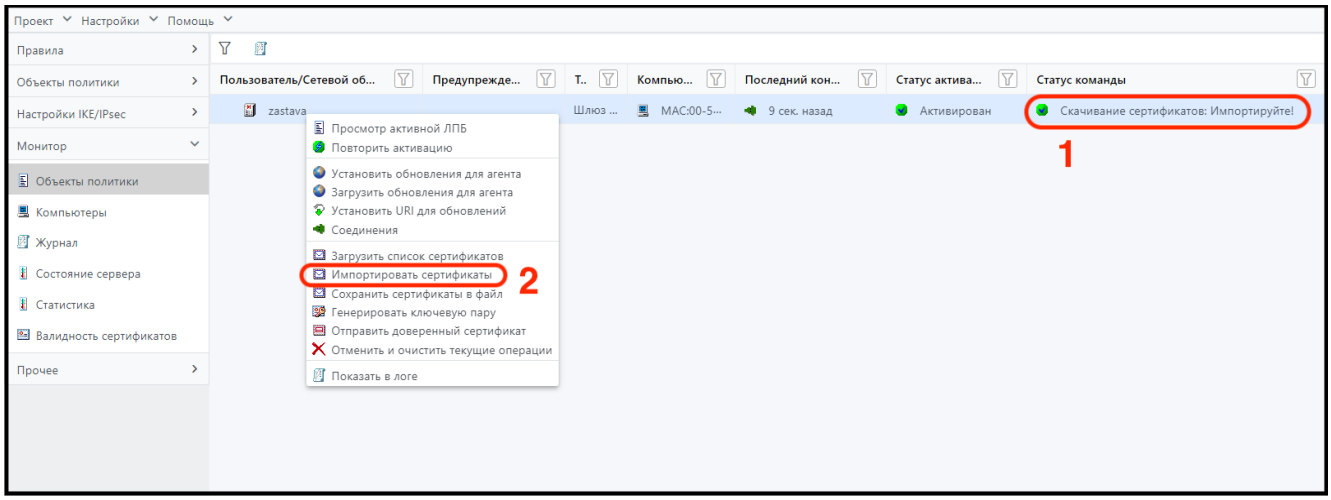


Рисунок 270 – Импорт сертификатов

В результате выполненных действий изменится статус команды на «Скачивание сертификатов: Импортируйте!» (цифра 1). Вызвать правой клавишей мыши контекстное меню объекта и выбрать команду «Импортировать сертификаты» (цифра 2).

8.5.2 Редактирование серверного правила

Убедиться, что в политике есть сервер требуемого типа, или создать его (см. п. 6.2.4.2). Для редактирования серверного правила необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 271).

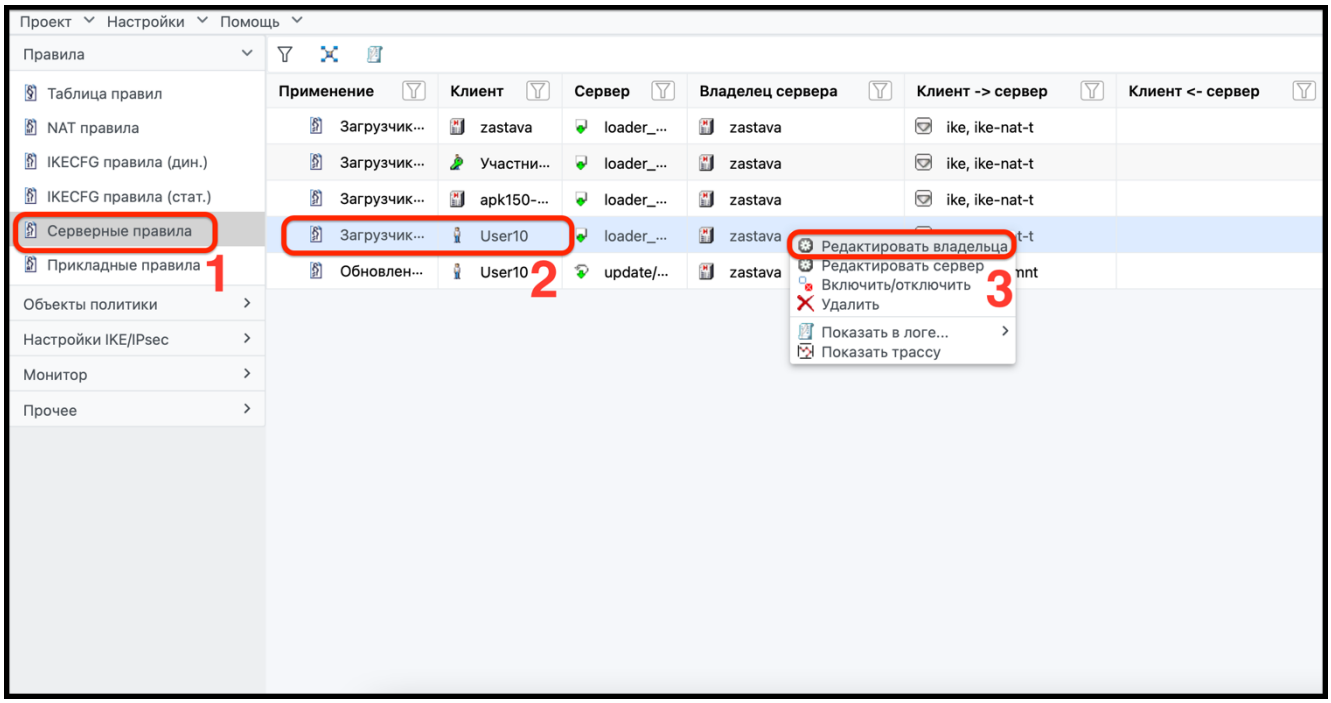


Рисунок 271 – Переход в редактирование владельца

Во вкладке боковой панели «Правила» перейти в элемент списка «Серверные правила» (цифра 1) и выбрать требуемый объект (цифра 2). Вызвать правой клавишей мыши контекстное меню объекта и выбрать команду «Редактировать владельца» (цифра 3).

В результате откроется окно настроек «Изменить пользователя» выбранного объекта, в котором необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 272).

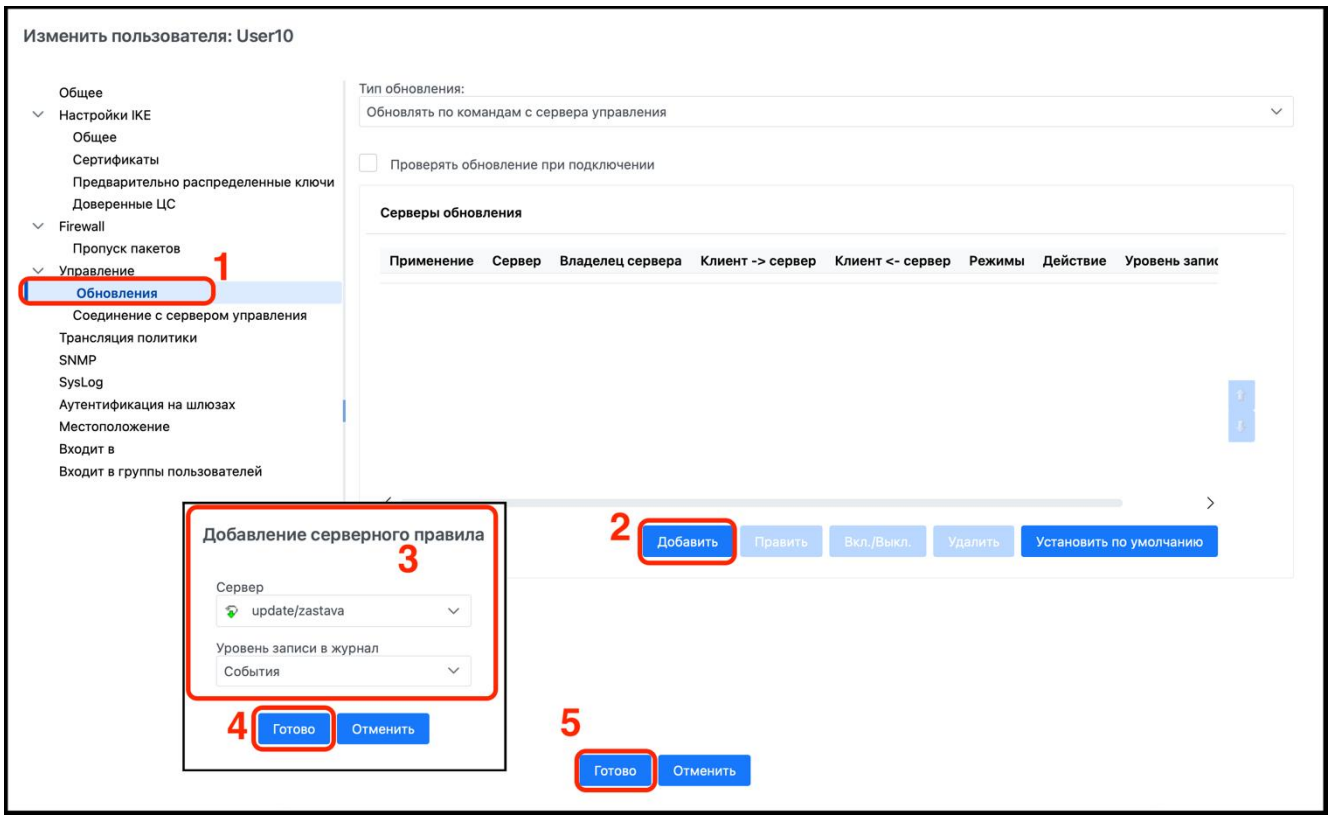


Рисунок 272 – Окно изменения серверного правила

Перейти в окно «Обновления» (цифра 1) и нажать кнопку «Добавить» (цифра 2). В открывшемся окне настроек «Добавления серверного правила» (цифра 3) необходимо выбрать «Сервер» и «Уровень записи в журнал». Нажать кнопку «Готово» (цифра 4). Затем нажать кнопку «Готово» в окне «Изменить пользователя» (цифра 5).

В результате выполненных действий в таблице отобразиться отредактированное серверное правило. Возможности управления правилами изображены на рисунке (см. Рисунок 273).

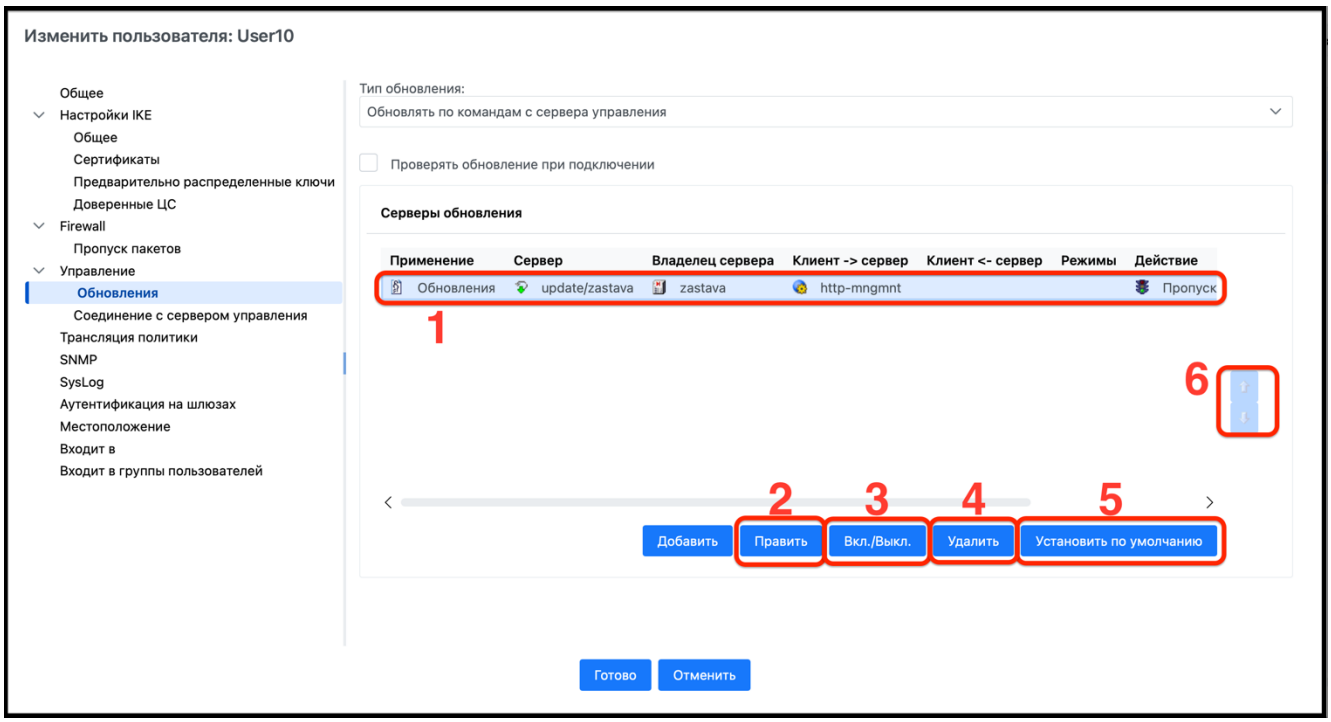


Рисунок 273 – Окно изменения серверного правила

Для управления правилом требуется выбрать его в списке (цифра 1) и произвести требуемые действия:

— редактировать, нажав кнопку «Править» (цифра 2);

— включить или выключить, нажав кнопку «Вкл/Выкл» (цифра 3);

— удалить правило, нажав кнопку «Удалить» (цифра 4);

— установить по умолчанию, нажав кнопку «Установить по умолчанию» (цифра 5);

— задать приоритет правилам: выделить требуемое правило, переместить его стрелкой вверх или вниз (цифра 6), указав нужный порядок их появления в ЛПБ.

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

1) в конфигурацию объекта будут добавлены команды и правила, обеспечивающие взаимодействие объекта с данным сервером;
2) в конфигурации самого объекта, привязанного сервера и, при включенном состоянии, - в конфигурациях промежуточных маршрутизаторов, будут созданы фильтры для пропускания соответствующего трафика.

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 «Клиент->сервер»). Если правило выключено, то соответствующие фильтры не транслируются.

8.5.3 Создание и редактирование NAT-правил для шлюзов безопасности

ПО ЗУ поддерживает работу с сетями, где используется трансляция сетевых адресов (NAT) различных видов:

– статическая трансляция адресов (static NAT);

– динамическая трансляция адресов (dynamic NAT, 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 ПО ЗУ необходимо создать объект «Шлюз безопасности».

Для некоторых типов агентов возможно активное управление NAT-конфигурацией (путем включения команд NAT в ЛПБ агента), для остальных агентов ПО ЗУ 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).

Подробное описание добавления и редактирования правил NAT представлено в п. 6.1.2.

8.5.4 Настройка получения обновлений агентов политики

Обновление агента производится по команде СВТ с установленным ПО ЗУ. Обращение к серверу обновлений производится по открытому протоколу HTTP. При необходимости защиты данного соединения можно воспользоваться штатными средствами ПО ЗУ (создать в ПО ЗУ правило для защищенного соединения между обновляемым агентом и сервером обновления).

Для настройки обновления агента через ПО ЗУ необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 274).

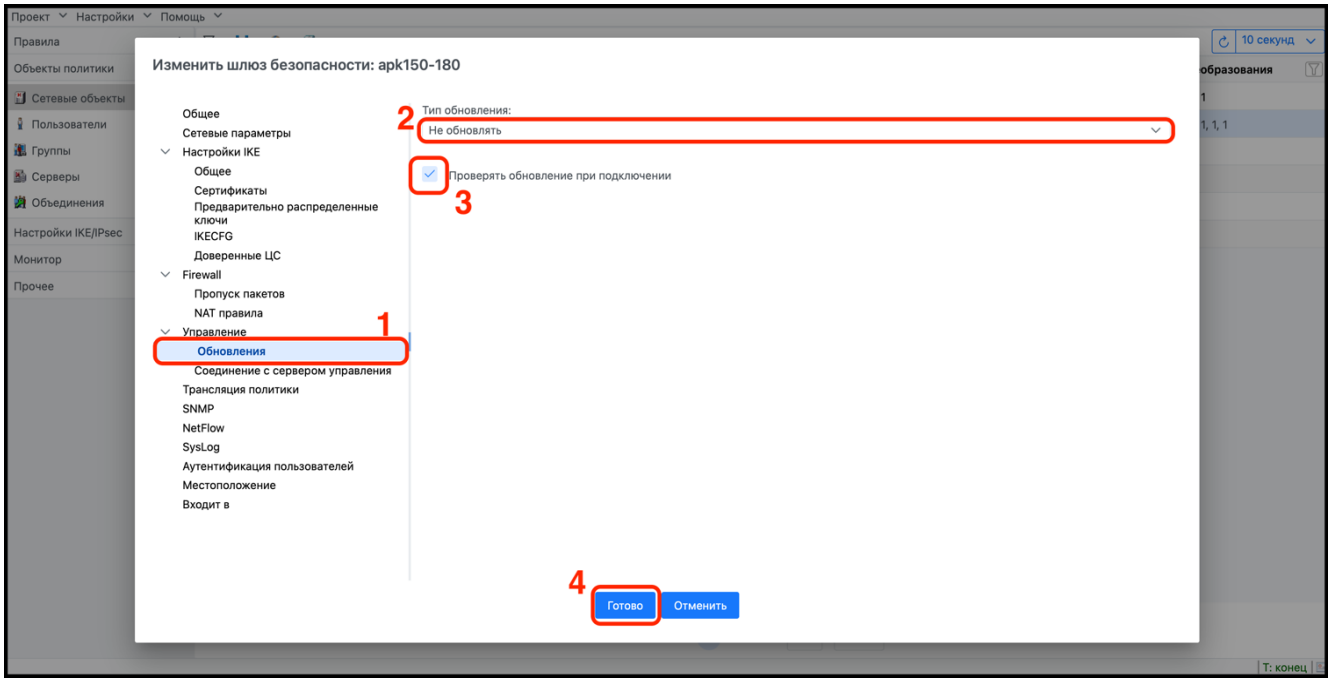


Рисунок 274 – Настройка автоматического обновления

Перейти в окно настроек выбранного объекта. В открывшемся окне «Изменить шлюз безопасности» перейти в окно «Обновления» (цифра 1), в котором:

1) выбрать из выпадающего списка «Тип обновления» требуемый вариант (цифра 2):
— обновлять по командам с сервера управления;
— не обновлять;
2) установить, если требуется, флажок напротив настройки «Проверять обновление при подключении» (цифра 3);
3) нажать кнопку «Готово» (цифра 4).

8.5.5 Управляемые шлюзы безопасности (ЗАСТАВА-Офис)

Установить курсор в рабочей области окна «Топология» или выбрать элемент списка «Сетевые объекты» во вкладке боковой панели «Объекты политики», вызвать правой клавишей мыши контекстное меню и выбрать команду «Добавить шлюз безопасности». В открывшемся

окно «Выберите версию агента» выполнить шаги, изображенные на рисунке (см. Рисунок 275).

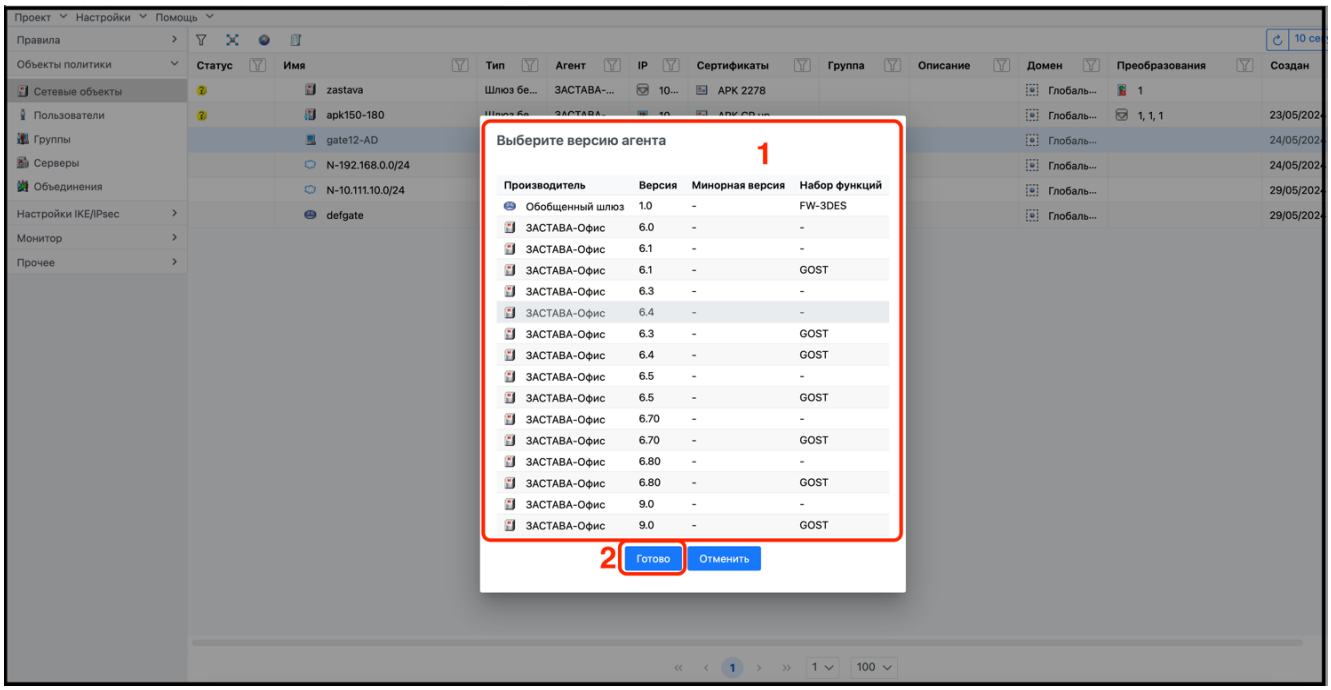


Рисунок 275 – Шлюз безопасности, выбор версии агента

В открывшемся окно «Выберите версию агента» (цифра 1) выбрать требуемого агента и нажать кнопку «Готово» (цифра 2).

Описание дальнейшей настройки приведено в п. 7.1.5.

8.5.6 Неуправляемые шлюзы безопасности

Установить курсор в элементе списка «Топология» или выбрать элемент списка «Сетевые объекты» в секции «Объекты политики», используя команду «Добавить», выбрать требуемый шлюз безопасности. В окне «Общее» выполнить действия:

1) указать производителя и версию агента, которого будет представлять этот шлюз безопасности в окне «Выбор дескриптора агента». В окне «Общее» ввести имя шлюза безопасности;
2) убрать отметку в поле «Управляемый»;

Далее настройка производится по описанию, приведённому в п. 7.1.5.

8.5.7 Объекты типа «Шлюз безопасности» в кластерном исполнении

Объекты типа «Шлюз безопасности» могут быть установлены и сконфигурированы для работы в режиме высокой надёжности в кластерной информационной системе.

Если создаваемый шлюз безопасности является кластером, то необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 277).

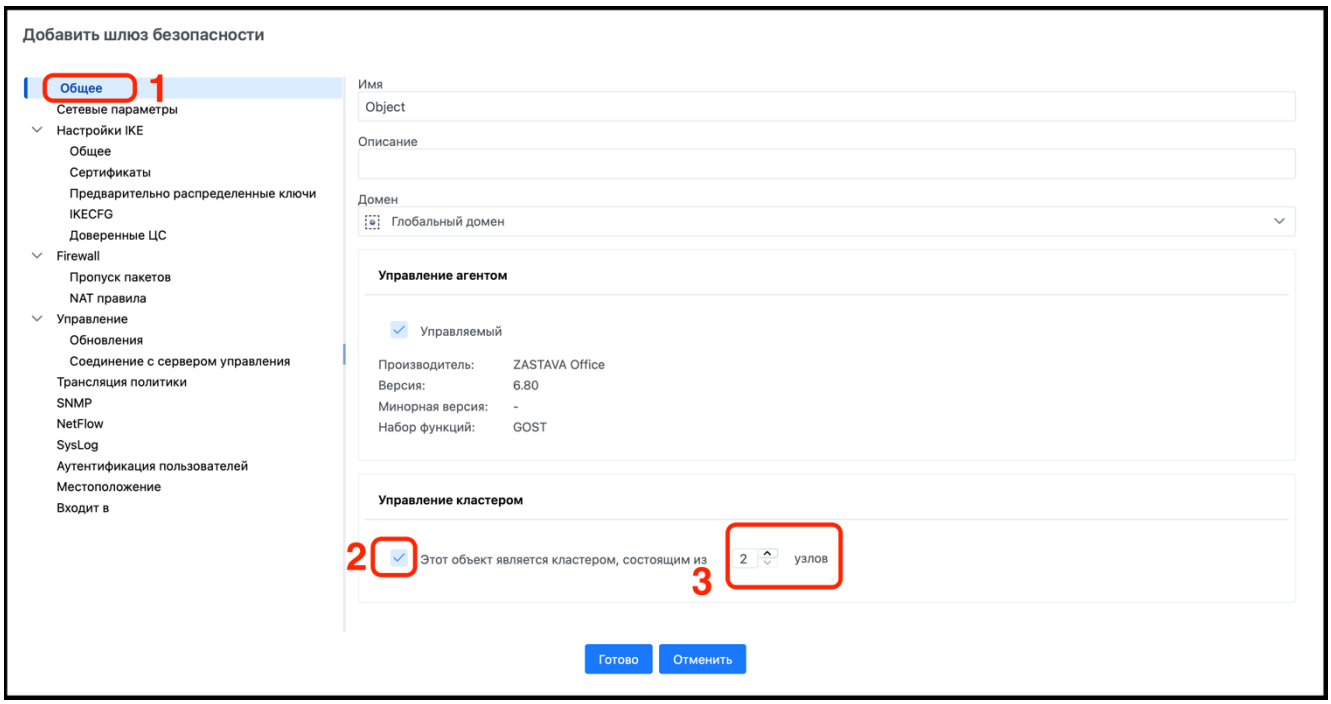


Рисунок 276 – Настройка шлюза безопасности в кластерном исполнении

Во вкладке «Общее» (цифра 1) установить флажок напротив «Этот объект является кластером» (цифра 2). Выбрать количество узлов (цифра 3). Перейти во вкладку настроек «Сетевые параметры и выполнить шаги, изображенные на рисунке (см. Рисунок 257).

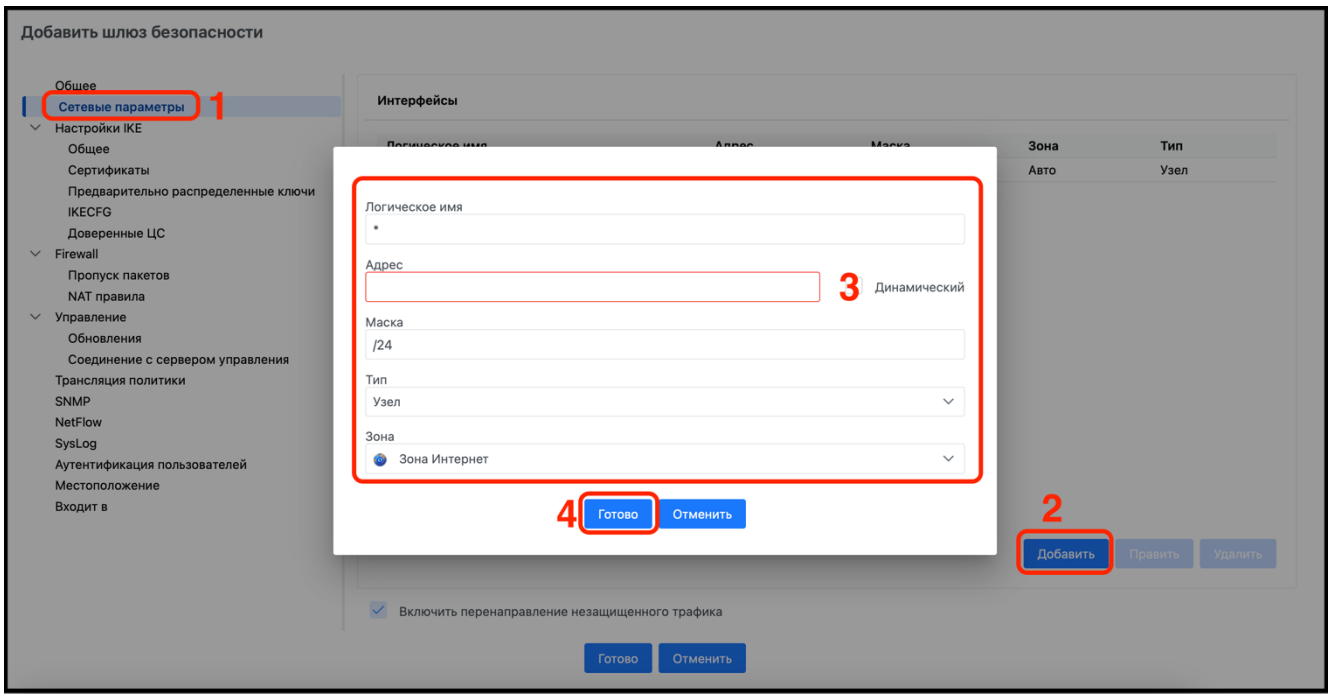


Рисунок 277 – Сетевые настройки шлюз безопасности в кластерном исполнении

Во вкладке «Сетевые настройки» (цифра 1) нажать кнопку «Добавить» (цифра 2). В открывшемся окне настроек (цифра 3) ввести:

— логическое имя;

— в поле «Адрес» указать 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;

— назначить маску;

— в выпадающем списке «Тип» выбрать тип интерфейса,

— в выпадающем списке «Зона» выбрать требуемый вариант.

Зарегистрировать локальные сертификаты каждого узла. В агентах на узлах кластера зарегистрировать эти сертификаты в качестве локальных и дать имена интерфейсам. Создать правило, транслировать и активировать ГПБ.

8.5.8 Загрузка сертификатов для каждого узла кластера

Для дескриптора агента версии 6.1 и выше доступна загрузка сертификатов для каждого узла кластера. Для этого необходимо во вкладке «Монитор» в элементе списка «Объекты политики» вызвать контекстное меню, нажав правой клавишей мыши на требуемый объект, затем выбрать требуемую команду «Загрузить список сертификатов» (описание приведено в п. 6.4.1.1.8).

В окне «Выберите узел кластера» выбрать номер узла кластера (Описание процесса работы с представлено 8.5.7) и нажать кнопку «Готово». После загрузки сертификатов необходимо выполнить команду «Добавить полученные сертификаты в политику». В появившемся окне «Импорт сертификатов» проверить полученные от агента сертификаты и нажать кнопку «Готово». обновление и загрузка обновлений для каждого узла кластера

8.5.9 Обновление шлюза безопасности в кластерном исполнении

Для дескриптора агента версии 6.1 и выше доступно обновление и загрузка обновлений для каждого узла кластера. Для этого необходимо воспользоваться командами контекстного меню «Загрузить обновления для агента» и «Обновить версию агента» (описание приведено в п. 6.4.1.1.4 и п. 6.4.1.1.5 соответственно).

Для обновления отдельного узла кластера необходимо выбрать в поле номер узел кластера. Если оставить в поле 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 «Сертификаты», это произойдет автоматически по следующему алгоритму:

— у сертификатов с ненулевым номером узла, но на НЕ кластерах, номер узла устанавливается равным 0;

— у сертификатов с нулевым номером узла (или номером узла больше размера кластера) на кластерах номер узла выбирается следующим образом: будет

присвоен первый номер, для которого еще нет сертификата, такие сертификаты рассматриваются в алфавитном порядке по полю sn;

— если свободных номеров нет, то номер узла не меняется.

Во всех трех случаях создаются предупреждения о не заданных номерах узлов кластеров:

— 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 vdb_server.log.

После этого можно прогружать агенты с ПО ЗУ по протоколу PMPv2.

8.5.10 Редактирование параметров шлюза безопасности

Для того чтобы отредактировать шлюз безопасности, надо выбрать его в элементе списка «Топология» или «Объекты политики», используя команду «Изменить». Появившееся окно «Свойства» идентично окну «Добавить объект шлюз безопасности» см. п. 7.1.5.

8.5.11 Работа с сообщениями 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 направлять серверу, указав их в окне настроек SNMP. Для изменения статуса SNMP-сообщения надо выделить его в списке и использовать кнопки со стрелками <вправо> и <влево> для его перемещения в списке. Сообщения используют не все агенты. Ниже в таблице (см. Таблица 33) приведён список сообщений.

Таблица 33 - 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 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
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
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 аутентифицировался в ПО линейки «ЗАСТАВА»
USER_LOGIN_ERROR	Ошибка при аутнитификации пользователя в ПО линейки «ЗАСТАВА»

Сообщения	Значение
USER_LOGOFF	Пользователь успешно вышел из в ПО линейки «ЗАСТАВА»
IPSEC_SA_CREATED	Успешно создано новое IPsec-соединение
IPSEC_SA_DELETED	IPsec-соединение удалено
ADMIN_LOGIN_OK	Администратор успешно вошёл в в ПО линейки «ЗАСТАВА»
ADMIN_LOGIN_ERROR	Ошибка при входе администратора в ПО линейки «ЗАСТАВА»
ADMIN_LOGOFF	Администратор успешно вышел из в ПО линейки «ЗАСТАВА»
VPNSVC_LOADED	Успешно загружены системные сервисы
VPNSVC_INLOADED	Системные сервисы не загружены

8.6 Объекты УЦ (ЦС)

Для просмотра объектов УЦ требуется выполнить шаги, изображенные на рисунке (см. Рисунок 278).

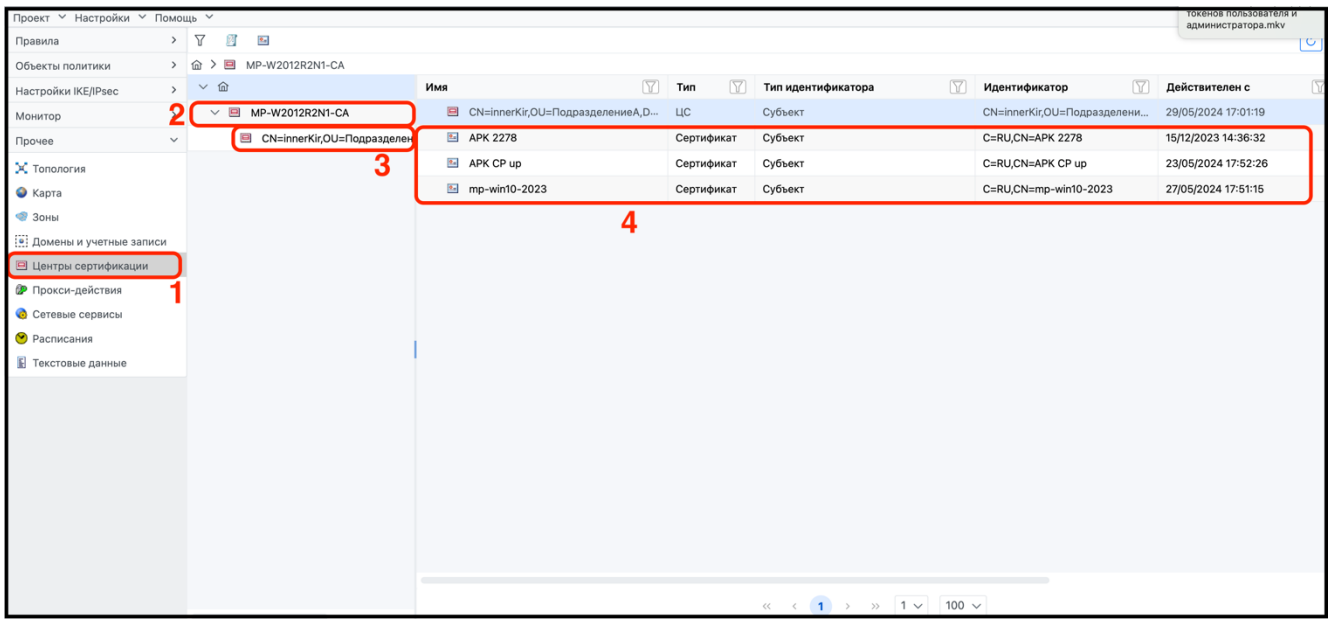


Рисунок 278 – Объекты УЦ

Выбрать вкладку боковой панели «Прочее», далее перейти в элемент списка «Центры сертификации» (цифра 1), выбрать в списке УЦ (цифра 2), в выпадающем списке выбрать ЦС (цифра 3), в области рабочей таблицы отобразится список сертификатов, принадлежащих выбранному УЦ (цифра 4).

8.6.1 Основные сведения

Окно ЦС содержит описания УЦ, которые издают сертификаты и СОС. Описание УЦ представляет собой описание сертификата УЦ, принадлежащего данному УЦ.

Вводить описание УЦ обязательно только в некоторых случаях, например, некоторые агенты требуют наличия в конфигурации информации о сертификате УЦ, которым подписан сертификат партнера по связи.

Для создания описания УЦ надо выбрать в контекстном меню элемент списка «Добавить ЦС» и заполнить все необходимые поля или выбрать в контекстном меню команду «Импорт», после чего указать файл с нужным сертификатом см. п 6.5.5.1.

Возможен также ввод описания УЦ вручную, перечень и описание параметров приведены в таблице (см. Таблица 33).

Таблица 34 – Описание параметров «Certificate Authority»

Параметр	Значение
Имя	Название объекта. При импорте 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»
Субъект (Subject)	Информация о владельце в формате DN (Distinguished Name). Владельцем сертификата является сам УЦ. При импорте реального сертификата это значение выбирается из его поля «Subject»
Действителен с	Время действия сертификата в формате «дд.мм.гггг чч.мм.сс»
Действителен по	Время действия сертификата в формате «дд.мм.гггг чч.мм.сс»

8.6.2 Дополнительные сведения

Объекты типа «Certificate Authority» могут создаваться в контекстном меню «Добавить ЦС», либо путем импорта 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 такого объекта там еще нет).

9 РАБОТА С ПРОЕКТАМИ И ГПБ

В результате добавления всех требуемых объектов политики, входящих в защищенную систему, настроенных правил, определяющих порядок взаимодействия этих объектов, добавленных и зарегистрированных сертификатов, будет создана ГПБ. ГПБ представляет собой набор правил, которые оперируют с набором объектов политики. Комбинация этих наборов правил и объектов политики, с которыми они оперируют, является проектом.

ПО ЗУ 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. Любая ЛПБ может быть экспортирована в текстовый файл в файловой системе. Когда ГПБ активируется, все ЛПБ автоматически доставляются ко всем управляемым агентам.

В ПО ЗУ можно применять правило к индивидуальным объектам политики или сразу к группе объектов (см. Приложение 1Когда объекты политики организованы в группы, для каждого устройства будут применены те же самые правила, что и во всей группе.

ПО ЗУ 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).

9.1 Работа с ГПБ и проектами

Различные вкладки ПО ЗУ обеспечивают функции для работы как с отдельной ГПБ, так и с проектом.

Проекты можно импортировать в ПО ЗУ и экспортировать из него. Чтобы иметь несколько ГПБ, которые отличаются в некотором отношении (не только правилами), следует использовать разные проекты. Импорт/экспорт XML-структур проекта сохранит или восстановит все объекты во всех окнах ПО ЗУ.

Проекты хранятся в GSP-формате и экспортируются из ПО ЗУ в файлы ОС. Проекты, которые хранятся в XML-формате, могут быть импортированы в ПО ЗУ. История трансляции ГПБ может быть очищена. Описание работы с вкладкой меню «Проект» представлено на рисунке (см. Рисунок 279).

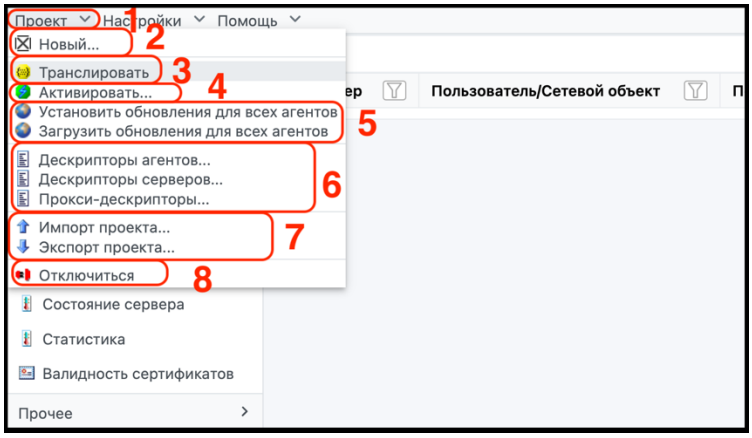


Рисунок 279 – Переход в панель вкладок меню «Проект»

Во вкладке меню «Проект» (цифра 1) отобразится:

1) список команд для создания проекта и его активации:

— «Новый» (цифра 2);

— «Транслировать» (цифра 3);

— «Активировать» (цифра 4);

2) список команд для управления обновлением (цифра 5):

— «Установить обновления для всех агентов»;

— «Загрузить обновления для всех агентов»;

3) список команд для просмотра и управления дескрипторами (цифра 6):

— «Дескрипторы агентов»;

— «Дескрипторы серверов»;

— «Прокси-дескрипторы»;

4) список команд для импорта и экспорта проектов (цифра 7):

— «Импорт проекта»;

— «Экспорт проекта»;

5) опция «Отключится» (цифра 8) для выхода из учетной записи. Описание опции приведено в подразделе 5.1.

9.1.1 Создание нового проекта

Для создания нового проекта во вкладке меню «Проект» выбрать команду «Новый». В результате создастся новый проект, который необходимо наполнить настроенными объектами, правилами и сертификатами. В случае создания следующего проекта сохранить созданный ранее проект, используя команду «Экспорт». В случае создания нового проекта созданный ранее проект и его настройки удалятся.

9.1.1.1 Трансляция проекта

Существуют три возможных результата трансляции ГПБ:

— «Трансляция завершилась успешно»;
— «Трансляция завершена, но есть предупреждения». 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.

Во вкладке меню «Проект» выбрать команду «Транслировать». Процесс трансляции заключается в том, чтобы транслировать созданную ГПБ в текстовом виде для ЛПБ.

Окно «Результат трансляции» с результатом «Трансляция завершена, но есть предупреждения» представлено на рисунке (см. Рисунок 280).

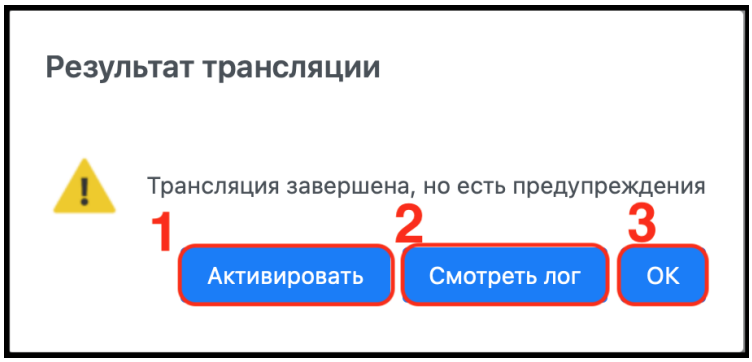


Рисунок 280 – Окно «Результат трансляции»

Кнопки управления результатом:

— «Активировать». При нажатии кнопки «Активировать» созданный и транслированный проект перейдет в активный режим;
— «Смотреть лог». В случае нажатия кнопки «Смотреть лог» откроется журнал, отображающий события и предупреждения;
— «ОК». В случае нажатия кнопки «ОК» проект сохранится в транслированном режиме.

Транслировать объекты или ГПБ необходимо каждый раз при внесении изменений в настройки.

9.1.1.2 Активация проекта

Для активации проекта во вкладке меню «Проект» выбрать команду «Активация». В результате откроется окно «Результат активации», представленное на рисунке (см. Рисунок 281), в котором необходимо нажать кнопку «ОК». Активировать объекты или ГПБ необходимо каждый раз при внесении изменений в настройки.

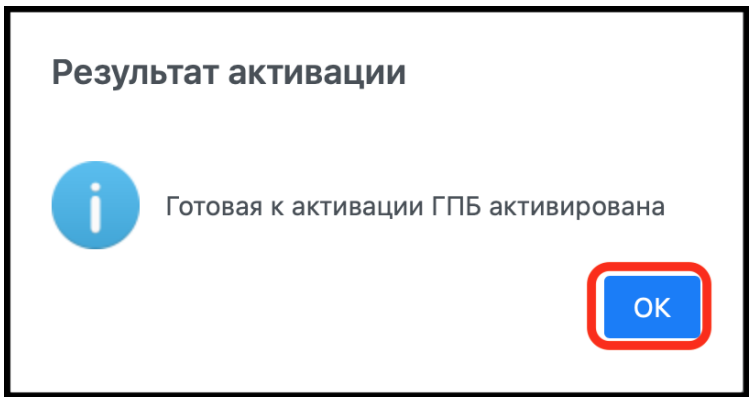


Рисунок 281 – Окно «Результат активации»

9.1.2 Экспорт (сохранение) проекта

Для экспорта проекта (сохранения его в GSP-структуру в виде файла с расширением. gsp) во вкладке меню «Проект» выбрать команду «Экспорт». В результате откроется окно «Опции экспорта», представленное на рисунке (см. Рисунок 282).

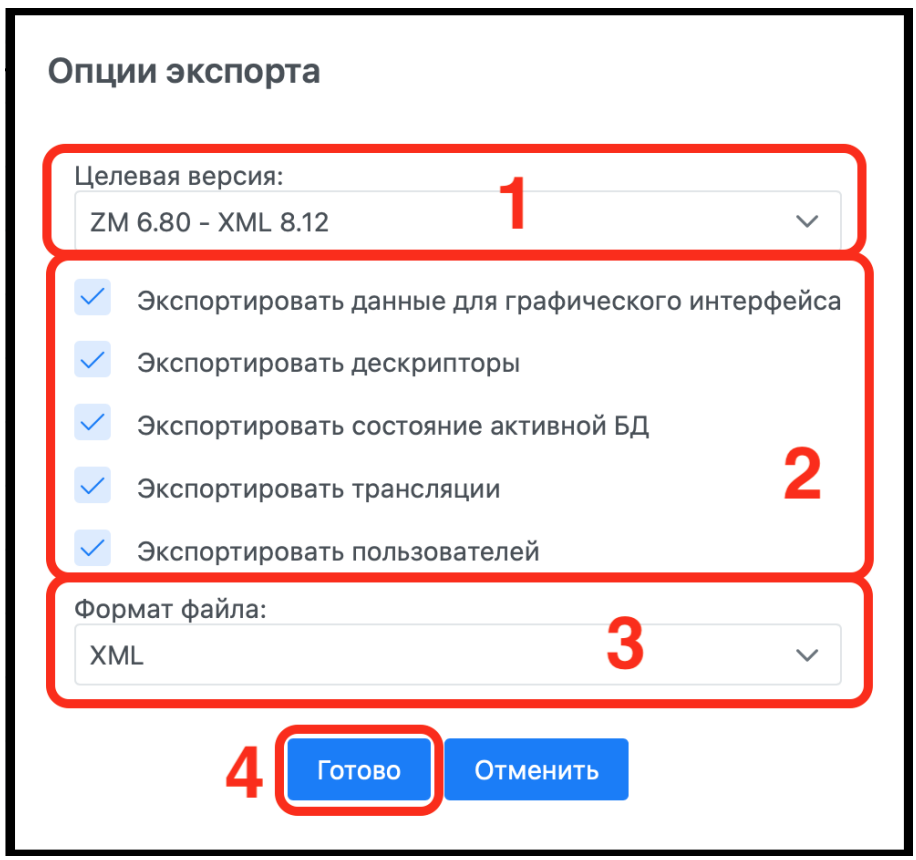


Рисунок 282 – Окно «Опции экспорта»

В окне «Опции экспорта» требуется:

1) выбрать из выпадающего списка целевую версию (цифра 1);
2) установить флажок напротив требуемых параметров экспорта (цифра 2);
3) выбрать из выпадающего списка «Формат файла» (цифра 3). Доступные форматы: XML, JSON, YAML.

9.1.3 Импорт проекта

Для импорта проекта во вкладке меню «Проект» выбрать команду «Импорт». В результате откроется окно с предупреждением о том, что все данные будут удалены, представленное на рисунке (см. Рисунок 283).

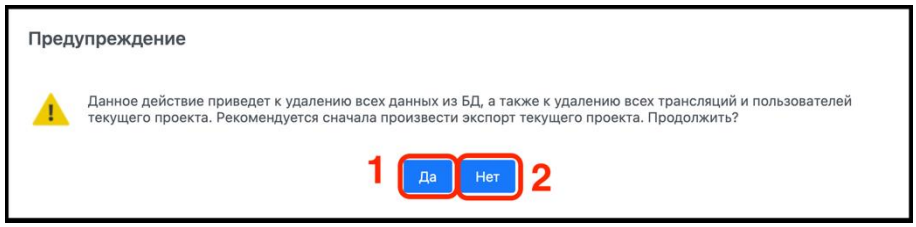


Рисунок 283 – Окно «Предупреждение»

В окне «Предупреждение» нажать кнопку «Да» (цифра 1). Если проект требуется сохранить, нужно нажать кнопку «Нет» (цифра 2).

9.1.4 Обновление агентов

Для обновления агентов необходимо воспользоваться контекстным меню выбранного объекта политики. Описание выполнения команд контекстного меню «Загрузить обновления для агента» и «Обновить версию агента» представлены в п. 6.4.1.1.4 и п. 6.4.1.1.5 соответственно.

9.1.5 Управление дескрипторами

9.1.5.1 Дескрипторы агентов

Для просмотра и редактирования или добавления дескрипторов агента требуется во вкладке меню «Проект» выбрать команду «Дескрипторы агентов». В результате откроется окно «Дескрипторы агентов», представленное на рисунке (см. Рисунок 284).

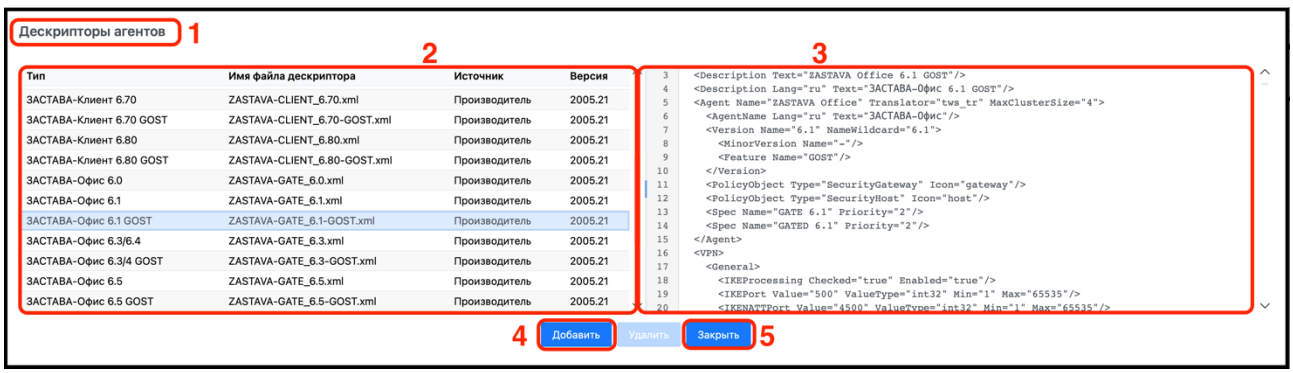


Рисунок 284 – Окно «Дескрипторы агентов»

В окне «Дескрипторы агентов» (цифра 1) в левой части окна будет отображаться список дескрипторов агентов (цифра 2), в котором можно выбрать требуемый дескриптор, в правой части окна будет отображаться выбранный дескриптор в текстовом виде (цифра 3), при необходимости, его можно редактировать. Для добавления дескриптора агента нажать кнопку «Добавить» (цифра 4). Выйти из окна «Дескрипторы агентов» можно, нажав кнопку «Закрыть» (цифра 5).

Вид окна «Выберите дескриптор» представлен на рисунке (см. Рисунок 285).

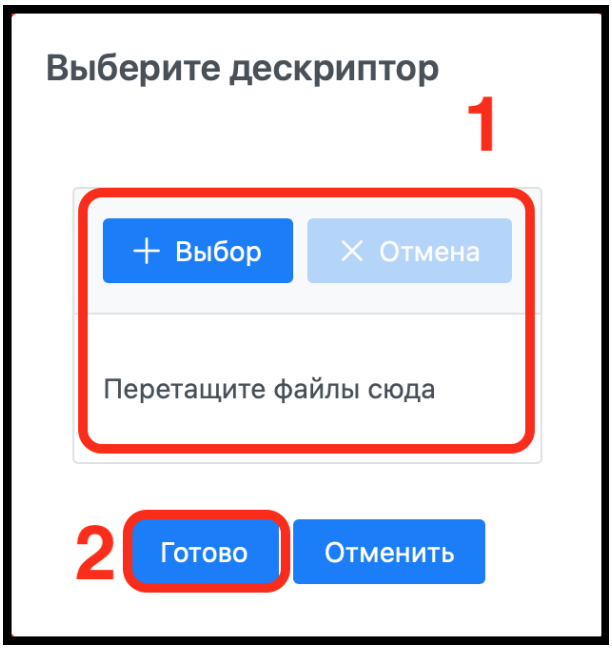


Рисунок 285 – Окно «Выберите дескриптор»

Нажать кнопку «+Выбор» в списке ранее добавленных дескрипторов выбрать требуемый, либо переместить файл в окно «Перетащить файлы сюда» (цифра 1). Нажать кнопку «Готово» (цифра 2).

9.1.5.2 Дескрипторы серверов

Для просмотра и редактирования или добавления дескрипторов агента требуется во вкладке меню «Проект» выбрать команду «Дескрипторы серверов». В результате откроется окно «Дескрипторы серверов», представленное на рисунке (см. Рисунок 286).

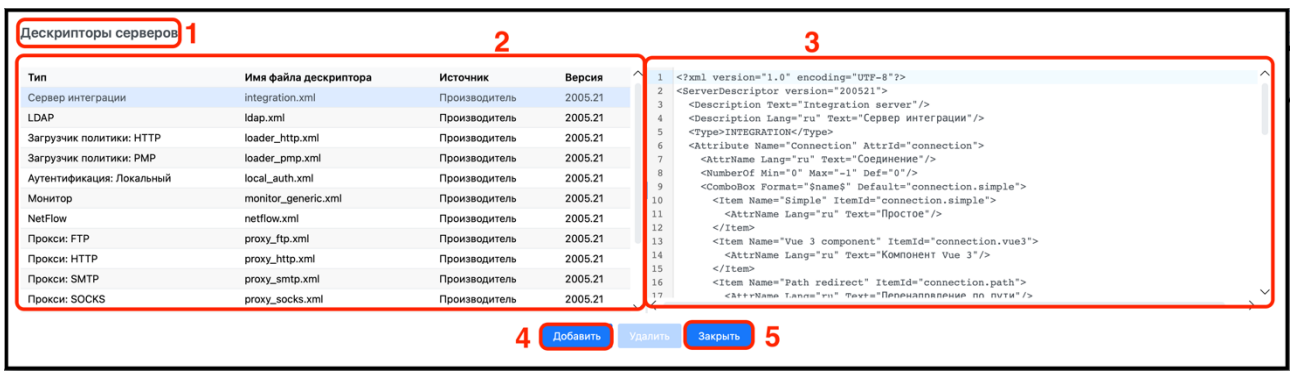


Рисунок 286 – Окно «Дескрипторы серверов»

В окне «Дескрипторы серверов» (цифра 1) в левой части окна будет отображаться список дескрипторов агентов (цифра 2), в котором можно выбрать требуемый дескриптор, в правой части окна будет отображаться выбранный дескриптор в текстовом виде (цифра 3), при необходимости, его можно редактировать. Для добавления дескриптора агента следует нажать кнопку «Добавить» (цифра 4). Выйти из окна «Дескрипторы серверов» можно, нажав кнопку «Закрыть» (цифра 5).

Окно «Выберите дескриптор» представлено на рисунке (см. Рисунок 287).

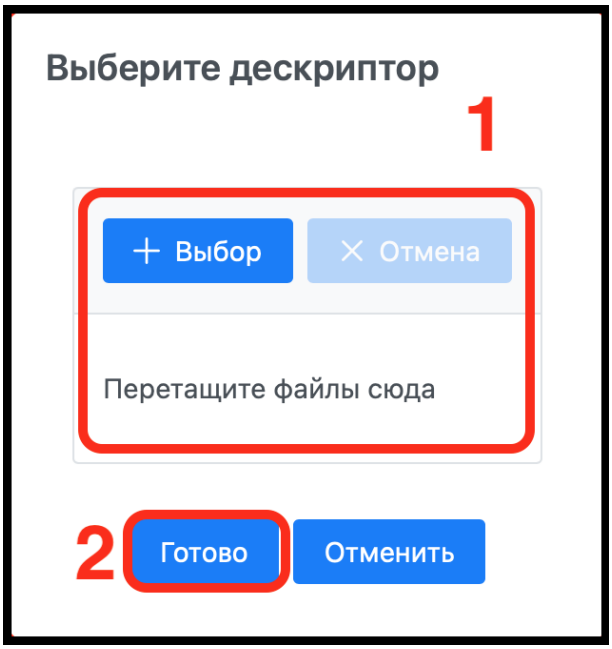


Рисунок 287 – Окно «Выберите дескриптор»

Нажать кнопку «+Выбор» в списке ранее добавленных дескрипторов и выбрать требуемый, либо переместить файл в окно «Перетащить файлы сюда» (цифра 1). Нажать кнопку «Готово» (цифра 2).

9.1.5.3 Прокси-дескрипторы

Для просмотра и редактирования или добавления дескрипторов агента требуется во вкладке меню «Проект» выбрать команду «Прокси-дескрипторы». В результате откроется окно «Прокси-дескрипторы», представленное на рисунке (см. Рисунок 288).

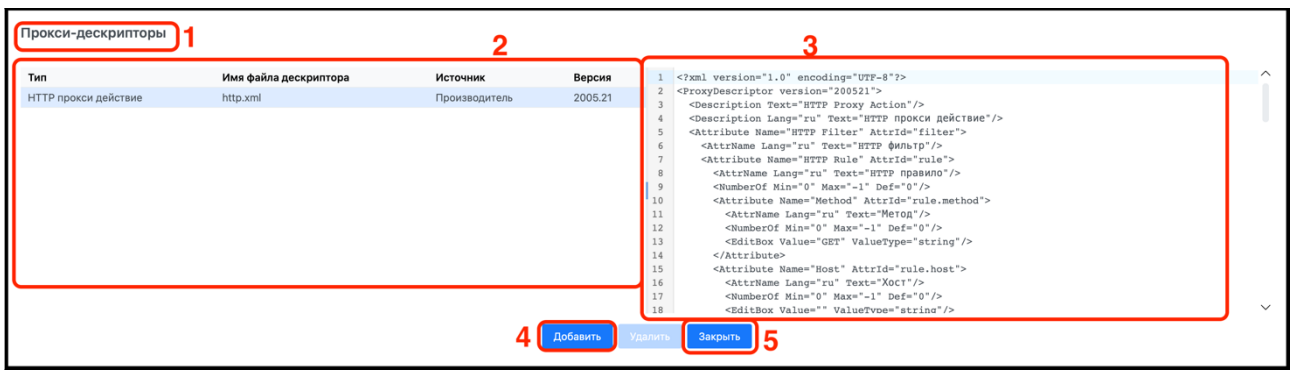


Рисунок 288 – Окно «Прокси-дескрипторы»

В окне «Прокси-дескрипторы» (цифра 1) в левой части будет отображаться список дескрипторов агентов (цифра 2), в котором можно выбрать требуемый дескриптор, в правой части будет отображаться выбранный дескриптор в текстовом виде (цифра 3), при необходимости его можно редактировать. Для добавления дескриптора агента следует нажать кнопку «Добавить» (цифра 4). Выйти из окна «Прокси-дескрипторы» можно, нажав кнопку «Закрыть» (цифра 5).

Окно «Выберите дескриптор» представлено на рисунке (см. Рисунок 289).

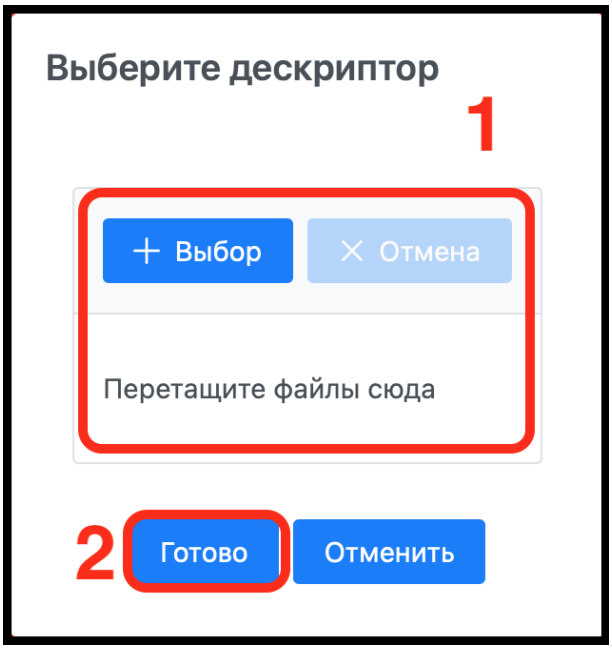


Рисунок 289 – Окно «Выберите дескриптор»

Нажать кнопку «+Выбор», в списке ранее добавленных дескрипторов выбрать требуемый, либо переместить файл в окно «Перетащить файлы сюда» (цифра 1). Нажать кнопку «Готово» (цифра 2).

9.1.5.4 Добавление специального дескриптора

По умолчанию ПО ЗУ работает с набором дескрипторов, включенных в ПО ЗУ, которые позволяют работать с большинством приложений. Однако, в некоторых случаях может понадобиться добавить в ПО ЗУ дополнительные дескрипторы.

Для добавления в ПО ЗУ нового криптоалгоритма выполнить следующее:

1) создать копию XML-файла для требуемого дескриптора агента (путь от главной директории ПО ЗУ: opt/ZASTAVAmanagement/etc/adesc/);
2) открыть скопированный XML-файл в текстовом редакторе, поддерживающем кодировку UTF-8, и внести необходимые изменения;
3) отредактировать в этом файле идентификатор дескриптора в тэге «Agent Name»;
4) открыть ПО ЗУ и выбрать окно «Дескрипторы агентов»;
5) нажать кнопку «Добавить» и добавить новый XML-файл дескриптора в список.

Теперь можно создавать объекты политики с новым типом агента, используя новый дескриптор.

9.1.6 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

тексты ЛПБ для определенного объекта безопасности в окне редактирования. Для этого надо выбрать объект политики, используя команду контекстного меню «Изменить», после чего перейти к настройкам.

9.1.6.1 Прямое редактирование

Текст ЛПБ хоста безопасности, шлюза безопасности или пользователя (агента «ЗАСАВА-Клиент») может непосредственно просматриваться и редактироваться в окне настроек выбранных объектов, для этого нужно перейти в окно «Трансляция политики» и выполнить шаги, изображенные на рисунке (см. Рисунок 290).

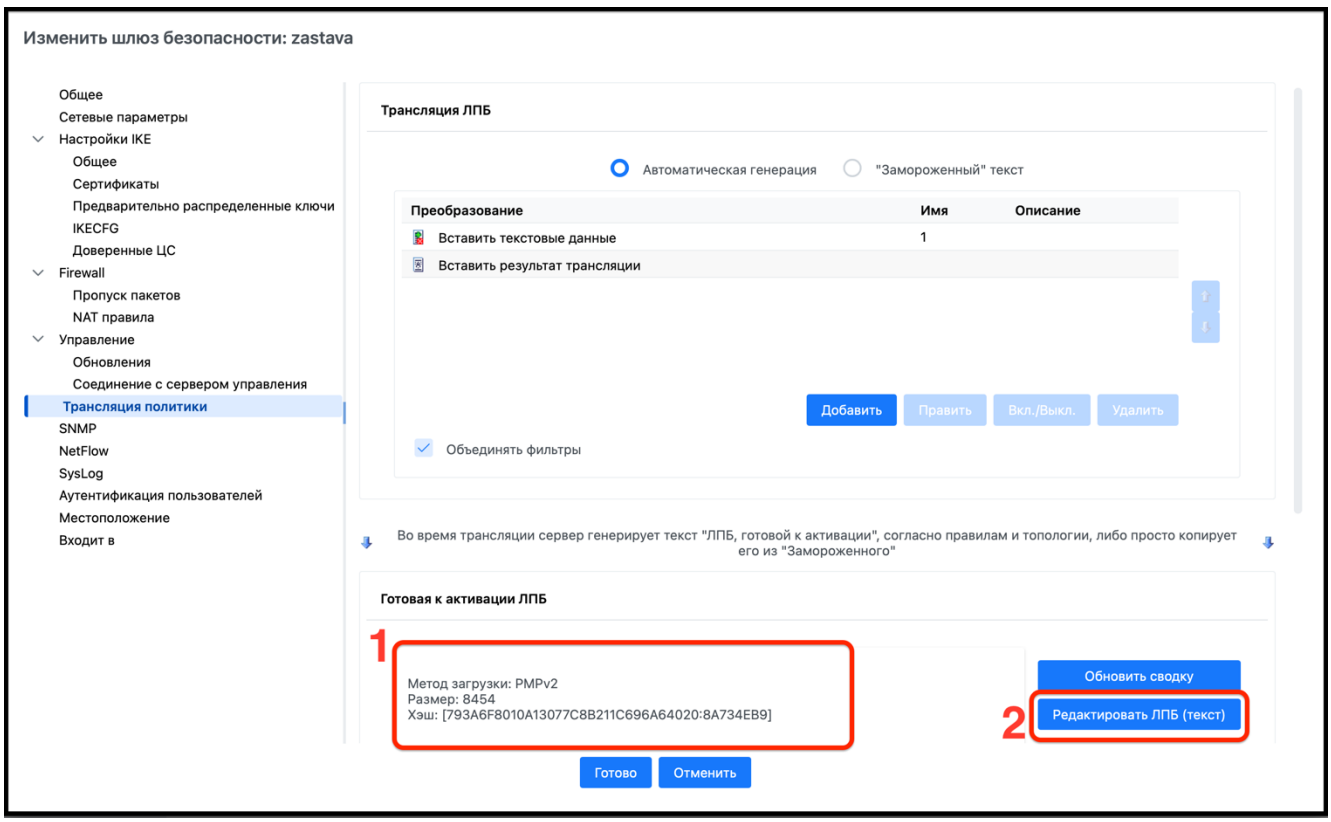


Рисунок 290 – Переход в текстовый редактор

Убедится, что есть готовая к активации ЛПБ (цифра 1), и нажать на кнопку «Редактировать ЛПБ (текст)» (цифра 2).

Вид окна «Текстовой редактор» представлен на рисунке (см. Рисунок 291).

Рисунок 291 – Текстовый редактор

В результате откроется простой «Текстовой редактор», который позволяет просматривать ЛПБ, вносить в её текст изменения и сохранять ЛПБ.

Для загрузки и сохранения ЛПБ требуется:

1) для загрузки ЛПБ из файла нажать на элемент «» (цифра 1);
2) для сохранения ЛПБ в файл нажать на элемент «» (цифра 2). Поддерживается сохранение в текстовом формате (файл *. txt);
3) нажать кнопку «Готово» (цифра 3).

9.1.6.2 Редактирование структуры ЛПБ

Редактирование структуры ЛПБ означает добавление или удаление определяемых пользователем фрагментов ЛПБ (см. п. 8.3), автоматически созданной из ГПБ при помощи ПО ЗУ для этого агента или изменения положений таких определяемых пользователем ЛПБ фрагментов относительно автоматически созданной конфигурации.

Фрагменты определяемых пользователем ЛПБ могут быть добавлены или удалены из автоматически созданной конфигурации перемещением определяемой пользователем ЛПБ из списка доступных пользовательских ЛПБ в список «Выбрать пользовательскую ЛПБ». Выбрать одну или более определяемых пользователем ЛПБ в одном из окон, используя клавиши со стрелками <вверх>/<вниз>, чтобы переместить их в другое окно.

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 созданной конфигурации, а затем автоматически созданную ЛПБ и любые фрагменты, появляющиеся позже неё. Для изменения порядка приоритетов необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 292).

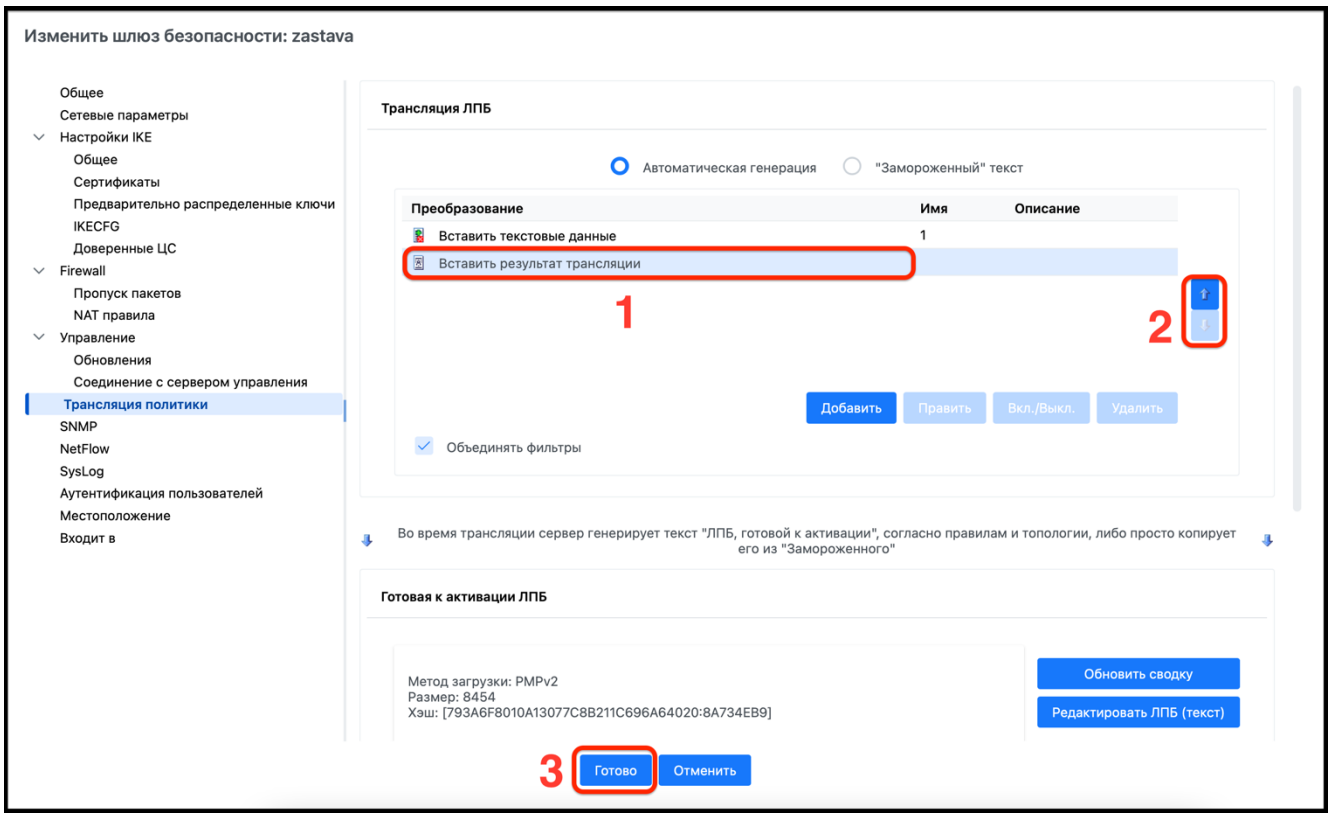


Рисунок 292 – Изменение порядка приоритетов

В списке «Преобразование» необходимо выбрать требуемую ЛПБ (цифра 1) и переместить ее с помощью кнопок верх/вниз (цифра 2). Нажать кнопку «Готово» (цифра 3).

9.2 Экспортирование ЛПБ

Обычно ЛПБ экспортируются вручную. Начальные ЛПБ распределяются к агентам так, чтобы они могли безопасно взаимодействовать с ПО ЗУ для получения полной ЛПБ. Последующее распределение ЛПБ обычно происходит автоматически с помощью команды «Активировать» в контекстном меню. ЛПБ могут экспортироваться в текстовый файл.

9.3 Активация ЛПБ на агентах

Для активации ЛПБ для всех сконфигурированных агентах необходимо выполнить шаги, изображенные на рисунке (см. Рисунок 293).

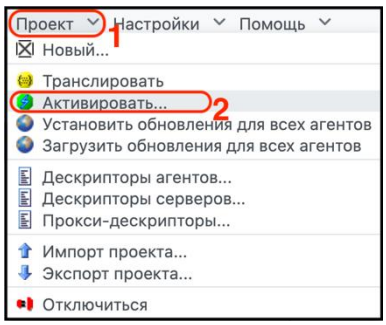


Рисунок 293 – Окно подтверждения активации ЛПБ

Выбрать ЛПБ для всех объектов политики, далее во вкладке меню «Проект» (цифра 1) выбрать команду «Активировать» (цифра 2).

Чтобы активировать ЛПБ для конкретного агента, надо выделить объект политики в элементах списка «Топология» или «Объекты политики», используя команду «Транслировать» из контекстного меню. Когда ПО ЗУ успешно обработало ЛПБ и готово активировать ЛПБ для агента(ов), во вкладке «Монитор» отобразится пиктограмма статуса активации таблице (см. Таблица 35). Активация будет завершена, когда все управляемые агенты установили связь с ПО ЗУ, получили и активировали их собственные ЛПБ. При попытке активации ЛПБ всех объектов политики с помощью команды «Активировать» во вкладке меню «Проект» появится окно, в нем необходимо подтвердить желание активировать ЛПБ для всех объектов или отменить данную операцию, нажав кнопку «Нет», если требуется обновить ЛПБ только на одном объекте безопасности.

9.3.1 Управляемые агенты

Новая ЛПБ должна быть загружена и активирована на устройствах безопасности со статусом «Управляемый». Чтобы получать и активировать ЛПБ из ПО ЗУ, агенты должны иметь:

1) локальный сертификат и/или предварительно распределенный ключ, зарегистрированный в агенте и в ПО ЗУ;
2) сертификат для верификации ЛПБ и соответствующий сертификат УЦ, он должен быть зарегистрирован как «Доверенный»;
3) настроенные условия получения ЛПБ на агенте.

9.3.2 Активация

Для «ЗАСТАВА-Офис» (см. Приложение 3), установленных на СВТ с постоянными IP-адресами, ЛПБ агента может быть «доставлена в» или «получена от» ПО ЗУ по умолчанию, как только ГПБ будет транслирована и подготовлена для определенного агента, ПО ЗУ 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 ПО ЗУ), то ASK ЛПБ

должна быть активирована в окне «Политика панели инструментов агента», после чего полная ЛПБ будет запрошена от ПО ЗУ.

9.3.3 Контроль статуса агента

Контролировать статус активации ЛПБ на агенте, а также определять, существуют ли какие-то проблемы взаимодействия с агентами в режиме реального времени, можно, выбрав режим мониторинга, как только будет транслирована ГПБ и активирована ЛПБ, пиктограммы статуса появятся в некоторых окнах элементов списка, колонках параметров «Статус» или «Статус активации». Цветовая индикация отображения статусов активации представлена в таблице (см. Таблица 35).

Таблица 35 – Отображение статуса активации ЛПБ

Пиктограмма	Описание
	Активирован
	Ошибка
	Ожидание доступа
	Ожидание подтверждения
	Подключен
	Несоответствие
	Отключен

Статус целостности ЛПБ прослеживает изменения ЛПБ агента, начиная с последней активации, с помощью отображения пиктограмм, представленных в таблице (см. Таблица 36).

Таблица 36 – Отображение статуса целостности ЛПБ

Пиктограмма	Описание
	На устройстве Cisco/Microsoft IPsec-агенте подлинная ЛПБ (согласно дате)
	ЛПБ на устройстве Cisco /Microsoft IPsec-агенте была изменена, начиная с последней активизации от ПО ЗУ. Для Cisco IOS маршрутизаторов этот статус будет также показан после начала сеанса администратора (даже если фактическая конфигурация устройства не была изменена)
	ПО ЗУ не может соединяться с устройством Cisco /Microsoft IPsec-агентом для проверки его взаимодействия с ЛПБ в настоящее время

10 МЕРЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ПО ЗУ

10.1 Краткий обзор проблем безопасности в ПО ЗУ

Безопасность ПО ЗУ включает следующие компоненты:

— безопасность сертификатов и ключей;

— безопасность управления соединениями;

— безопасность управления структурами данных (безопасность ЛПБ).

10.2 Безопасность сертификатов и ключей

Сертификаты и ключи для подтверждения подлинности ЛПБ и для защиты ВЧС-соединений могут храниться как PKCS#11 ключевые носители на сменных носителях данных. Этот метод защиты не обязателен, если выделенная и управляемая должным образом платформа используется для ПО ЗУ.

10.3 Безопасность управления сетевыми соединениями

Все ПО ЗУ-соединения, особенно соединения между распределенными частями ПО ЗУ, защищены службой «Пропуск пакетов». ПО ЗУ использует управление защищёнными соединениями, основанное на IKE-протоколе, чтобы загружать ЛПБ на хосты безопасности и шлюзы безопасности.

10.4 Защита данных ЛПБ

ПО ЗУ использует цифровую подпись, чтобы защитить ЛПБ, которая может пройти через потенциально непроверенные каналы доставки. Эта мера обеспечивает подлинность и целостность ЛПБ. ЛПБ обычно не содержит высокочувствительных данных; однако большинство каналов доставки ЛПБ защищено.

10.5 Рекомендации по политике безопасности ПО ЗУ

Значимость и уязвимость ПО ЗУ решения защиты корпоративной сети настолько важны, что стоит предпринять специальные меры безопасности. Наиболее важная и чувствительная информация в ПО ЗУ и наиболее уязвимые точки (в порядке уменьшения уязвимости), следующие:

— права доступа на систему управления;

— ключ для подписи ЛПБ;

— ВЧС ключи;

— спецификации политики безопасности.

Основная мера, которая должна быть осуществлена, чтобы защитить управляющую платформу, — это использование предназначенной платформы только для одного приложения (ПО ЗУ) и настройка безопасности этой платформы средствами администрирования и сетевой безопасности.

11 НАСТРОЙКА СЕРВЕРА ОБНОВЛЕНИЙ

11.1 Создание и настройка встроенного сервера обновления

Обновление агентов осуществляется по протоколу http.

Внимание! Использование незащищенного с помощью ПО ЗУ канала обновления запрещено!

Для настройки сервера обновлений необходимо:

— установить в конфигурационном файле http.ini переменную root, указать путь к папке с файлами обновления. Например, C:\Program Files\ELVIS+\ZASTAVA Management\update;

— в каталоге, на который указывает переменная root, создать каталог с именем 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; <ОС> - WINXX; <процессор> - i386, x64, x86 или amd64; <вендор> - zastava.

Пример: [GATE.WINXX.i386.zastava]

— [GATE.WINXX.i386.zastava] – начало секции для конфигурирования обновления ЗАСТАВА-Офис;

— version=X.X.XXXXX - версия дистрибутива, в формате как она указана в файле version.txt дистрибутива агента, например, 6.3.13690. Версия доступного обновления сравнивается с текущей версией агента, если значение версии обновления больше, то загружаются файлы обновления и выполняется команда;

— file=zastavaoffice.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 (запускается из-под vpnagent). Дополнительные исполняемые команды:

- exec_sys - исполняемая команда. exec_sys = "$download_path\zastavaoffice64.exe" если есть, значение - команда, запускаемая из-под vpndmn;
- exec_user - исполняемая команда. exec_user = "$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;
- 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 локального/системного администратора пользователя (C:\Windows\temp);
- $agent_bin – папка, в которой находятся запускаемые файлы агента (C:\Programm Files\ZASTAVA office);
- $agent_lib - папка, в которой находятся подгружаемые библиотеки агента (C:\Programm Files\ZASTAVA office);
- $agent_etc - папка, в которой находятся конфигурационные файлы (C:\Programm Files\ZASTAVA office);

— $system_etc - папка, в которой находятся конфигурационные файлы (C:\Programm Files\ZASTAVA office);
— $system_log - папка, в которой находятся файлы логирования (C:\Programm Files\ZASTAVA office\log);
— $system_var – папка, в которой находится файл с локальными настройками localsettings.ini (c:\Programm Files\ZASTAVA office);
— $system_var_etc - папка, в которой находится файл с настройками (c:\Programm Files\ZASTAVA office);
— $system_tmp - папка, в которой находятся временные файлы (C:\Windows\Temp);
— $agent_version - текущая версия агента.

Пример:

[GATE.WINXX.amd64.zastava]

version = 6.3.16253

file = zastavaoffice64.exe

exec = "$download_path\zastavaoffice64.exe" /l*v c:\zastava_setup.log

[GATE.WINXX.i386.zastava]

version = 6.3.16253

file = zastavaoffice32.exe

— для обновления агентов согласно ЛПБ при использовании встроенного сервера обновления в ПО ЗУ необходимо добавить сетевой сервис TCP с портом 3118. После создания сетевого сервиса надо создать сервер обновления с методом подключения «http». Для этого надо выбрать созданный сервис и указать URL, например, http://10.111.10.231:3118/agentupdate. В настройках объектах политики безопасности открыть «Управление», далее «Автоматическое обновление», в поле «Тип обновления» выбрать параметр «Обновлять согласно ЛПБ»;
— для обновления агентов с помощью команд сервера обновлений необходимо в настройках объекта политики выбрать окно «Управление», далее «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 из выпадающего списка меню команду «Проект» (обновить версию агентов или загрузить версию обновлений для агентов) или воспользоваться аналогичными командами контекстного меню для конкретного объекта политики. При обновлении кластера можно 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.

Нельзя использовать один и тот же сервер обновления для разных типов обновлений.

Для предотвращения нежелательных изменений, при использовании USER ACCOUTN CONTROL в ОС Windows, выполнить следующие действия:

— 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 графическому 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.

После отображения статуса об успешном обновлении в «Мониторе» ПО ЗУ локально на агенте существуют и непустые файлы с информацией об обновлении и дистрибутивом для установки обновления:

```
[root@apk-zastava:      ~]#      ls      -la      /var/vpnagent/update/
итого                                                                24
-rw-rw-rw-  1  root  root     10  дек  20  16:38  INSTALL_FLASH.version
-rw-rw-rw-   1   root   root    474   дек   20   16:38   vpndmn_update.ini
-rw------- 1 root root  599 дек 20 16:38 vpndmn_update_status.xml
[root@apk-zastava:       ~]#       ls       -la       /.image/update/
итого                                                             222600
-rw-rw-rw-    1    root    root    227932160    дек    20    16:33
INSTALL_FLASH_3.5.24609.tar
-rw-rw-rw- 1 root root         0 дек 20 16:38 os_update_ready
```

11.1.1 Настройка обновления агента

Для централизованного управления настройками обновлений через ПО ЗУ необходимо на самом агенте включить режим «Локальная политика безопасности» (Local Security Policy) (в окне «Настройки», далее «Настройки обновления»). В противном случае информация о настройках обновлений в ЛПБ будет игнорироваться агентом.

12 ФАЙЛЫ ПАРАМЕТРОВ

12.1 Настройка лимитов времени

Файл /var/vpnmgmt/settings.yaml, представленный в директории ПО ЗУ по умолчанию после установки, определяет некоторые соединения и параметры по превышению лимитов времени (timeout), которые управляют различными аспектами действий ПО ЗУ. Эти параметры редактируемы. Можно изменять величины превышения лимитов времени, редактируя файл /var/vpnmgmt/settings.yaml в любом текстовом редакторе.

12.2 Опции лимитов времени

Для редактирования файла параметров /var/vpnmgmt/settings.yaml необходимо изменить параметры файла в любом текстовом редакторе. Перечень параметров и их значения приведены в таблице (см. Таблица 37).

Таблица 37 – Описание параметров Timeouts.timeout

Параметр	Значение по умолчанию	Значение
agent	30	# If agent did not send requests to distrubuter during this time # then assume this agent is disconnected. Later access will # launch all checks for reconnect (check updates etc)
user	600	# Time for close socket if user send nothing after login. # This is mostly for curl/web access. # GUI send some data every several seconds and therefore resets this timeout
anon	30	# Like above but without login. # For example login is not used for download updates
close	60	# After close socket server will wait this time for reconnect to restore REST-session. # Used for correct curl work
dual	10	# Maximum time of simple commands request-reply
login	4	# Maximum time of login command
logout	2	# Maximum time of logout command

12.3 Параметры авторизации через пароль

Для редактирования файла параметров /var/vpnmgmt/settings.yaml и изменения общих параметров для всех устройств необходимо изменить параметры файла в любом текстовом редакторе. Перечень параметров и их значения представлены в таблице (см. Таблица 38).

Таблица 38 – Опции других параметров файла /var/vpnmgmt/settings.yaml # Login password options.password:

Параметр	Значение по умолчанию	Значение
rot	90	# Time (days) to change password. Use 0 to turn off this reminder
try	5	# Maximum attempts login with wrong password
ban	60	# Ban time (seconds) for IP after exceed those attempts

12.4 Параметры методов аутентификации

Для редактирования файла параметров /var/vpnmgmt/settings.yaml и изменения общих параметров для всех устройств необходимо изменить параметры файла в любом текстовом редакторе, перечень параметров и их значения приведены в таблице (см. Таблица 39).

Таблица 39 – Опции файла /var/vpnmgmt/settings.yaml # Authentication methods.auth:

Параметр	Значение по умолчанию	Значение
- vdb	gost	# GUI console. Supports: gost, none.
rest	digest	# REST. Supports: digest, basic, none.
agent	none	# Agents to distrubutor. Reserved for future.
other	none	# Other. Reserved for future.

12.5 Параметры трансляции

Эта секция содержит общие для всех устройств параметры настроек трансляции, представленные в таблице (см. Таблица 40).

Таблица 40 – Параметры настроек трансляции # Translator options.translation:

Параметр	Значение по умолчанию
stopTranslationAfterTPL	false
maxAllowedTraces:	1024
shouldSplitSubnetForNomadicRules	false

12.6 Другие параметры

Эта секция содержит параметры загрузки конфигурационных файлов, параметры и их значения представлены в таблице (см. Таблица 41).

Таблица 41 – Параметры загрузки конфигурационных файлов # Other parameters. options:

Параметр	Значение по умолчанию	Значение
distributor_port	3118	# Distributor server port
rest_port	8088	# REST server port
vdb_port	3117	# VDB server port
help	''	# Help files path. Allow special subpaths: [etc], [bin] and [var]
root:	'[etc]/web'	# Update files path. Allow special subpaths: [etc], [bin] and [var]
db:	'[var]'	# Database files path. Allow special subpaths: [etc], [bin] and [var]
lang	rus	# Select server language: eng, rus, default
syslog_max_tcp_sockets	100	# Max count of TCP connections for Syslog in TCP mode
max_gsp_size	100000000	# Max GSP size. Larger files will not be imported

13 УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Описание неисправностей	Решение
Невозможно сделать автоматическое обновление, если сертификат, которым подписан агент, просрочен	При автоматическом обновлении с параметром silent=0 (см. подраздел 11.1) 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: [GATE.WINXX.amd64.zastava] version = 6.1.15455 file = zastavaoffice64-exp.exe, cert.cer exec = cmd /C echo off & "C:\WINDOWS\system32\certutil.exe" -addstore trustedpublisher "$download_path\cert.cer" && "$download_path\zastavaoffice64-exp.exe" /l*v c:\distr\zastava1-setup.txt silent = 1 если путь к утилите не содержит пробел: [GATE.WINXX.amd64.zastava] version = 6.1.15455 file = zastavaoffice64-exp.exe, cert.cer exec = cmd /C certutil.exe -addstore trustedpublisher "$download_path\cert.cer" && "$download_path\zastavaoffice64-exp.exe" /l*v c:\distr\zastava1-setup.txt silent = 1
Неверно отображается статус активации узлов кластера	Вручную выставить соответствующие номера узлов кластера для каждого локального сертификата на вкладке ВЧС «Сертификаты»

ПРИЛОЖЕНИЕ 1. ПРИМЕР КОНФИГУРИРОВАНИЯ ГПБ В ПО ЗУ ДЛЯ ДВУХ АГЕНТОВ «ЗАСТАВА-ОФИС»

Ниже представлено описание примера конфигурирования ГПБ в ПО ЗУ для двух агентов «ЗАСТАВА-Офис», схема соединения которых приведена на рисунке (см. Рисунок 294).

Рисунок 294 – Схема конфигурации

Состав аппаратных и программных средств из рассматриваемого примера приведён в таблице (см. Таблица 42).

Таблица 42 – Состав аппаратных и программных средств

Аппаратные средства	IP-адрес	Установленные программные средства
СВТ 1	10.0.0.1.	Наличие ПО ЗУ и «ЗАСТАВА-Офис» (далее в рассматриваемом примере – ПО ЗО 1)
СВТ 2	10.0.0.2.	Наличие «ЗАСТАВА-Офис» (далее в рассматриваемом примере – ПО ЗО 2)

СВТ 1 и СВТ 2 имеют TCP/IP-соединение.

Примечание. - В случае использования динамических IP-адресов, получаемых для СВТ 1 и СВТ 2 с помощью DHCP-сервера, данный DHCP-сервер должен быть определён в ГПБ. В рассматриваемом примере рекомендуется использовать статические IP-адреса для СВТ 1 и СВТ 2.

Активация ГПБ будет невозможна, если:

- в ПО ЗУ не будет найден IP-адрес СВТ, на котором оно установлено;
- не будет установлено соединение ПО ЗУ с СВТ 1 и СВТ 2 с установленным ПО ЗО 1 и ПО ЗО 2 соответственно.

1.1. Порядок действий для конфигурирования ГПБ

1.2. Загрузка корневых сертификатов УЦ

Загрузить корневой сертификат УЦ (тип идентификатора: DN, значение идентификатора: CN=MainCA) в ПО ЗО 1.

Загрузить корневой сертификат УЦ (тип идентификатора: DN, значение идентификатора: CN=MainCA) в ПО ЗО 2.

1.3. Запрос и загрузка персонального сертификата для ПО ЗО 1

Для получения персонального сертификата для ПО ЗО 1 открыть программу эмулятора терминала на СВТ 1 и выполнить команды:

1) проинициализировать генератор случайных чисел:

```
vpnconfig -initrng token 0
```

2) пройти аутентификацию на функциональном ключевом носителе:

```
vpnconfig -login token 0 12345678 save
```

3) создать запрос на получение персонального сертификата:

```
vpnconfig -add request 0 "GOST R 34.10-2012 256" 512 "GOST 34.11-2012 256" "CN=gate1" eku=ipsec
```

4) подписать сертификат в УЦ;
5) сохранить на СВТ 1 подписанный персональный сертификат в ПО ЗО 1:

```
vpnconfig -add cert <file>
```

где: <file> - путь для сохранения

6) убедиться в наличии добавленного сертификата в списке:

```
*vpnconfig -list cert
```

1.4. Запрос и загрузка персонального сертификата для ПО ЗО 2

Для получения персонального сертификата для ПО ЗО 2 открыть программу эмулятора терминала на СВТ 2 и выполнить команды:

1) проинициализировать генератор случайных чисел:

```
vpnconfig -initrng token 0
```

2) пройти аутентификацию на функциональном ключевом носителе:

```
vpnconfig -login token 0 12345678 save
```

3) создать запрос на получение персонального сертификата:

```
vpnconfig -add request 0 "GOST R 34.10-2012 256" 512 "GOST
34.11-2012 256" "CN=gate2" eku=ipsec
```

4) подписать сертификат в УЦ;
5) сохранить на СВТ 1 подписанный персональный сертификат в ПО ЗО 2:

```
vpnconfig -add cert <file>
```

где: <file> - путь для сохранения

6) убедиться в наличии добавленного сертификата в списке:

```
*vpnconfig -list cert
```

1.5. Настройка получения ЛПБ в ПО ЗО 2

На СВТ 2 в программе эмулятора терминала выполнить команду для настройки получения ЛПБ ПО ЗО 2:

```
vpnconfig -a lsp system pmp 0/0 DN 10.0.0.1 3
```

1.6. Добавление объектов в ПО ЗУ, настройка их взаимодействия

В ПО ЗУ добавить ПО ЗО 1 и ПО ЗО 2 как объекты типа «Шлюз безопасности».

Настроить сетевые параметры для Шлюзов безопасности в соответствии с таблицей (см. Таблица 43).

Таблица 43 – Параметры для объектов типа «Шлюз безопасности»

Параметр	Шлюз безопасности с ПО ЗО 1	Шлюз безопасности с ПО ЗО 2
Логическое имя	eth0	eth0
Адрес	10.0.0.1	10.0.0.2
Маска	/24	/24
Зона	Зона Интернет	Зона Интернет

В ПО ЗУ импортировать локальные сертификаты для Шлюза безопасности с ПО ЗО 1 и Шлюза безопасности с ПО ЗО 2.

В ПО ЗУ для Шлюза безопасности с ПО ЗО 1 в окне «Соединение с сервером управления» выбрать метод загрузки «Direct Access».

В ПО ЗУ для Шлюза безопасности с ПО ЗО 2 в окне «Соединение с сервером управления» выбрать метод загрузки «PMPv2» и выбрать в качестве сервера загрузки ПО ЗО 1.

В ПО ЗУ создать Действие для обработки трафика.

В ПО ЗУ создать правило для взаимодействия между ПО ЗО 1 и ПО ЗО 2.

Выполнить проверку ГПБ. Для этого в ПО ЗУ перейти в меню «Проект» и выбрать команду «Транслировать». Убедиться в отсутствии сообщений об ошибках.

В ПО ЗУ перейти в меню «Проект» и выбрать команду «Активировать».

ПРИЛОЖЕНИЕ 2. СЕТЕВЫЕ СЕРВИСЫ И ГРУППЫ СЕТЕВЫХ СЕРВИСОВ ПО УМОЛЧАНИЮ

1.1. Сетевые сервисы

В ПО ЗУ существуют предопределенные сетевые сервисы, представленные в таблице (см. Таблица 44).

Таблица 44 – Сетевые сервисы в составе ПО ЗУ

Имя сервиса	Номер протокола по умолчанию	Номер(а) порта(ов) по умолчанию	ICMP тип	TCP сервис	UDP сервис	ICMP сервис
AH	51					
all-icmp						✓
all-tcp				✓		
all-udp					✓	
biff		512			✓	
bootp		67, 68[1)]			✓	
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[1)]			✓	
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[2)]		21		✓		
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		✓		

Имя сервиса	Номер протокола по умолчанию	Номер(а) порта(ов) по умолчанию	ICMP тип	TCP сервис	UDP сервис	ICMP сервис
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		✓		
radius		1645			✓	
radius-acc		1646			✓	
realaudio		7070		✓		
redirect		5				✓
rip		520			✓	
rtsp		554		✓		
shell		514		✓		
smb		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.						

Имя сервиса	Номер протокола по умолчанию	Номер(а) порта(ов) по умолчанию	ICMP тип	TCP сервис	UDP сервис	ICMP сервис
[1)] Обозначает исходный порт. [2)] Сетевой сервис FTP использует соответствующую процедуру МЭ («generic_ftp»), которая автоматически управляет вторичными соединениями для передачи данных. Например, в случае «активного» варианта FTP, TCP-порт 20 будет открыт автоматически.						

1.2. Группы сетевых сервисов

Некоторые сетевые сервисы, предопределенные в ПО ЗУ, были собраны в группы сервисов для удобства. По умолчанию те сетевые сервисы, в которых присутствуют и TCP-сервисы и UDP-сервисы, представлены группой сервисов, которая содержит TCP-сервисы и UDP-сервисы.

ПРИЛОЖЕНИЕ З. «ПОДДЕРЖИВАЕМЫЕ ИЗДЕЛИЯ ЛИНЕЙКИ «ЗАСТАВА»

1.1. Программные изделия линейки «ЗАСТАВА-Клиент»

ПО ЗУ поддерживает работу с программными изделиями линейки «ЗАСТАВА-Клиент»:

- МКЕЮ.00563-01 Программный комплекс «ЗАСТАВА-Клиент «VPN/FW «ЗАСТАВА, версия 6»;
- МКЕЮ.00614-01 Программный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 6 КС1 (исполнение ZC6-AS64-VF-01);
- МКЕЮ.00614-01 Программный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 6 КС1 (исполнение ZC6-AL64-VF-01);
- МКЕЮ.00614-01 Программный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 6 КС1 (исполнение ZC6-RD64-VF-01);
- МКЕЮ.00626-01 Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределённого межсетевого экранирования на основе интернет-протоколов семейства IPsec / IKE «VPN/FW «ЗАСТАВА-Клиент», версия 6 КС1 (исполнения: ZC6-WX64-VF-01, ZC6-L32-VF-01, ZC6-L64-VF-01);
- МКЕЮ.00642-01 Программный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 6 КС2 (исполнение ZC6-WX64-VF-02);
- МКЕЮ.00671-01 Программный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 8 КС1 (исполнения ZC8-WX64-VF-01, ZC8-RD64-VF-01, ZC8-AL64-VF-01, ZC8-AS64-VF-01, ZC8-AD64-VF-01);
- МКЕЮ.00689-01 Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Клиент», версия 8 КС3 (исполнение ZC8-AS64-VF-03).

1.2. Программные изделия линейки «ЗАСТАВА-Офис»

ПО ЗУ поддерживает работу с программными изделиями линейки «ЗАСТАВА-Офис»:

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

межсетевого экранирования на основе интернет-протоколов семейства IPsec / IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3» (исполнение ZO6-L64-FV-03);

- МКЕЮ.00599 Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3 (исполнение ZO6-EL64-FV-03);
- МКЕЮ.00651-01 Программный комплекс «VPN/FW «ЗАСТАВА-Офис», версия 8 КС1»;
- МКЕЮ.00652-01 Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Офис», версия 8 КС3».

1.3. Аппаратно-программные комплексы линейки «ЗАСТАВА»

ПО ЗУ поддерживает работу с аппаратно-программными изделиями линейки «ЗАСТАВА»:

- МКЕЮ.00557 Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150»;
- МКЕЮ.00630 Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6;
- МКЕЮ.00664 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-150» (исполнение ZO8-APK-150);
- МКЕЮ.00581 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-1500»;
- МКЕЮ.00653 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-1500» (исполнение ZO8-APK-1500);
- МКЕЮ.00661 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-1500» (исполнение ZO8-APK-1500-A);
- МКЕЮ.00582 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-6000»;
- МКЕЮ.00654 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-6000» (исполнение ZO8-APK-6000);
- МКЕЮ.00660 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-6000» (исполнение ZO8-APK-6000-A);
- МКЕЮ.00666 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-10000» (исполнение ZO8-APK-10000-A);
- МКЕЮ.00667 Аппаратно-программный комплекс «VPN/FW ЗАСТАВА-10000».

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

AH (от английского Authentication Header) – протокол из группы IPsec, отвечает за аутентификацию источника и проверку целостности данных

CRL (от английского Certificate Revocation List) – см. СОС

DHCP (от английского Dynamic Host Configuration Protocol) – стандартный протокол получения клиентами IP-адреса и другой информации от централизованного DHCP-сервера

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

GSP (от английского Global Security Policy) – см. ГПБ

IKE (от английского Internet Key Exchange) – протокол обмена ключевой информацией, используемый совместно с протоколами IPsec для организации первичного защищенного канала ISAKMP SA

IP (от английского Internet Protocol) – уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP

IPsec (от английского IP Security) – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP

LDAP (от английского Lightweight Directory Access Protocol) – группа стандартных протоколов для доступа к каталогам («Directories»)

NAT (от английского Network Address Translation) – преобразование сетевых адресов

PMP (от английского Policy Management Protocol) – протокол распределения политики безопасности (в контексте ПО ЗУ)

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

SMB (от английского Server Message Block) – протокол прикладного уровня для удаленного доступа к файлам

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

TCP (от английского Transmission Control Protocol) – сетевой протокол транспортного уровня (с гарантированной доставкой) в IP-сетях

UDP (от английского User Datagram Protocol) – сетевой протокол транспортного уровня (без гарантированной доставки) в IP-сетях

VPN (от английского Virtual Private Network) – см. ВЧС

ВЧС – виртуальная частная сеть

ГПБ – глобальная политика безопасности

ЛПБ – локальная политика безопасности

МЭ – межсетевой экран

ОС – операционная система

ПО – программное обеспечение

ПО ЗУ – программное обеспечение «ЗАСТАВА-Управление», версия 8 КС1»

СВТ– средства вычислительной техники

СКЗИ – средство криптографической защиты информации

СОС – список отозванных сертификатов

УЦ – удостоверяющий центр

ЦС – центр сертификации

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	Заме–ненных	Изме–ненных	Новых	Изъя–тых					