

ООО «АМИКОН»

УТВЕРЖДЕН

РОФ.ПЕРС.00115-01 32-ЛУ

**Удаленный администратор «ФПСУ-IP»
(версия 4.0.1)**

Руководство по применению

РОФ.ПЕРС.00115-01 32

Листов 401

2025

Аннотация

Документ предназначен для сотрудников службы безопасности и администраторов безопасности систем защиты от несанкционированного доступа с применением средств защиты информации семейства «ФПСУ-IP». В документе содержатся общие сведения о программе «Удаленный администратор ФПСУ-IP» версии 4.0.1 и дано описание последовательности действий при настройке параметров функционирования изделия, в процессе эксплуатации и в аварийных ситуациях.

Если у вас возникнут какие-либо вопросы или предложения, вы можете обратиться непосредственно в ООО «АМИКОН». Вам всегда будут представлены подробные консультации по телефону или электронной почте.

Отзывы и предложения по документации просьба высыпать на электронную почту.

Контакты:

Наш адрес: ООО "АМИКОН", Варшавское шоссе, д. 125 (секция 1, цокольный этаж), г. Москва, 117587.

Телефон и факс: +7-(495)797-64-12, +7-(495)797-64-13.

Адрес в Интернет: <https://www.amicon.ru/>

On-line документация по продукции ООО "АМИКОН": <https://wiki.amicon.ru/>

Электронная почта: info@amicon.ru

Веб-форум ООО "АМИКОН": <https://forum.amicon.ru>

Мы работаем с 10:00 до 19:00 по московскому времени, кроме субботы и воскресенья.

© ООО «АМИКОН», 1994-2025. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Документ входит в комплект поставки изделия.

Без специального письменного разрешения ООО «АМИКОН» настоящий документ или его часть в печатном или электронном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

Информация, содержащаяся в настоящем документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны ООО «АМИКОН».

Содержание

1. Список используемых определений и сокращений	10
2. Общие сведения	14
2.1. Применимость руководства	15
3. Контроль целостности программного обеспечения УА ФПСУ-IP	17
3.1. Первоначальный контроль целостности после инсталляции	17
3.2. Контроль целостности в процессе эксплуатации	18
4. Установка, удаление и обновление ПО	21
4.1. Порядок установки УА ФПСУ-IP	21
4.2. Обновление УА ФПСУ-IP	25
4.3. Удаление УА ФПСУ-IP	26
5. Установка, удаление и обновление ПО под WINE	28
5.1. Порядок установки УА ФПСУ-IP под WINE	29
5.2. Удаление УА ФПСУ-IP, установленного под WINE	33
6. Лицензирование	34
7. Начало работы с УА ФПСУ-IP	38
7.1. Подключение VPN-Key/UA	38
7.2. Первый запуск УА ФПСУ-IP с VPN/Key UA	40
7.3. Первый запуск УА ФПСУ-IP без VPN-Key/UA	43
7.4. Первоначальная настройка УА ФПСУ-IP (с VPN-Key/UA)	46
7.5. Первоначальная настройка УА ФПСУ-IP (без VPN-Key/UA)	51
7.6. Управление лицензиями	57
8. Взаимная регистрация УА ФПСУ-IP и ФПСУ-IP	59
8.1. Выдача открытого ключа УА ФПСУ-IP для регистрации на ФПСУ-IP	59
8.2. Регистрация ФПСУ-IP в УА ФПСУ-IP	60
8.2.1. Регистрация открытого ключа ФПСУ-IP в УА ФПСУ-IP	60
8.2.2. Установка параметров взаимодействия ФПСУ-IP с УА ФПСУ-IP	63
8.2.3. Регистрация резервного ФПСУ-IP по открытому ключу основного	68
8.2.4. Изменение IP-адресов ФПСУ-IP из файла	70
8.3. Работа со списком ФПСУ-IP	70
8.3.1. Редактирование имен ФПСУ-IP	70

8.3.2. Удаление описателей ФПСУ-IP из списка	71
8.3.3. Повторная регистрация ФПСУ-IP	73
8.3.4. Регистрация пустых ФПСУ-IP	73
8.4. Выдача открытых ключей ФПСУ-IP из базы данных УА ФПСУ-IP	75
9. Интерфейс УА ФПСУ-IP	77
9.1. Основное окно (отображение зарегистрированных ФПСУ-IP)	78
9.1.1. Контекстное меню раздела	80
9.1.2. Контекстное меню зарегистрированного ФПСУ-IP	81
9.1.3. Контекстное меню нескольких ФПСУ-IP	85
9.2. Главное меню УА ФПСУ-IP	86
9.2.1. ФПСУ-IP	86
9.2.2. Операции	87
9.2.3. Конфигурации	89
9.2.4. Вид	90
9.2.5. Параметры	91
9.2.6. Ключ УА	92
9.2.7. Статистика ФПСУ-IP	93
9.2.8. Справка	94
9.3. Панель инструментов	95
9.4. Панель информации	96
9.5. Панель команд	99
9.6. Поиск зарегистрированных ФПСУ-IP	102
9.7. Завершение работы	102
10. Защита от несанкционированного доступа	104
10.1. Вход в УА ФПСУ-IP по USB-ключу	104
10.2. Установка дополнительного пароля	104
11. Управление конфигурациями ФПСУ-IP	106
11.1. Дистанционное изменение конфигурации	106
11.2. Загрузка конфигурации ФПСУ-IP на УА ФПСУ-IP	109
11.2.1. Загрузка конфигурации из файла	109
11.2.2. Получение конфигурации с ФПСУ-IP	113
11.2.3. Массовая и фоновая загрузка конфигураций	115
11.2.4. Копирование конфигурации с другого ФПСУ-IP	117
11.2.5. Установить задание на получение конфигураций	119
11.3. Просмотр и изменение конфигурации	122
11.3.1. Редактирование конфигурации ФПСУ-IP	122
11.3.2. Архивы конфигураций ФПСУ-IP	124

11.4. Установка измененной конфигурации на ФПСУ-IP	126
11.4.1. Выдача конфигурации в файл	126
11.4.2. Дистанционная установка конфигурации на ФПСУ-IP	127
11.4.3. Дистанционная массовая установка конфигураций	132
11.5. Просмотр файла сравнения конфигурации	135
11.6. Замена номера используемого ключа	137
11.7. Массовое изменение конфигураций по шаблону	143
11.7.1. Изменение общих параметров	150
11.7.2. Добавление/удаление абонента	155
11.7.3. Добавление/удаление ФПСУ-IP	159
11.7.4. Изменение сетевых сервисов	164
11.7.4.1 Изменение параметров Syslog	164
11.7.4.2 Изменение SNMP	168
11.7.4.3 Изменение NTP-клиента	169
11.7.4.4 Добавление/удаление IPFIX-трафика	170
11.7.5. Изменение параметров межсетевого экрана	172
11.7.5.1 Добавление/удаление службы	172
11.7.5.2 Добавление/удаление группы IP-адресов	176
11.7.5.3 Добавление/удаление правила трафика	178
11.7.5.4 Изменение настроек МЭ	183
11.7.6. Изменение Клиентских настроек	188
11.7.6.1 Изменение клиентов	188
11.7.6.2 Изменение локальных настроек	191
11.7.6.3 Абоненты	192
11.7.6.4 Настройки RADIUS	193
11.8. Массовая замена объектов межсетевого экрана	195
12. Операции	200
12.1. Массовые операции с ключами	200
12.2. Массовые операции с блокировкой трафика	202
12.3. Блокировка трафика на выбранных ФПСУ-IP	203
12.4. Запрос с ФПСУ-IP данных	206
12.5. Процессы с ФПСУ-IP	209
12.6. Изменение UA на группе ФПСУ-IP	210
12.7. Просмотр состояния задания на рассылку	214
12.8. Рассылка обновления ПО	215
12.9. Обновление множества ПО	219
12.10. Wake On LAN	224
13. Настройка UA ФПСУ-IP	228

13.1. Меню «Параметры» → «Настройки»	228
13.1.1. Настройки списка ФПСУ-IP	228
13.1.2. Настройка журнала событий с ФПСУ-IP на УА ФПСУ-IP	229
13.1.3. Дополнительные настройки интерфейса УА ФПСУ-IP	231
13.1.4. Дополнительные настройки УА ФПСУ-IP при работе с ФПСУ-IP	233
13.1.5. Настройка параметров syslog	236
13.1.6. Настройка опроса SNMP ФПСУ-IP	238
13.2. Режим разграничения полномочий пользователей УА ФПСУ-IP	241
13.3. Режим работы с несколькими администраторами УА ФПСУ-IP	247
13.4. Изменение параметров работы УА ФПСУ-IP	249
13.5. Настройка базы данных статистики УА ФПСУ-IP	250
13.6. Очистка диска	253
13.7. Последние изменения	255
14. Окно ручного управления ФПСУ-IP	258
14.1. Вход в режим ручного управления	258
14.2. Добавление удаленных администраторов и изменение прав доступа УА	260
14.3. Дистанционная установка/удаление ключевых данных	263
14.3.1. Дистанционная установка/удаление ключевых данных ФПСУ-IP	263
14.3.2. Дистанционная установка/удаление ключевых данных ProtoQa и CRISP	265
14.3.3. Дистанционная установка/удаление ключевых данных ФПСУ-IP/Клиентов	267
14.4. Синхронизация времени	269
14.5. Срок использования ключей	270
14.6. Установка дополнений и изменений на ФПСУ-IP	272
14.7. Дистанционная перезагрузка ФПСУ-IP	276
14.7.1. Дистанционная перезагрузка ФПСУ-IP	277
14.7.2. Дистанционная перезагрузка ОС ФПСУ-IP	278
15. Резервирование и восстановление работы УА ФПСУ-IP	279
15.1. Резервирование рабочих установок УА ФПСУ-IP	279
15.1.1. Создание резервной копии УА ФПСУ-IP	280
15.1.2. Резервирование описателей отдельных ФПСУ-IP	281
15.2. Восстановление в случае повторной установки ПО УА ФПСУ-IP	282
16. Управление и мониторинг ФПСУ-IP	284
16.1. Контроль состояния ФПСУ-IP	284
16.1.1. Опрос состояния VPN-туннелей с другими ФПСУ-IP	284

16.1.2. Получение информации о работе абонентов	287
16.1.3. Получение информации о работе клиентов	290
16.1.4. Получение информации о работе администраторов УА ФПСУ-IP	292
16.1.5. Получение информации об изменениях программного обеспечения	292
16.1.6. Получение информации о состоянии портов	293
16.1.7. Получение информации о загрузке процессора ФПСУ-IP	295
16.1.8. Получение информации о маршрутах	296
16.1.9. Просмотр ARP-таблиц	297
16.1.10. Просмотр статистики ФПСУ-IP	298
16.1.11. Дистанционный запуск ping на управляемом ФПСУ-IP	300
16.1.12. Мониторинг сессий МЭ	301
16.1.13. Мониторинг заблокированного трафика	305
16.1.14. Состояние ФПСУ-IP	307
16.2. Запрос с ФПСУ-IP по SNMP	308
16.3. Работа с квантовым дополнением	310
16.4. Настройка пороговых значений по умолчанию	314
16.4.1. Установка типов сигналов о событиях	316
16.4.2. Настройка пороговых значений на ФПСУ-IP	319
16.5. Сообщения от ФПСУ-IP	321
16.6. Получение данных о состоянии «горячего» резервирования	321
16.7. Диагностика ошибок с помощью mlog	323
17. Ключи УА	325
17.1. Управление VPN-Key/UA	325
17.1.1. Работа УА ФПСУ-IP с несколькими VPN-Key/UA	326
17.1.2. Пересоздание ключевых данных администратора УА ФПСУ-IP	327
17.1.3. Управление доступом к базе данных УА ФПСУ-IP	327
17.1.4. Управление паролями	330
17.1.5. Резервирование VPN-Key/UA	331
17.1.5.1 Создание дубликата VPN-Key/UA	331
17.1.5.2 Резервирование с помощью ключа УА	332
17.1.6. Управление ключевыми данными администратора (при работе с VPN-Key)	336
17.2. Управление ключевыми данными администратора УА ФПСУ-IP (без VPN-Key/UA)	338
17.2.1. Выдача ключа администратора УА ФПСУ-IP в файл	338
17.2.2. Загрузка ключа администратора УА ФПСУ-IP с диска	339
17.2.3. Выдача ключа для подключения к внешней БД	340

18. Работа со внешними базами данных	342
18.1. Настройка подключения ко внешней БД	342
18.1.1. Первое подключение к БД	344
18.1.1.1 Особенности работы со внешними БД PostgreSQL	345
18.1.1.2 Повторное подключение ко внешней БД	348
18.1.1.3 Отключение работы со внешней БД	350
18.1.1.4 Доступ ко внешней БД	351
18.1.1.4.1 Добавление или обновление УА при помощи файла	352
18.1.1.4.2 Добавление или обновление УА при помощи VPN-key/UA	353
18.1.1.4.3 Изменение прав доступа УА к БД	354
18.1.1.4.4 Удаление доступа УА к БД	355
18.1.1.4.5 Блокировка доступа УА к БД	355
18.1.1.4.6 Создание нового ключа доступа к БД	356
18.1.1.4.7 Обновление ключей УА	358
18.1.5. Операции с внешней БД	359
18.1.5.1 Обновление параметров ФПСУ-IP из внешней БД	360
18.1.5.2 Сохранение ФПСУ-IP в БД	360
18.1.5.3 Проверка обновлений ФПСУ-IP во внешней базе данных	360
18.1.5.4 Проверка наличия изменений параметров ФПСУ-IP	361
18.1.5.5 Контейнеры списков ФПСУ-IP	361
18.1.5.5.1 Изменение прав доступа на контейнер	361
18.1.5.5.2 Заполнение контейнера	361
18.1.5.6 Конфигурация ФПСУ-IP	361
18.1.6. Учетная информация по ФПСУ-IP	363
18.1.6.1 Просмотр дополнительной информации по ФПСУ-IP	364
18.1.6.2 Настройка полей учетной информации	364
18.2. Взаимодействие ФПСУ-IP со внешней БД	364
18.2.1. Обновление ФПСУ-IP из внешней БД	365
18.2.2. Сохранение ФПСУ-IP во внешней БД	367
19. Управление статистикой ФПСУ-IP	369
19.1. Получение статистической информации	370
19.1.1. Автоматический сбор статистической информации	370
19.1.2. Получение статистики по сети по запросу администратора	371
19.1.3. Загрузка статистической информации из DOS архива УА ФПСУ-IP	374
19.2. Просмотр накопленных статистических данных	375
19.2.1. Наблюдение за автоматическим сбором статистики	378
19.3. Перемещение статистики в архив	378

19.3.1. Перемещение статистики в архив администратором	379
19.3.2. Автоматическое перемещение статистики в архив	379
19.4. Просмотр статистики из архива	381
20. Рекомендованные процедуры смены ключей УА	383
20.1. Процедура смены ключа УА	383
20.2. Процедура смены ключа шифрования БД УА	389
20.3. Процедура смены ключа доступа ко внешней БД	392
21. Способы разрешения возможных проблем при работе УА ФПСУ-IP	396

1. Список используемых определений и сокращений

Администратор внешней БД	пользователь (или администратор) УА ФПСУ-IP, имеющий полный доступ ко внешней базе данных;
Администратор VPN-Key/UA	учетная запись VPN-Key/UA с PIN-кодом доступа, позволяющая инициализировать VPN-Key/UA и менять настройки его системных данных;
Пользователь VPN-Key/UA	учетная запись VPN-Key/UA с PIN-кодом доступа, позволяющая считывать системные данные VPN-Key/UA;
Администратор ОС	учетная запись операционной системы рабочей станции с установленной программой УА ФПСУ-IP, имеющая права администратора операционной системы;
УА ФПСУ-IP	программа «Удаленный администратор «ФПСУ-IP», модификация 4.0.1 одного из следующих вариантов исполнения СКЗИ «ФПСУ-IP Amigo»: <ul style="list-style-type: none"> • «АРМ УА КС1»; • «АРМ УА КС2»; • «АРМ УА КС3».
БД	база данных;
Внешняя БД	состоящая из контейнеров база данных настроек ФПСУ-IP, доступ к которой УА ФПСУ-IP осуществляет по сети передачи данных;
Контейнер	составляемый администратором внешней БД список описателей ФПСУ-IP;
Учетная лицензия	основная лицензия на использование программы. Представляет собой файл, содержащий регистрационный номер изделия, даты начала и окончания гарантийного срока применения;

Лицензия на количество ФПСУ-IP	файл лицензии-расширения на количество зарегистрированных в УА ФПСУ-IP с ключом (в базовой комплектации на 5 ФПСУ-IP). Данная лицензия не будет работать без привязки к учетной лицензии;
Лицензия на работу с сетевой базой данных	файл лицензии-расширения, позволяющий подключаться ко внешней (сетевой) базе данных. Данная лицензия не будет работать без привязки к учетной лицензии;
Лицензия на использование с VPN-Key/UA	файл лицензии, позволяющий работу УА ФПСУ-IP с аппаратным ключом доступа к программе, устройством VPN-Key/UA;
Лицензия на продление гарантийного срока	файл-лицензия на продление гарантийного срока после окончания гарантийного срока учетной лицензии.
Описатель ФПСУ-IP	совокупность параметров ФПСУ-IP, необходимая УА ФПСУ-IP для соединения и управления комплексом ФПСУ-IP;
ОС	операционная система;
ПО	программное обеспечение;
Пользователь (администратор) УА ФПСУ-IP	сотрудник, работающий с УА ФПСУ-IP с использованием созданного для него при помощи добавления тех или иных ролей профиля;
Профиль пользователя (администратора)	роль или совокупность ролей, на основании которой пользователь может выполнять те или иные действия на УА ФПСУ-IP;
Роль	совокупность прав доступа к функциям УА ФПСУ-IP, на основании которой формируется профиль пользователя. По умолчанию существует 3 роли: 1. Администратор – эта Роль предполагает возможность редактировать все данные.

	<p>2. Роль Монитор – эта Роль предполагает право на мониторинг ФПСУ-IP.</p> <p>3. Роль УА ФПСУ-IP – эта Роль предполагает возможность управления ФПСУ-IP и ограничение в редактировании настроек.</p>
СКЗИ	средство криптографической защиты информации;
ФПСУ-IP	<p>общее обозначение для любого из следующих продуктов:</p> <ul style="list-style-type: none"> • криптомаршрутизатор и межсетевой экран «ФПСУ-IP Amigo» версии 4; • программный комплекс «ФПСУ-IP» версии 3; • программно-аппаратный комплекс «ФПСУ-IP» версии 3.
ФПСУ-IP/Клиент	программный или программно-аппаратный комплекс «ФПСУ-IP/Клиент»;
VPN-Key/UA	программно-аппаратное устройство «VPN-Key/UA» разработки ООО «АМИКОН», подключаемое к USB-порту рабочей станции, на которую установлен программный комплекс «Удаленный администратор "ФПСУ-IP"»;
PIN-код пользователя VPN-Key/UA (основной пароль)	код устройства «VPN-Key/UA», требующийся для запуска и последующей работы УА ФПСУ-IP;
PIN-код администратора VPN-Key/UA (резервный пароль)	код устройства «VPN-Key/UA», требующийся при первом запуске УА ФПСУ-IP, и в дальнейшем использующийся только для системной настройки VPN-Key/UA.
FPSUHash	Программа контроля целостности файлов, предназначенная для вычисления хэш-кодов (хэш-сумм) файлов с учетом их содержимого. При работе с АРМ УА используются WinFPSUHash (для запуска программы в ОС семейства Windows) и LinFPSUHash (для запуска программы в ОС семейства Linux).

ProtoQa	протокол прикладного уровня, использующий в качестве внешнего контура защиты протокол CRISP. Протокол применяется в целях информационно-логического взаимодействия между СКЗИ-Распределителем и СКЗИ-Потребителем.
CRISP	протокол защищенной передачи данных, в котором используются только механизмы защиты с секретным ключом, при этом обеспечиваются требуемые свойства безопасности.

2. Общие сведения

Программно-аппаратный комплекс шифрования «ФПСУ-IP» включает в себя средства, позволяющие осуществлять централизованное дистанционное управление работой группы (до 64 000) ФПСУ-IP и контроль их функционирования с помощью программного комплекса «Удаленный администратор «ФПСУ-IP».

На каждом отдельном ФПСУ-IP может быть зарегистрировано до 128 администраторов УА ФПСУ-IP, причём каждый из них может иметь исключительные права на осуществление отдельных операций по управлению ФПСУ-IP.

УА ФПСУ-IP осуществляет дистанционное управление ФПСУ-IP с использованием криптографически защищенного канала связи (VPN-туннеля), в котором производятся взаимная идентификация и строгая двусторонняя аутентификация ФПСУ-IP и УА ФПСУ-IP. Процедура взаимной регистрации описывается в разделе «Взаимная регистрация УА ФПСУ-IP и ФПСУ-IP» данного документа.

Подсистема удаленного администрирования предоставляет администратору УА ФПСУ-IP следующие возможности:

- мониторинг состояния ФПСУ-IP как в автоматическом режиме, так и в режиме непосредственного обращения;
- программирование автоматического анализа получаемой в процессе мониторинга информации с оперативно отображаемой графической и многоуровневой звуковой сигнализацией;
- получение указанной по виду и времени регистрационной информации с ФПСУ-IP как в автоматическом режиме, так и в режиме непосредственного обращения;
- получение (как по сети, так и посредством передачи на носителе) рабочих настроек (конфигурации) ФПСУ-IP, в частности установленных правил фильтрации;
- изменение и установка (как по сети, так и посредством передачи на носителе) в задаваемый момент времени новой конфигурации (в частности, правил фильтрации) на ФПСУ-IP;
- дистанционная установка и удаление ключевых данных, применяемых ФПСУ-IP для создания VPN-туннелей передачи данных между абонентами и пользователями ФПСУ-IP/Клиентов;
- дистанционная установка и удаление новых администраторов УА ФПСУ-IP;
- синхронизация времени на ФПСУ-IP с текущим временем УА ФПСУ-IP как в

автоматическом, так и в ручном режимах;

- дистанционная установка дополнительного программного обеспечения ФПСУ-IP и дистанционная замена установленных программных модулей ФПСУ-IP (в частности, дистанционное обновление версии);
- дистанционная перезагрузка операционной системы ФПСУ-IP;
- дистанционная передача управления работой ФПСУ-IP его партнеру по резервированию.

В подсистеме удаленного администрирования ФПСУ-IP реализованы следующие механизмы защиты от НСД:

- идентификация и аутентификация администратора УА ФПСУ-IP при запуске и настройке УА ФПСУ-IP с использованием ключа УА;
- защита работы УА ФПСУ-IP путем блокировки любых действий до введения дополнительного символьного пароля;
- разграничение и контроль доступа к подсистемам ФПСУ-IP для нескольких администраторов УА ФПСУ-IP;
- регистрация администраторов УА ФПСУ-IP и сбор регистрационной информации об их действиях на ФПСУ-IP.

Меры по защите работы УА ФПСУ-IP от несанкционированного доступа рассматриваются в разделе «Защита от несанкционированного доступа».

Рабочие установки УА ФПСУ-IP (параметры работы, список зарегистрированных ФПСУ-IP, имя администратора, базы статистики) могут быть выгружены в специальные файлы, что позволяет быстро восстанавливать работу УА ФПСУ-IP после аварий и сбоев внутреннего накопителя компьютера (см. раздел «Резервирование и восстановление работы УА ФПСУ-IP»).

2. 1. Применимость руководства

Руководство распространяется на программное обеспечение «Удаленный администратор «ФПСУ-IP» версии 4.0.1 и на на следующие указанные в таблице варианты поставки изделия:

Код варианта изделия	Наименование варианта изделия
FPSUIP-RADM-1USB	Автоматизированное рабочее место удаленного администратора (1 рабочее место, управление до 5 «ФПСУ-IP»)
FPSUIP-RADM-2USB	Автоматизированное рабочее место удаленного администратора (2 рабочих места, управление до 5 «ФПСУ-IP»)

3. Контроль целостности программного обеспечения УА ФПСУ-IP

Контроль целостности программного обеспечения УА ФПСУ-IP осуществляется при помощи программы контроля целостности файлов 2.0 (далее - программа FPSUHash).

Полная информация по использованию программы FPSUHash для создания эталонных контрольных сумм и проведения проверки указанных файлов представлена в документе РОФ.ПЕРС.00104-01 34 02 «Программа контроля целостности файлов. Инструкция по эксплуатации».

3. 1. Первонаучальный контроль целостности после инсталляции

Непосредственно после установки ПО УА ФПСУ-IP на рабочую станцию следует выполнить первонаучальный контроль целостности программных модулей УА ФПСУ-IP.

Контроль целостности осуществляется при помощи запуска программы WinFPSUHash с параметрами командной строки WRADM.EXE.HSH, GRN.DLL.HSH, SQLITE3.DLL.HSH, EDIT301.EXE.HSH, EDIT330.EXE.HSH, EDIT331.EXE.HSH, EDIT400.EXE.HSH, TMUSB10.SYS.HSH, CFG3DSR_330.EXE, CFG3DSR_400.EXE, DSR_DIFF.EXE, WINFPSUHASH.EXE, LINFPSUHASH, AMICHECK_WIN.EXE и AMICHECK_LIN (в случае, если они поставлены).

Для выполнения первонаучального контроля целостности после установки следует:

- Открыть рабочий каталог программы УА ФПСУ-IP (при установке по умолчанию это каталог «%C%\Wradm»);
- Запускать программу проверки WinFPSUHash из командной строки операционной системы Windows, указывая путь к программе с дополнительными параметрами.

```
C:\Wradm5>.\WinFPSUHash.exe .\Hash\wradm.exe.hsh -S

Программа контроля целостности файлов. Версия 2.0, (C) 000 "АМИКОН", 2022

Проверка хэш-кода на ".\wradm.exe"
Алгоритм хэш-кода: ГОСТ Р 34.11-2012
Эталонный хэш-код: 72E9220DB408033123A050B5014A80DF1C8667733BF0034752E5F99A6EE6CB82
Рассчитанный хэш-код: 72E9220DB408033123A050B5014A80DF1C8667733BF0034752E5F99A6EE6CB82
Результат: Верно. Рассчитанный хэш-код совпадает с эталонным.

Отчет: ".\Hash\wradm.exe.lst"
C:\Wradm5>
```

Рисунок 1 - Пример запуска программы проверки WinFPSUHash.exe

После отработки программы результаты проверки будут выданы в текстовом виде на экран монитора и в файлы WRADM.EXE.LST, GRN.DLL.LST, SQLITE3.DLL.LST, EDIT301.EXE.LST, EDIT330.EXE.HSH.LST, EDIT331.EXE.HSH.LST, EDIT400.EXE.HSH.LST, CFG3DSR_330.EXE.LST, CFG3DSR_400.EXE, DSR_DIFF.EXE.LST, WINFPSUHASH.EXE.LST, которые будут созданы в каталоге HASH рабочего каталога программы и могут быть прочитаны и обработаны средствами текстового редактора, поддерживающим кодировку OEM/DOS. Кроме этого, результат проверки следует сравнить с эталонными контрольными суммами.

При обнаружении нарушения целостности программного модуля УА ФПСУ-IP, программу необходимо повторно установить с инсталляционного носителя.

Первоначальный контроль целостности после инсталляции при установке АРМ УА на ПК под управлением ОС Linux можно производить как при помощи программы графического интерфейса WinFPSUHash (см. п. «Первоначальный контроль целостности после инсталляции» и справку по FPSUHASH v. 2.0), запуская её под WINE, так и при помощи программы LinFPSUHash. При проверке с использованием LinFPSUHash перечисленных выше файлов следует запускать программу контроля целостности с дополнительным параметром -C.

3. 2. Контроль целостности в процессе эксплуатации

Ниже приведен пример контроля целостности модулей УА ФПСУ-IP с помощью программы WinFPSUHash. Пример контроля целостности исполняемых файлов ОС, требующих такой проверки, в данном документе не приводится.

Контроль целостности модулей УА ФПСУ-IP в процессе эксплуатации следует осуществлять программой WINFPSUHASH.EXE, запуская её исполняемый файл

winfpsuhash.exe с параметрами командной строки WRADM.EXE.HSH, GRN.DLL.HSH, SQLITE3.DLL.HSH, EDIT301.EXE.HSH, EDIT330.EXE.HSH, EDIT331.EXE.HSH, EDIT400.EXE.HSH, TMUSB10.SYS.HSH, CFG3DSR_330.EXE, CFG3DSR_400.EXE, DSR_DIFF.EXE, WINFPSUHASH.EXE, LINFPSUHASH, AMICHECK_WIN.EXE и AMICHECK_LIN (в случае, если они поставлены).

Для выполнения контроля целостности в процессе эксплуатации следует:

- Открыть рабочий каталог программы УА ФПСУ-IP (при установке по умолчанию это каталог «%C%\Wradm»);
- Запускать программу проверки WinFPSUHash из командной строки операционной системы Windows, указывая путь к программе с дополнительными параметрами.

```
C:\Wradm5>.\WinFPSUHash.exe .\Hash\wradm.exe.hsh -S

Программа контроля целостности файлов. Версия 2.0, (С) ООО "АМИКОН", 2022

Проверка хэш-кода на ".\wradm.exe"
Алгоритм хэш-кода: ГОСТ Р 34.11-2012
Эталонный хэш-код: 72E9220DB408033123A050B5014A80DF1C8667733BF0034752E5F99A6EE6CB82
Рассчитанный хэш-код: 72E9220DB408033123A050B5014A80DF1C8667733BF0034752E5F99A6EE6CB82
Результат: Верно. Рассчитанный хэш-код совпадает с эталонным.

Отчет: ".\Hash\wradm.exe.lst"
C:\Wradm5>
```

Рисунок 2 - Пример запуска программы проверки WinFPSUHash.exe

Полная информация по использованию программы WinFPSUHash для создания эталонных контрольных сумм и проведения проверки указанных файлов представлена в документе РОФ.ПЕРС.00104-01 34 02 «Программа контроля целостности файлов. Инструкция по эксплуатации».

После отработки программы по описанному выше примеру, результаты проверки модулей УА ФПСУ-IP будут выданы в текстовом виде на экран монитора и в файлы WRADM.EXE.LST, GRN.DLL.LST, SQLITE3.DLL.LST, EDIT301.EXE.LST, EDIT330.EXE.HSH.LST, EDIT331.EXE.HSH.LST, EDIT400.EXE.HSH.LST, CFG3DSR_330.EXE.LST, CFG3DSR_400.EXE, DSR_DIFF.EXE.LST, WINFPSUHASH.EXE.LST, которые будут созданы в каталоге HASH рабочего каталога программы и могут быть прочитаны и обработаны средствами текстового редактора, поддерживающим кодировку UTF-8.

При обнаружении нарушения целостности любого программного модуля УА ФПСУ-

IP, необходимо повторно произвести инсталляцию.

Если в результате работы программы проверки появляется сообщение о нарушении целостности контролируемых файлов ОС и/или сторонних программ, работающих совместно с УА ФПСУ-IP, дальнейшая эксплуатация УА ФПСУ-IP не допускается. Следует проанализировать причину изменения контролируемых файлов, и затем, в случае необходимости, переустановить контролируемые файлы. До восстановления целостности контролируемых файлов использовать УА ФПСУ-IP запрещено.

Контроль целостности в процессе дальнейшей эксплуатации при установке АРМ УА на ПК под управлением ОС Linux можно производить как при помощи программы графического интерфейса WinFPSUHash (см. п. «Контроль целостности в процессе эксплуатации» и «Справку по FPSUHASH v. 2.0»), запуская её под WINE, так и при помощи программы LinFPSUHash. При проверке с использованием LinFPSUHash перечисленных выше файлов следует запускать программу контроля целостности с дополнительным параметром -C.

4. Установка, удаление и обновление ПО

Программное обеспечение УА ФПСУ-IP может быть установлено на компьютер, отвечающий следующим программным и аппаратным требованиям:

- операционная система — ОС Windows 10, Windows 11, Windows Server 2019, Ubuntu 24.04, Astra Linux SE 1.8.1.6, РЕД ОС 8;
- права локального администратора операционной системы для установки и запуска УА ФПСУ-IP;
- процессор — в соответствии с требованиями операционной системы;
- оперативная память — в соответствии с требованиями операционной системы;
- память внутреннего накопителя — в соответствии с требованиями операционной системы, и не менее 500 мегабайт свободной памяти с учетом накапливаемых данных статистики;
- USB порт — поддержка USB 2.0.

ВНИМАНИЕ! УА ФПСУ-IP во время эксплуатации должен находиться в защищенном средствами ФПСУ-IP фрагменте IP-сети.

Программная часть УА ФПСУ-IP поставляется на носителе, содержащей инсталляционный дистрибутив - файл SETUP_WRADM_#.##.##.EXE (#.##.## — номер версии программного обеспечения).

4. 1. Порядок установки УА ФПСУ-IP

Для установки программного обеспечения УА ФПСУ-IP требуется права администратора операционной системы.

Все снимки экрана и примеры в данном документе приводятся для ОС Windows 10 и версии УА ФПСУ-IP 4.0.1. При установке и использовании ПО в иных операционных системах во внешнем виде интерфейса, расположении иконок и пунктов меню могут наблюдаться отличия от приведенных снимков.

Для установки программного обеспечения необходимо:

1. Проверить соответствие компьютера условиям, описанным в п. «Установка, удаление и обновление ПО»;
2. Запустить инсталляционный дистрибутив SETUP_WRADM_#.##.##.EXE.

Дальнейшие шаги установки проводятся с помощью мастера установки:

3. Первое окно установки УА ФПСУ-IP содержит лицензионное соглашение. В случае несогласия следует нажать кнопку «Отмена» для прекращения установки. Для продолжения установки необходимо нажать кнопку «Принимаю»;

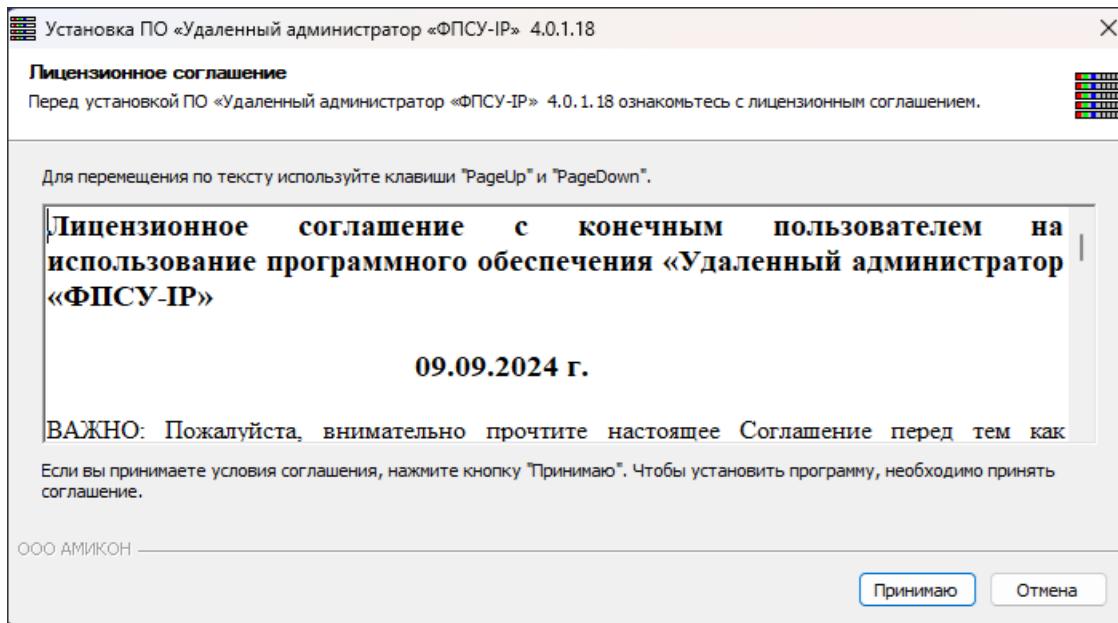


Рисунок 3 - Лицензионное соглашение

4. Второе окно мастера установки предлагает сделать выбор устанавливаемых опций:

- «Администратор ФПСУ-IP (Wradm)», основное устанавливаемое программное обеспечение, обязательный выбор;
- «Драйвер ТМ», библиотеки поддержки считывателя ТМ-идентификаторов, необходимых для передачи на ФПСУ-IP ключей ЦГКК.

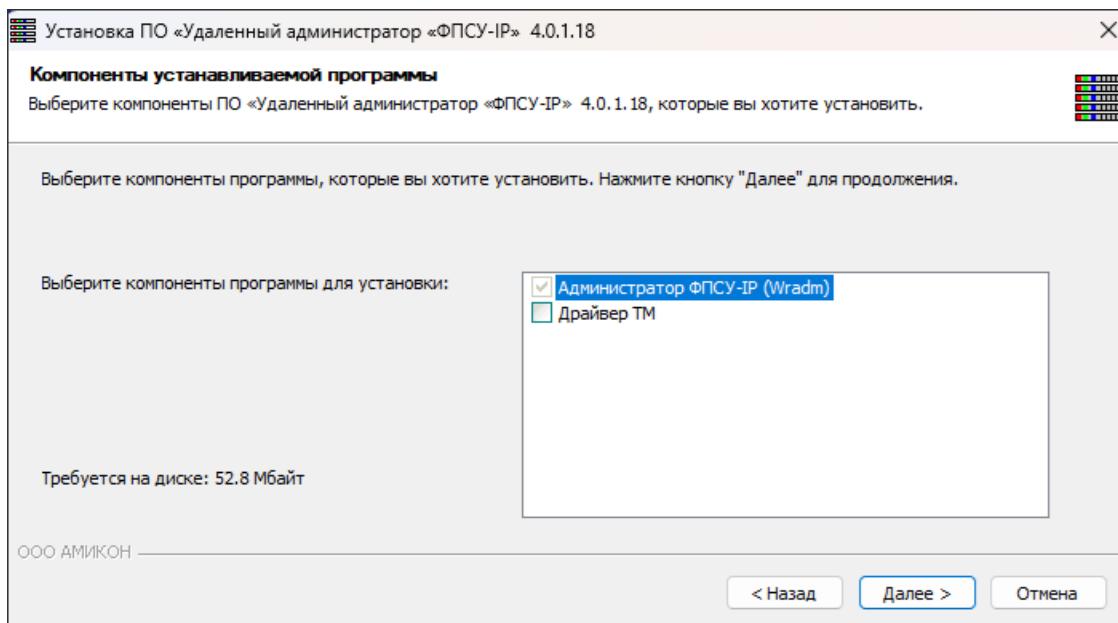


Рисунок 4 - Выбор компонентов УА ФПСУ-IP

5. Следующим шагом следует указать рабочий каталог, в котором будет находиться программное обеспечение УА ФПСУ-IP. Рабочим каталогом по умолчанию является \Wradm. Для изменения рабочего каталога необходимо ввести полный путь в строке выбора или, воспользовавшись кнопкой «Обзор», выбрать каталог в стандартном окне выбора.
6. Для запуска процесса установки УА ФПСУ-IP необходимо нажать кнопку «Установить» в окне выбора каталога.

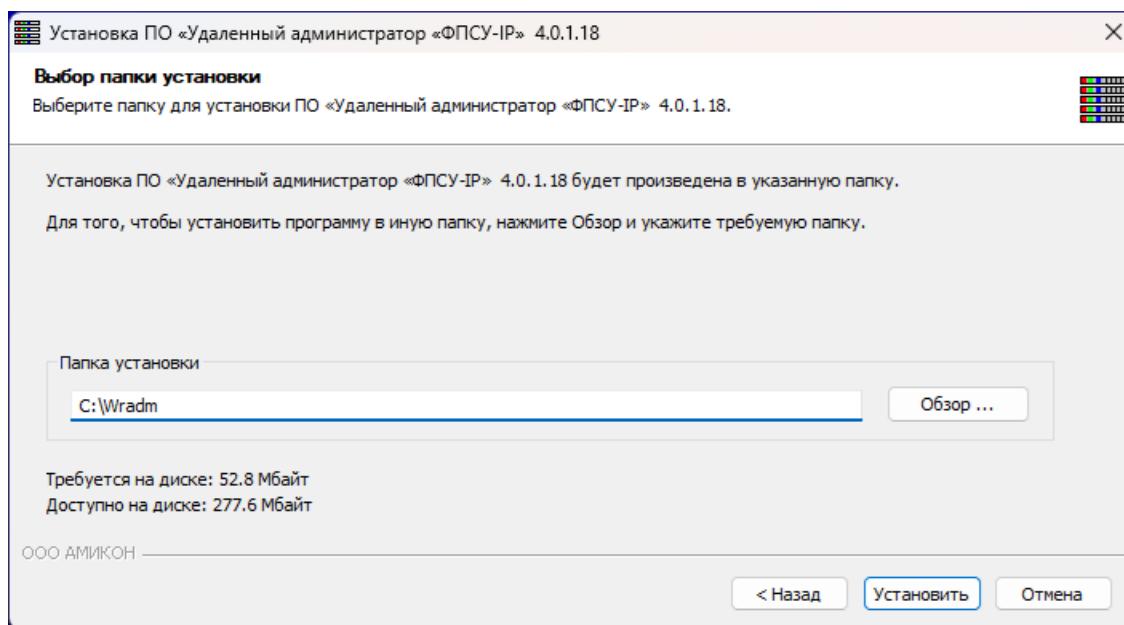


Рисунок 5 - Выбор каталога УА ФПСУ-IP

7. Процесс установки завершается состоянием «Готово» в окне прогресса установки.

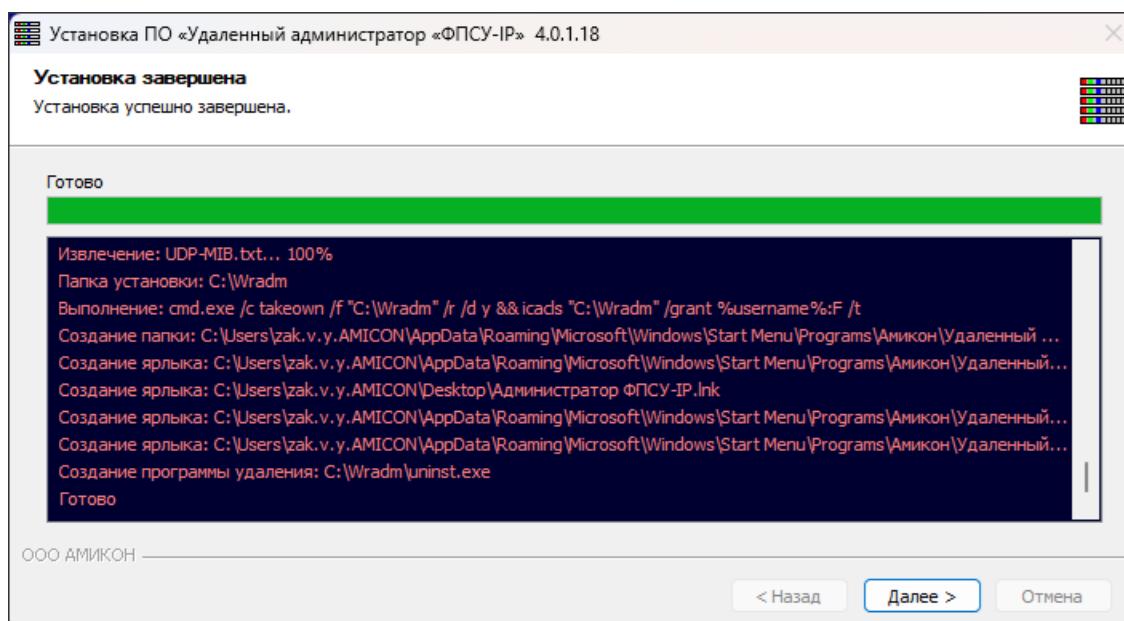


Рисунок 6 - Окно прогресса установки

Для завершения установки необходимо нажать кнопку «Далее» и в открывшемся окне подтвердить завершение установки нажатием кнопки «Готово».

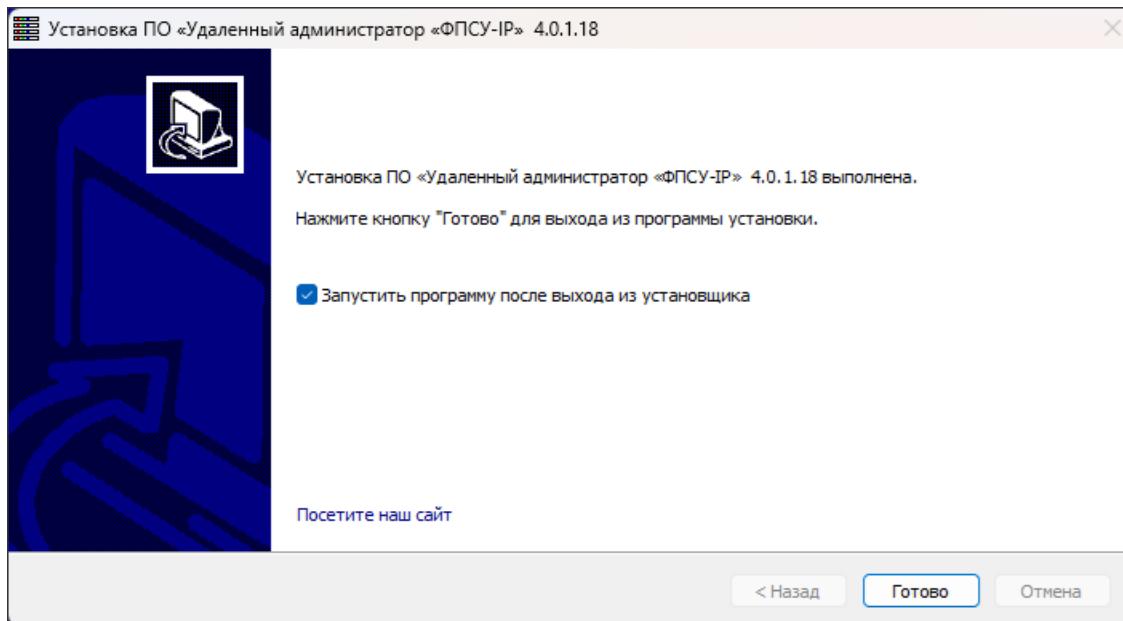


Рисунок 7 - Завершение установки

Перед дальнейшей эксплуатацией программы следует произвести начальные настройки УА ФПСУ-IP во время первого запуска, и зарегистрировать в УА ФПСУ-IP, которые требуется удаленно отслеживать и управлять.

Детальное рассмотрение первого запуска УА ФПСУ-IP находится в разделе «Начало работы с УА ФПСУ-IP».

Детальное рассмотрение интерфейса находится в разделе «Интерфейс УА ФПСУ-IP».

4. 2. Обновление УА ФПСУ-IP

При получении информации о выходе обновления программного обеспечения УА ФПСУ-IP, администратор безопасности должен определить необходимость установки данного обновления и обратиться в службу технической поддержки производителя УА ФПСУ-IP за получением обновления.

Обновление программного обеспечения УА ФПСУ-IP выполняется инсталляцией новой версии поверх старой, в рабочий каталог предыдущей версии.

Так же следует иметь в виду, что учетная лицензия содержит информацию о сроке гарантийной поддержки. По истечении срока действия система выдаст сообщение об окончании срока поддержки. Если установить обновление версии программного обеспечения УА ФПСУ-IP, выпущенное после даты окончания срока поддержки, программа не будет полноценно работать без обновления лицензии.

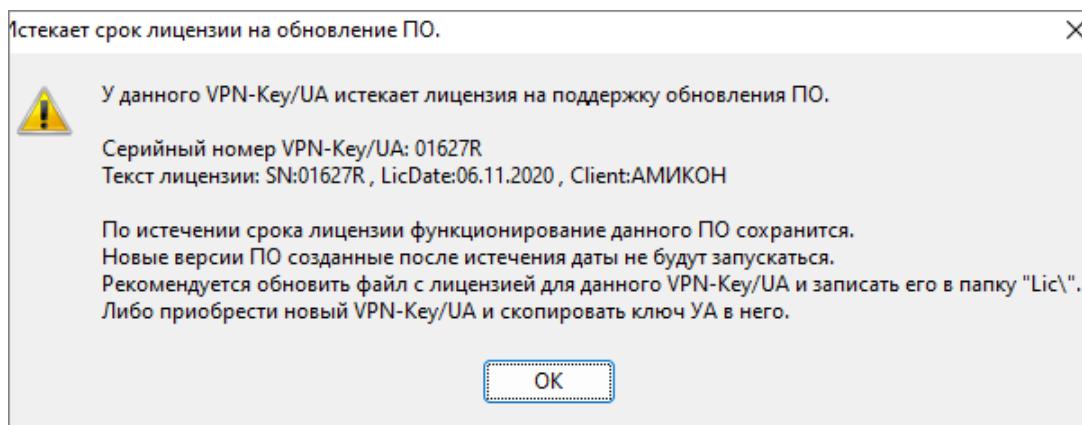


Рисунок 8 - Сообщение об истечении сроков лицензии на поддержку обновления

Для продления гарантийного срока необходимо получить лицензию на продление гарантийного срока поддержки FPSUIP-RADM-UPD и разместить ее в подкаталоге LIC рабочего каталога UA ФПСУ-IP.

4. 3. Удаление UA ФПСУ-IP

Для удаления программного обеспечения UA ФПСУ-IP из операционной системы следует использовать мастера удаления приложения. Запускается мастер удаления приложения одним из следующих способов:

- Выполнением команды «Пуск» → «АМИКОН» → «Администратор ФПСУ-IP» → «Uninstall»;
- Выбором в Панели управления Windows пункта «Программы» → «Удаление программ», с последующим нахождением в списке установленных программ объекта «ПО "Удаленный администратор ФПСУ-IP" X.0», и нажатием на кнопку «Заменить/Удалить»;
- Запуском файла UNINST.EXE, находящегося в рабочем каталоге программы UA ФПСУ-IP.

Работа мастера начинается с запроса подтверждения на выполнение операции:

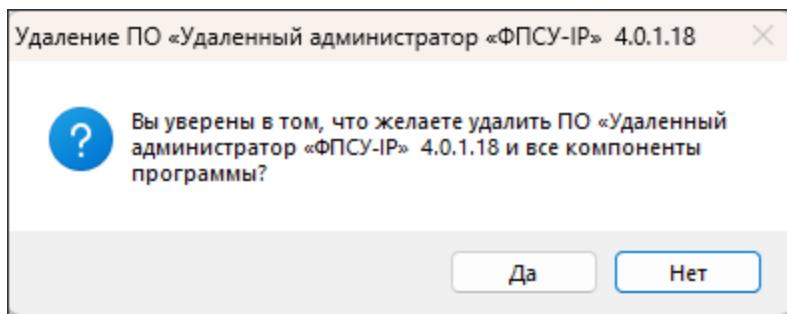


Рисунок 9 - Подтверждение удаления УА ФПСУ-IP

Успешное удаление с компьютера программного обеспечения УА ФПСУ-IP будет подтверждено служебным сообщением о том, что удаление программы было успешно завершено.

Мастер удаления УА ФПСУ-IP после завершения работы оставляет в рабочем каталоге программы созданные пользователем файлы. Для полного удаления УА ФПСУ-IP с компьютера следует удалить объекты, оставшиеся в рабочем каталоге УА ФПСУ-IP и его подкаталогах.

5. Установка, удаление и обновление ПО под WINE

Wine – свободное программное обеспечение, позволяющее пользователям UNIX-подобных операционных систем, например GNU/Linux и других UNIX-подобных с поддержкой архитектур CPU x86, AMD64 (и других архитектур CPU при наличии совместимости с ними запускаемых приложений) исполнять 16-, 32- и 64-битные приложения, созданные исключительно для Microsoft Windows, без наличия при этом установленной Microsoft Windows.

Программное обеспечение УА ФПСУ-IP может быть установлено на компьютер, отвечающий следующим программным и аппаратным требованиям:

- операционная система — РЕД ОС, Astra Linux;
- права локального администратора операционной системы для установки и запуска УА ФПСУ-IP;
- процессор — в соответствии с требованиями операционной системы;
- оперативная память — в соответствии с требованиями операционной системы;
- память внутреннего накопителя — в соответствии с требованиями операционной системы, и не менее 500 мегабайт свободной памяти с учетом накапливаемых данных статистики;
- USB порт — поддержка USB 2.0.

* - операционная система в комплект поставки программного обеспечения не входит. Запрещается устанавливать УА ФПСУ-IP на операционную систему, которая не поддерживается производителем.

ВНИМАНИЕ! УА ФПСУ-IP во время эксплуатации должен находиться в защищенном средствами ФПСУ-IP фрагменте IP-сети.

Программная часть УА ФПСУ-IP поставляется на носителе, содержащей инсталляционный дистрибутив - файл SETUP_WRADM_#.##.#.EXE (#.##.# — номер версии программного обеспечения), необходимые лицензии (см. п. Лицензирование) и файл dpkg -i astra_pack.deb (для ОС Astra Linux) или dnf install package.rpm (для РЕД ОС).

В данном руководстве описана работа с АРМ УА на примере установки под WINE на РЕД ОС.

Для установки последних версий wine для РЕД ОС необходимо открыть терминал (команда **ctrl+alt+T**) и выполнить последовательно следующие команды:

- *sudo yum install -y* (обновление пакетов системы);
- *sudo yum install -y wine* (непосредственно установка Wine);
- *sudo dnf install -y имя_файла.*

5. 1. Порядок установки УА ФПСУ-IP под WINE

Для установки программного обеспечения УА ФПСУ-IP в РЕД ОС под Wine необходимо:

1. Запустить инсталляционный дистрибутив SETUP_WRADM_#.##.##.EXE (а именно, открыть терминал и прописать в нем: "wine путь к установочному файлу/SETUP_WRADM_#.##.##.EXE"). Дальнейшие шаги установки проводятся с помощью мастера установки;
2. Первое окно установки УА ФПСУ-IP содержит лицензионное соглашение. В случае несогласия следует нажать кнопку «Отмена» для прекращения установки. Для продолжения установки необходимо нажать кнопку «Принимаю»;

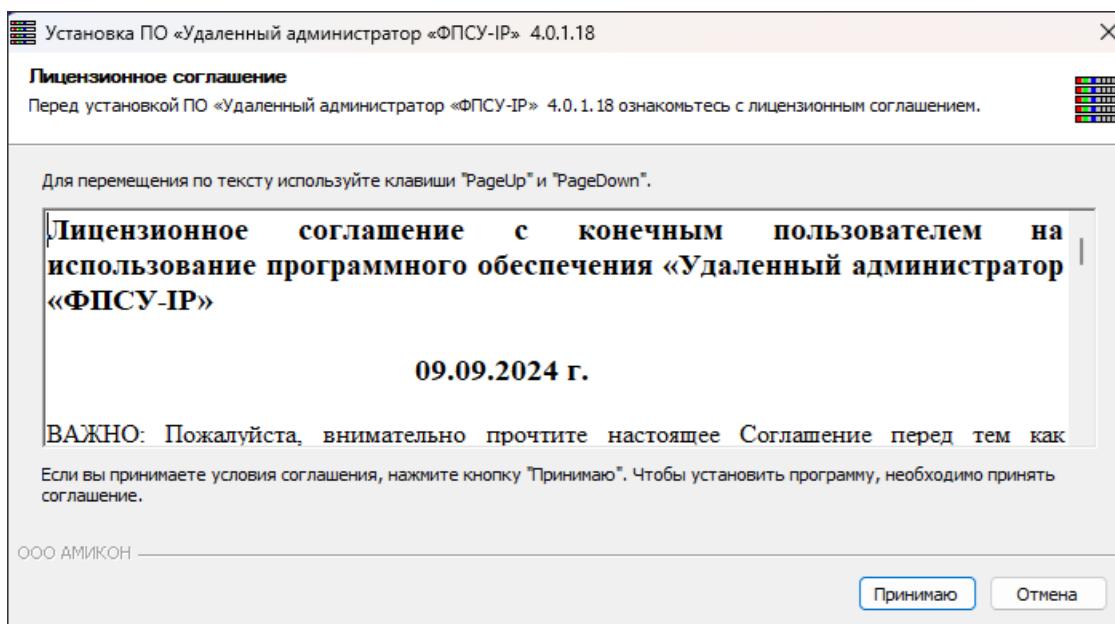


Рисунок 10 - Лицензионное соглашение

3. Второе окно мастера установки предлагает сделать выбор устанавливаемых опций:

- «Администратор ФПСУ-IP (Wradm)», основное устанавливаемое программное обеспечение, обязательный выбор;

- «Драйвер ТМ», библиотеки поддержки считывателя ТМ-идентификаторов, необходимых для передачи на ФПСУ-IP ключей ЦГКК.

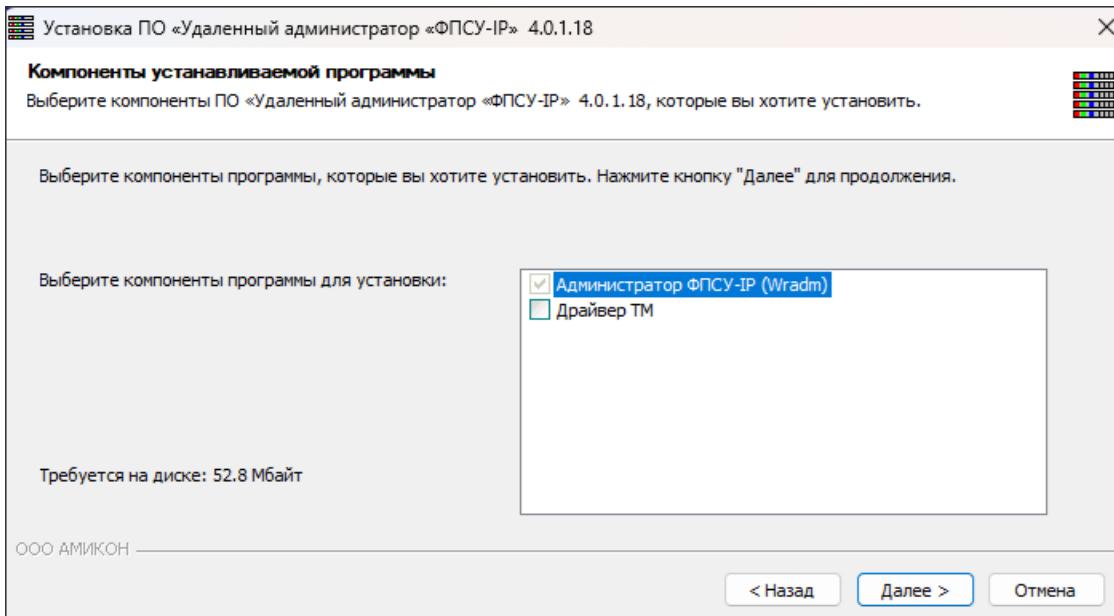


Рисунок 11 - Выбор компонентов УА ФПСУ-IP

4. Следующим шагом следует указать рабочий каталог, в котором будет находиться программное обеспечение УА ФПСУ-IP. Рабочим каталогом по умолчанию является \Wradm. Для изменения рабочего каталога необходимо ввести полный путь в строке выбора или, воспользовавшись кнопкой «Обзор», выбрать каталог в стандартном окне выбора.
5. Для запуска процесса установки УА ФПСУ-IP необходимо нажать кнопку «Установить» в окне выбора каталога.

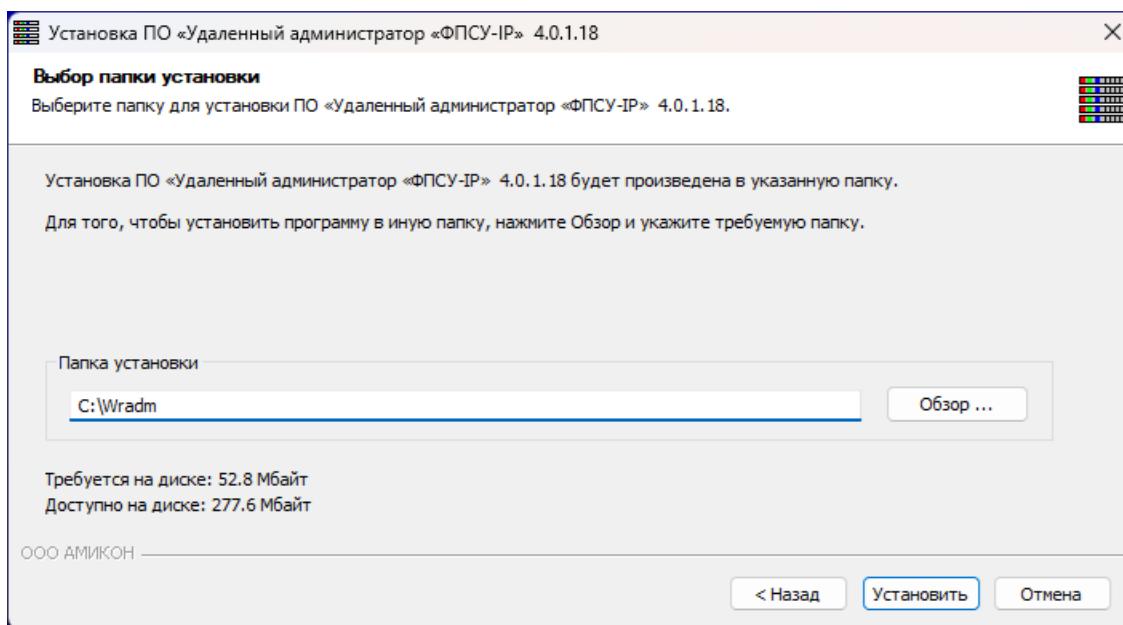


Рисунок 12 - Выбор каталога УА ФПСУ-IP

7. Процесс установки завершается состоянием «Готово» в окне прогресса установки.

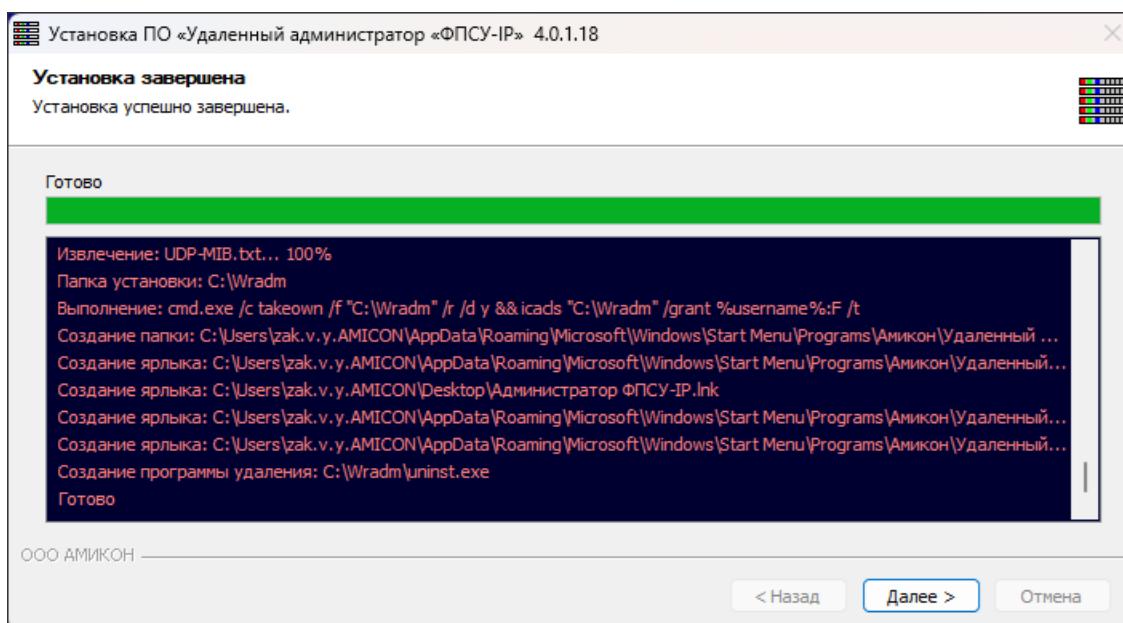


Рисунок 13 - Окно прогресса установки

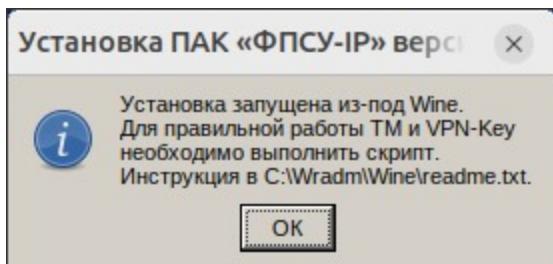


Рисунок 14 - Окно предупреждения об установке из-под Wine

По умолчанию диском С: в Wine является каталог `~/.wine/drive_c/`. Для показа скрытых каталогов (по умолчанию каталог `drive_c` скрыт) в домашнем каталоге необходимо перейти в него и нажать сочетание клавиш **Ctrl + H**.

Для завершения установки необходимо нажать кнопку «Далее» и в открывшемся окне подтвердить завершение установки нажатием кнопки «Готово».

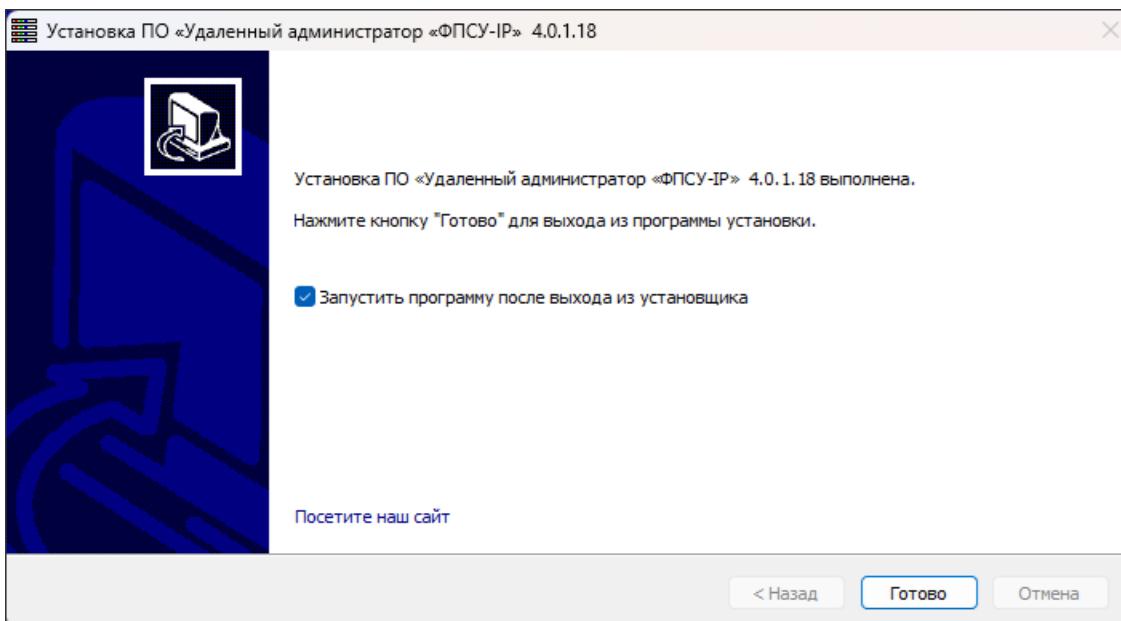


Рисунок 15 - Завершение установки

Перед дальнейшей эксплуатацией программы следует произвести начальные настройки УА ФПСУ-IP во время первого запуска, и зарегистрировать в УА ФПСУ-IP, которые требуется удаленно отслеживать и управлять.

Детальное рассмотрение первого запуска УА ФПСУ-IP находится в разделе «Начало работы с УА ФПСУ-IP».

Детальное рассмотрение интерфейса находится в разделе «Интерфейс УА ФПСУ-IP».

5. 2. Удаление УА ФПСУ-IP, установленного под WINE

Для удаления программного обеспечения УА ФПСУ-IP из операционной системы следует использовать мастера удаления приложения. Запуск мастера удаления приложения осуществляется при помощи файла UNINST.EXE, находящегося в каталоге `~/.wine`. Работа мастера начинается с запроса подтверждения на выполнение операции:

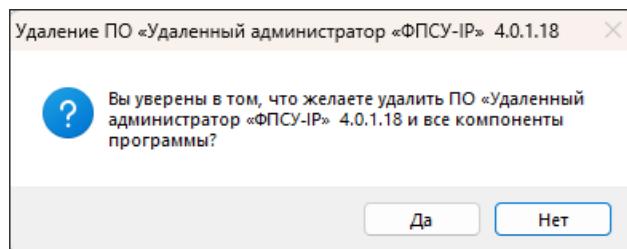


Рисунок 16 - Подтверждение удаления УА ФПСУ-IP

Успешное завершение удаления с компьютера программного обеспечения УА ФПСУ-IP будет подтверждено служебным сообщением о том, что удаление программы было успешно завершено.

Мастер удаления УА ФПСУ-IP после завершения работы оставляет в рабочем каталоге программы созданные пользователем файлы. Для полного удаления УА ФПСУ-IP с компьютера следует удалить объекты, находящиеся в рабочем каталоге УА ФПСУ-IP и его подкаталогах.

6. Лицензирование

Учетная лицензия для УА ФПСУ-IP является файлом, содержащим в себе регистрационный номер. Файл лицензии передается пользователю на носителе с дистрибутивом. После установки ПО файл учетной лицензии (RADM_XXX_YYY_N.NN.lic, где RADM - указатель учетной лицензии, XXX - префикс регистрационного номера, YYY - учетный номер экземпляра УА, N.NN - номер версии УА ФПСУ-IP) необходимо перенести в подкаталог «LIC» рабочего каталога программы УА ФПСУ-IP. В дальнейшем информацию о лицензиях можно просмотреть в сведениях «О программе» («?» → «О программе»).



Рисунок 17 - Информация о программе

Полную информацию о лицензиях можно просмотреть в окне «Управление лицензиями», открывающемся по нажатию кнопки «Управление лицензиями...» в окне «О программе» (см. рисунок выше) или при выборе пункта меню «?» → «Управление лицензиями» (см. п. «Управление лицензиями»). Кроме того, в этом окне так же предоставляется возможность добавить или удалить лицензию.

При старте УА ФПСУ-IP проверяет дату окончания поддержки и за 30 дней сообщает о ее истечении.

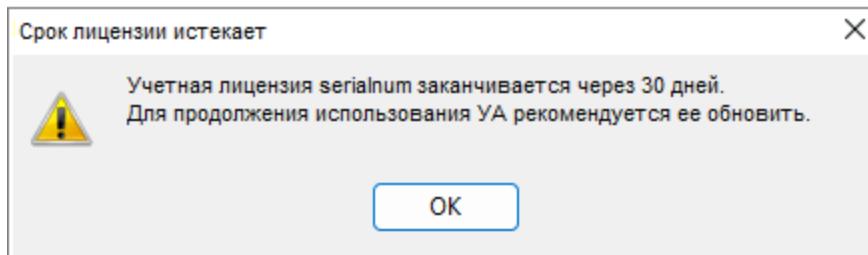


Рисунок 18 - Сообщение об окончании срока учетной лицензии через 30 дней

По окончании срока поддержки будет выдано сообщение о запрете ее использования.

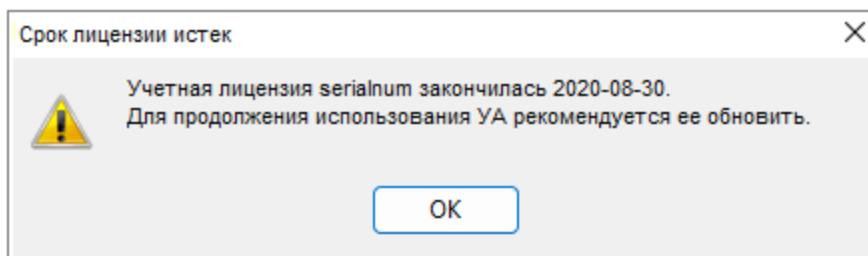


Рисунок 19 - Сообщение о том, что срок действия лицензии истек

При этом дата окончания учетной лицензии отсчитывается от даты сборки. Для продления срока поддержки необходимо разместить файл лицензии на продление поддержки в подкаталоге «LIC» рабочего каталога программы УА ФПСУ-IP. Файл лицензии на продление поддержки необходим для установки обновлений программы в течение указанного в файле лицензии срока.

Для получения файла лицензии можно воспользоваться контекстным меню окна «Управление лицензиями» (см. раздел «Управление лицензиями»).

В случае отсутствия лицензии УА ФПСУ-IP выдаст следующие сообщения:

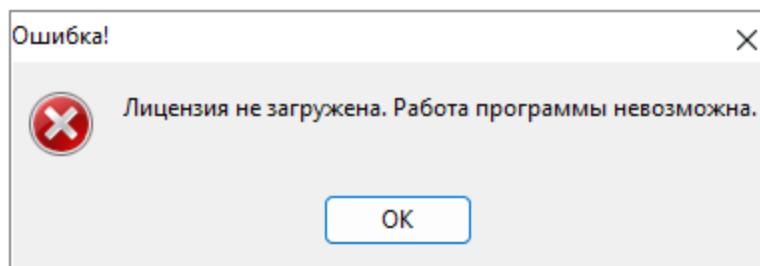


Рисунок 20 - Сообщение об отсутствии загруженной лицензии

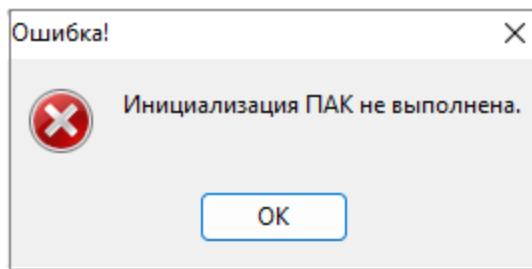


Рисунок 21 - Сообщение об отсутствии инициализации

Учетная лицензия обязательна для запуска УА ввиду привязки к ней Лицензии-расширения на количество зарегистрированных в УА ФПСУ-IP (файл FCNT_XXX_YYY_N.NN.lic, где FCNT - отметка лицензии-расширения на количество зарегистрированных в УА ФПСУ-IP с ключом, XXX - префикс регистрационного номера, YYY - учетный номер экземпляра УА, N.NN - номер версии УА ФПСУ-IP). В базовой комплектации лицензия рассчитана на 5 ФПСУ-IP. В случае наличия лицензии на меньшее количество соединений, при запуске УА ФПСУ-IP на экран будет выведено сообщение об этом:

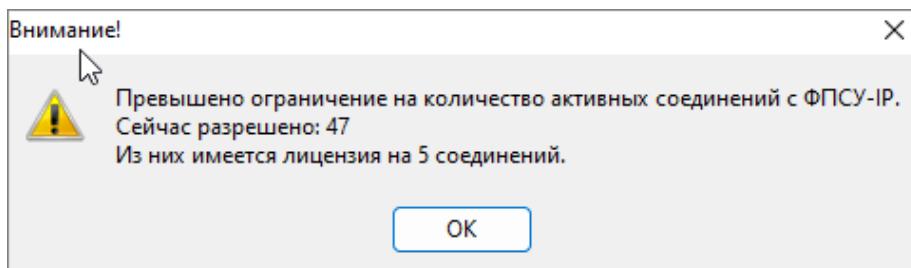


Рисунок 22 - Сообщение о превышении ограничения на количество активных соединений

По нажатию кнопки «OK» на экран будет выведено окно со списком всех зарегистрированных ФПСУ-IP с возможностью удаления лишних ФПСУ-IP. В том случае, если все разрешенные ФПСУ-IP будут оставлены в списке, УА произведет соединение с первыми ФПСУ-IP из этого списка (соответствующими по количеству лицензии-расширению). В дальнейшем соединение будет производиться с этими же, выбранными при первом соединении, ФПСУ-IP.

Кроме того, к учетной лицензии привязываются Лицензия на сетевую Базу Данных УА (файл EDB_XXX_YYY_N.NN.lic, где EDB - отметка лицензии-расширения на сетевую базу данных, XXX - префикс регистрационного номера, YYY - учетный номер экземпляра УА, N.NN - номер версии УА ФПСУ-IP; см. п. «Работа с внешними базами данных»).

Все лицензии должны располагаться в подкаталоге «LIC» рабочего каталога программы УА ФПСУ-IP.

7. Начало работы с УА ФПСУ-IP

ВНИМАНИЕ! Для запуска УА ФПСУ-IP потребуются права локального администратора операционной системы. Для первого запуска с УА ФПСУ-IP необходимо наличие установленного на рабочую станцию программного обеспечения, УА ФПСУ-IP учетной лицензии УА ФПСУ-IP и программы WINFPSUHASH.EXE. Программа WINFPSUHASH.EXE копируется в рабочий каталог УА ФПСУ-IP во время установки УА ФПСУ-IP.

При запуске УА ФПСУ-IP с использованием VPN-Key/UA необходим так же файл лицензии на использование VPN-Key/UA. В дальнейшем для работы с УА ФПСУ-IP необходимо наличие установленного на рабочую станцию программного обеспечения, учетной лицензии (с привязанными к ней лицензиями на количество зарегистрированных в УА ФПСУ-IP с ключом и на сетевую Базу Данных УА) и ключа УА.

Перед началом работы необходимо выполнить контроль целостности (см. пункт «Первоначальный контроль целостности после инсталляции»).

Учетная лицензия для УА ФПСУ-IP является файлом, содержащим в себе регистрационный номер. Файл лицензии передается пользователю на носителе с дистрибутивом.

Так же при установлении соединения между ФПСУ-IP и УА ФПСУ-IP используется ключевая пара УА (состоящая из открытого и секретного ключа удаленного администратора). Эти уникальные для каждого администратора УА ФПСУ-IP данные хранятся в VPN-Key/UA.

Без учетной лицензии и ключа УА запуск УА ФПСУ-IP и управление ФПСУ-IP невозможны, а интерфейс УА ФПСУ-IP становится недоступен пользователю.

7. 1. Подключение VPN-Key/UA

VPN-Key/UA имеет две учетные записи с PIN-кодами доступа - «Пользователь», имеющий непривилегированные права на эксплуатацию VPN-Key/UA, и «Администратор», который может инициализировать VPN-Key/UA и менять настройки его системных данных.

Пароли учетных записей «Пользователь» и «Администратор» по умолчанию установлены в значения «1111» или «111111». После проведения этапа первоначальной настройки (см. разделы «Первый запуск УА ФПСУ-IP с VPN/Key UA» и «Первоначальная настройка УА ФПСУ-IP (с VPN-Key/UA)») УА ФПСУ-IP потребует сменить предустановленные пароли VPN-Key/UA (см. пункт «Управление паролями»).

Если это первое подключение VPN-Key/UA к данному компьютеру, то операционная система выполнит поиск драйвера для подключенного устройства. Драйверы VPN-Key/UA устанавливаются в операционную систему вместе с УА ФПСУ-IP, поэтому поиск драйверов и распознавание устройства происходит в большинстве случаев автоматически без участия пользователя.

Для проверки установленных драйверов (пример для Windows 11) необходимо вставить в USB-порт один из VPN-Key/UA и открыть «Диспетчер устройств».

В списке установленных устройств следует найти объект «Устройство чтения смарт-карт».

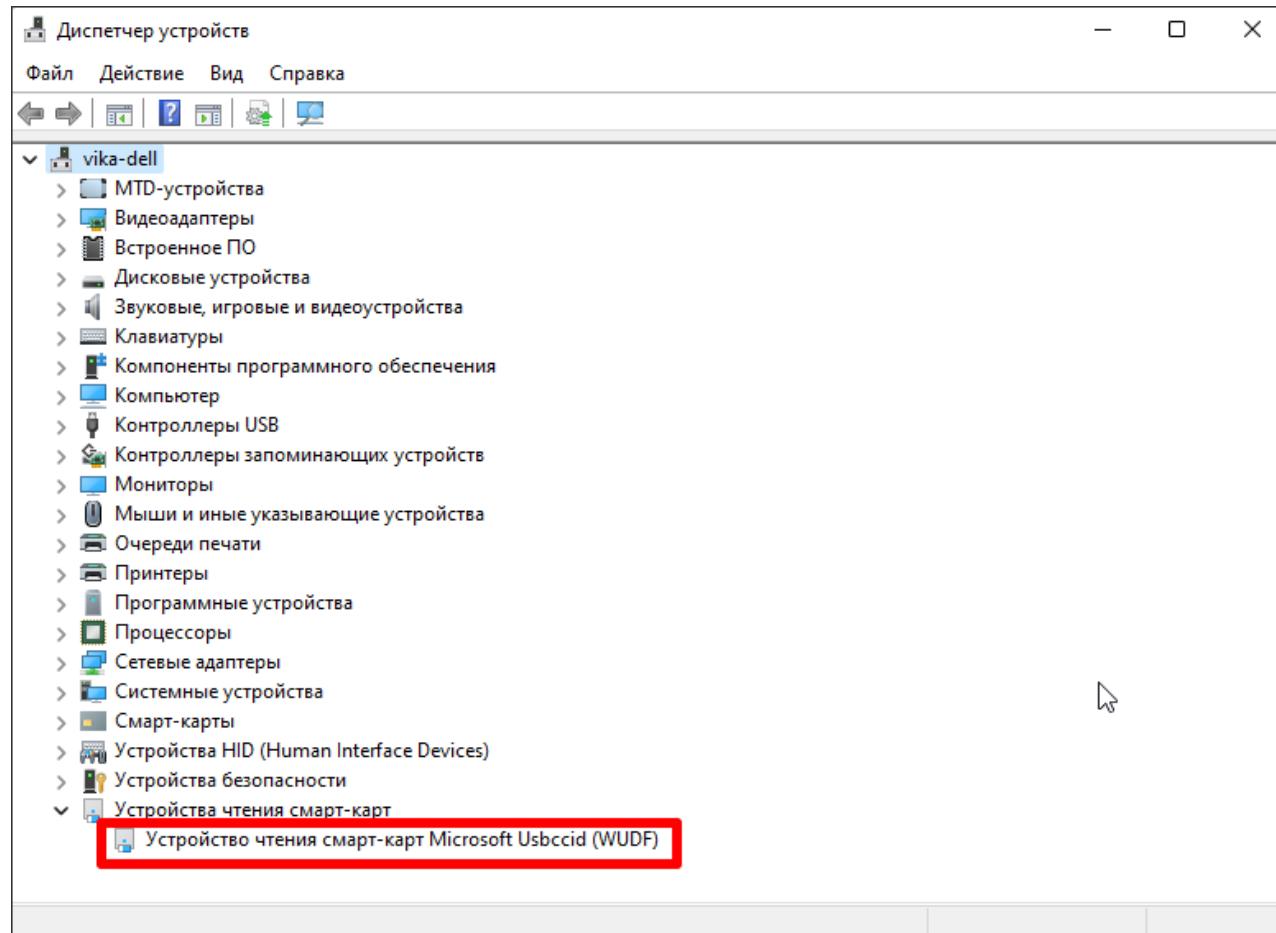


Рисунок 1 - Драйвер VPN-Key/UA обнаружен корректно

Если операционная система выдаёт сообщение о том, что обнаруженное новое устройство не опознано, следует установить его драйвер с инсталляционного носителя вручную.

7. 2. Первый запуск УА ФПСУ-IP с VPN/Key UA

После установки запуск программного обеспечения осуществляется:

- выполнением команды Пуск > АМИКОН > Администратор ФПСУ-IP;
- запуском файла wradm.exe, находящегося в рабочем каталоге программы.

Первый запуск ПО сопровождается выводом на экран окна с лицензионным соглашением. В случае несогласия следует нажать кнопку «Не принимаю» для прекращения работы. Для продолжения работы необходимо нажать кнопку «Принимаю данное соглашение».

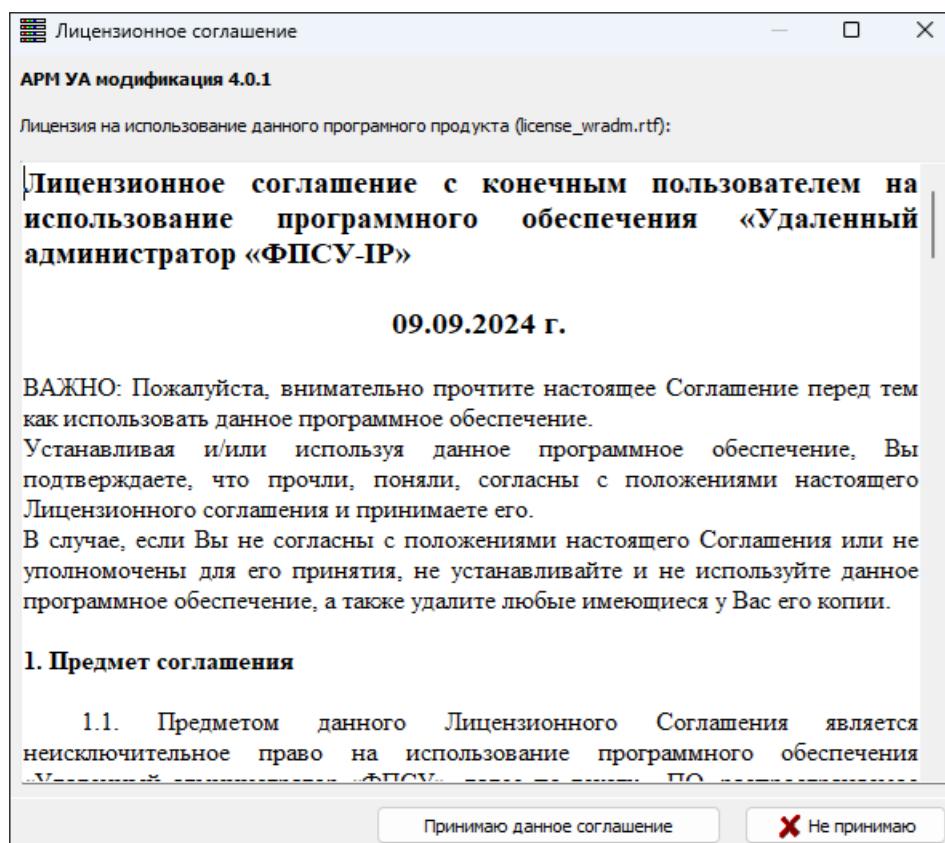


Рисунок 2 - Лицензионное соглашение

Для корректной работы требуется наличие файлов учетной лицензии и лицензии на использование подключенного к USB порту компьютера VPN-Key/UA.

Все файлы лицензии имеют формат *.lic. В файле учетной лицензии содержится регистрационный номер, дата окончания срока действия лицензии и информация об организации, для которой была выдана лицензия (см. «Лицензирование»). Файлы лицензии должны храниться в подкаталоге LIC рабочего каталога УА ФПСУ-IP. Файлы в каталог «LIC» могут быть скопированы или добавлены с использованием окна «Управление лицензиями».

Файлу лицензии на использование VPN-Key/UA соответствует единственный VPN-Key/UA. При запуске УА ФПСУ-IP происходит обращение к подкаталогу лицензий. Если файлов учетной лицензии не обнаружено, будет выдано служебное сообщение.

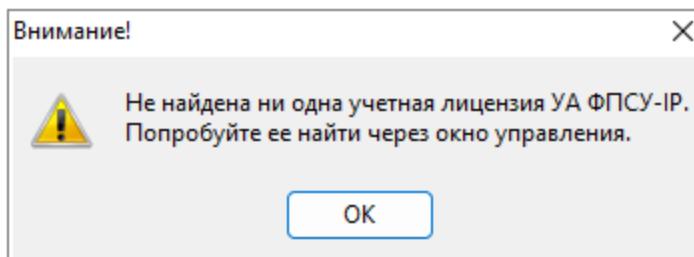


Рисунок 3 - Лицензия на VPN-Key/UA не обнаружена

После нажатия кнопки «OK» откроется окно управления лицензиями на УА ФПСУ-IP:

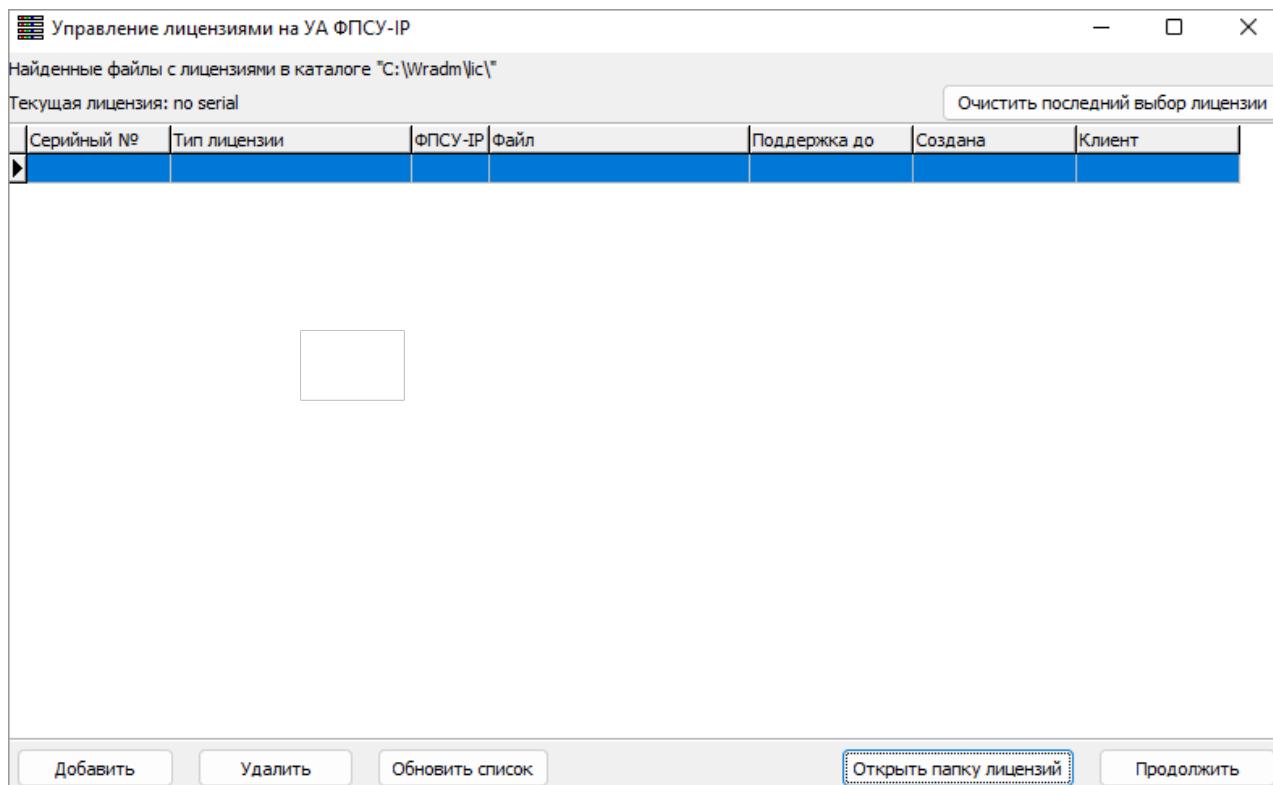


Рисунок 4 - Окно управления лицензиями на УА ФПСУ-IP

В открывшемся окне предоставляется возможность добавить или удалить лицензию по нажатию соответствующей кнопки. Кроме того можно обновить список лицензий или открыть каталог «LIC» для работы непосредственно в нем.

Для продолжения работы с УА ФПСУ-IP требуется подключить к USB-порту компьютера соответствующий имеющемуся файлу лицензии на использования VPN-Key/UA.

При отсутствии в каталоге «LIC» файла учетной лицензии или соответствующего VPN-Key файла лицензии на его использование, программное обеспечение выдаст сообщение об этом.

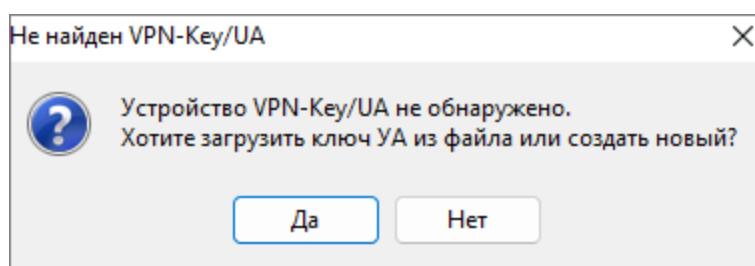


Рисунок 5 - Сообщение об отсутствии VPN_Key/UA

В случае обнаружения файлов учетной лицензии и лицензии на использование подключенного VPN-Key/UA, УА ФПСУ-IP предложит ввести PIN-код учетной записи пользователя VPN-Key/UA, входящий в комплект поставки.

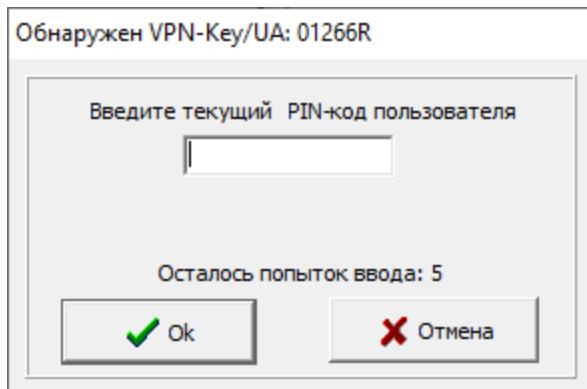


Рисунок 6 - Ввод PIN-кода VPN-Key/UA

В заголовке окна ввода PIN-кода отображается серийный номер подключенного VPN-Key/UA.

Если это первое использование VPN-Key/UA, то, в случае корректного ввода PIN-кода, программа не обнаружит записанных в устройство ключевых данных, и выдаст служебное сообщение:

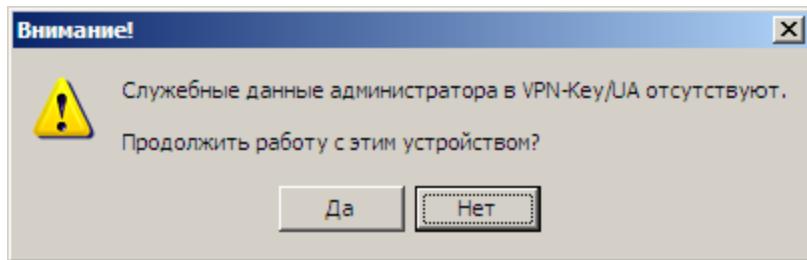


Рисунок 7 - VPN-Key/UA не инициализирован

Для перехода к процедуре первоначальной настройки VPN-Key/UA необходимо нажать кнопку «Да».

7. 3. Первый запуск УА ФПСУ-IP без VPN-Key/UA

После установки запуск программного обеспечения осуществляется:

- выполнением команды Пуск > АМИКОН > Администратор ФПСУ-IP;
- запуском файла wradm.exe, находящегося в рабочем каталоге.

Первый запуск ПО сопровождается выводом на экран окна с лицензионным соглашением. В случае несогласия следует нажать кнопку «Не принимаю» для прекращения работы. Для продолжения работы необходимо нажать кнопку «Принимаю данное соглашение».

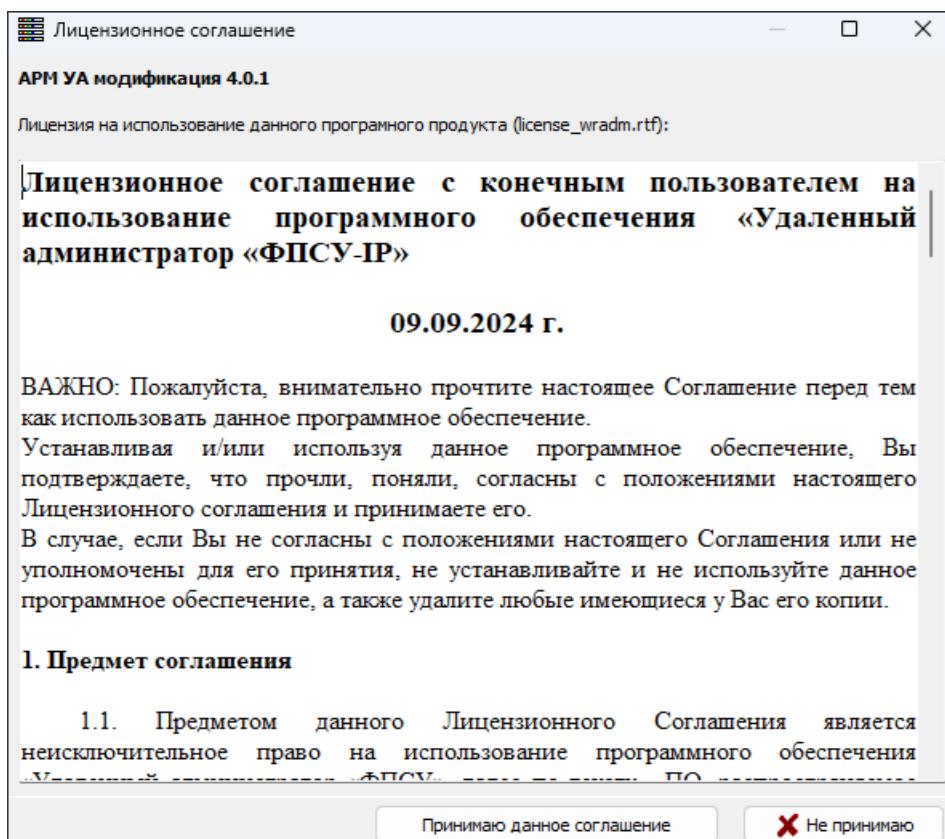
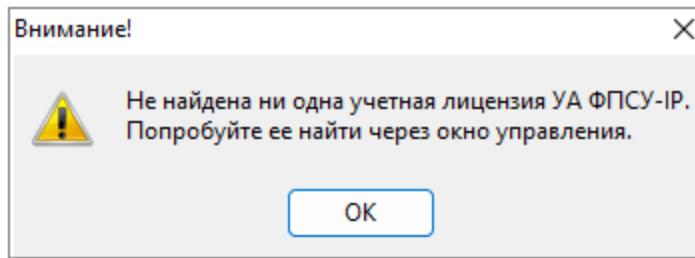


Рисунок 8 - Лицензионное соглашение

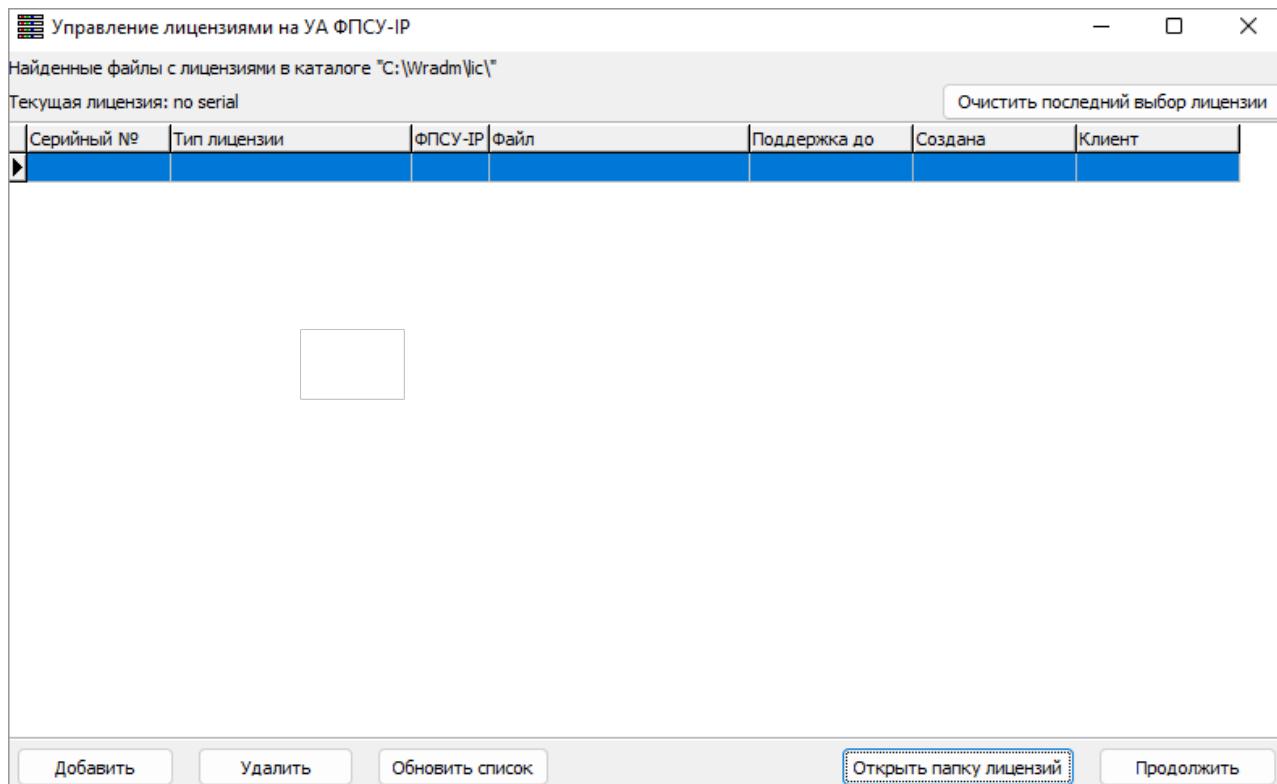
Для корректной работы требуется наличие файла учетной лицензии.

Файлы лицензии имеют формат *.lic. В файле учетной лицензии содержится серийный номер VPN-Key/UA, дата окончания срока действия лицензии и информация об организации, для которой была выдана лицензия (см. «Лицензирование»). Файлы лицензий должны храниться в подкаталоге LIC рабочего каталога УА ФПСУ-IP.

При запуске УА ФПСУ-IP происходит обращение к подкаталогу лицензий. Если файл учетной лицензии не обнаружен, будет выдано служебное сообщение.

**Рисунок 9 - Лицензия на VPN-Key/UA не обнаружена**

После нажатия кнопки «OK» откроется окно управления лицензиями на УА ФПСУ-IP:

**Рисунок 10 - окно управления лицензиями на УА ФПСУ-IP**

В открывшемся окне предоставляется возможность добавить или удалить лицензию по нажатию соответствующей кнопки. Кроме того, можно обновить список лицензий или открыть каталог «Lic» для работы непосредственно в нем.

По нажатию кнопки «Продолжить», программное обеспечение выдаст следующий запрос:

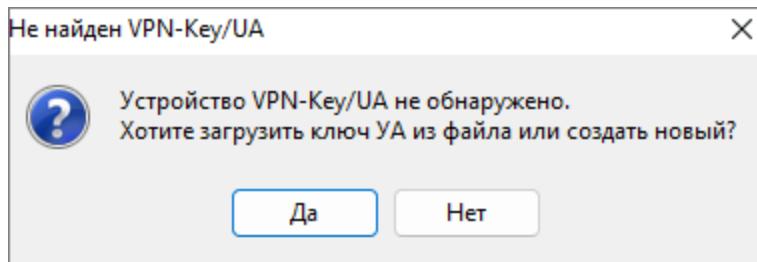


Рисунок 11 - Сообщение об отсутствии VPN_Key/UA

Для перехода к процедуре первоначальной настройки необходимо нажать кнопку «Да».

7. 4. Первоначальная настройка УА ФПСУ-IP (с VPN-Key/UA)

К первоначальной настройке УА ФПСУ-IP относится установка параметров администратора УА ФПСУ-IP и VPN-Key/UA. Пользователем выбираются параметры администратора УА ФПСУ-IP, и записываются в подключенный VPN-Key/UA (происходит инициализация VPN-Key/UA).

К параметрам администратора относятся уникальное имя из шести символов, под которым он будет регистрироваться на ФПСУ-IP, произвольный комментарий к имени и несколько рабочих опций.

Работа УА ФПСУ-IP будет блокирована до тех пор, пока не будут установлены параметры администратора УА ФПСУ-IP, которые необходимы для выработки его персональных ключевых данных, используемых при взаимной регистрации с ФПСУ-IP, шифровании локальной базы данных УА ФПСУ-IP, а также для идентификации и аутентификации передаваемой между УА ФПСУ-IP и ФПСУ-IP информации.

После введения PIN-кода VPN-Key/UA и подтверждения работы именно с этим VPN-Key/UA (см. «Первый запуск УА ФПСУ-IP с VPN/Key UA»), УА ФПСУ-IP отобразит диалоговое окно указания параметров профиля администратора.

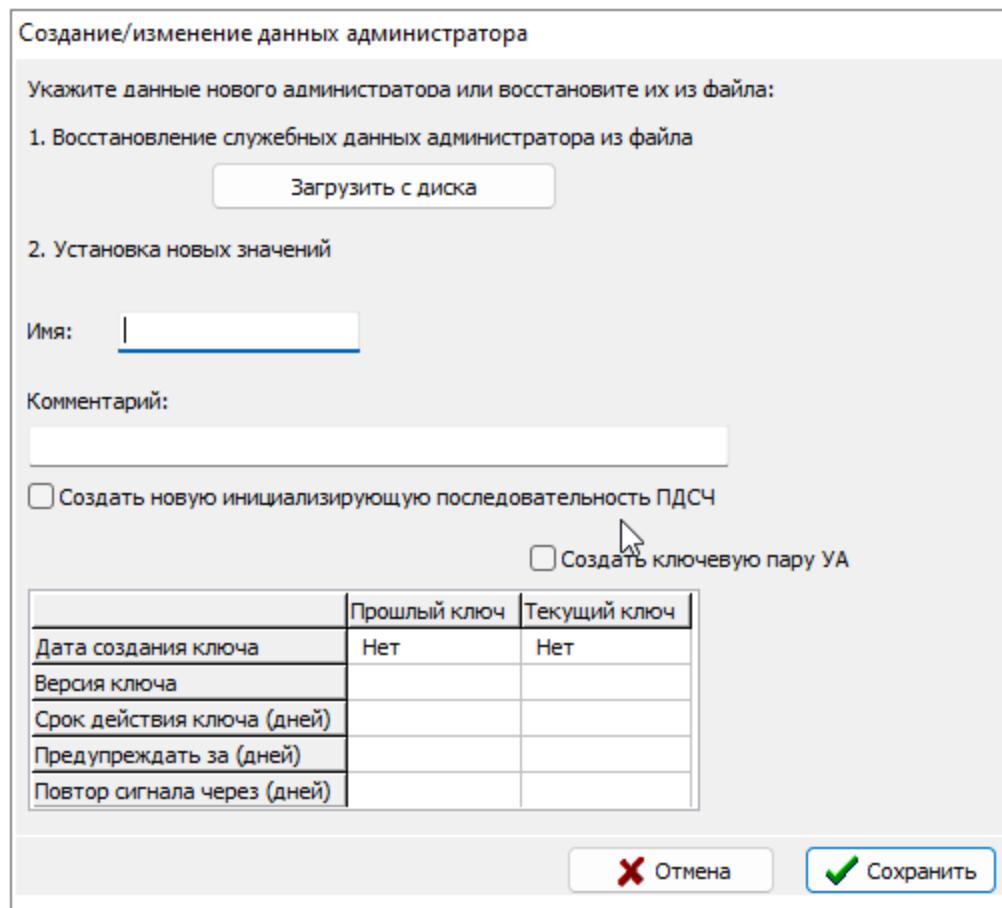


Рисунок 12 - Установка параметров администратора

Кнопка «Загрузить с диска» относится к восстановлению штатной работы УА ФПСУ-IP из резервной копии, и при первом запуске не используется. Подробнее о восстановлении работы УА ФПСУ-IP см. раздел «Резервирование и восстановление работы УА ФПСУ-IP».

Для продолжения работы следует ввести параметры администратора УА ФПСУ-IP:

- Имя — уникальный идентификатор администратора УА ФПСУ-IP, 6 символов на английской раскладке клавиатуры;
- Комментарий — произвольный текст, не превышающий 43 символов.

После ввода корректных имени и комментария, необходимо нажать кнопку «Сохранить». УА ФПСУ-IP начнет процедуру записи введенных параметров в подключенный VPN-Key/UA.

Для генерации ключевых данных создаваемого администратора потребуется сначала выполнить инициализацию датчика случайных чисел, о чём будет выдано служебное оповещение:

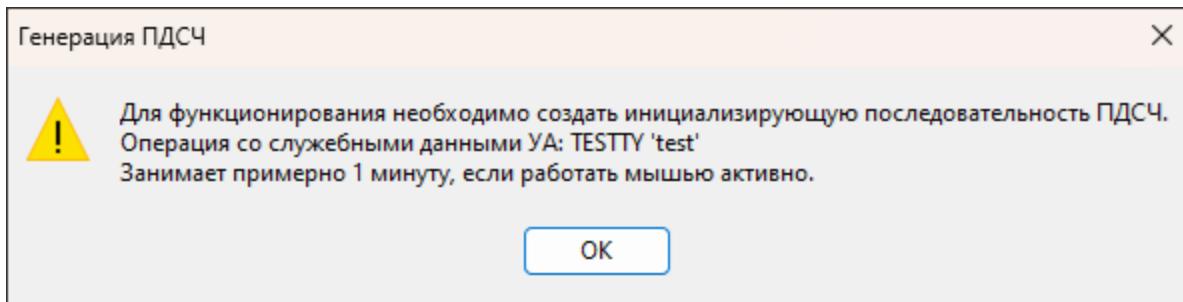


Рисунок 13 - Требуется инициализация датчика случайных чисел

Для продолжения следует нажать кнопку «OK». В появившемся окне создания инициализирующей последовательности для программного датчика случайных чисел от администратора УА ФПСУ-IP потребуется перемещать указатель мыши без нажатия на клавиши в пределах окна.

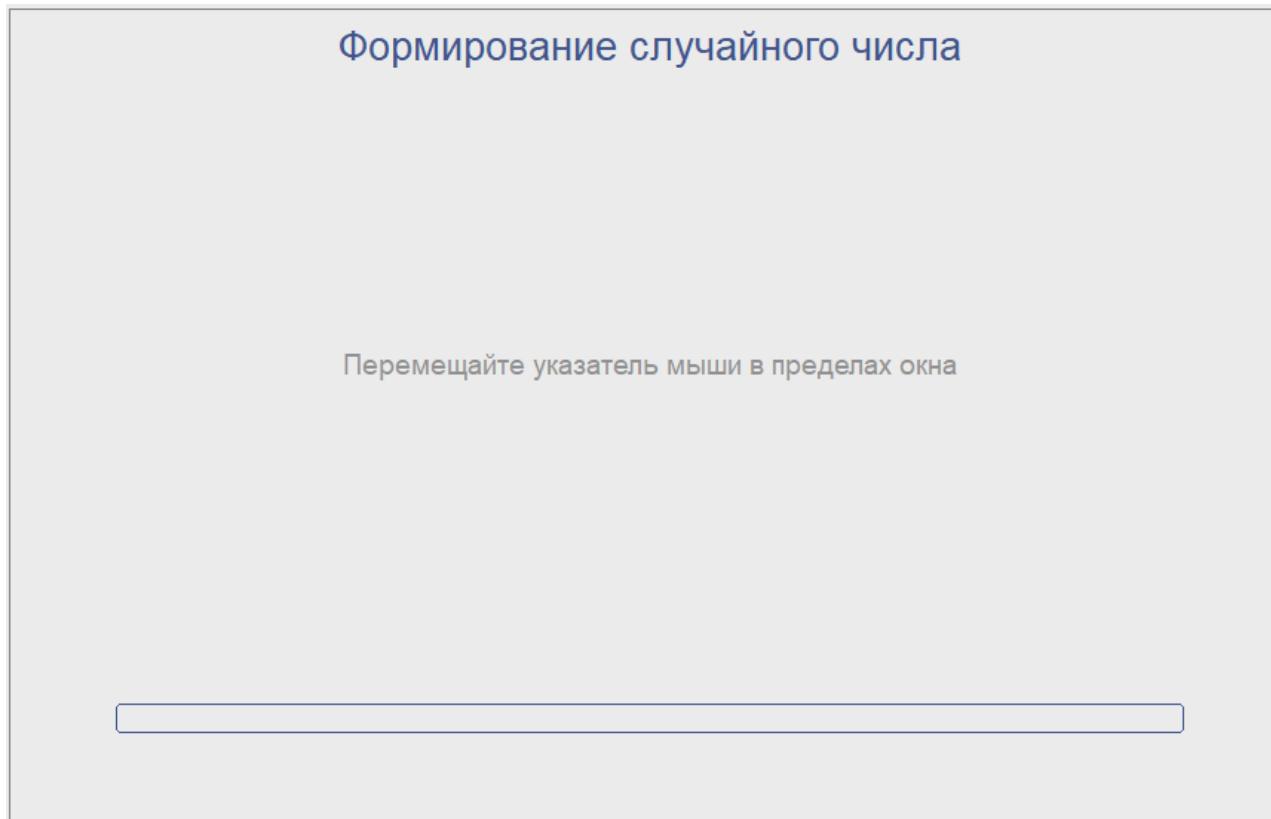


Рисунок 14 - Инициализация ПДСЧ

После заполнения строки состояния расположенной под текстом, датчик случайных чисел будет инициализирован и готов к созданию и записи ключевых данных администратора в VPN-Key/UA.

После проверки того, что к компьютеру подключен единственный VPN-Key/UA, следует нажать кнопку «Да» в появившемся служебном окне:

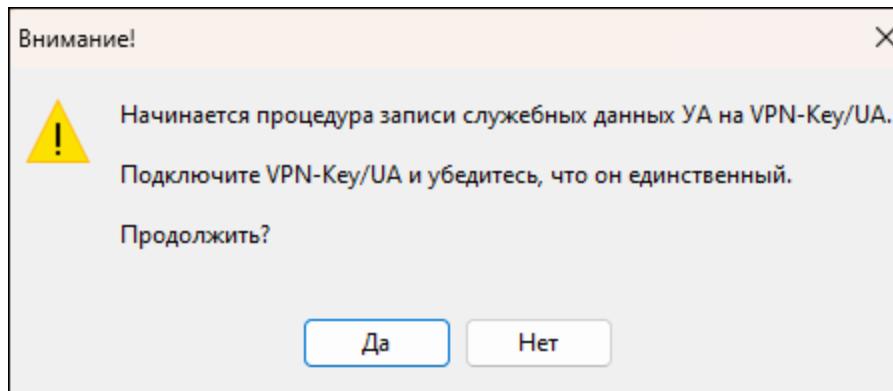


Рисунок 15 - Проверка количества подключенных к компьютеру VPN-Key/UA

Для продолжения потребуется предъявить права администратора VPN-Key/UA (PIN-код администратора VPN-Key/UA).

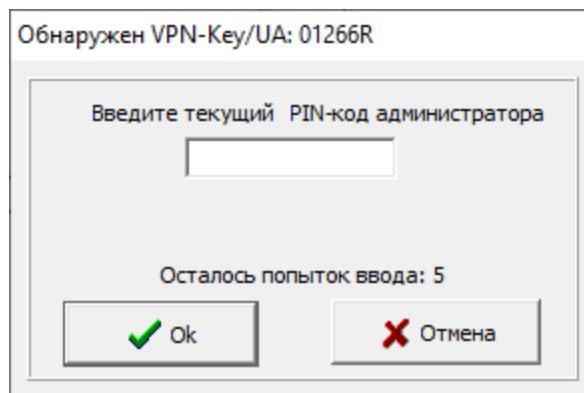


Рисунок 16 - Ввод PIN-код администратора VPN-Key/UA

После ввода PIN-кода администратора VPN-Key/UA, ключевые данные создаваемого администратора начнут записываться в VPN-Key/UA. В случае успешного завершения выдается системное оповещение:

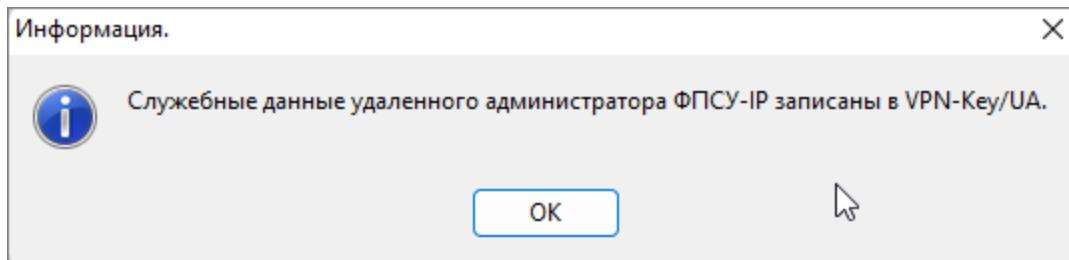


Рисунок 17 - Сообщение о записи данных администратора в VPN-Key/UA

Следующим этапом потребуется создать ключ, на котором будет зашифрована база данных УА ФПСУ-IP. После нажатия кнопки «OK» в предыдущем окне появится системное оповещение о необходимости создать ключ шифрования базы данных УА ФПСУ-IP:

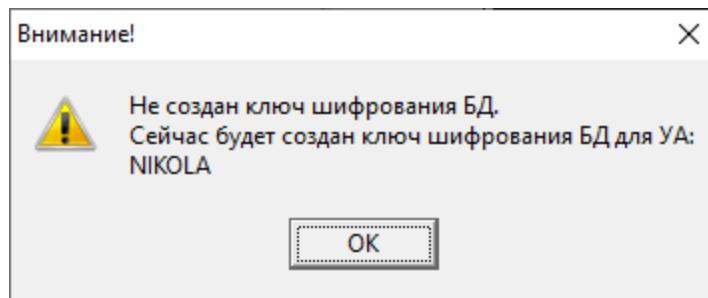
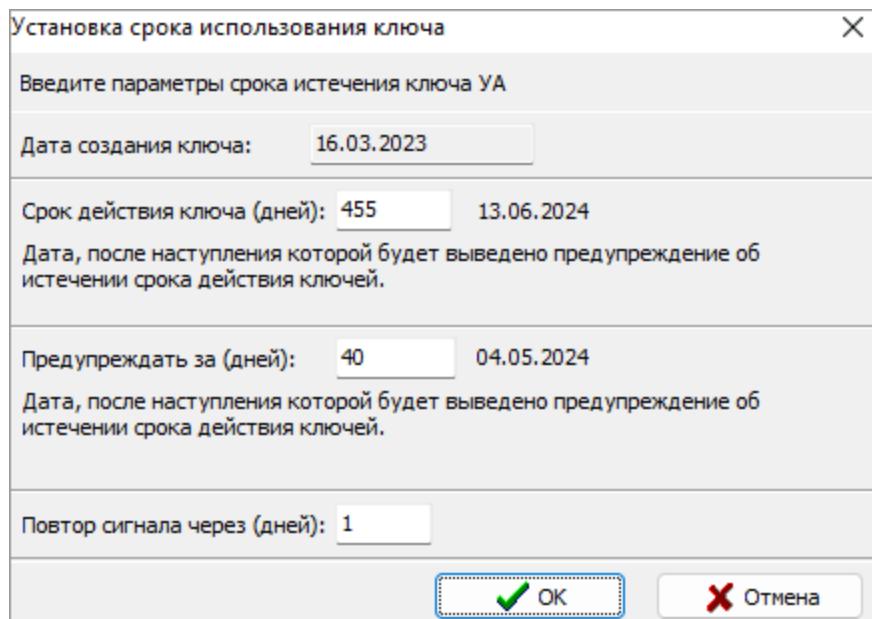


Рисунок 18 - Не создан ключ шифрования базы данных УА ФПСУ-IP

По нажатию кнопки «OK» откроется системное окно для установки параметров ключа шифрования базы данных УА ФПСУ-IP:

**Рисунок 19 - Установка срока использования ключа**

После установки сроков использования ключа шифрования базы данных УА ФПСУ-IP и нажатия кнопки «OK» этап первоначальной настройки закончен. УА ФПСУ-IP готова к выполнению своих основных функций.

При повторных запусках УА ФПСУ-IP будет требовать:

- наличие подключенного VPN-Key/UA, в который были записаны служебные данные созданного администратора УА ФПСУ-IP;
- наличие в подкаталоге LIC основного каталога УА ФПСУ-IP файлов учетной лицензии и лицензии на использование VPN-Key/UA, соответствующей подключенному VPN-Key/UA;
- ввода PIN-кода пользователя VPN-Key/UA;
- (опционально) ввода символьного пароля (см. пункт «Главное меню УА ФПСУ-IP»).

7. 5. Первоначальная настройка УА ФПСУ-IP (без VPN-Key/UA)

К первоначальной настройке УА ФПСУ-IP относится установка параметров администратора УА ФПСУ-IP. Пользователем выбираются параметры администратора УА ФПСУ-IP, и записываются в файл с ключом УА.

К параметрам администратора относятся уникальное имя из шести символов, под которым он будет регистрироваться на ФПСУ-IP, произвольный комментарий к имени и

несколько рабочих опций.

Работа УА ФПСУ-IP будет блокирована до тех пор, пока не будут установлены параметры администратора УА ФПСУ-IP, которые необходимы для выработки его персональных ключевых данных, используемых при взаимной регистрации с ФПСУ-IP, шифровании локальной базы данных УА ФПСУ-IP, а также для идентификации и аутентификации передаваемой между УА ФПСУ-IP и ФПСУ-IP информации.

После введения сообщения о том, что VPN_Key/UA не найден (см. «Первый запуск УА ФПСУ-IP без VPN-Key/UA»), УА ФПСУ-IP отобразит диалоговое окно указания параметров профиля администратора.

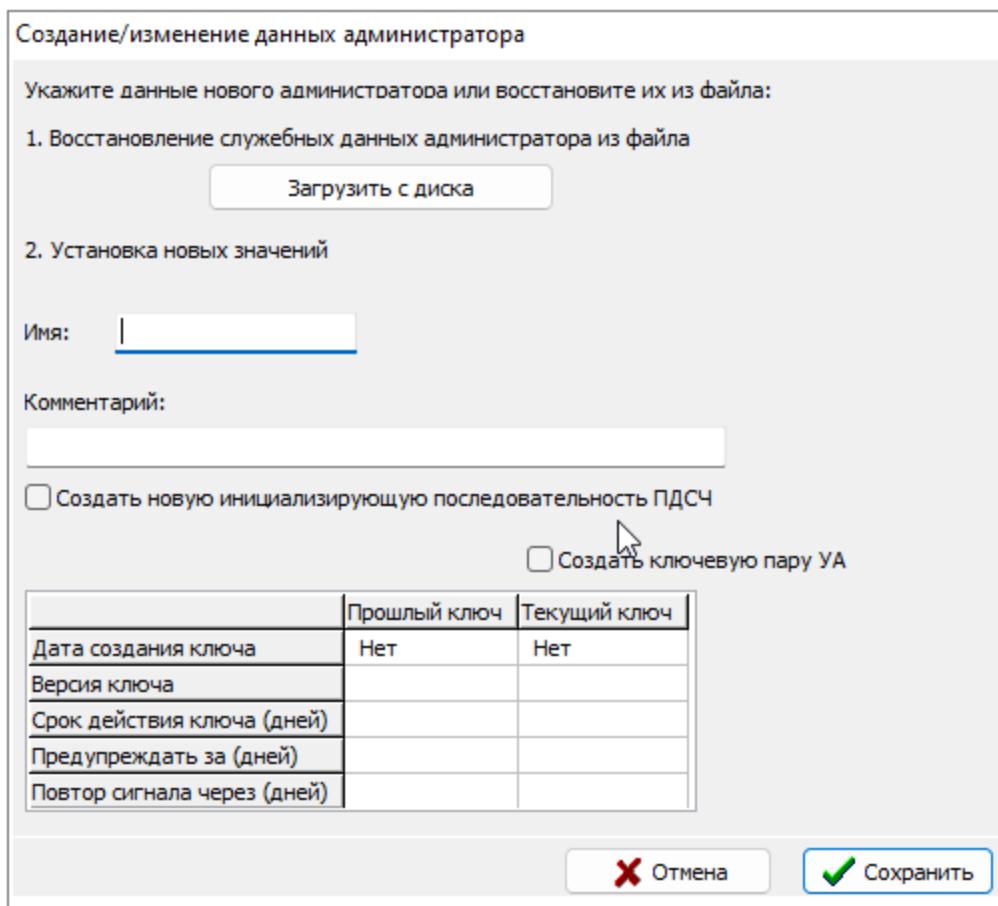


Рисунок 20 - Установка параметров администратора

Кнопка «Загрузить с диска» относится к восстановлению штатной работы УА ФПСУ-IP из резервной копии, и при первом запуске не используется. Подробнее о восстановлении работы УА ФПСУ-IP см. раздел «Резервирование и восстановление работы УА ФПСУ-IP».

Для продолжения работы следует ввести параметры администратора УА ФПСУ-IP:

- Имя — уникальный идентификатор администратора УА ФПСУ-IP, 6 символов на английской раскладке клавиатуры;
- Комментарий — произвольный текст, не превышающий 43 символов.

После ввода корректных имени и комментария, необходимо нажать кнопку «Сохранить». Откроется системное окно для установки параметров ключа шифрования базы данных УА ФПСУ-IP:

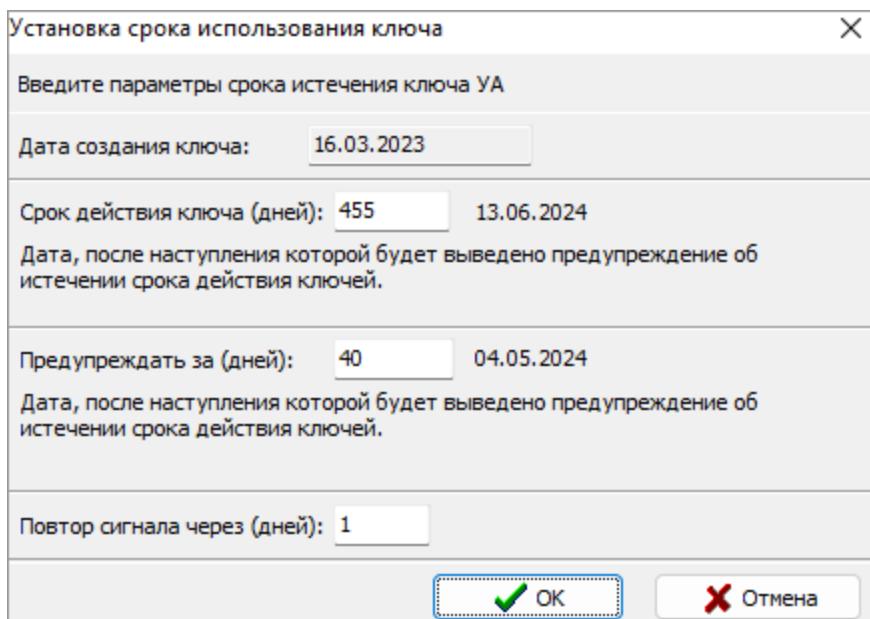


Рисунок 21 - Установка срока использования ключа

После установки сроков использования ключа шифрования базы данных УА ФПСУ-IP и нажатия кнопки «OK» УА ФПСУ-IP выведет следующее предупреждение:

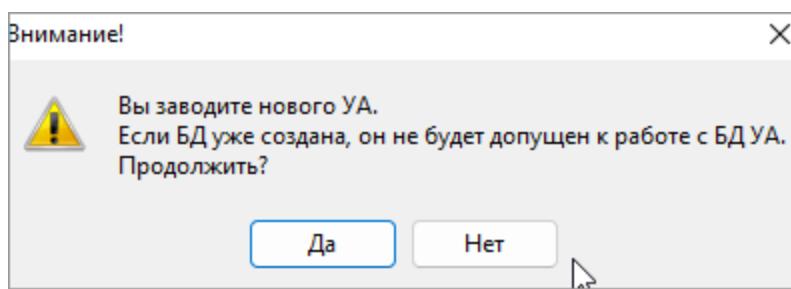


Рисунок 22 - Установка срока использования ключа

После нажатия кнопки «Да» следует указать путь к каталогу, в который будет сохранен новый ключ УА.

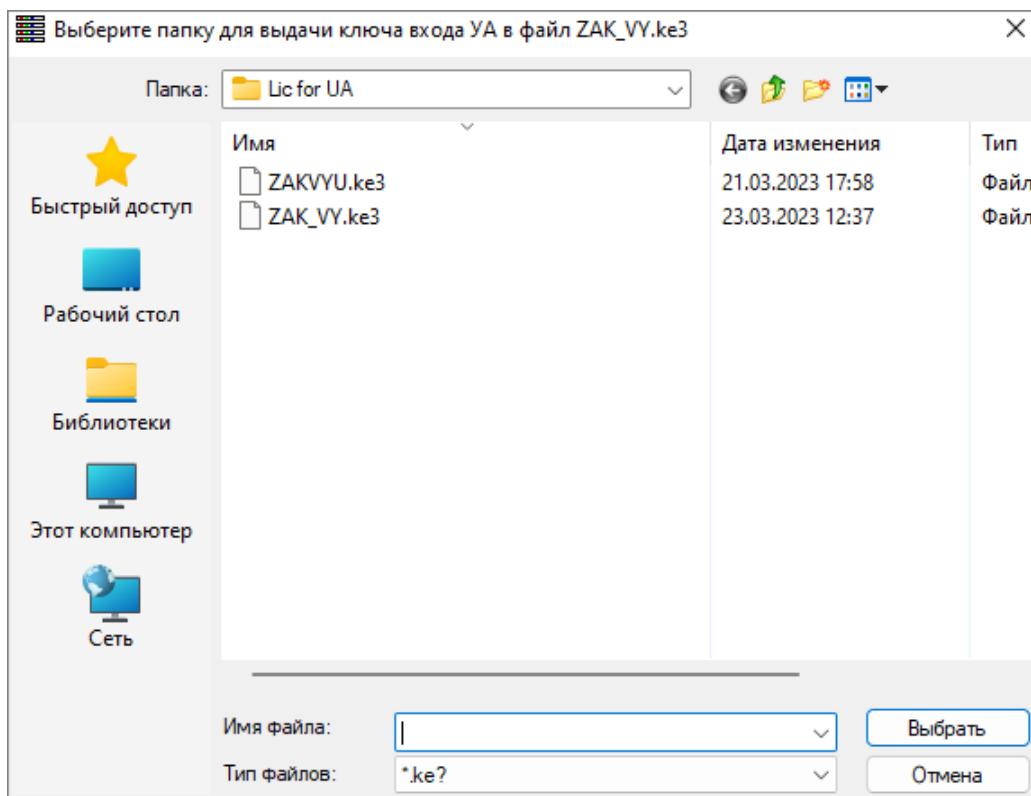


Рисунок 23 - Установка срока использования ключа

УА ФПСУ-IP выведет на экран окно для создания нового пароля:

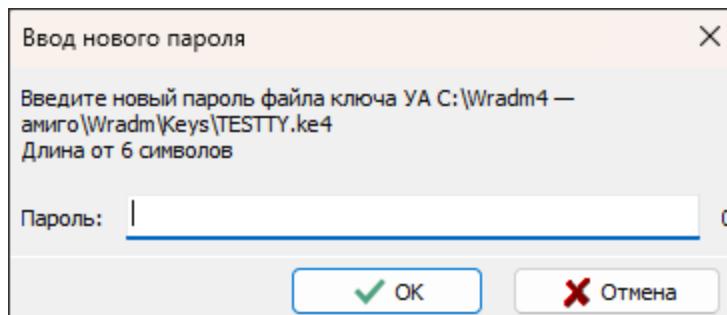


Рисунок 24 - Создание пароля для ключа УА

После ввода пароля необходимо нажать кнопку «OK». Программа потребует ввести пароль повторно для подтверждения.

После подтверждения пароля УА ФПСУ-IP выведет на экран сообщение о выдаче ключа УА в файл:

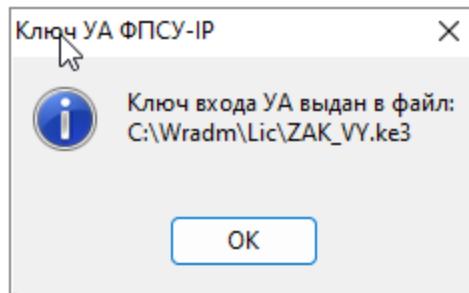
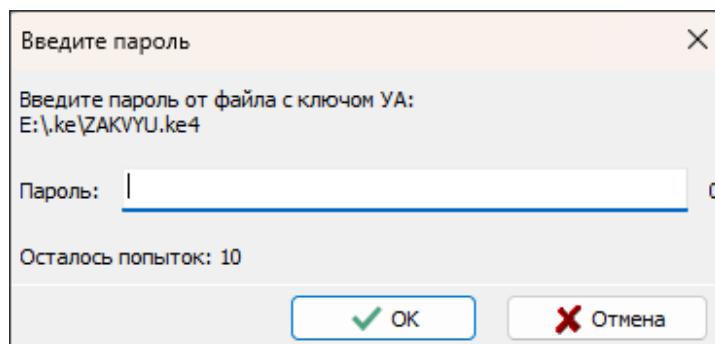


Рисунок 25 - Сообщение о выдаче ключа УА в файл

После выдачи ключа УА ФПСУ-IP предложит ввести пароль от файла с ключом УА:



Для генерации ключевых данных создаваемого администратора потребуется сначала выполнить инициализацию датчика случайных чисел, о чем будет выдано служебное оповещение:

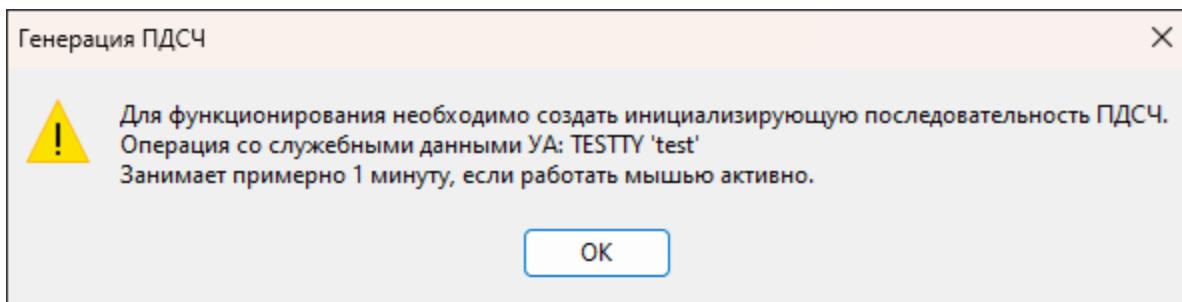


Рисунок 26 - Требуется инициализация датчика случайных чисел

Для продолжения следует нажать кнопку «OK». В появившемся окне создания инициализирующей последовательности для программного датчика случайных чисел от администратора УА ФПСУ-IP потребуется перемещать указатель мыши без нажатия на клавиши в пределах окна.

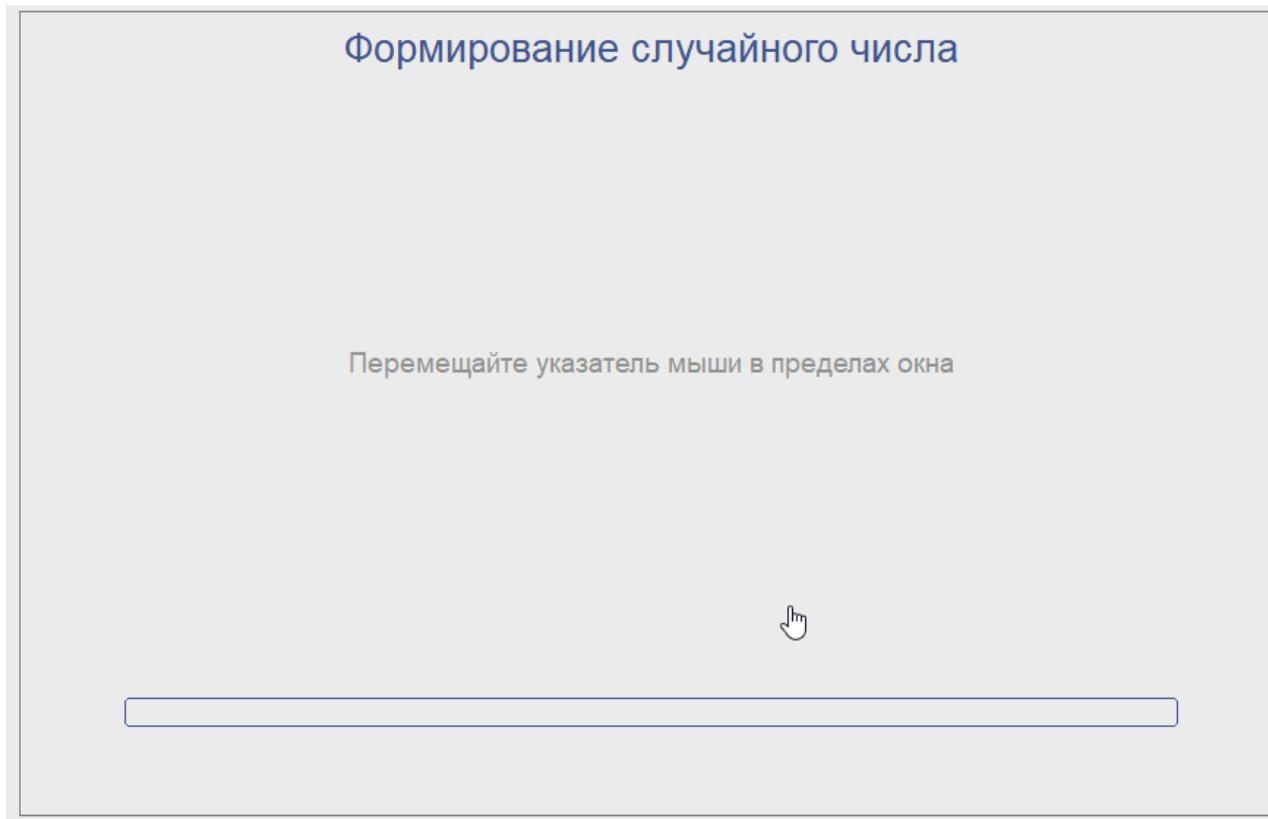


Рисунок 27 - Инициализация ПДСЧ

После заполнения строки состояния, расположенной под текстом, датчик случайных чисел будет инициализирован.

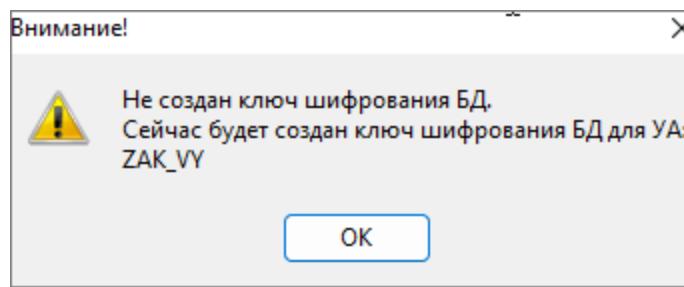


Рисунок 28 - Сообщение о создании ключа шифрования

Повторно откроется системное окно для установки параметров ключа шифрования базы данных УА ФПСУ-IP:

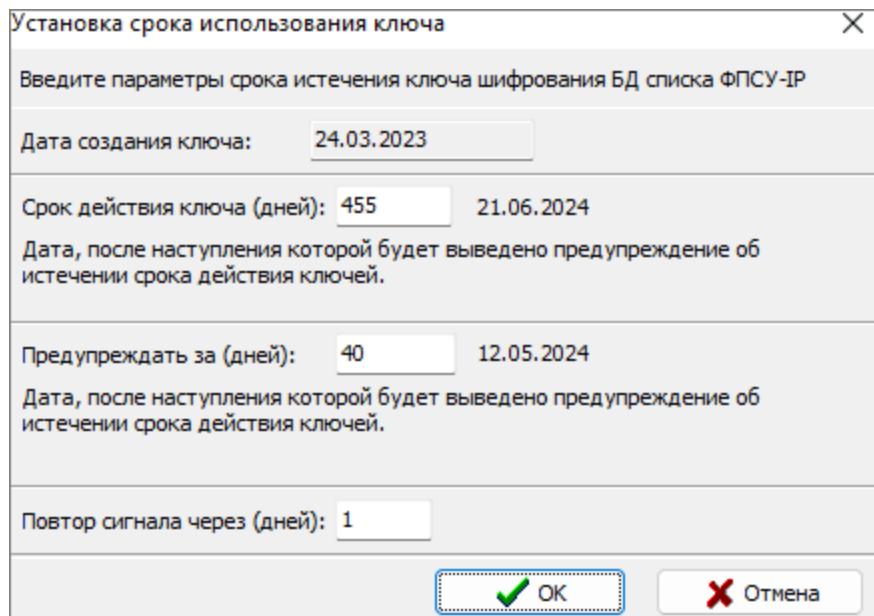


Рисунок 29 - Установка срока использования ключа

После установки сроков использования ключа шифрования базы данных УА ФПСУ-IP и нажатия кнопки «OK» этап первоначальной настройки закончен. УА ФПСУ-IP готова к выполнению своих основных функций.

При повторных запусках УА ФПСУ-IP будет требовать:

- наличие в подкаталоге LIC основного каталога УА ФПСУ-IP, файла учетной лицензии;
- наличие в указанном при создании каталоге ключа УА, в который были записаны служебные данные созданного администратора УА ФПСУ-IP;
- ввода PIN-кода ключа УА;
- (опционально) ввода символьного пароля (см. пункт «Главное меню УА ФПСУ-IP»).

7. 6. Управление лицензиями

Информацию о лицензиях можно просмотреть в окне «Управление лицензиями», открывающемся по нажатию кнопки «Управление лицензиями...» в окне «О программе» («?» → «О программе...») или при выборе пункта меню «?» → «Управление лицензиями».

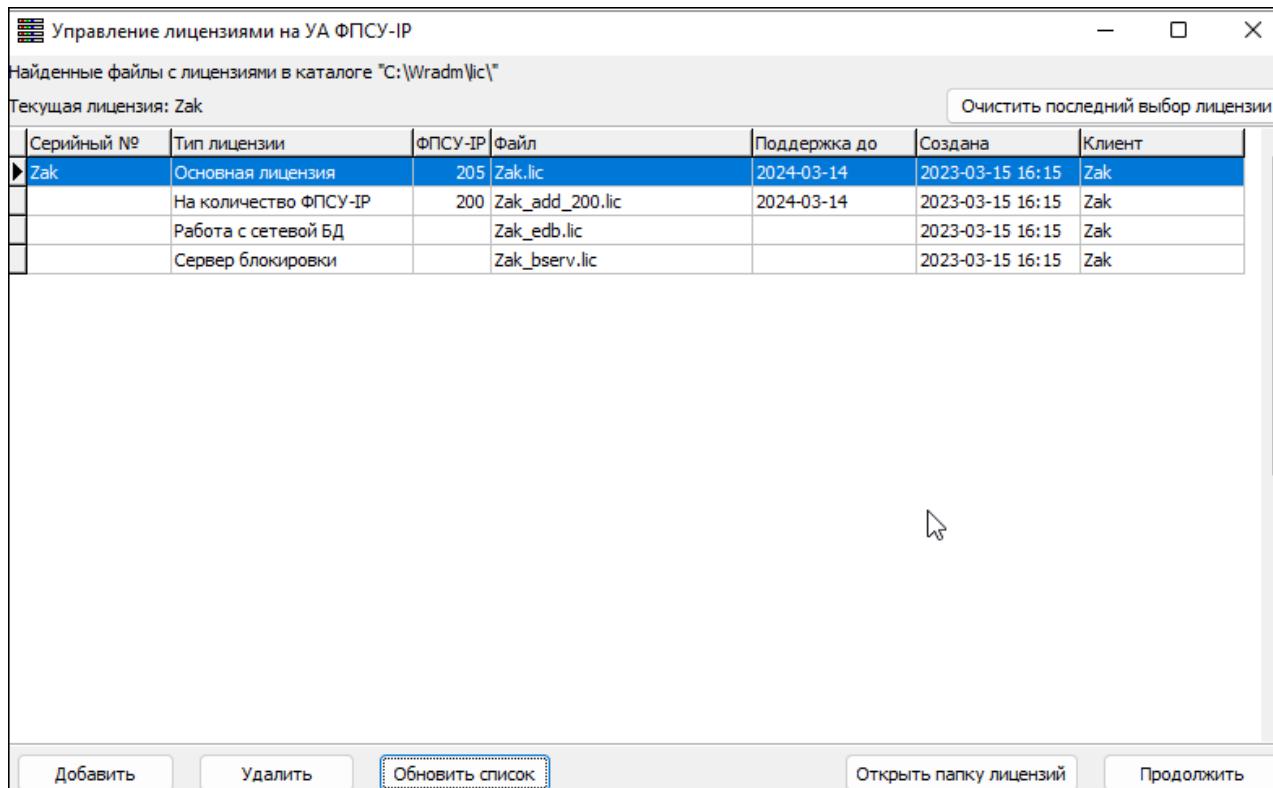


Рисунок 30 - Отображение лицензий в окне «Управление лицензиями»

В открывшемся окне предоставляется возможность добавить или удалить лицензию по нажатию соответствующей кнопки. Кроме того, можно обновить список лицензий или открыть каталог «LIC» для работы непосредственно в нем.

Добавить, удалить лицензию, а также обновить список лицензий можно при помощи контекстного меню окна «Управление лицензиями». Для этого необходимо выбрать лицензию в окне «Управление лицензиями», нажать на неё правой клавишей мыши и выбрать необходимый пункт контекстного меню.

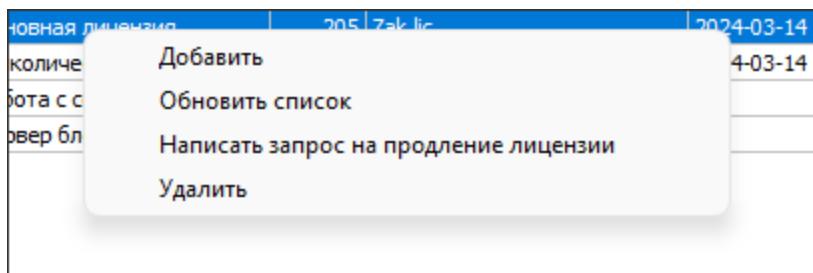


Рисунок 31 - Контекстное меню окна «Управление лицензиями»

8. Взаимная регистрация УА ФПСУ-IP и ФПСУ-IP

Взаимная регистрация ФПСУ-IP и УА ФПСУ-IP является обязательным условием для реализации удаленного управления: все операции по дистанционному контролю и управлению осуществляются УА ФПСУ-IP только по отношению к зарегистрированным ФПСУ-IP, а ФПСУ-IP могут обмениваться данными только с зарегистрированным ими администраторами УА ФПСУ-IP. Взаимная регистрация осуществляется посредством обмена специальными файлами — открытыми ключами.

8.1. Выдача открытого ключа УА ФПСУ-IP для регистрации на ФПСУ-IP

Для выдачи открытого ключа УА ФПСУ-IP на носитель необходимо выполнить команду главного меню «Ключ УА» → «Выдать открытый ключ УА». По приглашению УА ФПСУ-IP следует выбрать диск и каталог, куда должен быть выдан открытый ключ.

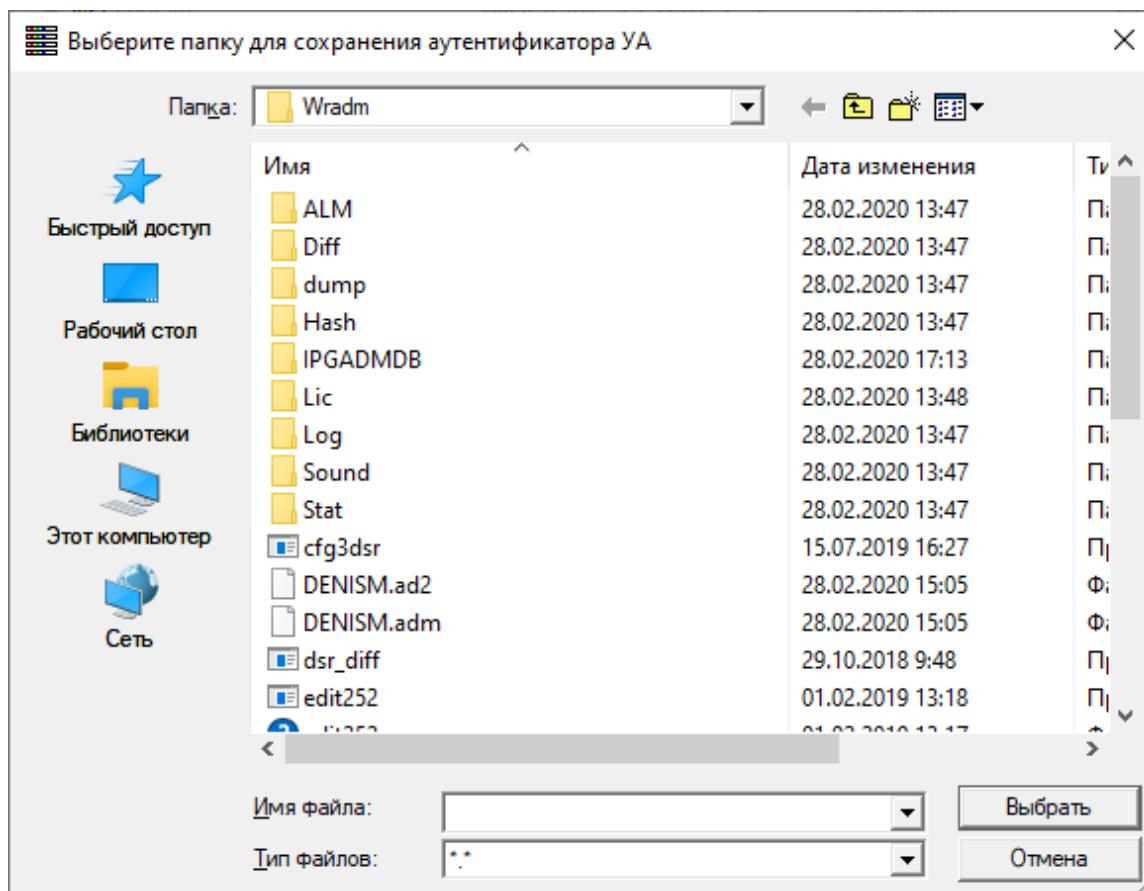


Рисунок 32 - Выбор каталога для сохранения открытого ключа

При нажатии кнопки «Выбрать», открытый ключ администратора УА ФПСУ-IP будет сохранен в указанный каталог как файл «Имя_администратора_УА ФПСУ-IP» с расширением .AD2 (и/или .AD4).

Файл с открытым ключом УА следует записать на носитель для дальнейшей передачи локальному администратору ФПСУ-IP с целью регистрации им администратора УА ФПСУ-IP. (см. документ «Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4.0.1. Руководство администратора»).

8. 2. Регистрация ФПСУ-IP в УА ФПСУ-IP

Чтобы зарегистрировать ФПСУ-IP в УА ФПСУ-IP, необходимо предварительно получить от их локальных администраторов файлы с открытыми ключами ФПСУ-IP (см. документ «Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4.0.1. Руководство администратора»), зарегистрировать их на УА ФПСУ-IP, после чего установить параметры взаимодействия УА ФПСУ-IP с ФПСУ-IP.

При перерегистрации открытого ключа ФПСУ-IP на УА требуется:

1. Зарегистрировать открытый ключ ФПСУ-IP на УА;
2. Перезапустить ФПСУ-IP.

В случае перерегистрации открытого ключа ФПСУ-IP на УА требуется зарегистрировать ключ на УА и перезапустить ФПСУ.

УА имеет возможность удаленно получить открытый ключ резервного ФПСУ-IP, имея только открытый ключ основного ФПСУ-IP (см. пункт «Регистрация резервного ФПСУ-IP по открытому ключу основного»).

8. 2. 1. Регистрация открытого ключа ФПСУ-IP в УА ФПСУ-IP

Для регистрации открытого ключа ФПСУ-IP в УА ФПСУ-IP необходимо:

1. Выполнить команду главного меню «ФПСУ-IP» → «Зарегистрировать ФПСУ-IP», либо нажать клавишу «Ins» при нахождении в основном окне УА ФПСУ-IP. Появится стандартное для ОС окно выбора каталога, в котором требуется указать путь к каталогу с открытыми ключами ФПСУ-IP.

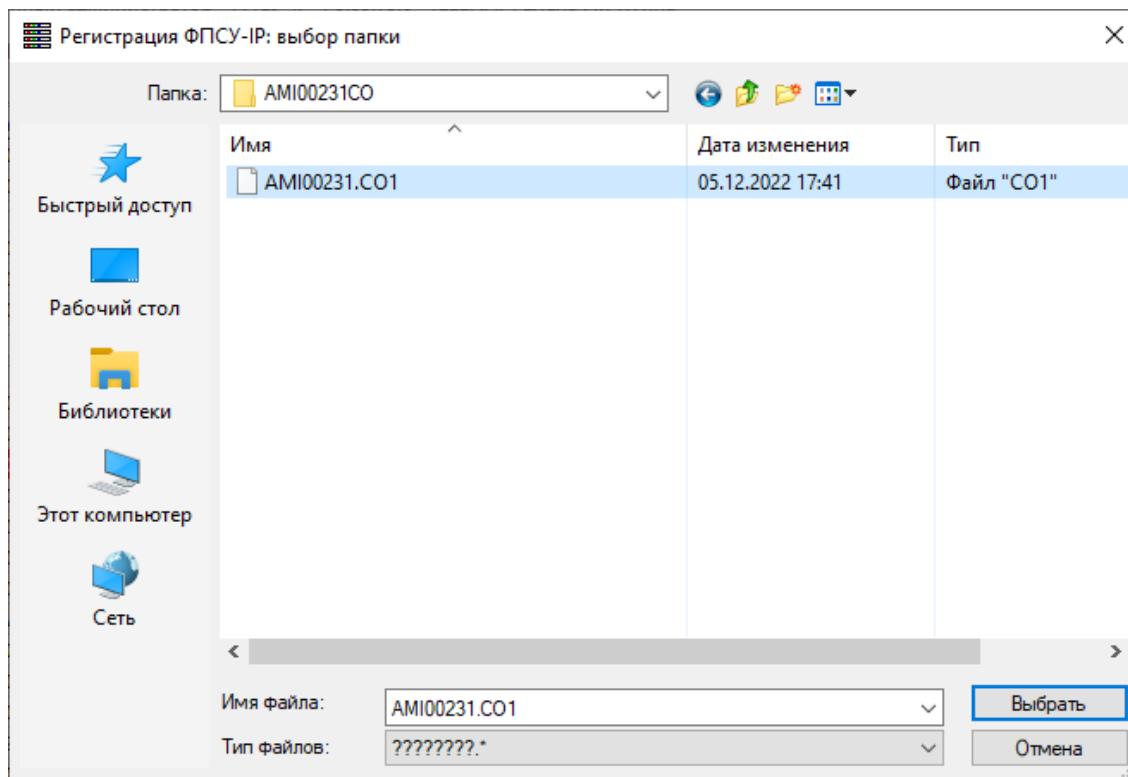
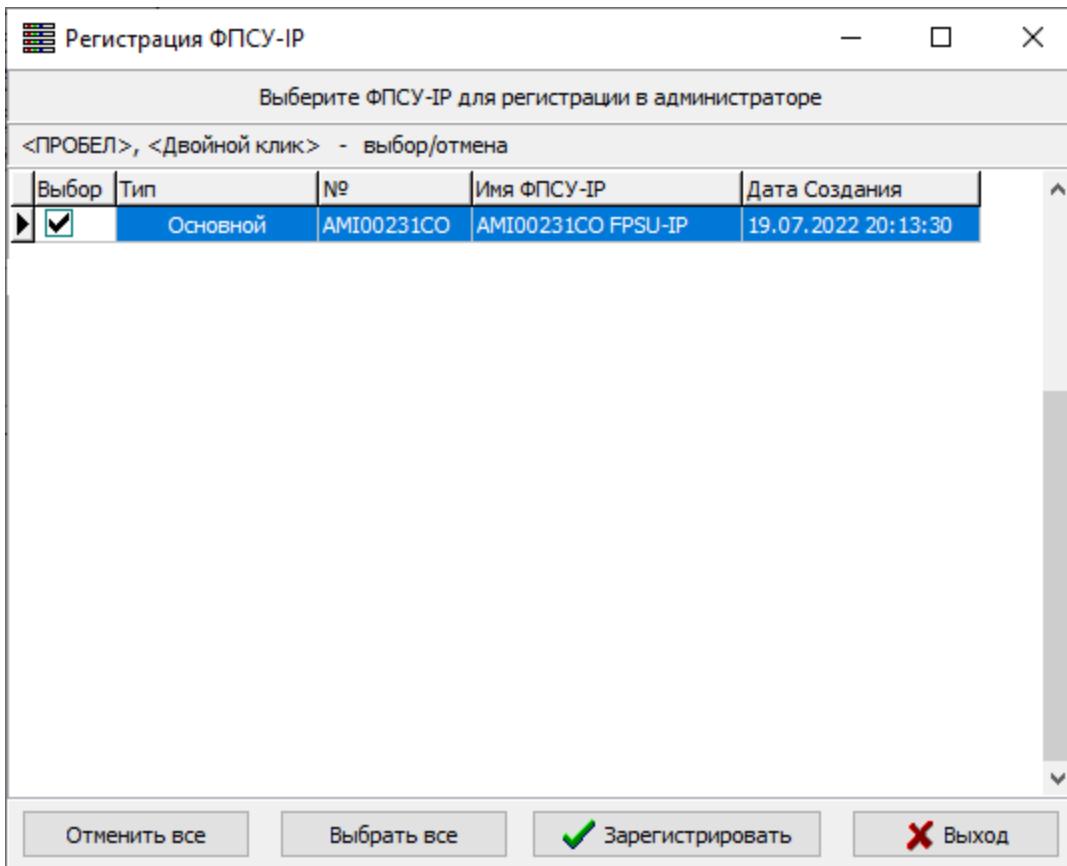


Рисунок 33 - Выбор каталога с открытыми ключами ФПСУ-IP

2. Если УА ФПСУ-IP найдет файлы с открытыми ключами ФПСУ-IP в указанном каталоге (файлы .CO1 и .CO2), откроется окно регистрации, содержащее список открытых ключей ФПСУ-IP. Для каждого из ФПСУ-IP отображаются: режим функционирования («Основной» – основной, «Резервный» – резервный), серийный номер, имя (данное локальным администратором) и дата генерации его открытого ключа. Необходимо отметить ФПСУ-IP, которые нужно зарегистрировать, установив флаг ячейки «Выбор» мышкой или нажимая клавишу «Пробел» при установленном на ФПСУ-IP курсоре. Затем следует нажать кнопку «Регистрировать», после чего при успешном выполнении операции появится служебное сообщение «Регистрация завершена», а зарегистрированные администратором ФПСУ-IP будут в списке помечены знаком успешной регистрации, «+».

**Рисунок 34 - Найденные описатели с открытыми ключами ФПСУ-IP**

3. Если ФПСУ-IP использует подсистему «горячего» резервирования, то основной и резервный ФПСУ-IP регистрируются по отдельности, но в списке зарегистрированных ФПСУ-IP для них создается единая запись списка. Для только что зарегистрированных ФПСУ-IP работа с УА ФПСУ-IP запрещена, и на панели информации в поле «Состояние VPN» будет значение «ФПСУ-IP запрещен», показывая таким образом, что не установлены необходимые параметры и работа с ФПСУ-IP пока невозможна.
4. После регистрации открытого ключа, новая запись ФПСУ-IP появится в окне списка.

Для дальнейшей работы с ним требуется установить рабочие параметры взаимодействия ФПСУ-IP с УА (см. пункт «Установка параметров взаимодействия ФПСУ-IP с УА ФПСУ-IP»).

В том случае, если при регистрации ФПСУ-IP обнаружится зарегистрированный ФПСУ-IP с идентичными идентификаторами, УА ФПСУ-IP предложит обновить его

открытый ключ:

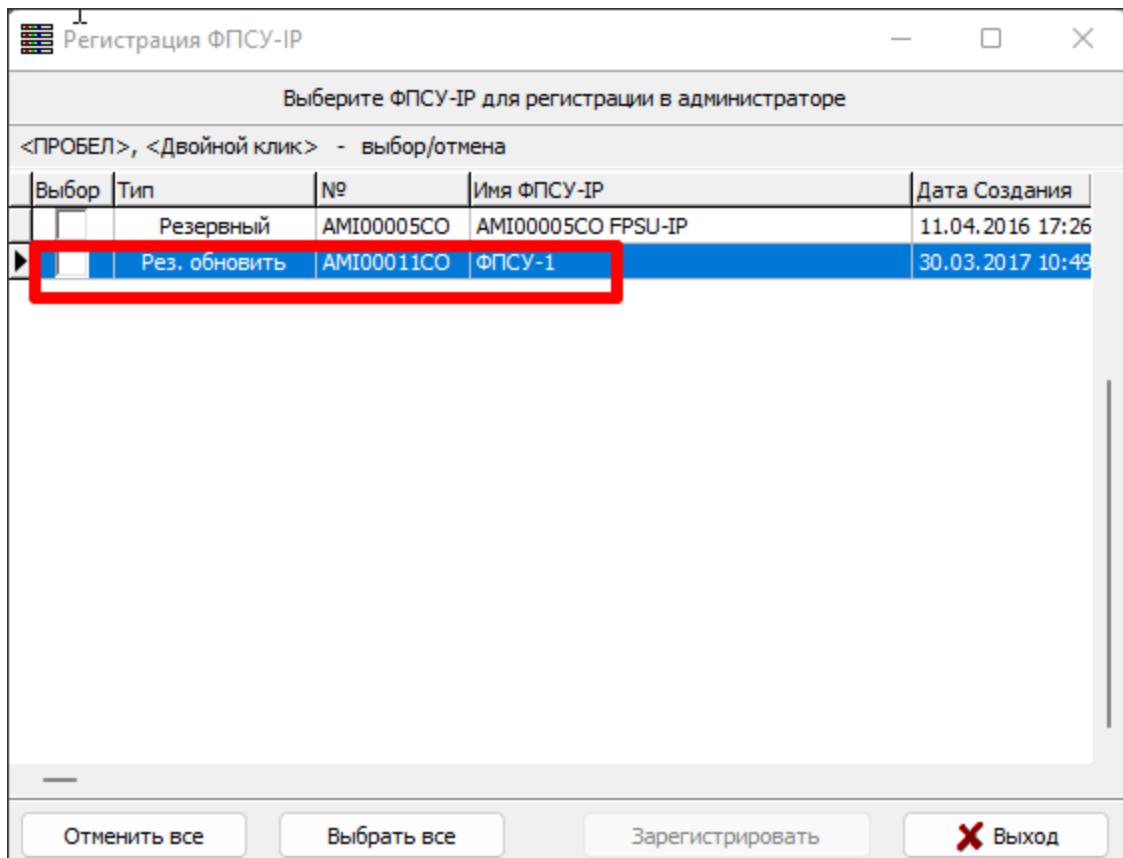


Рисунок 35 - Предложение обновить открытый ключ ФПСУ-IP

8. 2. 2. Установка параметров взаимодействия ФПСУ-IP с УА ФПСУ-IP

Для перехода в окно настройки параметров взаимодействия ФПСУ-IP с УА ФПСУ-IP необходимо отметить ФПСУ-IP в окне списка и нажать <F4> или кнопку панели инструментов «Параметры ФПСУ-IP», после чего на экран будет выдано окно установки параметров ФПСУ-IP.

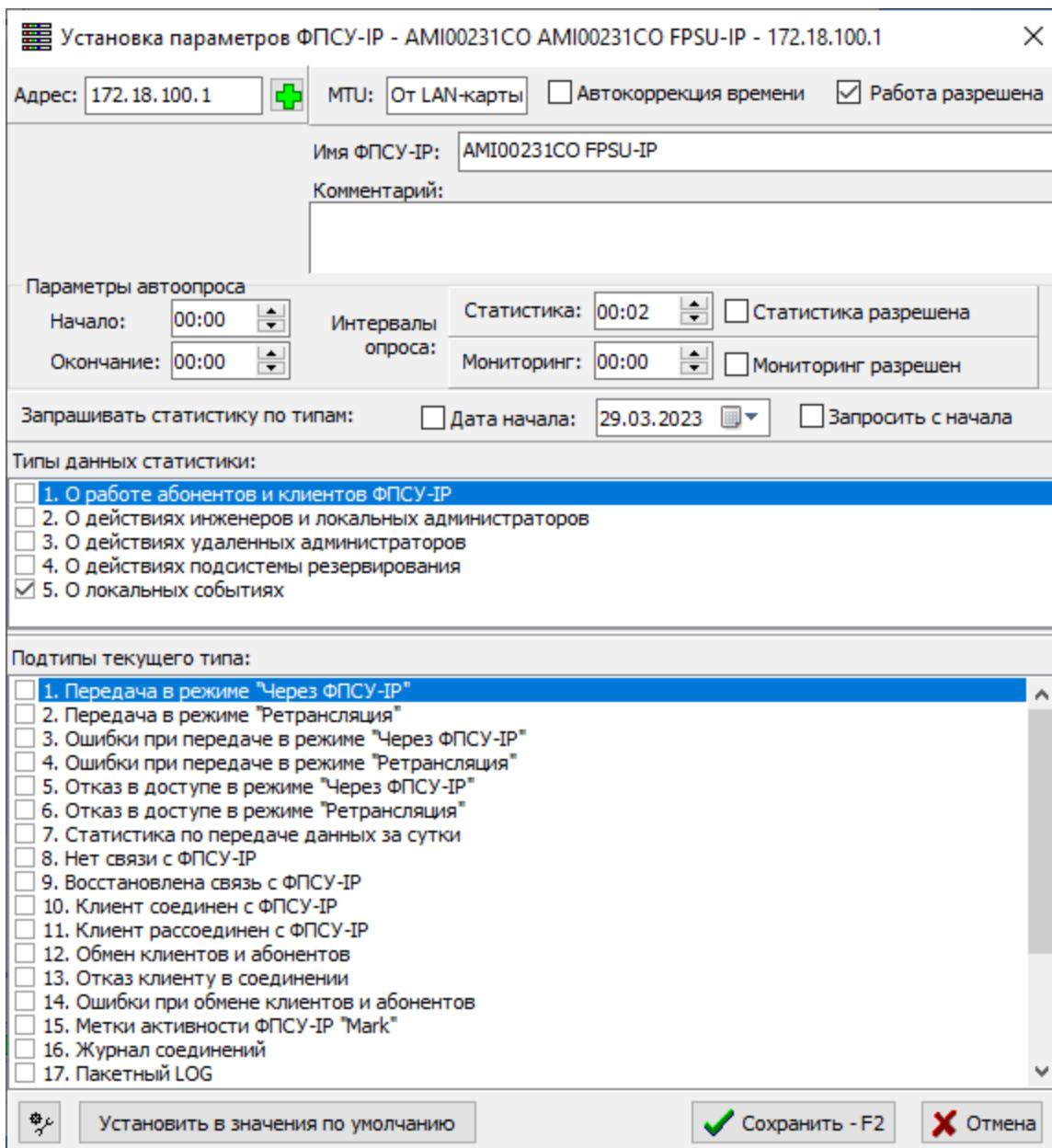


Рисунок 36 - Параметры ФПСУ

В этом диалоговом окне предлагается установить следующие параметры:

- Адрес — IP-адрес ФПСУ-IP; это обязательный основной параметр, без установки которого соединения УА ФПСУ-IP с ФПСУ-IP будут невозможны.
- Работа разрешена — флаг, позволяющий разрешить или запретить установку соединения и обмен информацией между УА ФПСУ-IP и ФПСУ-IP. Если он выключен, то никакие дальнейшие действия по удаленному управлению ФПСУ-IP

невозможны.

- Автокоррекция времени – если флаг установлен, текущее время на ФПСУ-IP будет автоматически синхронизироваться с текущим временем УА ФПСУ-IP (в том случае, если администратору УА ФПСУ-IP при регистрации на ФПСУ-IP было предоставлено право на изменение времени, см. документ «Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4.0.1. Руководство администратора»). Автокоррекция будет производиться с той же периодичностью, которая установлена для автоматического опроса данных мониторинга, но не реже одного раза в час.

Команда на изменение времени и даты будет автоматически передаваться ФПСУ-IP в тех случаях, когда, в результате автоматического опроса, рассогласование текущего времени УА ФПСУ-IP и ФПСУ-IP превышает 10 сек. При этом время корректируется с точностью до 1 секунды.

Необходимо отметить, что для адекватной синхронизации времени следует поддерживать точное время на компьютере, куда установлен УА ФПСУ-IP, осуществляющий коррекцию.

- MTU — максимальный размер (в байтах) пакетов, отправляемых УА ФПСУ-IP к управляемому ФПСУ-IP и обратно. Значение может быть «От LAN-карты» (рекомендуется) или явно заданное значение. Явная установка значения MTU может потребоваться, например, в том случае, когда на компьютере с установленным УА ФПСУ-IP находится программное обеспечение, увеличивающее размер передаваемого в сеть передачи данных пакета (установлен любой VPN-клиент, в том числе «ФПСУ-IP/Клиент»).
- Имя ФПСУ-IP — администратор УА ФПСУ-IP для удобства работы со списком зарегистрированных ФПСУ-IP может присвоить символьное имя, которое будет отображаться в списке. Имя ФПСУ-IP может быть произвольным, является необязательным параметром, и служит для удобства поиска ФПСУ-IP по списку;
- Комментарий — необязательный параметр, произвольная символьная строка, устанавливаемая администратором УА ФПСУ-IP;
- Параметры автоопроса — параметры автоматического опроса ФПСУ-IP для получения новых записей статистики, и происходящих на нём событий (подробнее см. разделы «Управление и мониторинг ФПСУ-IP» и «Управление статистикой ФПСУ-IP»);
- Начало — время суток в формате ЧЧ:ММ (где ЧЧ - часы, ММ - минуты), в которое

будет начинаться автоматический опрос.

- Окончание — время суток в формате ЧЧ:ММ, в которое опрос будет прекращаться.

Если установленное значение времени окончания опроса меньше установленного значения времени начала, автоматический опрос будет завершаться в указанное время следующих суток (например, чтобы производить опрос с 8 часов утра до 5 часов утра следующего дня необходимо указать начало и окончание опроса как 08:00 и 05:00 соответственно).

- Интервалы опроса — интервалы времени в формате ЧЧ:ММ, с которыми будут производиться во время автоматического опроса получение статистической информации от ФПСУ-IP и мониторинг событий на нем.

Интервал, с которым будет производиться мониторинг ФПСУ-IP, следует подбирать достаточно малым, чтобы иметь оперативную информацию о состоянии ФПСУ-IP, но и достаточно большим, чтобы постоянный опрос не создавал перегрузки в сети. Минимальное возможное значение интервала автоопроса составляет 10 минут для статистики и 1 минута для мониторинга. Если установленные интервалы автоопроса больше отрезка времени от установленного начала до установленного конца автоопроса, автоопрос будет производиться раз в сутки в момент времени, указанный как начало. Кроме того, автоопрос (если работа с данным ФПСУ-IP разрешена, см. выше) производится каждый раз при запуске УА ФПСУ-IP, если запуск происходит в момент времени между началом и окончанием автоопроса.

- Статистика разрешена — переключатель, позволяющий разрешить или запретить получение на УА ФПСУ-IP данных статистики с ФПСУ-IP.
- Мониторинг разрешен — переключатель, позволяющий разрешить или запретить получение на УА ФПСУ-IP данных мониторинга с ФПСУ-IP.
- Дата начала - дата в формате ДД.ММ.ГГГГ (ДД - день, ММ - месяц, ГГГГ - год), начиная с которой будет производиться ежедневный автоматический опрос с установленными выше временными интервалами.
- Запросить с начала - переключатель, позволяющий получать статистику, начиная с указанной даты с первого сообщения.
- Запрашивать статистику по типам —администратор УА ФПСУ-IP может выбирать, статистику по каким событиям он должен получать от данного ФПСУ-IP.

Каждый тип регистрируемых событий имеет набор подтипов. Отметка требуемого типа производится нажатием левой клавиши мыши по переключателю или по нажатию клавиши «Пробел» при нахождении на отмечаемой строке.

Внимание: независимо от отмеченных здесь типов, администратор УА ФПСУ-IP получит только те данные, которые ему было разрешено получать при регистрации его на ФПСУ-IP локальным администратором.

Установленные параметры автоопроса относятся только к получению информации в автоматическом режиме и не влияют на получение информации в режиме непосредственного обращения к ФПСУ-IP.

У администратора УА ФПСУ-IP есть возможность установить параметры ФПСУ-IP из заранее настроенного шаблона параметров, нажав кнопку «Установить значения по умолчанию». Настройка этого шаблона должна быть выполнена предварительно, и доступна по кнопке , расположенной в левом нижнем углу окна «Установка параметров ФПСУ», или по команде главного меню «Параметры» → «Параметры ФПСУ-IP по умолчанию».

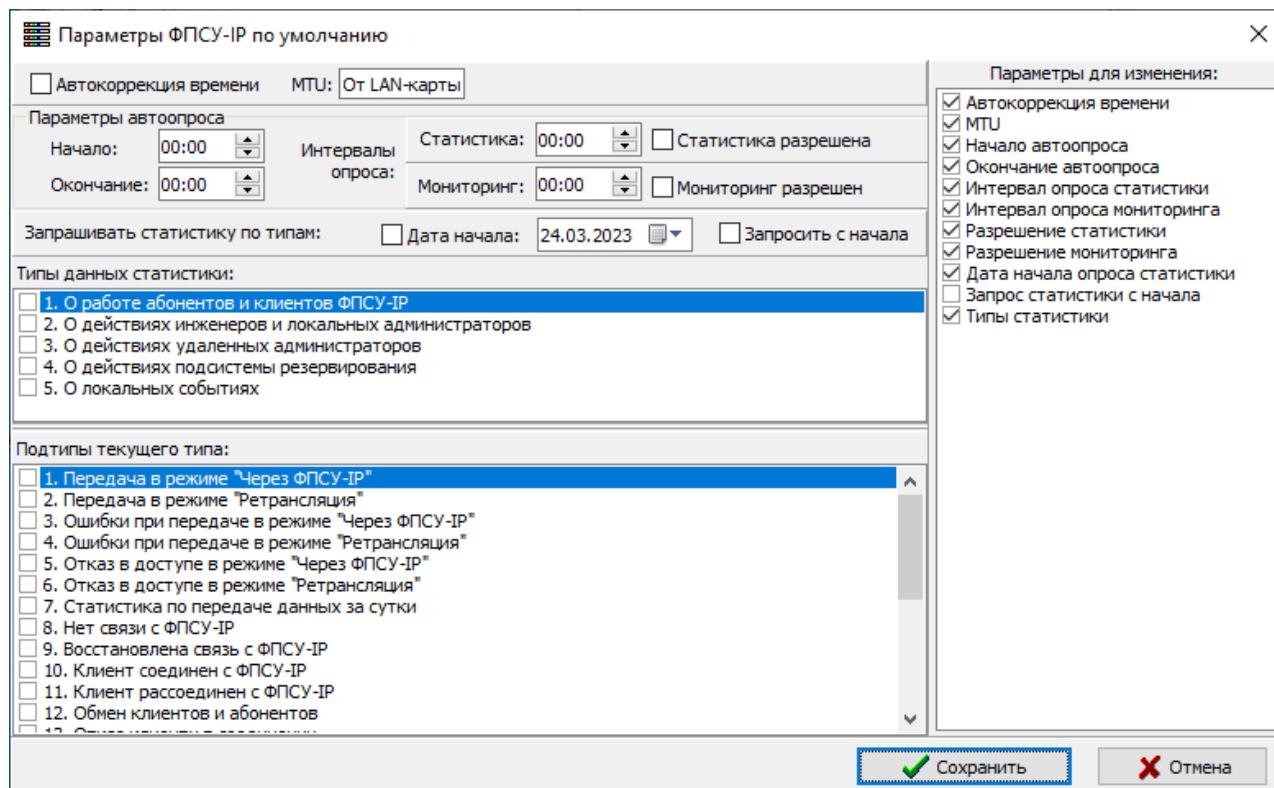


Рисунок 37 - Параметры ФПСУ по умолчанию

Когда все необходимые установки произведены, необходимо нажать кнопку

«Сохранить - F2» или клавишу <F2>, после чего измененные настройки будут применены, и произойдет выход из окна параметров ФПСУ-IP в основное окно УА ФПСУ-IP.

Для отказа от внесённых изменений и выхода в основное окно УА ФПСУ-IP следует нажать кнопку «Отмена».

8. 2. 3. Регистрация резервного ФПСУ-IP по открытому ключу основного

Чтобы зарегистрировать резервный ФПСУ-IP в УА, необходимо предварительно зарегистрировать основной ФПСУ-IP (см. пункт «Регистрация открытого ключа ФПСУ-IP в УА ФПСУ-IP»).

Для регистрации открытого ключа резервного ФПСУ-IP в УА по открытому ключу основного необходимо:

Выбрать ФПСУ-IP в списке и вызвать команду контекстного меню «Ручное управление» → «Редактирование УА». Если резервный ФПСУ-IP ранее не был зарегистрирован, в открывшемся окне внизу справа будет присутствовать кнопка «Обновить ключ рез. ФПСУ-IP».

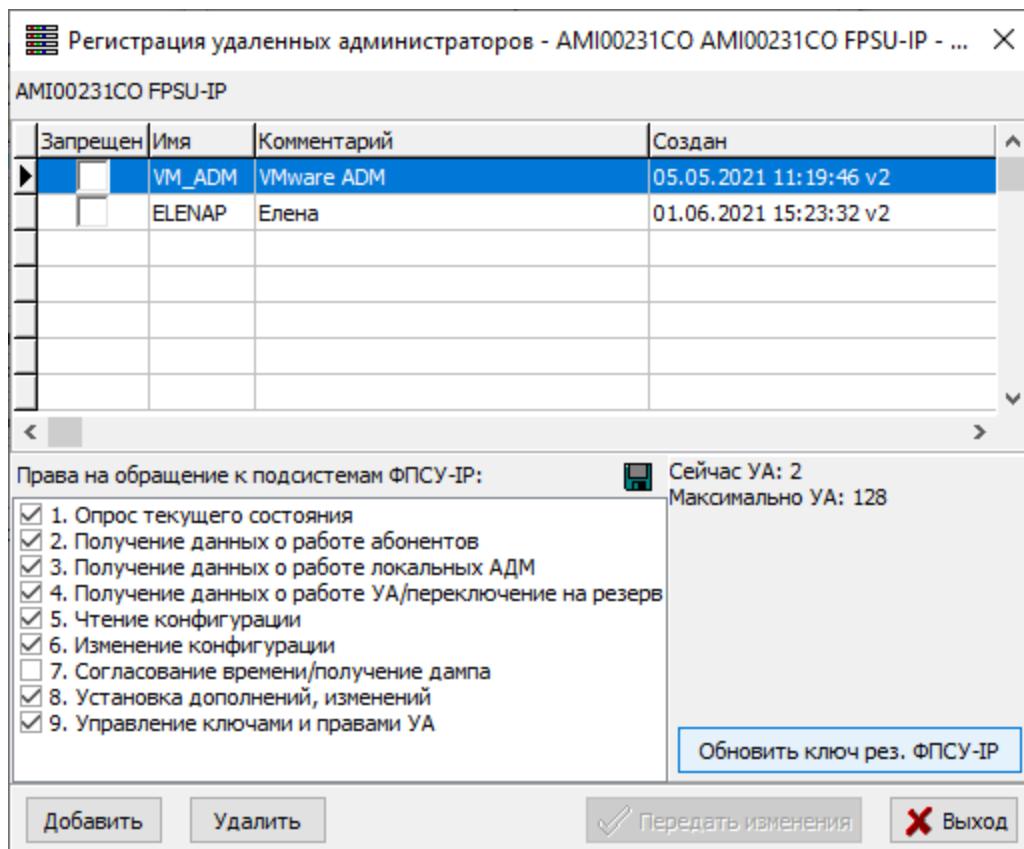


Рисунок 38 - Окно «Регистрация удаленных администраторов»

По нажатию кнопки «Обновить ключ рез. ФПСУ-IP» на экран будет выдано сообщение о подтверждении обновления открытого ключа ФПСУ-IP.

После подтверждения действия на экран будет выдано сообщение об успешном обновлении ключа открытого ключа резервного ФПСУ-IP.

Обновление открытого ключа автоматически инициализирует пересоединение УА с ФПСУ-IP, а состояние резервного ФПСУ-IP изменится на рабочее (см. пункт «Получение данных о состоянии «горячего» резервирования»).

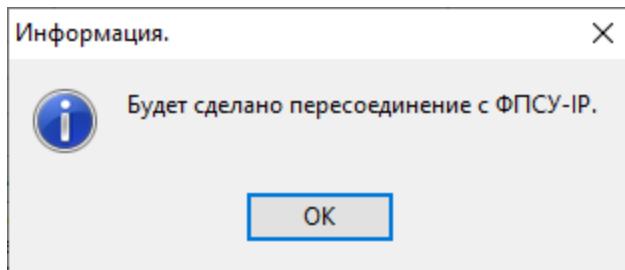


Рисунок 39 - Сообщение о пересоединении ФПСУ-IP

8. 2. 4. Изменение IP-адресов ФПСУ-IP из файла

При выборе пункта «Изменение IP-адресов ФПСУ-IP из файла» меню «ФПСУ-IP» предоставляется возможность обновить IP-адреса управления ФПСУ с УА ФПСУ-IP из текстового файла. Для этого необходимо выбрать пункт «Изменение IP-адресов ФПСУ-IP из файла» меню «ФПСУ-IP» и в открывшемся стандартном окне указать путь к файлу текстового формата *.txt, содержащему необходимую информацию. Структура файла должна включать строки с серийным номером и IP-адресом или IP-адресами, перечисленными через запятую.

8. 3. Работа со списком ФПСУ-IP

8. 3. 1. Редактирование имен ФПСУ-IP

Для удобства управления списком зарегистрированных ФПСУ-IP, администратор УА ФПСУ-IP может изменять их символьное название. Выполнить изменение имени можно или отдельно для каждого ФПСУ-IP при его регистрации, или массово для всех зарегистрированных ФПСУ-IP.

Массовое изменение имен для зарегистрированных на УА ФПСУ-IP осуществляется из окна «Редактирование имен ФПСУ-IP», вызываемое выбором пункта «Редактирование имён ФПСУ-IP...» меню «ФПСУ-IP»:

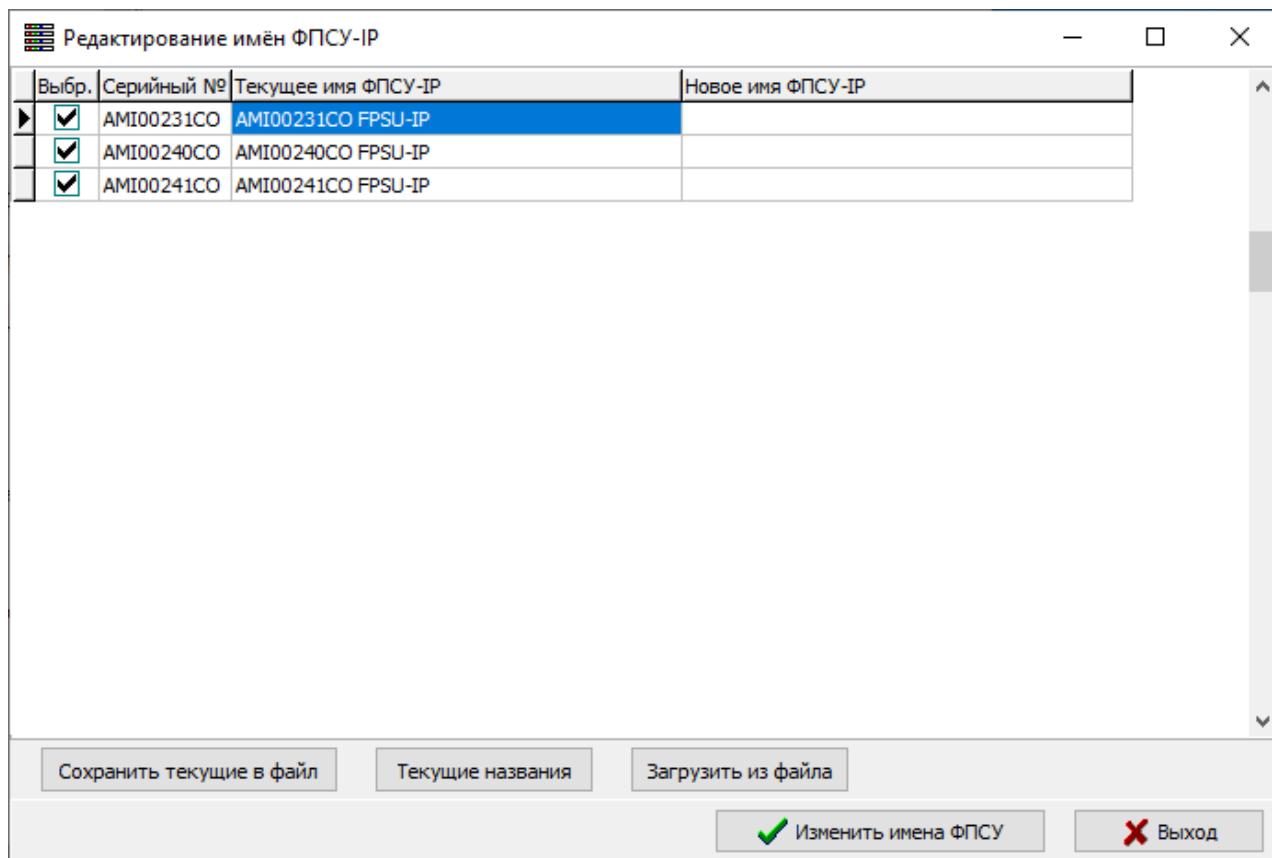


Рисунок 40 - Редактирование имен ФПСУ-IP

Изменяемое имя ФПСУ-IP вносится в столбец «Новое имя ФПСУ-IP», после чего требуется подтвердить вносимые изменения нажатием кнопки «Изменить имена ФПСУ-IP». При подтверждении изменения серийный номер и текущее имя ФПСУ-IP подцвечиваются оранжевым цветом. Измененная запись подцвечивается желтым цветом.

Для отмены внесенных изменений следует нажать кнопку «Выход».

Используемые в списке зарегистрированных ФПСУ-IP имена можно сохранить в текстовый файл, нажав кнопку «Сохранить текущие в файл».

Имена зарегистрированных ФПСУ-IP можно загрузить из текстового файла, нажав кнопку «Загрузить из файла».

Текущее имя ФПСУ-IP отображается столбце «Новое имя ФПСУ-IP» по нажатию кнопки «Текущие названия».

8. 3. 2. Удаление описателей ФПСУ-IP из списка

Чтобы удалить описатель ФПСУ-IP из УА ФПСУ-IP требуется выбрать пункт

«Удалить ФПСУ-IP» контекстного меню данного ФПСУ-IP. На экран будет выдано окно удаления, в котором можно увидеть системные параметры выбранного ФПСУ-IP (серийный номер и имя), а также выбрать параметры выполняемой операции:

- Удалить конфигурацию — удалить описатель ФПСУ-IP из списка зарегистрированных с удалением загруженных конфигураций данного ФПСУ-IP. Не удаляет описатель ФПСУ-IP из списка, если операция удаления конфигурации выполнялась для ФПСУ-IP с горячим резервом;
- Удалить конфигурацию из архива — удалить описатель ФПСУ-IP из списка зарегистрированных с удалением загруженных конфигураций и всех архивных конфигураций данного ФПСУ-IP. Не удаляет описатель ФПСУ-IP из списка, если операция удаления конфигурации выполнялась для ФПСУ-IP с горячим резервом;
- Удалить основной — удалить описатель основного ФПСУ-IP из списка зарегистрированных;
- Удалить резервный — удалить описатель резервного ФПСУ-IP из списка зарегистрированных;

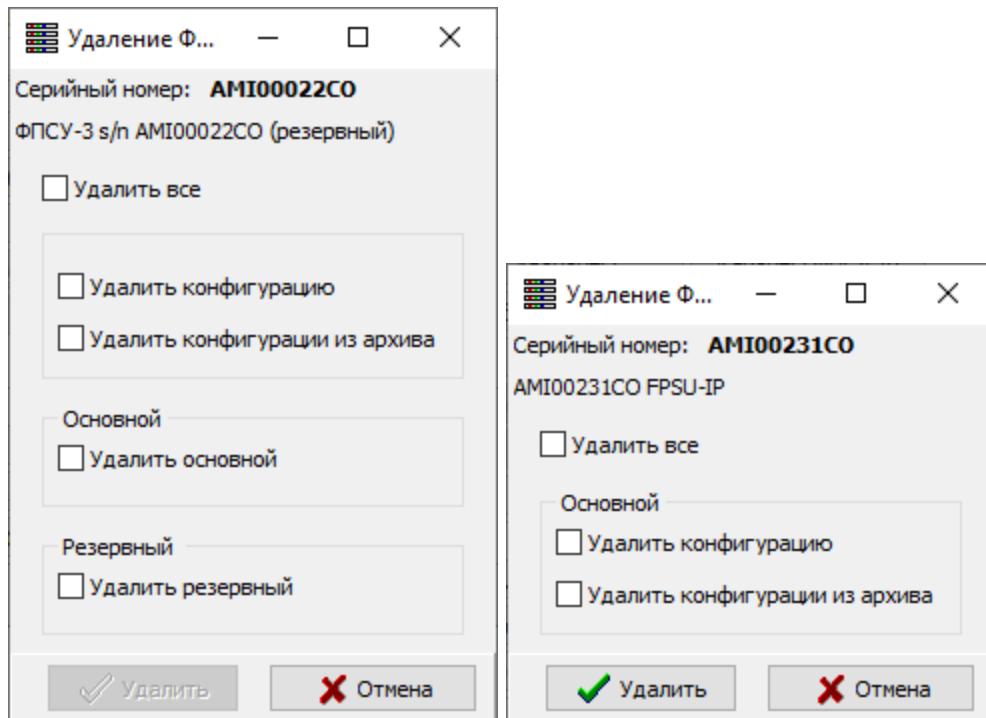


Рисунок 41 - Удаление ФПСУ-IP

- Удалить все — удалить описатель ФПСУ-IP из списка зарегистрированных с

параметрами «Удалить конфигурацию» и «Удалить конфигурации из архива».

Внимание! Данная операция окончательно удаляет из УА ФПСУ-IP параметры работы и открытый ключ выбранного ФПСУ-IP, для возвращения его в список потребуется повторно провести процедуру регистрации ФПСУ-IP на УА ФПСУ-IP.

8. 3. 3. Повторная регистрация ФПСУ-IP

Если в процессе работы возникает необходимость перерегистрировать какой-либо ФПСУ-IP (для работы с новым регистрационным открытым ключом), следует выбрать ФПСУ-IP, и вызывать из контекстного меню команду «Обновить открытый ключ». УА ФПСУ-IP предложит указать каталог, в котором находится новый открытый ключ ФПСУ-IP в стандартном окне выбора. Если в каталоге находится корректный новый открытый ключ, он будет обновлён, иначе будет выдано сообщение об отсутствии в каталоге подходящего файла.

Повторная регистрация для работы с новым открытым ключом возможна как для одного ФПСУ-IP, так и для группы. Если требуется обновить открытые ключи для группы ФПСУ-IP, следует в основном окне УА ФПСУ-IP выбрать их в окне списка, и в контекстном меню выбрать команду «Обновление аутентификаторов». Под аутентификаторами имеются в виду открытые ключи ФПСУ-IP.

8. 3. 4. Регистрация пустых ФПСУ-IP

К списку ФПСУ-IP могут быть применены массовые операции и массовое конфигурирование, перед этим следует создать пустые ФПСУ-IP. ФПСУ-IP могут быть зарегистрированы массово для дальнейшей настройки параметров выбором пунктов «Регистрация пустых ФПСУ-IP...» или «Регистрация пустых ФПСУ-IP из файла» меню «ФПСУ-IP».

При выборе пункта «Регистрация пустых ФПСУ-IP...» меню «ФПСУ-IP» предоставляется возможность зарегистрировать ФПСУ-IP. В открывшемся стандартном окне указать серийный номер создаваемых ФПСУ-IP и количество. Каждый следующий серийный номер ФПСУ-IP, будет присвоен по порядку, начиная с указанного.

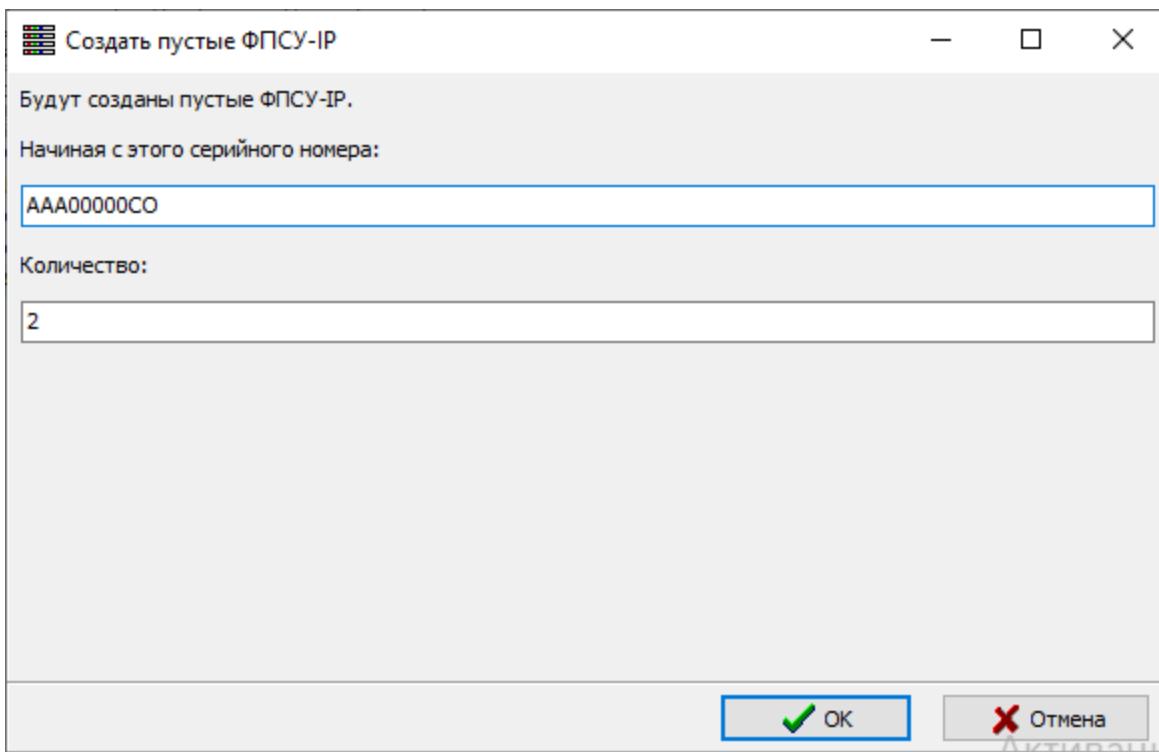


Рисунок 42 - Создание пустых ФПСУ-IP

На экран будет выдано окно о зарегистрированных пустых ФПСУ-IP. ФПСУ-IP будут добавлены в корневой раздел с созданным серийным номером и названием «Пустой ФПСУ-IP».

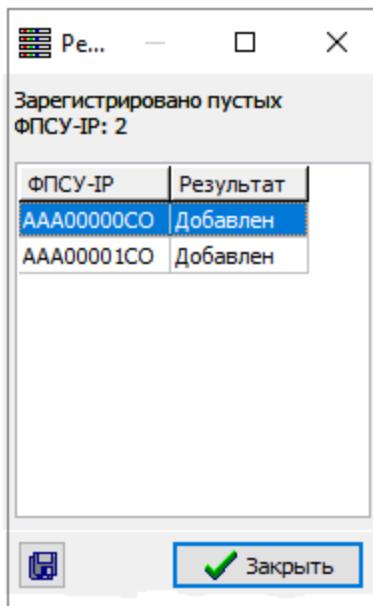


Рисунок 43 - Созданные ФПСУ-IP

При выборе пункта «Регистрация пустых ФПСУ-IP из файла» меню «ФПСУ-IP» в открывшемся стандартном окне указать путь к файлу текстового формата, содержащему необходимую информацию. Структура файла должна включать строки с серийными номерами создаваемых ФПСУ-IP. Дополнительно в строке через знак табуляции или пробел может быть указан IP-адрес или IP-адреса, перечисленные через запятую.

8. 4. Выдача открытых ключей ФПСУ-IP из базы данных УА ФПСУ-IP

Открытые ключи ФПСУ-IP могут быть выданы из базы данных УА ФПСУ-IP на внутренний накопитель автоматизированного рабочего места удаленного администратора ФПСУ-IP или на отчуждаемый носитель.

Для выдачи регистрационных данных ФПСУ-IP необходимо в окне списка отметить один или несколько ФПСУ-IP, а затем выполнить команду главного меню «ФПСУ-IP» → «Выдать открытый ключ ФПСУ-IP».

Появится стандартное окно выбора каталога. После выбора, куда выгружать открытые ключи, они будут выгружены в указанный каталог, в отдельные файлы вида XXX#####.XX№, где XXX#####.XX — серийный номер ФПСУ, а № равен «1», если ФПСУ-IP основной или единственный, и «2», если ФПСУ-IP резервный системы «горячего» резерва.

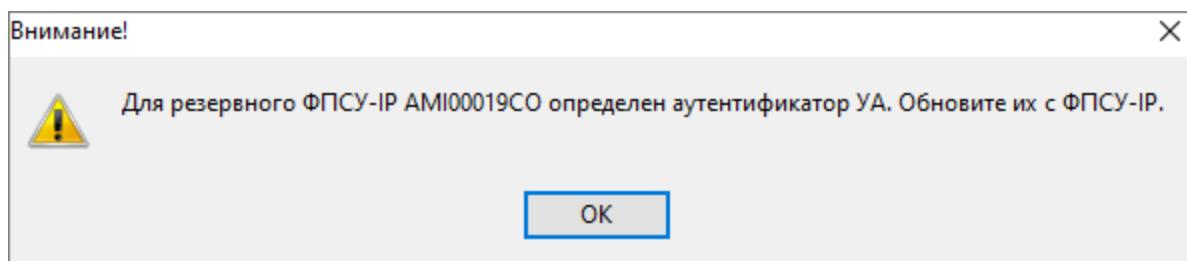


Рисунок 44 - Сообщение об определении открытого ключа

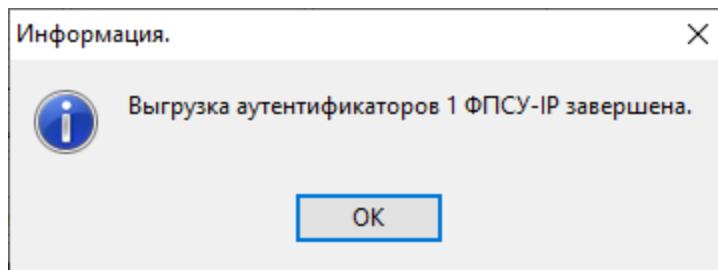


Рисунок 45 - Сообщение завершении выгрузки открытого ключа

9. Интерфейс УА ФПСУ-IP

После запуска УА ФПСУ-IP на экран выводится основное окно, состоящее из следующих элементов:

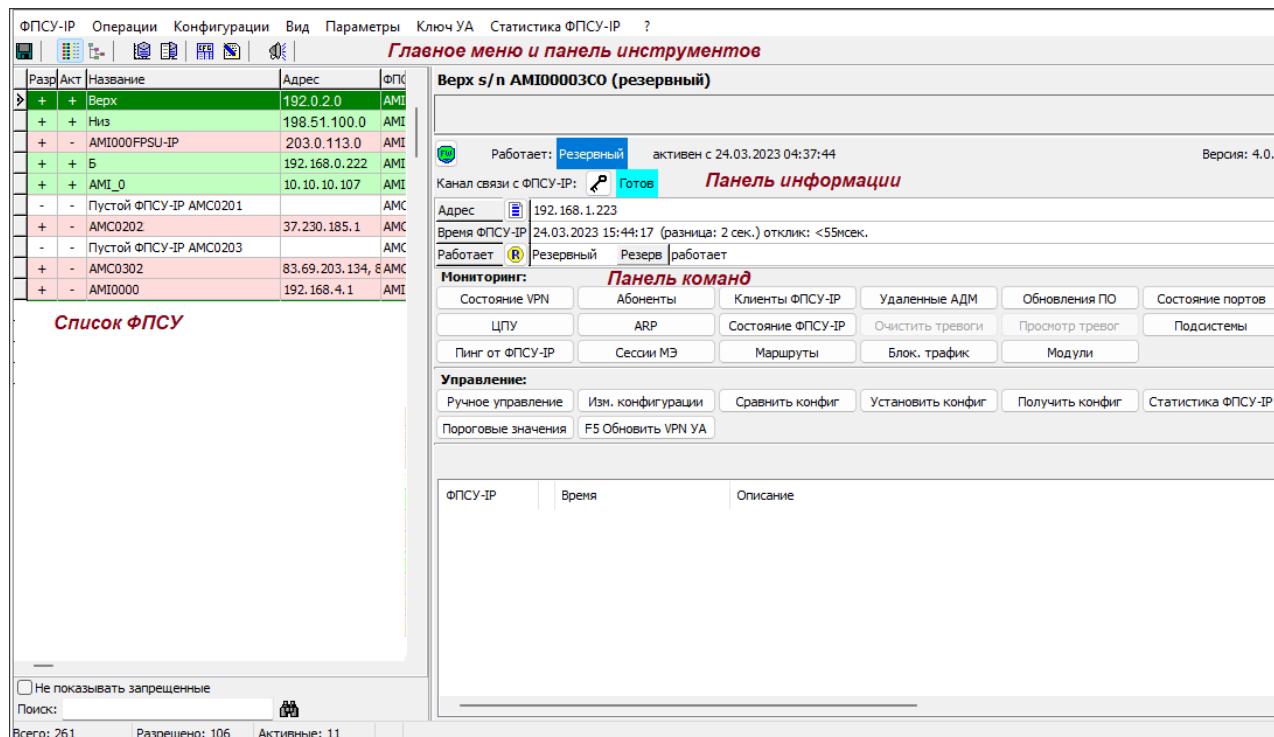


Рисунок 46 - Основное окно УА ФПСУ-IP

- главное меню и панель инструментов в верхней части основного окна (см. пункты «Главное меню УА ФПСУ-IP» и «Панель инструментов»);
- окно списка ФПСУ-IP, зарегистрированных на УА ФПСУ-IP, в левой части;
- панели информации и команд, доступные при выборе раздела или отдельного ФПСУ-IP, в правой верхней части (см. пункты «Панель информации» и «Панель команд»);
- окно оповещений в правой нижней части;
- панель поиска ФПСУ-IP по списку зарегистрированных, в левой нижней части;
- строка состояния в правой нижней части.

Подробнее возможности и описание интерфейса УА ФПСУ-IP описывается в следующих разделах.

9. 1. Основное окно (отображение зарегистрированных ФПСУ-IP)

В левой части основного окна находится список зарегистрированных ФПСУ-IP, которые могут отображаться как в виде простого списка, так и в виде иерархического дерева. При отображении ФПСУ-IP в виде списка, выводится на экран информация о названии ФПСУ-IP, состоянии разрешения работы ФПСУ-IP (знак «+» или «-» в графе «Разр.»), IP-адресе ФПСУ-IP, серийном номере (в графе «ФПСУ-IP») и версии программного обеспечения ФПСУ-IP.

Разр	Акт	Название	Адрес	ФПСУ-IP
>	+	Верх	192.0.2.0	AMI00001
	+	Низ	198.51.100.0	AMI00002
	-	AMI0000FPCU-IP	10.10.10.17	AMI00003
	+	Б	192.168.0.222	AMI00004
	+	AMI_0	10.10.10.107	AMI00005

Рисунок 47 - Отображение ФПСУ-IP в виде списка

При отображении ФПСУ-IP в виде иерархического дерева, на экран выводится древовидная структура разделов, в которой «файлами» являются зарегистрированные ФПСУ-IP. Каждый раздел содержит текстовый комментарий и краткую сводку о содержащихся в нем ФПСУ-IP. Каждый раздел (в том числе и «Корневой раздел») может быть переименован, содержать произвольное число подразделов и ФПСУ-IP. Общее количество ФПСУ-IP не может превышать 8192.

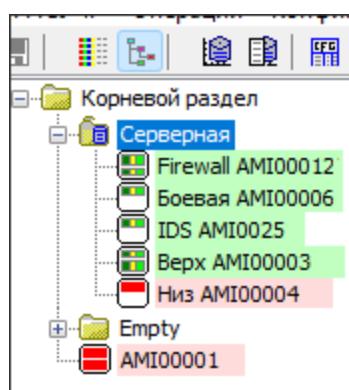


Рисунок 48 - Отображение ФПСУ-IP в виде иерархии

Значки в списке с одной или двумя цветными полосами перед названием и серийным номером ФПСУ-IP графически отражают состояние ФПСУ-IP. Если цвет значка ярко зеленый, то работа с данным ФПСУ-IP разрешена, соединение с ФПСУ-IP установлено, и он

опрашивается в штатном режиме. Если цвет значка красный, то работа с данным ФПСУ-IP разрешена, но установить защищенное соединение с ним не удалось. Если цвет значка серо-зеленый, то работа с данным ФПСУ-IP запрещена администратором УА ФПСУ-IP.

Если в значке находится одна цветовая полоса, это означает, что данный ФПСУ-IP работает без подсистемы «горячего» резервирования, и две — если с ней.

В нижней части окна списка находится переключатель «Не показывать запрещенные», при установке которого в списке не будут отображаться те ФПСУ-IP, которые были зарегистрированы в УА ФПСУ-IP, но при регистрации не было установлено разрешение на работу данных ФПСУ-IP (см. раздел «Регистрация ФПСУ-IP в УА ФПСУ-IP»).

При работе с окном списка УА ФПСУ-IP доступны два вида контекстного меню, объекта «раздел» (см. пункт «Контекстное меню раздела») и объекта «ФПСУ-IP» (см. пункты «Контекстное меню зарегистрированного ФПСУ-IP» и «Контекстное меню нескольких ФПСУ-IP»).

9. 1. 1. Контекстное меню раздела

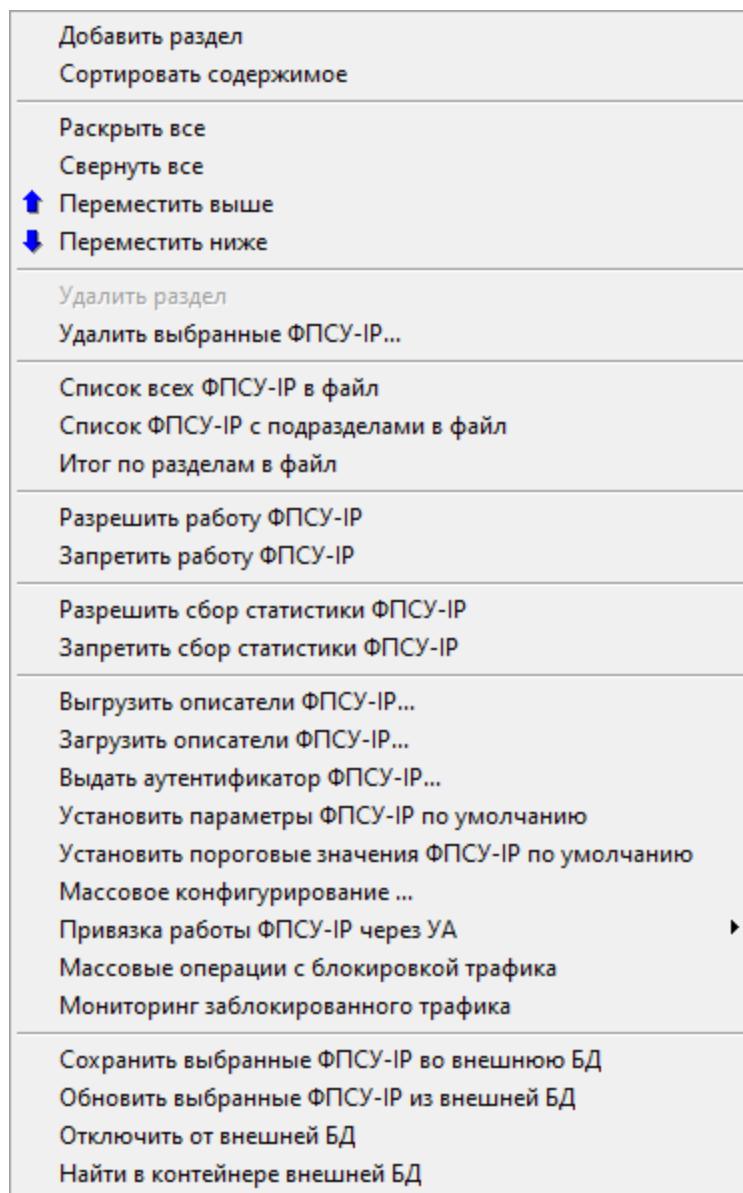


Рисунок 49 - Контекстное меню каталога иерархии

Контекстное меню раздела вызывается при нажатии правой клавиши мыши, и содержит следующие пункты:

- добавить новый вложенный подраздел;
- сортировать список ФПСУ-IP и подразделов иерархического дерева в алфавитном порядке;
- раскрыть все подразделы и ФПСУ-IP выбранного раздела;

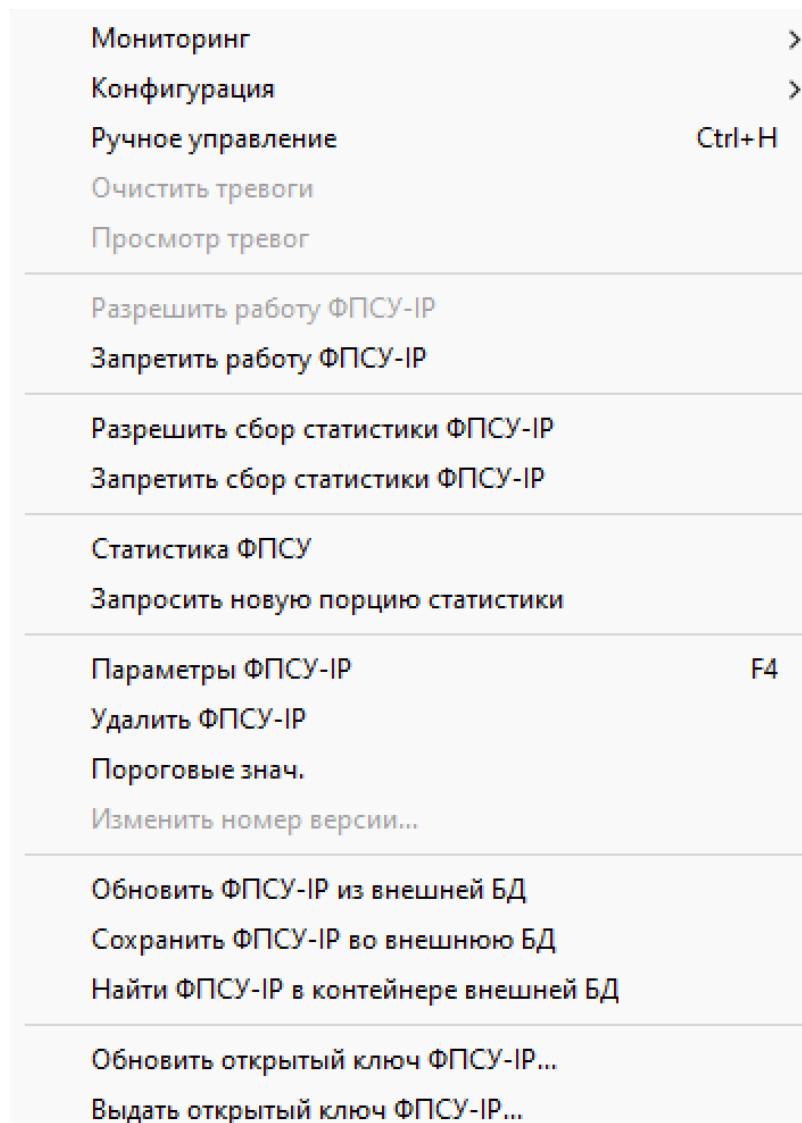
- свернуть все подразделы и ФПСУ-IP выбранного раздела;
- переместить выше/ниже подраздел по списку;
- удалить пустой раздел. Раздел, в котором находятся записи ФПСУ-IP, удалить нельзя. Требуется сначала переместить запись о ФПСУ-IP в другой раздел;
- удалить выбранные ФПСУ-IP;
- выдать список ФПСУ-IP данного раздела, или ФПСУ-IP раздела и подразделов в текстовый файл, содержащий имя ФПСУ-IP, IP адрес, серийный номер и указание о наличии или отсутствии горячего резерва;
- выгрузить/загрузить описатели ФПСУ-IP в файл (см пункт «Настройка УА ФПСУ-IP»);
- установить параметры и пороговые значения событий для находящихся в каталоге ФПСУ-IP в параметры, заданные администратором по умолчанию (см. пункт «Регистрация ФПСУ-IP в УА ФПСУ-IP»);
- отправить конфигурации находящихся в данном каталоге ФПСУ-IP в массовые операции (подробнее см. подраздел «Дистанционная массовая установка конфигураций»);
- Массовое конфигурирование...;
- Привязка работы ФПСУ-IP через УА;
- Массовые операции с блокировкой трафика;
- Мониторинг заблокированного трафика.

Пункты, относящиеся к работе со внешней БД:

- Сохранить выбранные ФПСУ-IP во внешнюю БД - сохранить описатель ФПСУ-IP во внешнюю БД;
- Обновить выбранные ФПСУ-IP из внешней БД - обновить описатели ФПСУ-IP в соответствии с информацией, сохраненной во внешней БД;
- Отключить от внешней БД;
- Найти в контейнере внешней БД - найти ФПСУ-IP в контейнере внешней базы данных.

9. 1. 2. Контекстное меню зарегистрированного ФПСУ-IP

Контекстное меню зарегистрированного ФПСУ-IP вызывается нажатием правой клавиши мыши на нем, и содержит следующие команды, аналогичные кнопкам панели информации и команд:

**Рисунок 50 - Контекстное меню ФПСУ-IP окна списка**

- Мониторинг - содержит подменю, состоящее из следующих пунктов:
 - «Абоненты», информация о состоянии работы абонентов ФПСУ-IP, подробнее см. пункт «Получение информации о работе абонентов»;
 - «Удаленные АДМ», информация о работе администраторов УА ФПСУ-IP на ФПСУ-IP, подробнее см. пункт «Получение информации о работе администраторов УА ФПСУ-IP»;
 - «Состояние VPN», информация о состоянии VPN-туннелей на данном ФПСУ-IP, подробнее см. пункт «Опрос состояния VPN-туннелей с другими ФПСУ-IP»;

- «Клиенты ФПСУ-IP», информация о состоянии работы клиентов ФПСУ-IP, подробнее см. пункт «Получение информации о работе клиентов»;
 - «Состояния портов», информация о состоянии LAN-адаптеров ФПСУ-IP, подробнее см. пункт «Получение информации о состоянии портов»;
 - «Обновления ПО», информация о выполненных на ФПСУ-IP обновлениях программного обеспечения, подробнее см. пункт «Получение информации об изменениях программного обеспечения»;
 - «ЦПУ», вывод графика загрузки процессора ФПСУ-IP, подробнее см. пункт «Получение информации о загрузке процессора ФПСУ-IP»;
 - «ARP», вывод ARP-таблицы ФПСУ-IP, подробнее см. пункт «Просмотр ARP-таблиц»;
 - «Резерв», информация о работе подсистемы горячего резервирования, подробнее см. пункт «Получение данных о состоянии «горячего» резервирования»;
 - «Состояние ФПСУ-IP» - вызов краткого отчёта о состоянии аппаратной части, подробнее см. пункт «Состояние ФПСУ-IP».
- Конфигурация – содержит подменю, состоящее из следующих пунктов:
- «Перейти в окно «Архива конфигураций» (см. «Архивы конфигураций ФПСУ-IP»);
 - «Сравнить конфиг» (раздел «Просмотр файла сравнения конфигурации»);
 - «Изм. конфигурации» - вызов редактора полученной с ФПСУ-IP конфигурации. Опция доступна, если в базе данных УА ФПСУ-IP есть ранее полученная конфигурация этого ФПСУ-IP;
 - «Установить конфиг», передать и установить на ФПСУ-IP измененную администратором УА ФПСУ-IP конфигурацию;
 - «Внести в Кфг файл блокировок клиентов» - позволяет запрещать или разрешать работу с группами и отдельными клиентами ФПСУ ;
 - «Изменить в кфг ACL», переход в окно изменения правил межсетевого экрана на ФПСУ-IP с помощью списка доступа (access list);
 - отправить для данного ФПСУ-IP «Конфигурацию в массовые операции», (подробнее см. подраздел «Дистанционная массовая установка конфигураций»);
- «Ручное управление», переход к управлению выбранным ФПСУ-IP, см. пункт «Вход в режим ручного управления»;

- «Очистить тревоги», остановка графического и звукового оповещения о произошедших на ФПСУ-IP событиях (см. п. «Панель команд»);
- «Просмотр тревог», просмотр сообщений от ФПСУ-IP о произошедших на нем событиях (см. п. «Панель команд»);
- «Разрешить работу ФПСУ-IP»;
- «Запретить работу ФПСУ-IP»;
- «Разрешить сбор статистики ФПСУ-IP»;
- «Запретить сбор статистики ФПСУ-IP»;
- «Статистика ФПСУ-IP» - просмотр накопленных статистических данных, см. подраздел «Просмотр накопленных статистических данных»;
- «Запросить новую порцию статистики» - используется при остановке сбора статистики;
- «Параметры ФПСУ-IP» - переход к окну настройки параметров взаимодействия УА ФПСУ-IP и выбранного ФПСУ-IP, горячая клавиша для этой команды «F4»;
- «Удалить ФПСУ-IP» - удалить описатель ФПСУ-IP из УА ФПСУ-IP;
- «Пороговые знач.», перейти к окну настроек сигнальных оповещений о событиях мониторинга зарегистрированного ФПСУ-IP (см. пункт «Настройка пороговых значений по умолчанию»);
- «Иzm. номер версии», перейти к окну ручного изменения установленной версии ПО зарегистрированного ФПСУ-IP. Такое изменение доступно только в том случае, когда нет связи с управляемым ФПСУ-IP, иначе версия автоматически берётся с него;
- «Привязка работы ФПСУ-IP через УА»;
- «Обновить ФПСУ-IP из внешней БД» - обновление параметров одного ФПСУ-IP в соответствии со сведениями, сохраненными во внешней БД (см. п. «Обновление ФПСУ-IP из внешней БД»);
- «Сохранить ФПСУ-IP во внешнюю БД» - сохранение измененных параметров одного ФПСУ-IP во внешней БД (см. п. «Сохранение ФПСУ-IP во внешней БД»);
- «Найти ФПСУ-IP в контейнере внешней БД» (см. п. «Контейнеры списков ФПСУ-IP»);
- «Обновить открытый ключ», обновление выданного локальным администратором открытого ключа ФПСУ-IP для перерегистрации ФПСУ-IP в УА ФПСУ-IP (см.

пункт «Регистрация ФПСУ-IP в УА ФПСУ-IP»);

- «Выдать открытый ключ ФПСУ-IP», выдача открытого ключа выбранного ФПСУ-IP в файл (см. пункт «Выдача открытых ключей ФПСУ-IP из базы данных УА ФПСУ-IP»).

9.1.3. Контекстное меню нескольких ФПСУ-IP

Если в окне списка выбрать (с помощью клавиши «Shift») несколько ФПСУ-IP, то для них можно вызвать контекстное меню массовых операций с ФПСУ-IP. Контекстное меню содержит следующие команды:

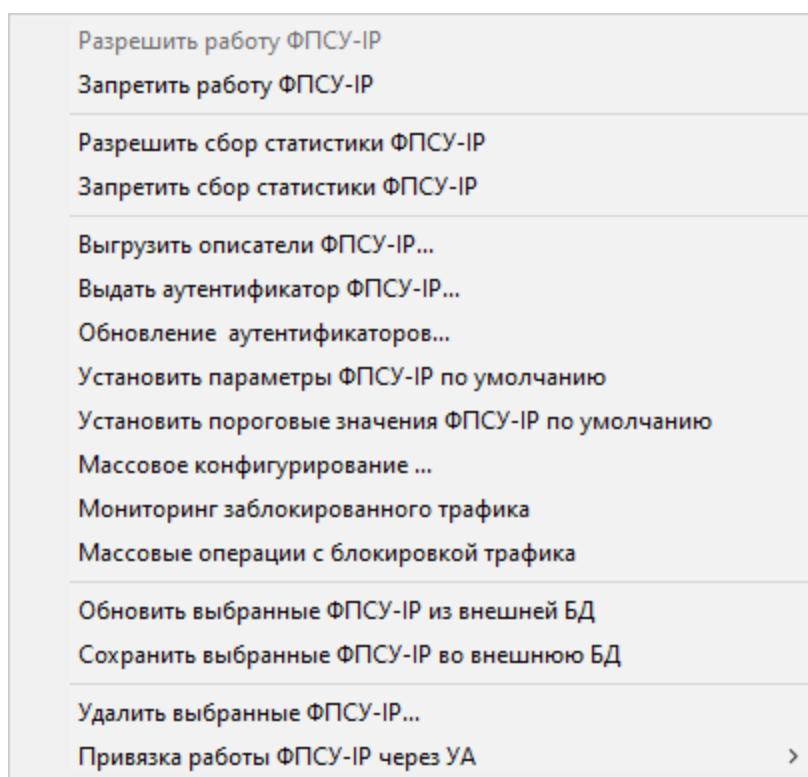


Рисунок 51 - Контекстное меню нескольких ФПСУ-IP

- Разрешить/запретить работу выбранных ФПСУ-IP с УА ФПСУ-IP;
- Разрешить/запретить сбор статистики с выбранных ФПСУ-IP в УА ФПСУ-IP;
- Выгрузить описатели ФПСУ-IP в файлы (см. пункт «Резервирование и восстановление работы УА ФПСУ-IP»);
- Выдать открытый ключ ФПСУ-IP;
- «Обновление аутентификаторов» - обновление выданных локальными

администраторами открытых ключей ФПСУ-IP для перерегистрации ФПСУ-IP в УА ФПСУ-IP (см. пункт «Регистрация ФПСУ-IP в УА ФПСУ-IP»);

- «Установить параметры ФПСУ-IP по умолчанию» из ранее созданного шаблона параметров;
- «Установить пороговые значения ФПСУ-IP по умолчанию» из ранее созданного шаблона пороговых значений (настройка пороговых значений ФПСУ-IP по умолчанию см. в пункте «Настройка пороговых значений по умолчанию»);
- Массовое конфигурирование...;
- Мониторинг заблокированного трафика;
- Массовые операции с блокировкой трафика;
- «Удалить выбранные ФПСУ-IP» - удалить описатель ФПСУ-IP из УА ФПСУ-IP;
- Привязка работы ФПСУ-IP через УА.

Пункты, относящиеся к работе со внешней БД:

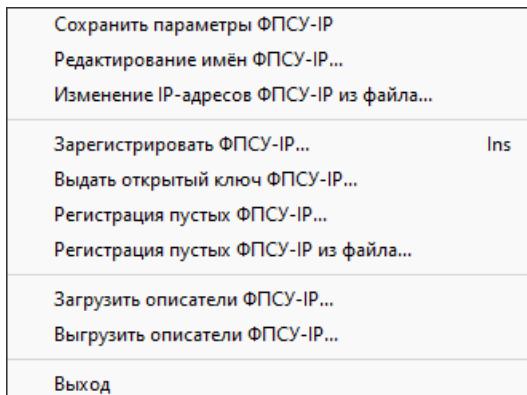
- Обновить выбранные ФПСУ-IP из внешней БД - обновить описатели ФПСУ-IP в соответствии с информацией, сохраненной во внешней БД;
- Сохранить выбранные ФПСУ-IP во внешнюю БД - сохранить описатель ФПСУ-IP во внешнюю БД.

9. 2. Главное меню УА ФПСУ-IP

Главное меню УА ФПСУ-IP содержит восемь пунктов, список содержимого которых открывается в виде меню при нажатии с помощью мыши или клавиатуры соответствующего поля главного меню.

9. 2. 1. ФПСУ-IP

Пункт меню «ФПСУ-IP» содержит команды для работы с ФПСУ-IP:

**Рисунок 52 - Пункт меню «ФПСУ-IP»**

- внесение последних изменений параметров работы зарегистрированных ФПСУ-IP в конфигурационные файлы УА ФПСУ-IP, «Сохранить параметры ФПСУ-IP». Помимо этого ручного сохранения, параметры работы ФПСУ-IP сохраняются по завершению работы УА ФПСУ-IP;
- изменение символьных имен зарегистрированных ФПСУ-IP в интерфейсе УА ФПСУ-IP, «Редактирование имён ФПСУ-IP» (подробнее см. пункт «Редактирование имён ФПСУ-IP»);
- изменение IP ФПСУ-IP из файла (см. подраздел «Изменение IP-адресов ФПСУ-IP из файла»);
- зарегистрировать ФПСУ-IP (регистрация ФПСУ-IP без выдачи открытого ключа УА);
- выдать открытый ключ ФПСУ-IP в файл;
- регистрация пустых ФПСУ-IP (см. пункт «Регистрация пустых ФПСУ-IP»);
- регистрация пустых ФПСУ-IP из файла (см. пункт «Регистрация пустых ФПСУ-IP»);
- выгрузить/загрузить описатели ФПСУ-IP в файл (см. пункт «Настройка УА ФПСУ-IP»);
- выход из УА ФПСУ-IP.

9. 2. 2. Операции

Пункт меню «Операции» содержит команды:

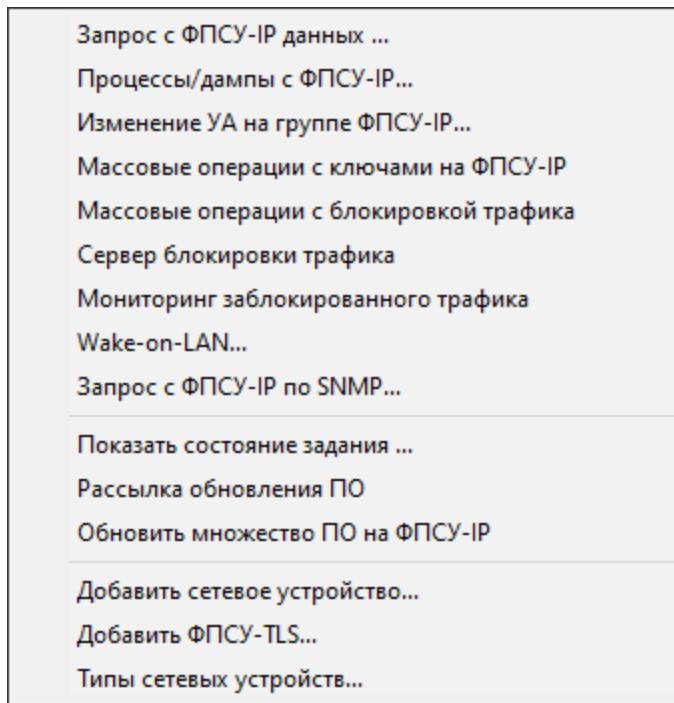


Рисунок 53 - Пункт меню «Операции»

- переход в окно запроса дат окончания поддержки и прочих параметров зарегистрированных ФПСУ-IP;
- переход в окно отображения находящихся на зарегистрированных ФПСУ-IP дампах (см. подраздел «Процессы с ФПСУ-IP»);
- Изменение УА в группе ФПСУ-IP (см. подраздел «Изменение УА на группе ФПСУ-IP»);
- Массовые операции с ключами на ФПСУ-IP (см. подраздел «Массовые операции с ключами»);
- Массовые операции с блокировкой трафика (см. подраздел «Массовые операции с блокировкой трафика»);
- Мониторинг заблокированного трафика (см. подраздел «Блокировка трафика на выбранных ФПСУ-IP»);
- Wake-on-LAN (Диалоговое окно с MAC хостов) (см. подраздел «Wake On LAN»);
- Запрос с ФПСУ-IP по SNMP (см. подраздел «Запрос с ФПСУ-IP по SNMP»);
- Показать состояние задания (см. подраздел «Просмотр состояния задания на рассылку»);

- Рассылка обновления ПО (см. подраздел «Рассылка обновления ПО»);
- Обновить множество ПО на ФПСУ-IP (см. подраздел «Обновление множества ПО»);
- Добавить сетевое устройство (см. подраздел «Добавление сетевого устройства»);
- Добавить ФПСУ-TLS (см. подраздел «Добавление ФПСУ-TLS»);
- Типы сетевых устройств (см. подраздел «Типы сетевых устройств»).

9. 2. 3. Конфигурации

Пункт меню «Конфигурации» содержит команды:

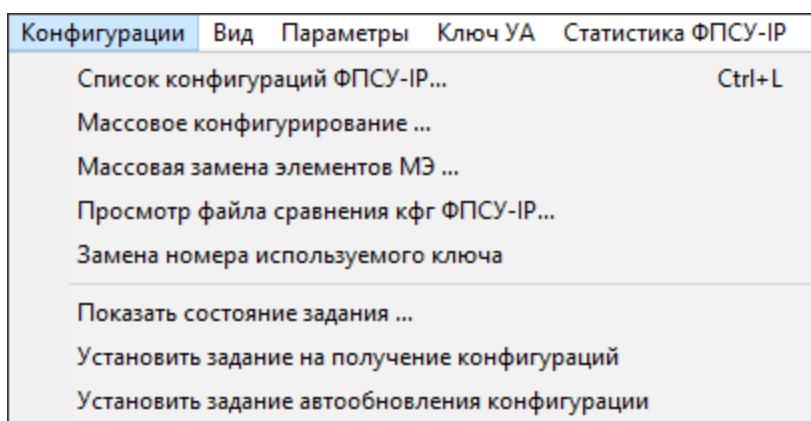


Рисунок 54 - Пункт меню «Конфигурации»

- переход в окно управления хранящимися в базе данных УА ФПСУ-IP конфигурациями ФПСУ-IP, «Список конфигураций ФПСУ-IP» (подробнее см. раздел «Управление конфигурациями ФПСУ-IP»);
- Массовое конфигурирование (подробнее см. раздел «Массовое изменение конфигураций по шаблону»);
- Массовая замена элементов МЭ (подробнее см. раздел «Массовая замена объектов межсетевого экрана»);
- Просмотр файла сравнения с кфг ФПСУ-IP (подробнее см. раздел «Просмотр файла сравнения конфигурации»);
- Замена номера используемого ключа(подробнее см. раздел «Замена номера используемого ключа»);
- Показать состояние задания (подробнее см. раздел «Дистанционная массовая установка конфигураций»);

- Установить задание на получение конфигураций (подробнее см. раздел «Установить задание на получение конфигураций»);
- Установить задание на автообновления конфигурации (подробнее см. раздел «Дистанционная массовая установка конфигураций»).

9.2.4. Вид

Пункт меню «Вид» содержит команды по настройке внешнего вида основного окна УА ФПСУ-IP:

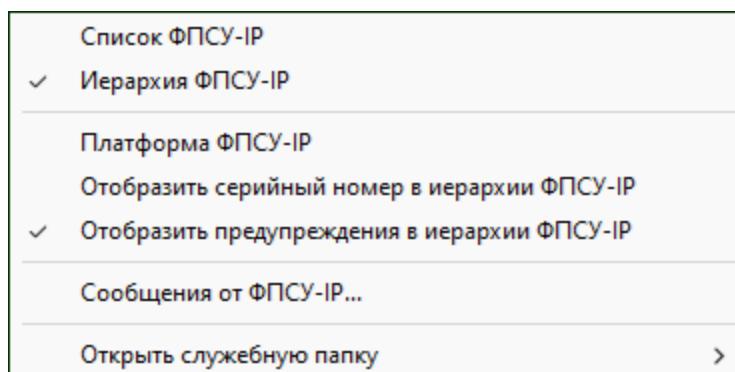


Рисунок 55 - Пункт меню «Вид»

- «Список ФПСУ-IP/Иерархия ФПСУ-IP» — команды, работающие как переключатель внешнего вида списка ФПСУ-IP, зарегистрированных в УА ФПСУ-IP. Список ФПСУ-IP представляет собой обычный не иерархический список, Иерархия ФПСУ-IP отображает зарегистрированные ФПСУ-IP в виде дерева каталогов, состоящего из корневого раздела и добавляемых вручную администратором УА ФПСУ-IP, по мере необходимости, новых разделов;
- «Платформа ФПСУ-IP» - команда, отображающая в панели информации внешний вид ФПСУ-IP;
- «Показать серийный номер в иерархии ФПСУ-IP» – в случае отображения списка зарегистрированных ФПСУ-IP как иерархии ФПСУ-IP, показывать после названия серийный номер управляемого ФПСУ-IP;
- «Отобразить предупреждения в иерархии ФПСУ-IP» – в случае отображения списка зарегистрированных ФПСУ-IP как иерархии ФПСУ-IP, показывать оповещения в виде восклицательного знака о произошедших на управляемом ФПСУ-IP событии;
- просмотр событий связи УА ФПСУ-IP с ФПСУ-IP, «События связи с ФПСУ-IP» и просмотр сообщений от ФПСУ-IP, «Сообщения от ФПСУ-IP» (подробнее см. пункт

«Сообщения от ФПСУ-IP»);

- «Открыть служебную папку» – открыть в новом окне один из служебных каталогов, где хранятся те или иные связанные с УА ФПСУ-IP данные: журналы, дампы от ФПСУ-IP, основной каталог УА ФПСУ-IP, медиафайлы для звуковых оповещений, архивы статистики с ФПСУ-IP, резервная копия УА ФПСУ-IP.

9.2.5. Параметры

Пункт меню «Параметры» содержит команды для настройки и определения режимов функционирования УА ФПСУ-IP:

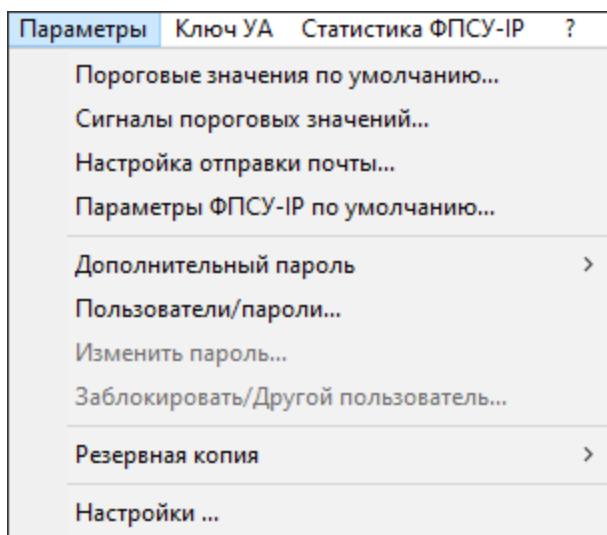


Рисунок 56 - Пункт меню «Параметры»

- настройка пороговых значений происходящих на ФПСУ-IP событий, по умолчанию (подробнее см. пункт «Настройка пороговых значений по умолчанию»);
- настройка звуковых оповещений событий и учетной записи для отправки оповещений с помощью электронной почты (см. пункт «Установка типов сигналов о событиях»);
- настройка отправки почты (см. пункт «Наблюдение за автоматическим сбором статистики»);
- настройка параметров «по умолчанию» для регистрируемых ФПСУ-IP (см. пункт «Регистрация ФПСУ-IP в УА ФПСУ-IP»);
- установка/отмена требования дополнительного пароля для входа в УА ФПСУ-IP (подробнее см. пункт «Установка дополнительного пароля»);

- настройка режима разграничения полномочий администраторов УА ФПСУ-IP в пункте «Пользователи/пароли» (подробнее см. пункт «Режим разграничения полномочий пользователей УА ФПСУ-IP»);
- изменение пароля;
- блокировка текущего пользователя и вход под другим;
- настройка параметров создания резервной копии базы данных УА ФПСУ-IP, и выполнение восстановления базы данных из резервной копии (см. пункт «Резервирование рабочих установок УА ФПСУ-IP»);
- переход в окно настроек УА ФПСУ-IP (подробнее см. пункт «Настройка УА ФПСУ-IP»).

9.2.6. Ключ УА

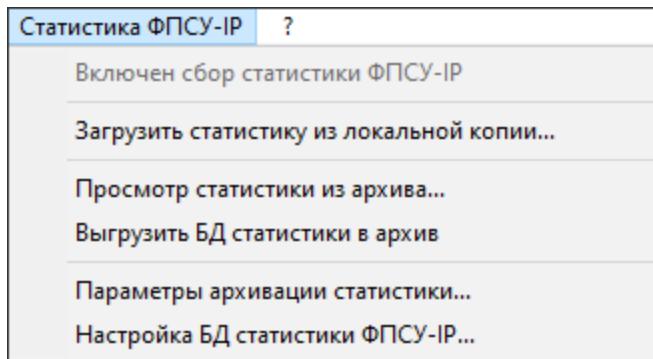
Пункт меню «Ключ УА» содержит команды для работы с ключевыми данными УА ФПСУ-IP и VPN-Key/UA, настройки и определения режимов функционирования УА ФПСУ-IP:

- просмотр информации о VPN-Key/UA и лицензии на него с помощью команды «Информация о USB-ключе и лицензии». Выдается серийный номер VPN-Key/UA, версия его внутреннего программного обеспечения (прошивки), срок действия лицензии и название организации, которой лицензия была выдана (подробнее в пункте «Управление VPN-Key/UA»);
- команда установки необязательного имени подключенного VPN-Key/UA, «Задать имя текущего USB-ключа» (подробнее в пункте «Управление VPN-Key/UA»);
- управление работой УА ФПСУ-IP с несколькими учетными записями, «Используемые УА», подробнее в пункте «Работа УА ФПСУ-IP с несколькими VPN-Key/UA»;
- выдача открытого ключа администратора УА ФПСУ-IP для регистрации на управляемых ФПСУ-IP (подробнее см. пункт «Выдача открытого ключа УА ФПСУ-IP для регистрации на ФПСУ-IP»);
- изменение ключевых данных администратора УА ФПСУ-IP, «Просмотр/Изменение ключа УА» (подробнее см. пункт «Пересоздание ключевых данных администратора УА ФПСУ-IP»);
- выдача резервной копии ключевых данных администратора, «Выдать ключ УА в файл» (подробнее см. пункт «Выдача ключа администратора УА ФПСУ-IP в файл»);

- восстановление ключевых данных администратора из резервной копии, «Загрузить ключ УА с диска», подробнее в пункте «Загрузка ключа администратора УА ФПСУ-IP с диска»;
- выдача резервной копии ключа шифрования БД ФПСУ-IP, «Выдать ключ БД УА на диск», подробнее в пункте «Выдача ключа для подключения к внешней БД»;
- создание новой учетной записи администратора УА ФПСУ-IP, «Создать нового УА», подробнее в пункте «Первоначальная настройка УА ФПСУ-IP (с VPN-Key/UA)»;
- управление доступом администраторов УА ФПСУ-IP к базе данных УА ФПСУ-IP, «Доступ УА к ключу шифрования БД ОК ФПСУ-IP», подробнее в пункте «Управление доступом к базе данных УА ФПСУ-IP»;
- запись ключевых данных текущего УА в другой VPN-Key/UA;
- запись ключевых данных УА из файла в VPN-Key/UA;
- запись ключевых данных УА из VPN-Key/UA в файл;
- запись ключевых данных УА из подключенного VPN-Key/UA в другой VPN-Key/UA, «Записать УА из USB-ключа в USB-ключ» («Создание дубликата VPN-Key/UA»);
- удаление из VPN-Key/UA всех данных администратора УА ФПСУ-IP, «Стереть ключ УА из USB-ключа»;
- изменение PIN-кода пользователя и администратора устройства, см. пункт «Управление паролями».

9.2.7. Статистика ФПСУ-IP

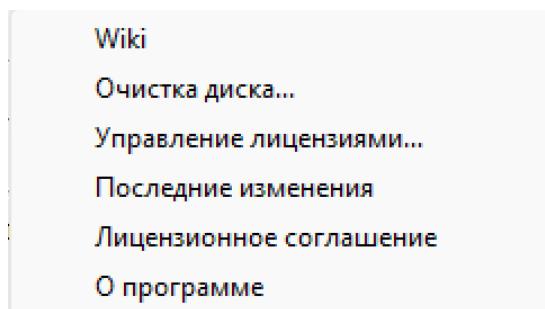
Пункт меню «Статистика ФПСУ-IP» содержит команды для работы с регистрационной информацией подконтрольных ФПСУ-IP (см. пункт «Управление статистикой ФПСУ-IP»):

**Рисунок 57 - Пункт меню «Статистика»**

- включение режима сбора статистики (см. пункт «Получение статистической информации»);
- загрузка статистики из архива, созданного DOS-версией УА ФПСУ-IP и просмотр статистики из такого архива, «Загрузить статистику из локальной копии» (см. пункт «Получение статистической информации»);
- просмотр статистики из указанного архива (см. пункт «Просмотр статистики из архива»);
- настройка параметров автоматической архивации регистрационных данных управляемых ФПСУ-IP (см. пункт «Перемещение статистики в архив»);
- настройка параметров базы данных, содержащей статистику по управляемым ФПСУ-IP (см. пункт «Настройка базы данных статистики УА ФПСУ-IP»).

9. 2. 8. Справка

Пункт меню «?» содержит справочную информацию по УА ФПСУ-IP, команды позволяют выполнить:

**Рисунок 58 - Пункт меню «?»**

- доступ к справочной информации по АРМ УА, размещенной на сайте разработчика;
- вызов окна настройки параметров очистки диска в основном каталоге УА ФПСУ-IP;
- вызов окна просмотра и добавления лицензий («Управление лицензиями»);
- вызов текстового списка о содержании последних изменений;
- вызов текста Лицензионного соглашения на использование УА ФПСУ-IP (см. п. «Порядок установки УА ФПСУ-IP»);
- вызов информационного окна «О программе».

9. 3. Панель инструментов

Панель инструментов основного окна УА ФПСУ-IP содержит кнопки быстрого доступа, дублирующие следующие команды главного меню:



- «ФПСУ-IP»→«Сохранить параметры ФПСУ-IP»;



- «Вид»→«Список ФПСУ-IP»;



- «Вид»→«Иерархия ФПСУ-IP»;



- «ФПСУ-IP»→«Список Конфигураций», или сочетание клавиш «Ctrl+L»;



- Переход в окно массового изменения конфигураций зарегистрированных ФПСУ-IP по шаблону;



- «Внешняя БД» (не отображается при отсутствии лицензии на сетевую базу данных);



- Показ учетной информации по ФПСУ-IP (не отображается при отсутствии лицензии на сетевую базу данных);



- «ФПСУ-IP»→«Сообщения от ФПСУ-IP...»;



- графическое оповещение, что сбор статистики со всех ФПСУ-IP остановлен администратором.

9. 4. Панель информации

В правой части основного окна находятся информационный блок и блок команд управления зарегистрированными ФПСУ-IP.

Информационный блок выводит справочную информацию по параметрам выбранного в окне списка объекта.

Если в списке выбран раздел, то панель информации отображает название раздела, произвольный текстовый комментарий к разделу, и сводные данные по ФПСУ-IP, которые находятся в разделе:

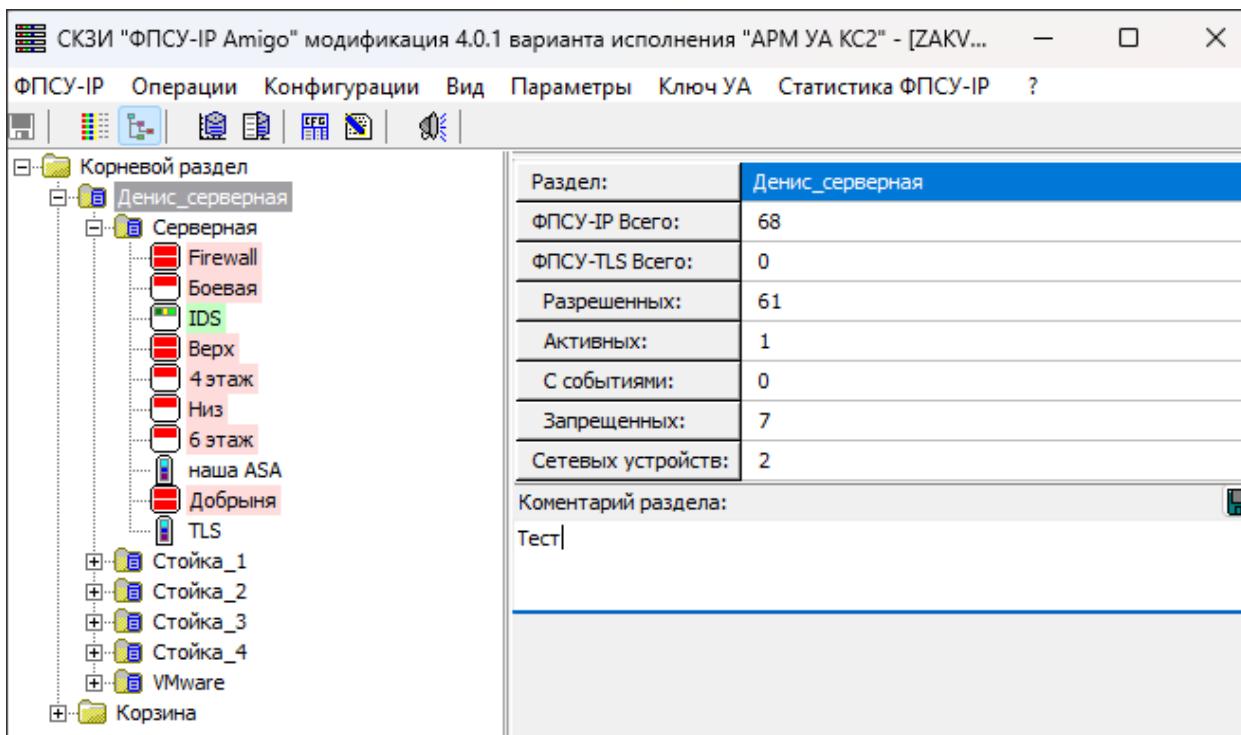


Рисунок 59 - Панель информации раздела

- общее количество зарегистрированных ФПСУ-IP раздела;
- общее количество зарегистрированных ФПСУ-TLS раздела;
- количество ФПСУ-IP, разрешенных для удаленного управления посредством УА ФПСУ-IP,
- количество ФПСУ-IP, с которыми в данный момент установлено активное соединение УА ФПСУ-IP;
- количество ФПСУ-IP, на которых произошло отслеживаемое администратором УА

ФПСУ-IP событие;

- количество ФПСУ-IP, с которыми администратор УА ФПСУ-IP запретил в параметрах зарегистрированного ФПСУ-IP устанавливать активные соединения для мониторинга (см. подраздел «Регистрация ФПСУ-IP в УА ФПСУ-IP»);
- общее количество сетевых устройств.

Если в окне списка выбран ФПСУ-IP, то панель информации отображает сводные данные по нему:

- имя и серийный номер выбранного ФПСУ-IP;
- кнопка перехода в мониторинг сессий, когда межсетевой экран включен;
- режим работы. Если используется подсистема горячего резервирования, то указывает на то, какой ФПСУ-IP в данный момент является активным, основной или резервный;
- версия программного обеспечения ФПСУ-IP;
- количество записей принятой с ФПСУ-IP статистики;
- IP-адрес ФПСУ-IP;
- состояние (VPN) соединения между УА ФПСУ-IP и ФПСУ-IP с указанием длительности этого соединения, а также даты и времени последнего опроса по мониторингу и статистике (список состояний см. ниже);
- дата и время, установленные на ФПСУ-IP с указанием разницы во времени с УА ФПСУ-IP и времени отклика ФПСУ-IP на запросы УА ФПСУ-IP;
- состояние подсистемы горячего резервирования, задействована или нет;
- версия, дата и время создания открытых ключей ФПСУ-IP, переданных УА ФПСУ-IP.

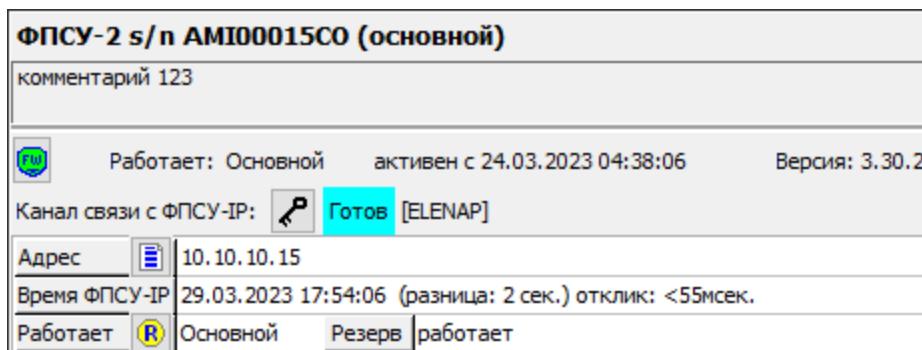


Рисунок 60 - Панель информации выбранного ФПСУ-IP

Поле «Канал связи с ФПСУ-IP» может принимать следующие значения:

- Нерабочие состояния:

- «Не задан IP-адрес» — при регистрации ФПСУ-IP не задан его сетевой адрес и соединения с ним невозможны «Нет MAC-адреса. Поиск» — производится ARP-запрос MAC-адреса, возможно, ФПСУ-IP или транзитные маршрутизаторы не функционируют;
- «НЕ ГОТОВ» — ФПСУ-IP не готов к передаче информации;
- «Запрос открытия VPN» — производится запрос открытия VPN-туннеля между УА ФПСУ-IP и ФПСУ-IP, возможно, ФПСУ-IP или транзитные маршрутизаторы не функционируют, или не сходится процесс взаимной аутентификации;
- «Открытие VPN» — начал процесс открытия VPN-туннеля между УА ФПСУ-IP и ФПСУ-IP;
- «Закрытие VPN»;

- Рабочие состояния:

- «ГОТОВ» — ФПСУ-IP готов к передаче информации, которая начнется в заданный момент планового автоопроса;
- «Передача запроса» по нажатию клавиши «Enter» можно перейти в режим ручного управления;
- «Ожидание ответа»;
- «Прием ответа».

9. 5. Панель команд

Блок команд, находящийся под панелью информации , относится непосредственно к управлению и мониторингу ФПСУ-IP, зарегистрированных на УА ФПСУ-IP, и в большинстве своем («Состояние VPN», «Абоненты», «Клиенты ФПСУ-IP», «Удаленные АДМ», «Обновления ПО», «Состояние портов», «ЦПУ», «ARP», «Общ. Статистика», «Очистить тревоги», «Просмотр тревог», «Ручное управление», «Изм. конфигурации») дублируют команды контекстного меню описателя ФПСУ-IP из окна списка (см. подраздел «Контекстное меню зарегистрированного ФПСУ-IP»).

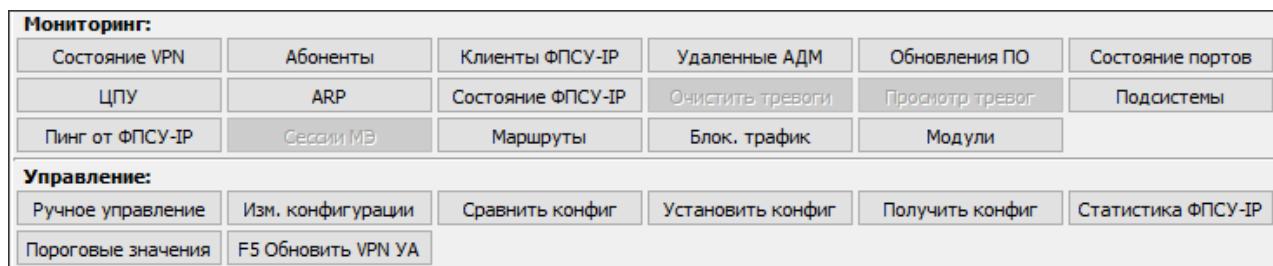


Рисунок 61 - Панель команд

Помимо дублирующих кнопок, на панели находятся кнопки с дополнительным функциями:

- «Состояние VPN» – нажатие кнопки выводит на экран окно, отображающее состояние VPN-туннелей для выбранного ФПСУ-IP. При этом в графе «Режим» квантовые тунNELи будут помечены сокращением «QKD» (см. раздел «Опрос состояния VPN-туннелей с другими ФПСУ-IP»)..

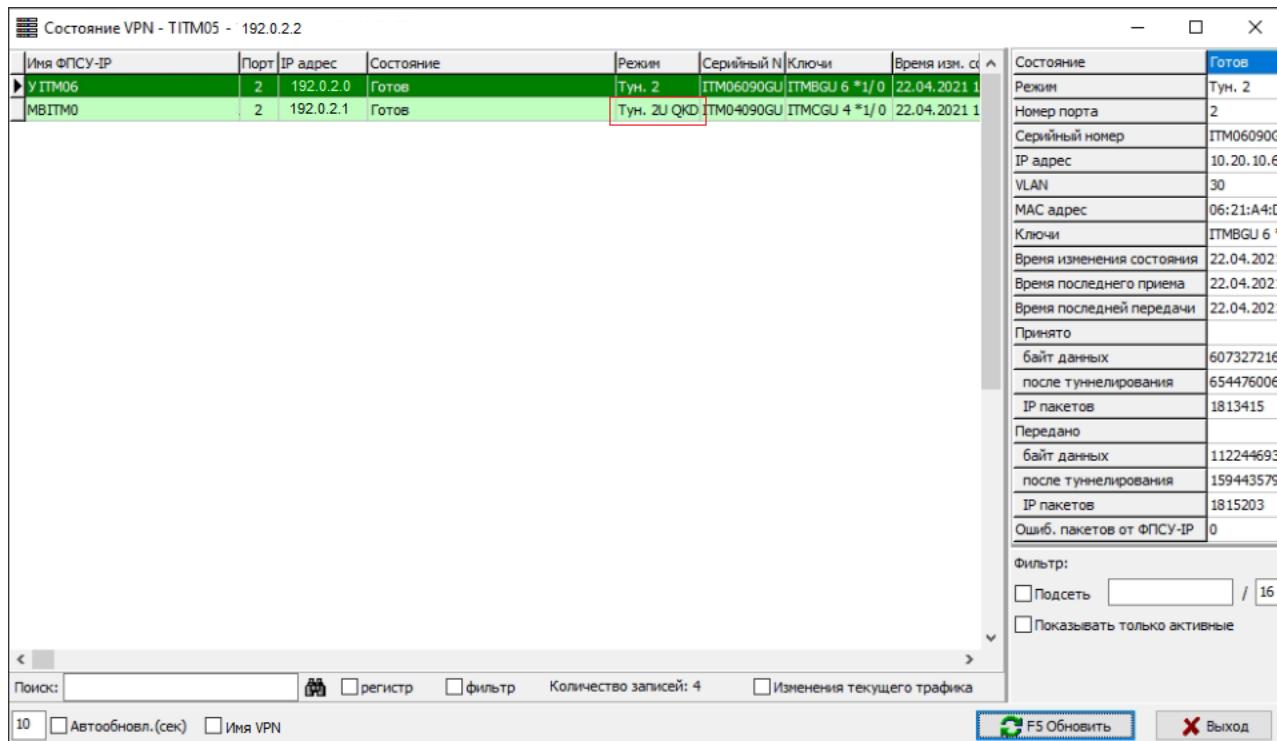


Рисунок 62 - Состояние VPN

- «Просмотр тревог» – кнопка активна при получении каких-либо сообщений от ФПСУ-IP и по нажатию выводит на экран служебное окно, которое содержит список полученных от ФПСУ-IP сообщений. Очистить список сообщений можно по нажатию кнопки «Очистить тревоги».
- «Подсистемы» – нажатие кнопки выводит на экран служебное окно, которое содержит список установленных на ФПСУ-IP подсистем и перечень полномочий, предоставленных данному администратору УА ФПСУ-IP локальным администратором ФПСУ-IP. Зеленым цветом в окне выделены установленные подсистемы и предоставленные полномочия; красный цвет указывает, что данной подсистемы нет, или данного полномочия администратор УА ФПСУ-IP не имеет.

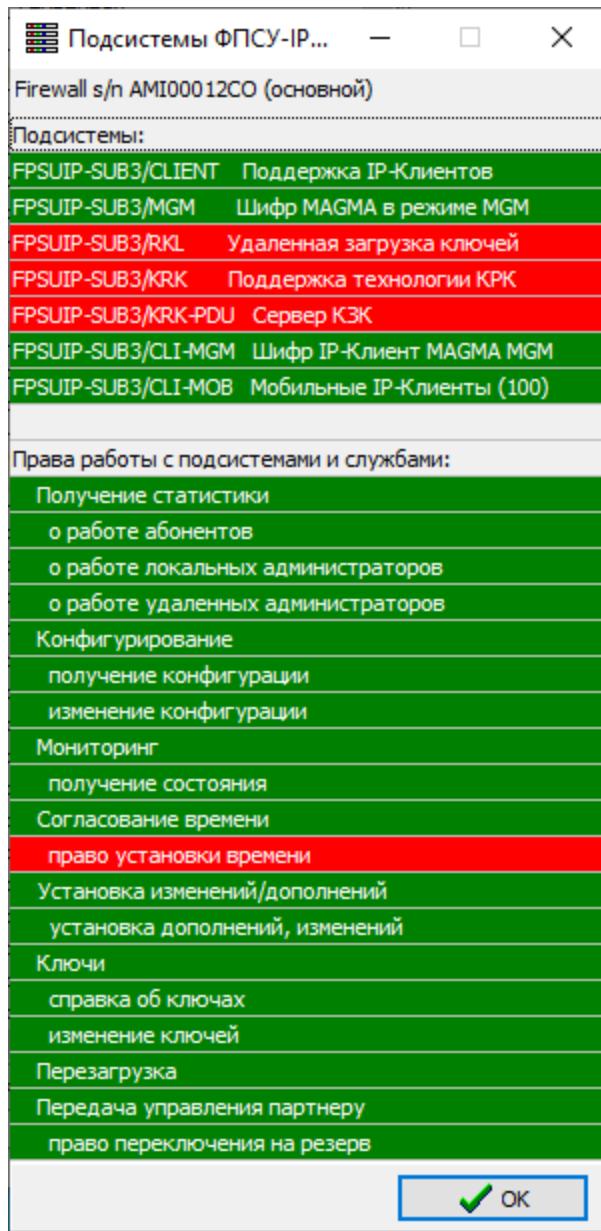


Рисунок 63 - Подсистемы ФПСУ-IP

- «Пинг от ФПСУ-IP» – переход в окно дистанционного управления служебной утилиты ping, запущенной на управляемом ФПСУ-IP (см. пункт «Дистанционный запуск ping на управляемом ФПСУ-IP»).
- «Сессии МЭ» – мониторинг сессий, когда межсетевой экран включен (см. пункт «Мониторинг сессий МЭ»).
- «Блокировать трафик» – мониторинг заблокированного трафика и возможность временного блокирования трафика без внесения изменений в конфигурацию

ФПСУ-IP (см. пункт «Мониторинг заблокированного трафика»).

- «Модули» – просмотр и диагностика работы подключенных модулей.

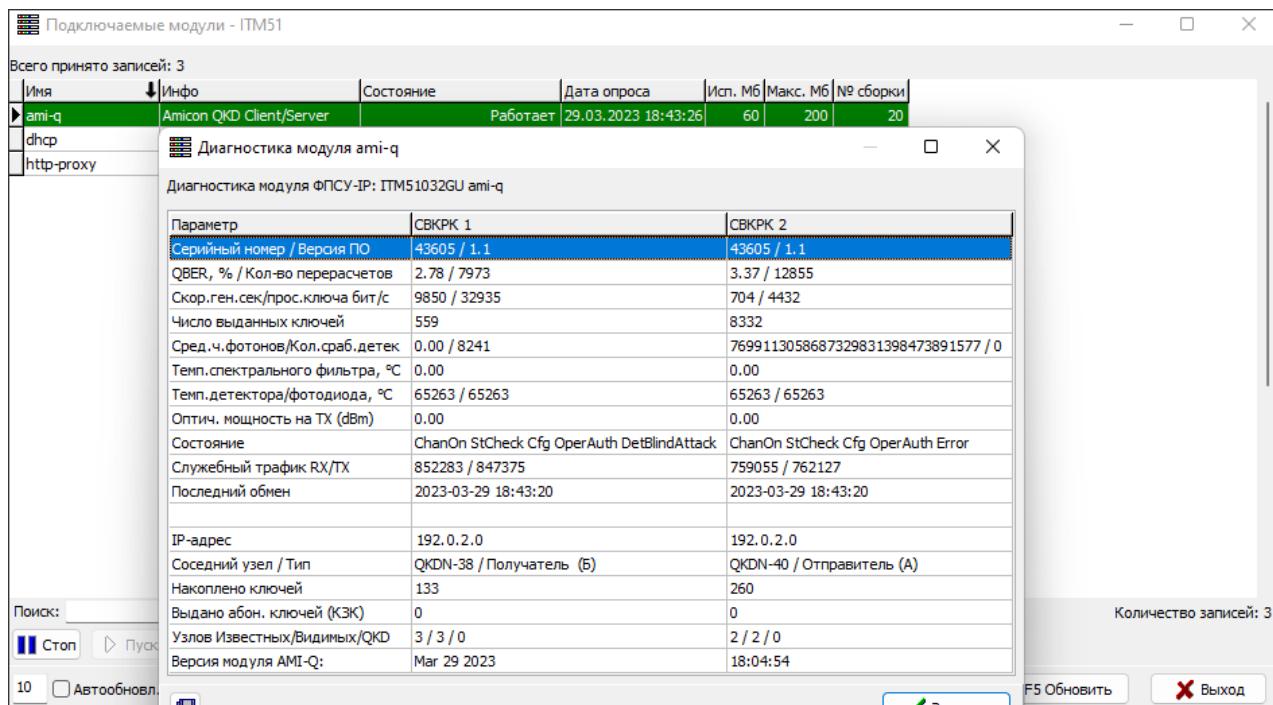


Рисунок 64 - Модули

9. 6. Поиск зарегистрированных ФПСУ-IP

Поиск можно производить по текстовому имени ФПСУ-IP (название), серийному номеру ФПСУ-IP (номер), и IP-адресу, указанному в параметрах описателя ФПСУ-IP.



Рисунок 65 - Поле поиска

Чтобы осуществить быстрый переход в поле ввода поиска ФПСУ-IP, следует нажать сочетание клавиш <Ctrl+F>.

9. 7. Завершение работы

Завершение работы с УА ФПСУ-IP осуществляется выполнением команды главного меню «ФПСУ-IP» → «Выход», на символ закрытия [X] в правой верхней части окна, или нажатием комбинации клавиш <Alt+F4>.

После завершения работы программного обеспечения УА ФПСУ-IP с VPN-Key/UA,

следует извлечь VPN-Key/UA из USB порта компьютера.

При завершении работы УА ФПСУ-IP выполняется ряд служебных задач: сохранение параметров зарегистрированных ФПСУ-IP в базе данных УА ФПСУ-IP, сохранение резервной копии УА ФПСУ-IP (если включено).

10. Защита от несанкционированного доступа

Для предотвращения доступа посторонних лиц к работе с УА ФПСУ-IP, реализовано несколько средств защиты: эксплуатация УА ФПСУ-IP только при наличии USB-ключа VPN-Key/UA, установка дополнительного пароля на вход.

10. 1. Вход в УА ФПСУ-IP по USB-ключу

При установлении соединения между ФПСУ-IP и УА ФПСУ-IP используется ключевая пара УА (состоящая из открытого и секретного ключа удаленного администратора). Эти уникальные для каждого администратора УА ФПСУ-IP данные могут храниться в VPN-Key/UA или в ПЗУ.

Без ключа администратора УА ФПСУ-IP запуск УА ФПСУ-IP и управление ФПСУ-IP невозможны; интерфейс УА ФПСУ-IP становится недоступен пользователю.

10. 2. Установка дополнительного пароля

В качестве дополнительной меры защиты от НСД, в УА ФПСУ-IP может быть установлен символный пароль на доступ к УА ФПСУ-IP, который будет запрашиваться для выполнения следующих действий: вход в УА ФПСУ-IP (начало работы), изменение пароля, внесение изменений в работу с VPN-Key/UA, изменение имени администратора, отмена пароля.

Для установки пароля необходимо выполнить команду главного меню «Параметры» → «Дополнительный пароль для запуска АРМ УА» → «Установить дополнительный пароль для запуска АРМ УА».

В открывшемся окне следует ввести пароль - комбинацию из 6-15 символов, а затем подтверждение пароля. Пароль будет установлен после корректного подтверждения.

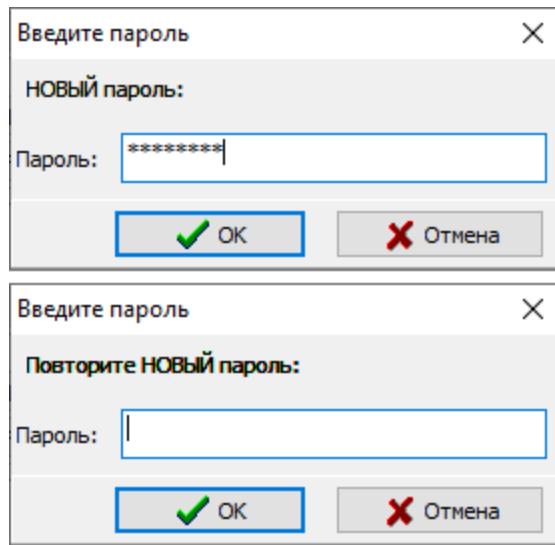


Рисунок 66 - Установка дополнительного пароля

Для отмены пароля необходимо воспользоваться командами «Параметры» → «Дополнительный пароль для запуска АРМ УА» → «Отменить пароль» и предъявить текущий пароль для подтверждения полномочий.

Для изменения пароля необходимо воспользоваться командой «Установить дополнительный пароль для запуска АРМ УА», подтвердить текущий пароль, затем дважды ввести новый.

11. Управление конфигурациями ФПСУ-IP

11. 1. Дистанционное изменение конфигурации

Дистанционное изменение конфигурации ФПСУ-IP производится администратором УА ФПСУ-IP в три этапа:

- получение текущей конфигурации ФПСУ-IP;
- редактирование параметров полученной конфигурации средствами УА ФПСУ-IP;
- установка новой конфигурации на ФПСУ-IP.

Получение конфигурации и передача измененной конфигурации на ФПСУ-IP могут производиться как по сети, в режиме непосредственного соединения, так и посредством внешних носителей, что может быть удобно при неполадках в сети или ввиду требований политики безопасности. Изменение конфигурации происходит с помощью встроенного редактора.

Для работы с конфигурациями подконтрольных ФПСУ-IP необходимо выбрать последовательность команд «Конфигурации» → «Список конфигураций ФПСУ-IP», либо нажать комбинацию клавиш <Ctrl+L>.

На экране появится окно «Список конфигураций», содержащее список описателей ФПСУ-IP, конфигурационные данные которых уже были получены и загружены в базу данных УА ФПСУ-IP. Если конфигурация ФПСУ-IP была изменена администратором УА ФПСУ-IP после загрузки в локальную базу данных, то в поле «Изменена» отмечается дата произведенных изменений.

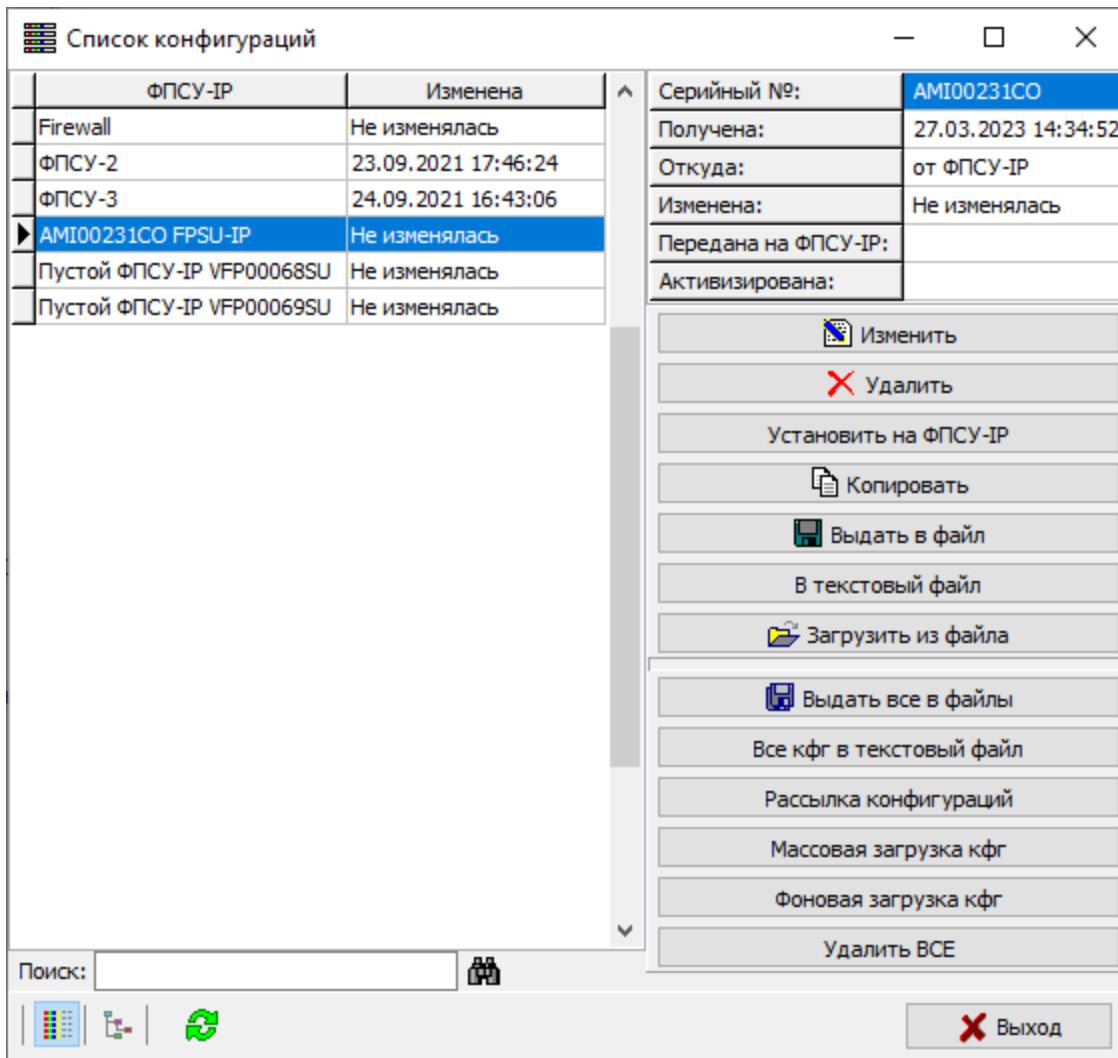


Рисунок 67 - Список конфигураций ФПСУ-IP на УА ФПСУ-IP

Кнопки в правой части окна списка конфигураций ФПСУ-IP отображают возможности администратора по работе с ними:

- просмотр и изменение конфигурационных параметров выбранного ФПСУ-IP по нажатию кнопки «Изменить» или клавиши «Enter» (см. пункт «Обновление УА ФПСУ-IP»);
- удаление данных о конфигурации выбранного ФПСУ-IP по нажатию кнопки «Удалить» или клавиши «Del»;
- переход в режим соединения с выбранным ФПСУ-IP и передача ему команды на установку измененной конфигурации по нажатию кнопки «Установить на ФПСУ-IP» или комбинации клавиш «Ctrl+Enter» (эта операция становится доступной

только в том случае, если администратор производил изменение полученной конфигурации и если УА ФПСУ-IP установил соединение с ФПСУ-IP);

- перенос, по нажатию кнопки «Копировать», конфигурационных настроек выбранного ФПСУ-IP на другой без установки, скопированная конфигурация появляется в списке как новая для другого ФПСУ-IP. Внимание! Для дальнейшей редакции скопированной конфигурации версии программного обеспечения ФПСУ-IP должны совпадать;
- запись конфигурации на внутренний накопитель УА ФПСУ-IP или внешний носитель, во внутреннем формате ФПСУ-IP по нажатию кнопки «Выдать в файл» или комбинации клавиш «Alt+F». Можно выдать в файлы все записи, хранящиеся в базе данных УА ФПСУ-IP с помощью кнопки «Выдать все в файлы»;
- запись конфигурации ФПСУ-IP в текстовом виде в файл по нажатию кнопки «В текстовый файл» или комбинации клавиш «Alt+T» для обработки ее сторонней программой, или для печати. Можно выдать в текстовом виде все конфигурации, хранящиеся в базе данных УА ФПСУ-IP с помощью кнопки «Все кфг в текстовый файл»;
- загрузка конфигурационных установок ФПСУ-IP из файла на внутреннем накопителе рабочей станции УА ФПСУ-IP, или с внешнего носителя по нажатию кнопки «Загрузить из файла»;
- вызов задачи массовой установки конфигураций на управляемые ФПСУ-IP по кнопке «Рассылка конфигураций» (подробнее см. пункт «Дистанционная массовая установка конфигураций»);
- загрузка конфигураций ФПСУ-IP в базу данных УА ФПСУ-IP по нажатию кнопки «Массовая загрузка кфг»;
- вызов задачи массовой загрузки конфигураций ФПСУ-IP в базу данных УА ФПСУ-IP по нажатию кнопки «Фоновая загрузка кфг» (подробнее см. пункт «Массовая и фоновая загрузка конфигураций»);
- удаление всех находящихся в базе данных УА ФПСУ-IP конфигураций по нажатию кнопки «Удалить ВСЕ».

Также из контекстного меню отдельной выбранной конфигурации администратору доступны дополнительные опции:

- изменение версии хранящейся конфигурации;
- выдача списка разрешенных к взаимодействию с ФПСУ-IP в конфигурации

клиентов. Список выдается в указанный каталог, в текстовый файл «Серийный_Номер_ФПСУ_CliList.txt»;

- переход в архив конфигураций для ФПСУ-IP выбранного серийного номера (подробнее см. пункт «Архивы конфигураций ФПСУ-IP»).

11. 2. Загрузка конфигурации ФПСУ-IP на УА ФПСУ-IP

11. 2. 1. Загрузка конфигурации из файла

Для загрузки полученных от локальных администраторов ФПСУ-IP конфигураций со внешнего носителя, внутреннего накопителя рабочей станции УА ФПСУ-IP или с сетевого диска необходимо выполнить следующую последовательность действий:

1. Находясь в окне списка конфигураций, нажать клавишу «Загрузить из файла». При этом на экран будет выдано диалоговое окно выбора каталога, в котором следует указать расположение файлов с конфигурациями ФПСУ-IP:

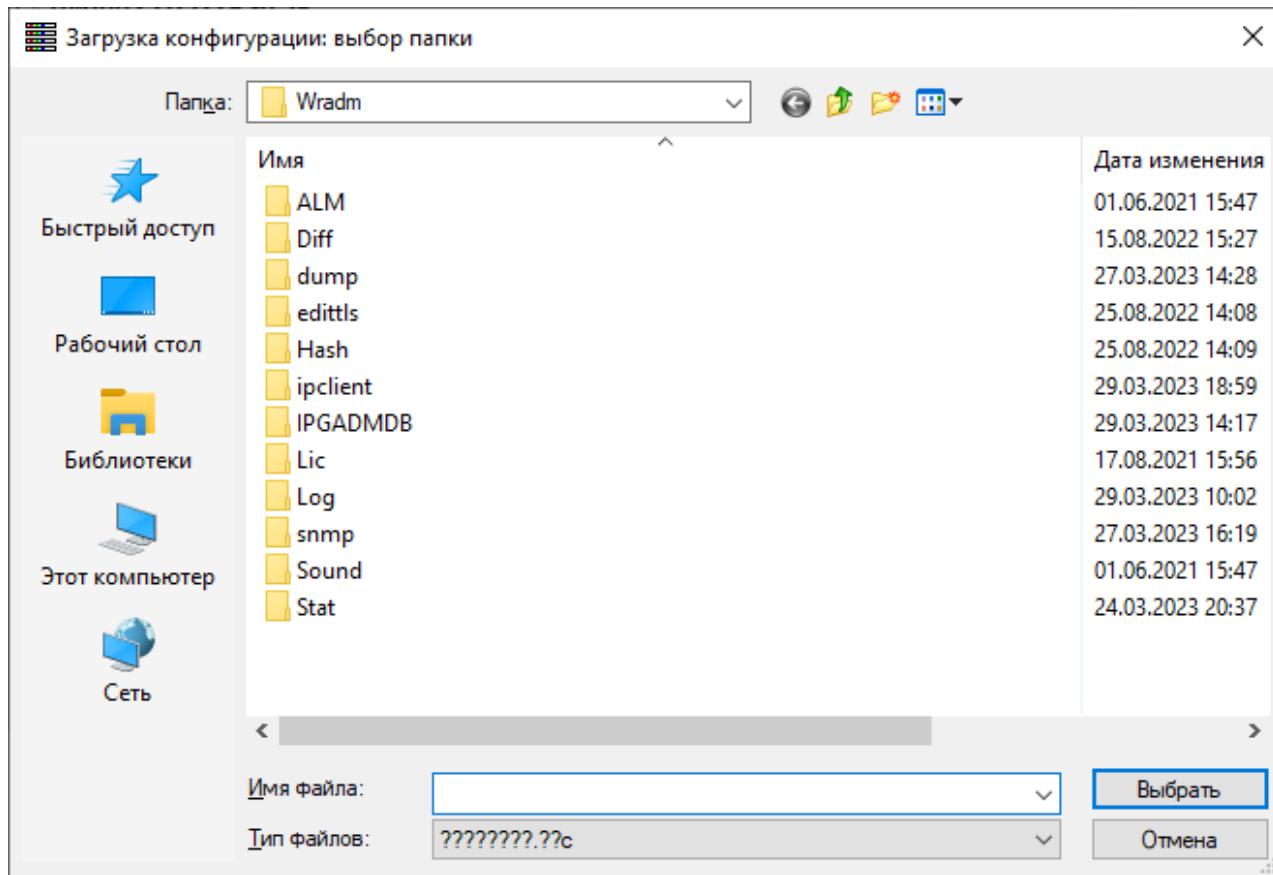


Рисунок 68 - Выбор каталога с файлами конфигураций ФПСУ-IP

2. Перейдя в требуемый каталог, нажать кнопку «Выбрать» для поиска в нем файлов конфигураций ФПСУ-IP, зарегистрированных в УА ФПСУ-IP. Если они присутствуют в указанном каталоге, на экран будет выдано окно загрузки конфигурации в базу данных УА ФПСУ-IP:

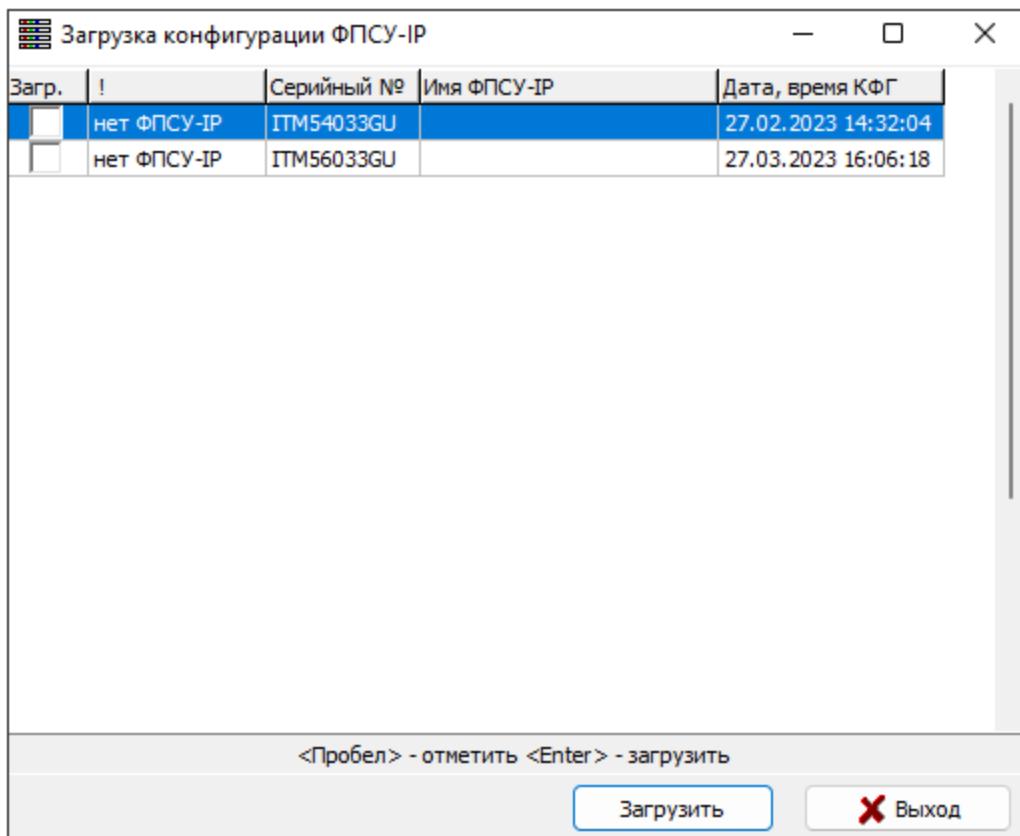


Рисунок 69 - Загрузка конфигураций ФПСУ-IP

3. В окне будет содержаться список всех найденных в каталоге конфигурационных данных, с указанием имени и серийного номера ФПСУ-IP, к которому относится найденная конфигурация, а также датой и временем ее создания. При помощи двойного нажатия левой клавиши «мыши» или клавиши «Пробел» требуется отметить те конфигурации, которые следует загрузить в базу данных УА ФПСУ-IP, и подтвердить действие нажатием клавиши «Enter» или кнопки «Загрузить».

Если какая-то конфигурация уже содержится в базе данных администратора, УА ФПСУ-IP выдаст сообщение с указанием времени и даты создания обоих файлов и предложит либо загрузить конфигурацию с удалением ранее содержащейся (кнопка «Да»), либо отказаться от загрузки.

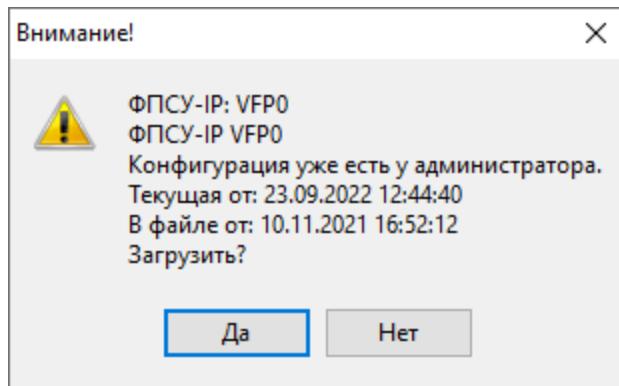


Рисунок 70 - Обновление конфигурации ФПСУ-IP

В случае отсутствия в каталоге конфигурационных данных, УА ФПСУ-IP выдаст предупреждение:

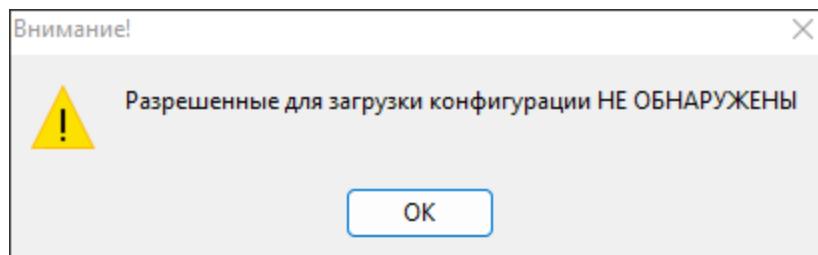


Рисунок 71 - Сообщение об отсутствии конфигураций

Если ФПСУ-IP, к которому относится найденная конфигурация, не зарегистрирован в УА ФПСУ-IP, на экран будет выведено предложение о создании пустого ФПСУ-IP (описание пустых ФПСУ-IP представлено в разделе «Регистрация пустых ФПСУ-IP»):

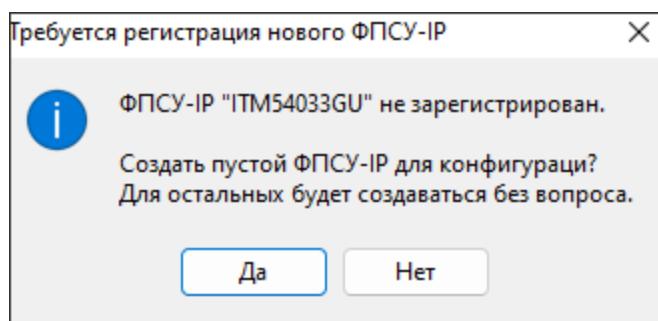


Рисунок 72 - предложение о создании пустого ФПСУ-IP

11. 2. 2. Получение конфигурации с ФПСУ-IP

Конфигурация ФПСУ-IP может быть получена администратором УА ФПСУ-IP через сеть передачи данных, в режиме непосредственного соединения с ФПСУ-IP. Следует обратить внимание на то, что эта операция возможна только в том случае, если администратору УА ФПСУ-IP при регистрации на ФПСУ-IP было предоставлено право на получение конфигурации (см. документ *Криптотомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4.0.1. Руководство администратора*).

Для соединения с ФПСУ-IP необходимо перейти в режим ручного управления, выбрав его в списке основного окна и нажав клавишу «Enter» или кнопку «Ручное управление», или сочетание клавиш <Ctrl+G>. Кнопка будет доступна только в том случае, если успешно установлено защищенное соединение ФПСУ-IP — УА ФПСУ-IP. После нажатия кнопки появляется окно ручного управления выбранным ФПСУ-IP.

В окне отображаются: серийный номер ФПСУ-IP, его имя, состояние VPN-соединения с УА ФПСУ-IP, режим функционирования (основной/резервный), количество принятых записей статистики и список операций по дистанционному управлению, доступных данному администратору УА ФПСУ-IP (в соответствии с правами, предоставленными ему локальным администратором ФПСУ-IP при регистрации).

Если администратор УА ФПСУ-IP имеет право на получение текущей конфигурации ФПСУ-IP, то в разделе «Конфигурация» окна ручного управления будет доступна клавиша «Получить», по нажатию которой текущая конфигурация ФПСУ-IP будет получена и загружена в базу данных УА ФПСУ-IP.

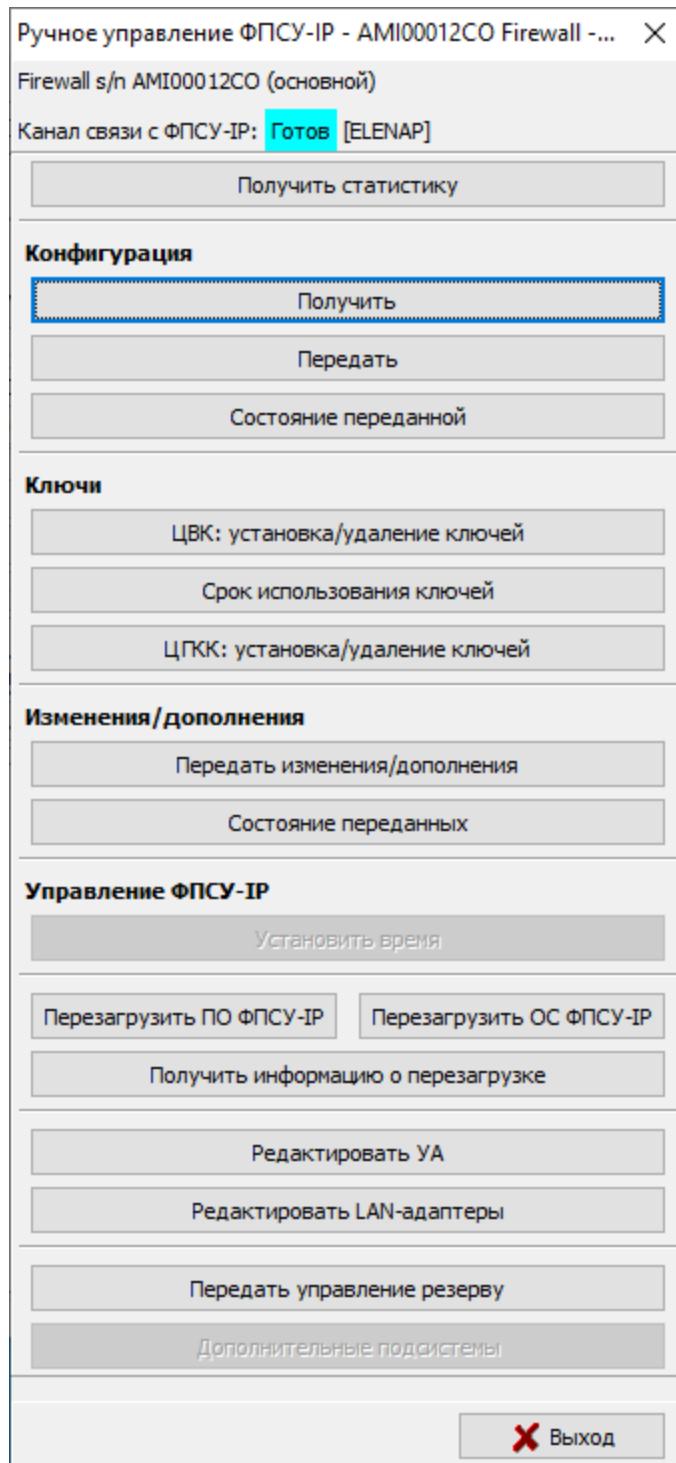


Рисунок 73 - Получение конфигурации через ручное управления ФПСУ-IP

11. 2. 3. Массовая и фоновая загрузка конфигураций

Загрузка конфигураций более чем с одного ФПСУ-IP возможна двумя способами — массовая и фоновая загрузка конфигураций, обе опции доступны из окна выбора конфигураций ФПСУ-IP, которое открывается при выборе последовательности команд «Конфигурации» → «Список конфигураций ФПСУ-IP», либо нажатием комбинации клавиш <Ctrl+L>.

Окно управления массовой загрузкой конфигураций сразу с нескольких ФПСУ-IP вызывается по кнопке «Массовая загрузка кфг» из окна выбора конфигураций ФПСУ-IP.

Администратор может отметить знаком [X] ФПСУ-IP из списка. Задание на загрузку конфигураций с отмеченных ФПСУ-IP устанавливается нажатием кнопки <Загрузить>, в результате чего УА ФПСУ-IP начнет последовательно устанавливать соединения с отмеченными ФПСУ-IP и загружать с них конфигурации в локальную базу данных.

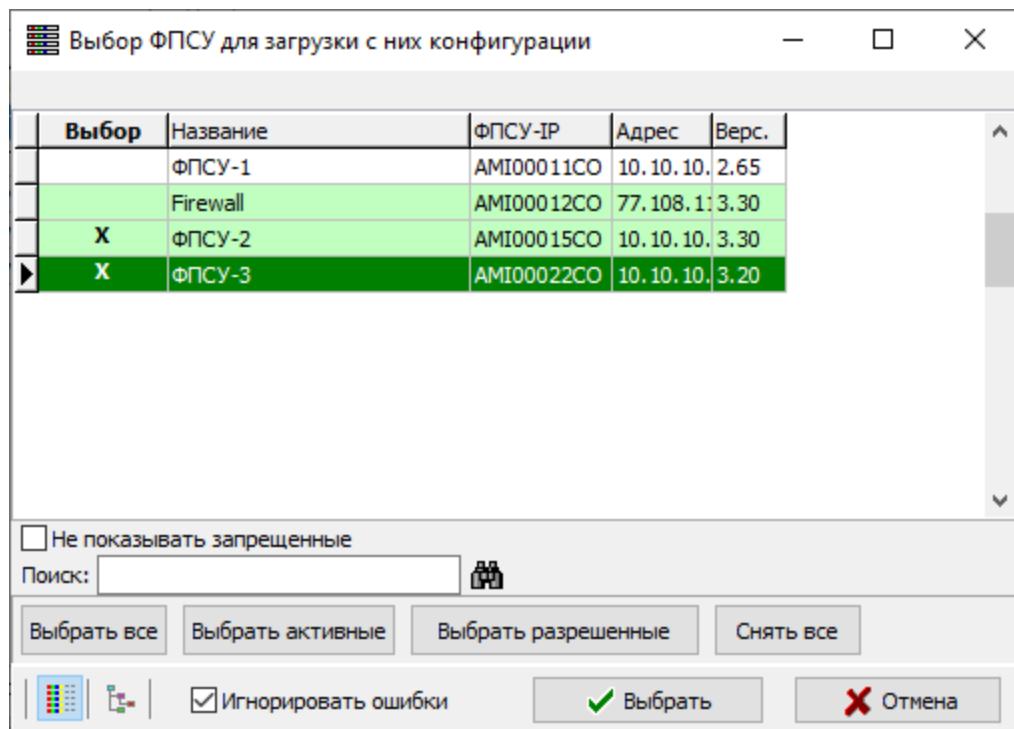


Рисунок 74 - Окно массовой загрузки конфигураций с ФПСУ

Управление интерфейсом этого окна:

- опция «Не показывать запрещенные» скрывает из списка те ФПСУ-IP, в параметрах которых не установлен флаг «Работа разрешена»;
- кнопка «Выбрать все» отмечает [X] все записи из списка зарегистрированных

ФПСУ-IP;

- кнопка «Выбрать активные» отмечает [X] все записи ФПСУ, с которыми в данный момент установлено соединение;
- кнопка «Выбрать разрешенные» отмечает [X] записи всех ФПСУ-IP, в параметрах которых администратором УА ФПСУ-IP выставлена опция «Работа разрешена»;
- кнопка «Снять все» отменяет все ранее отмеченные [X] записи ФПСУ-IP;
- переключатель «Игнорировать ошибки». По умолчанию, конфигурации из списка отмеченных ФПСУ-IP загружаются последовательно, в случае недоступности очередного ФПСУ-IP будут повторяться попытки установить с ним соединение. Выставленный переключатель означает, что, при однократной неудаче загрузки конфигурации с очередного ФПСУ-IP, УА ФПСУ-IP перейдет к следующему ФПСУ-IP по списку, не пытаясь больше загрузить с него конфигурацию и не ожидая восстановления соединения.

Для загрузки конфигураций с большого числа управляемых ФПСУ-IP рекомендуется воспользоваться фоновой загрузкой конфигураций. Окно управления фоновой загрузкой конфигураций сразу с нескольких ФПСУ-IP вызывается по кнопке «Фоновая загрузка кфг» из окна выбора конфигураций ФПСУ-IP. Интерфейс и принцип выставления задания на загрузку конфигураций — такой же, как и в «Массовой загрузке конфигураций». Отличается только механизм загрузки конфигураций с ФПСУ-IP — в случае «Фоновой» загрузки конфигурации загружаются не последовательно, а одновременно со всех доступных ФПСУ-IP.

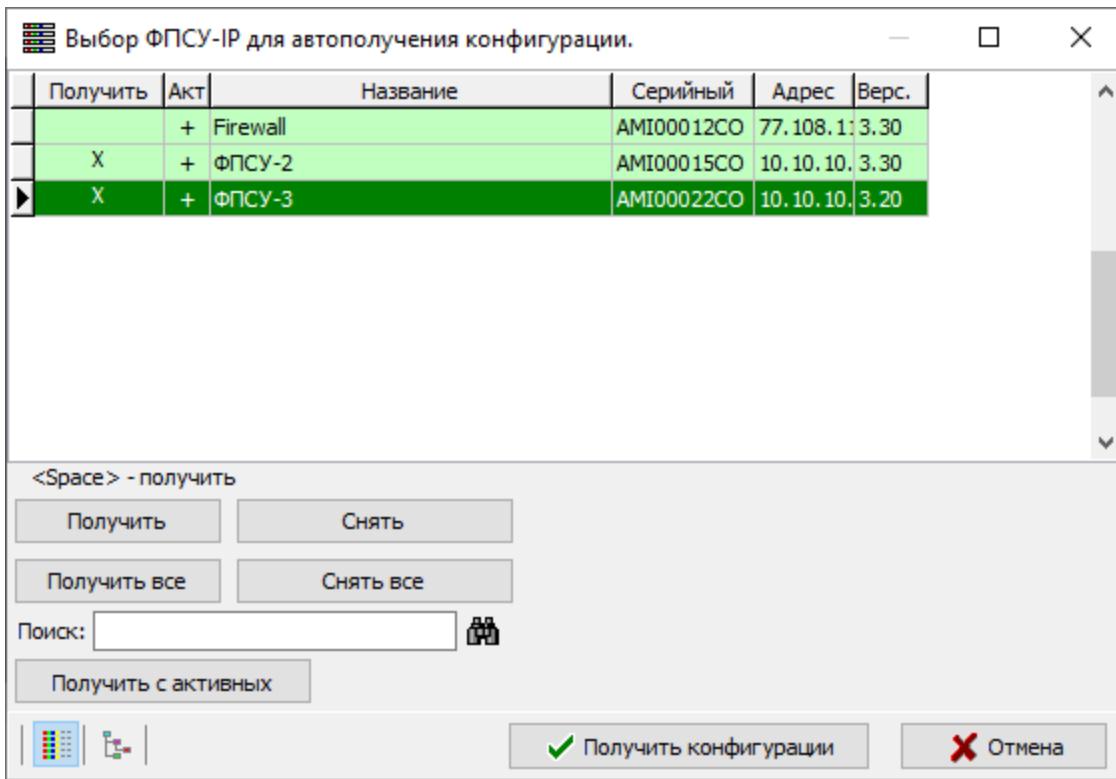


Рисунок 75 - Окно фоновой загрузки конфигураций с ФПСУ

11.2.4. Копирование конфигурации с другого ФПСУ-IP

Конфигурация для зарегистрированного ФПСУ-IP может быть получена путем копирования уже имеющейся конфигурации для другого зарегистрированного ФПСУ-IP. Следует обратить внимание на то, что для корректной работы скопированной конфигурации во внутреннем редакторе и на ФПСУ-IP, у них должны совпадать версии программного обеспечения.

Для копирования конфигурации необходимо:

- в окне «Выбор конфигураций» выбрать тот ФПСУ-IP, конфигурацию которого нужно скопировать;

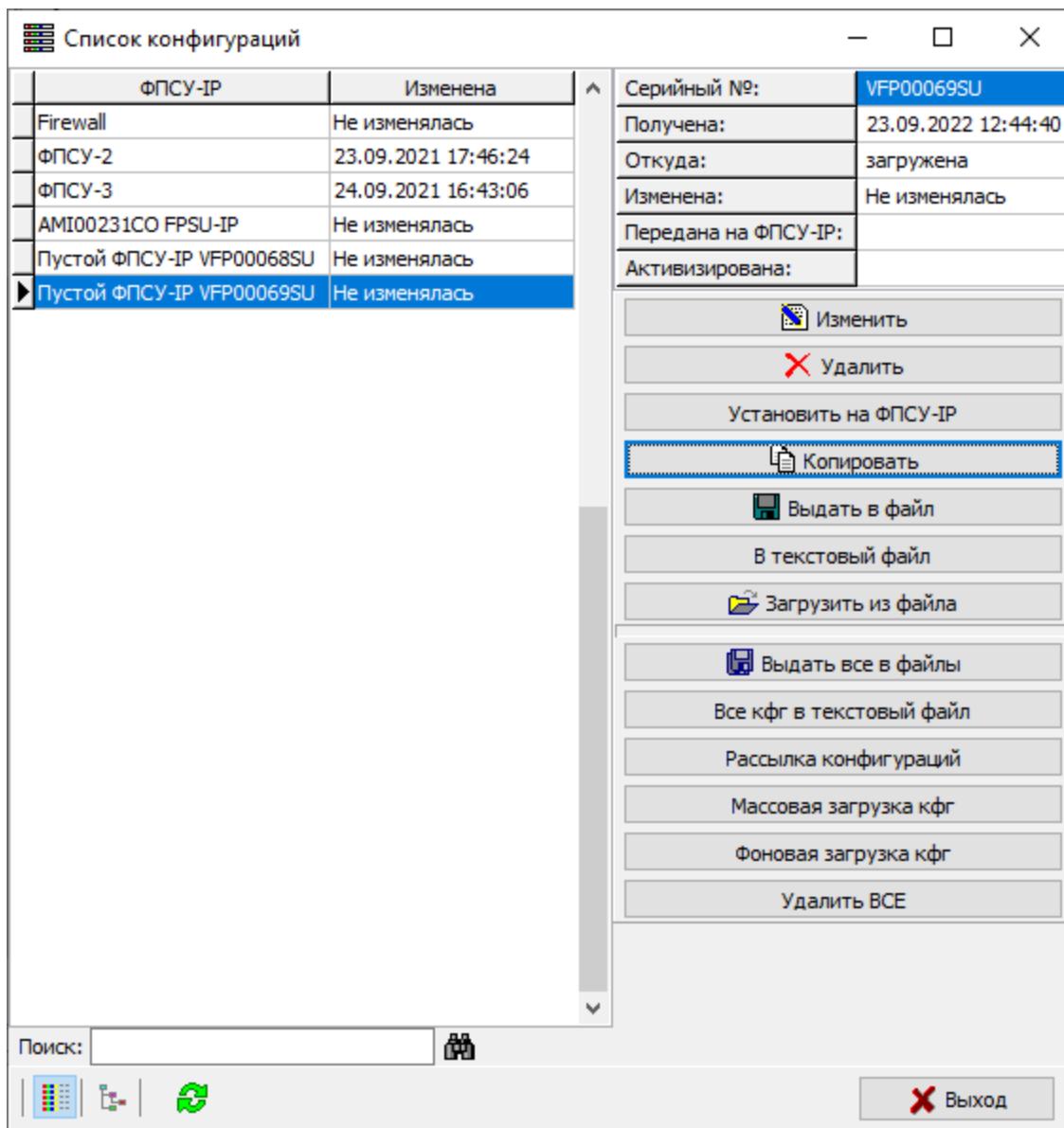


Рисунок 76 - Выбор FPCSU-IP для копирования конфигурации

- нажать кнопку «Копировать». Откроется окно, в котором требуется указать, на какой из FPCSU-IP будет копироваться существующая конфигурация и подтвердить выбор нажатием кнопки «Выбрать».

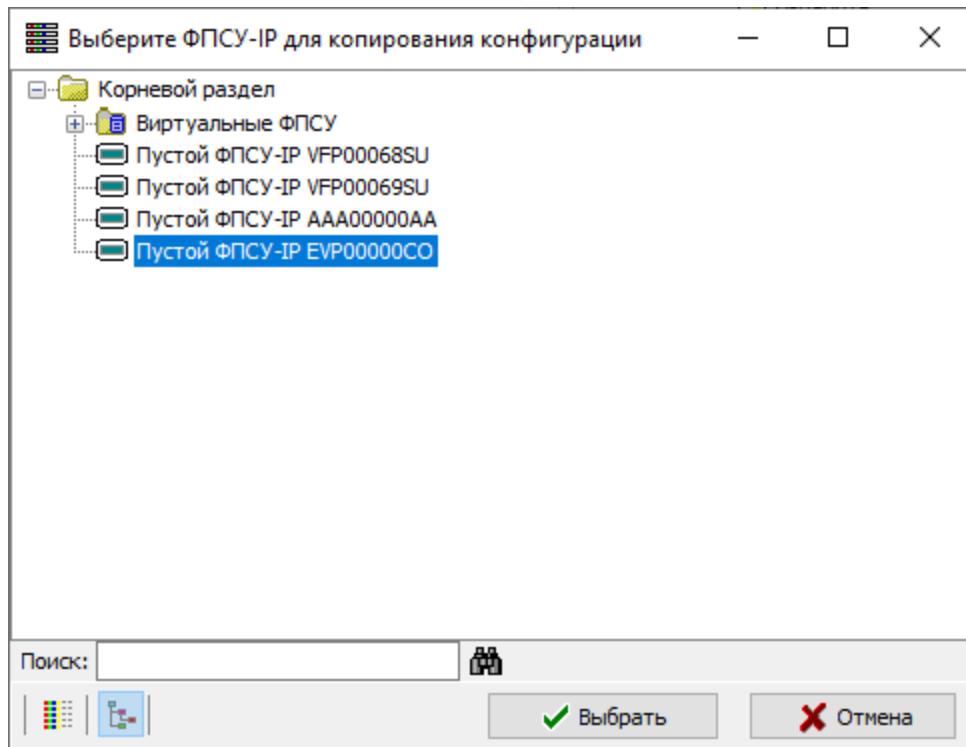


Рисунок 77 - ФПСУ-IP, на который копируется конфигурация

В окне «Список конфигураций» появится новая конфигурация, с которой можно дальше работать в обычном режиме.

11. 2. 5. Установить задание на получение конфигураций

Конфигурации ФПСУ-IP могут быть загружены списком, в этом случае формируется задание, по которому осуществляется прием конфигураций. Для создания задания массовой загрузки конфигураций на УА ФПСУ-IP необходимо выполнить команду главного меню «Конфигурации» → «Установить задание на получение конфигураций».

На экран будет выдано окно со списком ФПСУ-IP, конфигурации с которых могут быть получены.

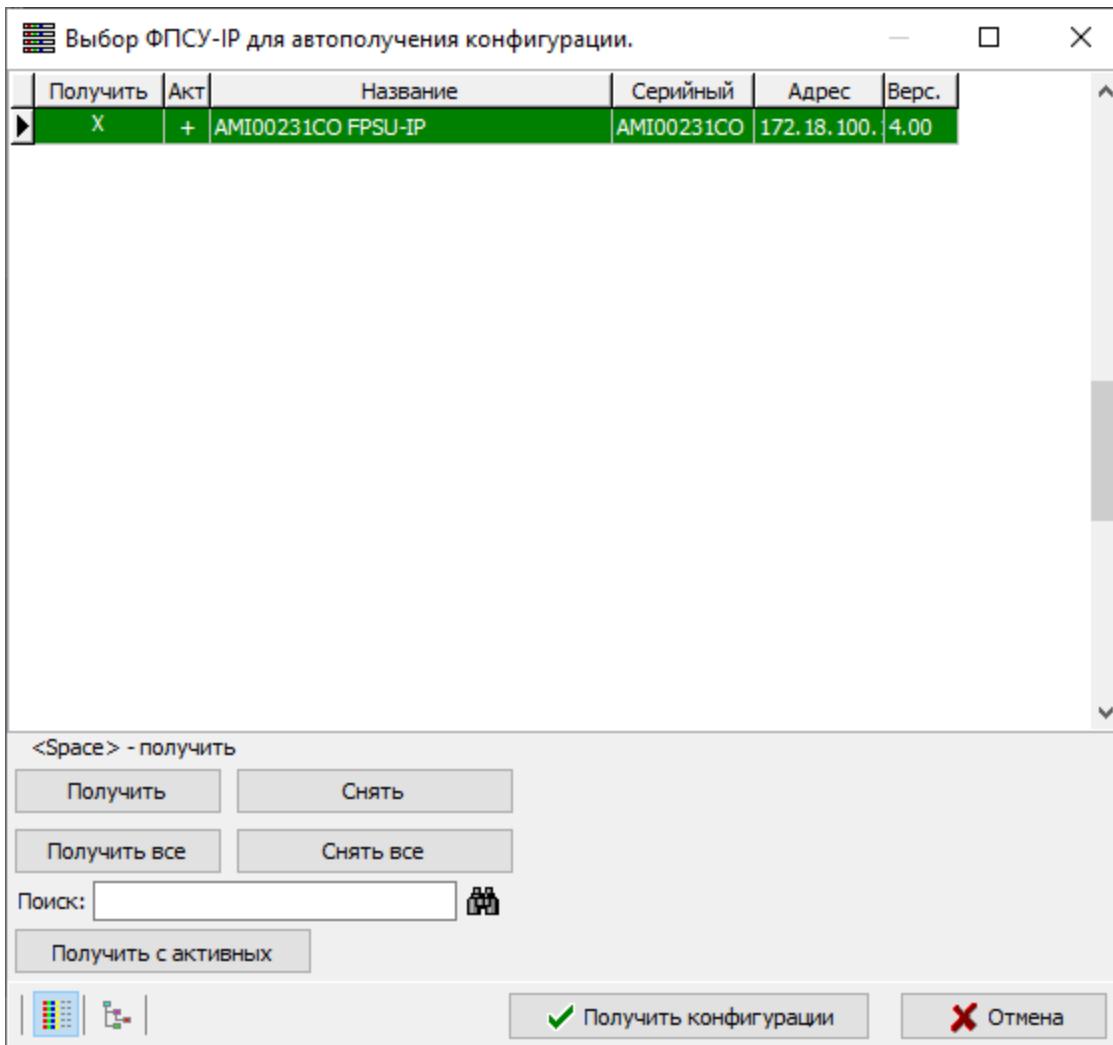


Рисунок 78 - Выбор конфигурации ФПСУ-IP

В списке необходимо отметить ФПСУ-IP знаком [X] для выбора в задание. Для этого требуется выбрать ФПСУ-IP и нажать на кнопку «Получить» или клавишу «Пробел», или нажать левой клавишей мыши в строке ФПСУ-IP в колонке «Получить».

Если выбираются конфигурации всех ФПСУ-IP из списка, следует воспользоваться кнопкой «Получить все».

Если выбираются конфигурации только активных ФПСУ-IP из списка, следует воспользоваться кнопкой «Получить с активных».

Кнопки «Снять» и «Снять все» отменяют выбор конфигурации ФПСУ-IP в задание.

После того как ФПСУ-IP выбраны и задание сформировано, необходимо нажать кнопку «Получить конфигурации».

Появится окно, в котором будет отображаться список тех ФПСУ-IP, с которых прием конфигурации запланирован, но еще не окончен.

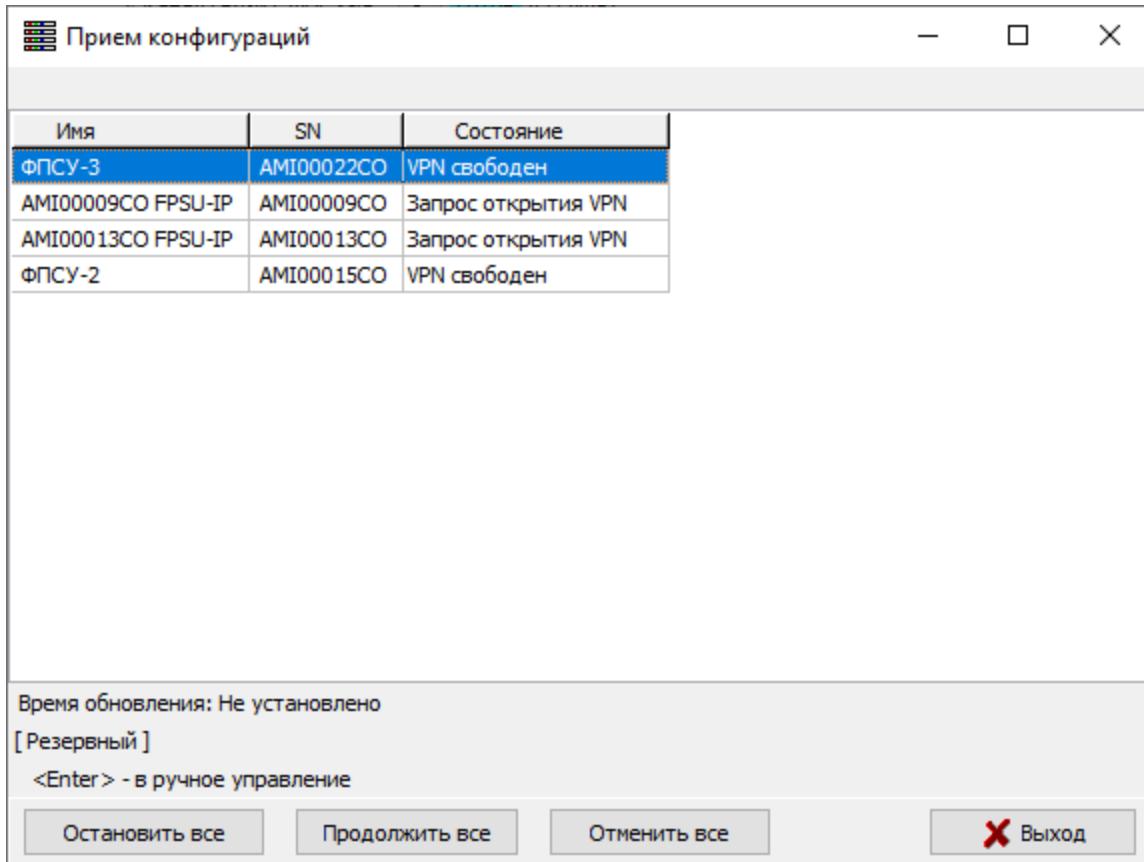


Рисунок 79 - Задание для получения с ФПСУ-IP конфигураций

Как только конфигурации будут приняты со всех отмеченных ФПСУ-IP, окно закроется, выдав служебное сообщение «Прием конфигураций с ФПСУ-IP выполнен».

Если требуется остановить (продолжить) или отменить прием конфигураций всей группе ФПСУ-IP, следует воспользоваться командами окна «Остановить все», «Продолжить все» и «Отменить все».

Нажав кнопку «Выход», можно скрыть окно передачи. При необходимости, его можно вернуть на экран, выполнив команду главного меню УА ФПСУ-IP «Конфигурации» → «Показать состояние задания».

11. 3. Просмотр и изменение конфигурации

Полученные с ФПСУ-IP конфигурации могут быть доступны в УА ФПСУ-IP в двух вариантах — текущая конфигурация и архив.

11. 3. 1. Редактирование конфигурации ФПСУ-IP

Для просмотра и редактирования конфигурационных данных ФПСУ-IP, которые были получены и загружены в хранилище УА ФПСУ-IP, используется встроенный редактор с интерфейсом ФПСУ-IP.

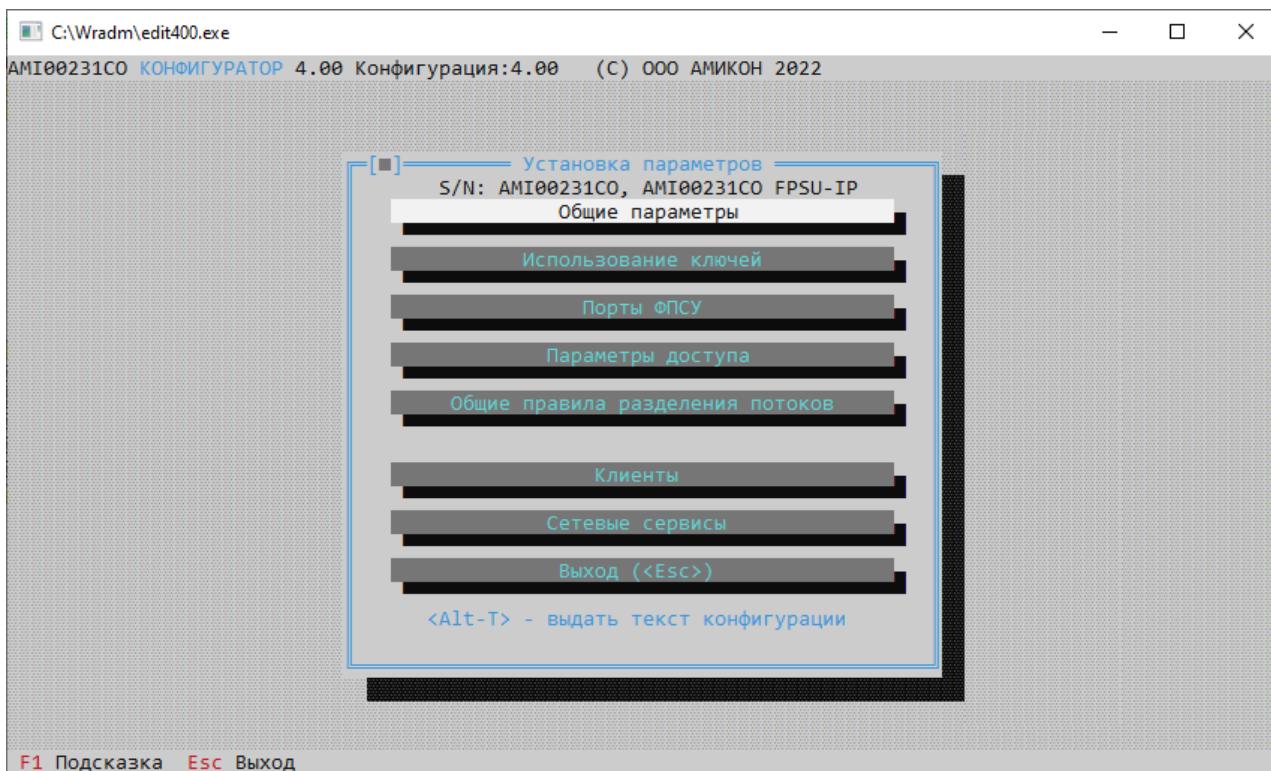


Рисунок 80 - Редактор конфигураций ФПСУ-IP

Для вызова редактора необходимо:

- выбрать нужный ФПСУ-IP из списка окна «Список конфигураций» и нажать клавишу «Enter» либо кнопку «Изменить»
- выбрать нужный ФПСУ-IP в списке основного окна УА ФПСУ-IP, и нажать кнопку «Изм. конфигурации» или сочетание клавиш <Ctrl+E>.

После выполнения любой последовательности на экране появится окно редактора конфигурации, интерфейс которого совпадает с интерфейсом ФПСУ-IP при локальном

администрировании, при настройке пунктов «Общие параметры», «Использование ключей», «Порты ФПСУ-IP», «Параметры доступа», «Общие правила разделения потоков», «Клиенты», «Сетевые сервисы». Возможности дальнейших настроек подробно описаны в документе «Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4.0.1. Руководство администратора ФПСУ-IP».

Если в процессе работы с конфигуратором администратор УА ФПСУ-IP внес изменения в настройки, после выхода из него в списке окна «Список конфигураций» поле «Изменена» будет отображать дату последнего редактирования. Если после получения конфигурации ФПСУ-IP в базу данных УА ФПСУ-IP изменения конфигурации не случалось, поле «Изменена» будет пустым.

Находясь в основном окне редактора установки параметров конфигурации, можно выдать конфигурацию (как текущую, так и измененную) в текстовом виде в каталог на внутренний накопитель УА ФПСУ-IP при помощи комбинации клавиш «Alt+T» (об этом сообщает подсказка внизу основного окна редактора). При этом УА ФПСУ-IP из интерфейса конфигуратора запросит имя каталога, в который нужно записать текстовые файлы, и путь к нему - на экран будет выдаваться окно выбора каталога. Следует обратить внимание, если выдача текста конфигурации производится на внутренний накопитель УА ФПСУ-IP, указываемый каталог должен существовать, то есть быть создан средствами операционной системы до текущего сеанса работы с УА ФПСУ-IP.



Рисунок 81 - Выбор каталога для текста конфигурации

Текст конфигурации выдается или в выбранный каталог УА ФПСУ-IP в файл с именем, образованным из серийного номера ФПСУ-IP с добавлением буквы «T» в конце расширения (например, для ФПСУ-IP с серийным номером АМ100001СО конфигурация будет выдана в текстовый файл с именем АМ100001.COT). Такой файл может быть прочитан и обработан (в частности, распечатан) средствами любого текстового редактора, поддерживающего кодировку OEM/DOS.

11. 3. 2. Архивы конфигураций ФПСУ-IP

Архивы конфигураций ФПСУ-IP предназначены для хранения всех конфигураций, полученных с управляемых ФПСУ-IP, которые изменились администратором УА ФПСУ-IP. После каждого изменения в архив добавляется новая копия измененной конфигурации.

Архив конфигураций по умолчанию не задействован. Чтобы включить сохранение изменяемых конфигураций в архив, следует установить переключатель «Автоматически сохранять каждую конфигурацию ФПСУ-IP в архив». Переключатель находится во вкладке «Работа с ФПСУ-IP» окна настроек УА ФПСУ-IP, вызываемом по команде основного меню «Параметры» → «Настройки...»:

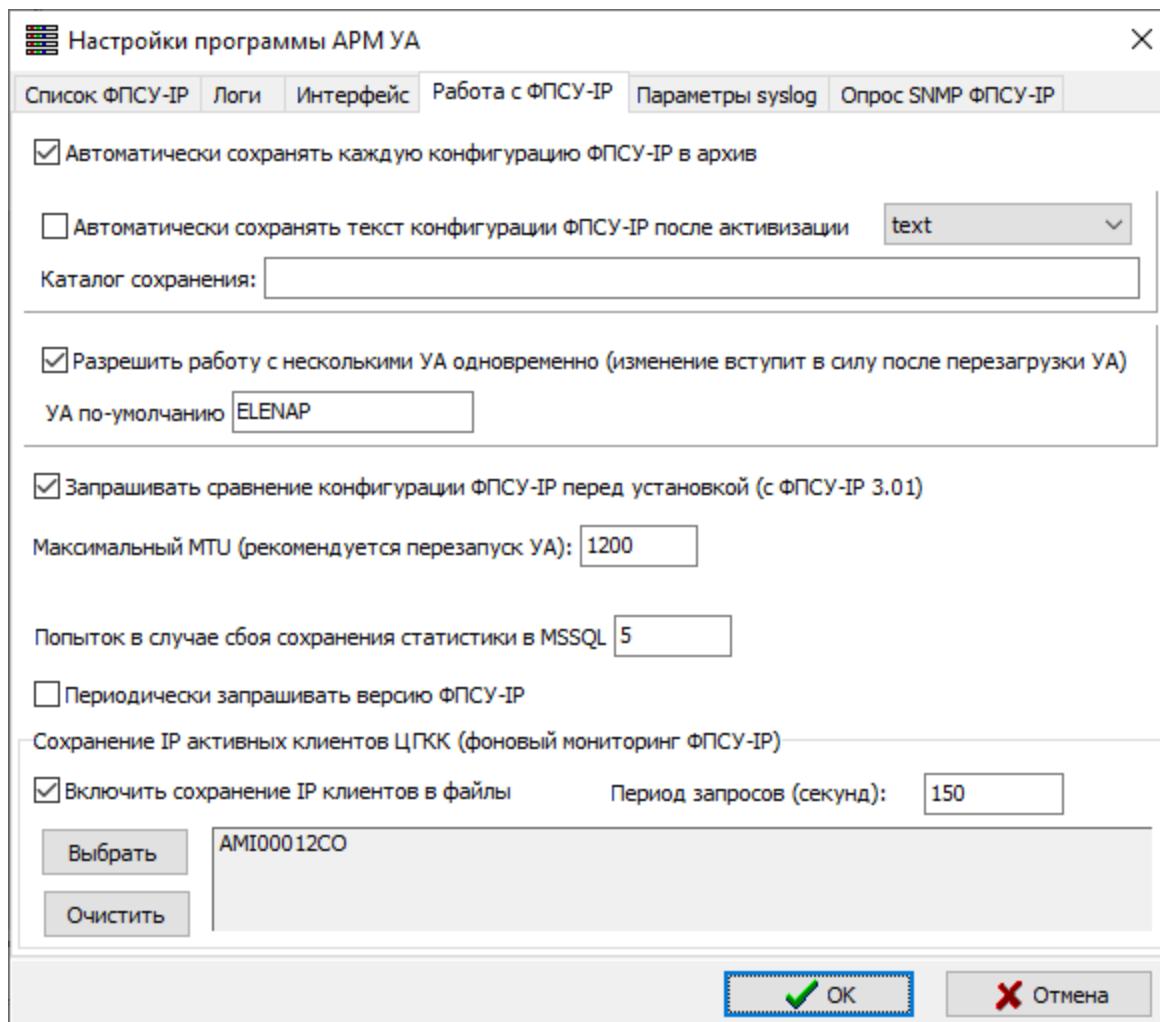


Рисунок 82 - Включение архива конфигурации ФПСУ

Архив конфигураций ведется для каждого ФПСУ-IP отдельно и доступен из контекстного меню выбранного ФПСУ-IP основного окна, команда «Конфигурация → Архив конфигураций» и команды контекстного меню «Архив конфигураций» отдельной конфигурации в окне «Список конфигураций» (см. пункт «Дистанционное изменение конфигурации»).

Если конфигурация не изменялась, архив будет пустой, иначе в нем будут храниться все измененные администратором УА ФПСУ-IP конфигурации выбранного ФПСУ-IP:

Архив конфигураций ФПСУ-IP - AMI00231CO AMI00231CO FPSU-IP - 172.18.100.1										
SN	Дата архива	Верс кфг	Причина	Комент.	Время получ. кфг	Изм. на ФПСУ-IP	Изм. админом	Конфиг байт	Всего байт	Пользователь
AMI00231CO	27.03.2023 14:34:51	4.00	Загружена с ФПСУ-IP		27.03.2023 14:34:	27.03.2023 14:27	27.03.2023 14:34:	1742	1878	ELENAP
AMI00231CO	05.04.2023 11:03:14	4.00	Загружена с ФПСУ-IP		05.04.2023 11:03:	28.03.2023 16:11	05.04.2023 11:03:	1786	1922	ELENAP
AMI00231CO	05.04.2023 11:03:55	4.00	Загружена с ФПСУ-IP		05.04.2023 11:03:	28.03.2023 16:11	05.04.2023 11:03:	1786	1922	ELENAP
AMI00231CO	05.04.2023 11:04:37	4.00	Загружена с ФПСУ-IP		05.04.2023 11:04:	28.03.2023 16:11	05.04.2023 11:04:	1786	1922	ELENAP
► AMI00231CO	05.04.2023 12:21:32	4.00	Загружена с ФПСУ-IP		05.04.2023 12:21:	28.03.2023 16:11	05.04.2023 12:21:	1786	1922	ELENAP

Записей в архиве: 5
Всего записей: 64 Размер Бд: 0МБ

Обновить Выход

Рисунок 83 - Архив конфигураций отдельного ФПСУ-IP

Для каждой сохраненной версии конфигурации ФПСУ-IP доступны следующие действия:

- сравнить выбранную конфигурацию с текущей;
- изменить комментарий — дополнительно устанавливаемое администратором текстовое пояснение для сохраненной копии конфигурации;
- выдать архивную конфигурацию в отдельный файл для указанного серийного номера ФПСУ-IP;
- загрузить из указанного файла конфигурацию ФПСУ-IP в архив;
- сделать конфигурацию текущей для дальнейшей работы с ней в УА ФПСУ-IP. Текущая конфигурация становится основной для редактирования и установки на управляемый ФПСУ-IP;
- переход к ФПСУ-IP;
- удалить выбранную версию архивной конфигурации или все хранящиеся в архиве конфигурации текущего ФПСУ-IP.

Кнопка «Обновить» окна архива конфигураций предназначена для повторного считывания из базы данных УА ФПСУ-IP списка хранящихся версий конфигурации данного ФПСУ-IP (обновления списка архивных конфигураций).

11. 4. Установка измененной конфигурации на ФПСУ-IP

11. 4. 1. Выдача конфигурации в файл

Конфигурации ФПСУ-IP могут быть выданы из базы данных УА ФПСУ-IP во внутреннем формате в файл, с целью резервного хранения или последующей установки на ФПСУ-IP (средствами локального администратора).

Для записи конфигурации в файл внутреннего формата, в окне «Список конфигураций» необходимо отметить нужный ФПСУ-IP и нажать кнопку «Выдать в файл».

После нажатия на кнопку УА ФПСУ-IP запросит серийный номер ФПСУ-IP, для которого выдается конфигурация. Если отредактированная конфигурация передается на тот же ФПСУ-IP, от которого она была получена, следует нажать «Enter» или кнопку «OK». Если же в поле запроса ввести серийный номер другого зарегистрированного данным администратором ФПСУ-IP, УА ФПСУ-IP выдаст конфигурационные данные в файл, из которого они могут быть установлены на ФПСУ-IP с введенным серийным номером. Следует обратить внимание, что для корректной установки конфигурации на другой ФПСУ-IP у них должны совпадать версии программного обеспечения.

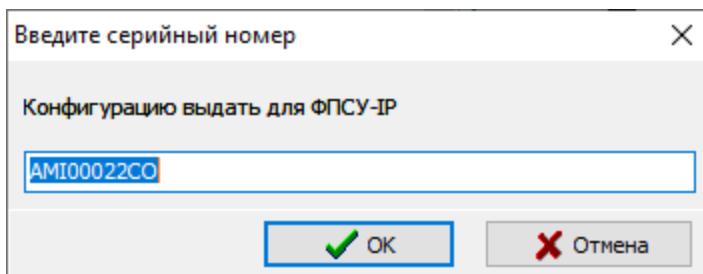


Рисунок 84 - Указание серийного номера ФПСУ-IP

После указания серийного номера, УА ФПСУ-IP вызовет окно выбора каталога, в который нужно записать файл с конфигурацией.

Конфигурация выдается в указанный каталог, создавая файл с именем, образованным из выбранного серийного номера ФПСУ-IP с расширением .SOC (например, для ФПСУ-IP с серийным номером AMI00022CO конфигурация будет выдана в файл с именем AMI00022.SOC).

11. 4. 2. Дистанционная установка конфигурации на ФПСУ-IP

Отредактированная администратором УА ФПСУ-IP конфигурация может быть дистанционно установлена на подконтрольный ФПСУ-IP по сети передачи данных. Эта операция возможна при соблюдении следующих условий:

- администратор УА ФПСУ-IP ранее загрузил конфигурацию ФПСУ-IP (по сети или с внешнего носителя) и внес в нее изменения;
- у администратора УА ФПСУ-IP в данный момент времени есть выданное локальным администратором ФПСУ-IP право на передачу конфигурации данному ФПСУ-IP;

- конфигурация ФПСУ-IP с момента ее получения не была изменена локальным администратором или другим администратором УА ФПСУ-IP;
- УА ФПСУ-IP установил соединение с ФПСУ-IP.

Для отправления измененной конфигурации на ФПСУ-IP необходимо:

- в окне списка ФПСУ-IP главного окна УА ФПСУ-IP выбрать ФПСУ-IP и нажать комбинацию клавиш <Ctrl+Enter>;
- войти в окно «Список конфигураций» (нажать <Ctrl+L> при открытом основном окне УА ФПСУ-IP). Выбрать из списка тот ФПСУ-IP, на который следует передать измененную конфигурацию. Нажать комбинацию клавиш <Ctrl+Enter> или кнопку «Установить на ФПСУ»;
- вызвать окно режима ручного управления (в окне списка выбрать ФПСУ-IP и нажать клавишу «Enter» или кнопку «Ручное управление» на панели команд). В режиме ручного управления выбрать команду «Передать» в разделе «Конфигурация». Команда будет доступна только при выполнении условий 1-4 из предыдущего пункта. Если такой доступной кнопки нет в списке - возможно, с момента получения конфигурация на локальном ФПСУ-IP была изменена. Следует заново получить конфигурацию с ФПСУ-IP.

В результате выполнения любого из перечисленных выше действий появится окно подтверждения решения отправления измененной конфигурации на ФПСУ-IP. По нажатию кнопки «Да» конфигурация будет отправлена на ФПСУ-IP.

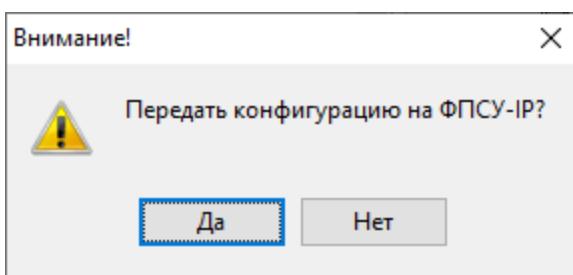


Рисунок 85 - Подтверждение передачи конфигурации

Если передача начинается и не завершается (индикатор прогресса передачи не изменяется в течение нескольких минут), то следует проверить состояние VPN-соединения между УА ФПСУ-IP и ФПСУ-IP. Если соединение активно, то следует уменьшить параметр «МТУ» для взаимодействия между УА ФПСУ-IP и данным ФПСУ-IP до 1000 (см. подраздел «Регистрация ФПСУ-IP в УА ФПСУ-IP»).

Следующий шаг состоит в активации пересланной конфигурации — то есть установки ее как основной для ФПСУ-IP. УА ФПСУ-IP, в случае успешной пересылки конфигурации, выдаст диалоговое окно, запрашивающее время активизации переданной конфигурации по часам ФПСУ-IP (дату и время суток с точностью до секунды, в которое переданная конфигурация должна вступить в силу). После ввода требуемых данных следует нажать кнопку «Установить». Кнопка «Отказ» предназначена для отмены активации переданной конфигурации.

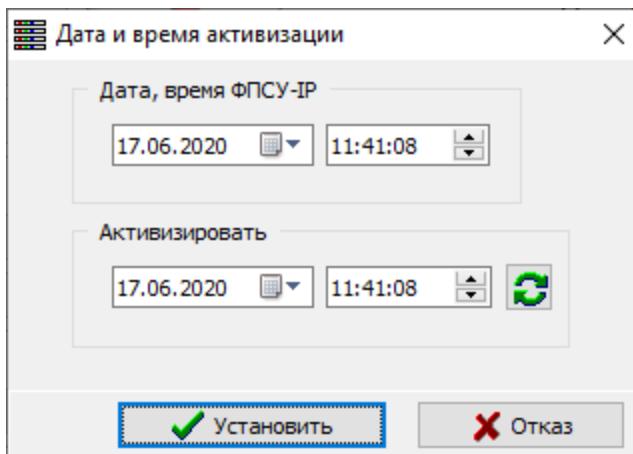


Рисунок 86 - Выбор времени активации конфигурации

Такой способ переключения на новую конфигурацию позволяет, помимо всего прочего, произвести одновременное переключение на новый набор ключевых данных, используемых сетью ФПСУ-IP (см. пункт «Дистанционная установка/удаление ключевых данных ФПСУ-IP»).

После нажатия кнопки будет выдано служебное окно с таймером активации конфигурации на ФПСУ-IP. Администратор УА ФПСУ-IP может отменить активацию, нажав в этом окне кнопку «Стоп». Если окно таймера активации конфигурации не требуется отображать на УА ФПСУ-IP дальше, следует нажать клавишу <Esc>.

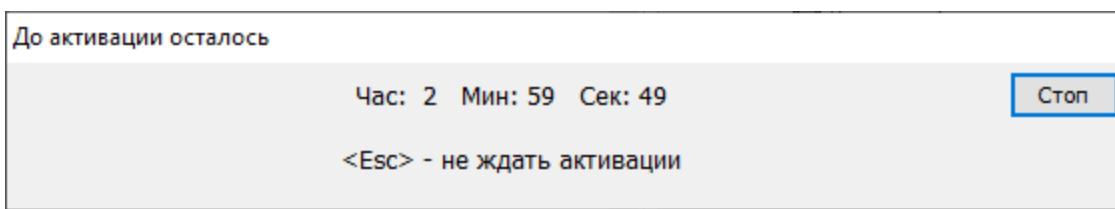


Рисунок 87 - Таймер активации конфигурации

В момент активации конфигурации на ФПСУ-IP, администратору УА ФПСУ-IP будет

отправлено сообщение об успешности или отказе операции, в последнем случае — с указанием причины ошибки активации.

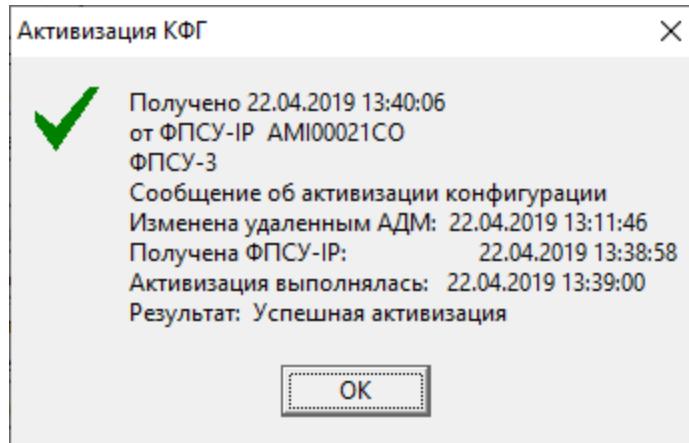


Рисунок 88 - Сообщение об успешной активации

Администратор УА ФПСУ-IP в любой момент может получить информацию о ранее переданных конфигурациях на каждый ФПСУ-IP. Для этого в режиме ручного управления необходимо нажать кнопку «Состояние переданной» в разделе «Конфигурация».

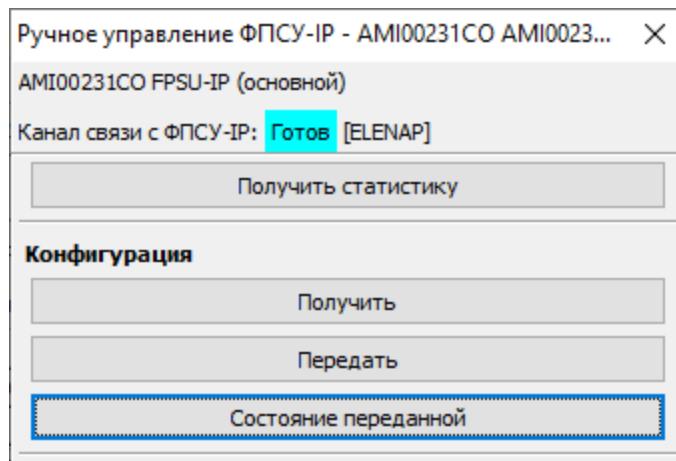


Рисунок 89 - Ручное управление ФПСУ-IP

Кнопка «Состояние переданной» будет активной только в том случае, если на ФПСУ-IP ранее передавалась конфигурация хотя бы один раз. Нажатие кнопки вызывает служебное окно с информацией о последней переданной на ФПСУ-IP конфигурации.

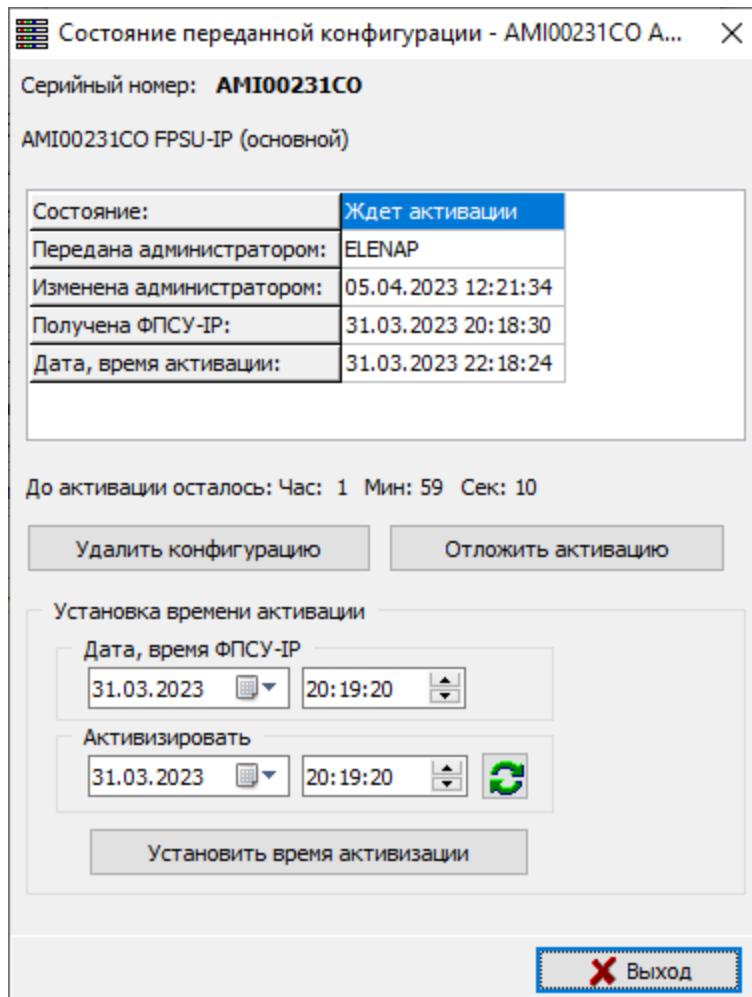


Рисунок 90 - Информация о переданной конфигурации

В окне отображается:

- состояние последней переданной конфигурации (список состояний см. ниже);
- имя администратора УА ФПСУ-IP, отправившего конфигурацию;
- дата изменения конфигурации администратором УА ФПСУ-IP;
- дата и время передачи на ФПСУ-IP;
- дата и время активации конфигурации.

В строке «Состояние» может отображаться следующая информация:

- Получена не вся — процесс приема конфигурации на ФПСУ-IP не завершен вследствие обрыва связи;

- Получена — конфигурация успешно принята, но время активизации не задано;
- Ждет активизации — конфигурация успешно принята, но время ее активизации еще не наступило;
- Активизирована — конфигурация успешно принята и вступила в силу;
- Были неполадки — в процессе активизации успешно принятой конфигурации возникли ошибки, и она не была установлена.

Если конфигурация еще не была активизирована, то окно содержит дополнительные опции управления переданной, но не активированной конфигурацией:

- <Удалить конфигурацию> — нажатие кнопки приводит к удалению переданной, но пока еще не активированной конфигурации из памяти внутреннего накопителя ФПСУ-IP;
- <Отложить активизацию> — нажатие кнопки приводит к отмене установленного времени активизации. Без повторного указания времени активизации, конфигурация не будет задействована на ФПСУ-IP;
- поле «Дата, время ФПСУ-IP», отображающее текущее время на ФПСУ-IP (которое может отличаться от локального времени на УА ФПСУ-IP);
- поле «Активизировать», с указанием времени, когда следует задействовать конфигурацию;
- <Установить время активации> - кнопка, подтверждающая новое время активации конфигурации.

11. 4. 3. Дистанционная массовая установка конфигураций

Помимо рассылки и установки измененной конфигурации на отдельный ФПСУ-IP, УА ФПСУ-IP предоставляет администратору УА ФПСУ-IP возможность создания задач массовых рассылок конфигурации. Окно управления такими задачами может быть вызвано следующими способами:

- входом в окно «Список конфигураций» (для этого необходимо нажать <Ctrl+L> при открытом основном окне УА ФПСУ-IP) и нажатием кнопки «Рассылка конфигураций»;
- выполнением команды главного меню УА ФПСУ-IP «Конфигурации» → «Установить задание автообновления конфигурации».

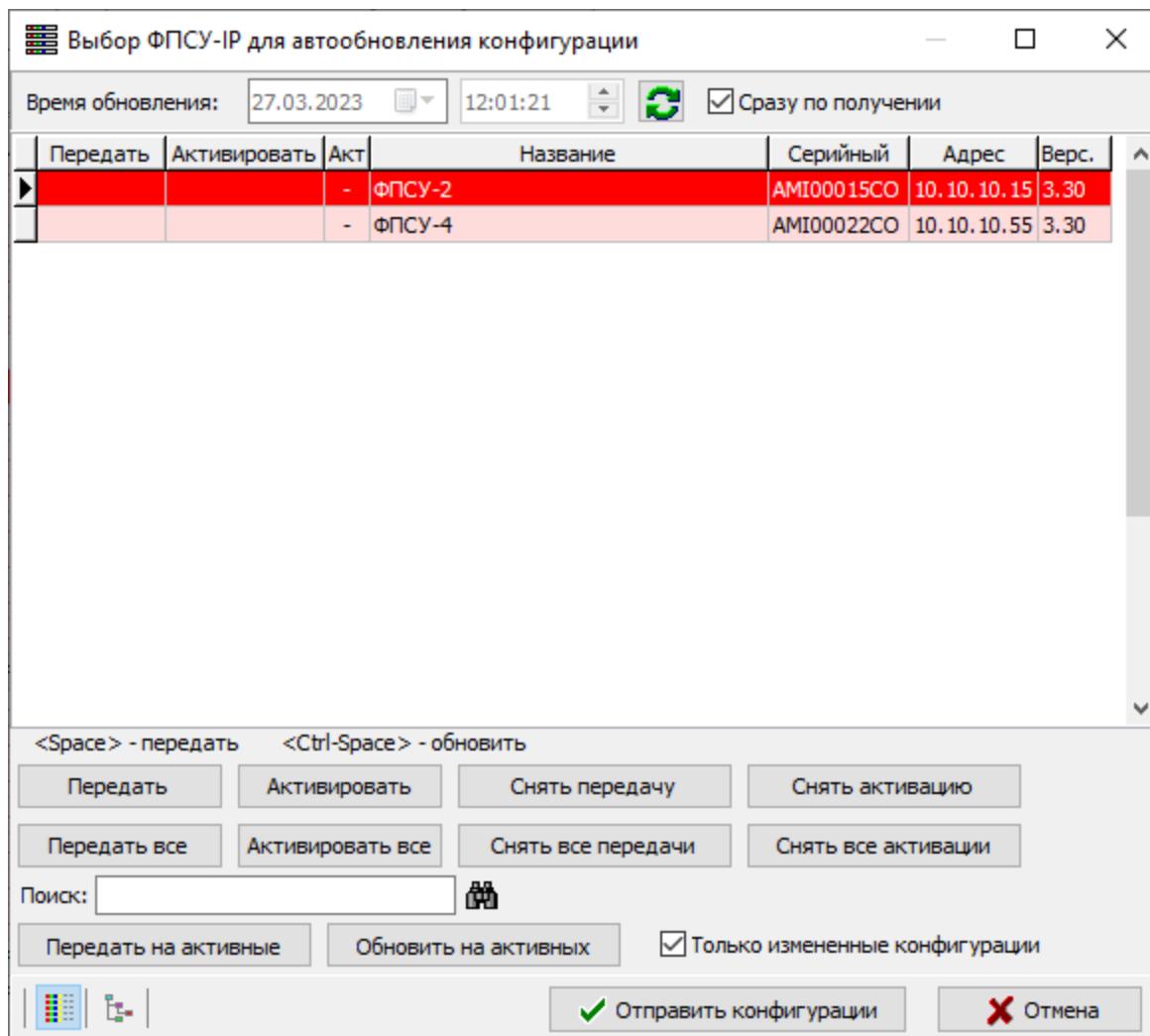


Рисунок 91 - Выбор ФПСУ-IP для обновления конфигурации

Окно управления задачами автообновления конфигурации содержит следующие опции:

- флаг «Сразу по получении», при установке которого конфигурация будет активирована сразу после ее получения на ФПСУ-IP;
- поле времени обновления (активации) конфигурации, позволяющее указать дату и время активации присланной конфигурации (доступно при снятом флаге «Сразу по получении») на ФПСУ-IP;
- область списка зарегистрированных ФПСУ-IP, из которых можно выбирать те, на которые высыпается новая конфигурация. При выборе строкой ФПСУ-IP отметить его как получателя новой конфигурации можно, нажав на кнопку «Передать»;

клавишу <Пробел>, или нажав левой клавишей мыши на поле области «Передать». Похожим образом, нажимая на кнопку «Активировать», сочетание клавиш <Ctrl+Пробел>, или поле «Активировать», отмечаются те ФПСУ-IP, на которых переданные конфигурации следует активировать;

- панель поиска в этом списке ФПСУ-IP по имени и серийному номеру;
- панель команд управления передачей и активацией конфигураций для зарегистрированных ФПСУ-IP.

Отметив в списке те ФПСУ-IP, на которые следует передать и активировать конфигурацию, следует нажать на кнопку «Передать обновление», которая будет доступна, если в списке помечен хотя бы один ФПСУ-IP.

Появится окно, в котором будет отображаться список тех ФПСУ-IP, на которых передача конфигураций была запланирована, но еще не окончена. Как только конфигурации будут переданы на все отмеченные ФПСУ-IP, окно закроется, выдав служебное сообщение «Рассылка выполнена».

Нажав кнопку «Выход», можно скрыть окно передачи. При необходимости, его можно вернуть на экран, выполнив команду главного меню УА ФПСУ-IP «Конфигурации» → «Показать состояние задания».

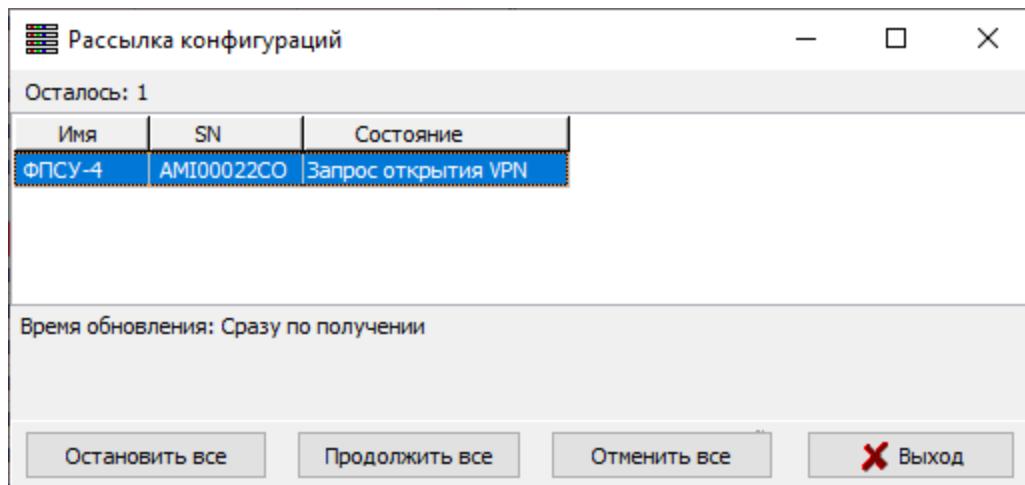


Рисунок 92 - Окно работающего задания рассылки конфигураций

При активации пересланных конфигураций администратор УА ФПСУ-IP может столкнуться со следующими ошибками, указанными в таблице 1:

Таблица 1. Сообщения об ошибках

Сообщение	Причина	Действия администратора
Неправильный циклический номер	За время ожидания активизации переданной конфигурации, конфигурация ФПСУ была изменена локальным администратором или другим удаленным администратором;	Получить заново конфигурацию ФПСУ-IP, внести в нее соответствующие изменения и передать обратно.
Не читаются данные конфигурации	ошибка внутреннего накопителя ФПСУ-IP;	Заменить внутренний накопитель ФПСУ-IP с переустановкой ПО и перерегистрацией ФПСУ-IP на УА ФПСУ-IP.
Непонятный код ответа	для подключения к ФПСУ-IP используется УА более старой версии, чем необходимо ФПСУ-IP, удаленный администратор не может интерпретировать код ошибки;	Обновить версию программного обеспечения УА ФПСУ-IP.
Не установлены номера портов	возникает при попытке установить на ФПСУ-IP нерабочую конфигурацию (с одинаковыми или пустыми номерами рабочих портов);	Отредактировать конфигурацию, назначить правильные номера рабочим портам и передать заново.
Нет описанных абонентов на одном из портов	В переданной конфигурации отсутствует описание абонентов со стороны одного из портов ФПСУ-IP, такая конфигурация не может быть активизирована.	Отредактировать конфигурацию, добавив абонента на «пустой» порт и передать заново.

11. 5. Просмотр файла сравнения конфигурации

Для просмотра файлов конфигурации необходимо выбрать пункт «Просмотр файла сравнения кфг ФПСУ-IP» меню «Конфигурации».

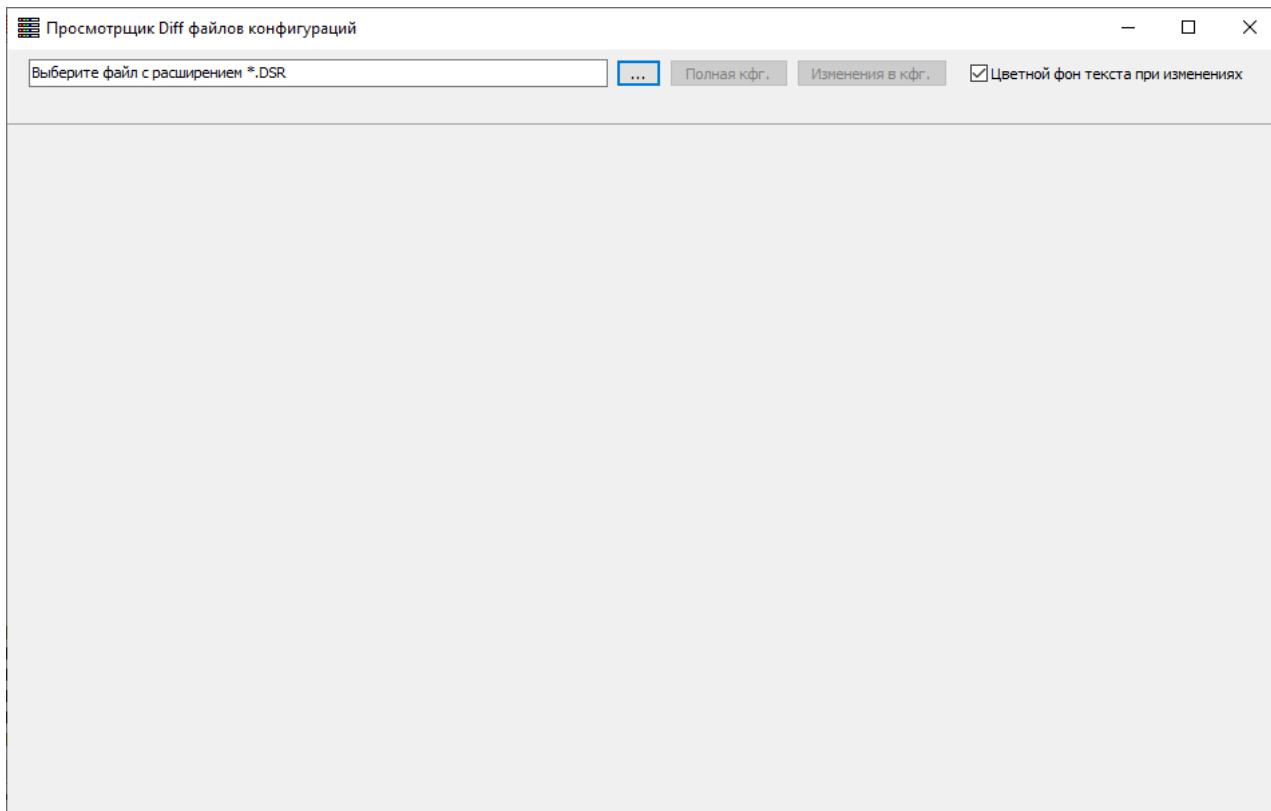


Рисунок 93 - Просмотрщик файла сравнения

В открывшемся окне «Просмотрщик Diff файлов конфигураций» предоставляется возможность выбрать путь к файлу *.DSR. После нажатия кнопки «Полная кфг» можно будет просмотреть всю информацию по конфигурации ФПСУ.

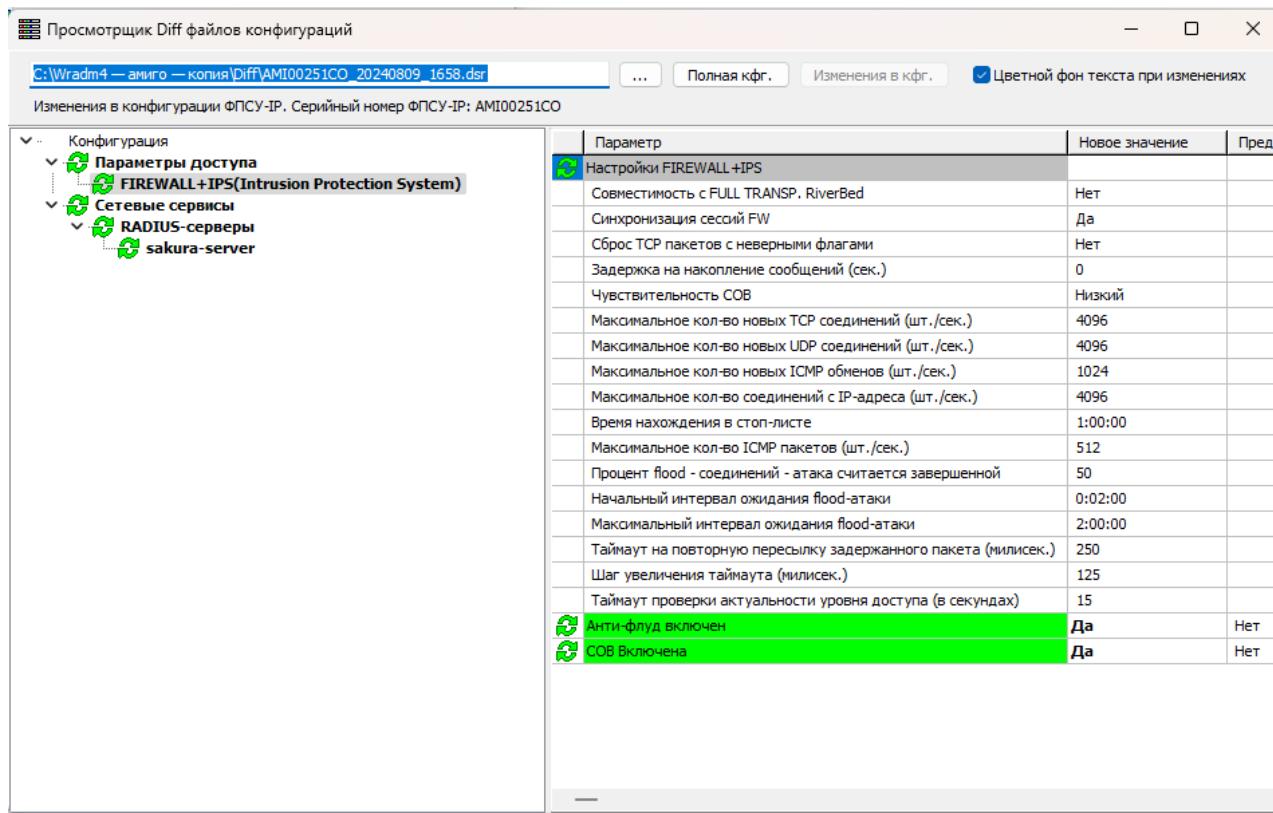


Рисунок 94 - Просмотр полной конфигурации

В случае установки флага «Цветной фон текста при изменениях» соответствующие пункты списка (при наличии изменений в конфигурации) будут подзачечены.

По нажатию кнопки «Изменения в кфг» можно просмотреть только изменения выбранной конфигурации ФПСУ-IP.

11. 6. Замена номера используемого ключа

Замена номера используемого ключа используется для создания конфигурации на основе уже имеющейся, но с другим номером ключевой информации в рамках криптосети.

Для замены номера ключевой информации необходимо выбрать пункт «Замена номера используемого ключа» меню «Конфигурации».

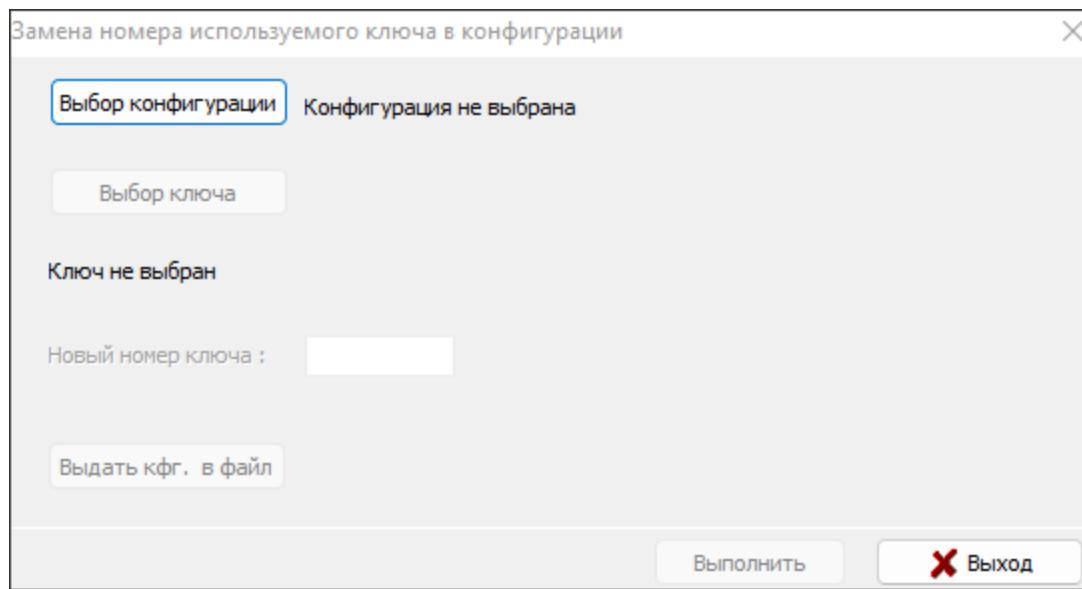


Рисунок 95 - Окно замены номера ключевой информации

В открывшемся окне следует нажать кнопку «Выбор конфигурации». Откроется окно выбора конфигурации ФПСУ-IP для замены номера ключевой информации.

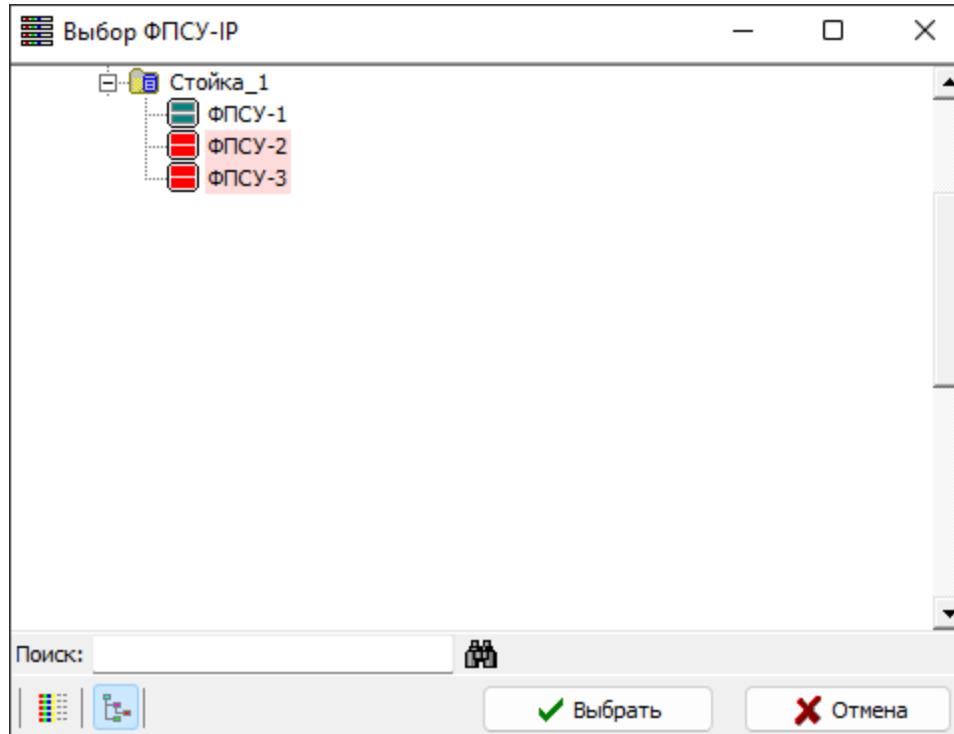


Рисунок 96 - ФПСУ-IP, на который копируется конфигурация

После выбора ФПСУ-IP и нажатия кнопки «Выбрать» в окне «Замена номера используемого ключа в конфигурации» отобразится конфигурация выбранного ФПСУ-IP. По кнопке «Выбор ключа» предоставляется возможность выбрать ключ из используемых в выбранной конфигурации.



Рисунок 97 - Окно выбора ключа для обновления на ФПСУ-IP

Выбранные ключ отобразится в окне «Замена номера используемого ключа в конфигурации»:

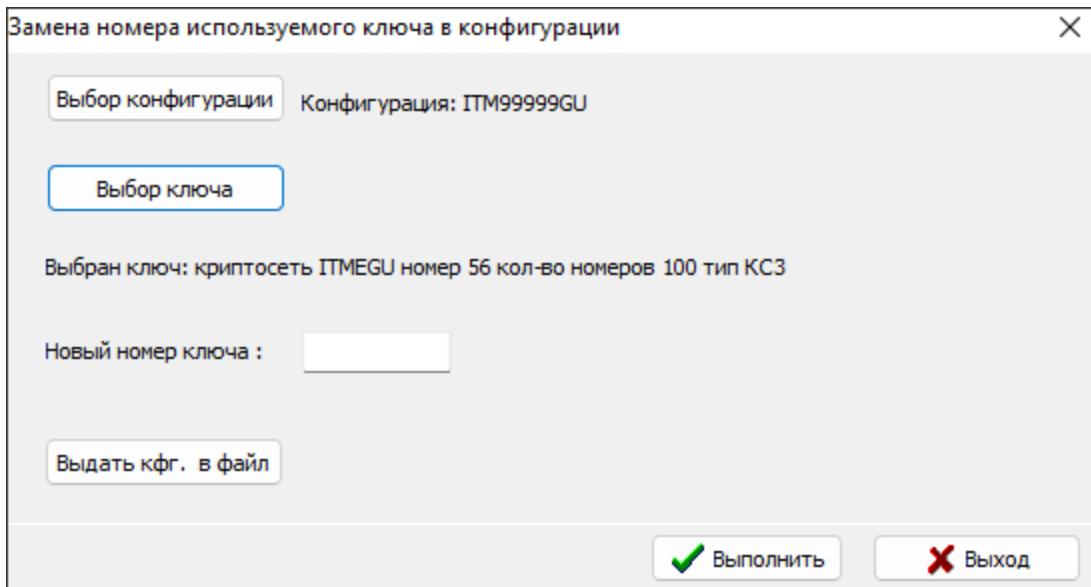


Рисунок 98 - Окно замены номера используемого ключа в конфигурации

После ввода в одноименное поле нового номера ключа конфигурацию можно сохранить в виде файла (по нажатию кнопки «Выдать кфг. в файл» на экран будет выведено окно ввода серийного номера ФПСУ-IP, для которого выдается конфигурация):

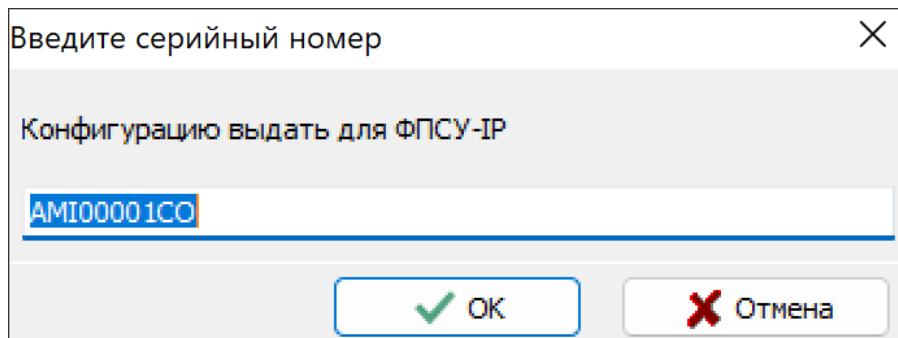


Рисунок 99 - Окно ввода серийного номера ФПСУ-IP для выдачи конфигурации в файл

По нажатию кнопки «OK» в этом окне на экран будет выдано сообщение о выдаче конфигурации в файл:

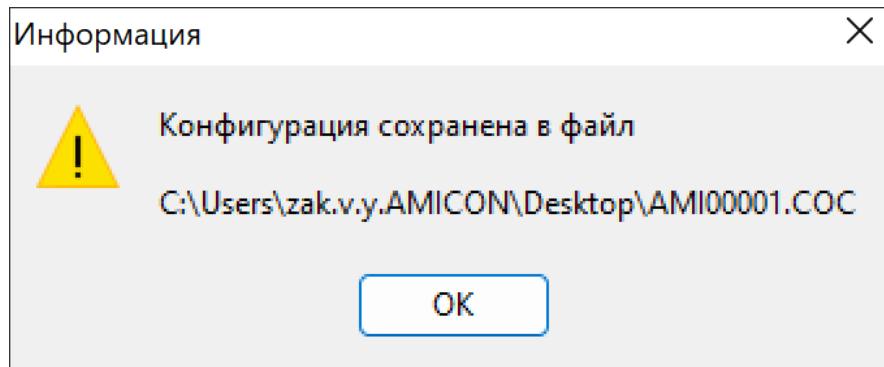


Рисунок 100 - Сообщение о выдаче конфигурации в файл

После нажатия кнопки «OK» предоставляется возможность нажатием кнопки «Выход» закрыть окно «Замена номера используемого ключа в конфигурации» и перейти непосредственно к работе с конфигурацией - см. разделы «Загрузка конфигурации ФПСУ-IP на УА ФПСУ-IP», «Загрузка конфигурации ФПСУ-IP на УА ФПСУ-IP»).

Для того, чтобы перейти к замене номера ключевой информации в выбранной конфигурации, необходимо нажать кнопку «Выполнить». После нажатия кнопки «Выполнить» откроется стандартное окно выбора каталога, в котором хранятся ключи для замены. После выбора каталога и нахождения в нем ключей откроется окно «Установка ключей ФПСУ-IP»:

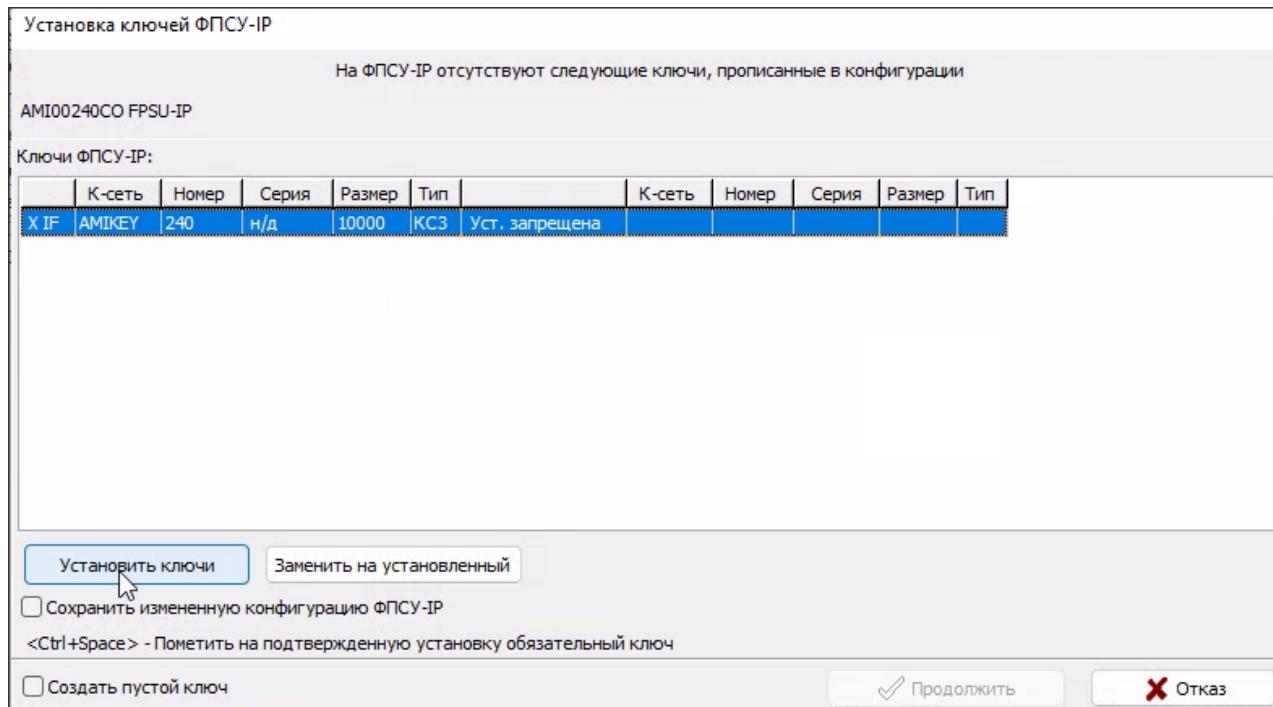


Рисунок 101 - Окно установки ключей ФПСУ-IP

В данном окне будут отображен список ключей, помеченных в первой колонке следующими флагами:

- "X" - установка обязательна;
- "+" - установка выполнена;
- "F" - запрещен к установке;
- "S" - подтвержденная установка запрещенного и обязательного ключа (флаг появляется в том случае, если ключ запрещен к установке, но при этом был установлен; для пометки такого ключа на этапе выбора используется комбинация клавиш Ctrl+Space, после чего запрещенный к установке ключ может быть установлен).

Новый ключ будет отмечен как обязательный для установки "X"(используется в конфигурации) и запрещенный "F"(на ФПСУ-IP уже установлен ключ с другим номером). Выбранный ключ можно установить (нажатием одноименной кнопки), оставить ключ без изменений (нажатием кнопки «Заменить на установленный»), а так же создать пустой ключ и/или сохранить измененную конфигурацию на ФПСУ-IP (путем установки одноименных флагов). Все действия подтверждаются нажатием кнопки «Продолжить».

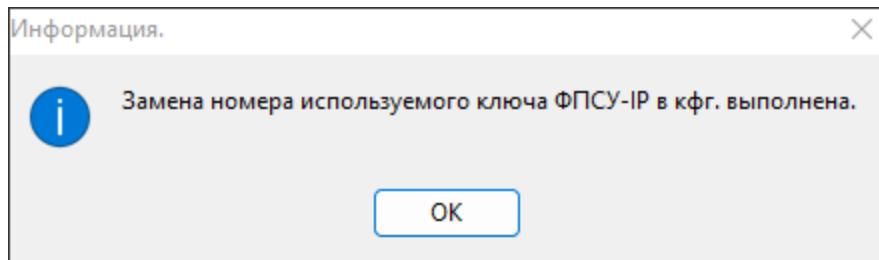


Рисунок 102 - Сообщение о выполнении замены номера используемого ключа

Для отмены процедуры замены необходимо нажать кнопку «Отказ» в окне «Установка ключей ФПСУ-IP».

11. 7. Массовое изменение конфигураций по шаблону

В УА ФПСУ-IP реализована возможность внесения одного и того же изменения сразу в множество конфигураций разных ФПСУ-IP.

Текущие конфигурации ФПСУ-IP, в которые требуется внести изменения, должны быть предварительно загружены на УА ФПСУ-IP (см. пункт «Загрузка конфигурации ФПСУ-IP на УА ФПСУ-IP»).

После массового изменения конфигураций по шаблону, загруженных на УА ФПСУ-IP, требуется активизировать измененные конфигурации на всех указанных ФПСУ-IP, описание приведено в пункте «Дистанционная массовая установка конфигураций».

Окно изменения конфигураций нескольких ФПСУ-IP по шаблону может быть вызвано путем выбора в основном окне ФПСУ-IP, а затем пункта меню «Конфигурации» → «Конфигурацию в массовые операции»; также после выбора ФПСУ-IP предоставляется возможность вызвать в контекстном меню «Конфигурация» → «Конфигурацию в массовые операции».

По команде меню на экран будет выдано окно ввода настроек для массовой модификации конфигураций.

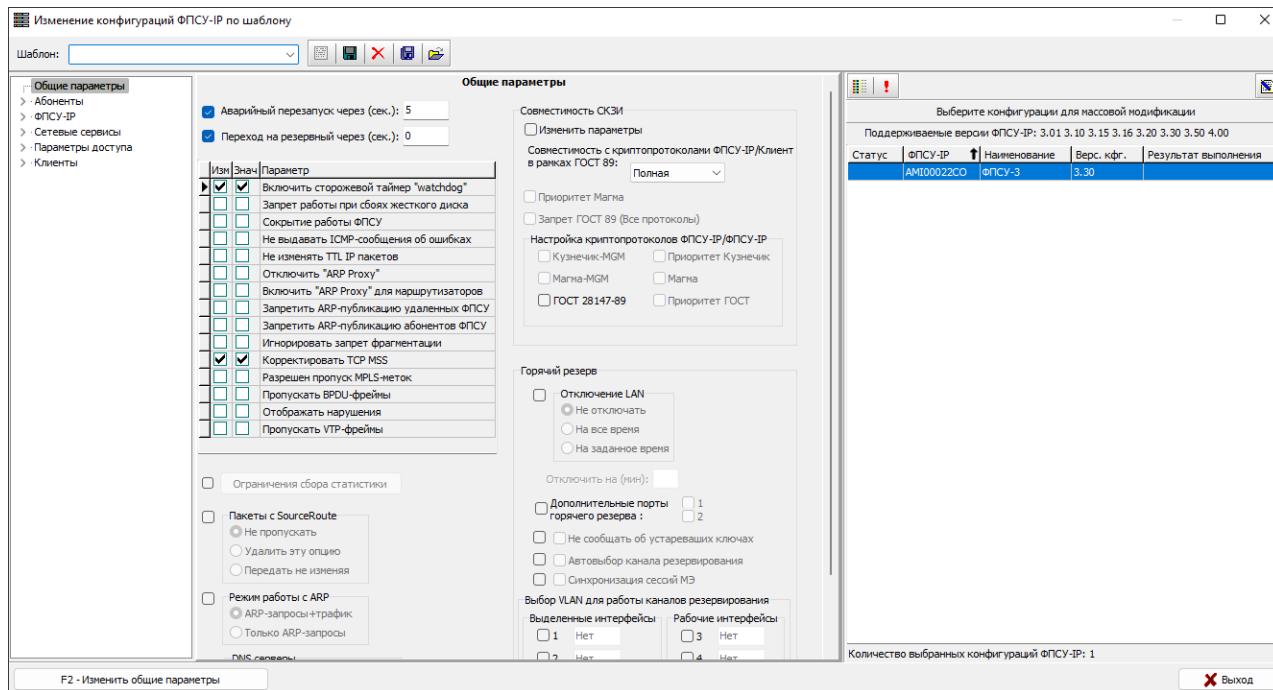


Рисунок 103 - Изменение конфигурации по шаблону

По нажатию кнопки выбора конфигураций откроется окно выбора ФПСУ-IP, в конфигурации которых требуется внести изменения. Следует отметить выбранные ФПСУ-IP и нажать кнопку «Выбрать». ФПСУ-IP добавятся в список для изменения.

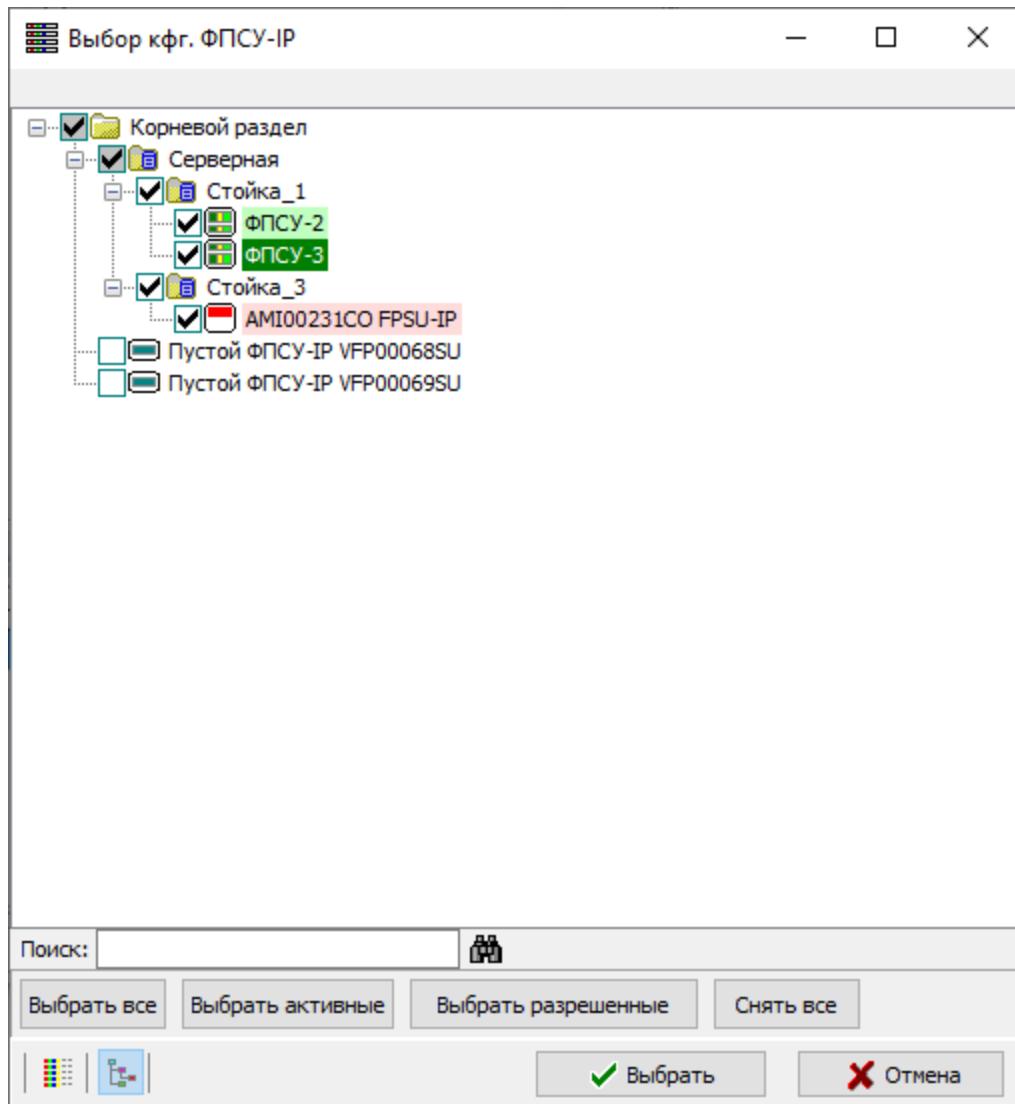


Рисунок 104 - Выбор ФПСУ-IP

После выбора списка ФПСУ-IP, в конфигурацию которых требуется внести изменения, следует указать что именно будет меняться. Не все возможные параметры конфигурации, изменяемые в ручном режиме правки конфигурации, можно запланировать к массовому изменению. В левой части окна доступен определенный список изменений, которые выбираются администратором УА ФПСУ-IP в поле «Текущий режим». В качестве текущего режима внесения изменений могут быть выбраны:

- изменение общих параметров;
- добавление/удаление абонентов;
- добавление/удаление ФПСУ-IP;

- работа с сетевыми сервисами, а именно:
 - изменение параметров Syslog;
 - изменение параметров SNMP;
 - изменение настроек NTP-клиента;
 - изменить общие параметры;
 - учет трафика IPFIX (добавление/удаление IPFIX сервера);
- изменение параметров доступа, а именно:
 - добавление/удаление ACL;
 - добавление/удаление службы;
 - добавление/удаление правила трафика;
 - добавление/удаление группы IP-адресов;
 - изменение настроек МЭ;
- изменение параметров работы с клиентами, а именно:
 - изменение настроек клиентов;
 - изменение локальных настроек клиентов;
 - изменение настроек абонентов;
 - изменение настроек RADIUS.

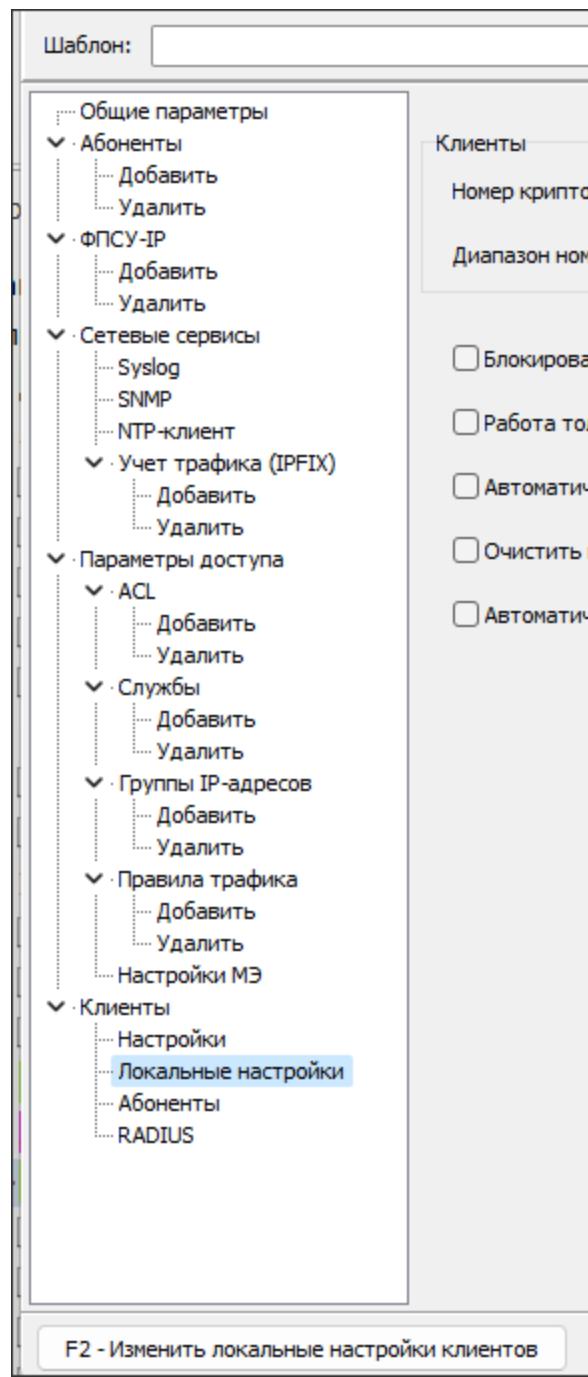


Рисунок 105 - Режимы внесения изменений в конфигурации ФПСУ-IP

Для каждого режима в области слева отображаются опции и поля для настройки текущего режима. После того, как отмечены опции и заполнены поля, указанные в интерфейсе изменения для выбранного режима могут быть просто применены в конфигурациях выбранных ФПСУ-IP, а могут быть сохранены в качестве шаблона. Для этого

необходимо дать название шаблону в поле «Выбор шаблона» и нажать кнопку сохранить параметры шаблона.

Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Выбор шаблона» и могут быть применены в дальнейшем. Наименование сохраненного шаблона можно изменить по нажатию одноименной кнопки.

По нажатию клавиши <F2> выбранные в указанном режиме изменения будут выполнены для конфигураций списка, настройки в конфигурациях будут изменены на заданные в шаблоне.

Создание шаблона для изменения общих параметров

В примере ниже приведено создание шаблона для изменения общих параметров и внесение изменений в конфигурации по сохраненному шаблону.

В окне «Изменение конфигураций ФПСУ-IP по шаблону» следует выбрать текущий режим «Изменить общие параметры». В области слева будут отображаться настройки для выбранного режима. Задайте шаблон изменяемых общих параметров. На рисунке ниже заданы параметры для изменения, напротив каждого параметра для изменения установлен флаг:

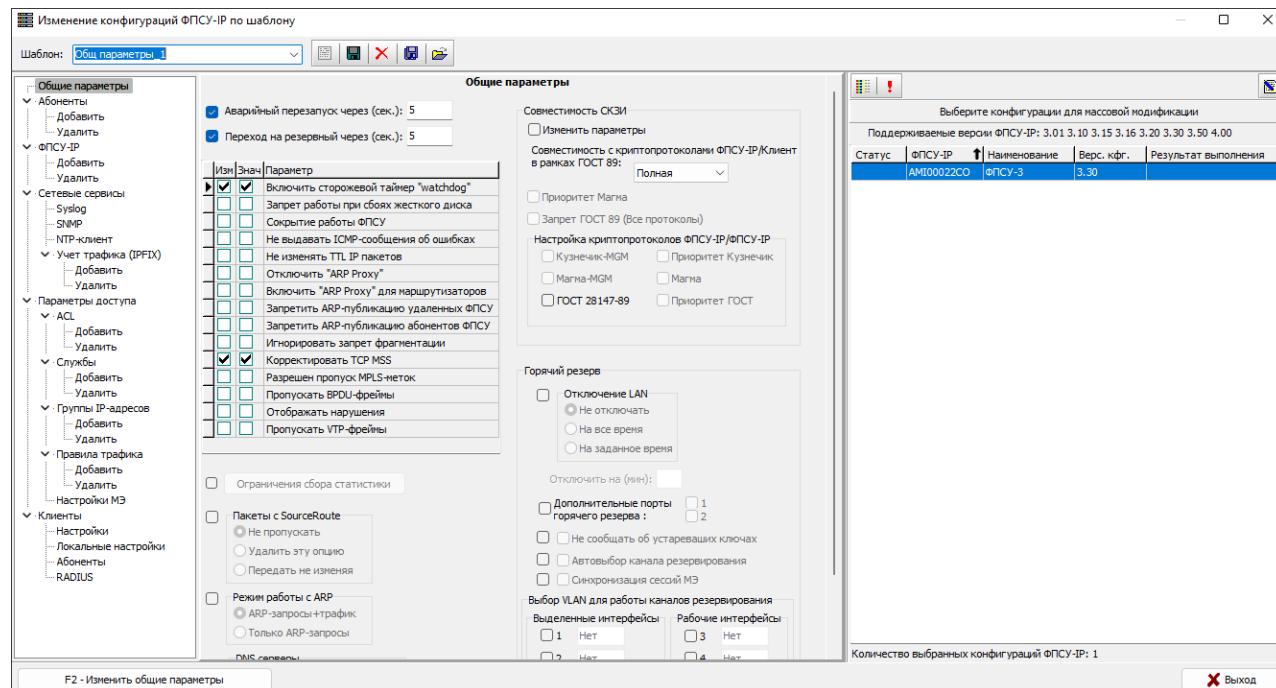


Рисунок 106 - Заданы общие параметры для изменения

Для сохранения данного шаблона в поле «Выбор шаблона» необходимо ввести

название шаблона, на рисунке - «Общ параметры_1», и нажать кнопку сохранения  . Шаблон сохраняется в УА ФПСУ-IP.

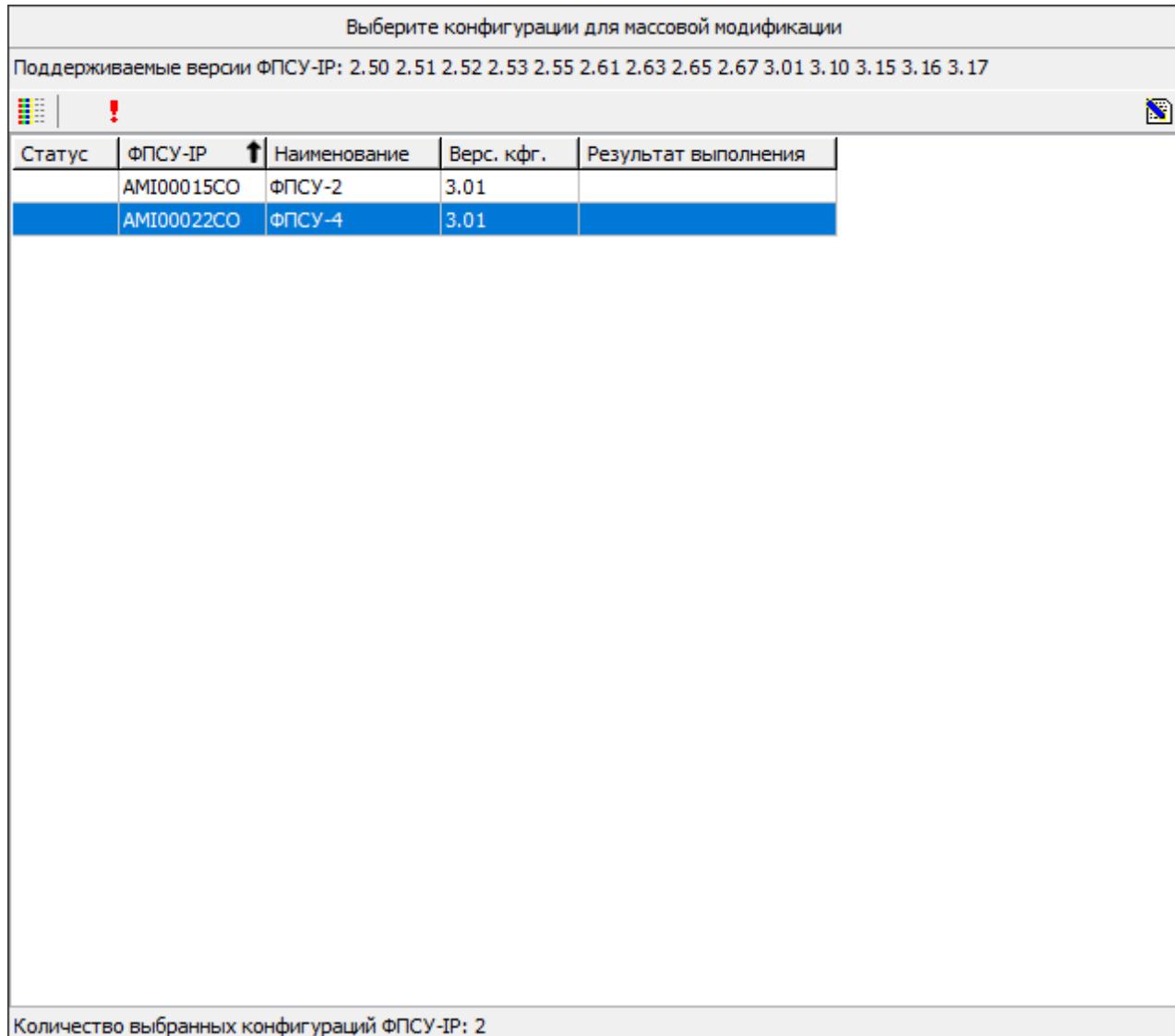


Рисунок 107 - Создан шаблон

Для изменения конфигураций ФПСУ-2 и ФПСУ-4 в соответствии с шаблоном «Общ параметры_1» необходимо, чтобы конфигурации этих ФПСУ-IP были выбраны и отображались в списке, как показано на рисунке выше и в поле «Выбор шаблона» был выбран этот шаблон. По нажатию клавиши <F2> указанные в шаблоне изменения будут применены для конфигураций ФПСУ-2 и ФПСУ-4. В списке ФПСУ-IP будет отображаться статус и результаты изменения конфигураций.

Статус	ФПСУ-IP	Наименование	Верс. кфг.	Результат выполнения
✓	AMI00015CO	ФПСУ-2	3.01	Выполнено.
✓	AMI00022CO	ФПСУ-4	3.01	Выполнено.

Рисунок 108 - Успешное массовое изменение конфигураций

11. 7. 1. Изменение общих параметров

При выборе текущего режима массового изменения конфигураций «Изменить общие параметры», администратор может изменять в списке выбранных конфигураций следующие параметры ФПСУ-IP:

The screenshot displays the 'Общие параметры' (General parameters) configuration page. On the left, a sidebar lists navigation options: Общие параметры, Абоненты, ФПСУ-IP, Сетевые сервисы, Параметры доступа, and Клиенты. The main area contains several sections:

- Аварийный перезапуск через (сек.):** 5 (checkbox checked)
- Переход на резервный через (сек.):** 0 (checkbox checked)
- Параметры:** A large table with columns Изм (Is changed), Знач (Value), and Параметр (Parameter). It lists numerous parameters such as 'Включить сторожевой таймер "watchdog"', 'Запрет работы при сбоях жесткого диска', and 'Корректировать TCP MSS'. Most parameters have checkboxes checked.
- Совместимость СКЗИ:** Includes checkboxes for 'Изменить параметры' and 'Совместимость с криптошлюзами ФПСУ-IP/Клиент в рамках ГОСТ 89:' with a dropdown menu set to 'Полная'.
- Настройка криптошлюзов ФПСУ-IP/ФПСУ-IP:** Includes checkboxes for 'Кузнецик-MGM', 'Магма', 'ГОСТ 28147-89', and 'Приоритет Кузнецик', 'Магма', and 'ГОСТ'.
- Горячий резерв:** Includes checkboxes for 'Отключение LAN' (radio buttons: 'Не отключать', 'На все время', 'На заданное время') and 'Отключить на (мин.)' with a dropdown menu.
- Дополнительные порты горячего резерва:** Includes checkboxes for 'Не сообщать об устаревших ключах', 'Автоворыбор канала резервирования', and 'Синхронизация сессий МЭ'.
- Выбор VLAN для работы каналов резервирования:** Includes tables for 'Выделенные интерфейсы' and 'Рабочие интерфейсы' with checkboxes for interfaces 1-4.

Рисунок 109 - Изменение конфигурации по шаблону

- Флаг «Аварийный перезапуск». Если при работе ФПСУ-IP происходит аппаратный сбой сетевых адаптеров, ФПСУ-IP способен детектировать это событие и выдать на экран монитора специальное сообщение, сопровождающееся звуковым сигналом, после чего через некоторое время ПО сетевых адаптеров и ПО ФПСУ-IP автоматически перегружается, после чего и ФПСУ-IP попытается восстановить работу режима фильтрации пакетов. В диалоговом поле строки укажите время, в течение которого будет выдаваться сообщение перед перезагрузкой (в диапазоне от 5 секунд до 1 часа).

Если автоматический перезапуск не нужен (например, необходимо ознакомиться с диагностикой неполадок, выданной на экран монитора), оставьте поле пустым; в таком случае при возникновении аппаратного сбоя сообщение, сопровождаемое звуковым сигналом, будет выдаваться до его отмены администратором при локальном управлении.

- Флаг «Переход на резервный». Если при работе ФПСУ-IP получает сигнал от сетевой аппаратуры об отсутствии физического соединения на каком-либо из рабочих портов, ФПСУ-IP может передать управление партнеру по системе горячего резервирования. В диалоговом поле строки укажите время, по истечении которого будет задействован резервный ФПСУ-IP (в диапазоне от 5 до 255 секунд), или оставьте поле пустым, если такая операция не требуется.
- Список параметров. Выбрать параметр для изменения можно, установив флаг в столбце «Изм» в строке параметра, и указав значение параметра - установленный флаг в столбце «Знач» означает, что опция активирована. Подробное описание параметров приведено в руководствах «Программно-аппаратный комплекс «ФПСУ-IP 3.X» и «Криптотранзитор и межсетевой экран «ФПСУ Amigo» версии 4.0.1. Руководство по эксплуатации» в пункте «Общие параметры конфигурации ФПСУ-IP».
- «Ограничения по сбору статистики». Установленный флаг активирует одноименную кнопку, нажатие на которую позволяет наложить ограничения на сбор регистрационной информации ФПСУ-IP:

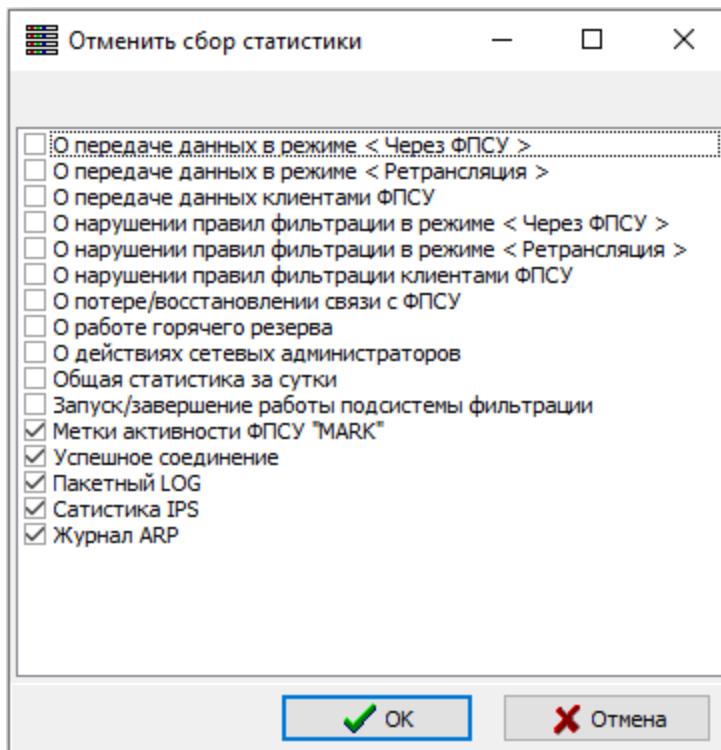


Рисунок 110 - Сбор статистики

- Флаг «Пакеты с SourceRoute». Опция SourceRoute, если она содержится в заголовке IP пакета, требует, чтобы пакет следовал по указанному ею маршруту, что может приводить к передаче пакета в обход ФПСУ-IP и нарушению безопасности. С другой стороны, игнорирование этой опции может влиять на работу сети и приводить к каким-либо другим нарушениям. Поэтому администратор в индивидуальном порядке должен решить, как ФПСУ-IP будет обрабатывать эту опцию и указать это в описываемом поле.

ФПСУ-IP предоставляет три возможных способа обработки опции SourceRoute:

- Не пропускать — пакеты, содержащие эту опцию, сбрасываются без отправки сообщения;
 - Удалить эту опцию — передать пакет получателю (если он удовлетворяет требованиям фильтрации), но удалить заданный маршрут и передать пакет по маршруту, который установил при конфигурировании для данного абонента администратор;
 - Передать не изменяя — передать пакет, оставив опцию без изменения.
- Установленный флаг «Режим работы с ARP» позволяет выбирать режим формирования ARP-таблицы на ФПСУ-IP. Возможны два варианта настройки:

- ARP-запросы + трафик — опция по умолчанию, ARP-таблица формируется из ответов на собственные ARP-запросы, а также из входящих пакетов, передаваемых через ФПСУ-IP;
 - Только ARP-запросы — при выборе этой опции, ARP-таблица формируется только из ответов на собственные ARP-запросы. Рекомендуется при использовании ФПСУ-IP вместе со сторонними решениями оптимизации передаваемого трафика (таких как Riverbed SteelHand).
- DNS-серверы - задание IP-адреса основного и дополнительного DNS-сервера. IP-адреса DNS-серверов должны быть предварительно добавлены в конфигурации порта ФПСУ-IP как абоненты - записи типа «Хост» или «Подсеть», для которых установлен флаг «Работа разрешена».
 - Совместимость СКЗИ:
 - Установленный флаг «Изменить параметры» разрешает тестовую работу ФПСУ-IP с пользователями ФПСУ-IP/Клиентов, которые используют СКЗИ предыдущих версий. Возможные параметры:
 - ✓ КРОМЕ Тун 1 —принимаются пользовательские подключения от ФПСУ-IP/Клиентов, на которых установлена версия СКЗИ, отличная от «Туннель/Клиент»;
 - ✓ КРОМЕ Тун 2 — принимаются пользовательские подключения от ФПСУ-IP/Клиентов, на которых установлена версия СКЗИ, отличная от «Туннель 2.0»;
 - ✓ Полная — принимаются пользовательские подключения от ФПСУ-IP/Клиентов с любой версией СКЗИ;
 - ✓ Отключена — принимаются пользовательские подключения только от ФПСУ-IP/Клиентов с последней версией СКЗИ.
 - Приоритет Магма - при установлении флага передаваемые данные между ФПСУ-IP и ФПСУ-IP/Клиентом будут шифроваться по алгоритму «Магма», если и ФПСУ-IP, и ФПСУ-IP/Клиент поддерживают этот алгоритм.
 - Запрет ГОСТ 89 (Все протоколы) - при установлении флага на ФПСУ-IP будут запрещены любые соединения, использующие алгоритм шифрования ГОСТ 28147-89.
 - Настройка криптовалют ФПСУ-IP/ФПСУ-IP - опции, устанавливающие работу ФПСУ-IP с ФПСУ-IP в режиме шифрования по заданному алгоритму:
 - ✓ Кузнецик-MGM - флаг, разрешающий шифрование данных блочным

шифром «Кузнецик» в режиме MGM (Multilinear Galois Mode), активируется лицензией;

- ✓ Магма-MGM - флаг, разрешающая шифрование данных блочным шифром «Магма» в режиме MGM, активируется лицензией. Если опция «Приоритет Кузнецик» не установлена, то работа ФПСУ-IP будет происходить по алгоритму шифрования «Магма MGM», в случае если партнер поддерживает этот алгоритм;
- ✓ Магма - флаг, разрешающая работу по алгоритму шифрования «Магма». Если опция «Приоритет ГОСТ» не установлена, то работа ФПСУ-IP будет происходить по алгоритму шифрования «Магма», в случае если партнер поддерживает этот алгоритм.
- ✓ ГОСТ 28147-89 - флаг, разрешающий работу по алгоритму шифрования ГОСТ 28147-89.
- ✓ Приоритет ГОСТ - при установке флага передаваемые данные между ФПСУ-IP будут шифроваться по алгоритму ГОСТ 28147-89, в случае если этот алгоритм не запрещен у партнера. Если флаг «ГОСТ 28147-89» не установлен, данная опция недоступна.
- ✓ Приоритет Кузнецик - при установке флага передаваемые данные между ФПСУ-IP будут шифроваться по алгоритму «Кузнецик MGM», в случае если партнер поддерживает этот алгоритм. Если флаг «Кузнецик-MGM» не установлен, данная опция недоступна.

- Горячий резерв:

- Установленный флаг «Отключение LAN» позволяет ФПСУ-IP горячего резерва, работающего в данный момент в пассивном режиме, отключать все сетевые адAPTERы, кроме адAPTERа, соединяющего с партнером по резервированию. Данный механизм позволяет сетевым устройствам класса сетевой коммутатор (switch) быстрее обновить таблицу соответствия MAC-адреса ФПСУ-IP физическому порту коммутатора при переключении управления между основным и резервным комплексами.
- Установленный флаг «Дополнительные порты горячего резерва» позволяет комплексу устанавливать через сетевые адAPTERы, настроенные как рабочие порты 1 и/или 2, туннель с партнером горячего резерва. Без включения данной опции туннель между комплексами ФПСУ-IP, работающими в режиме горячего резервирования, устанавливается через специально выделенные для этой цели дополнительные LAN-адAPTERы. Опция не работает со включенными опциями «Отключение LAN». Опция не работает, если для рабочего порта

ФПСУ-IP настроен работающий в режиме моста туннель.

- «Не сообщать об устаревших ключах». Установленный флаг активирует опцию. Если на ФПСУ-IP установлены ключевые данные класса КС3, то ФПСУ-IP при старте выдает информационное оповещение об истечении срока действия ключей. Для отмены выдачи такого информационного оповещения следует включить опцию «Не сообщать об устаревших ключах», установив второй флаг. По умолчанию опция отключена.
- Примечание. При использовании ФПСУ-IP по классу КС3, в настройках должен быть включен режим информирования об использовании ключа при превышении срока его действия (опция «Не сообщать об устаревших ключах» должна быть отключена).
- Автовыбор канала резервирования - опция, позволяющая в случае обрыва канального соединения переключаться на следующий активный канал связи с партнером по горячему резервированию (в том числе доступно переключение на резервный канал связи с использованием «рабочих» интерфейсов).
- Синхронизация сессий МЭ - опция, позволяющая передавать активные сессии абонентов при передаче управления партнеру по горячему резервированию. При включении такой синхронизации работа сетевых сервисов абонентов не прерывается из-за передачи управления горячemu резерву.
- Выбор VLAN для работы каналов резервирования - назначение тега VLAN для каналов «горячего» резервирования. Фреймы «горячего» резервирования будут тегированы соответствующим идентификатором VLAN. Для включения данной опции должен быть задан хотя бы один Дополнительный интерфейс горячего резерва. Рабочие интерфейсы - поля 3 и 4 - это 1 и 2 LAN-адаптеры в настройках конфигурации. Выделенные интерфейсы - поля 1 и 2 - это 3 и 4 LAN-адAPTERЫ в настройках конфигурации для горячего резерва.

По нажатию клавиши <F2> изменения общих параметров будут внесены в конфигурацию.

Данные настройки могут быть сохранены в качестве шаблона. Для этого необходимо дать название шаблону в поле «Шаблон» и нажать кнопку «Сохранить параметры шаблона». Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Шаблон» и могут быть применены в дальнейшем.

11. 7. 2. Добавление/удаление абонента

При выборе текущего режима массового изменения конфигураций «Добавление

абонента по шаблону», администратор может добавить абонента в список выбранных конфигураций.

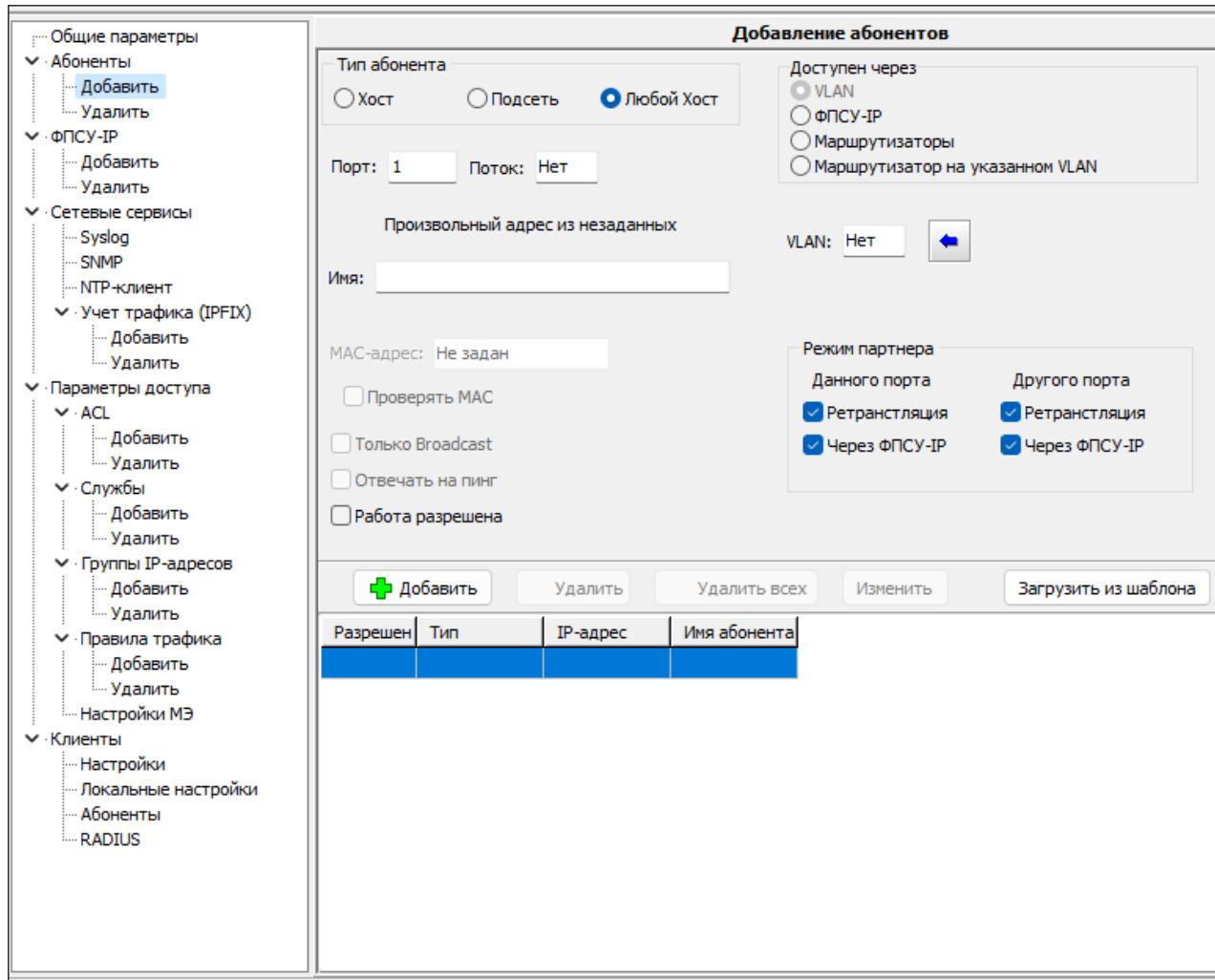


Рисунок 111 - Добавление абонента

Указываются следующие параметры абонента ФПСУ-IP:

- «Тип абонента» - индивидуальный (адрес хоста), групповой (IP-адрес подсети) или специальный адрес «Любой хост». Остальные поля окна будут различными в зависимости от указанного типа адреса;
- «Порт» - для описываемого абонента можно установить номер порта 1, 2;
- «Поток» – для описываемого абонента можно установить номер потока (от 1 до 128), в который будут направлены обмены абонента при передаче данных в туннеле между ФПСУ-IP;

- «Адрес» – IP-адрес абонента хоста или IP-адрес подсети с указанием размера маски сети через слеш (<IP-адрес подсети>/<предфикс сети>), в случае выбора в качестве типа абонента положения переключателя «Любой хост» в качестве адрес будет выбираться произвольный адрес из незаданных;
- «Всего» - поле позволяет добавить группу хост-абонентов с одинаковыми дополнительными параметрами, IP-адреса которых начинаются с указанного;
- «Имя» – имя абонента типа хост или подсеть (произвольное), которое будет отображаться в списке абонентов порта.

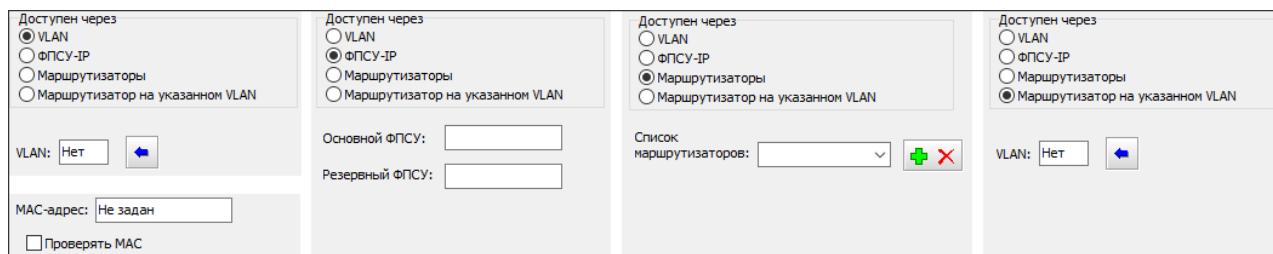


Рисунок 112 - Режим доступа абонента

Доступен через:

- «VLAN» - при установлении переключателя, указывается номер виртуальной локальной сети VLAN, в которой участвует данный IP-адрес, задается при выборе режима работы абонента «Ретрансляция».
 - MAC-адрес – Только для абонентов в режиме «Ретрансляция». Статически заданный аппаратный адрес для этого абонента. Если параметр задан, ФПСУ-IP будет отправлять пакеты в адрес этого абонента именно на указанный аппаратный адрес, вне зависимости от приходящих на ФПСУ-IP ARP-пакетов от IP-адреса абонента.
 - Проверять MAC – Только для абонентов типа «Хост», работающих в режиме «Ретрансляция». Требует заполненного поля «MAC». При включенной опции, ФПСУ-IP проверяет полученные от IP-адреса абонента пакеты на соответствие указанному MAC-адресу. Если MAC-адрес полученного пакета от IP-адреса описываемого абонента не совпадает с указанным в поле «MAC», пакет будет сброшен.
- «ФПСУ» - при установлении переключателя, указывается «Основной ФПСУ», «Резервный ФПСУ» - ФПСУ-IP, через которые будет доступен IP-адрес или подсеть.
- «Маршрутизаторы» - список маршрутизаторов, через который будет доступен IP-

адрес или подсеть.

- «Маршрутизатор на указанном VLAN» - при установлении переключателя, указывается номер виртуальной локальной сети VLAN.
- «Только Broadcast» — флаг, указывающий ФПСУ-IP, что данная запись типа «подсеть» создана специально для определения правил работы с широковещательными передачами. Если флаг выключен - описываемая подсеть по установленным правилам будет обмениваться с партнерами как широковещательными IP-пакетами, так и IP-пакетами для отдельных хостов, входящих в данную подсеть.
- Флаг «Отвечать на пинг» - указание конфигурируемому ФПСУ-IP отвечать на ICMP (ECHO) пакеты, направленные от IP-адреса описываемого абонента в IP-адреса портов ФПСУ-IP.
- Флаг «Работа разрешена» - установленный флаг разрешает передавать данные описываемого абонента. Если флаг снят, пакеты от этого абонента и пакеты в адрес абонента, приходящие на ФПСУ-IP, будутброшены.

«Режим партнера». В этом поле требуется установить флаги разрешенных режимов работы с партнерами-абонентами (подробнее см. руководство по эксплуатации ФПСУ-IP).

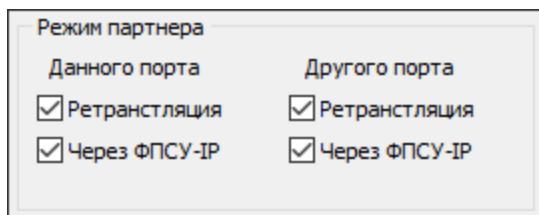


Рисунок 113 - Добавление абонента. Режим партнера

По нажатию клавиши <F2> указанный абонент (или группа абонентов-хостов, если счетчик поля «Всего» больше единицы) будет добавлен в конфигурации ФПСУ-IP списка массовой модификации.

Данные настройки могут быть сохранены в качестве шаблона. Для этого необходимо дать название шаблону в поле «Шаблон» и нажать кнопку «Сохранить параметры шаблона». Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Шаблон» и могут быть применены в дальнейшем.

Удаление абонента

При выборе текущего режима массового изменения конфигураций «Удаление

абонента», администратор может удалить абонента из списка выбранных конфигураций ФПСУ-IP. Для этого следует выбрать тип абонента для удаления, задать соответствующие параметры и удалить абонента по нажатию клавиши <F2>.

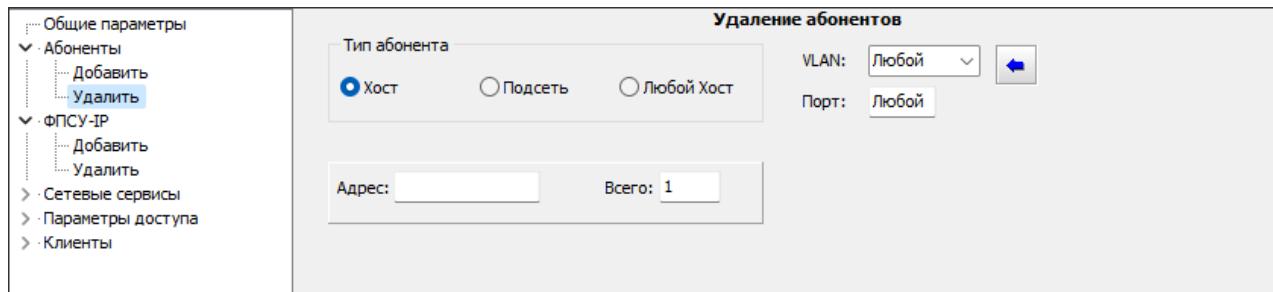


Рисунок 114 - Удаление абонента

11. 7. 3. Добавление/удаление ФПСУ-IP

При выборе текущего режима массового изменения конфигураций «Добавление ФПСУ-IP», администратор может добавить ФПСУ-IP в список выбранных конфигураций.

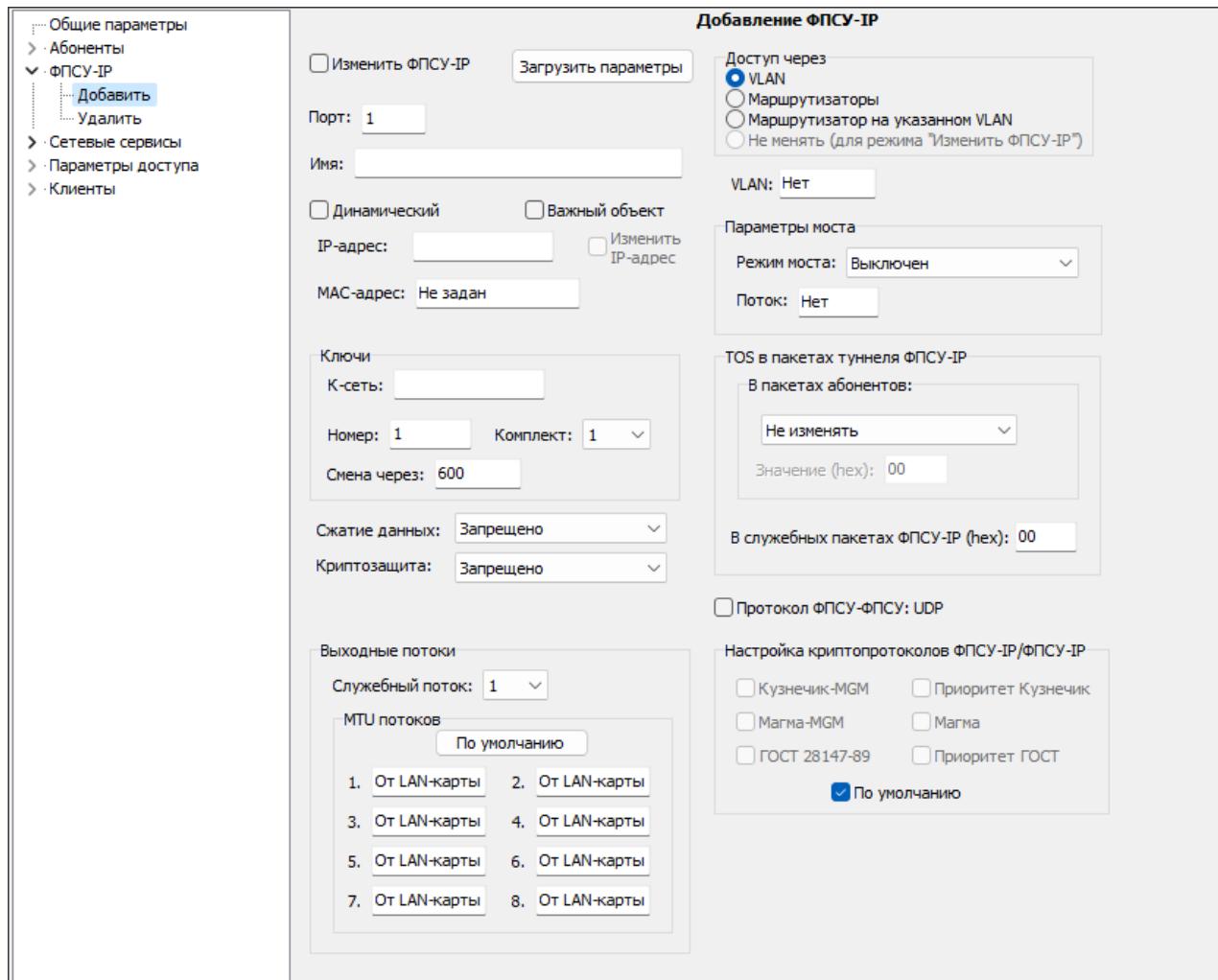


Рисунок 115 - Добавление ФПСУ-IP

- Изменить ФПСУ-IP - флаг, установка которого позволяет использовать параметры ФПСУ-IP из списка (открывающегося по нажатию кнопки «Загрузить параметры») для добавления нового ФПСУ-IP\$
- Порт
- Имя – название ФПСУ-IP;
- Динамический - флаг, установка которого разрешает установление туннеля с произвольного IP-адреса;
- Важный объект – флаг в положении «включено» запрещает удалять описание маршрутизатора из интерфейса портов ФПСУ-IP. Признак «Важный объект» добавлен как дополнительная защита от случайного удаления записи о маршрутизаторе при редактировании конфигурации.

- IP-адрес – основной IP-адрес порта маршрутизатора, связанного с описываемым портом ФПСУ-IP;
- Изменить IP-адрес - флаг, активный только в случае установки флага «Изменить ФПСУ-IP», и позволяющий изменить загруженную информацию (если флаг «Изменить IP-адрес» установлен, появляется дополнительное поле «Новый IP-адрес»);
- MAC-адрес – аппаратный адрес порта маршрутизатора, связанного с ФПСУ-IP;
- Ключи — параметр, определяющий какие именно ключи парно-выборочной связи, из числа установленных и разрешенных к использованию на ФПСУ-IP, будут применяться в процессе шифрования. Указывается криптосеть, номер и комплект используемых другим ФПСУ-IP ключей (комплект указывается только для ключей класса КС2); также указывается время, по истечении которого при взаимодействии другого ФПСУ-IP с конфигурируемым на основе выделенных ключей парно-выборочной связи будут вырабатываться новые сеансовые ключи (от 1 до 3600 секунд).
- Криптозащита – указание ФПСУ-IP, каким образом при работе с описываемым партнером согласовывать использование режима шифрования передаваемой информации в соответствии с ГОСТ 28147-89.
- Сжатие данных – указание ФПСУ-IP при работе с удаленным ФПСУ-IP использовать режим проходного архивирования передаваемых данных, уменьшая объем передаваемого трафика. ВНИМАНИЕ! Использовать этот режим по умолчанию не рекомендуется, поскольку он уменьшает общую скорость передачи данных между двумя ФПСУ-IP. Рекомендуется к применению на медленных каналах связи (например, ADSL или спутниковых).

Возможные варианты установки каждого из режимов сжатия и шифрования:

- запрещено – режим запрещен для канала передачи данных;
 - нежелательно – использование режима нежелательно, но допускается по конфигурации удаленного ФПСУ-IP;
 - желательно – режим желателен, но может быть использован только при соответствующих установках на удаленном ФПСУ-IP. Он является режимом по умолчанию;
 - обязательно – для канала передачи данных режим является обязательным.
- Выходные потоки - правила разделения поступающих в VPN-туннель между

ФПСУ-IP данных на несколько различных потоков.:

- Служебный - позволяет установить номер потока, в который будут направляться служебные данные при взаимодействии ФПСУ-IP с удаленным партнером;
- MTU-потоков - предназначено для установки максимального размера передаваемых IP-пакетов (в байтах), которые будут передаваться по потокам с соответствующими номерами. MTU - максимальный размер IP-пакетов (в байтах), которые будут передаваться с конфигурируемого порта ФПСУ-IP удаленному ФПСУ-IP через VPN-туннель. Значение этого поля возможно установить в диапазоне от 576 до размера 65535 байт. По умолчанию («От LAN-платы») будет использоваться значение MTU, которое конфигурируемый ФПСУ-IP автоматически получит от сетевого адаптера описываемого порта.
- Доступен через:
 - «VLAN» - при установлении переключателя, указывается номер виртуальной локальной сети VLAN, в которой участвует данный IP-адрес, задается при выборе режима работы абонента «Ретрансляция»;
 - «Маршрутизаторы» - список маршрутизаторов, через который будет доступен IP-адрес или подсеть;
 - «Маршрутизатор на указанном VLAN» - при установлении переключателя, указывается номер виртуальной локальной сети VLAN;
 - Не менять (для режима «Изменить ФПСУ-IP»).
- «TOS в пакетах туннеля ФПСУ»- выбор типа обслуживания пользовательских пакетов;
 - В пакетах абонентов - настройки для пользовательского трафика:
 - ✓ Не изменять - не изменять тип обслуживания в пакете;
 - ✓ Во все пакеты - изменить тип обслуживания для всех пакетов на заданное значение;
 - ✓ В пакеты с ненулевым TOS - изменить тип обслуживания на заданный для пакетов с установленным типом обслуживания;
 - ✓ Значение (hex) - значение в байтах.
 - В служебных пакетах ФПСУ TOS - значение в байтах.
- Протокол ФПСУ-ФПСУ: IP или UDP – флаг, меняющий основной протокол

взаимодействия между двумя ФПСУ-IP с протокола по умолчанию, сетевой IP№53, на альтернативный транспортный UDP: 30004;

- Настройка криптовидиков ФПСУ-IP/ФПСУ-IP - опции, устанавливающие работу ФПСУ-IP с ФПСУ-IP в режиме шифрования по заданному алгоритму:
 - ✓ Кузнецик-MGM - флаг, разрешающий шифрование данных блочным шифром «Кузнецик» в режиме MGM (Multilinear Galois Mode), активируется лицензией;
 - ✓ Мagma-MGM - флаг, разрешающий шифрование данных блочным шифром «Магма» в режиме MGM, активируется лицензией. Если опция «Приоритет Кузнецик» не установлена, то работа ФПСУ-IP будет происходить по алгоритму шифрования «Магма MGM», в случае если партнер поддерживает этот алгоритм;
 - ✓ Магма - флаг, разрешающий работу по алгоритму шифрования «Магма». Если опция «Приоритет ГОСТ» не установлена, то работа ФПСУ-IP будет происходить по алгоритму шифрования «Магма», в случае если партнер поддерживает этот алгоритм.
 - ✓ ГОСТ 28147-89 - флаг, разрешающий работу по алгоритму шифрования ГОСТ 28147-89.
 - ✓ Приоритет ГОСТ - при установке флага передаваемые данные между ФПСУ-IP будут шифроваться по алгоритму ГОСТ 28147-89, в случае если этот алгоритм не запрещен у партнера. Если флаг «ГОСТ 28147-89» не установлен, данная опция недоступна.
 - ✓ Приоритет Кузнецик - при установке флага передаваемые данные между ФПСУ-IP будут шифроваться по алгоритму «Кузнецик MGM», в случае если партнер поддерживает этот алгоритм. Если флаг «Кузнецик-MGM» не установлен, данная опция недоступна.

По нажатию клавиши <F2> указанный абонент (или группа абонентов-хостов, если счетчик поля «Всего» больше единицы) будет добавлен в конфигурации ФПСУ-IP списка массовой модификации.

Данные настройки могут быть сохранены в качестве шаблона. Для этого необходимо дать название шаблону в поле «Шаблон» и нажать кнопку «Сохранить параметры шаблона». Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Шаблон» и могут быть применены в дальнейшем.

Удаление ФПСУ-IP

При выборе текущего режима массового изменения конфигураций «Удаление ФПСУ-IP», администратор может удалить ФПСУ-IP из списка выбранных конфигураций. Для этого следует выбрать тип действия с абонентами после удаления, задать имя или IP-адрес удаляемого ФПСУ-IP и удалить ФПСУ-IP по нажатию клавиши <F2>.

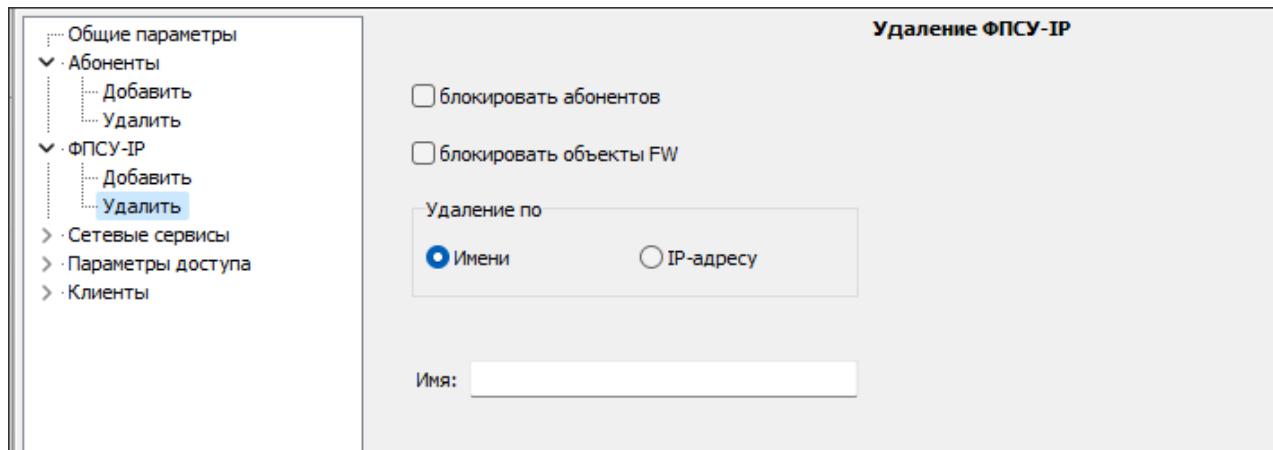


Рисунок 116 - Удаление абонента

11.7.4. Изменение сетевых сервисов

11.7.4.1. Изменение параметров Syslog

При выборе текущего режима массового изменения конфигураций «Изменить параметры Syslog», администратор может изменить в списке выбранных конфигураций следующие параметры Syslog-клиента ФПСУ-IP:

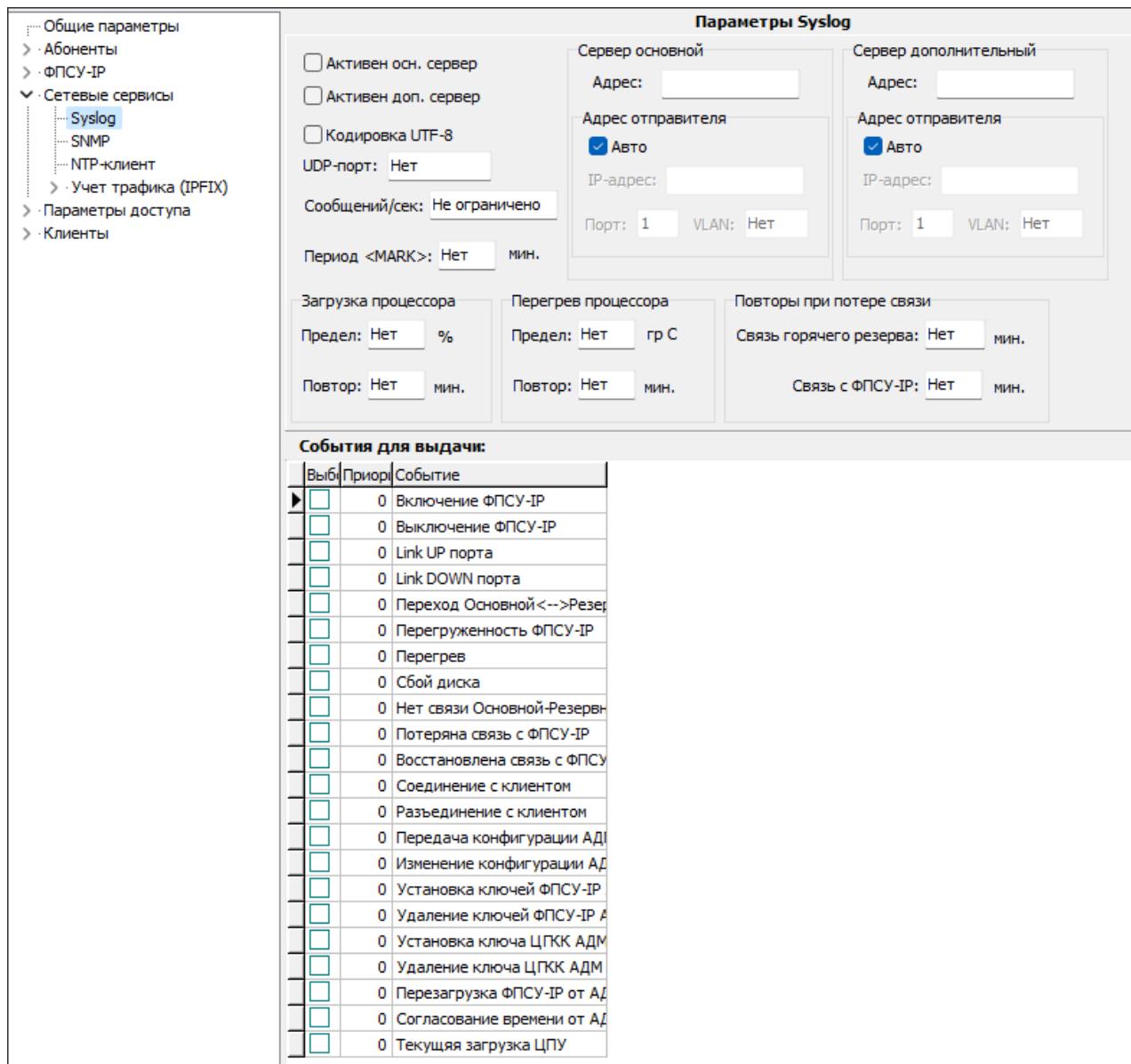


Рисунок 117 - Изменение параметров Syslog

«Параметры Syslog»:

- Активен осн. сервер , доп. сервер — при включении флага в IP-адрес SysLog сервера основного и/или дополнительного, на них будут отправляться SysLog-сообщения.
- Адрес сервера — порт ФПСУ-IP, чей IP-адрес будет указан в качестве отправителя SysLog-сообщений. По умолчанию, режима «Авто», в качестве отправителя будет

указан тот порт, на котором описан принадлежащий Syslog-серверу IP-адрес. Администратор может безусловно указать, что сообщения следует отправлять от IP-адреса 1 или 2 порта ФПСУ-IP.

- Код UTF-8 — флаг, указывающий изменение кодировки отправляемых сообщений на UTF-8 (по умолчанию OEM/DOS 866).
- UDP-порт — порт для отправления Syslog-сообщений от ФПСУ-IP Syslog-серверу, по умолчанию 514.
- «Сообщений/сек» — максимальное количество SysLog-сообщений о событиях на настраиваемом ФПСУ-IP, отправляемое в секунду. Рекомендуется устанавливать значение не более 100. По умолчанию не ограничено;
- «Период <MARK>» — ФПСУ-IP отправляет на SysLog сервер служебное оповещение с заданной периодичностью, указывается в минутах.

«Загрузка процессора»:

- «Предел» — отправка сообщения SysLog серверу о процентной загрузке центрального процессора ФПСУ-IP. Работает при включенном учёте события «Перегруженность ФПСУ». Если стоит значение «Нет», то сообщение будет отправляться вне зависимости от загрузки ЦПУ. Если стоит числовое значение от 0 до 100, то сообщение будет отправляться только в случае загрузки ЦПУ, превышающей указанное предельное значение;
- «Повтор» — указание на периодичность отправки сообщений SysLog серверу о процентной загрузке центрального процессора ФПСУ-IP. Работает при включенном учёте события «Перегруженность ФПСУ» и/или «Текущая загрузка ЦПУ». Для события «Перегруженность ФПСУ» - если стоит значение «Нет», то сообщение будет отправлено однократно при наступлении события, если установить числовое значение то, при продолжительном превышении предела загрузки ЦПУ, через каждый указанный промежуток времени сообщение будет отправляться повторно.

«Перегрев процессора»:

- «Предел» — отправка сообщения SysLog серверу о температуре центрального процессора ФПСУ-IP. Работает при включенном учёте события «Перегрев». Если стоит значение «Нет», то сообщение будет отправляться вне зависимости от нагрева ЦПУ. Если стоит числовое значение, то сообщение будет отправляться только в случае нагрева ЦПУ до температуры, превышающей указанное предельное значение

в градусах Цельсия;

- «Повтор» — периодичность отправки сообщений SysLog серверу о температуре центрального процессора ФПСУ-IP. Работает при включенном учёте события «Перегрев» и/или «Текущая Температура». Для события «Перегрев» - если стоит значение «Нет», то сообщение будет отправлено однократно при наступлении события, если установить числовое значение то, при продолжительном превышении предельной температуры ЦПУ, через каждый указанный промежуток времени сообщение будет отправляться повторно.

«Повторы при потере связи»:

- «Связь горячего резерва» — отправка сообщения SysLog серверу в случае отсутствия ответа от партнёра по горячему резерву. Работает при включенном учёте события «Нет связи Основной - Резервный». Если стоит значение «Нет», то сообщение будет отправлено однократно при наступлении события. Если установить числовое значение, то при продолжительном отсутствии связи с партнёром по горячему резерву, через заданный период времени сообщение будет отправляться повторно;
- «Связь с ФПСУ» — отправка сообщения SysLog серверу в случае отсутствия ответа от удаленного ФПСУ-IP. Работает при включенном учёте события «Потеряна связь с ФПСУ». Если стоит значение «Нет», то сообщение будет отправлено однократно при наступлении события. Если установить числовое значение, то при продолжительном отсутствии ответа от удаленного ФПСУ-IP через заданный период времени сообщение будет отправляться повторно.

«События для выдачи»:

- Список событий, при наступлении которых следует отправить сообщение SysLog серверу. Установленный флаг в строке события в столбце «Выб» означает, что оповещение о данном событии будет отправлено серверу SysLog. Каждому из событий в соответствии с протоколом SysLog может быть установлен приоритет от 0 до 7 вручную администратором УА ФПСУ-IP. Подробное описание событий приведено в руководствах «Программно-аппаратный комплекс «ФПСУ-IP 3.X» и «КриптоМаршрутизатор и межсетевой экран «ФПСУ-IP Amigo» версии 4. Руководство по эксплуатации» в пункте «Настройка SysLog событий ФПСУ-IP».

По нажатию клавиши <F2> изменения параметров SysLog будут внесены в конфигурацию.

Данные настройки могут быть сохранены в качестве шаблона. Для этого необходимо

дать название шаблону в поле «Шаблон» и нажать кнопку «Сохранить параметры шаблона». Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Шаблон» и могут быть применены в дальнейшем.

11.7.4.2. Изменение SNMP

При выборе текущего режима массового изменения конфигураций «Изменить SNMP», администратор может изменять в списке выбранных конфигураций следующие параметры ФПСУ-IP:

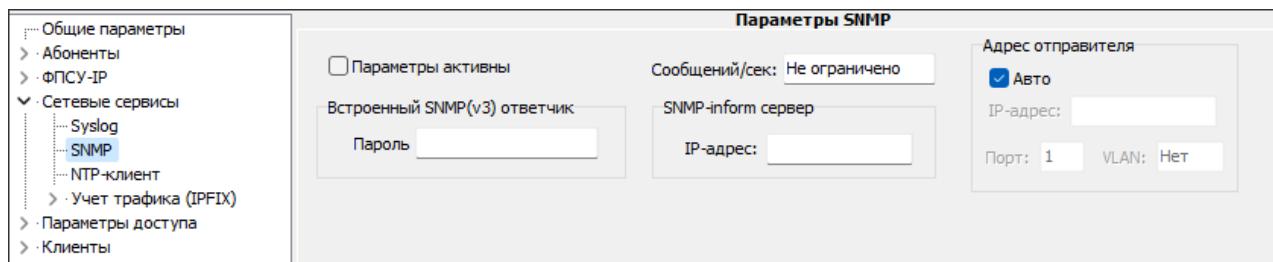


Рисунок 118 - Изменение параметров SNMP

- «Параметры активны» — установленный флаг позволяет обрабатывать и отправлять сообщения в ответ на SNMP-запросы, поддерживать отправку SNMP-trap сообщений в критических ситуациях.
- «Встроенный SNMP(v3)-ответчик, Пароль» — символьный пароль, указание которого требуется при направлении запроса к SNMP-агенту, работающему на ФПСУ-IP, от SNMP-менеджера. Поле можно оставить пустым, в таком случае пароль не установлен.
- «Сообщений/сек» — максимальное количество SysLog-сообщений о событиях на настраиваемом ФПСУ-IP, отправляемых в секунду. Рекомендуется устанавливать значение не более 100. По умолчанию не ограничено.
- «SNMP-inform сервер, IP-адрес» — IP-адрес SNMP-менеджера, на него будут отправляться SNMP-trap сообщения.
- «Адрес отправителя» — порт ФПСУ-IP, чей IP-адрес будет указан в качестве отправителя SNMP-сообщений. По умолчанию, режима «Авто», в качестве отправителя будет указан тот порт, на котором описан принадлежащий SNMP TRAP серверу IP-адрес. Администратор может безусловно указать, что сообщения следует отправлять от IP-адреса 1 или 2 порта ФПСУ-IP.

По нажатию клавиши <F2> изменения SNMP будут внесены в конфигурации ФПСУ-IP.

Данные настройки могут быть сохранены в качестве шаблона. Для этого необходимо дать название шаблону в поле «Шаблон» и нажать кнопку «Сохранить параметры шаблона». Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Шаблон» и могут быть применены в дальнейшем.

11.7.4.3. Изменение NTP-клиента

На ФПСУ-IP может быть установлен режим автоматической синхронизации текущего времени с одним из задаваемых тайм-серверов, работающих по протоколу NTP. NTP-клиент на ФПСУ-IP поддерживает синхронизацию с двумя NTP-серверами, которые указываются как «первичный» и «вторичный» в интерфейсе ФПСУ-IP. Синхронизация со вторичным сервером включается при недоступности первичного.

ВНИМАНИЕ! НЕ СЛЕДУЕТ одновременно задействовать NTP-клиента и синхронизацию времени на ФПСУ-IP с удаленным администратором (см. пункт «Установка параметров взаимодействия ФПСУ-IP с УА ФПСУ-IP»)!

Настройка синхронизации времени выполняется из пункта «Сетевые сервисы→NTP-клиент» окна изменения конфигурации ФПСУ-IP по шаблону:

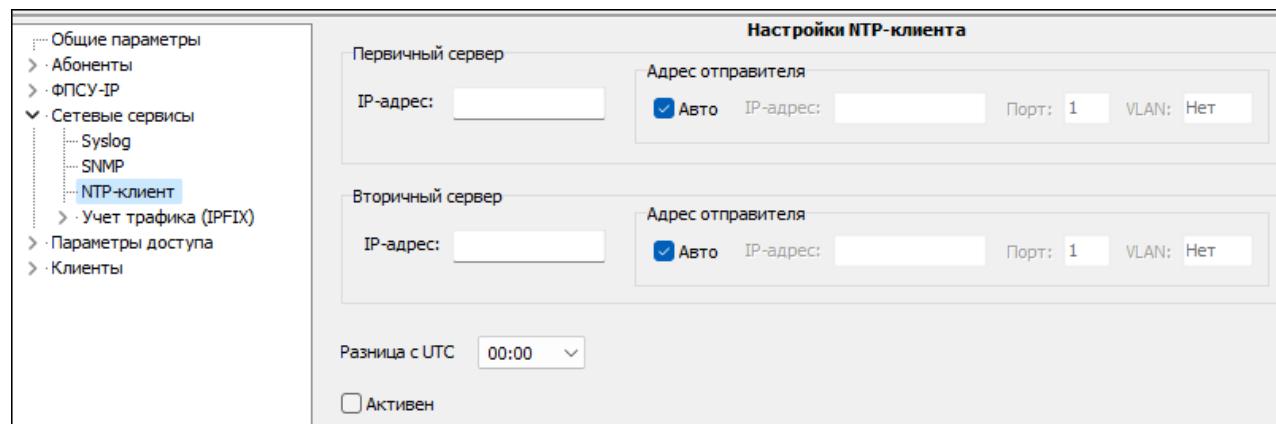


Рисунок 119 - Команда меню «Сетевые сервисы→NTP-клиент»

По умолчанию, параметры синхронизации времени не определены и NTP-клиент не задействован:

Для включения NTP-клиента на ФПСУ-IP, следует выполнить следующие действия:

- указать адрес первичного NTP-сервера;
- задать для первичного NTP-сервера адрес отправителя - порт ФПСУ-IP или оставить автономную настройку;

- указать адрес вторичного NTP-сервера, если требуется;
- задать для вторичного NTP-сервера адрес отправителя - порт ФПСУ-IP или оставить автономную настройку;
- установить разницу временного пояса, в котором работает ФПСУ-IP, с UTC временем;
- задействовать флаг «Активен»;
- внести изменения нажатием клавиши <F2>.

Адрес отправителя - порт ФПСУ-IP, чей IP-адрес будет указан в качестве отправителя NTP-серверу. По умолчанию в режиме «Авто» в качестве отправителя будет указан тот порт, на котором описан принадлежащий NTP-серверу IP-адрес. Администратор может безусловно указать, что сообщения следует отправлять от IP-адреса 1 или 2 порта ФПСУ-IP.

IP-адрес вторичного NTP-сервера указывать не обязательно. После запуска ФПСУ-IP с задействованным NTP-клиентом, ФПСУ-IP каждую минуту опрашивает NTP-сервер и синхронизирует с ним время в случае расхождения.

Данные настройки могут быть сохранены в качестве шаблона. Для этого необходимо дать название шаблону в поле «Шаблон» и нажать кнопку «Сохранить параметры шаблона». Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Шаблон» и могут быть применены в дальнейшем.

11. 7. 4. 4. Добавление/удаление IPFIX-трафика

ФПСУ-IP может выступать в качестве сенсора сетевой структуры IPFIX (выступать в качестве IPFIX Device согласно RFC 5470).

ФПСУ-IP может собирать информацию о проходящем через него трафике, создавать на основе полученной информации шаблоны с данными IP-потоков, и периодически отправлять эти шаблоны на указанные IP-адреса коллекторов IPFIX.

Поддерживается протокол IPFIX (v. 10), основанный на протоколе Cisco NetFlow версии 9.

Доступ к окну добавления настроек параметров учета трафика IPFIX на ФПСУ-IP выполняется из пункта «Сетевые сервисы → Учет трафика (IPFIX) → Добавить» окна изменения конфигурации ФПСУ-IP по шаблону:

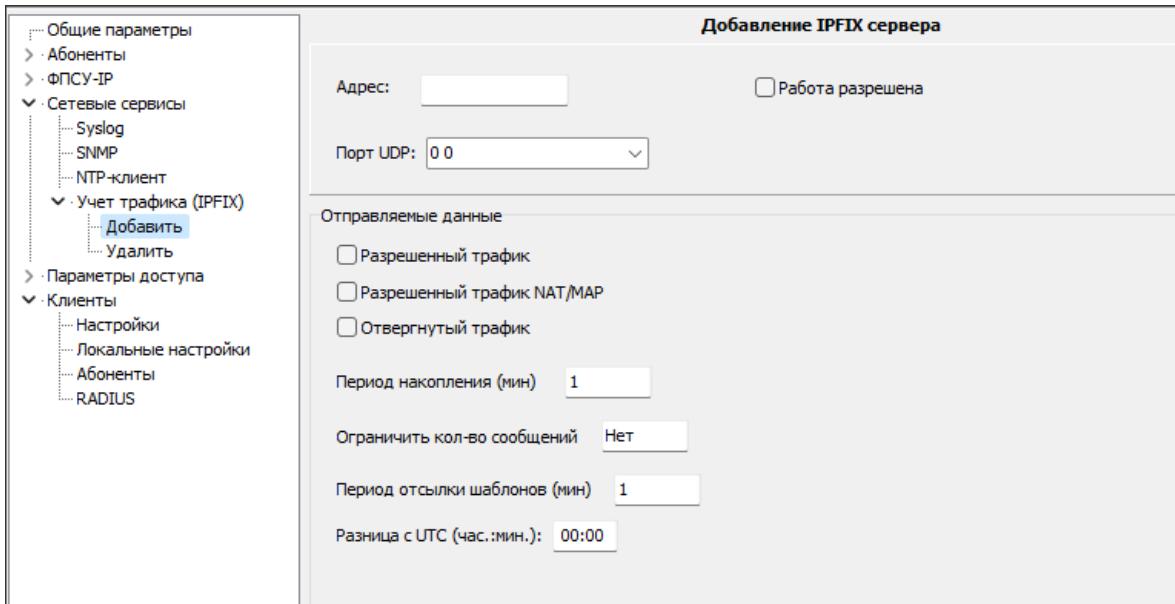


Рисунок 120 - Добавление IPFIX сервера

Включение поддержки IPFIX может замедлять работу межсетевого экрана ФПСУ-IP.

Флаг «Работа разрешена» при включении разрешает отправку шаблонов на указанный IP-адрес коллектора IPFIX.

Отправляемые данные распределяются по нескольким шаблонам в зависимости от типа трафика:

- Разрешенный трафик;
- Разрешенный трафик с NAT/MAP;
- Отвергнутый трафик.

Устанавливаются периоды накопления и отсылки шаблонов в минутах. Может быть задано ограничение на количество сообщений в шаблоне. Устанавливается разница временного пояса, в котором работает ФПСУ-IP, с UTC временем.

По нажатию клавиши <F2> изменения параметров будут внесены в конфигурацию.

Удаление IPFIX сервера

При выборе текущего режима массового изменения конфигураций «Удаление ФПСУ-IP», администратор может удалить IPFIX сервер из списка выбранных конфигураций. Для этого следует задать IP-адрес удаляемого IPFIX сервера и удалить запись по нажатию клавиши <F2>.

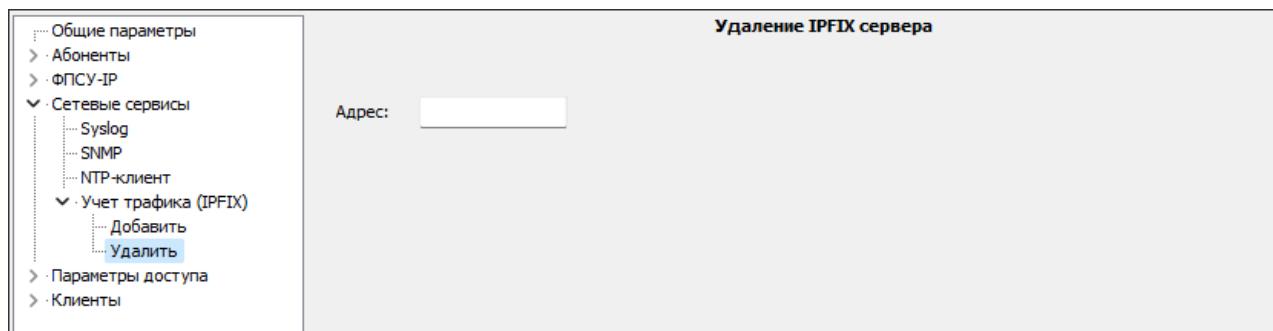


Рисунок 121 - Добавление IPFIX сервера

Данные настройки могут быть сохранены в качестве шаблона. Для этого необходимо дать название шаблону в поле «Шаблон» и нажать кнопку «Сохранить параметры шаблона». Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Шаблон» и могут быть применены в дальнейшем.

11. 7. 5. Изменение параметров межсетевого экрана

11. 7. 5. 1. Добавление/удаление службы

При выборе текущего режима массового изменения конфигураций «Добавление службы», администратор может добавить службу в список выбранных конфигураций ФПСУ-IP.

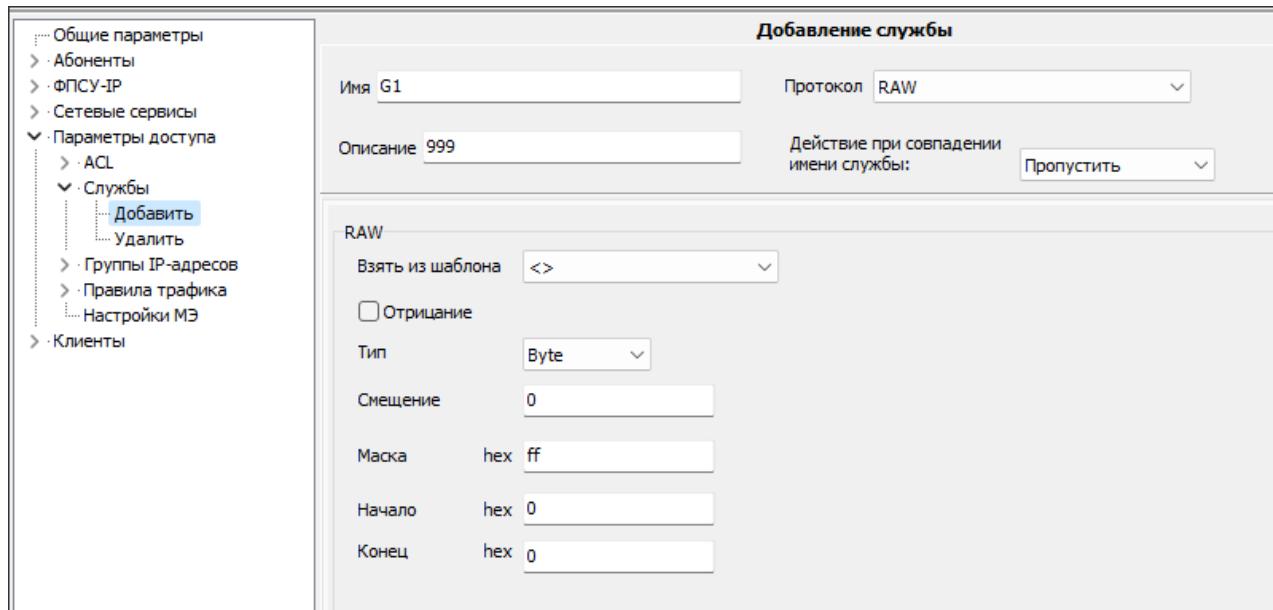


Рисунок 122 - Добавление службы

При добавлении новой службы на ФПСУ-IP через массовое изменение конфигурации ФПСУ-IP доступны следующие параметры:

- «Имя» — обязательный параметр, символьное название службы. Это имя используется администратором для прикрепления службы к правилу трафика, поэтому стоит выдавать как можно более точное название (например, «TCP:80», если правило будет распространяться на протокол TCP, обращающийся к назначению по 80-му порту протокола TCP).
- «Описание» — произвольное текстовое описание службы, опционально.
- «Протокол» — список протоколов передачи данных создаваемой службы. В качестве протокола могут быть выбраны следующие:
 - TCP — служба ограничивает правило трафиком, передаваемым с помощью протокола Transmission Control Protocol;
 - UDP — служба ограничивает правило трафиком, передаваемым с помощью протокола User Datagram Protocol;
 - TCP/UDP — служба ограничивает правило трафиком, передаваемым с помощью протоколов TCP или UDP;
 - ICMP — служба ограничивает правило трафиком, передаваемым с помощью протокола ICMP;
 - Другие (IP) — служба ограничивает правило трафиком, передаваемым с помощью протокола IP;
 - DSCP — служба ограничивает правило трафиком, указанным в поле приоритета согласно RFC 2474 (значение от 0 до 63);
 - RAW — служба, предназначенная для установки произвольных фильтров на основе значений битов заголовков сетевого уровня или на основе символьных строк и регулярных выражений.
- «Действие при совпадении имени службы» - могут быть выбраны следующие действия:
 - Пропустить - служба не будет добавлена в конфигурацию;
 - Перезаписать - найденная служба (последняя добавленная в конфигурацию) будет изменена.
- «Порт источника» и «Порт назначения» — задается для протоколов TCP, UDP или TCP/UDP протоколов. В условии указывается порт отправителя и порт получателя данных соответственно. Можно указать отдельный номер порта или диапазон.

Установленное значение «Любой» означает, что служба будет задействована при передаче любого трафика указанного транспортного протокола.



Рисунок 123 - Условия для протоколов TCP, UDP или TCP/UDP

- «Типы сообщений» - задаются для протокола ICMP. Следует установить флаг для ICMP-сообщений, которые будут обрабатываться создаваемой службой. Установленное значение «Любой» обозначает, что служба включает передачу любого ICMP трафика, всех типов и кодов.



Рисунок 124 - Условия для протокола ICMP

- «Номер протокола» — задается для протокола Другие (IP). В условии указывается номер сетевого протокола, привязанный к создаваемой службе. Можно указать отдельный номер или диапазон. Установленное значение «Любой» обозначает, что служба будет задействована при передаче любого IP трафика.
- «DSCP» - задается часть заголовка IP пакета. В поле указывается приоритет.
- Опции протокола RAW и пример применения службы протокола RAW описываются в руководстве по эксплуатации ФПСУ-IP.

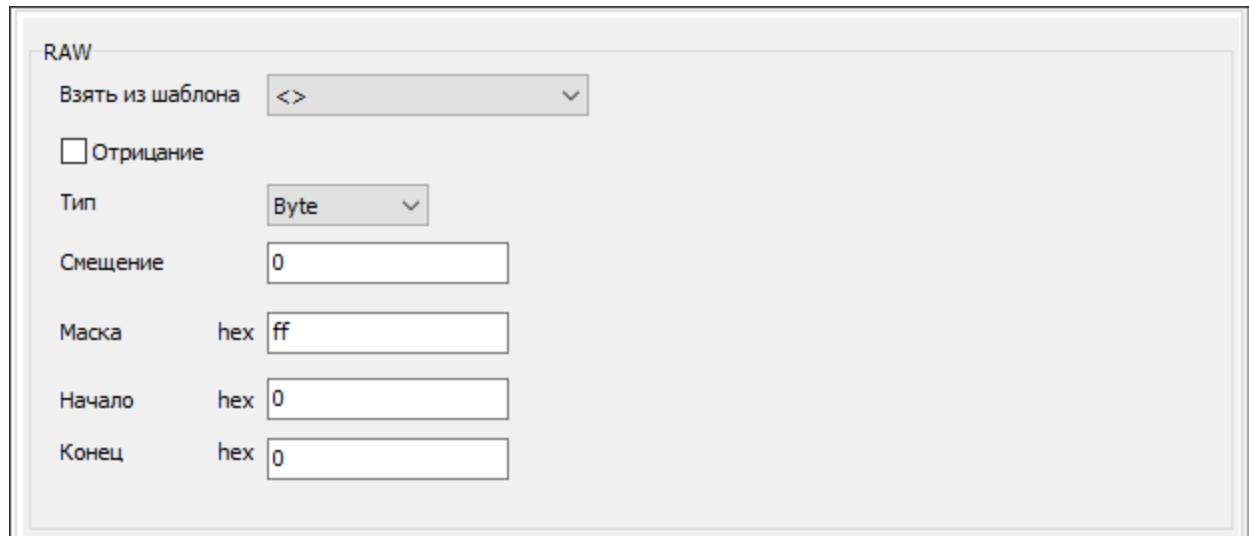


Рисунок 125 - Опции протокола RAW

По нажатию клавиши <F2> служба будет добавлена в конфигурацию.

Данные настройки могут быть сохранены в качестве шаблона. Для этого необходимо дать название шаблону в поле «Шаблон» и нажать кнопку «Сохранить параметры шаблона». Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Шаблон» и могут быть применены в дальнейшем.

Удаление службы

При выборе текущего режима массового изменения конфигураций «Удаление службы», у администратора есть возможность удалить службу или сразу все службы в списке выбранных конфигураций.

При выборе режима в поле «Имя службы» отображается название последней удаленной службы. В поле «Имя службы» необходимо указать полное название службы с учетом регистра символов, в данном поле не поддерживается режим автозаполнения. При необходимости задать действие при наличии нескольких служб с указанным именем. И удалить службу по нажатию клавиши <F2>.

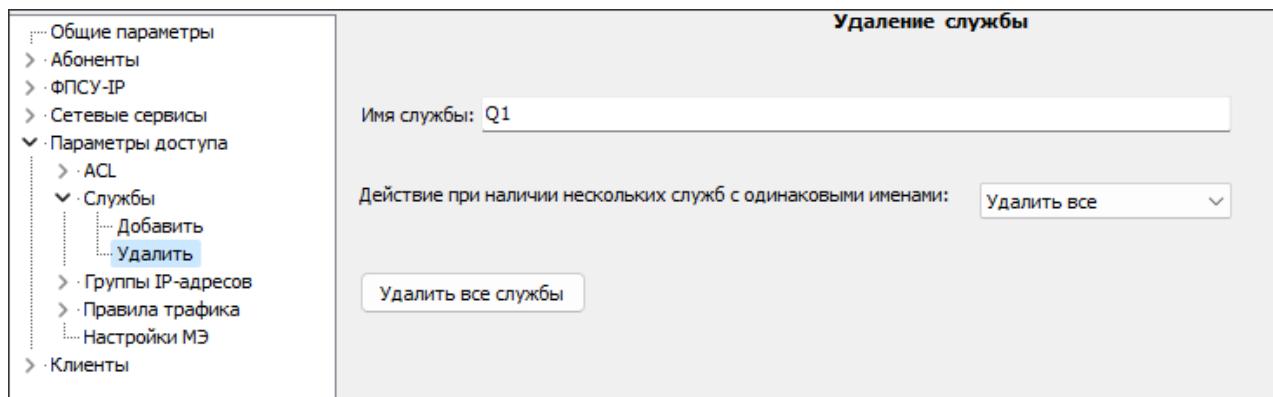


Рисунок 126 - Удаление службы

Могут быть удалены все службы по нажатию соответствующей кнопки.

11.7.5.2. Добавление/удаление группы IP-адресов

При выборе текущего режима массового изменения конфигураций «Добавление группы IP-адресов», администратор может добавить группу IP-адресов в список выбранных конфигураций ФПСУ-IP.

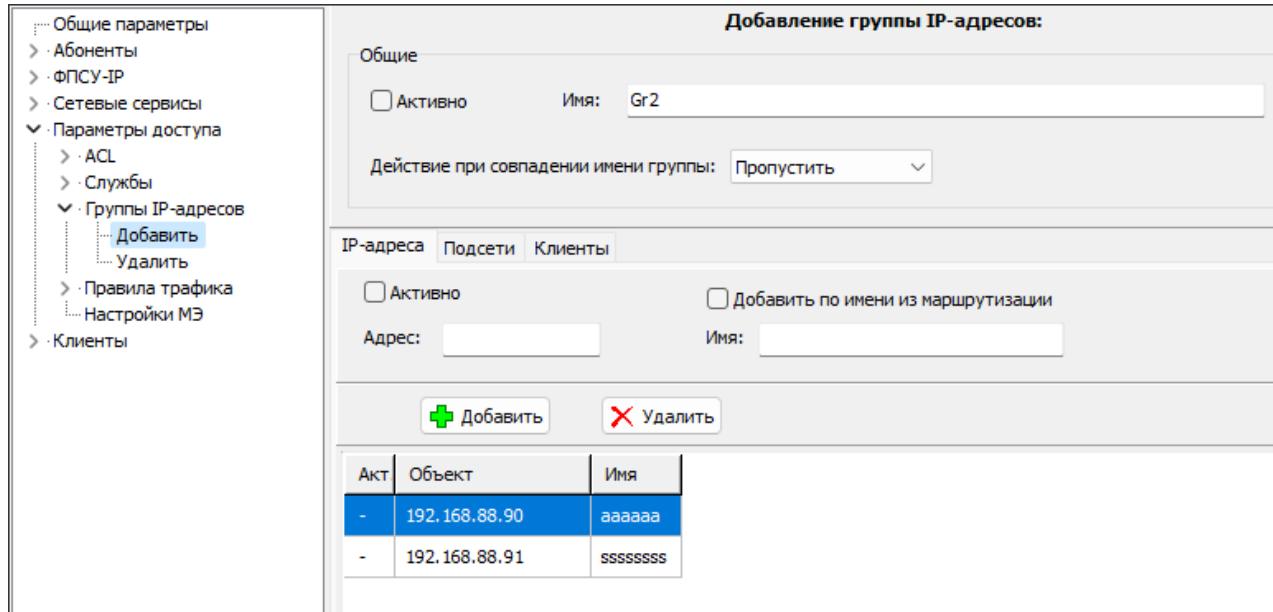


Рисунок 127 - Добавление группы IP-адресов

Добавляемые группы IP-адресов используются при создании и изменении правил трафика.

Для изменения будут доступны следующие параметры:

- «Имя» - символическое название создаваемой группы, которое будет использоваться для привязки группы IP-адресов к тому или иному правилу трафика;
- Флаг «Активно» - подтверждает действие внесенных в группу изменений;
- «Действие при совпадении имени группы» - могут быть выбраны следующие действия:
 - Пропустить - группа не будет добавлена в конфигурацию;
 - Перезаписать - найденная группа (последняя добавленная в конфигурацию) будет изменена.

Вкладки «IP-адреса» и «Подсети»:

- Установленный флаг «Активно» - задействует IP-адрес или подсеть.
- «Адрес» - IP-адрес абонента хоста или IP-адрес подсети с указанием размера маски сети через слеш (<IP-адрес подсети>/<префикс сети>). Должен быть предварительно описан как абонент любого типа, другой ФПСУ-IP или маршрутизатор;
- «Имя» - имя добавляемого объекта, может совпадать с IP-адресом.
- Кнопка «Добавить». По нажатию кнопки указанный объект будет добавлен в список.
- Кнопка «Удалить». По нажатию кнопки выбранный объект в списке будет удален.

Вкладка «IP-адреса» содержит список входящих в группу отдельных IP-адресов (по умолчанию пустой). IP-адреса, вносимые в список, должны принадлежать диапазону описанных и разрешенных к маршрутизации IP-адресов.

Вкладка «Подсети» содержит список входящих в группу подсетей, выбранных из маршрутизации (по умолчанию пустой). Подсети IP-адресов, вносимые в список, должны принадлежать диапазону описанных и разрешенных к маршрутизации IP-адресов.

По нажатию клавиши <F2> группа IP-адресов будет добавлена в конфигурацию.

Данные настройки могут быть сохранены в качестве шаблона. Для этого необходимо дать название шаблону в поле «Шаблон» и нажать кнопку «Сохранить параметры шаблона». Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Шаблон» и могут быть применены в дальнейшем.

Удаление группы IP-адресов

При выборе текущего режима массового изменения конфигураций «Удаление группы IP-адресов», у администратора есть возможность удалить группу или сразу все группы.

При выборе режима в поле «Имя группы IP-адресов» отображается название последней удаленной группы. В поле «Имя группы IP-адресов» указывается полное название группы с учетом регистра символов, в данном поле не поддерживается режим автозаполнения. При необходимости следует задать действие при наличии нескольких групп с указанным именем и удалить группу по нажатию клавиши <F2>.

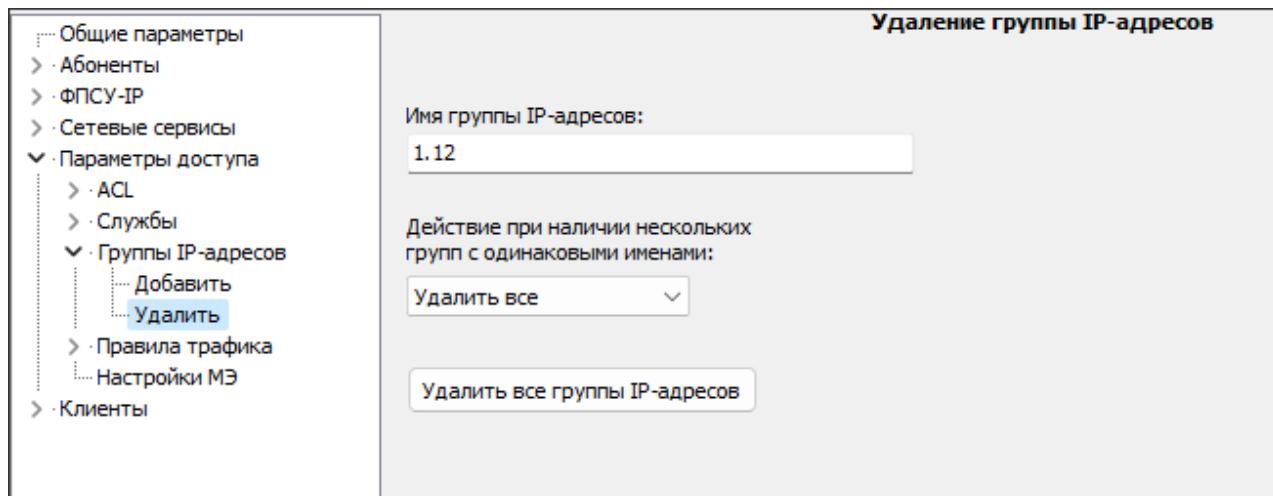


Рисунок 128 - Удаление группы IP-адресов

Могут быть удалены все группы IP-адресов по нажатию соответствующей кнопки.

11. 7. 5. 3. Добавление/удаление правила трафика

При выборе текущего режима массового изменения конфигураций «Добавление правила трафика», администратор может добавить правило в список выбранных конфигураций ФПСУ-IP.

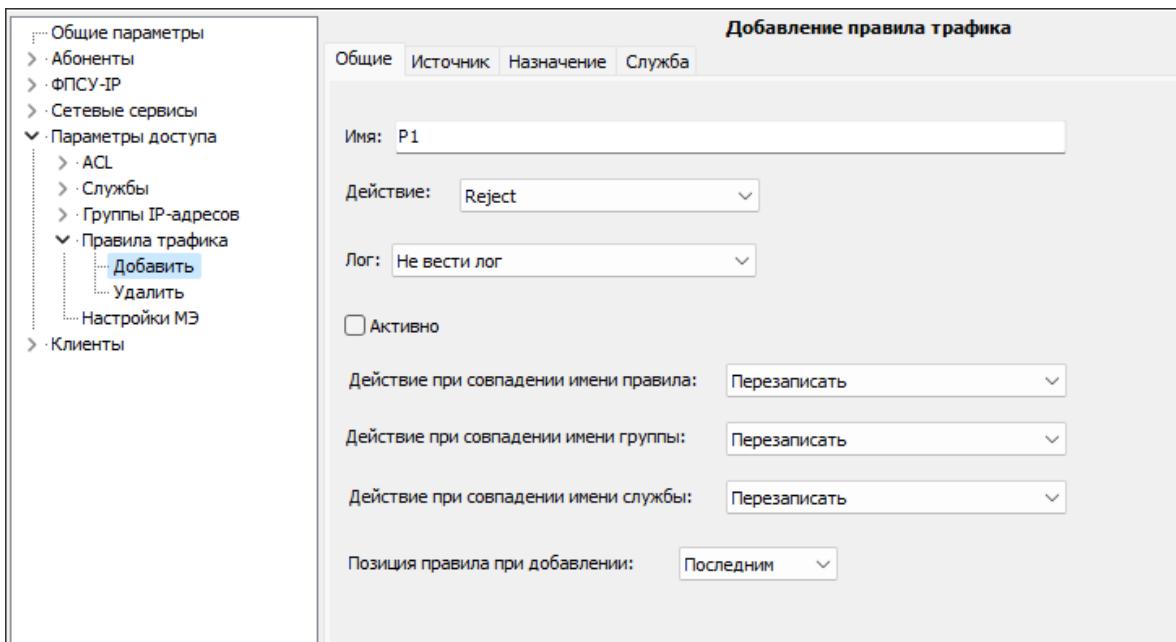


Рисунок 129 - Вкладка «Общие»

Правило трафика применяется только к тем пакетам, IP-адреса источника и назначения которых указаны в соответствующих вкладках. Исключение: если во вкладках «Источник» и «Назначение» нет ни одной записи (список пуст), то правило трафика применяется ко всем пакетам. Вкладка «Службы» позволяет ограничить действие правила не ко всем пакетам, а только тем, которые используют указанные в списке этой вкладки протоколы (службы). Для подробного рассмотрения правил управления трафиком рекомендуется ознакомиться с руководством по эксплуатации ФПСУ-IP.

Для изменения будут доступны четыре вкладки с настраиваемыми опциями:

Вкладка «Общие»

- «Имя» - наименование правила, обязательное произвольное текстовое поле.
- «Действие» — обязательное правило, определяющее, как поступить с передаваемым пакетом. В выпадающем меню могут быть выбраны следующие варианты основного действия:
 - Drop — действие по умолчанию, пакет данных будет сброшен, ICMP-оповещение об отказе передачи пакета не будет передано отправителю;
 - Reject — пакет данных будет сброшен, отправителю будет передано ICMP-оповещение об отказе передачи пакета;
 - Accept — пакет данных будет передан по назначению.

- «Лог» — если требуется вести журнал, содержащий разрешенные и запрещенные в рамках данного правила передачи данных, то следует выбрать из выпадающего списка опцию «Вести лог» или «Вести лог, писать заголовки пакетов». Значение по умолчанию - «Не вести лог».
- Флаг «Активно» позволяет задействовать все настройки указанные в правиле.
- «Действие при совпадении имени правила» - могут быть выбраны следующие действия:
 - Пропустить - новое правило не будет добавлена в конфигурацию;
 - Перезаписать - найденное правило (последнее добавленное в конфигурацию) будет изменено.
- «Действие при совпадении имени группы» - могут быть выбраны следующие действия:
 - Использовать найденную группу - найденная группа (последняя добавленная в конфигурацию) будет добавлена в правило;
 - Пропустить - новая группа не будет добавлена в правило;
 - Перезаписать - найденная группа (последняя добавленная в конфигурацию) будет изменена.
- «Действие при совпадении имени службы» - могут быть выбраны следующие действия:
 - Использовать найденную службу - найденная служба (первая добавленная в конфигурацию) будет добавлена в правило;
 - Пропустить - новая служба не будет добавлена в правило;
 - Перезаписать - найденная служба (последняя добавленная в конфигурацию) будет изменена.
- «Позиция правила при добавлении». Правила располагаются в списке правил трафика по приоритету, и, в случае возникновения взаимоисключающих настроек, будет работать правило, находящееся выше по списку. Поле «Позиция» позволяет указывать приоритет правила при добавлении.

Вкладки «Источнику» и «Назначение» содержат списки объектов, к которым будет применяться правило трафика.

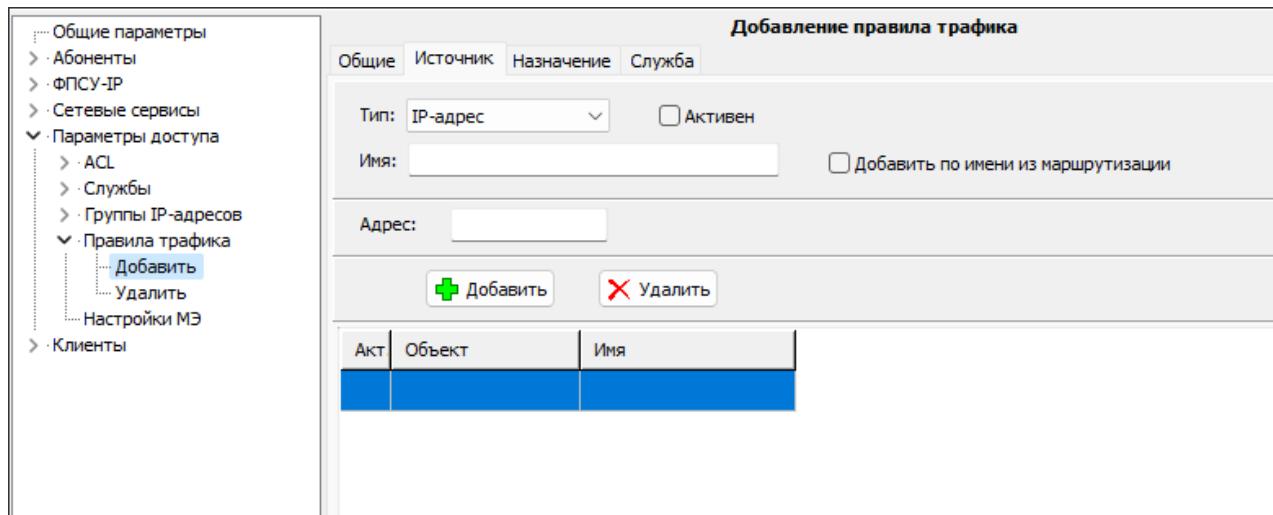


Рисунок 130 - Вкладка «Источник»

- «Тип» - указывается тип добавляемого объекта: IP-адрес, подсеть или группа IP-адресов. Подсеть должна быть выбрана из диапазона подсетей, прописанных в маршрутизации на портах ФПСУ-IP, либо входить в такую. Логическая группа IP-адресов должна быть заранее создана.
- Флаг «Активен». Каждая запись добавляется в список вкладок Источник или Назначение в состоянии активна или не активна. Если флаг снят, то объект будет добавлен в список, но правило трафика по нему отрабатывать не будет.
- «Имя» - имя добавляемого объекта, может совпадать с IP-адресом.
- «Адрес» - указываемый IP-адрес должен быть предварительно описан как абонент любого типа, другой ФПСУ-IP или маршрутизатор.
- «Список групп». Для выбранного типа «Группа IP-адресов» из списка выбирается наименование группы.
- Кнопка «Добавить». По нажатию кнопки указанный объект будет добавлен в список.
- Кнопка «Удалить». По нажатию кнопки выбранный объект в списке будет удален.

Вкладка «Служба» содержит список служб: дополнительных фильтров, указывающих межсетевому экрану ФПСУ-IP на необходимость применения правила трафика к соединению абонентов из списков «Источнику» и «Назначение».

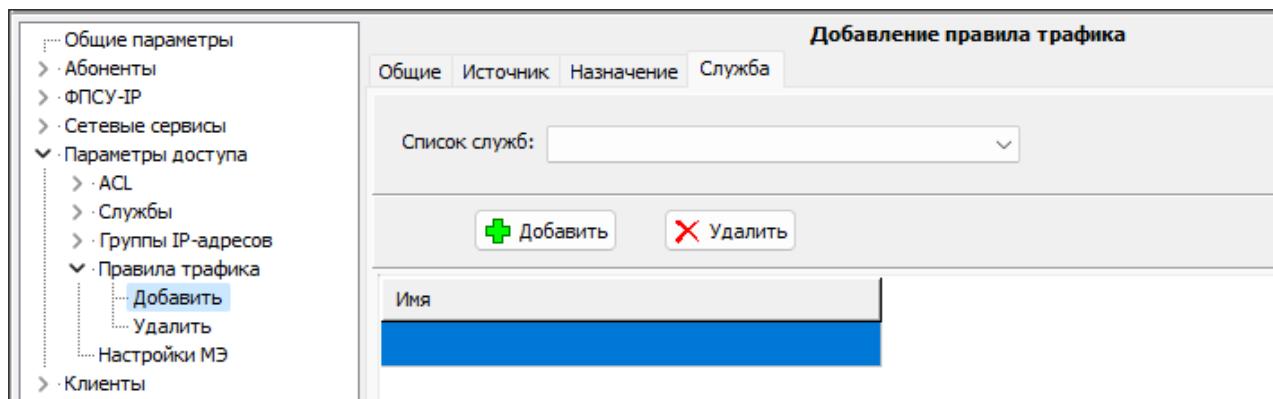


Рисунок 131 - Вкладка «Служба»

- «Список служб». Для внесения новой службы в список, нажмите кнопку «Добавить службу» и выберите из появившегося перечня заранее созданных шаблонов служб.

По нажатию клавиши <F2> правило трафика будет добавлено в конфигурацию.

Данные настройки могут быть сохранены в качестве шаблона. Для этого необходимо дать название шаблону в поле «Шаблон» и нажать кнопку «Сохранить параметры шаблона». Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Шаблон» и могут быть применены в дальнейшем.

Удаление правила трафика

При выборе текущего режима массового изменения конфигураций «Удаление правила трафика», у администратора есть возможность удалить одно правило или сразу все правила трафика.

При выборе режима в поле «Имя правила трафика» отображается название последнего удаленного правила. В поле «Имя правила трафика» указывается полное название правила с учетом регистра символов, в данном поле не поддерживается режим автозаполнения. При необходимости следует задать действие при наличии нескольких правил с указанным именем и удалить правило по нажатию клавиши <F2>.

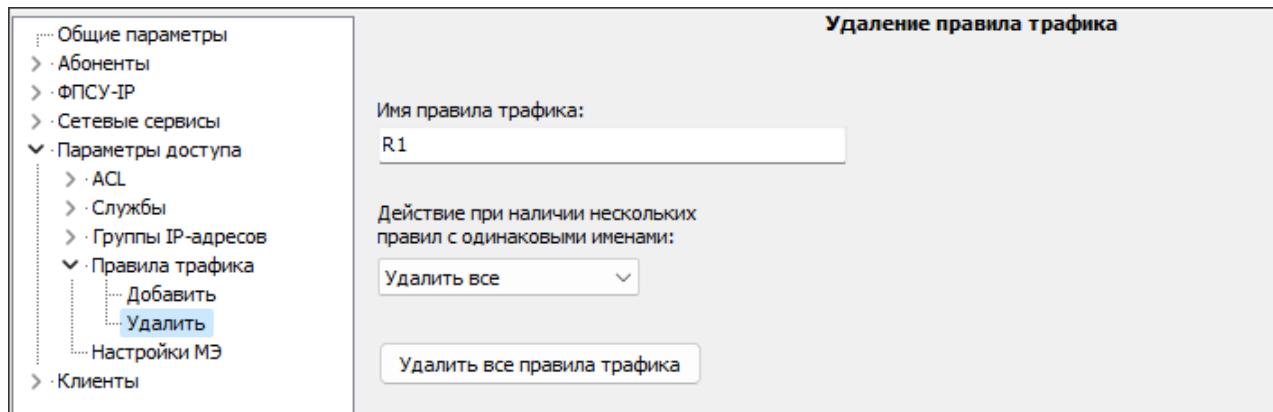
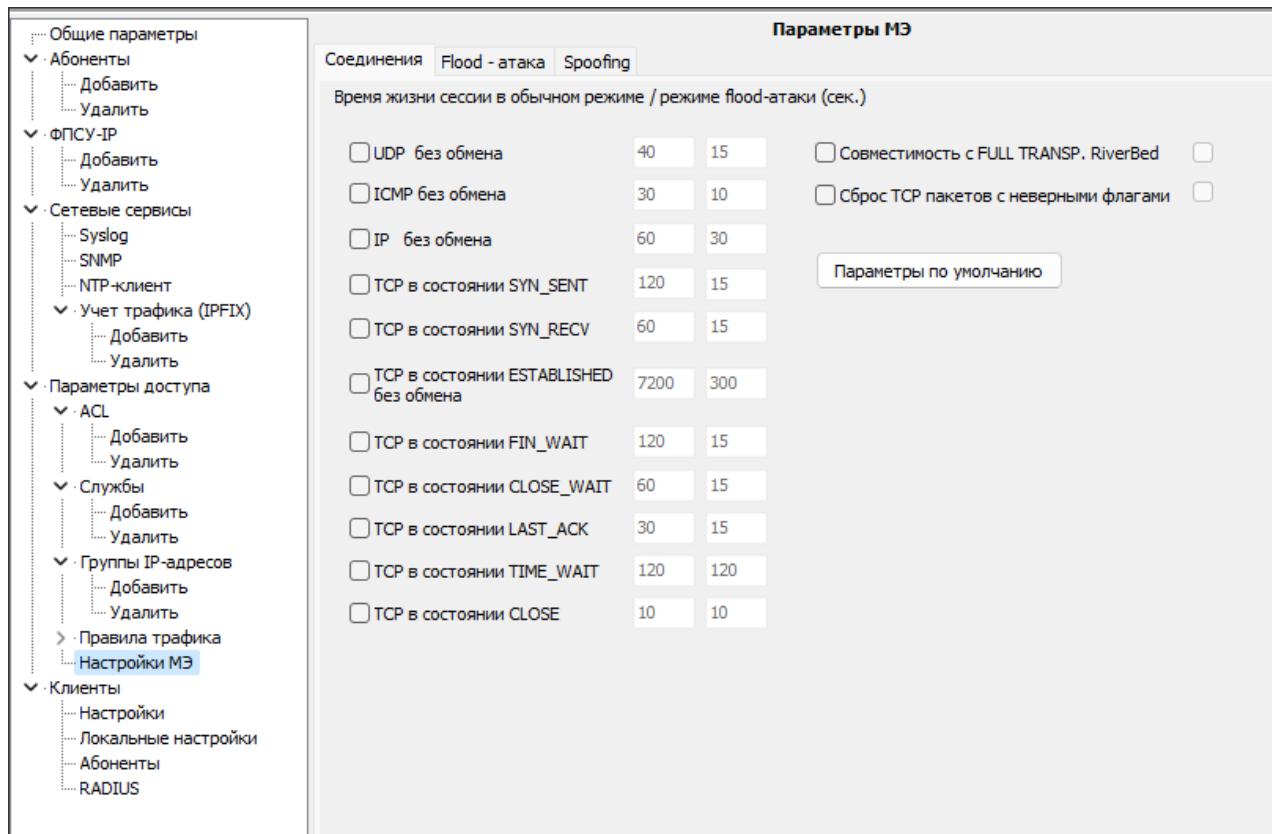


Рисунок 132 - Изменение конфигурации

В случае если удалены все правила по нажатию соответствующей кнопки, то список правил становится пустым. Ограничения на передачу трафика отменяются. В этом случае все пакеты передаются в соответствии с заданными основными правилами фильтрации и маршрутизации абонентского трафика.

11. 7. 5. 4. Изменение настроек МЭ

Данный пункт содержит список дополнительных опций межсетевого экрана.

**Рисунок 133 - Параметры ограничения соединений**

Окно состоит из трех вкладок. Первые две, «Соединения» и «Flood-атака», предназначены для настройки системы защиты ФПСУ-IP от атак отказа в обслуживании (flood-атак).

Вкладка «Соединения» содержит установленные по умолчанию параметры работы межсетевого экрана ФПСУ-IP с IP/TCP/UDP соединениями в обычном режиме и в режиме после обнаружения атаки.

Здесь настраиваются таймауты, по истечению которых неактивное соединение будет удалено из внутренней таблицы контроля соединений межсетевого экрана. Указывается два типа таймаутов – время удаления записи о соединении из таблицы при штатном режиме работы ФПСУ-IP (первый столбец), и время обнаружения атаки отказа в обслуживании (второй столбец).

Учитываются таймауты удаления из таблицы контроля соединения межсетевого экрана для следующих типов соединений:

- UDP без обмена – соединением в этом случае считается трафик между уникальными UDP портами разных IP-адресов абонентов ФПСУ-IP. В случае отсутствия UDP-

трафика по указанным портам, по таймауту запись о соединении удаляется из таблицы;

- ICMP без обмена – соединением в этом случае считается ICMP обмен между двумя абонентами ФПСУ-IP. В случае отсутствия обмена ICMP-сообщениями в течение указанного таймаута, запись о соединении удаляется из таблицы;
- IP без обмена – соединением в этом случае считаются все прочие виды трафика между двумя абонентами, не являющиеся TCP, UDP или ICMP. Запись удаляется из таблицы по таймауту при отсутствии новых обменов;
- TCP в состоянии ... – учитывается каждое соединение с разными TCP портами отправителя и получателя между любой парой абонентов ФПСУ-IP. По таймауту запись будет удалена из таблицы, и дальнейшее взаимодействие между этой парой абонентов должно будет начаться с повторного установления TCP-соединения. Новые пакеты, не относящиеся к установлению TCP-соединения, после удаления записи из таблицы будут сброшены. Для каждого состояния TCP-соединения используется одна запись в таблице контроля соединений межсетевого экрана ФПСУ-IP, но таймауты различаются.
- Совместимость с FULL TRANSP. RiverBed – флаг, активирующий на ФПСУ-IP механизм совместимости с оптимизаторами трафика RiverBed, которые отклоняются от стандартных схем работы TCP-соединений (в том разрешение на пропуск ACK без данных).
- Сброс TCP-пакетов с неверными флагами – флаг, указывающий межсетевому экрану ФПСУ-IP сбрасывать пакеты, в IP-заголовке которых обнаружены некорректные (не соответствующие рекомендуемым RFC) комбинации флагов протокола TCP.

Вкладка «Flood-атака» содержит параметры, по которым ФПСУ-IP определяет начало атаки в свои адреса или адреса защищаемых абонентов и управляет списком заблокированных IP-адресов.

Следует учитывать, что ФПСУ-IP безусловно переходит в режим защиты от flood-атаки, если оперативная память ФПСУ-IP загружается на 100%.

В режиме защиты от flood-атаки ФПСУ-IP использует тайминги удаления соединений, указанные во вкладке Соединения, а также заносит в стоп-лист IP-адреса абонентов, передающих больше пакетов в секунду, чем разрешено настройками.



Рисунок 134 - Параметры работы ФПСУ-IP во время flood атаки

ФПСУ-IP переходит в режим защиты от атаки, если превышен хотя бы один из следующих критериев:

- Максимальное кол-во новых TCP соединений (шт./сек.) – количество новых, то есть отсутствующих в таблице контроля соединений межсетевого экрана, TCP-соединений в секунду;
- Максимальное кол-во новых UDP соединений (шт./сек.) – количество новых, то есть между новыми парами IP-адресов: UDP-порт, UDP-обменов в секунду;
- Максимальное кол-во новых ICMP обменов (шт./сек.) – количество новых ICMP-обменов в секунду;
- Максимальное кол-во новых ICMP пакетов (шт./сек.) – общее количество ICMP эхо-запросов (и только эхо-запросов) в секунду.

Во время защиты от flood-атаки, ФПСУ-IP начинает считать количество пакетов в секунду, отправленных с IP-адресов абонентов. Если это число превышает параметр «Максимальное кол-во соединений с IP-адреса (шт./сек.)», то этот IP-адрес заносится в стоп-лист, то есть все исходящие от него пакеты будут блокироваться.

- Анти-флуд включен. Если флаг «Flood control» установлен, то IP-адрес будет находиться в стоп-листе в течение времени, указанного в поле «Время нахождения в

стоп-листе (мин.)». Если флаг «Flood control» не установлен, то IP-адрес будет находиться в стоп-листе до перезагрузки ФПСУ-IP.

Флаг «Flood control» влияет на активность параметров «Максимальное кол-во новых TCP соединений (шт./сек.)», «Максимальное кол-во новых UDP соединений (шт./сек.)», «Максимальное кол-во новых ICMP обменов (шт./сек.)», «Максимальное кол-во соединений с IP-адреса (шт./сек.)». Если флаг снят, то ФПСУ-IP будет переходить в режим защиты от flood-атаки только в случаях полной загрузки оперативной памяти и в случае превышения порога ICMP эхо-запросов.

- На момент начала атаки ФПСУ-IP запоминает общее количество всех типов соединений – это значение потребуется для определения времени завершения атаки. Для начала выхода ФПСУ-IP из режима защиты от flood-атак, общее количество соединений сначала должно упасть до указанной в поле «Процент flood-соединений – атака считается завершенной» доли соединений, по сравнению с количеством соединений на начало атаки.
- После первоначального уменьшения соединений до процентного значения, указанного в поле «Процент flood-соединений – атака считается завершенной», ФПСУ-IP запускает таймер обратного отсчета, с указанным в поле «Начальный интервал ожидания flood-атаки (мин.)» значением. Если в течение этого времени общее количество соединений не поднялось обратно выше порога, то атака считается завершенной и ФПСУ-IP переходит в обычный режим работы.
- Если общее количество соединений за указанное время превысило пороговое значение, то ФПСУ-IP остается в режиме защиты от flood-атаки, таймер увеличивается в полтора раза и запускается заново. Максимальное значение таймера указывается в поле «Максимальный интервал ожидания Flood-атаки (мин.)».

Вкладка «Spoofing» содержит параметры, отвечающие за работу ФПСУ-IP с TCP-соединениями в режиме spoofing на медленных каналах связи.

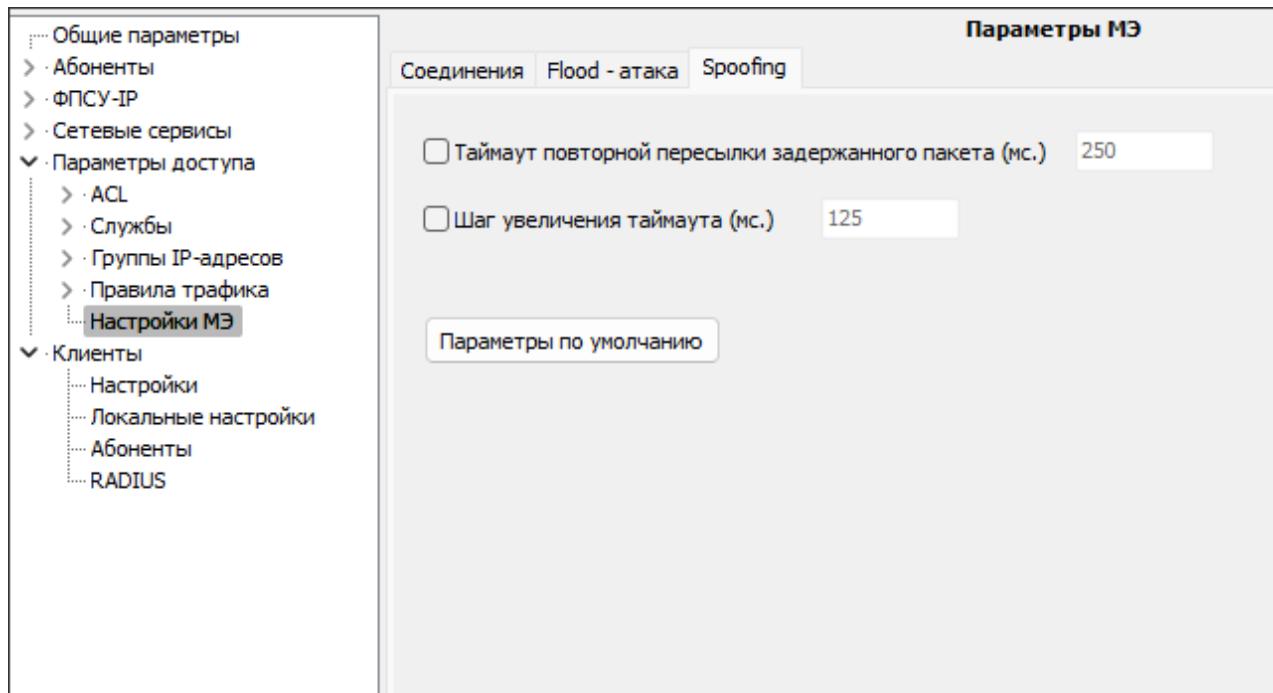


Рисунок 135 - Параметры передачи подтверждений в режиме Spoofing

Некоторые параметры отправки подтверждения о передаче пакета получателем отправителю самостоятельно, без подтверждения от получателя, можно изменить, а именно:

- Таймаут повторной пересылки задержанного пакета (мс.) – время в миллисекундах, через которое ФПСУ-IP будет проводить повторную пересылку пакета, в отсутствие ответа от получателя;
- Шаг увеличения таймаута (мс.) – с каждым разом повторной отправки пакета, время очередного повтора пересылки увеличивается на указанное в этом параметре количество миллисекунд.

11. 7. 6. Изменение Клиентских настроек

11. 7. 6. 1. Изменение клиентов

При выборе текущего режима массового изменения конфигураций «Клиенты → Настройки», администратор может изменить настройки работы Клиентами в шаблоне конфигурации ФПСУ-IP.

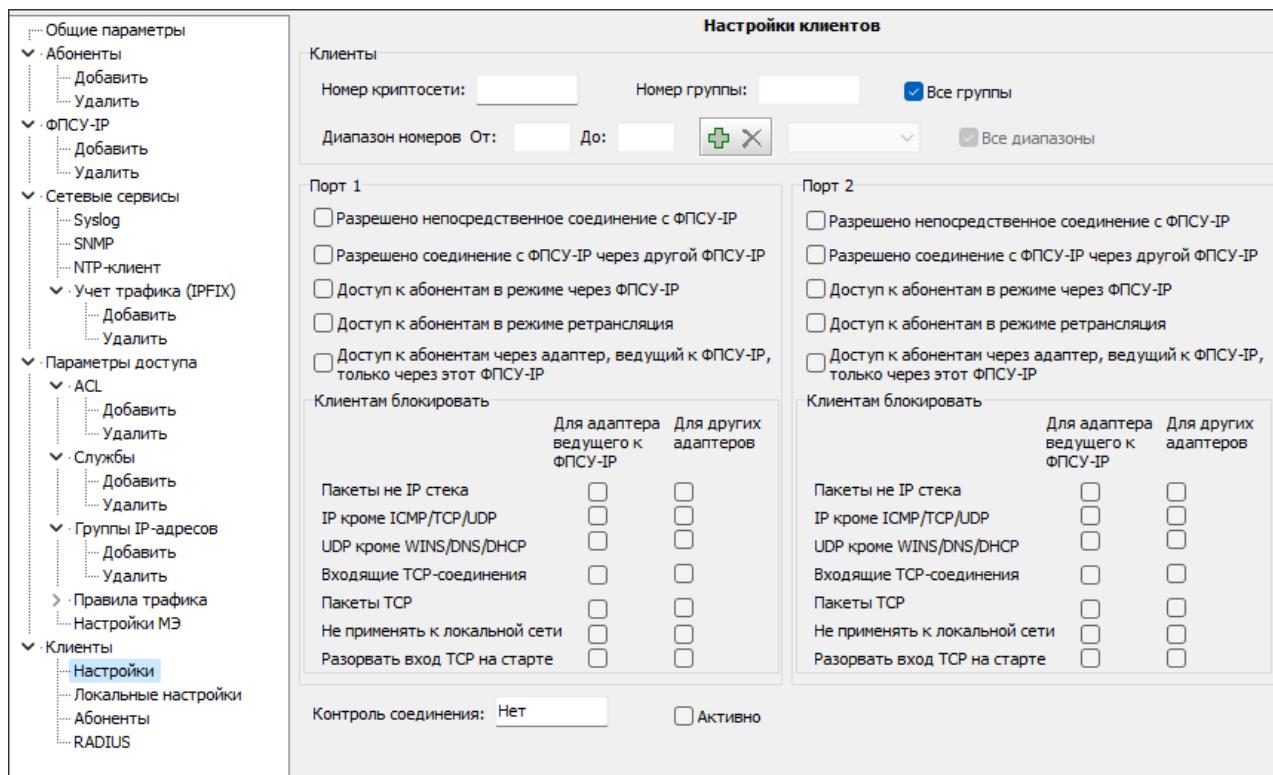


Рисунок 136 - Изменение настроек для работы с клиентами

- «Клиенты» — пункт включает в себя номер криптосети, номер логической группы пользователей, диапазон номеров генерации; при этом предусматривается возможность выбрать все группы и/или все диапазоны путем установки одноименных флагов.
- Порт 1/Порт 2- номера внешнего и внутреннего порта соответственно.
- Разрешено непосредственное соединение с ФПСУ-IP - разрешение ФПСУ-IP производить соединения с клиентами со стороны данного порта в задаваемом режиме (обмениваться данными с описываемыми клиентами непосредственно).
- Разрешено соединение с ФПСУ-IP через другой ФПСУ-IP - разрешение ФПСУ-IP производить соединения с клиентами со стороны данного порта в задаваемом режиме (обмениваться данными с описываемыми клиентами через другой ФПСУ-IP).
- Доступ к абонентам в режиме ФПСУ- разрешение ФПСУ-IP предоставлять клиентам, работающим со стороны данного порта, доступ к станциям назначения только в задаваемом режиме (обмен между абонентом и портом ФПСУ-IP будет производиться через туннель со смежным ФПСУ-IP).
- Доступ к абонентам в режиме ретрансляция - разрешение ФПСУ-IP предоставлять

клиентам, работающим со стороны данного порта, доступ к станциям назначения только в задаваемом режиме обмен данных ФПСУ-IP с абонентом осуществляется без шифрования, соединения с ним только фильтруются межсетевым экраном).

- Доступ к абонентам через адаптер, ведущий к ФПСУ-IP, только через этот ФПСУ-IP - опция, изменяющая сетевые настройки на стороне рабочей станции Клиента. После её включения, все IP-пакеты, отправляемые рабочей станцией Клиента через сетевой адаптер, ведущий к ФПСУ-IP, будут зашифрованы и отправлены в туннель к ФПСУ-IP. При включении опции открытые соединения рабочей станции Клиента через ведущий к ФПСУ-IP сетевой адаптер будут невозможны;

Правила блокировки межсетевого экрана со стороны Клиентов состоят из следующих полей:

- Пакеты не IP стека — блокируются пакеты, не принадлежащие к стеку протоколов TCP/IP (например, блокируются протоколы PPP и PPPoE);
- IP кроме PING/TCP/UDP — блокируются все пакеты стека протоколов TCP/IP, кроме эхо-запросов (ping) и транспортных протоколов TCP и UDP;
- UDP кроме WINS, DNS, DHCP — блокируются все UDP пакеты, кроме WINS, DNS, DHCP;
- Входящие TCP-соединения — блокируются все IP пакеты с TCP трафиком, если инициатором соединения является другой хост;
- Пакеты TCP — блокируются все TCP соединения;
- Не применять к локальной сети — не использовать все указанные выше блокировки, если рабочая станция Клиента взаимодействует с хостами своей собственной подсети;
- Разорвать вход TCP на старте — после установления соединения с ФПСУ-IP принудительно завершить все TCP-соединения, инициатором которых является другой хост.

В группе флагов нужно отметить те соединения, которые будут запрещены во время сеансов с ФПСУ-IP. Ограничения на прием и передачу пакетов могут быть установлены как для сетевого адаптера, связанного с ФПСУ-IP, так и для других сетевых адаптеров ФПСУ-IP/Клиент.

11.7.6.2. Изменение локальных настроек

При выборе текущего режима массового изменения конфигураций «Клиенты→Локальные настройки», администратор может изменить локальные настройки работы с Клиентами.

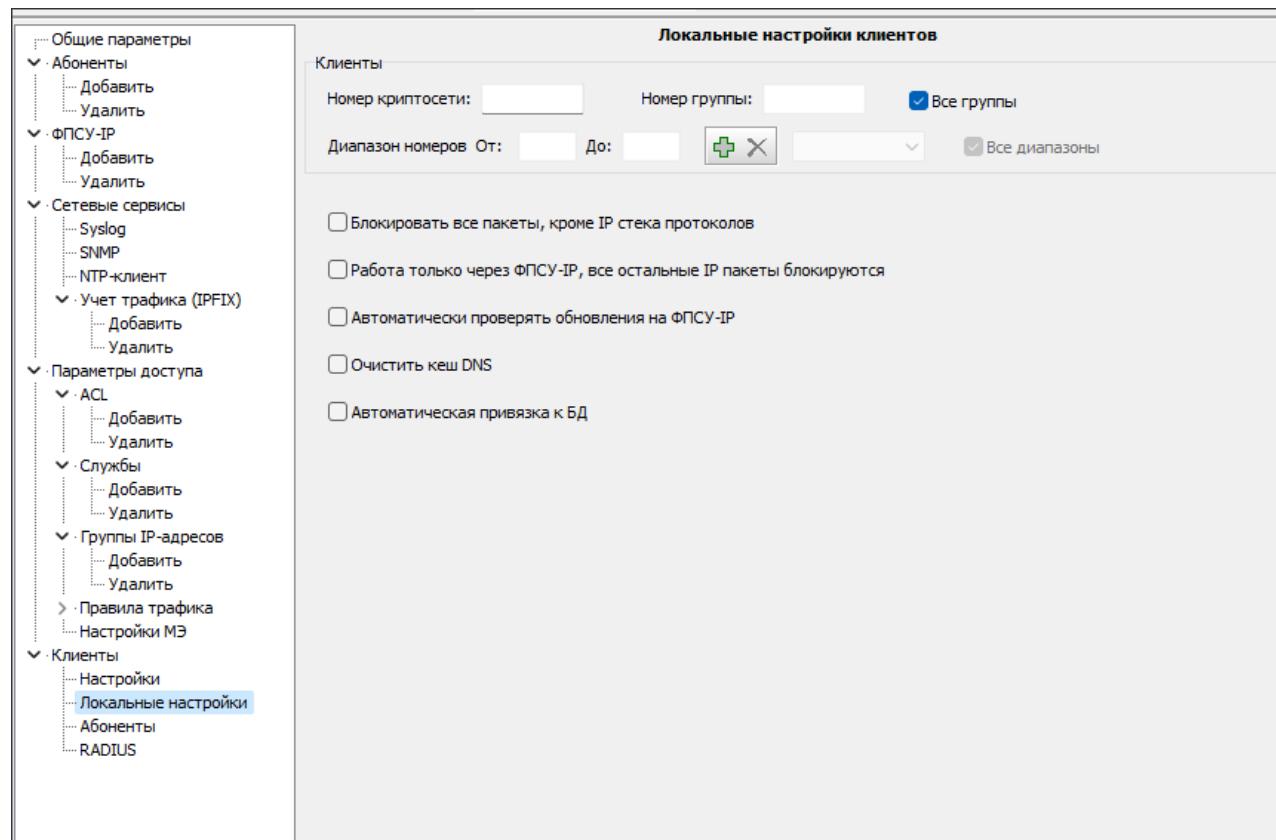


Рисунок 137 - Настройка локального межсетевого экрана ФПСУ-IP/Клиента

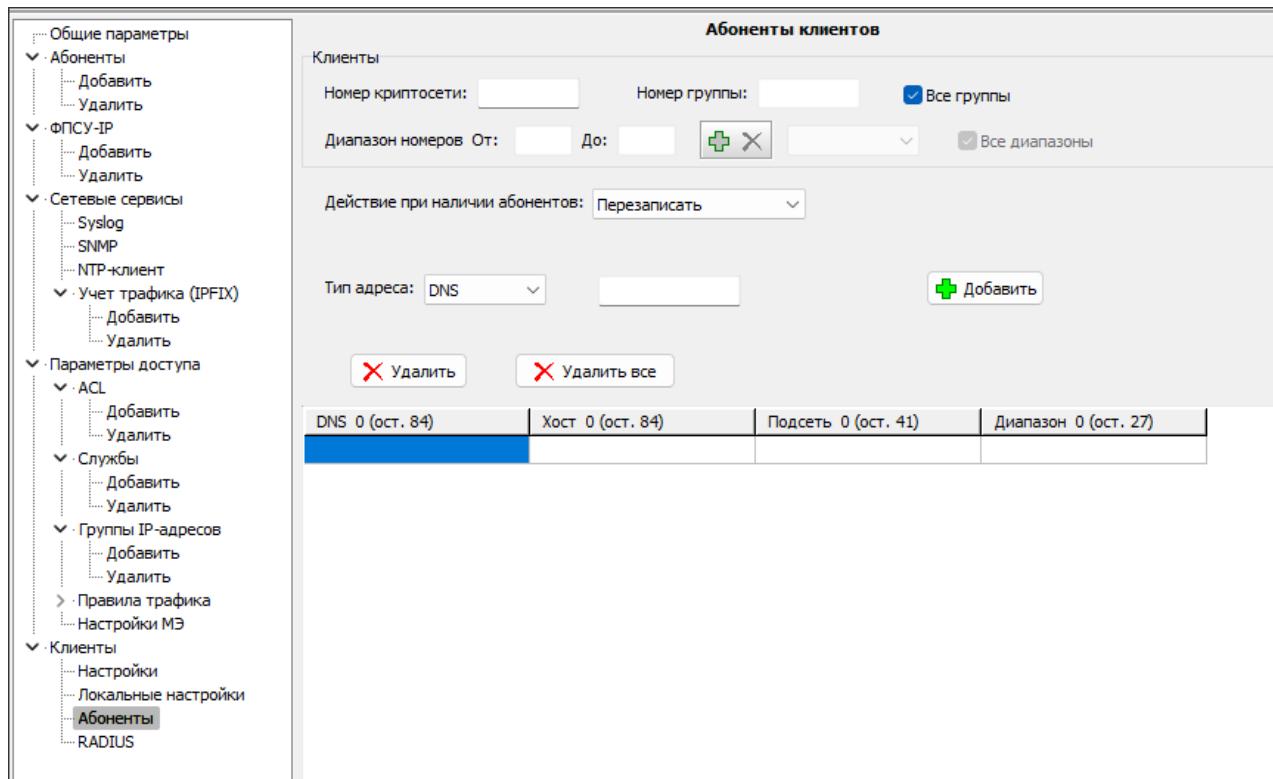
- «Клиенты» — пункт включает в себя номер криптосети, номер логической группы пользователей, диапазон номеров генерации; при этом предусматривается возможность выбрать все группы и/или все диапазоны путем установки одноименных флагов.
- «Блокировать все пакеты, кроме IP-стека протоколов» – установленный флаг означает, что при приеме и передаче все пакеты, не соответствующие формату пакетов стека TCP/IP, будут сброшены.
- «Работа только через ФПСУ - IP, остальные IP-пакеты блокируются» – установленный флаг означает, что, при отсутствии соединения между ФПСУ-IP/Клиент и ФПСУ-IP, рабочая станция с установленным программным

обеспечением ФПСУ-IP/Клиент будет блокировать передачу в сеть всех IP пакетов, кроме служебных в адрес ФПСУ-IP. После установления соединения между ФПСУ-IP/Клиент и ФПСУ-IP блокировка передачи пакетов в сеть с помощью этой опции не осуществляется.

- «Автоматически проверять обновления на ФПСУ-IP» - флаг проверки новых версий программного обеспечения ФПСУ-IP/Клиент.
- «Очистить кэш DNS» - установленный флаг позволяет очистить локальный кэш DNS рабочей станции.
- Очистить кэш DNS - флаг, при установке которого выполняется сброс кэша DNS на рабочей станции ФПСУ-IP/Клиента при установлении соединения с ФПСУ-IP.
- Автоматическая привязка в БД - установленный флаг позволяет привязать Клиента к рабочей станции или устройству с установленным программным обеспечением ФПСУ-IP/Клиент, чтобы пользователь мог работать с этим Клиентом только на одном компьютере. Привязка клиента хранит данные о серийных номерах ОС (только для Windows), материнской платы и системного диска устройства с установленным программным обеспечением ФПСУ-IP/Клиент в базе данных на ФПСУ-IP. Каждый раз при подключении ФПСУ-IP/Клиента к ФПСУ-IP эти данные сверяются, в случае подключения клиента с другого устройства работа данного клиента блокируется. База данных с привязками клиентов синхронизируется с дополнительным ФПСУ-IP, заданным в настройках ФПСУ-IP/Клиента.

11. 7. 6. 3. Абоненты

При выборе текущего режима массового изменения конфигураций «Клиенты → Абоненты», администратор может создать или скорректировать список абонентов путем создания списка передаваемых клиенту IP-адресов.



«Клиенты» — пункт включает в себя номер криптосети, номер логической группы пользователей, диапазон номеров генерации; при этом предусматривается возможность выбрать все группы и/или все диапазоны путем установки одноименных флагов.

Абонентами могут выступать описатели отдельного IP-адреса («Хост»), подсети («Подсеть»), диапазон последовательно идущих IP-адресов («Диапазон») и специальный абонент «DNS» («DNS»).

11. 7. 6. 4. Настройки RADIUS

RADIUS (Remote Authentication in Dial-In User Service) — протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и оборудованием. При выборе текущего режима массового изменения конфигураций «Настройки RADIUS», администратор может добавить нужные настройки для аутентификации ФПСУ-IP/Клиентов в сети.

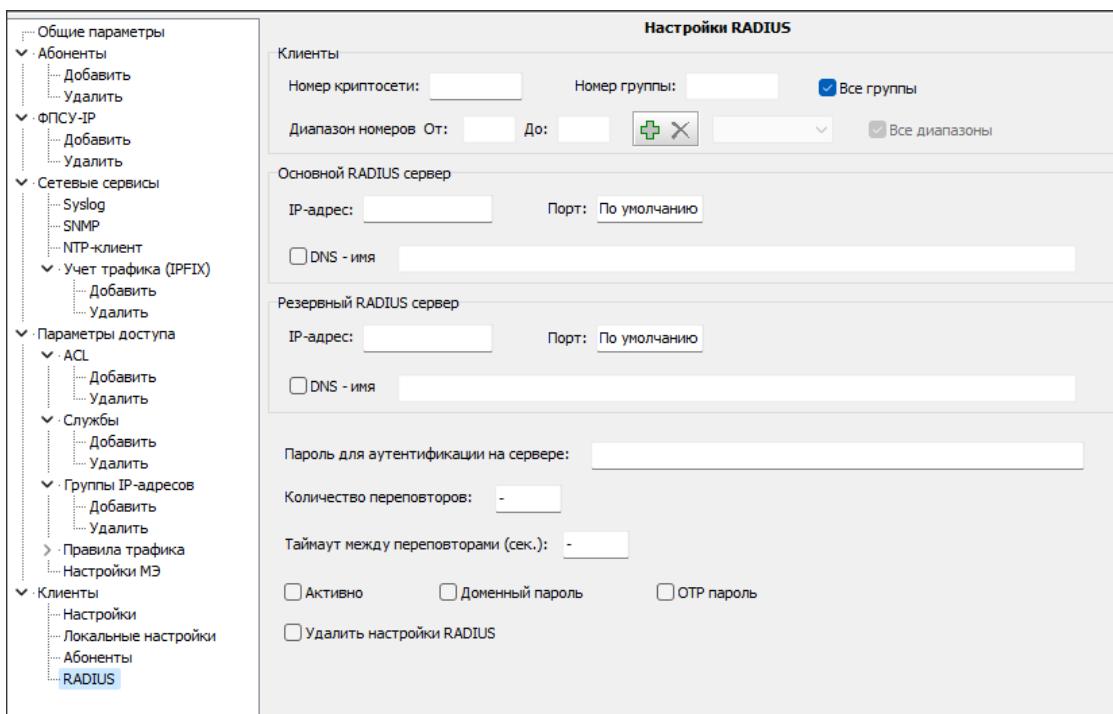


Рисунок 138 - Изменение конфигурации по шаблону

- «Клиенты» — пункт включает в себя номер криптосети, номер логической группы пользователей, диапазон номеров генерации; при этом предусматривается возможность выбрать все группы и/или все диапазоны путем установки одноименных флагов.
- «Основной/резервный RADIUS сервер» — в поле необходимо ввести IP-адрес сервера. RADIUS сервер разрешает или запрещает работу ФПСУ-IP/Клиента, в зависимости от полученных данных аутентификации, ФПСУ-IP получает сведения и отправляет на RADIUS сервер.
- «Пароль для аутентификации на сервере» — ФПСУ-IP является RADIUS-клиентом и проходит аутентификацию на RADIUS-сервере с данным паролем. Требования к паролю определяются RADIUS-сервером.
- «Количество переповторов» - количество переповторов запроса пароля в случае отсутствия ответа RADIUS сервера.

По нажатию клавиши <F2> изменения будут внесены в выбранные конфигурации ФПСУ-IP.

Данные настройки могут быть сохранены в качестве шаблона. Для этого необходимо дать название шаблону в поле «Шаблон» и нажать кнопку «Сохранить параметры шаблона». Сохраненные в УА ФПСУ-IP шаблоны отображаются в списке «Шаблон» и могут быть

применены в дальнейшем.

11. 8. Массовая замена объектов межсетевого экрана

УА ФПСУ-IP предоставляет администратору УА ФПСУ-IP возможность создания задач массовой замены параметров межсетевого экрана. При этом выбирается исходная конфигурация, в которую, по необходимости, вносятся изменения, после чего данная конфигурация устанавливается на необходимые ФПСУ-IP. Окно управления такими задачами вызывается выполнением команды главного меню УА ФПСУ-IP «Конфигурации» → «Массовая замена элементов МЭ».

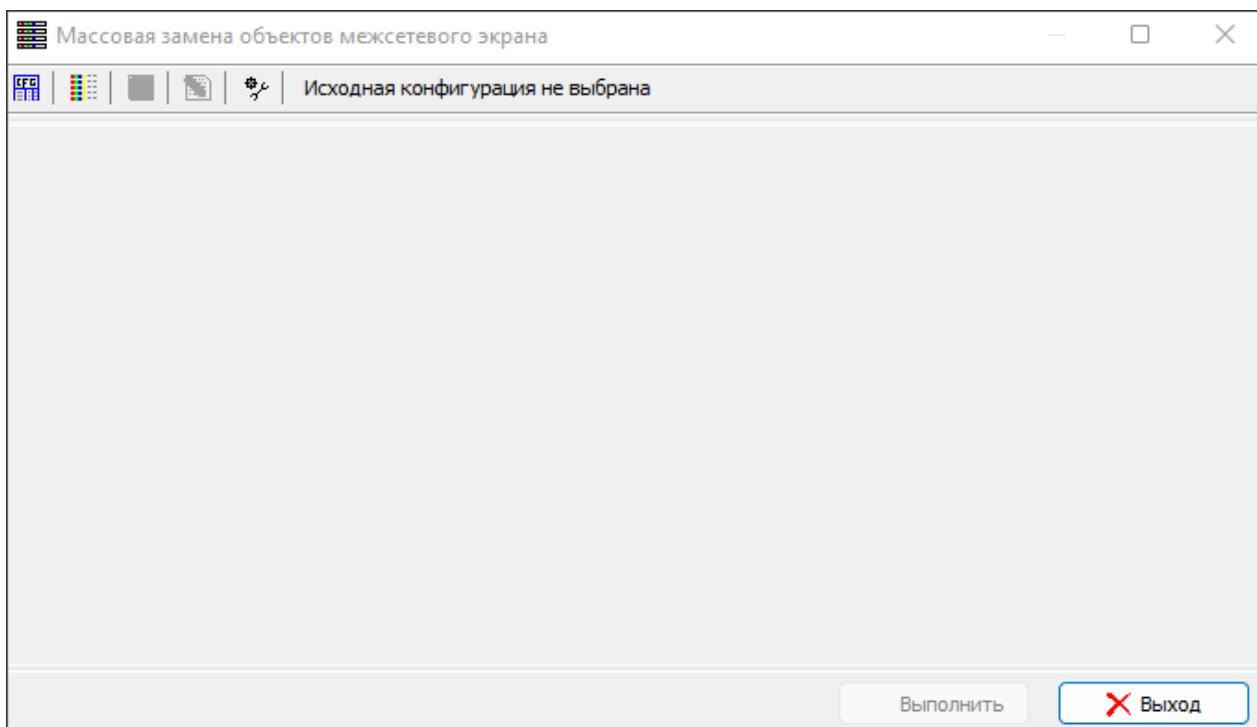


Рисунок 139 - Окно массовой замены объектов межсетевого экрана

В открывшемся окне «Массовая замена объектов межсетевого экрана»



необходимо нажать кнопку **Выбор исходного ФПСУ-IP**. Появится окно, в котором будет отображаться список тех ФПСУ-IP, конфигурация которых может быть выбрана в качестве исходной. При необходимости найти в этом списке ФПСУ-IP по имени и серийному номеру, предлагается воспользоваться расположенной в нижней части окна панелью поиска.

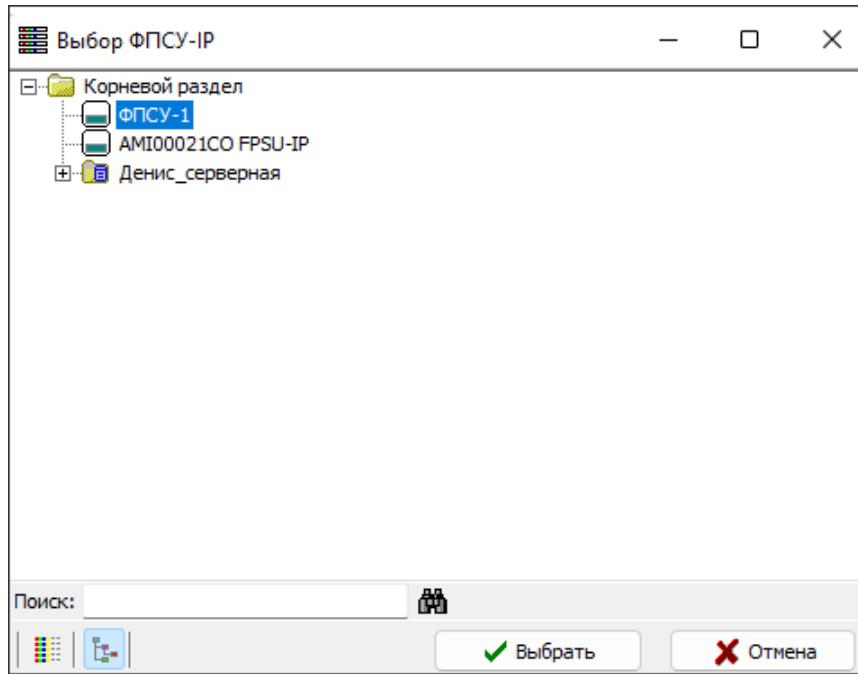
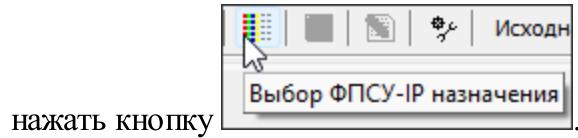


Рисунок 140 - Окно выбора исходного ФПСУ-IP

После выбора ФПСУ-IP и подтверждения действия нажатием кнопки «Выбор» информация об этом отобразится в окне массовой замены параметров межсетевого экрана вместо надписи «Исходная конфигурация не выбрана».

Для выбора ФПСУ, на которые будет отправлена конфигурация, необходимо



нажать кнопку

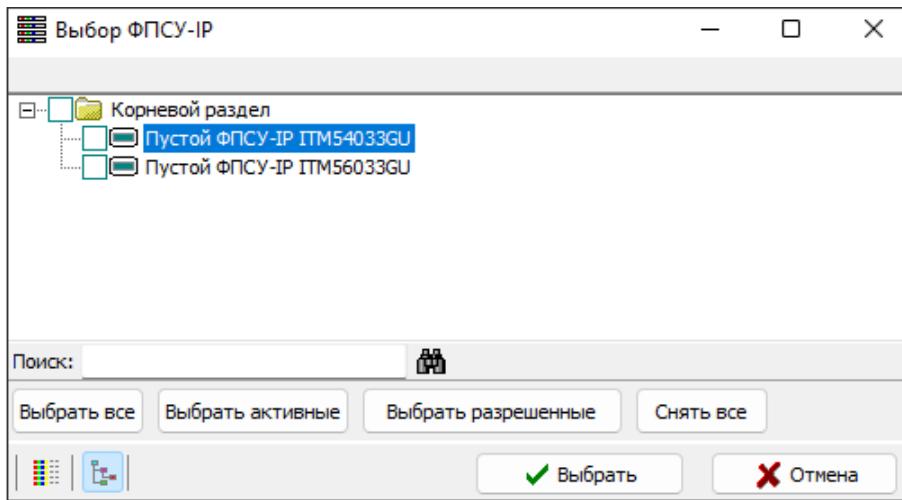


Рисунок 141 - Окно выбора ФПСУ-IP назначения

Открывшееся окно содержит следующие опции:

- область списка зарегистрированных ФПСУ-IP, из которых можно выбирать те, на которые высыпается новая конфигурация. При выборе строкой ФПСУ-IP отметить его как получателя новой конфигурации можно, нажав на клавишу <Пробел> или установив флаг слева от записи;
- кнопки, позволяющие выбрать все записи, выбрать активные ФПСУ-IP, выбрать разрешенные и сбросить выбор;
- панель поиска в этом списке ФПСУ-IP по имени и серийному номеру.

Отметив в списке те ФПСУ-IP, на которые следует передать конфигурацию, следует нажать на кнопку «Выбрать».

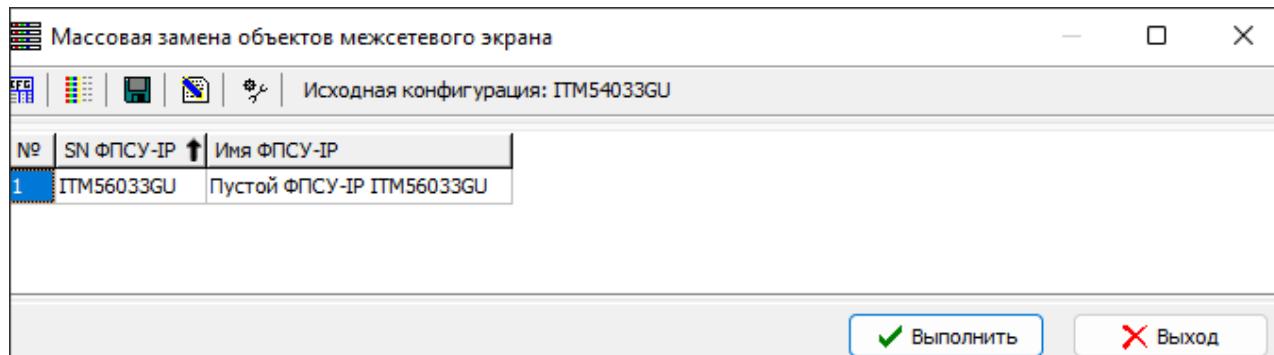
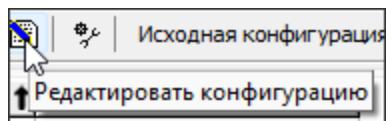
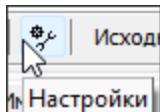


Рисунок 142 - Пункты назначения

Пересылаемую конфигурацию можно изменить, нажав кнопку



Редактирование конфигураций описано в разделе «Редактирование конфигурации ФПСУ-IP».



По нажатию кнопки **Настройки** предоставляется возможность настроить действия при наличии Клиентов в исходной конфигурации:

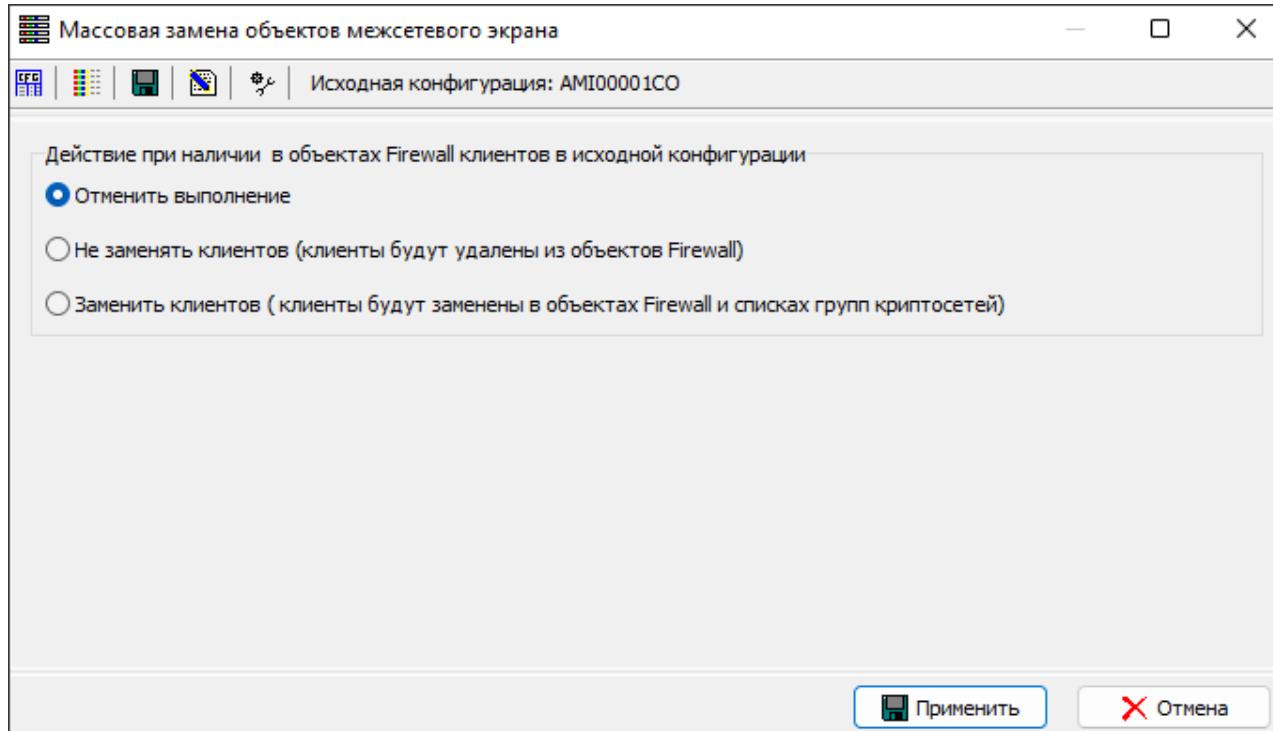


Рисунок 143 - Окно настроек

Установка переключателя в необходимое положение подтверждается нажатием кнопки «Применить».

Замена объектов межсетевых экранов осуществляется по нажатию кнопки «Выполнить» в окне с пунктами назначения (см. выше). Результат выполнения операции при этом отображается в отдельной колонке:

Исходная конфигурация: ITM54033GU			
№	SN ФПСУ-IP ↑	Имя ФПСУ-IP	Результат выполнения
1	ITM56033GU	Пустой ФПСУ-IP ITM56033GU	Выполнено

Рисунок 144 - Отображение результатов операции замены

12. Операции

12. 1. Массовые операции с ключами

Для проведения массовых операций с ключами необходимо выбрать пункт меню «Операции» → «Массовые операции с ключами на ФПСУ-IP». В открывшемся окне «Массовые операции с ключами на ФПСУ-IP» следует указать путь к каталогу, в котором расположены файлы с ключевыми данными, выбрав путь в стандартном окне, открывающемся по нажатию кнопки «Выбор каталога».

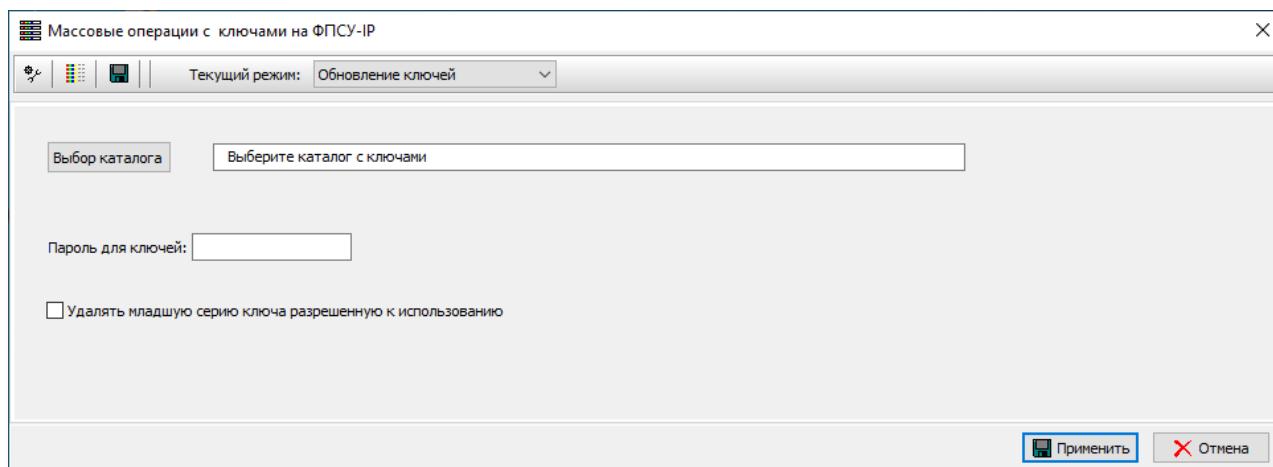


Рисунок 145 - Выбор каталога

Для выбора ФПСУ-IP необходимо нажать кнопку «Выбор ФПСУ-IP» и в открывшемся окне отметить нужные ФПСУ-IP знаком X в колонке «Выбор ФПСУ-IP». При необходимости можно выбрать все отображающиеся в списке ФПСУ-IP, выбрать только активные и\или только разрешенные ФПСУ-IP, а также найти необходимую запись путем ввода комбинации букв и\или цифр из названия ФПСУ-IP в поле поиска.

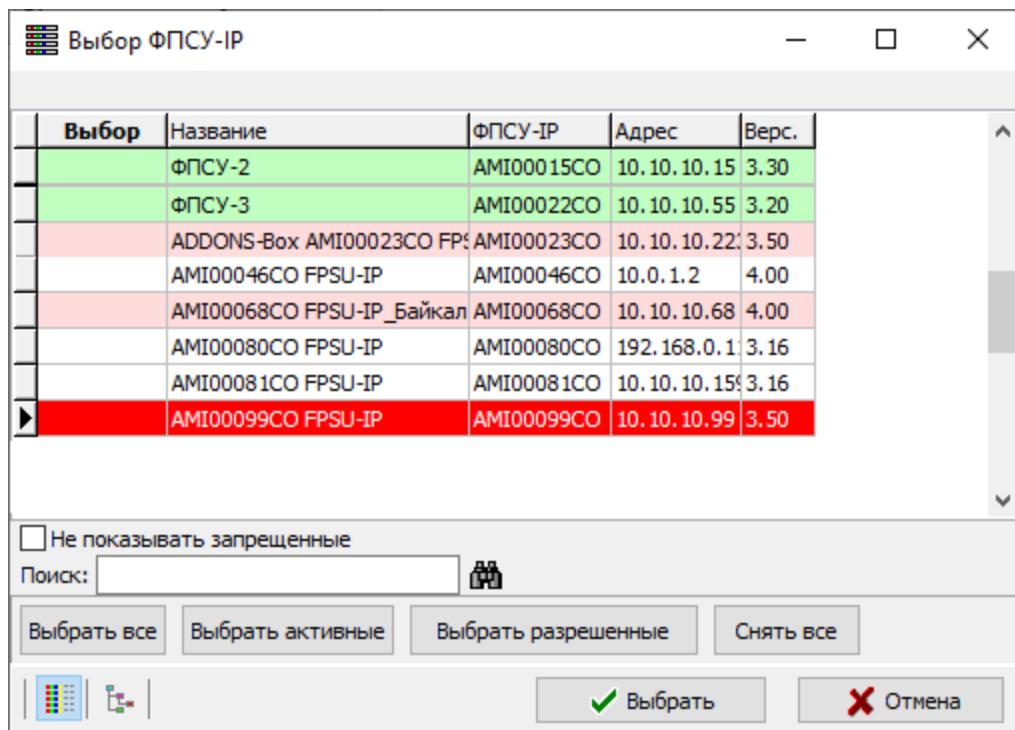


Рисунок 146 - Выбор каталога

По нажатию кнопки «Обновить» ключи из каталога будут загружены на выбранные на предыдущем этапе ФПСУ-IP.

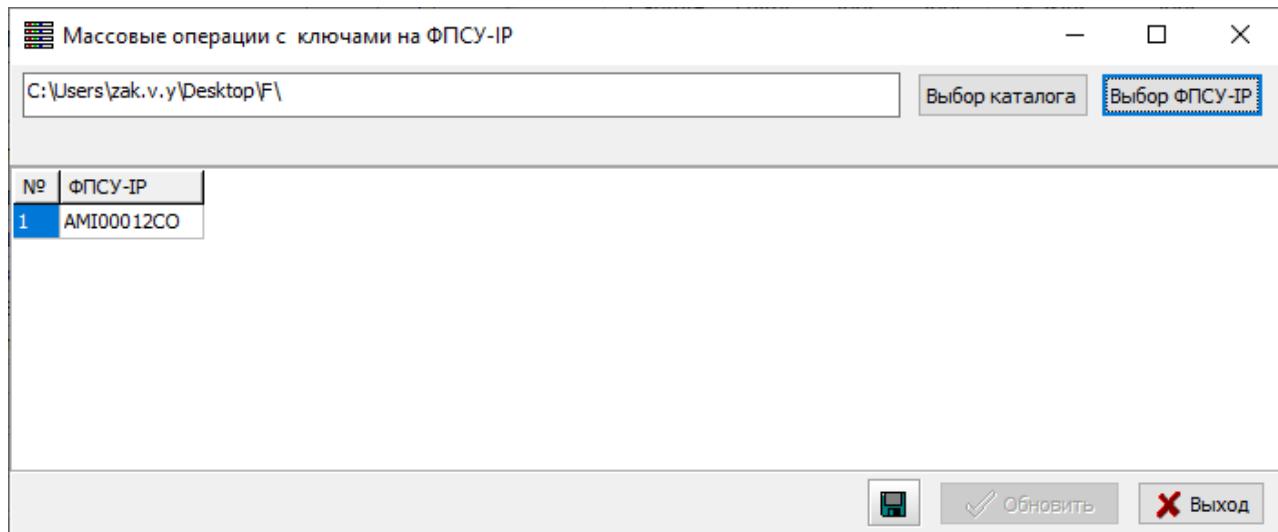


Рисунок 147 - Заполненная форма для массовых операций с ключами

12. 2. Массовые операции с блокировкой трафика

Для настройки трафика выбранного ФПСУ-IP необходимо выбрать пункт «Массовые операции с блокировкой трафика» меню «Операции». В открывшемся окне предоставляется возможность:

- выбрать ФПСУ-IP, трафик которого будет заблокирован (путем нажатия кнопки «Выбор ФПСУ-IP»);
- задать условия для блокировки трафика (путем нажатия кнопки «Опции блокировки»);
- сохранить созданные условия для блокировки.

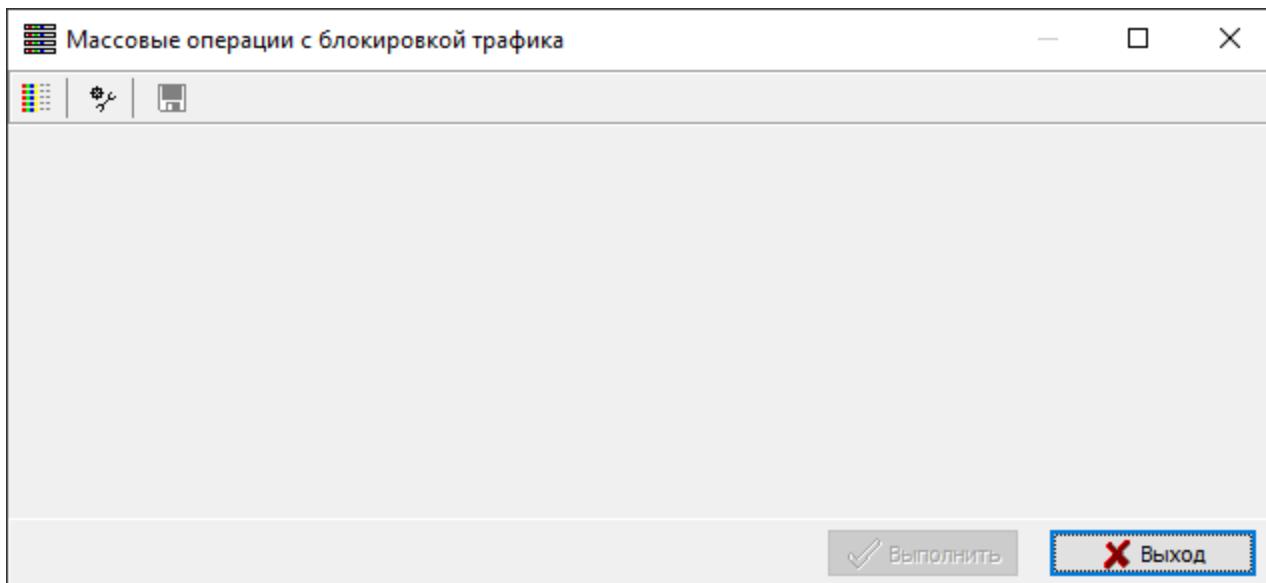


Рисунок 148 - Массовые операции с блокировкой трафика

При блокировке трафика требуется: выбрать один из типов трафика - хост, подсеть, протокол, порт назначения TCP или UDP; задать значение или список значений для выбранного типа; установить период времени блокировки или разблокировки.

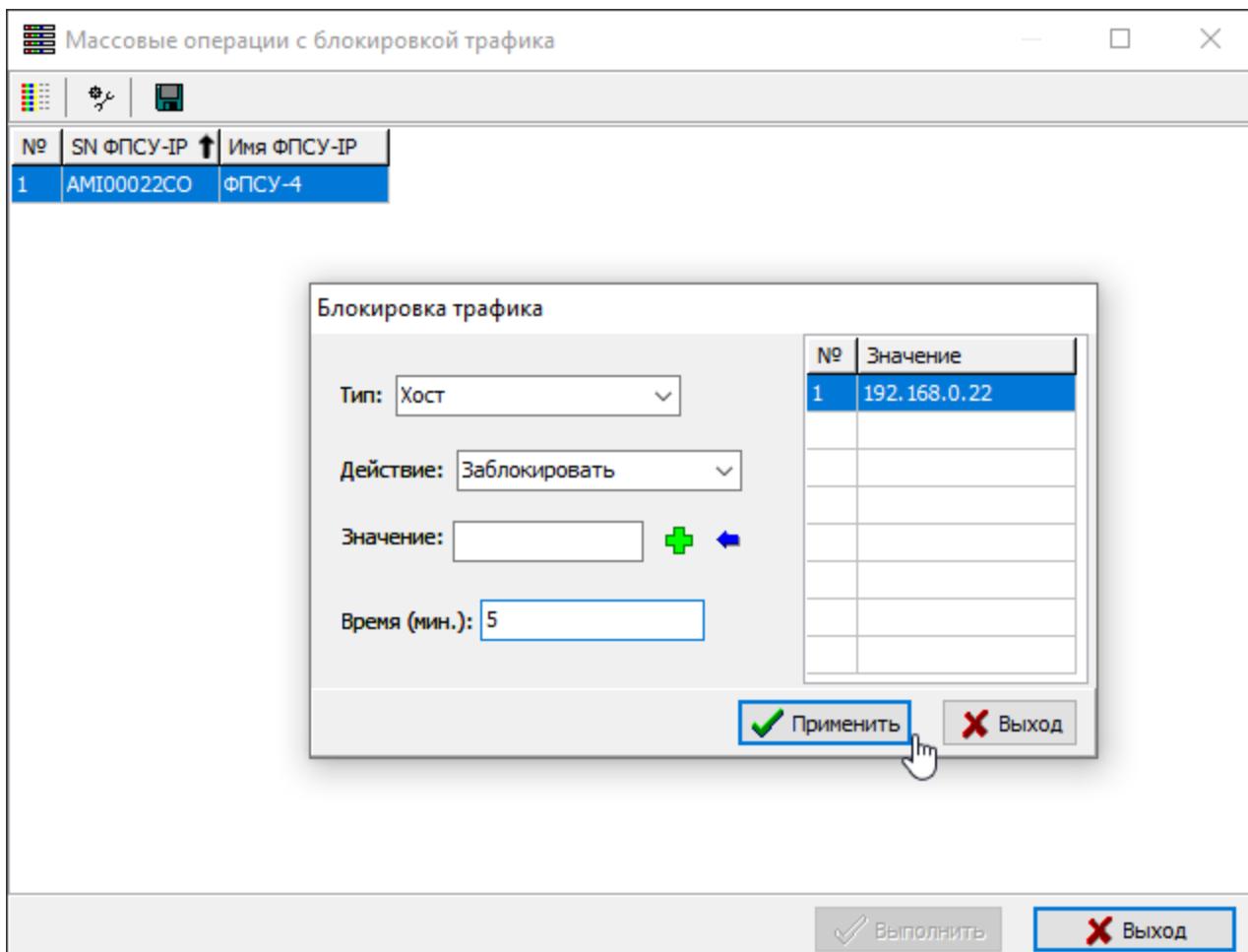


Рисунок 149 - Задание условий для блокировки трафика

12. 3. Блокировка трафика на выбранных ФПСУ-IP

Для отслеживания трафика, который блокирован в текущий момент на ФПСУ-IP, необходимо выбрать пункт меню «Операции» → «Мониторинг заблокированного трафика».

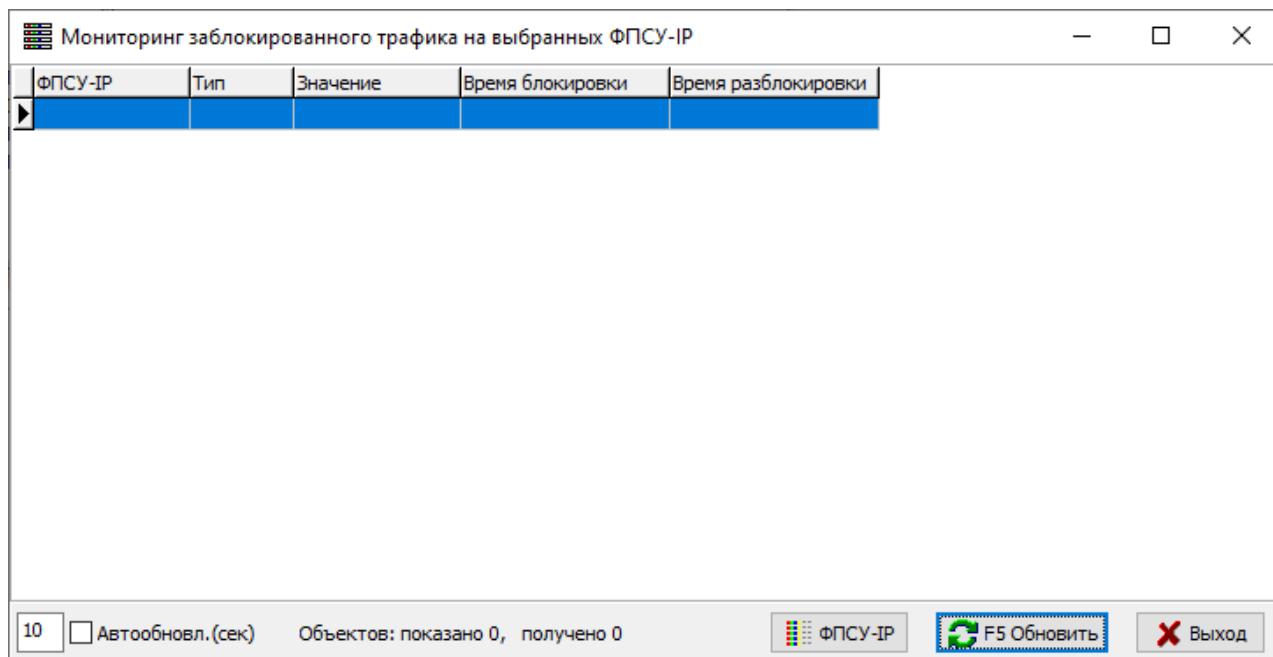


Рисунок 150 - Мониторинг заблокированного трафика

Выбрать ФПСУ-IP можно по нажатию кнопки «ФПСУ-IP». На экран будет выдано окно, в котором следует отметить знаком X в столбце «Выбор» те ФПСУ-IP, заблокированный трафик которых требуется отслеживать.

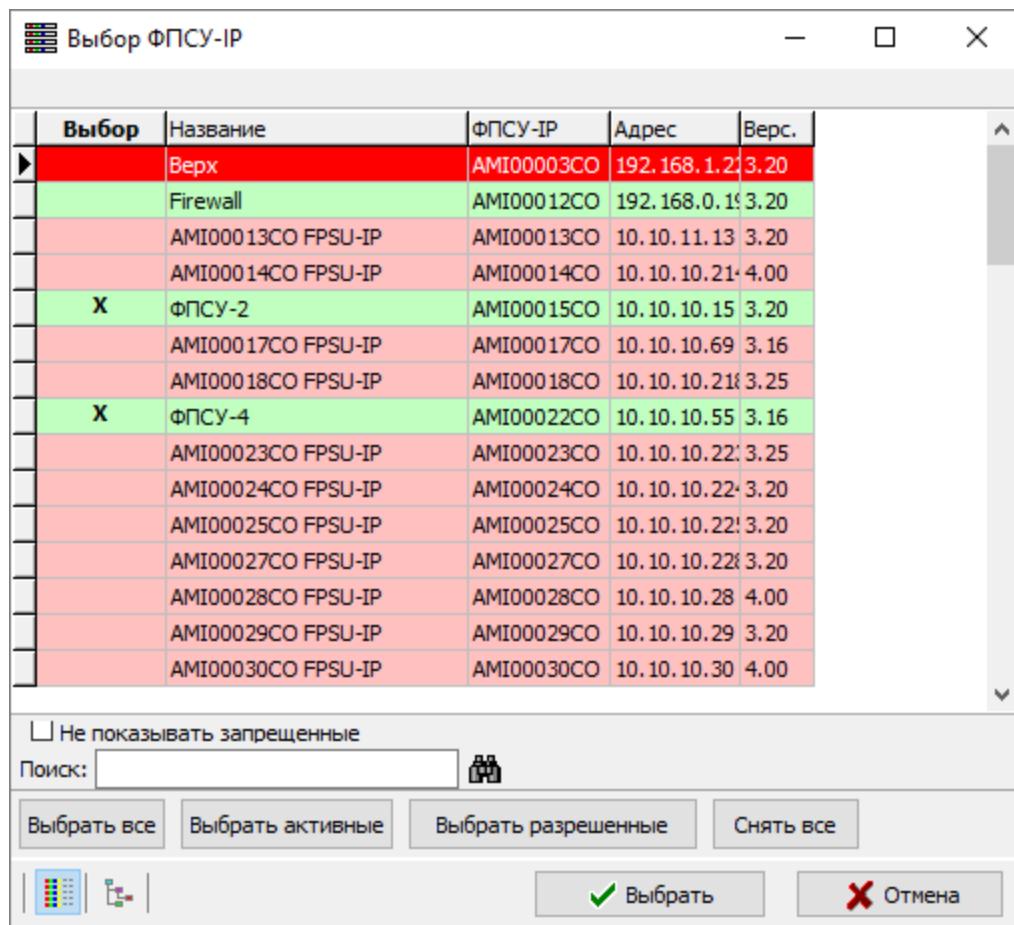


Рисунок 151 - Выбор ФПСУ-IP

В списке отобразится информация о заблокированном трафике на выбранных ФПСУ-IP.

Мониторинг заблокированного трафика на выбранных ФПСУ-IP				
ФПСУ-IP	Тип	Значение	Время блокировки	Время разблокировки
AMI00022CO	IP-адрес	8.8.8.8	25.08.2021 16:12:50	25.08.2021 16:32:50
AMI00022CO	IP-адрес	1.1.1.1	25.08.2021 16:12:50	25.08.2021 16:32:50

Рисунок 152 - Мониторинг заблокированного трафика

12. 4. Запрос с ФПСУ-IP данных

Для запроса данных с ФПСУ-IP необходимо выбрать пункт «Запрос данных с ФПСУ-IP» меню «Операции». Откроется окно выбора параметров для загрузки с ФПСУ-IP.

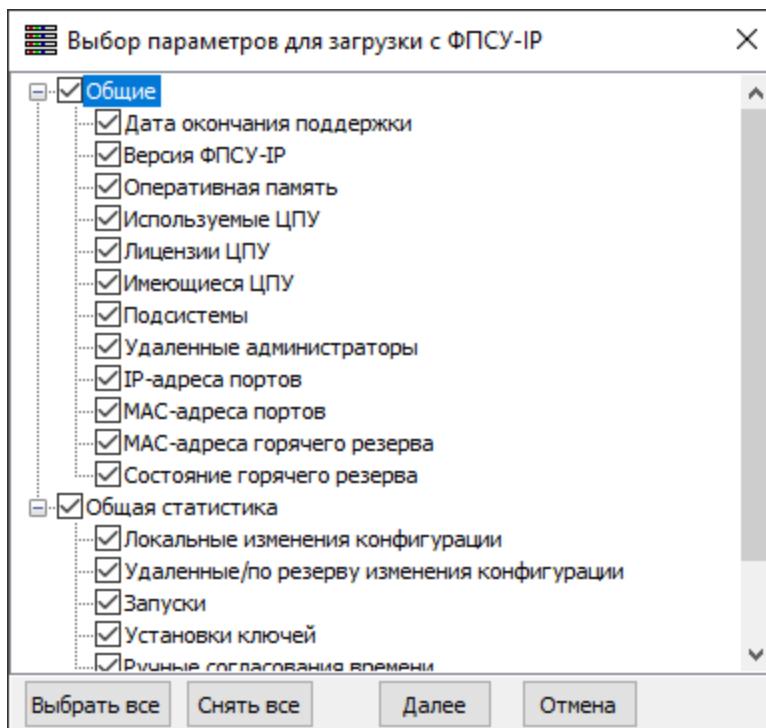


Рисунок 153 - Выбор параметров для загрузки с ФПСУ-IP

После того, как отмечены параметры для загрузки с ФПСУ-IP необходимо нажать кнопку «Далее» и в открывшемся окне отметить нужные ФПСУ-IP знаком X в колонке «Выбор ФПСУ-IP». При необходимости можно выбрать все отображающиеся в списке ФПСУ-IP, выбрать только активные и\или только разрешенные ФПСУ-IP, а также найти необходимую запись путем ввода комбинации букв и\или цифр из названия ФПСУ-IP в поле поиска.

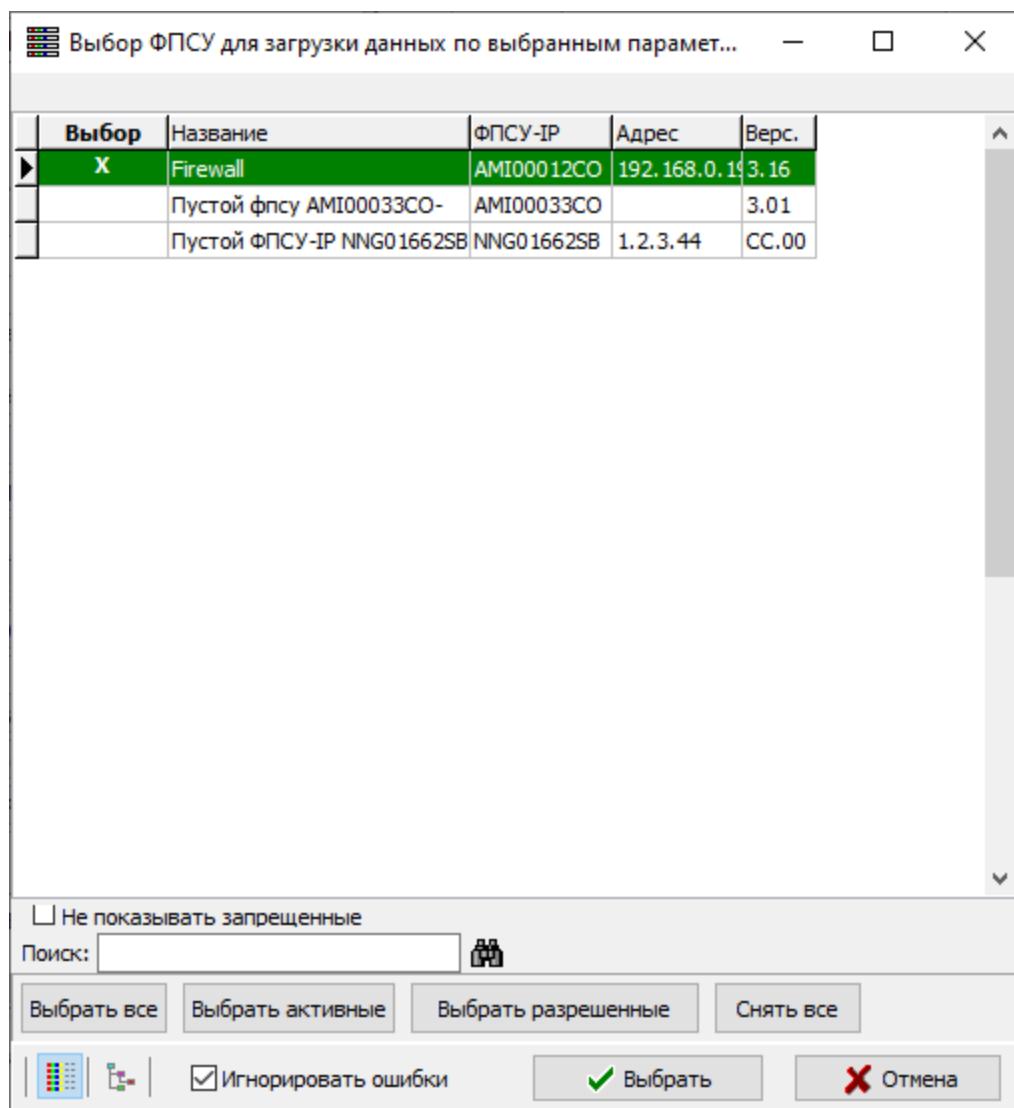


Рисунок 154 - Выбор ФПСУ-IP

По нажатию кнопки «Выбрать» параметры будут загружены с ФПСУ-IP.

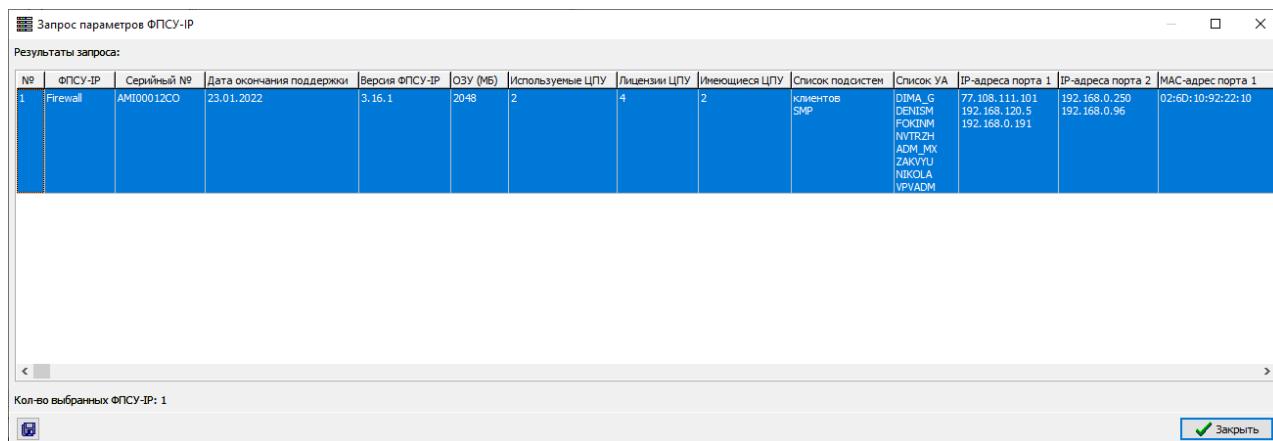


Рисунок 155 - Загрузка параметров с ФПСУ-IP

12. 5. Процессы с ФПСУ-IP

Дамп памяти позволяет записывать критические ошибки в работе ФПСУ-IP без необходимости приостанавливать его работу. В случае если дамп сформирован, администратор с правами управления дампами памяти имеет возможность загрузить дамп памяти в виде архива на УА ФПСУ-IP для дальнейшей передачи этого архива Разработчику (ООО «АМИКОН»).

Для работы с дампами необходимо выбрать пункт меню «Операции» → «Процессы/дампы с ФПСУ-IP».

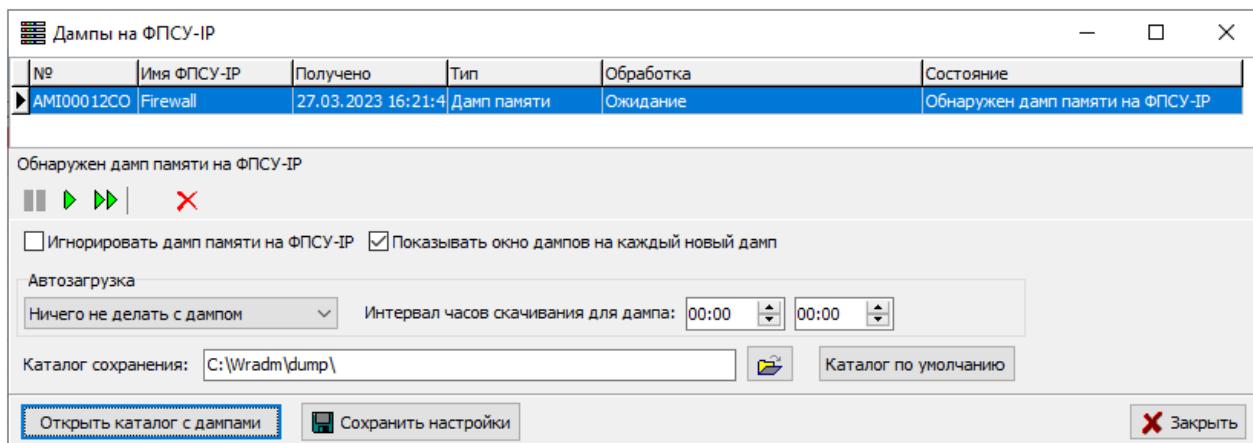


Рисунок 156 - Дамп памяти в виде архива с ФПСУ-IP

Кнопки для управления дампами памяти:



- остановить загрузку архива дампа памяти;



- загрузить архив с ФПСУ-IP на УА ФПСУ-IP;



- загрузить одновременно все найденные архивы.

Флаг «Игнорировать дамп памяти на ФПСУ-IP» – при установлении флага если обнаружен дамп, окно со списком дампов не показывается. При выключенном флаге отображается окно со списком дампов при обнаружении дампа.

12. 6. Изменение УА на группе ФПСУ-IP

Назначение администратора УА ФПСУ-IP в группе ФПСУ-IP может производиться выбором команды пункта меню «Операции» → «Изменение УА на группе ФПСУ-IP». В открывшемся окне отображается область для выбора удаленного администратора и область для выбора группы ФПСУ-IP.

В области выбора администратора УА ФПСУ-IP доступны кнопки:



- добавить/изменить администратора УА ФПСУ-IP на ФПСУ-IP;



- удалить администратора УА ФПСУ-IP с ФПСУ-IP;



- изменить администратора УА ФПСУ-IP на ФПСУ-IP;



- удалить администратора УА ФПСУ-IP.

В области выбора группы ФПСУ-IP доступны кнопки:



- добавить/изменить ФПСУ-IP;



- удалить ФПСУ-IP.

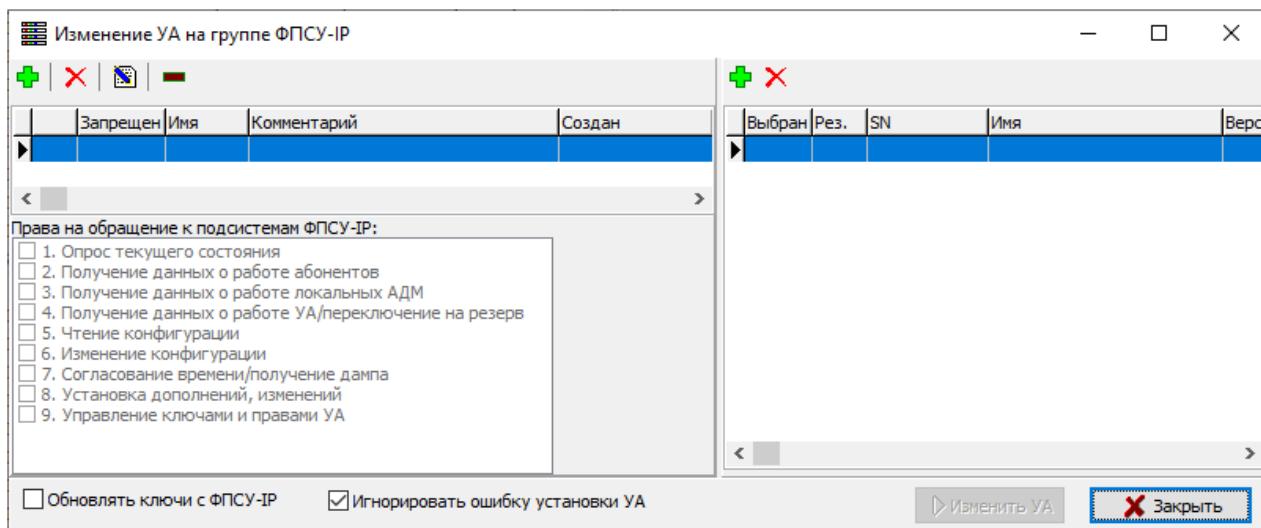


Рисунок 157 - Окно для изменения UA в группе ФПСУ-IP

В области выбора администратора UA ФПСУ-IP по нажатию кнопки «Добавить/изменить UA на ФПСУ-IP» или клавиши <Ins> откроется стандартное окно выбора каталога с данными администраторов, в котором требуется выбрать каталог.

После выбора каталога будет выдано окно с найденными данными администраторов. Следует отметить в списке строку с устанавливаемым администратором UA ФПСУ-IP нажатием клавиши «Пробел» или нажатием левой клавиши мыши в поле переключателя. В списке могут быть сняты или выделены все найденные администраторы UA ФПСУ-IP по нажатию соответствующих кнопок.

Для выбора отмеченных в списке администраторов UA ФПСУ-IP следует нажать кнопку «Да».

Возврат в окно «Изменение UA в группе ФПСУ-IP» осуществляется по кнопке «Нет».

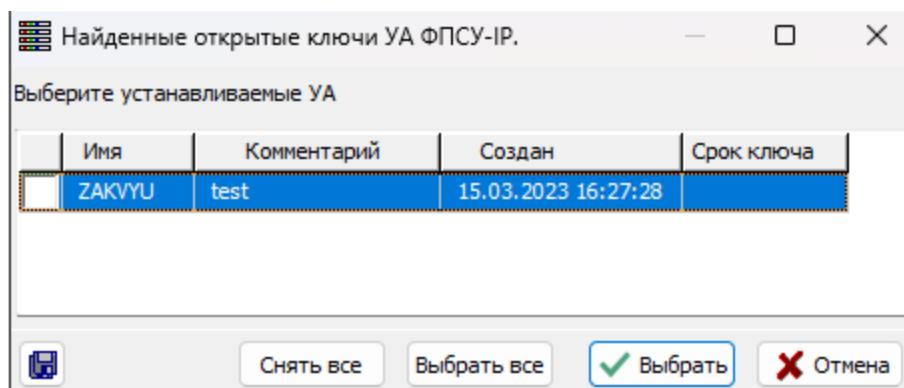


Рисунок 158 - Окно выбора открытых ключей УА

В области выбора администраторов УА ФПСУ-IP отобразятся устанавливаемые администраторы. Администратору или группе администраторов УА ФПСУ-IP назначаются права на обращение к подсистемам ФПСУ-IP, выбираются из списка с помощью переключателей.

В области выбора ФПСУ-IP необходимо нажать кнопку в открывшемся окне отметить в списке ФПСУ-IP нажатием клавиши «Пробел» или нажатием левой клавиши мыши в поле «Выбор», для которых будет назначен администратор УА ФПСУ-IP. Подтвердить выбор следует нажатием кнопки «Выбрать».

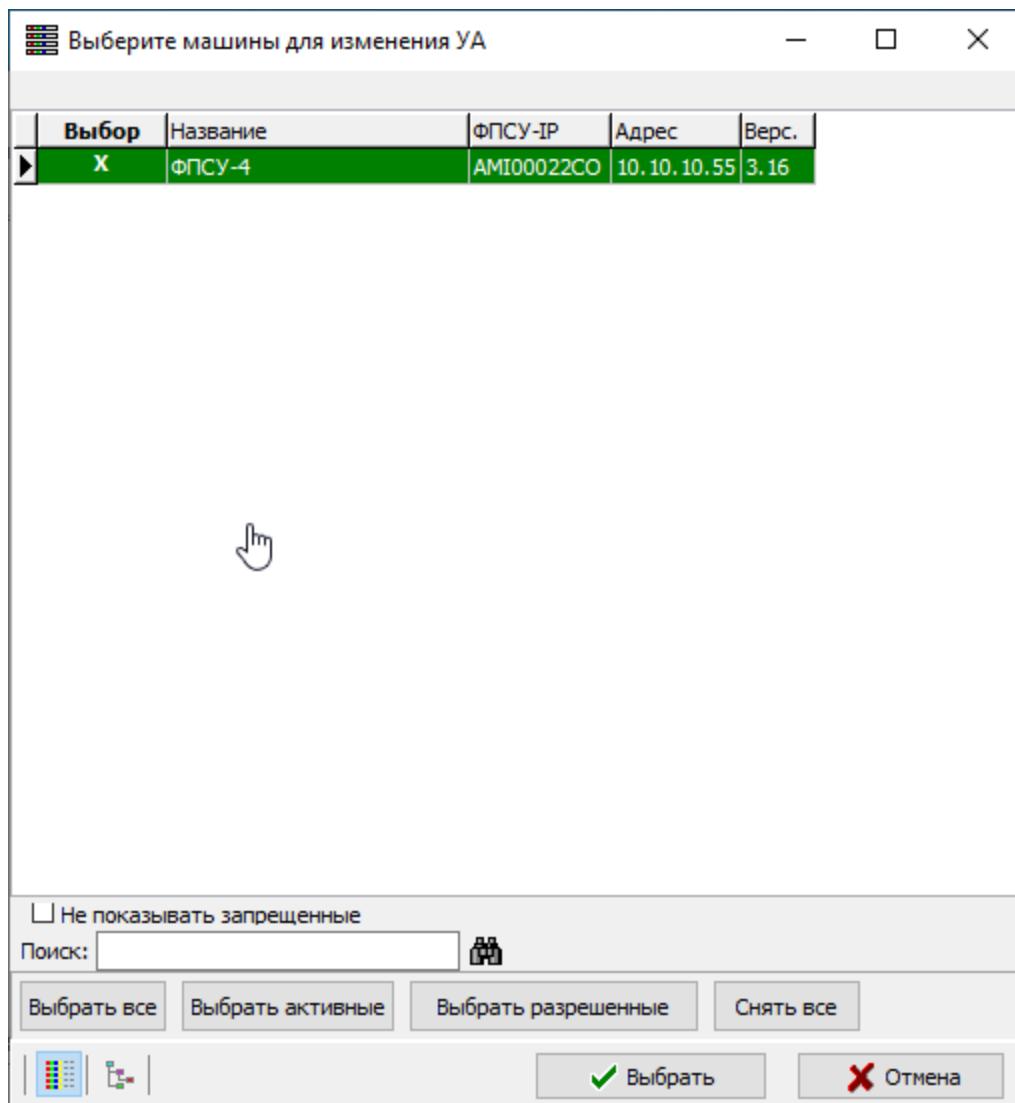


Рисунок 159 - Выбор группы ФПСУ-IP

В окне «Изменение UA в группе ФПСУ-IP» в области выбора ФПСУ-IP отобразится группа ФПСУ-IP. Для назначения группе ФПСУ-IP администратора UA ФПСУ-IP необходимо нажать кнопку «Изменить UA». Результат будет выведен в таблице в строке для каждого ФПСУ-IP и внизу окна будет отображаться журнал изменений.

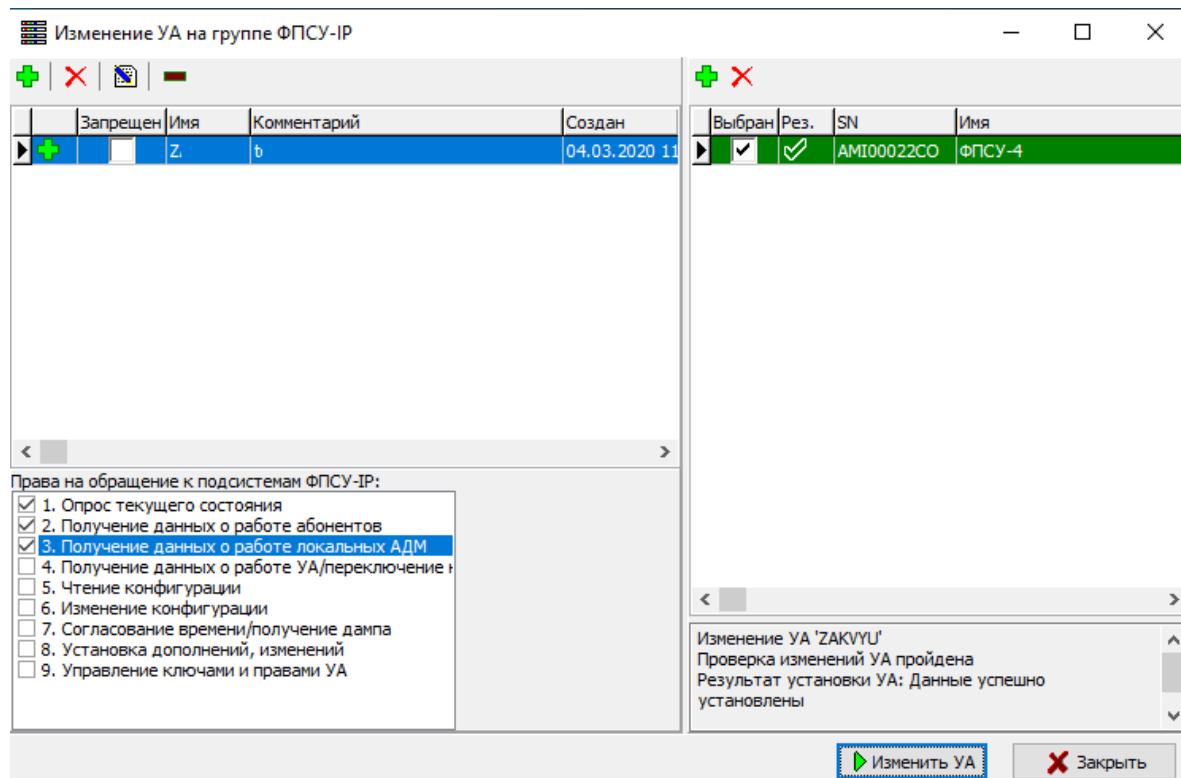


Рисунок 160 - Изменение администраторов УА ФПСУ-IP

12. 7. Просмотр состояния задания на рассылку

Для просмотра состояния рассылки обновлений ПО на ФПСУ-IP следует выбрать пункт меню «Операции» → «Показать состояние задания». На экран будет выдано окно, содержащее список ФПСУ-IP, на которые отправляется рассылка, где можно отслеживать состояние отправки.

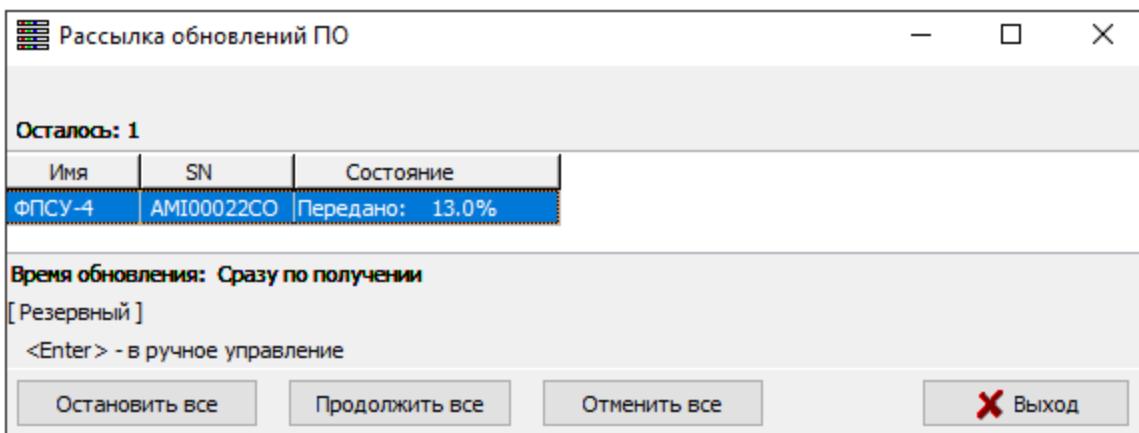


Рисунок 161 - Окно рассылки ПО на ФПСУ-IP

Если требуется остановить (продолжить) или отменить рассылку всей группе ФПСУ-IP, следует воспользоваться командами окна «Остановить все», «Продолжить все» и «Отменить все».

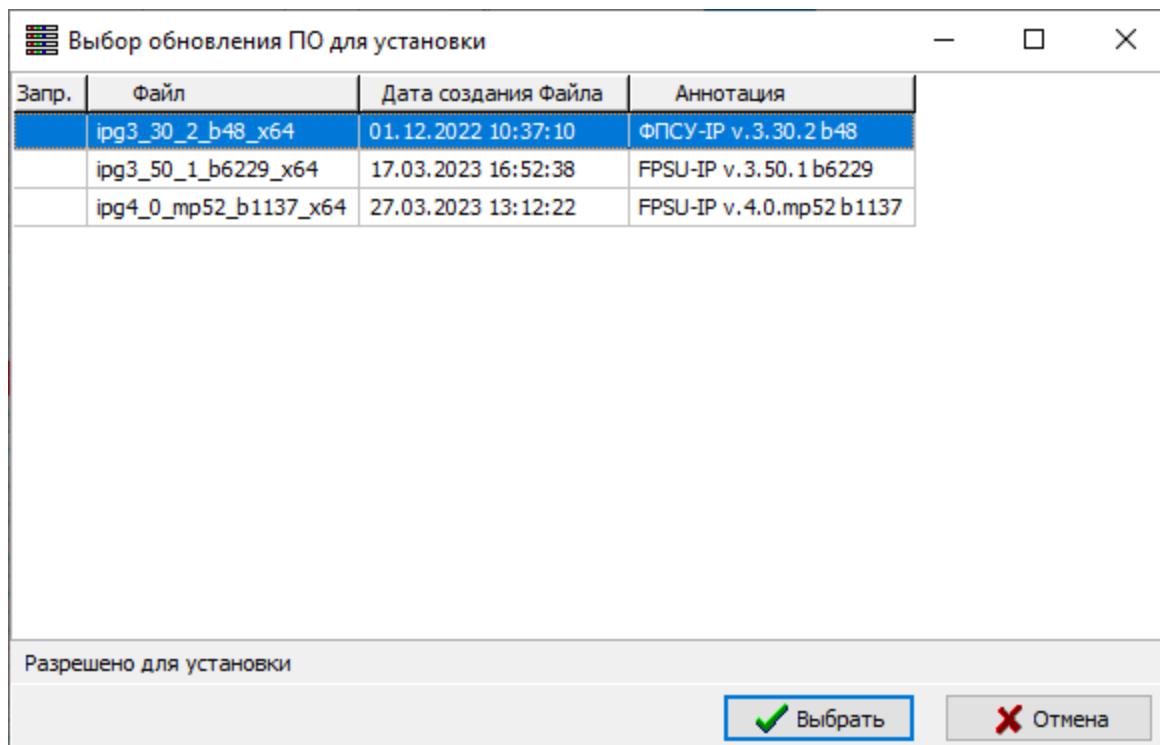
Нажав кнопку «Выход», можно скрыть окно рассылки.

12. 8. Рассылка обновления ПО

Передача изменений и дополнений программного обеспечения на множество ФПСУ-IP сразу может быть запланирована на УА ФПСУ-IP для выполнения в фоновом режиме. В этом случае формируется пакет рассылок, которые передаются указанным ФПСУ-IP во время установки туннелей.

Для создания задачи пакетной загрузки необходимо выполнить команду главного меню УА ФПСУ-IP «Операции» → «Рассылка обновления ПО».

На экран будет выдано окно выбора каталога, содержащего ПО для передачи, как и в случае установки обновления на единственный ФПСУ-IP, в котором необходимо указать путь к каталогу с файлом обновления ПО. Так же, как и в случае обновления ПО на одном ФПСУ-IP, необходимо выбрать из списка найденных в каталоге обновлений одно, которое требуется разослать на несколько ФПСУ-IP.

**Рисунок 162 - Выбор обновления ПО**

После выбора файла обновления, появится окно управления задачами автообновления ПО, которое содержит следующую информацию и опции:

- описание файла обновления вверху окна (ФПСУ-IP v. 3.20.5 на рисунке);
- установленный флаг «Сразу по получении» указывает на то, что обновление ПО будет установлено на выбранные ФПСУ-IP сразу после его отправки;
- поле «Время обновления» позволяет задать дату и время активации присланного файла (доступно при снятом флаге «Сразу по получении») на ФПСУ-IP (дата и время установки на ФПСУ-IP, не на УА ФПСУ-IP!);
- область списка зарегистрированных на УА ФПСУ-IP ФПСУ-IP, в котором выбираются получатели обновления. При выборе строкой ФПСУ-IP отметить его как получателя обновления ПО можно, нажав на кнопку «Передать», клавишу <Пробел> или нажав левой клавишей мыши на поле области «Передать». Похожим образом, нажимая на кнопку «Обновить», сочетание клавиш <Ctrl+Пробел> или поле «Обновить», отмечаются те ФПСУ-IP, на которых переданные обновления следует установить;
- панель поиска в этом списке ФПСУ-IP по имени и/или серийному номеру;

- панель команд управления передачей и установкой обновления для зарегистрированных ФПСУ-IP.

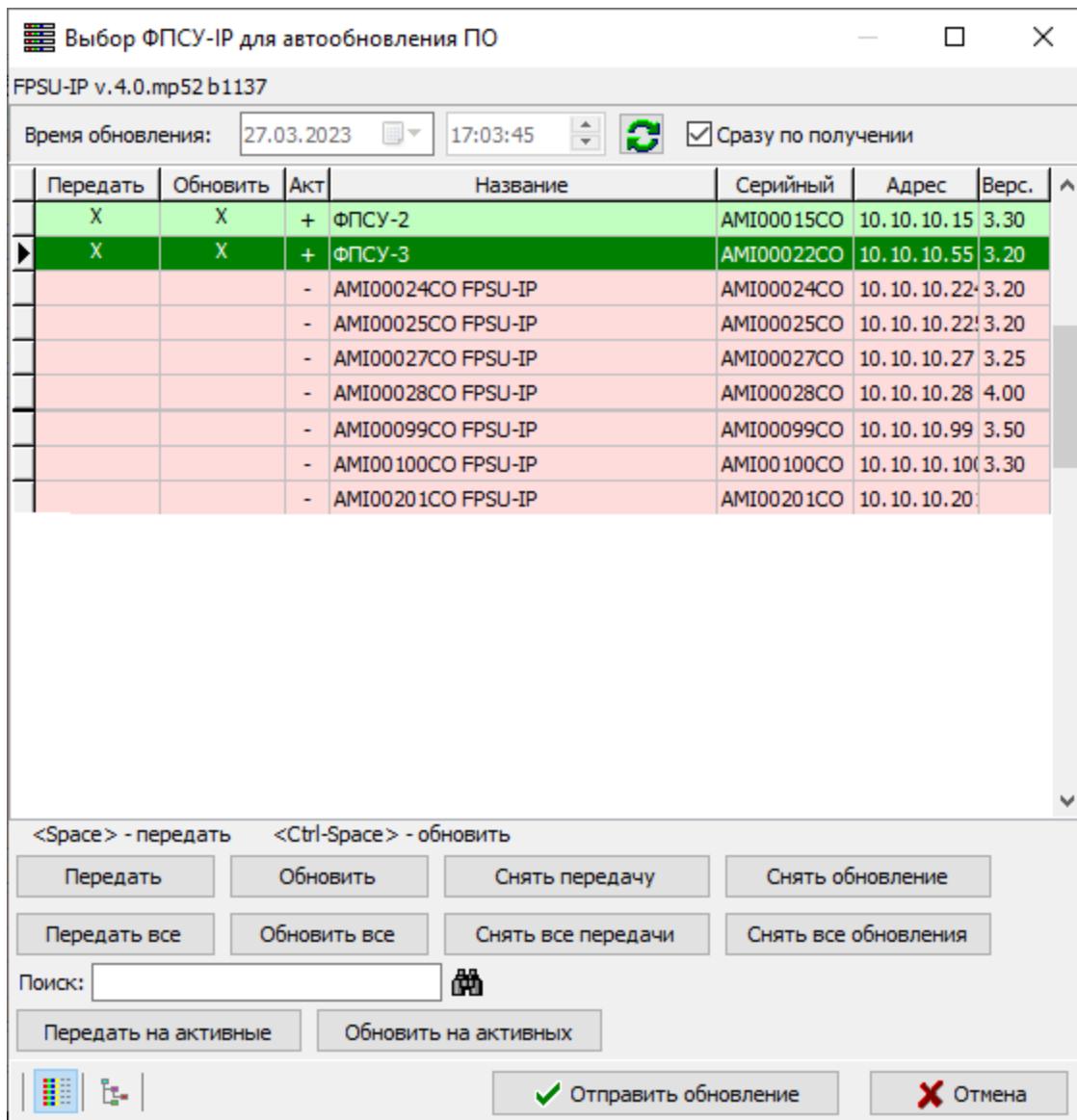


Рисунок 163 - Выбор нескольких ФПСУ-IP для обновления ПО

Если изменения ПО рассылаются всем ФПСУ-IP из списка, следует воспользоваться кнопками «Передать все» и «Обновить все».

Когда все установки произведены, необходимо нажать кнопку «Отправить обновление».

Появится окно выполнения рассылки обновлений ПО, в котором будет отображаться список тех ФПСУ-IP, на которых передача обновлений была запланирована, но еще не

окончена:

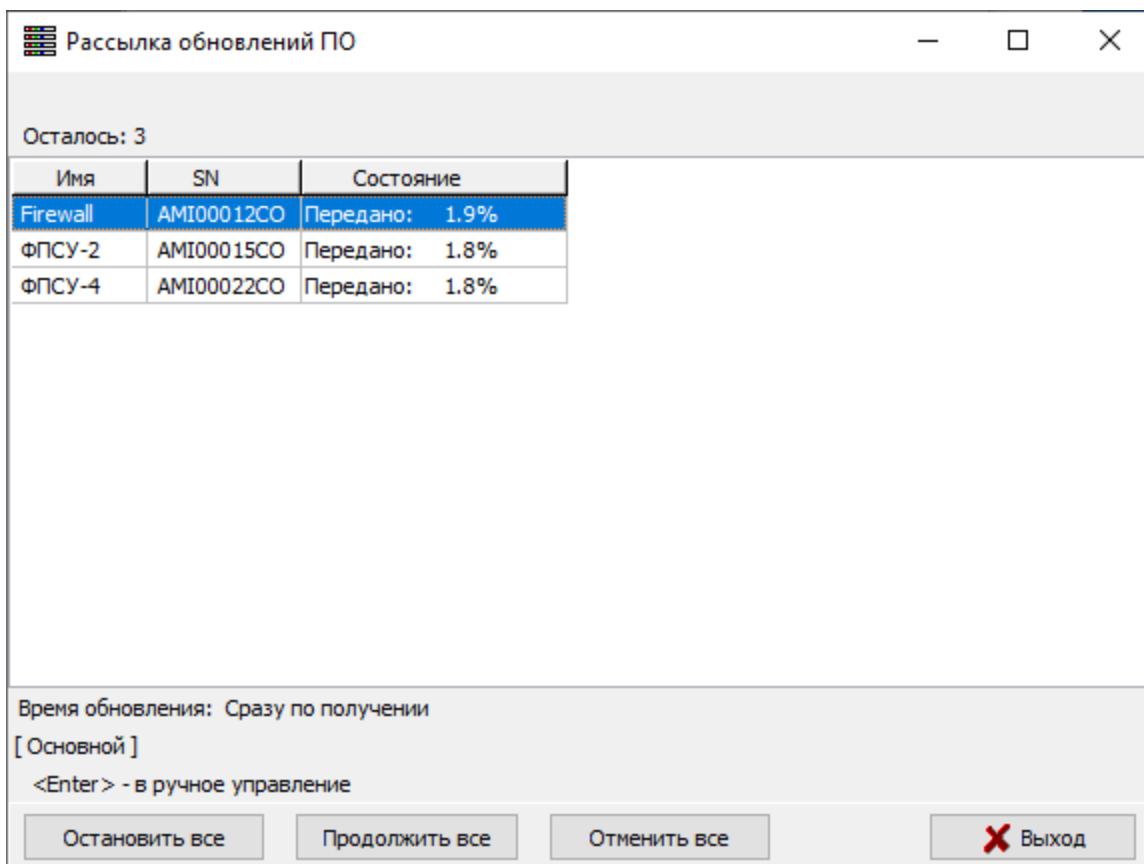


Рисунок 164 - Рассылка одного обновления ПО нескольким ФПСУ-IP

Если требуется остановить (продолжить) или отменить рассылку всей группе ФПСУ-IP, следует воспользоваться командами окна «Остановить все», «Продолжить все» и «Отменить все».

Нажав кнопку «Выход», можно скрыть окно передачи. При необходимости, его можно вернуть на экран, выполнив команду главного меню УА ФПСУ-IP «Конфигурации» → «Показать состояние задания».

Как только обновления будут переданы на все отмеченные ФПСУ-IP, окно закроется, выдав служебное сообщение «Рассылка выполнена».

Сообщение об активизации обновления на каждом ФПСУ-IP будет выдано сразу после доставки и установки его на ФПСУ-IP.

12. 9. Обновление множества ПО

Массовая загрузка обновлений ПО может быть произведена по сформированному списку ФПСУ-IP, где для каждого ФПСУ-IP выбирается одно из доступных обновлений ПО. Обновления загружаются на ФПСУ-IP сразу массово, могут быть установлены на ФПСУ-IP при получении, либо в заданное время.

Для обновления ПО на ФПСУ-IP следует выполнить команду главного меню УА ФПСУ-IP «Операции» → «Обновить множество ПО на ФПСУ-IP». На экран будет выдано окно выбора каталога, содержащего ПО для передачи, в котором следует указать путь к каталогу с файлами обновлений ПО.

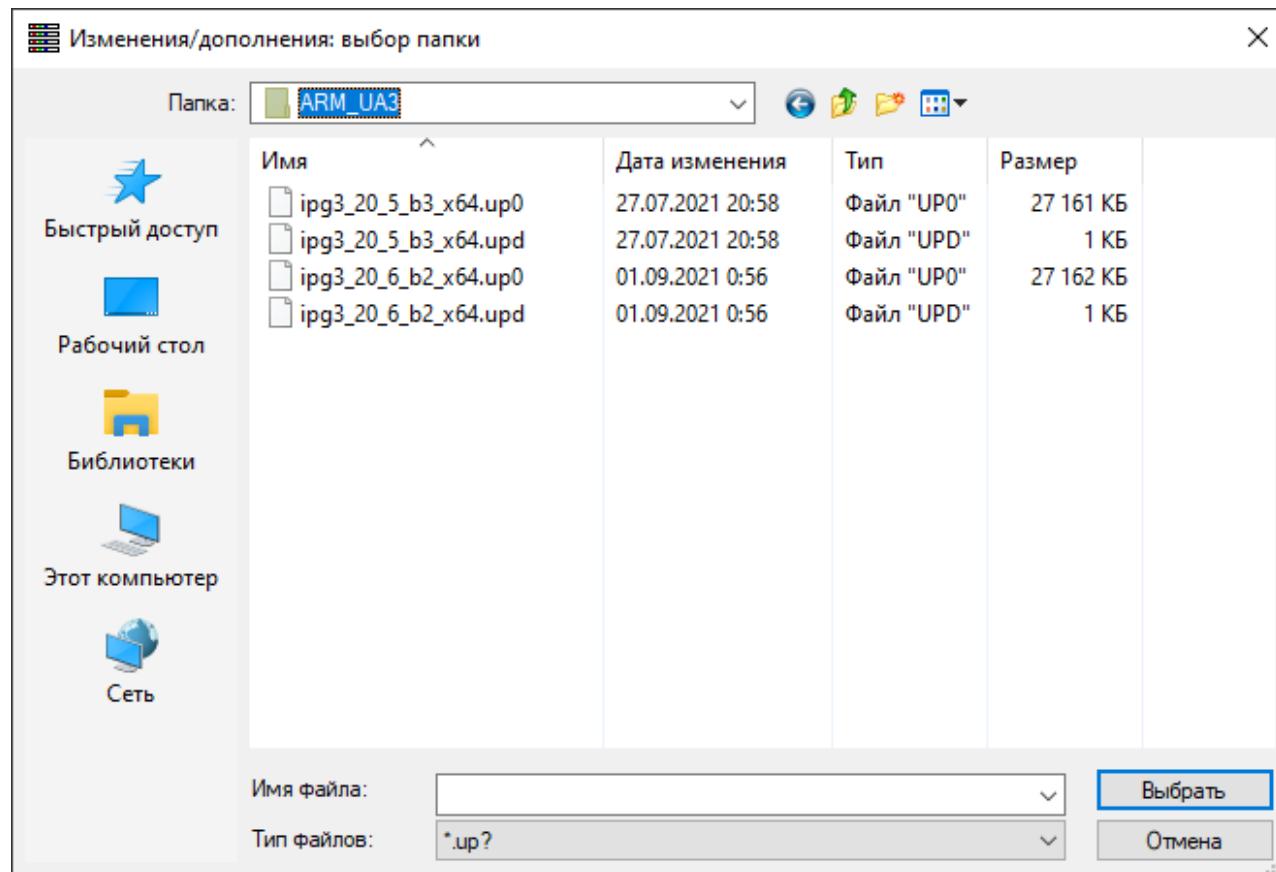


Рисунок 165 - Стандартное окно выбора файлов для обновления ПО

После выбора каталога на экран будет выведено окно со списком доступных обновлений ПО для ФПСУ-IP с указанием описания обновления, наименования файла обновления и пути к файлу с обновлением:

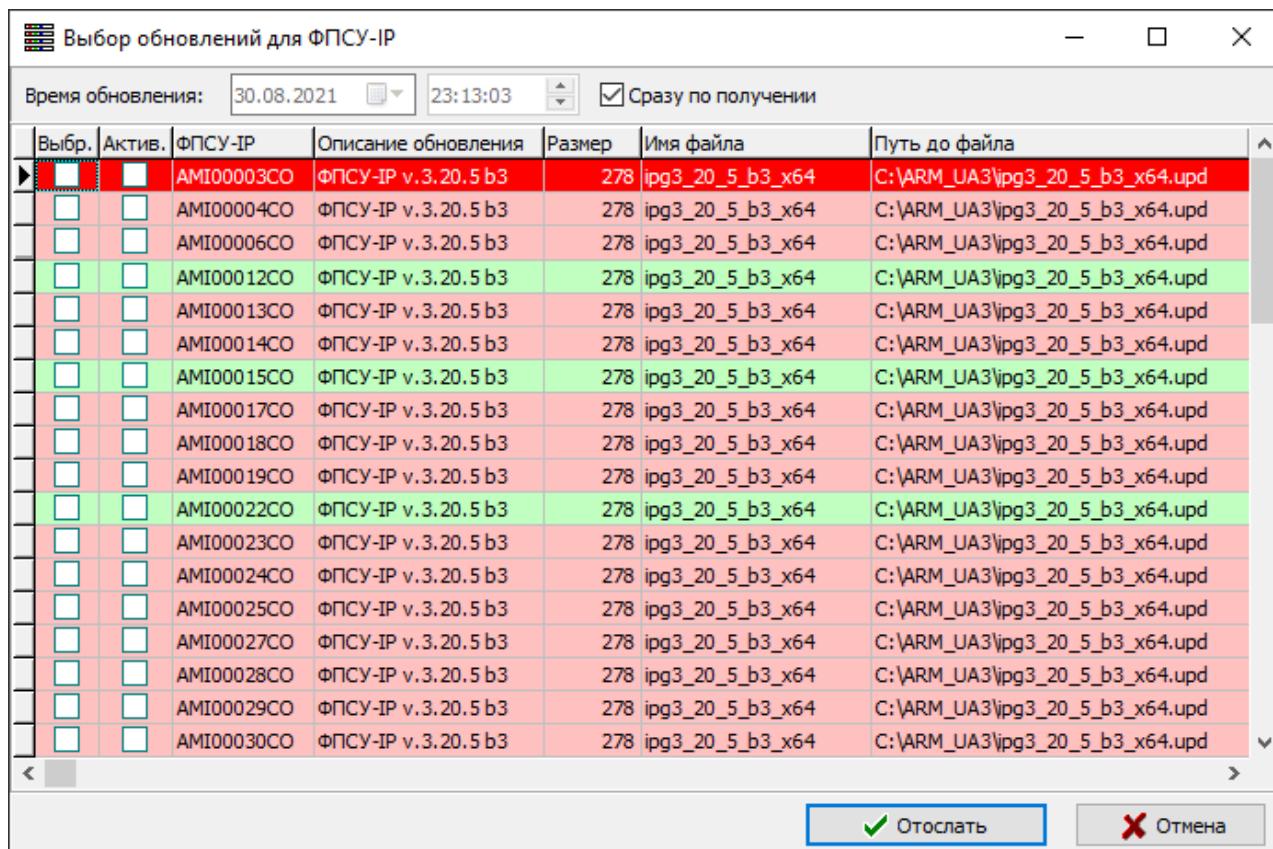


Рисунок 166 - Доступные обновления для ФПСУ-IP

Для каждого ФПСУ-IP может быть выбрано обновление из списка доступных, для этого в строке с ФПСУ-IP дважды нажать левую кнопку мыши. Откроется окно со списком файлов обновлений ПО.

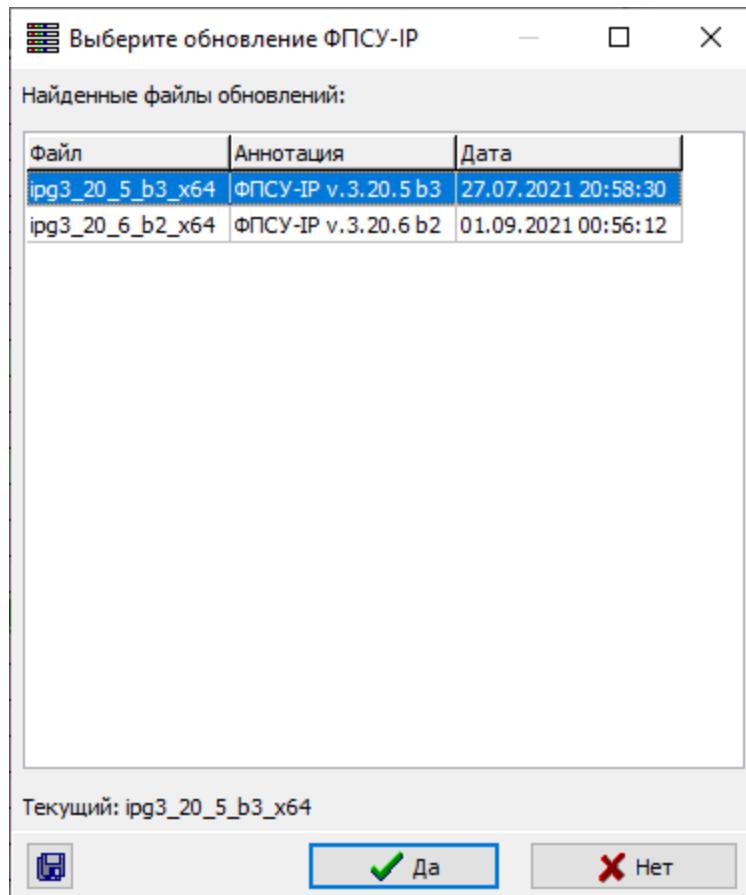


Рисунок 167 - Выбор обновления ПО для рассылки на ФПСУ-IP

Требуется отметить файл обновления и нажать кнопку «Да» для подтверждения выбора.

В списке обновлений в строке для выбранного ФПСУ-IP (строке, выделенной зеленым цветом) отобразится имя выбранного файла обновления ПО. Для загрузки данного файла на ФПСУ-IP следует установить флаг в строке ФПСУ-IP в столбце «Вызвано». Для установки данного обновления на ФПСУ-IP следует установить флаг в строке ФПСУ-IP в столбце «Актив.» (активировать).

Для установки обновлений на ФПСУ-IP требуется задать время обновления сразу при получении, установив соответствующий флаг, либо снять флаг «Сразу по получении» и установить дату и время обновления. Время обновления задаётся для всех ФПСУ-IP из списка.

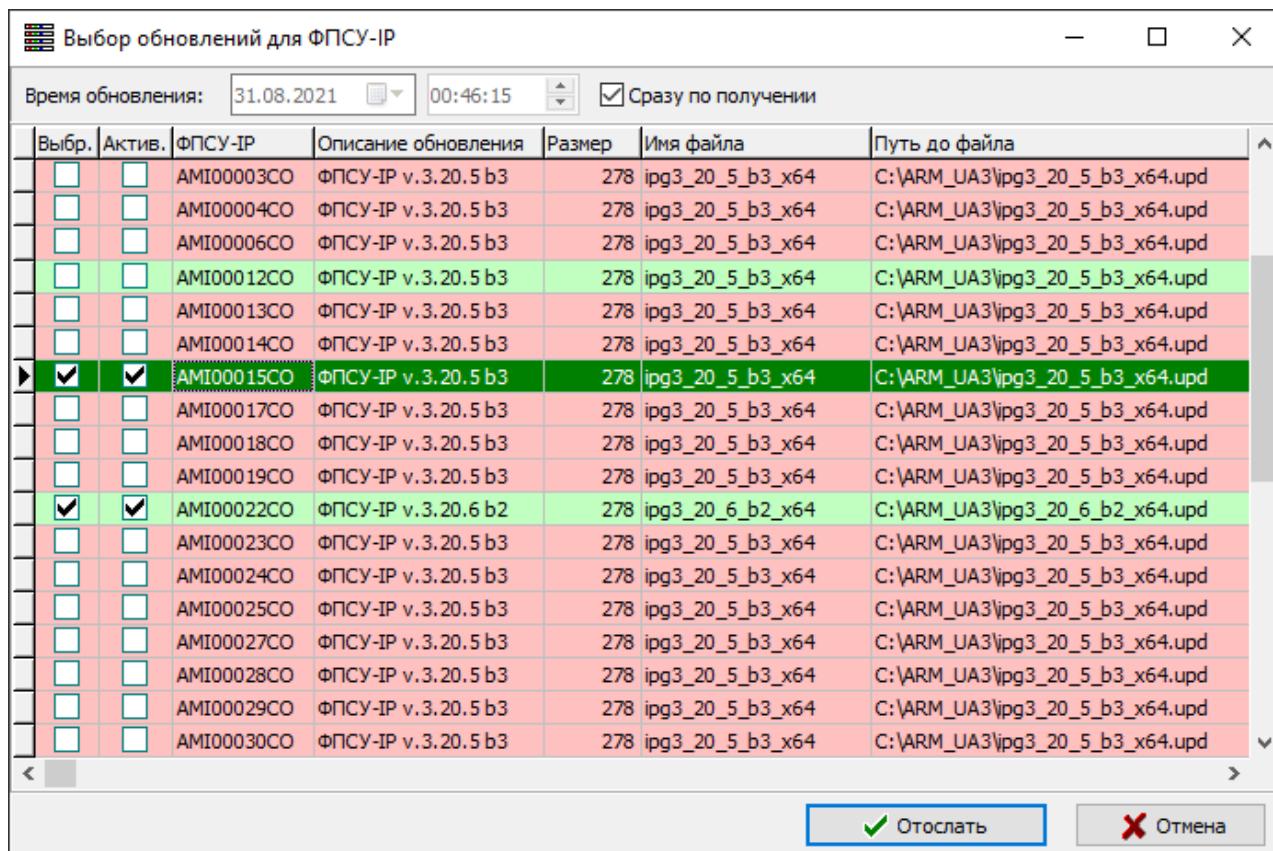


Рисунок 168 - Список обновлений ПО для рассылки на ФПСУ-IP

После того, как в списке выбраны обновления, которые требуется разослать на ФПСУ-IP, необходимо нажать кнопку «Отослать».

В открывшемся окне будет отображаться состояние загрузки обновлений ПО на ФПСУ-IP:

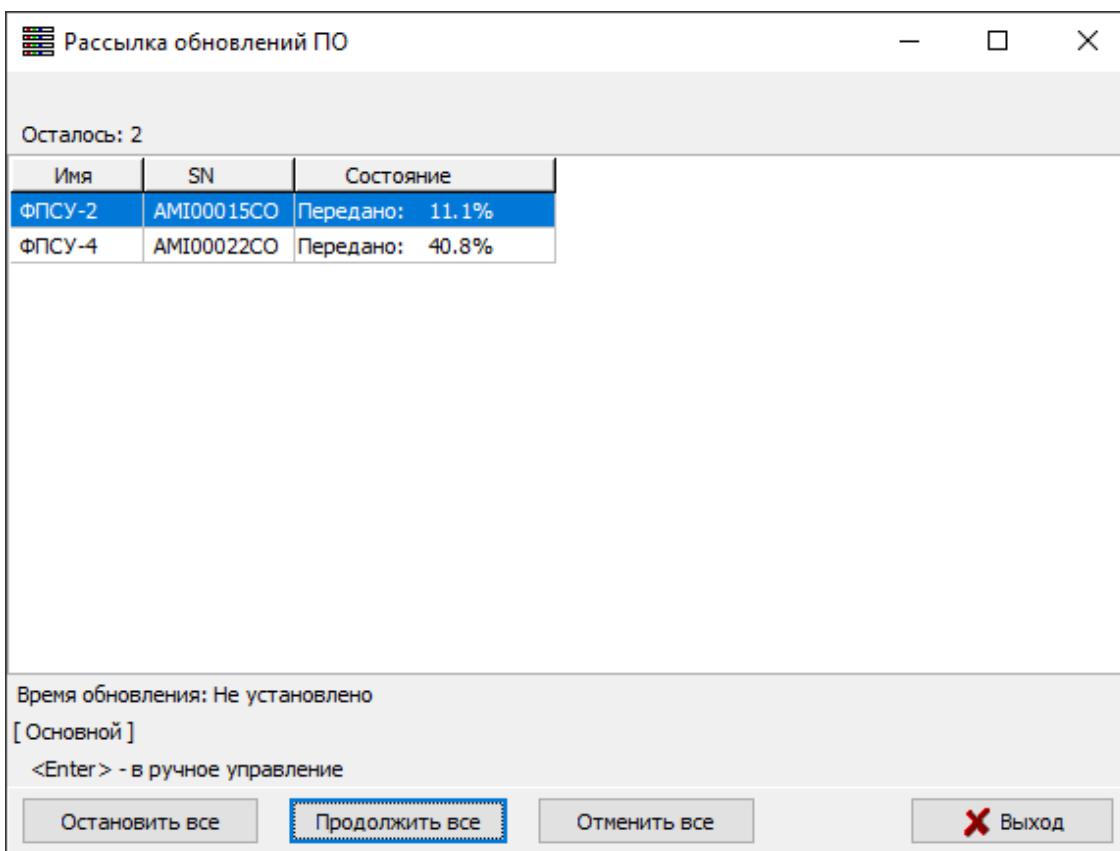


Рисунок 169 - Отображение процесса рассылки обновлений ПО на ФПСУ-IP

Процесс рассылки может быть остановлен, возобновлен и отменен с помощью команд окна «Остановить все», «Продолжить все» и «Отменить все».

Нажав кнопку «Выход», можно скрыть окно передачи. При необходимости, его можно вернуть на экран, выполнив команду главного меню УА ФПСУ-IP «Операции» → «Показать состояние задания».

Сообщение об активизации обновления на каждом ФПСУ-IP будет выдано сразу после доставки и установки его на ФПСУ-IP. Если время установки обновления отложено, то сообщение будет выдано после активизации:

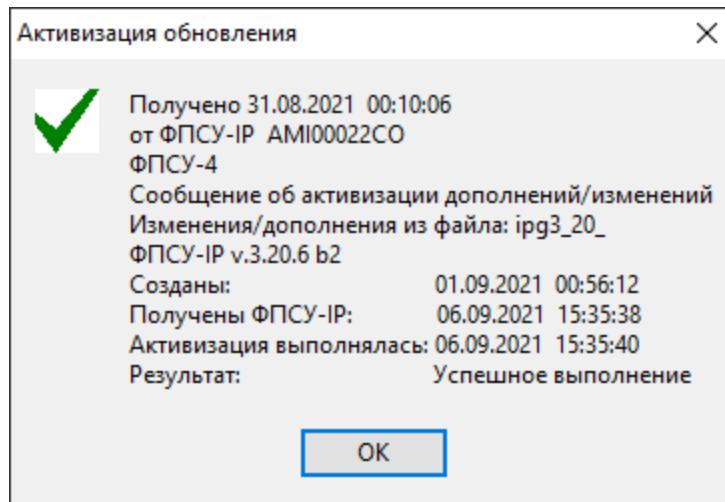


Рисунок 170 - Успешная установка обновления ПО на ФПСУ-IP

После того, как все обновления ПО доставлены на ФПСУ-IP, на экран будет выдано сообщение об успешной рассылке:

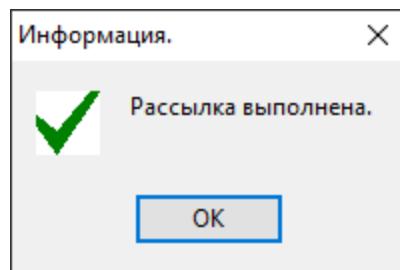


Рисунок 171 - Успешная рассылка обновлений ПО на ФПСУ-IP

12. 10. Wake On LAN

Wake-on-LAN является технологией, позволяющей удаленно включить хост посредством отправки через локальную сеть специального пакета данных (так называемого magic packet — «волшебного пакета»). Данная функция доступна при работе УА ФПСУ-IP с ФПСУ-IP начиная с версии 3.20.1.

Для настройки Wake on LAN на ФПСУ-IP следует выбрать ФПСУ-IP в общем списке и выполнить команду главного меню УА ФПСУ-IP «Операции» → «Wake-on-LAN». На экран будет выдано одноименное окно, позволяющее составить список хостов для удаленного включения.

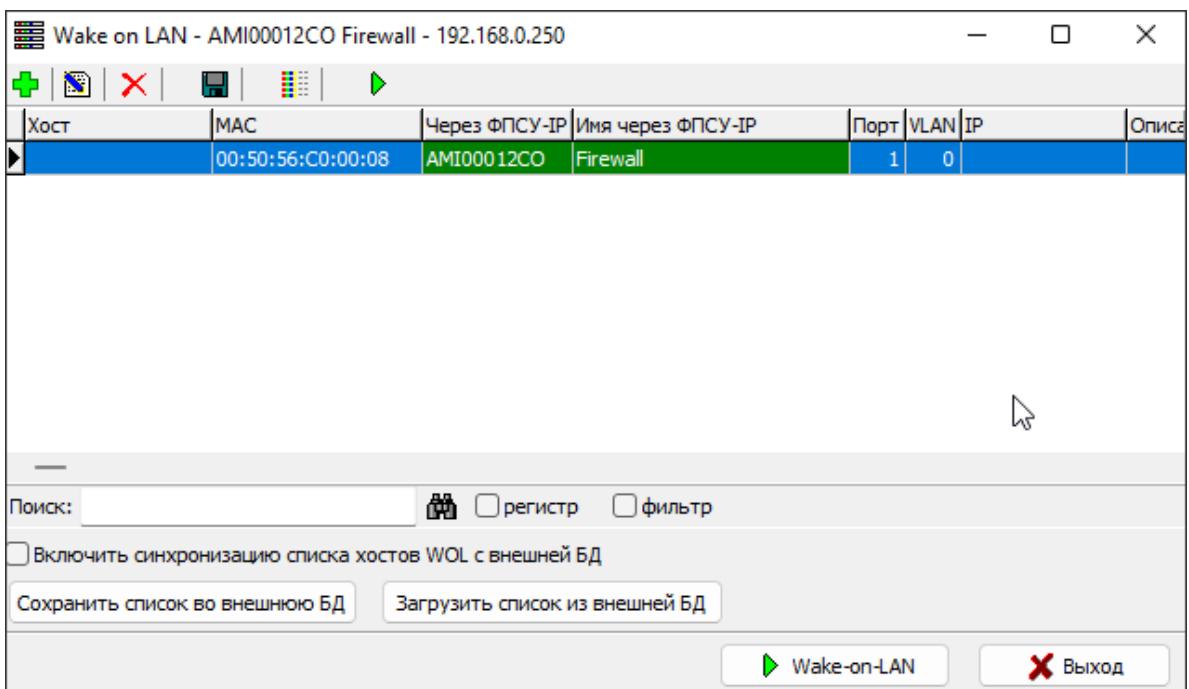


Рисунок 172 - Работа с Wake-on-LAN

В открывшемся окне предоставляется возможность просмотреть список хостов, добавленных ранее, изменить этот список (добавить хост в список, удалить или изменить параметры хоста), сохранить список во внешнюю БД или загрузить заранее сохраненный список из нее.

Для того, чтобы добавить хост в список необходимо в окне «Wake on LAN» нажать

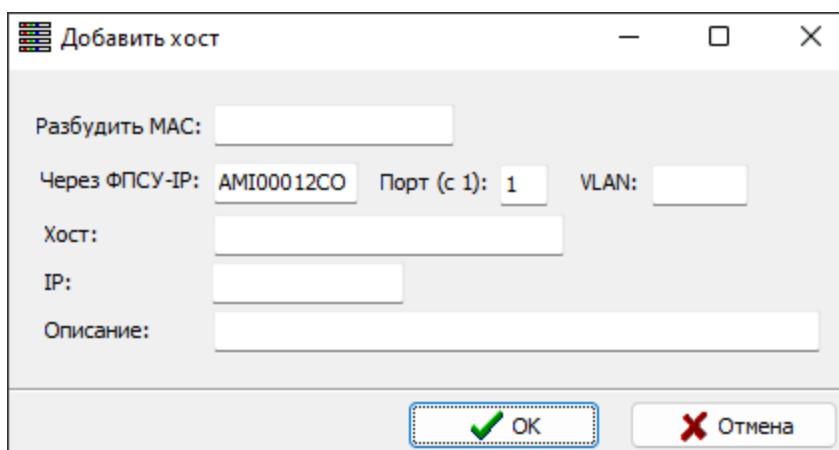


Рисунок 173 - Добавление хоста для WOL

В открывшемся окне следует ввести MAC-адрес хоста, на который будет отправлен «магический пакет», доменное имя хоста и/или его IP-адрес. Кроме того, предоставляется возможность добавить необходимый комментарий в поле «Описание», а так же ФПСУ-IP (и/или такие его параметры, как порт или VLAN), через который будет отправлен «магический пакет». Для подтверждения добавления хоста в список необходимо нажать кнопку «OK».

При необходимости параметры внесенного в список хоста можно изменить. Для

этого следует нажать кнопку «Изменить хост»

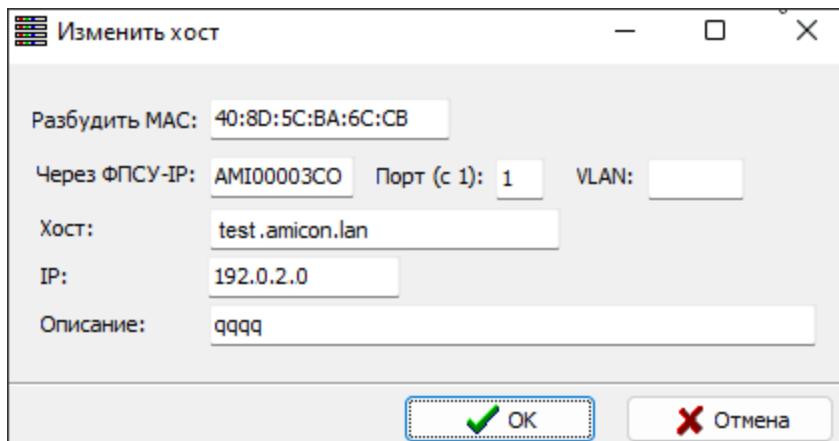
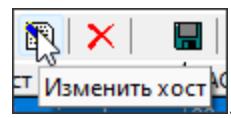


Рисунок 174 - Изменение параметров хоста для WOL

В окне «Изменить хост» предоставляется возможность изменить параметры выбранного хоста и подтвердить изменения нажатием кнопки «OK». Необходимо иметь в виду, что в случае некорректного ввода серийного номера ФПСУ-IP, через который будет отправляться «магический пакет», по нажатию «OK» программа выдаст сообщение об этом:

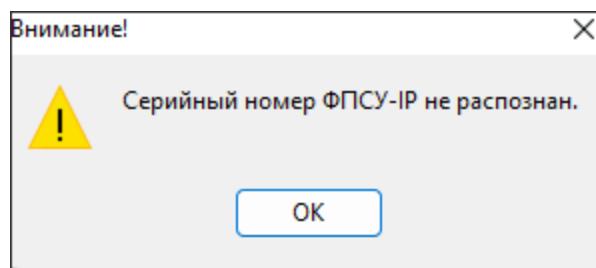


Рисунок 175 - Окно предупреждения

Составленный список хостов можно сохранить во внешнюю базу данных нажатием одноименной кнопки. По кнопке «Загрузить список из внешней БД» предоставляется

возможность загрузить ранее сохраненный во внешней базе данных список.

По нажатию кнопки «Wake-on-LAN» на экран будет выведено сообщение об отправке пакета:

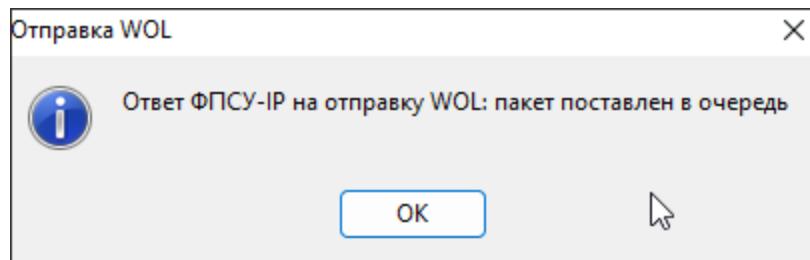


Рисунок 176 - Ответ ФПСУ-IP на отправку WOL

13. Настройка УА ФПСУ-IP

В разделе приведены сведения о настройке УА ФПСУ-IP: журнала работы УА ФПСУ-IP (лога), внешнего вида УА ФПСУ-IP, режима работы с разграничением полномочий пользователей, включение режима сохранения версий конфигураций ФПСУ-IP в архив.

13. 1. Меню «Параметры» → «Настройки»

Доступ к настройке журнала работы и внешнего вида УА ФПСУ-IP осуществляется командой главного меню «Параметры» → «Настройки». При выполнении команды на экран будет выведено служебное окно настроек, содержащее шесть вкладок — «Список ФПСУ-IP», «Логи», «Интерфейс», «Работа с ФПСУ-IP», «Параметры syslog», «Опрос SNMP ФПСУ-IP».

13. 1. 1. Настройки списка ФПСУ-IP

Вкладка «Список ФПСУ-IP» предоставляет пользователю возможность выбора порядка отображения имени зарегистрированных ФПСУ-IP в окне списка УА ФПСУ-IP, и содержит два флага.

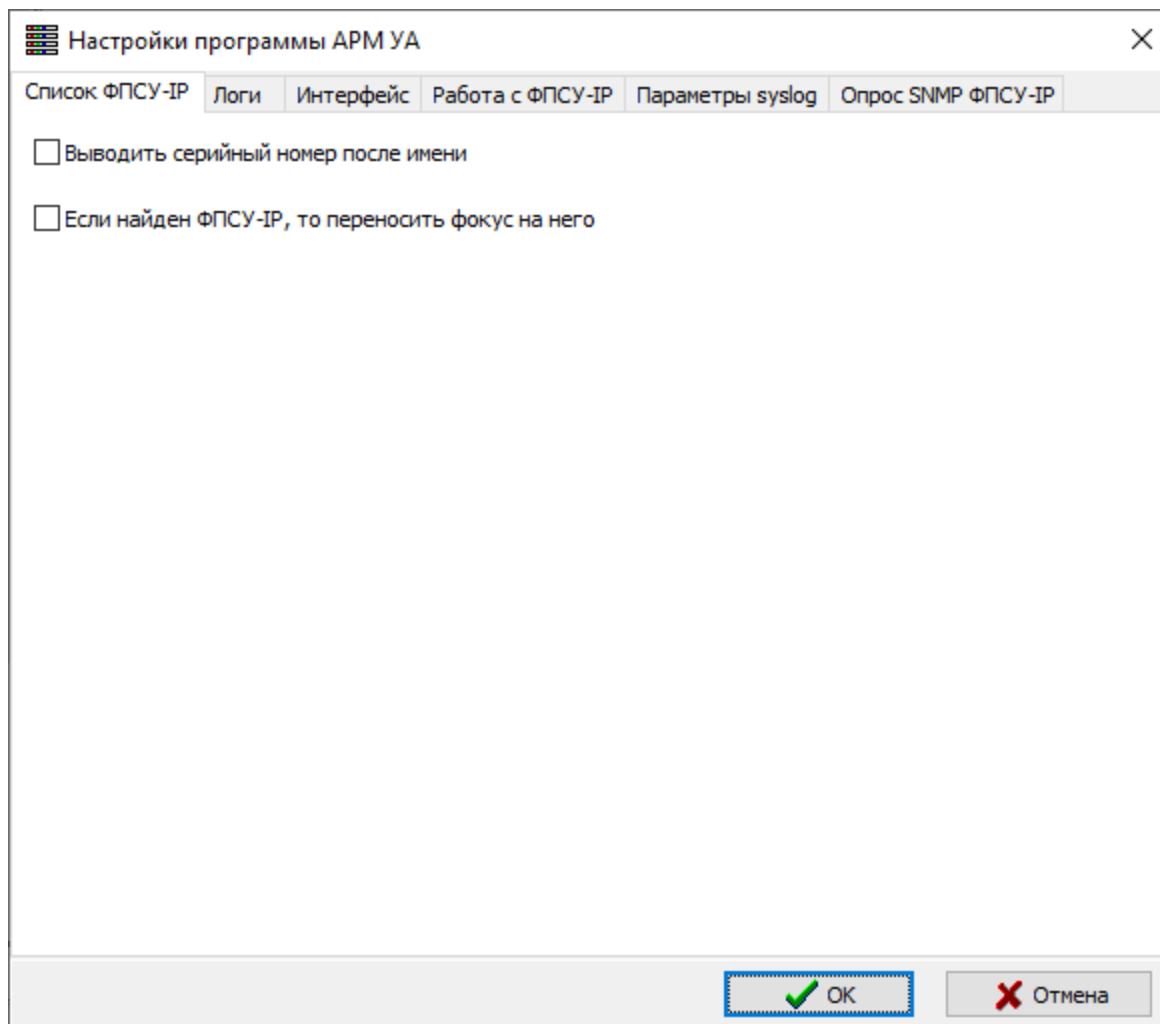


Рисунок 177 - Вкладка «Список ФПСУ-IP»

Установленный флаг «Выводить серийный номер после имени» добавляет к отображаемому имени зарегистрированного ФПСУ-IP его серийный номер. При снятом флаге в окне списка отображаются имена ФПСУ-IP, заданные по умолчанию, или переименованные администратором УА ФПСУ-IP.

Переключатель «Если найден ФПСУ-IP, то переносить фокус на него» относится к работе панели поиска основного окна УА ФПСУ-IP. Во включенном состоянии при выполнении поиска, переключатель переносит активный курсор выбора строки в поле списка на найденный ФПСУ-IP.

13. 1. 2. Настройка журнала событий с ФПСУ-IP на УА ФПСУ-IP

УА ФПСУ-IP может регистрировать, вести журнал событий, связанных с

управлением и мониторингом ФПСУ-IP. Могут регистрироваться события связи с ФПСУ-IP (отсутствие связи, выход на связь с ФПСУ-IP), и дополнительные сообщения от ФПСУ-IP, отправляемые на УА ФПСУ-IP.

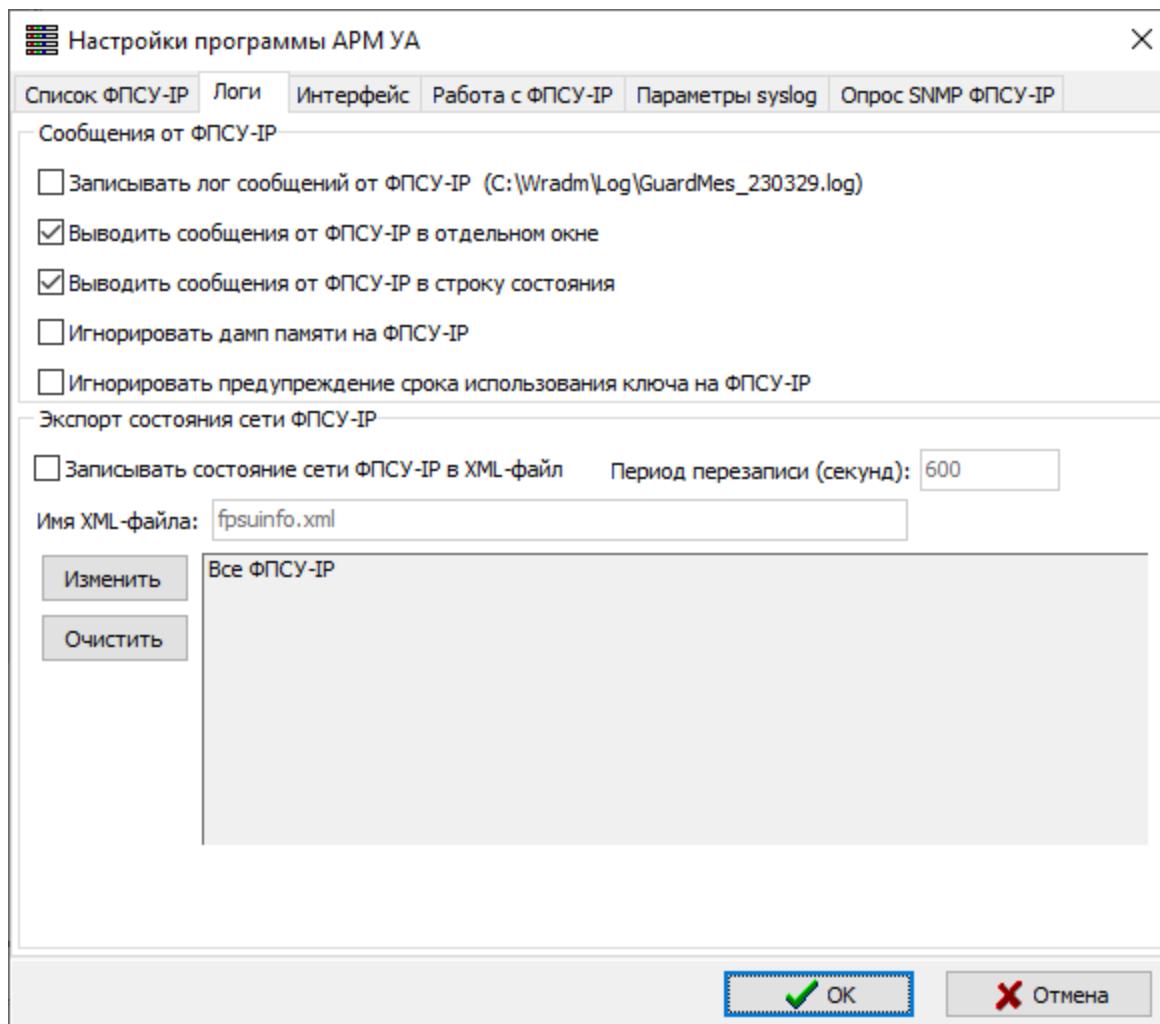


Рисунок 178 - Настройки журналов УА ФПСУ-IP (логов)

Если требуется вести журнал событий связи с ФПСУ-IP, следует установить флаг «Записывать лог событий связи с ФПСУ-IP». Путь к файлам журнала, в которые заносятся регистрируемые события, указан в скобках. Файлы носят название «ConEvent_ГГММДД.log» (год, месяц и число событий за сутки), и могут быть прочитаны средствами любого текстового редактора и/или средствами редактора электронных таблиц.

Установленный флаг «Поддерживать список для формы событий связи с ФПСУ-IP»

Если требуется вести журнал других сообщений (из перечня в разделе «Управление и мониторинг ФПСУ-IP»), отправляемых к УА ФПСУ-IP от ФПСУ-IP, следует установить

флаг «Записывать лог сообщений от ФПСУ-IP». Будут созданы файлы журнала, GuardMesГГММДД.log, в которые будут записываться отправленные ФПСУ-IP сообщения.

Флаг «Выдавать сообщения от ФПСУ-IP в отдельном окне» позволяет отображать каждое новое присланное от ФПСУ-IP сообщение в отдельном всплывающем окне.

Флаг «Выводить сообщения от ФПСУ-IP в строку состояния» включает мигание строки состояния УА ФПСУ-IP при получении сообщения от ФПСУ-IP.

При снятых флагах «Записывать лог событий связи с ФПСУ-IP», «Выдавать сообщения от ФПСУ-IP в отдельном окне», «Выводить сообщения от ФПСУ-IP в строку состояния», оповещение о событии на управляемом ФПСУ-IP будет производится только звуковым сигналом спикера (по умолчанию, если не выбран другой сигнал);

При установленном флаге «Игнорировать предупреждение срока использования ключа на ФПСУ-IP» предупреждение об истечении срока выводиться не будет.

Установленный флаг «Записывать состояние сети ФПСУ-IP в XML-файл» позволяет хранить статистику по выбранным ФПСУ-IP в формате xml. Требуется задать период перезаписи и имя xml-файла, либо оставить по умолчанию. По кнопке «Изменить» выбрать ФПСУ-IP, для которых будет записываться статистика, по умолчанию отмечены все ФПСУ-IP.

13. 1. 3. Дополнительные настройки интерфейса УА ФПСУ-IP

Вкладка «Интерфейс» содержит флаги:

- «Информационные окна всегда поверх главного». Следует установить этот флаг, если необходимо видеть получаемые информационные и служебные сообщения УА ФПСУ-IP, всегда поверх основного окна УА ФПСУ-IP;
- «Минимизировать программу в Системную область Панели задач». Следует установить его, если требуется при сворачивании УА ФПСУ-IP перемещать её не на панель задач Windows, а в область уведомлений.

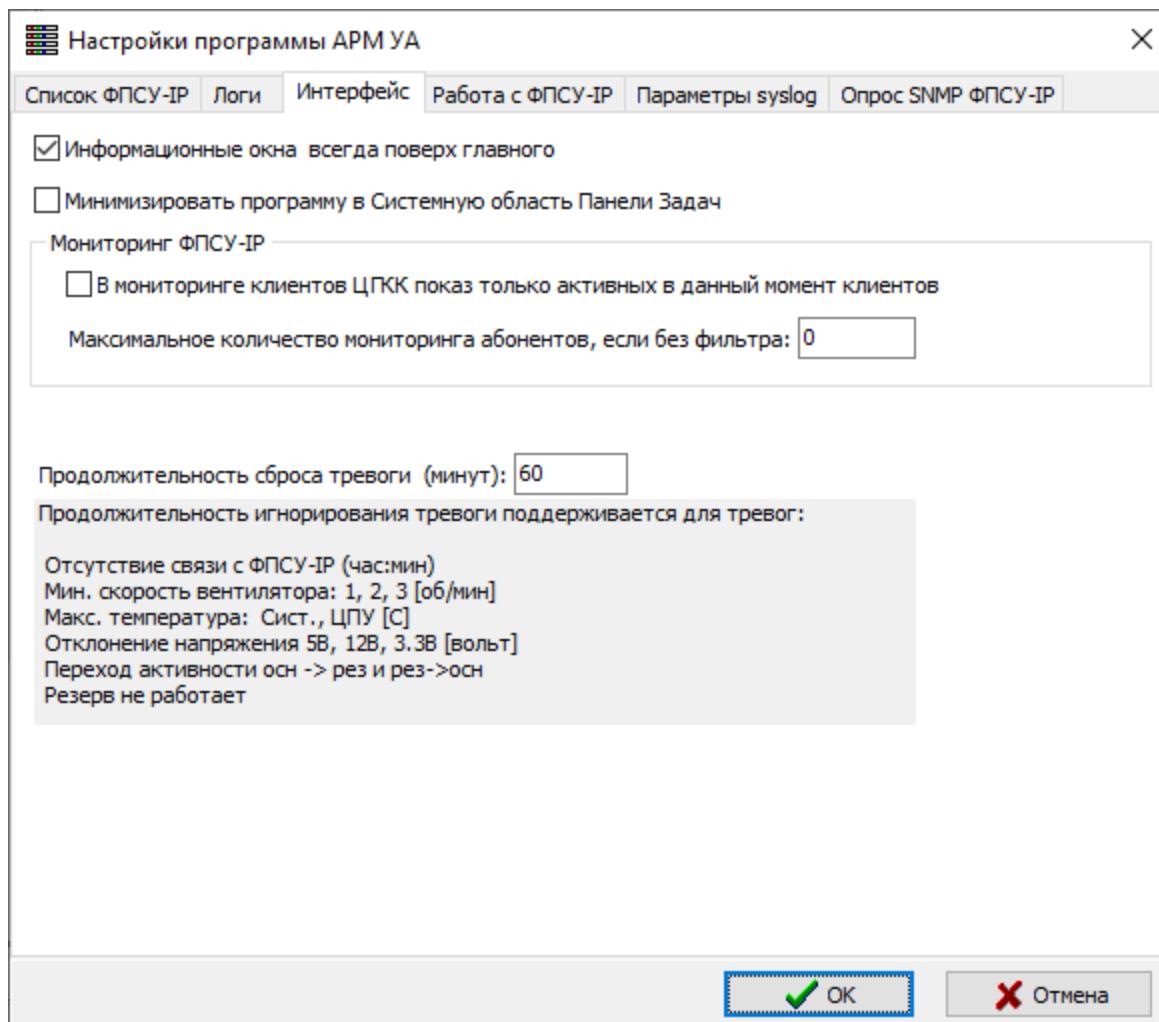


Рисунок 179 - Вкладка «Интерфейс»

- «Мониторинг клиентов ФПСУ-IP»- флаг «В мониторинге клиентов ЦГКК показ только активных в данный момент клиентов». Установка этого флага приводит к тому, что в интерфейсе просмотра данных ФПСУ-IP/Клиентов, передаваемых через ФПСУ-IP (см. пункт «Получение информации о работе клиентов»), запрашиваются и отображаются данные только тех клиентов, которые в настоящий момент соединены с ФПСУ-IP. Эта настройка работает глобально, для всех ФПСУ-IP, зарегистрированных на УА ФПСУ-IP;
- «Продолжительность сброса тревоги (минут)». В данном поле устанавливается время, когда УА ФПСУ-IP не будет доступен. По умолчанию — 60 минут. Ниже идет список событий, для которого работает данная опция:
 - отсутствие связи с ФПСУ-IP (в формате ЧЧ:ММ);

- минимальная скорость вентилятора номер 1, 2 и 3 в оборотах в минуту;
- максимальная температура материнской платы и процессоров;
- отклонение напряжения в схемах 5 В, 12 В и 3.3 В;
- передача управления от основного к резервному ФПСУ-IP и наоборот в системе «горячего» резервирования;
- оповещение неработоспособности одного из комплексов в системе «горячего» резерва.

13. 1. 4. Дополнительные настройки УА ФПСУ-IP при работе с ФПСУ-IP

Вкладка «Работа с ФПСУ-IP» настроек УА ФПСУ-IP предназначена для указания прочих настроек, например включения ведения архива конфигураций ФПСУ-IP и режима работы УА ФПСУ-IP с несколькими администраторами УА ФПСУ-IP (несколькими подключенными к компьютеру VPN-Key/UA с учетными данными разных администраторов) одновременно.

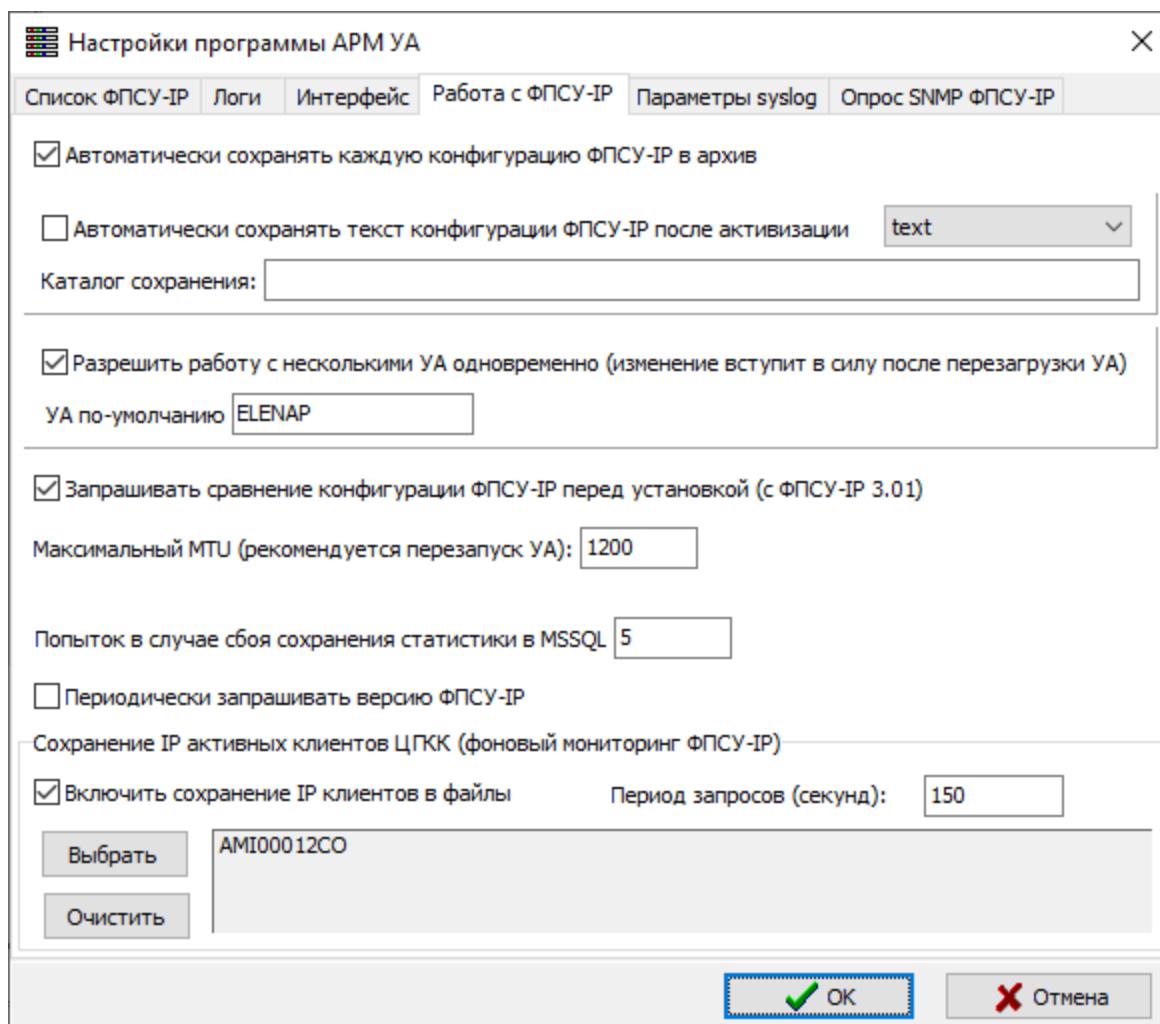


Рисунок 180 - Дополнительные настройки УА ФПСУ-IP, работа с ФПСУ-IP

- Флаг «Автоматически сохранять каждую конфигурацию ФПСУ-IP в архив» указывает на необходимость ведения истории версий конфигураций. Когда администратор УА ФПСУ-IP несколько раз изменяет полученную с ФПСУ-IP конфигурацию, то каждое изменение, подтвержденное корректным выходом из конфигуратора ФПСУ-IP, сохраняется УА ФПСУ-IP в специальном архиве версий конфигураций ФПСУ-IP. Любую такую архивированную версию конфигурации отдельного ФПСУ-IP администратор УА ФПСУ-IP может вернуть из архива, сделав актуальной. Подробнее см. пункт «Архивы конфигураций ФПСУ-IP».
- Флаг «Автоматически сохранять текст конфигурации ФПСУ-IP после активизации» позволяет вести историю изменений конфигурации, используется для отчётности. В выпадающем списке указывается формат файла, в котором будет сохранена конфигурация. Форматы text и dsr используются сторонними парсерами

конфигурации.

- Флаг «Разрешить работу с несколькими УА одновременно» позволяет работать с несколькими подключенными к компьютеру VPN-Key/UA с учетными данными разных администраторов (см. пункт «Режим работы с несколькими администраторами УА ФПСУ-IP»). В многопользовательском режиме работы УА ФПСУ-IP может быть задан администратор УА ФПСУ-IP по умолчанию.
- Флаг «Запрашивать сравнение конфигурации ФПСУ-IP перед установкой» позволяет сравнивать конфигурации перед внесением изменений.
- «Максимальный MTU» рекомендуется устанавливать в значение 1200. В этом поле указывается MTU на отправку пакетов от УА ФПСУ-IP до ФПСУ-IP.
- Количество попыток в случае сбоя сохранения статистики MSSQL позволяет продолжить ведение статистики после сбоя записи в базу данных статистики, отказа доступа к сети или аппаратной проблемы сетевого адаптера. В случае, если проблема устранена, запись статистики в базу данных под управлением СУБД MSSQL возобновляется с момента успешной повторной попытки записи. Запросы на сохранение статистики продолжаются непрерывно (без тайм-аута). При исчерпании попыток записи статистики в базу данных возобновить ведение статистики можно только с помощью перезагрузки УА ФПСУ-IP. В случае, если статистика потеряна, её можно восстановить из файла архива (см. пункт «Управление статистикой ФПСУ-IP»).
- Установка флага «Периодически запрашивать версию ФПСУ-IP» означает то, что все ФПСУ-IP, зарегистрированные на УА ФПСУ-IP будут постепенно опрошены для получения версии и даты окончания поддержки ПО.
- В области «Сохранение IP активных клиентов ЦГКК (фоновый мониторинг ФПСУ-IP)» задаются настройки для постепенного опроса выбранных ФПСУ-IP для получения IP-адресов активных клиентов. Данные мониторинга сохраняются в текстовый файл с расширением txt, текст структурирован в формате CSV.

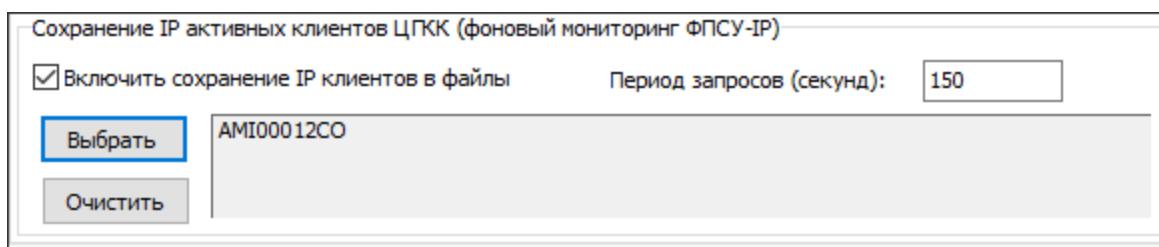


Рисунок 181 - Настройка фонового мониторинга ФПСУ-IP

Для включения фонового мониторинга ФПСУ-IP в области «Сохранение IP активных клиентов ЦГКК (фоновый мониторинг ФПСУ-IP)» необходимо выполнить действия:

1. Установить флаг «Включить сохранение IP клиентов в файлы».
2. Задать период запросов.
3. Для выбора опрашиваемых ФПСУ-IP следует нажать кнопку «Выбрать» и в открывшемся окне выбрать ФПСУ-IP, отметив знаком X в столбце «Выбор».

При наведении курсора мыши на флаг «Включить сохранение IP клиентов в файлы» во всплывающей подсказке отображается путь сохранения в рабочем каталоге и имя файла для заданного ФПСУ-IP в формате «\ipclient\SN_ГГММДД_ЧЧММ.txt» (где SN - серийный номер ФПСУ-IP). Для каждого выбранного ФПСУ-IP будет создан файл со списком IP-адресов активных клиентов.

После сохранения настроек УА ФПСУ-IP по нажатию кнопки «OK», результаты фонового мониторинга ФПСУ-IP будут доступны в указанных файлах.

13. 1. 5. Настройка параметров syslog

Во вкладке Параметры syslog предоставляется возможность включить отправку сообщений о происходящих в УА событиях (то есть создания событийных журналов).

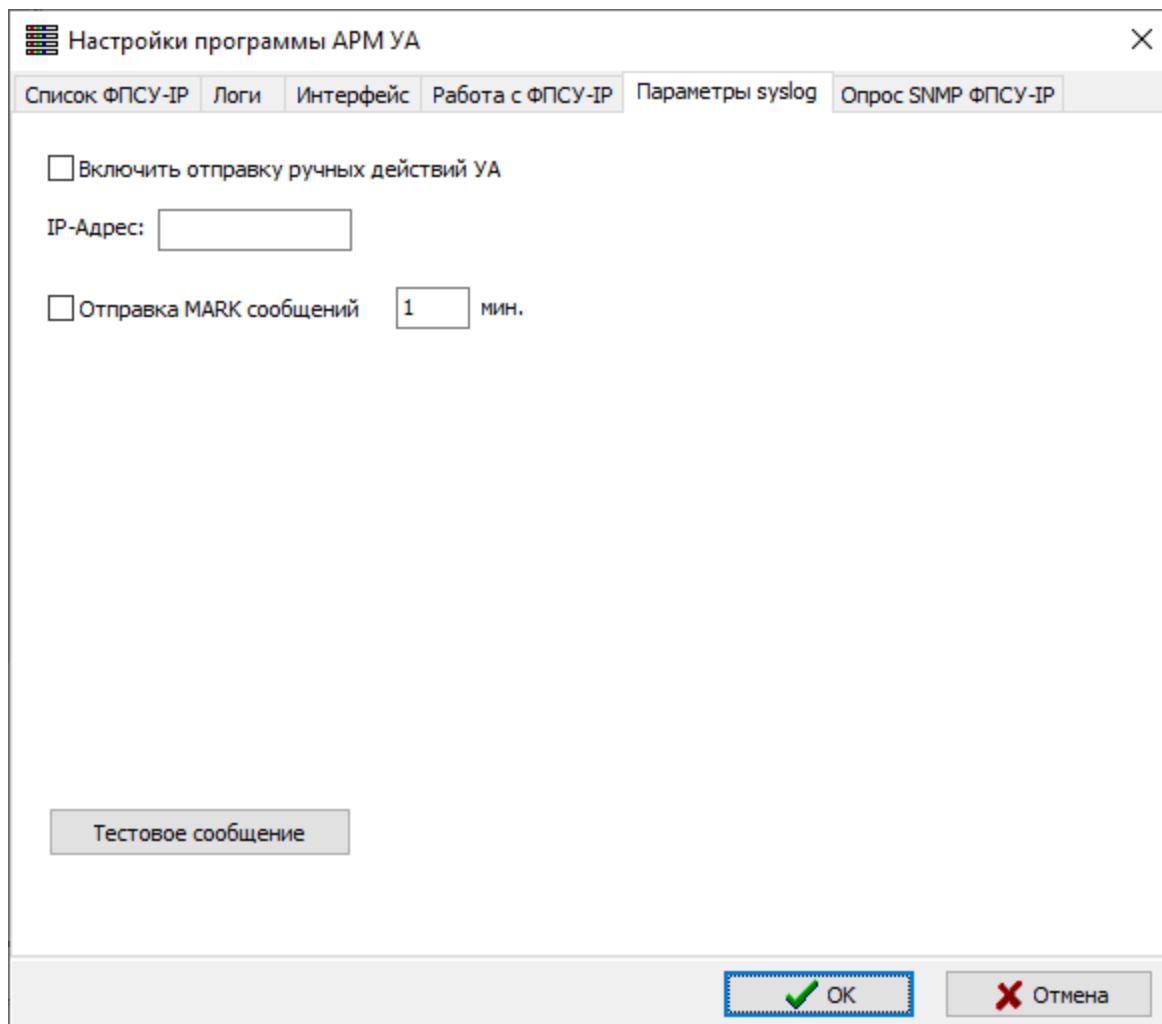


Рисунок 182 - Параметры syslog

В случае настроенного syslog сервера системные сообщения о событиях на ФПСУ-IP будут отправляться на указанный IP-адрес.

При установлении флага «Включить отправку ручных действий УА» необходимо указать IP-адрес syslog сервера, на который будут отправляться действия удаленного администратора.

При установлении флага «Отправка MARK сообщений» необходимо указать время, по истечении которого будет отправляться данное сообщение. MARK сообщение подтверждает, что УА на связи, является аналогом keepalive сообщения с заданным интервалом времени.

13. 1. 6. Настройка опроса SNMP ФПСУ-IP

Во вкладке «Опрос SNMP ФПСУ-IP» предоставляется возможность проводить опрос списка ФПСУ-IP. Фиксированный набор параметров запрашивается SNMP-менеджером, начиная с указанной даты, с заданной периодичностью.

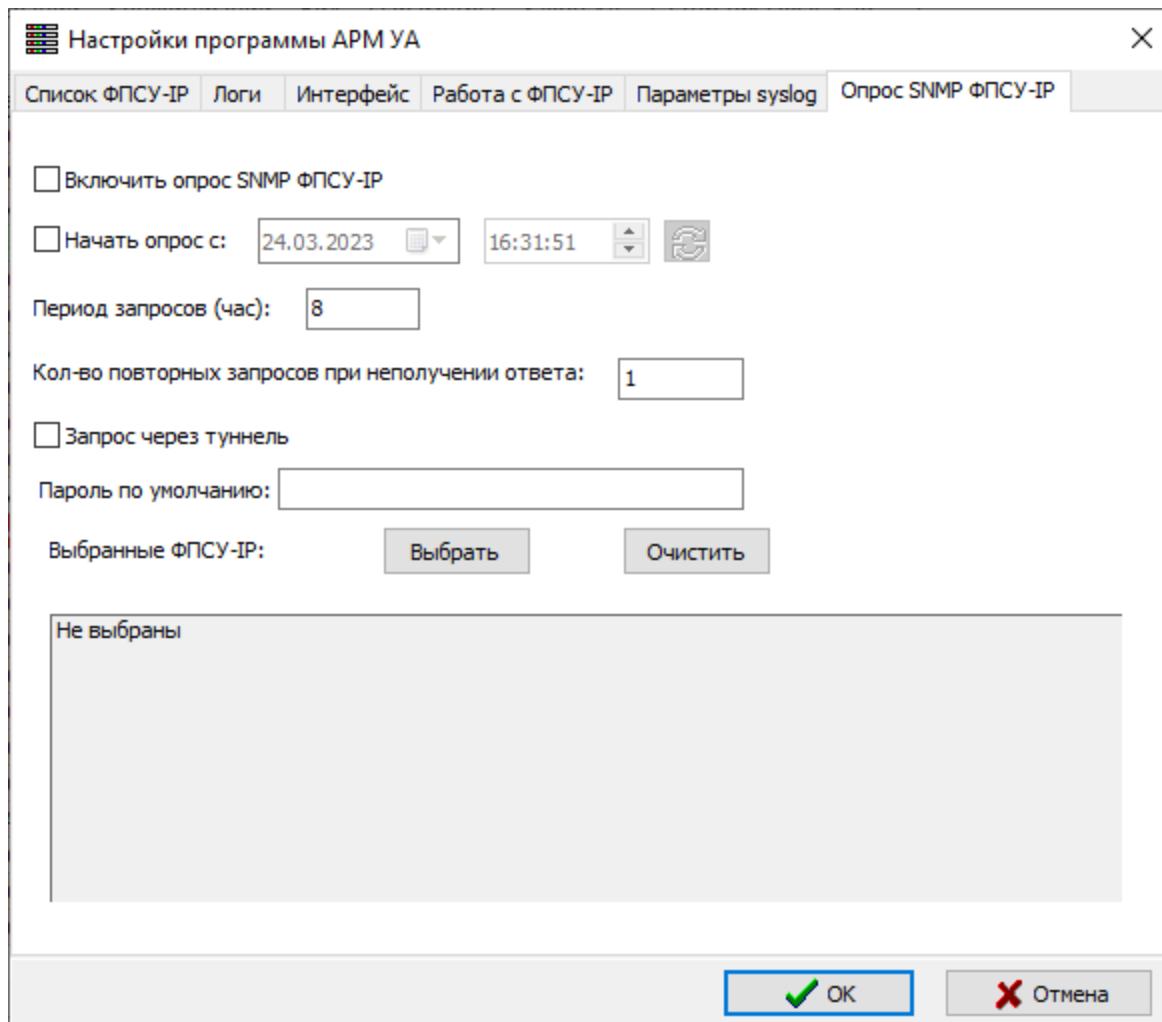


Рисунок 183 - Параметры опроса SNMP

Для включения опроса необходимо установить соответствующий флаг. Задать дату и время начала опроса, установить период запросов, в случае неполучения ответа может быть указано количество повторных запросов.

При установлении флага «Запрос через туннель» SNMP сообщения от ФПСУ-IP будут отправлены по защищенному соединению через VPN-туннель «УА-ФПСУ-IP» (применяется для ФПСУ-IP версии 3.30.1 и выше).

Необходимо указать пароль, который запрашивается при направлении запроса к SNMP-агенту, работающему на ФПСУ-IP, от SNMP-менеджера.

Требуется задать список опрашиваемых ФПСУ-IP по нажатию кнопки «Выбрать». В открывшемся окне отметьте ФПСУ-IP в столбце «Выбор», нажмите кнопку «Выбрать».

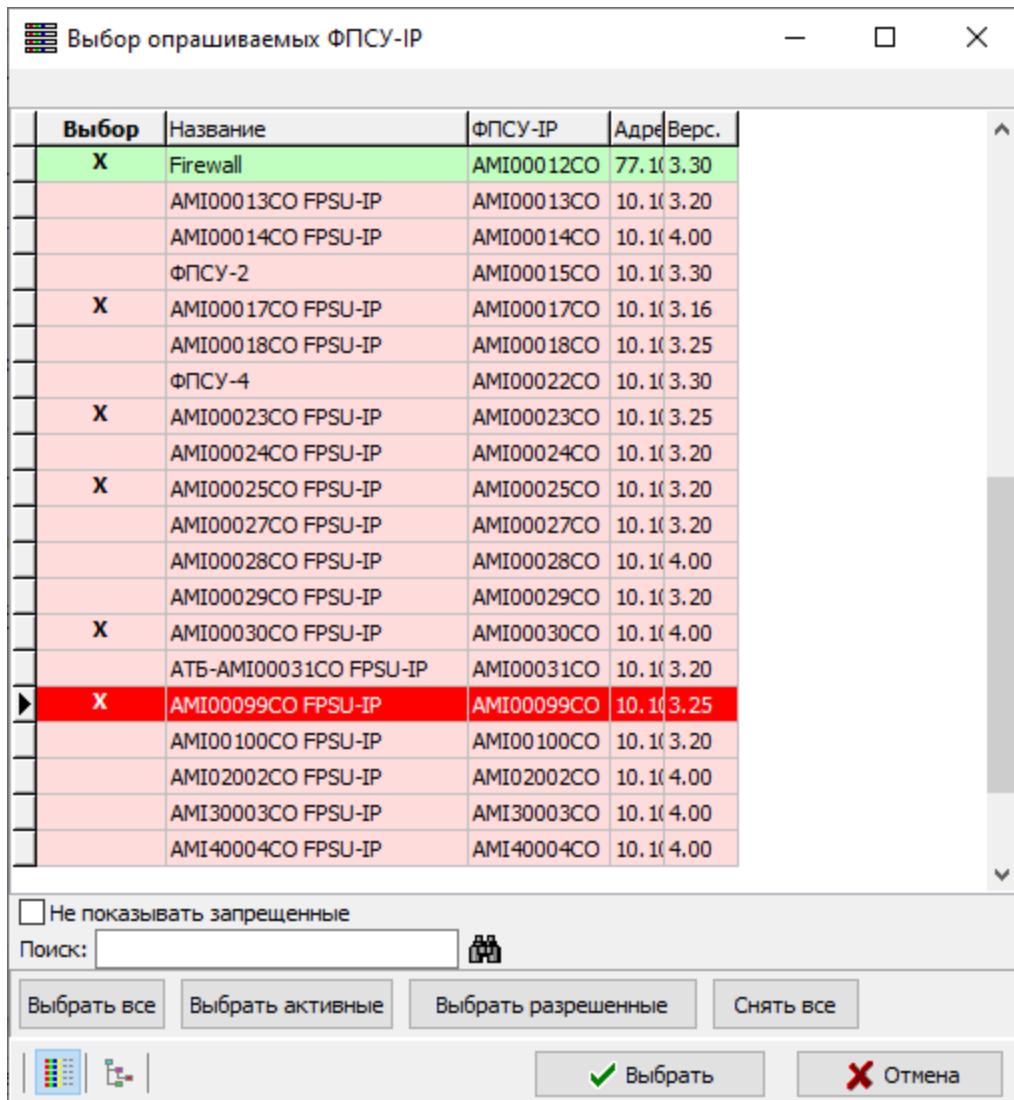
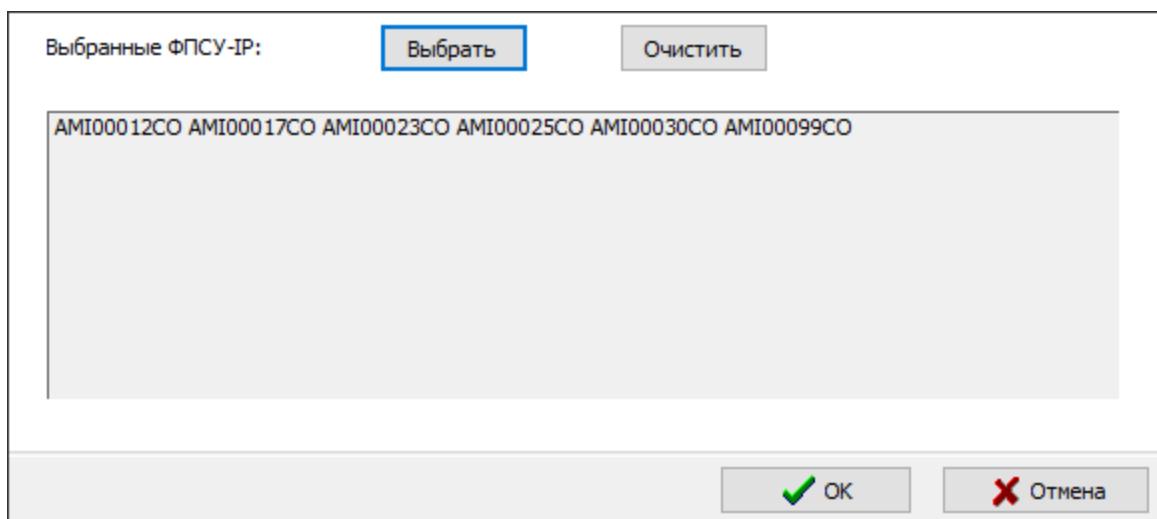


Рисунок 184 - Выбор списка опрашиваемых ФПСУ-IP

На вкладке «Опрос SNMP ФПСУ-IP» в поле «Выбранные ФПСУ-IP» отобразится список выбранных для опроса ФПСУ-IP.

**Рисунок 185 - Опрашиваемые ФПСУ-IP**

При опросе ФПСУ-IP отправляет SNMP сообщение, состоящее из строк параметров ФПСУ-IP, формат строки параметра приводится в таблице ниже. Стока параметра состоит из информационных полей. Границы полей обозначаются запятой «,».

Таблица 2. Формат строки параметра

Значение параметра основного ФПСУ-IP	Значение параметра резервного ФПСУ-IP	Имя параметра	OID	MIB
--------------------------------------	---------------------------------------	---------------	-----	-----

Для каждого ФПСУ-IP запрашиваются параметры, перечисленные в таблице.

Таблица 3. Параметры ФПСУ-IP, запрашиваемые при опросе SNMP

Имя параметра	OID	MIB
Версия	1.3.6.1.4.1.37249.1.1.1.2.4.1	aFpsuSwVer
Дата поддержки	1.3.6.1.4.1.37249.1.1.1.2.4.3	aFpsuSwEndSupportDate
Дата изготовления ФПСУ-IP	1.3.6.1.4.1.37249.1.1.1.2.2	aFpsuBuildDate

Имя параметра	OID	MIB
Аппаратная платформа	1.3.6.1.4.1.37249.1.1.1.2.3.1.2	aFpsuHwSystemName
Серийный номер платформы	1.3.6.1.4.1.37249.1.1.1.2.3.2.4	aFpsuHwMainboardSerialNumber
Дата установки ПО ФПСУ-IP	1.3.6.1.4.1.37249.1.1.1.2.4.2	aFpsuSwInstallationDate
CPU	1.3.6.1.4.1.37249.1.1.1.2.3.6.1.7.1	aFpsuHwCpuInfoVersion_1
ОЗУ в мегабайтах	1.3.6.1.4.1.37249.1.1.1.2.3.4.1	aFpsuHwMemoryRamMbs
Модель системной платы	1.3.6.1.4.1.37249.1.1.1.2.3.2.2	aFpsuHwMainboardName
Автозапуск системы	1.3.6.1.4.1.37249.1.1.1.2.4.4	aFpsuSwAutostart
MAC-адрес осн. порт 1	1.3.6.1.4.1.37249.2.1.12.1.5.1	aFpsuHotReserveStateLocalMac_1
MAC-адрес осн. порт 2	1.3.6.1.4.1.37249.2.1.12.1.5.2	aFpsuHotReserveStateLocalMac_2
MAC-адрес рез. порт 1	1.3.6.1.4.1.37249.2.1.12.1.6.1	aFpsuHotReserveStateRemoteMac_1
MAC-адрес рез. порт 2	1.3.6.1.4.1.37249.2.1.12.1.6.2	aFpsuHotReserveStateRemoteMac_2
Установленные открытые ключи администраторов	1.3.6.1.4.1.37249.2.1.3.1.3	aFpsuAdminPackedName

13. 2. Режим разграничения полномочий пользователей УА ФПСУ-IP

По умолчанию использование УА ФПСУ-IP не предусматривает администраторов с

разными правами. Администратор УА ФПСУ-IP может выполнять все команды, управлять базой данных статистики и параметров работы УА ФПСУ-IP, управлять ФПСУ-IP без дополнительных ограничений, в соответствии с правами, выанными локальным администратором администратору УА ФПСУ-IP.

Для реализации возможности работы пользователя ФПСУ-IP в режиме наблюдателя, не имеющего дополнительных прав по настройке УА ФПСУ-IP, введена возможность включения многопользовательского режима. Включение выполняется командой главного меню «Параметры» → «Пользователи/Пароли...».

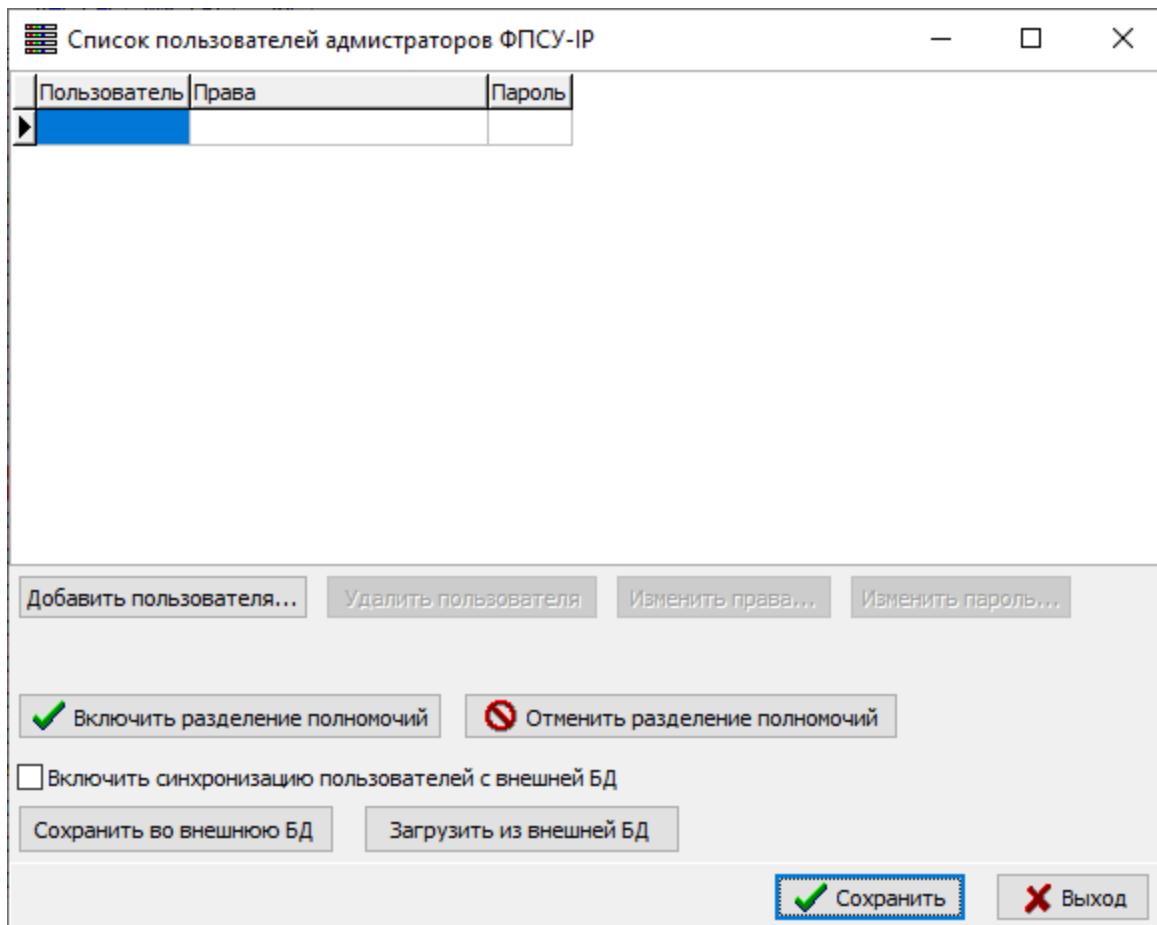


Рисунок 186 - Список пользователей администраторов ФПСУ-IP

«Включить разделение полномочий» – При выполнении команды отобразится служебное сообщение. Необходимо подтвердить включение режима разделения полномочий пользователей УА ФПСУ-IP.

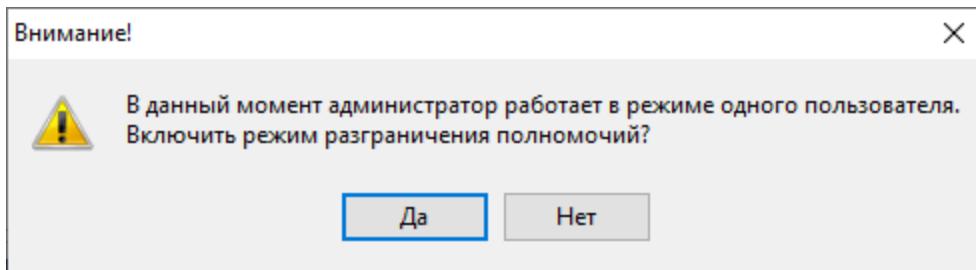


Рисунок 187 - Включение режима разграничения пользователей

При включении многопользовательского режима в список пользователей УА ФПСУ-IP будут добавлены три учетные записи по умолчанию:

- Admin, которая имеет полномочия роли «Администратор», аналогичные правам при работе в режиме одного пользователя;
- Monitor, имеющий полномочия роли «Мониторинг»;
- Radmin, имеющий полномочия роли «УА ФПСУ-IP», аналогичные роли «Администратор» без права редактирования режима разграничения полномочий.

Пользователь с полномочиями роли «Администратора» получает полный доступ к настройкам УА ФПСУ-IP и возможностям по работе с управляемыми ФПСУ-IP. Пользователь с полномочиями роли «Мониторинг» не получает прав по изменению конфигураций зарегистрированных ФПСУ-IP, отправки изменений и дополнений, дистанционной установке ключевых данных, изменению параметров работы УА ФПСУ-IP и зарегистрированных в ней ФПСУ-IP, регистрации новых ФПСУ-IP, изменению внутренней базы данных УА ФПСУ-IP. Пользователь, с полномочиями УА, получает все права ролей «Администратор» и «Мониторинг» кроме возможности редактирования режима разграничения полномочий.

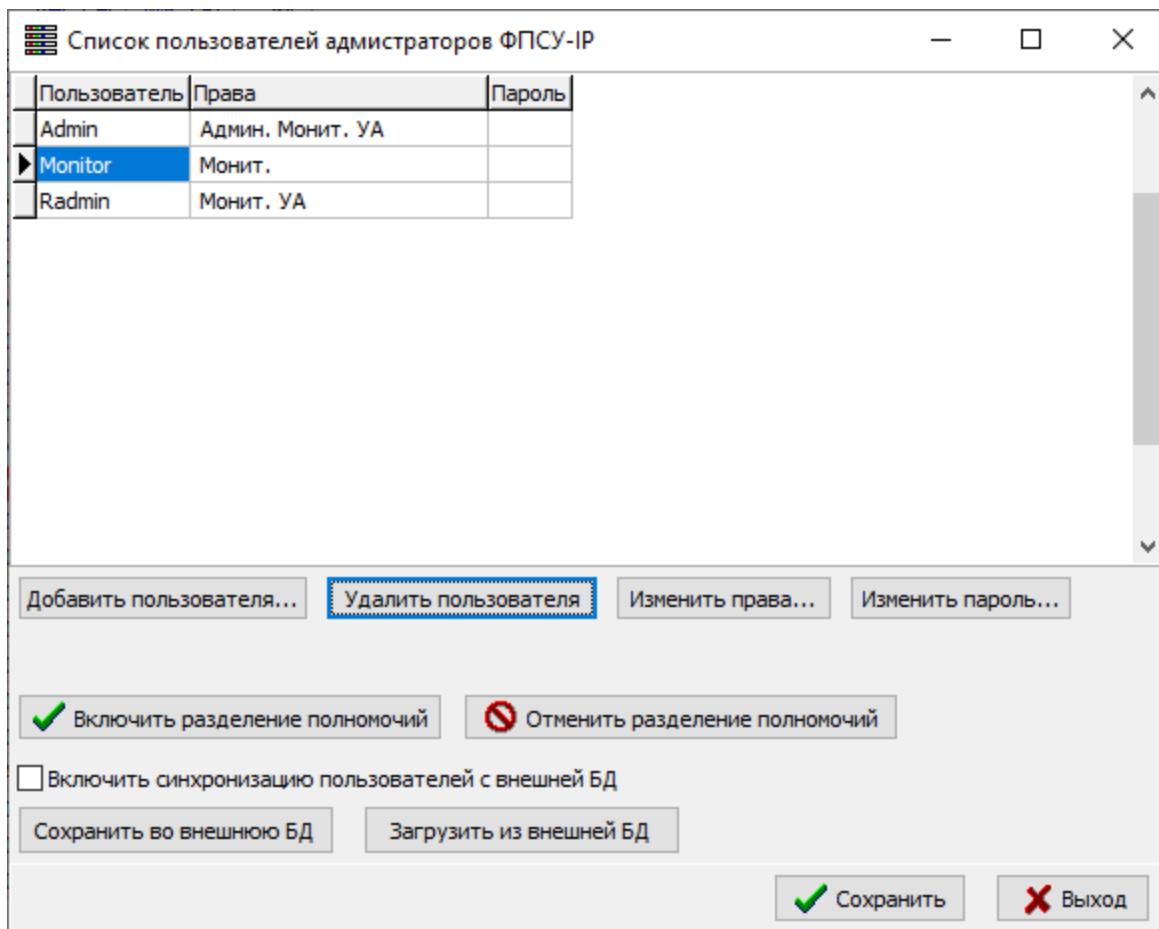


Рисунок 188 - Список пользователей УА ФПСУ-IP

Переход в многопользовательский режим осуществляется при перезапуске УА ФПСУ-IP. В данном режиме текущий пользователь может быть заблокирован и управление УА ФПСУ-IP может быть передано другому пользователю. Для этого в многопользовательском режиме следует выбрать команду главного меню «Параметры» → «Заблокировать/Другой пользователь...». При выполнении команды появится служебное окно с сообщением о блокировке пользователя для ввода данных другого зарегистрированного пользователя. После подтверждения по кнопке «OK» произойдет смена пользователя.

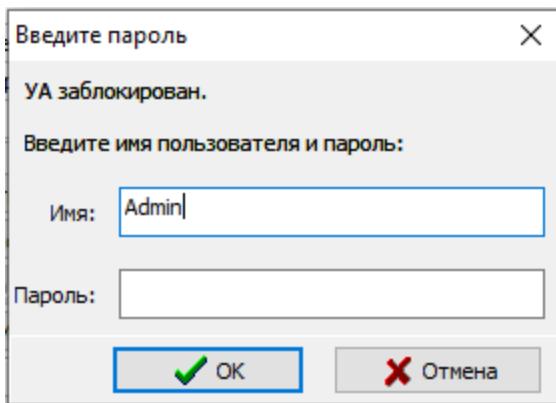


Рисунок 189 - Смена пользователя

«Добавить пользователя» – создание нового пользователя с произвольным именем. В открывшемся окне введите имя пользователя и сохраните по кнопке «OK». Новый пользователь по умолчанию имеет полномочия роли «Мониторинг».

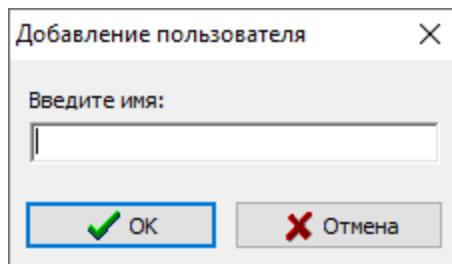


Рисунок 190 - Окно добавления пользователя

«Удалить пользователя» – Выделите пользователя в списке и выполните команду, пользователь будет удален из списка.

«Изменить права» – добавление, изменение или удаление роли полномочий, присвоенных данному пользователю. В открывшемся окне отметьте роль пользователя и сохраните по кнопке «OK».

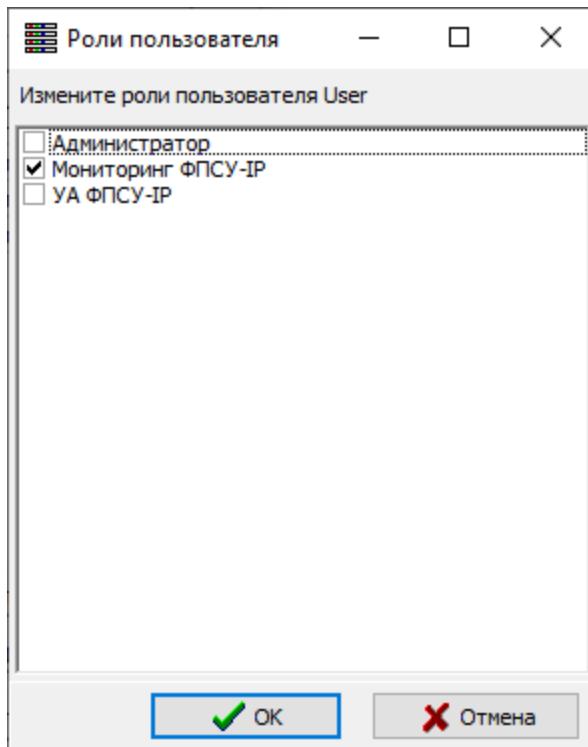


Рисунок 191 - Выбор прав пользователя

«Изменить пароль» – При смене пароля требуется ввести новый пароль и подтвердить его повторным вводом.

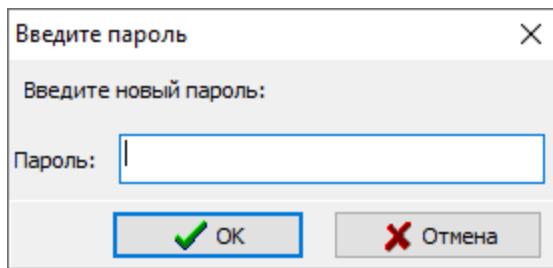


Рисунок 192 - Смена пароля

«Отменить разделение полномочий» – отменить режим разделения полномочий может пользователь с полномочиями роли «Администратор». При выполнении команды отобразится служебное сообщение. Необходимо подтвердить переход в режим одного пользователя. Возврат в режим одного пользователя происходит при перезапуске УА ФПСУ-IP.

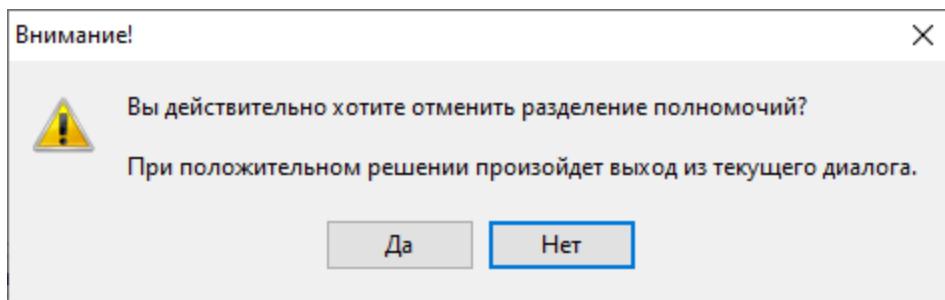


Рисунок 193 - Отмена разграничения пользователей

Флаг «Включить синхронизацию пользователей с внешней БД» – при установлении флага сохранение во внешнюю БД пользователей выполняется автоматически, при изменении во внешней БД, список пользователей автоматически обновится.

«Сохранить во внешнюю БД» – сохранение списка пользователей и локальных изменений во внешнюю БД.

«Загрузить из внешней БД» – загрузка списка пользователей из внешней БД. Может быть использована в случае, если список пользователей не синхронизировался с внешней БД.

13. 3. Режим работы с несколькими администраторами УА ФПСУ-IP

Режим работы УА ФПСУ-IP с несколькими администраторами УА ФПСУ-IP предполагает подключение к компьютеру VPN-Key/UA с учетными данными разных администраторов одновременно.

Для настройки многопользовательского режима следует выбрать команду главного меню «Параметры» → «Настройки» и перейти на вкладку «Работа с ФПСУ-IP».

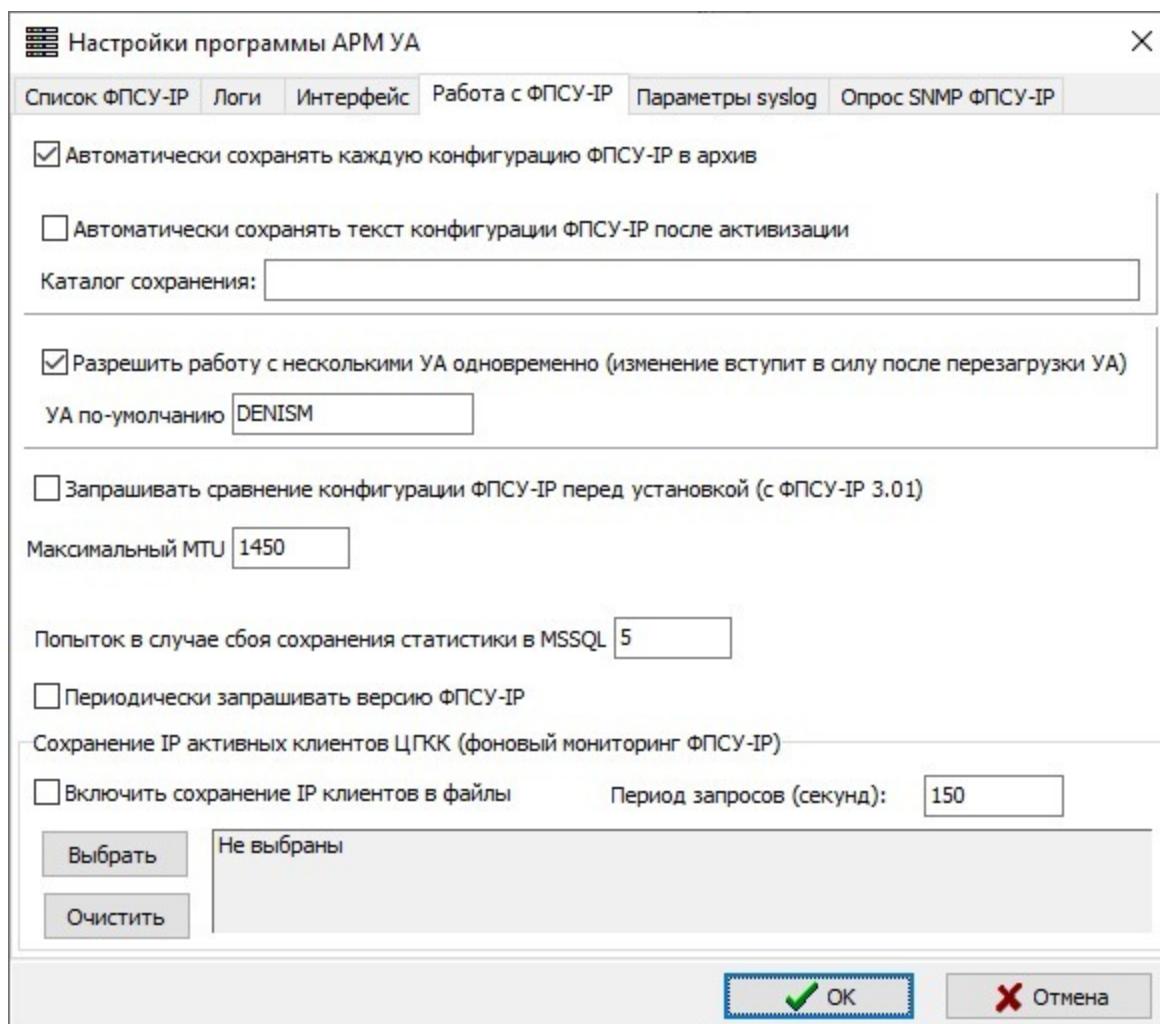


Рисунок 194 - Вкладка «Работа с ФПСУ-IP»

В открывшейся вкладке установить флаг «Разрешить работу с несколькими УА одновременно». При необходимости может быть задан администратор УА по умолчанию.

Файлы лицензий всех подключенных к компьютеру VPN-Key/UA должны быть в наличии в подкаталоге LIC рабочего каталога УА ФПСУ-IP (см. пункт «Первый запуск УА ФПСУ-IP с VPN/Key UA»).

При запуске УА после перезагрузки на экран будет выдано окно со списком подключенных к компьютеру VPN-Key/UA.

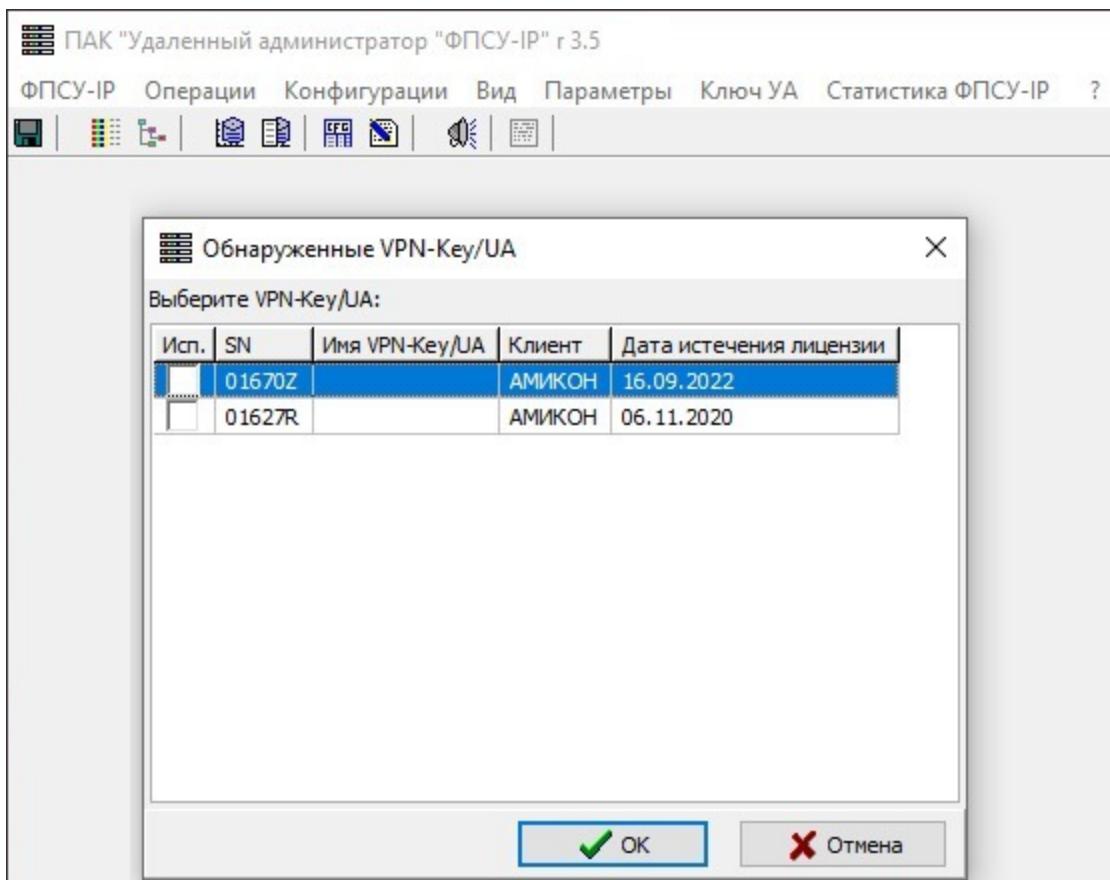


Рисунок 195 - Запуск УА ФПСУ-IP в многопользовательском режиме

В списке выбрать VPN-Key/UA, установив флаг в строке, и нажать кнопку «OK». На экран будет выдано окно для ввода пароля.

Дальнейшая работа с УА ФПСУ-IP осуществляется администратором в обычном режиме. Для переключения между администраторами необходимо перезапустить УА ФПСУ-IP.

13. 4. Изменение параметров работы УА ФПСУ-IP

В процессе работы УА ФПСУ-IP изменение ряда параметров самого УА ФПСУ-IP или учетной записи администратора УА ФПСУ-IP требует специальных действий или решений.

Изменение комментария или переключение рабочих опций может производиться непосредственно в процессе работы. При смене IP-адреса рабочей станции УА ФПСУ-IP требуется перезапуск УА ФПСУ-IP для корректной работы с ФПСУ-IP.

Внимание! Изменение имени администратора УА ФПСУ-IP следует производить в исключительных случаях (например, при возникновении подозрения на утечку информации), поскольку это приведет к изменению ключевых данных, и последующий опрос подконтрольных ФПСУ-IP станет возможным только после повторной регистрации ими администратора УА ФПСУ-IP, имя которого было изменено.

При изменении имени администратора УА ФПСУ-IP фактически происходит создание нового администратора УА ФПСУ-IP. Для этого следует выбрать команду «Ключ УА» → «Создать нового УА». В открывшемся окне требуется указать полностью все данные администратора с новым именем, так же как и при первом запуске УА ФПСУ-IP (см. пункт «Первоначальная настройка УА ФПСУ-IP (с VPN-Key/UA)»).

13. 5. Настройка базы данных статистики УА ФПСУ-IP

При эксплуатации УА ФПСУ-IP все получаемые от ФПСУ-IP сведения по статистике помещаются в базу данных администратора. При новой установке УА ФПСУ-IP в качестве базы по умолчанию используется база данных SQLite. Файл базы данных автоматически создается при запуске УА ФПСУ-IP в подкаталоге STAT его рабочего каталога и называется dbstat.db. В процессе эксплуатации администратор может изменить как используемую базу данных, так и место хранения статистики.

Для вызова окна настройки базы данных сохранения статистики следует выполнить команду главного меню «Статистика ФПСУ-IP» → «Настройка БД статистики ФПСУ-IP».

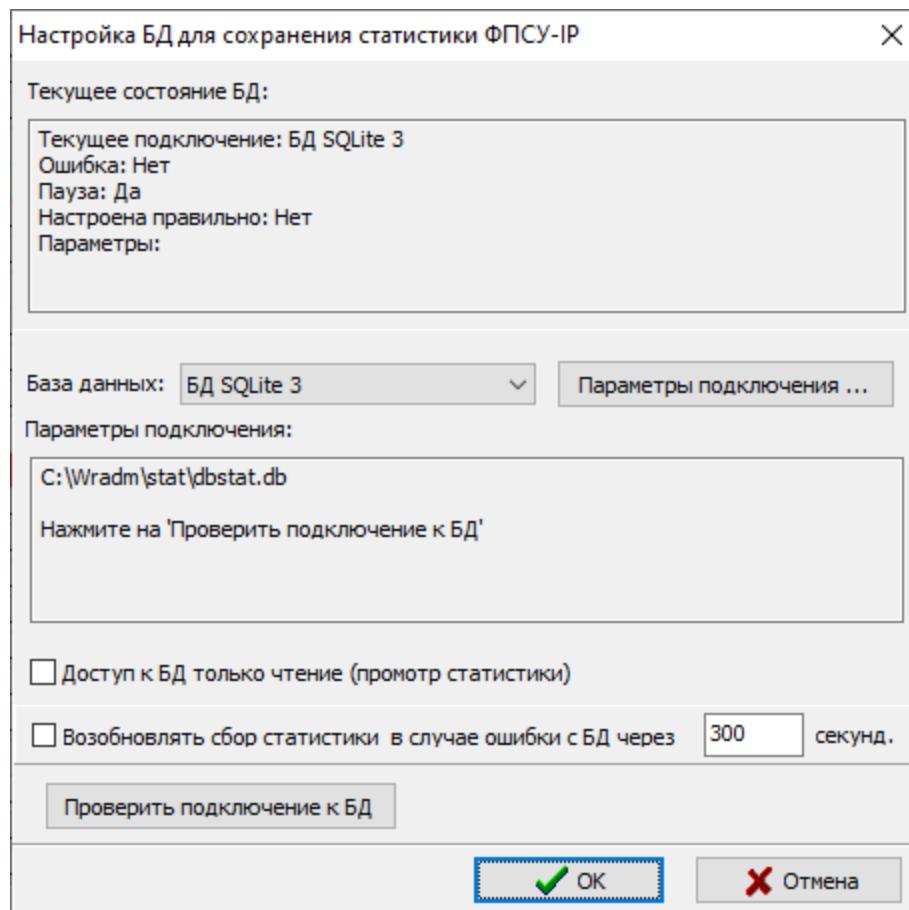


Рисунок 196 - Окно настроек параметров базы данных статистики

В открывшемся окне верхняя часть отображает текущее состояние настроек базы данных, ниже находятся поле выбора типа базы данных, кнопка её настройки «Параметры подключения», и кнопка тестирования корректности настроек «Проверить подключение к БД».

В качестве базы данных могут быть выбраны:

- SQLite, вся база данных статистики (включая определения, таблицы, индексы и данные) хранится в одном указанном администратором файле. Нажав на кнопку «Параметры подключения», администратор может изменить путь и имя файла этой базы данных;
- Microsoft SQL Server. В этом случае администратору следует нажатием на кнопку «Параметры подключения» вызвать окно настроек подключения к базе данных, и указать способ подключения к MS SQL, назначить провайдера доступа к данным. Провайдером по умолчанию является Microsoft OLE DB Provider for SQL Server, «SQLOLEDB.1». Помимо этого, требуется указать адрес сервера Microsoft SQL, базу

данных на сервере, и данные пользователя, имеющего права администратора на работу с указанной базой данных.

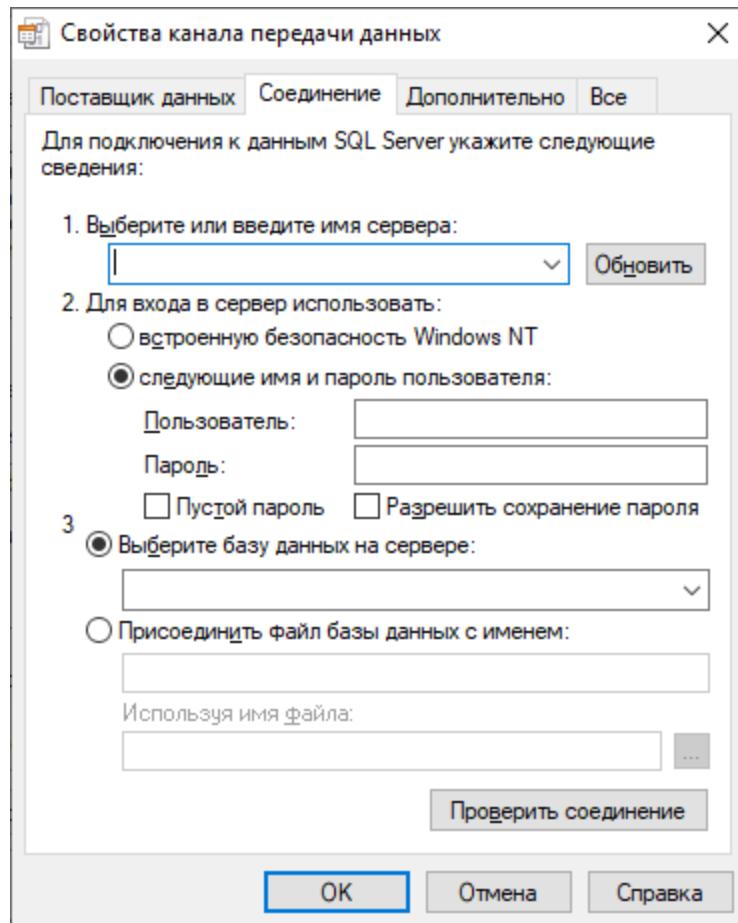


Рисунок 197 - Параметры подключения MS SQL

- PostgreSQL. В параметрах подключения необходимо задать имя хоста с базой данных, IP-адрес хоста с базой данных, номер порта, имя базы данных, данные пользователя, имеющего права администратора на работу с указанной базой данных (см. пункт «Особенности работы со внешними БД PostgreSQL»).

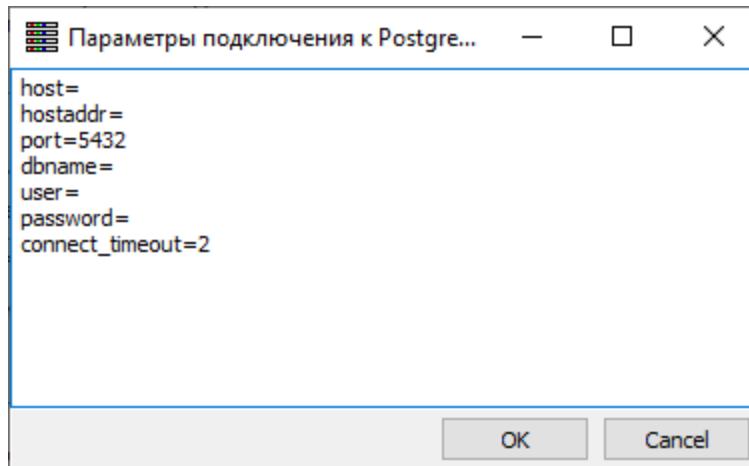


Рисунок 198 - Параметры подключения PostgreSQL

Флаг «Доступ к БД только чтение (просмотр статистики)» - при снятом флаге УА ФПСУ-IP может загружать статистику с ФПСУ-IP в базу данных статистики, в этом случае доступен режим сбора статистики с управляемых ФПСУ-IP (см. пункт «Получение статистической информации»).

Флаг «Возобновить сбор статистики в случае ошибки с БД» - при установке флага требуется указать время, через которое сбор статистики будет возобновлен.

13. 6. Очистка диска

При необходимости предоставляется возможность очистить место в корневом каталоге установки УА ФПСУ-IP. Для выполнения очистки диска необходимо выбрать пункт «? → Очистка диска...» и в открывшемся окне нажать кнопку для выбора действия по очистке диска:

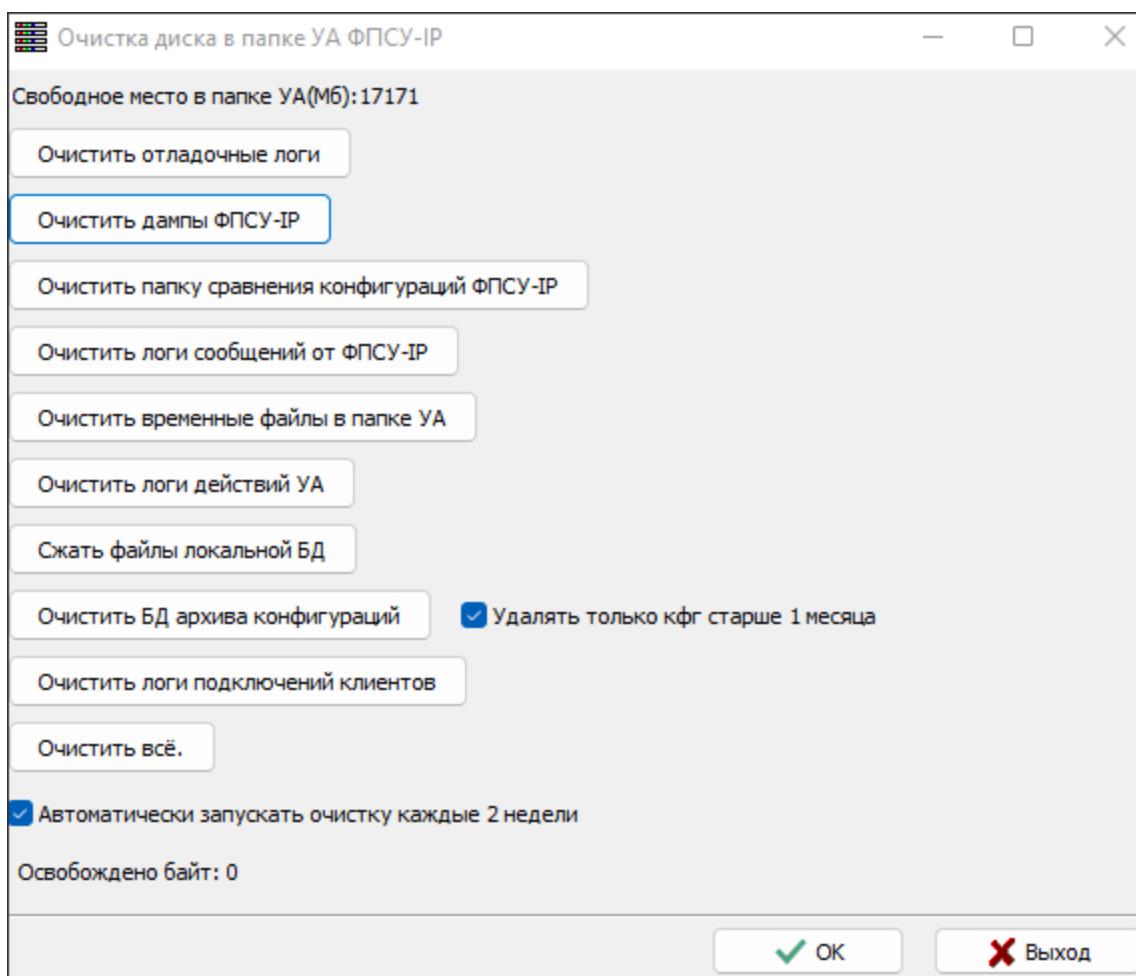


Рисунок 199 - Окно очистки диска

Варианты действий по очистке диска в каталоге УА:

- очистить отладочные логи - удалить историю с информацией, которая помогает выявлять и исправлять ошибки в программном коде УА;
- очистить дампы ФПСУ-IP - удаление созданных при сбоях файлов (см. п. «Вид»);
- очистить папку сравнения конфигураций ФПСУ-IP - см. п. «Просмотр файла сравнения конфигурации»;
- очистить логи сообщений от ФПСУ-IP - удаление истории сообщений о событиях от ФПСУ-IP (см. п. «Настройка журнала событий с ФПСУ-IP на УА ФПСУ-IP»);
- очистить временные файлы в папке УА - удаление временных файлов, которые создаются при запуске задач или программ на компьютере;

- очистить логи действий УА - очистка истории действий УА;
- сжать файлы локальной БД - уменьшить размеры файлов в локальной БД при сохранении исходных данных;
- очистить БД архива конфигураций - очистка предназначенных для хранения всех конфигураций, полученных с управляемых ФПСУ-IP, архивов которые изменялись администратором УА ФПСУ-IP (см. п. «Архивы конфигураций ФПСУ-IP»); можно установить возможность удалять только конфигурации, срок хранения которых более одного месяца, для чего необходимо установить одноименный флаг;
- очистить логи подключений клиентов - очистка истории подключения Клиентов (см. п. «Получение информации о работе клиентов»);
- очистить все - очистка места на диске по всем вышеуказанным параметрам.

Установленный флаг «Автоматически запускать очистку каждые 2 недели» позволяет запускать очистку места в корневом каталоге установки УА ФПСУ-IP каждые две недели в автоматическом режиме.

13. 7. Последние изменения

При необходимости можно просмотреть историю изменений и доработок, произведенных в различных версиях программы. Для просмотра истории изменений необходимо выбрать пункт «? → Последние изменения.». Откроется окно, отображающая список изменений, начиная с последнего:

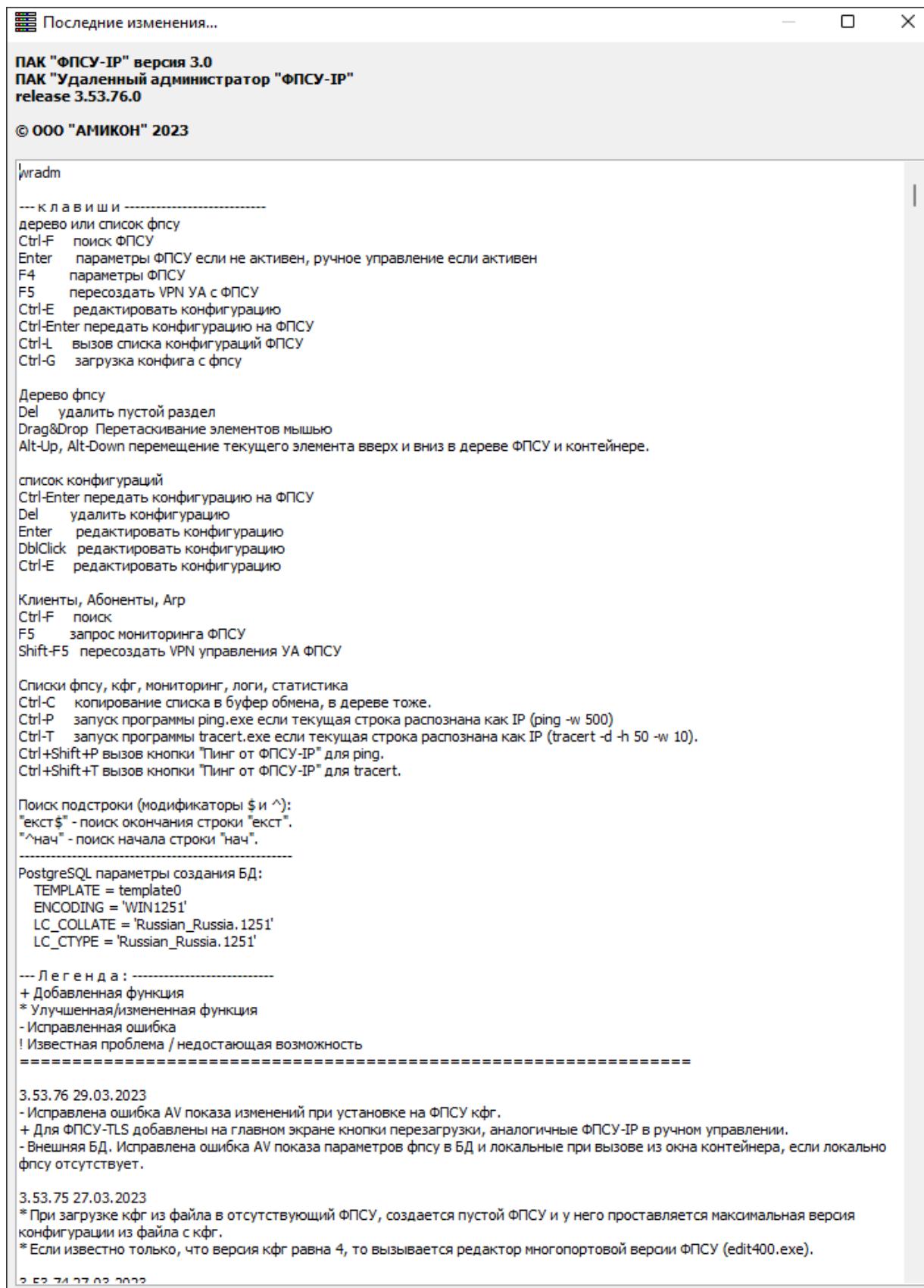


Рисунок 200 - Просмотр последних изменений

14. Окно ручного управления ФПСУ-IP

Помимо рассмотренных функций управления конфигурациями, УА ФПСУ-IP позволяет осуществить такие операции по дистанционному управлению отдельно взятым ФПСУ-IP, как установка и удаление ключевых данных, установка дополнений и изменений программного обеспечения ФПСУ-IP, синхронизация времени ФПСУ-IP с текущим временем УА ФПСУ-IP, перезагрузка ФПСУ-IP и передача управления ФПСУ-IP его партнеру по резервированию, изменять настройки LAN-адаптеров ФПСУ-IP, добавлять на ФПСУ-IP новых администраторов УА ФПСУ-IP.

Для осуществления указанных операций требуется установленное соединение с ФПСУ-IP либо в режиме ручного управления, либо в процессе автоматического опроса.

14. 1. Вход в режим ручного управления

Для непосредственного соединения с ФПСУ-IP (выхода в режим ручного управления) необходимо выбрать в окне списка УА ФПСУ-IP описатель требуемого ФПСУ-IP и нажать клавишу «Enter» или кнопку на панели команд «Ручное управление».

Ручное управление возможно только в том случае, если с выбранным ФПСУ-IP установлено защищенное соединение, в поле «Канал связи с ФПСУ-IP» содержатся сведения о ключевых данных для удаленного управления ФПСУ-IP и сведения о состоянии VPN («Готов») панели информации основного окна:

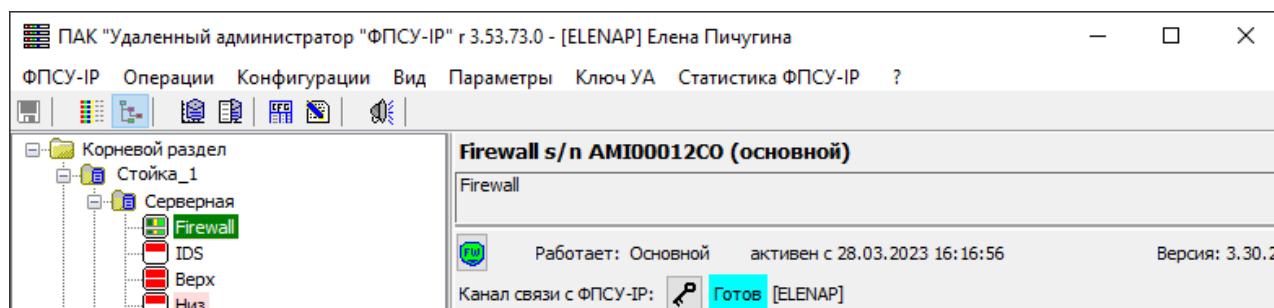


Рисунок 201 - Соединение с ФПСУ-IP установлено

В случае успешной установки защищенного соединения и выполнения команды выхода в режим ручного управления, УА ФПСУ-IP вызывает служебное окно «Ручное управление ФПСУ-IP», которое содержит список операций по дистанционному управлению, доступных в данный момент администратору УА ФПСУ-IP.

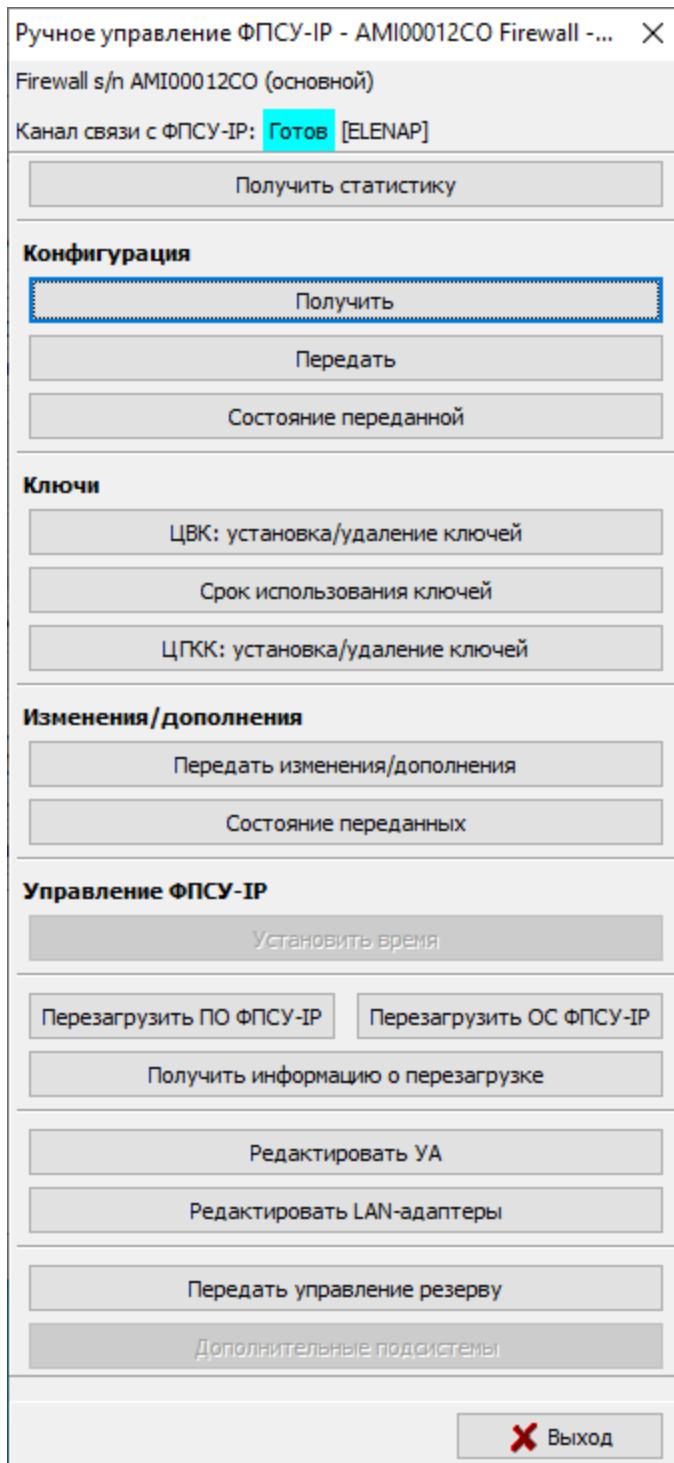


Рисунок 202 - Ручное управление ФПСУ-IP

Кнопка «Получить статистику» позволяет выполнить копирование записей статистики с ФПСУ-IP в базу данных УА ФПСУ-IP (подробнее см. пункт «Получение

статистической информации»).

Операции по работе с конфигурацией в режиме ручного управления, кнопки «Получить» и «Передать», были подробно описаны в пунктах «Загрузка конфигурации ФПСУ-IP на УА ФПСУ-IP» и «Дистанционная установка конфигурации на ФПСУ-IP».

Кнопка «Состояние переданной» раздела «Конфигурация» отображает информацию об изменении и активизации последней переданной на ФПСУ-IP конфигурации.

Кнопка «Передать управление резерву» раздела «Управление ФПСУ-IP» позволяет выполнить немедленную передачу управления работой ФПСУ-IP его партнеру по горячему резервированию. Команда доступна, если локальный администратор ФПСУ-IP выдал соответствующее право данному администратору УА ФПСУ-IP.

14. 2. Добавление удаленных администраторов и изменение прав доступа УА

Все настройки внешней БД осуществляются в одноименном окне, открывающемся по нажатию кнопки «Редактировать УА» в окне «Ручное управление ФПСУ-IP»:

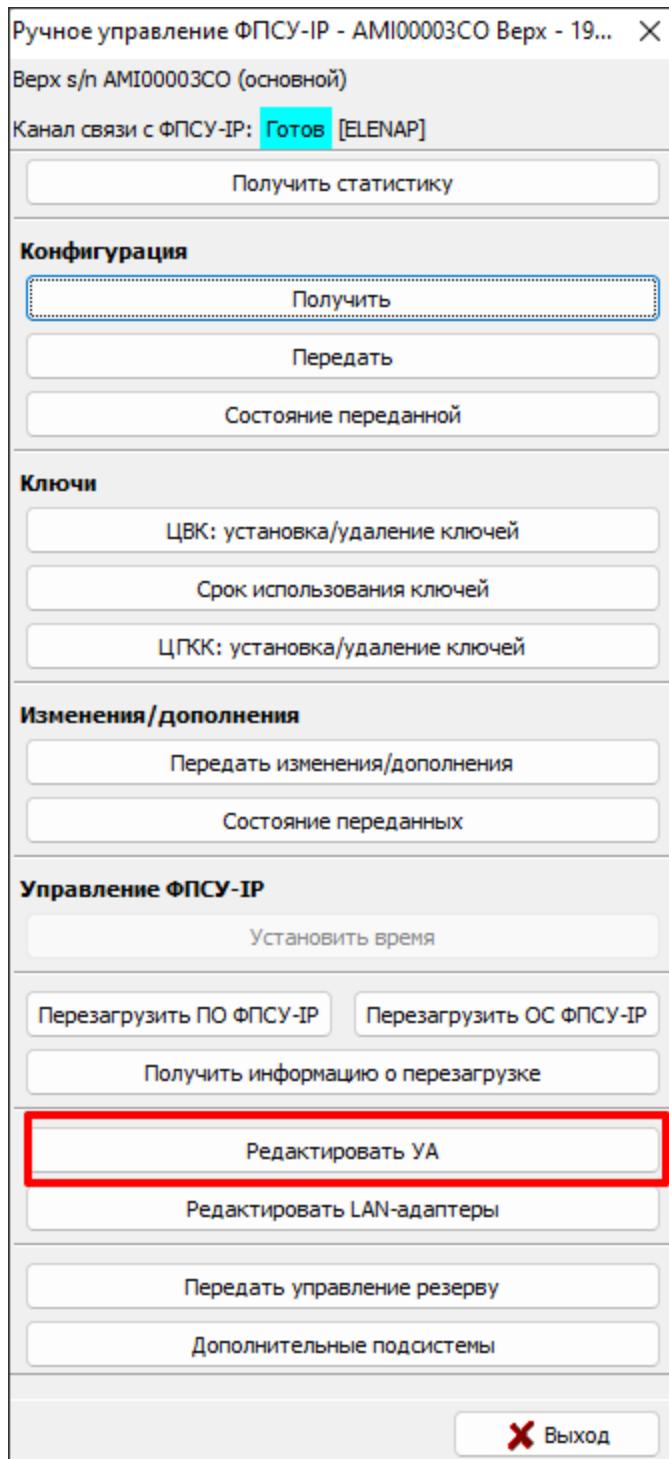


Рисунок 203 – Ручное управление ФПСУ-IP

Для получения тех или иных возможностей администратору внешней БД необходимо создать список профилей пользователей УА ФПСУ-IP, а также наделить их

соответствующими правами.

Профили пользователей УА ФПСУ-IP создаются из либо из файла (с расширением *.dk или *.ke), формируемого удаленным администратором, или при помощи данных из VPN-Key/UA. Изначально существует одна запись, созданная при первом запуске УА ФПСУ-IP. В дальнейшем можно добавить или удалить новую запись путем нажатия одноименных кнопок.

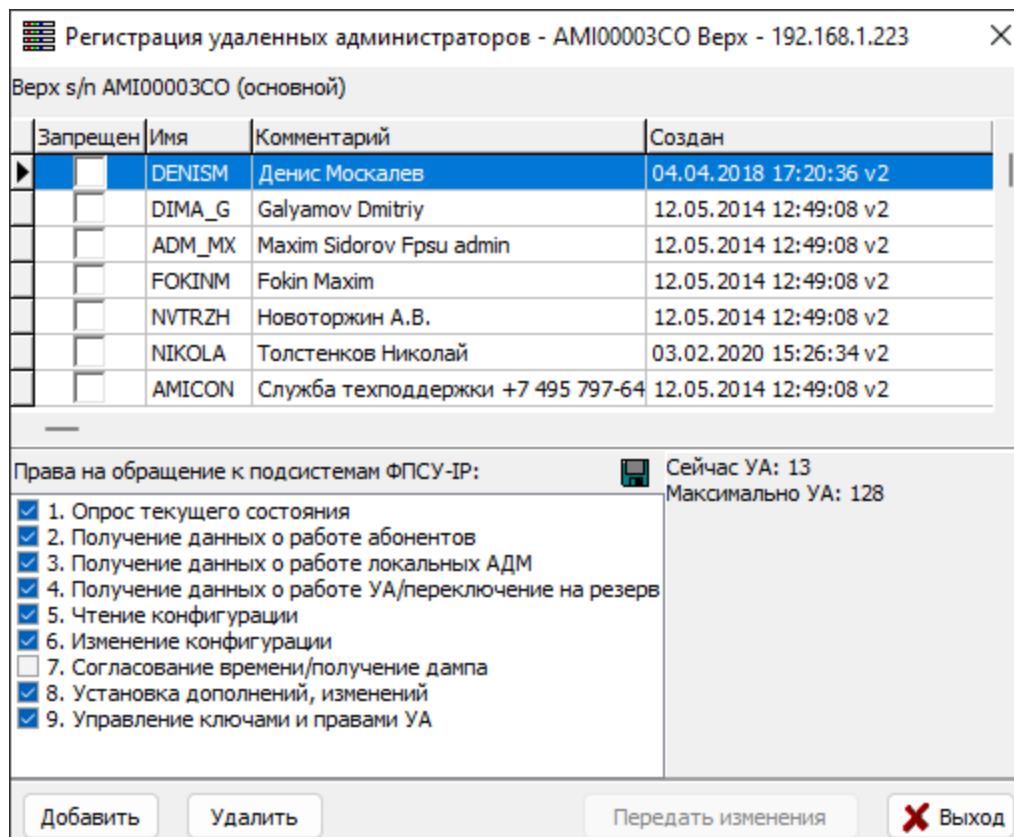


Рисунок 204 – Список пользователей УА ФПСУ-IP с правами доступа для каждого из них

Все изменения, производимые в этом окне, необходимо сохранять путем нажатия на кнопку «Передать изменения».

Доступ удаленным администраторам может быть предоставлен на:

- чтение ФПСУ-IP (ситуация, в которой запись о параметрах ФПСУ-IP забирается на УА ФПСУ-IP, после чего удаленный администратор может просматривать описатель);
- изменение параметров ФПСУ-IP (ситуация, в которой запись о параметрах ФПСУ-

IP забирается на УА ФПСУ-IP, после чего удаленный администратор может просматривать и редактировать описатель);

- назначение контейнера тому или иному удаленному администратору для работы;
- создание контейнера;
- удаление контейнера.

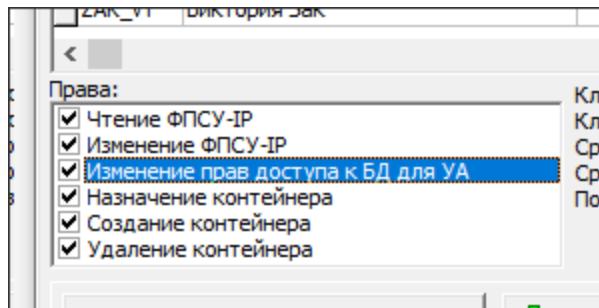


Рисунок 205 – Права доступа к БД для УА

14. 3. Дистанционная установка/удаление ключевых данных

Операции по работе с ключевыми данными доступны администратору УА ФПСУ-IP только в том случае, если при регистрации на ФПСУ-IP ему было предоставлено такое право локальным администратором ФПСУ-IP.

14. 3. 1. Дистанционная установка/удаление ключевых данных ФПСУ-IP

Для установки на ФПСУ-IP или удаления с него парно-выборочных ключей ФПСУ-IP, выработанных ЦВК (подробнее см. документ «Центр выработки ключей. Руководство по применению»), следует запустить режим ручного управления ФПСУ-IP и нажать кнопку «ЦВК: Установка/удаление ключей» в разделе «Ключи».

На экране появится окно, левая половина которого содержит сведения об установленных на ФПСУ-IP ключах парно-выборочной связи, а правая содержит окно для выбора устанавливаемых ключевых данных.

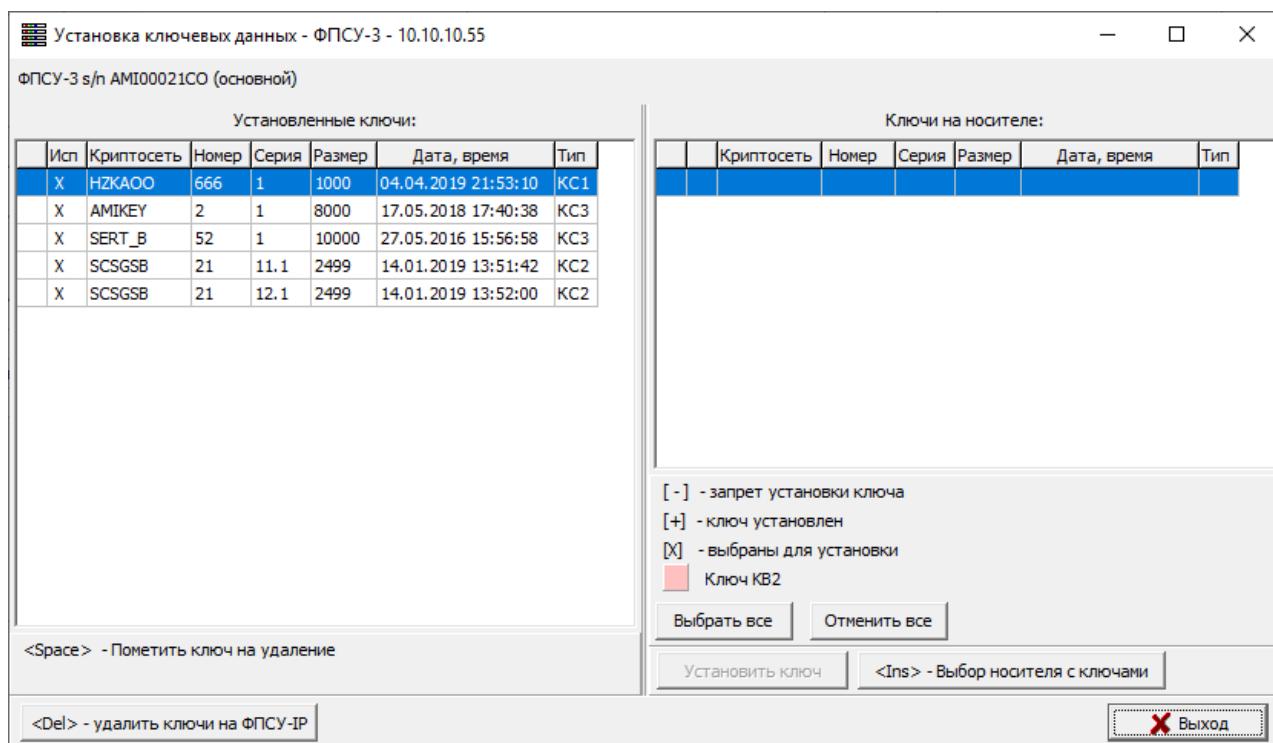


Рисунок 206 - Установка ключевых данных на ФПСУ-IP

Для дальнейшей установки ключевых данных на ФПСУ-IP, администратор УА ФПСУ-IP должен их получить от администратора ЦВК, и, нажав кнопку «<Ins> - Выбор носителя с ключами» и вызвав окно выбора каталога, указать УА ФПСУ-IP путь к ним.

Если в указанном каталоге УА ФПСУ-IP найдет файлы с ключевыми данными, информация по ним будет выведена в поле списка «Ключи на носителе».

Если какие-либо данные нельзя установить на ФПСУ-IP, они будут отмечены знаком «-» в начале строки. Знаком «+» в начале строки отмечаются данные, которые уже установлены на ФПСУ-IP.

Посредством строки выбора в правой части окна следует отметить описатели тех ключевых данных, которые необходимо установить на ФПСУ-IP, после чего нажать «Enter» или кнопку «Установить ключ».

В результате описанной операции отмеченные ключи парно-выборочной связи будут установлены на ФПСУ-IP. Для того чтобы эти данные были применены ФПСУ-IP для реализации защищенных режимов работы, необходимо внести соответствующие изменения в конфигурацию ФПСУ-IP.

Для удаления установленных на ФПСУ-IP ключевых данных следует отметить в левой половине окна их описатели и нажать «Del». Удалить отмеченные данные можно только в том случае, если они не используются в конфигурации ФПСУ-IP. В противном случае, перед удалением, следует отредактировать конфигурацию ФПСУ-IP и отменить выбор использования удаляемых ключей. Используемые в конфигурации ФПСУ-IP ключевые данные отмечены символом «X».

14. 3. 2. Дистанционная установка/удаление ключевых данных ProtoQa и CRISP

Для установки на ФПСУ-IP или удаления с него ключевых данных ProtoQa и CRISP, следует выбрать ФПСУ-IP в основном окне и нажать кнопку «Модули» на панели команд.

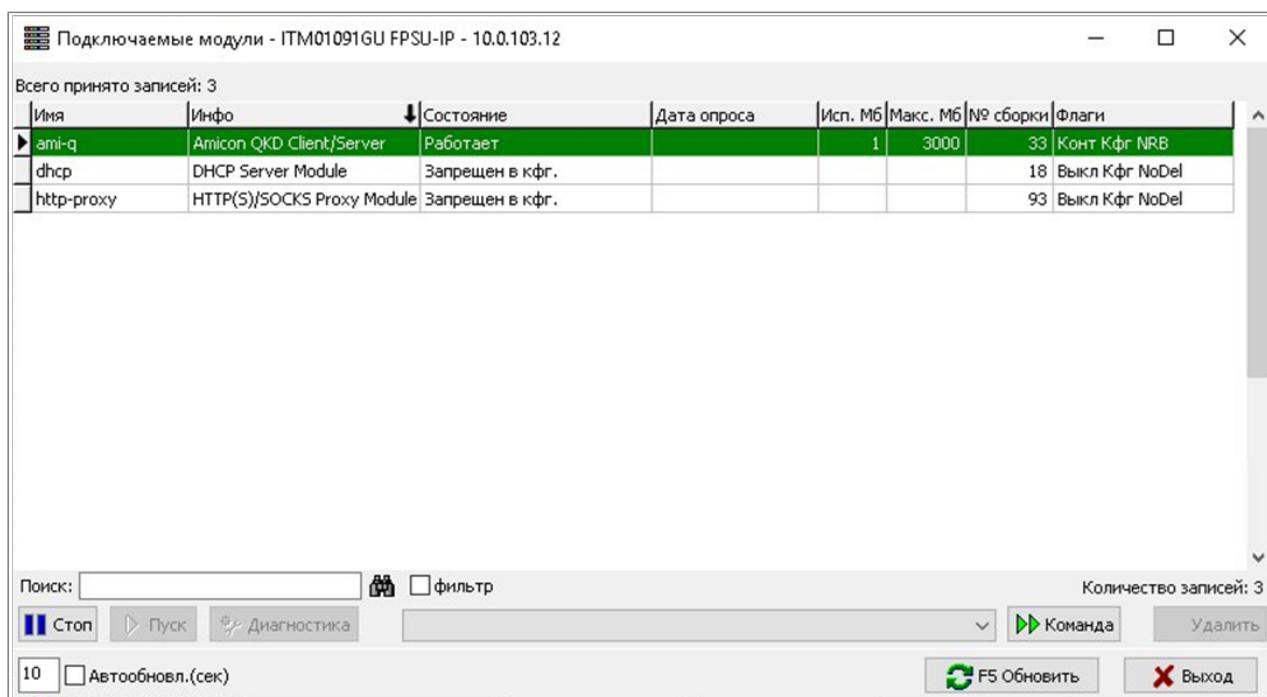


Рисунок 207 - Модули

На экране появится окно, в котором предлагается выбрать нужный модуль, нажать на него правой клавишей мыши и нажать левой клавишей на появившейся кнопке «Управление ключами»:

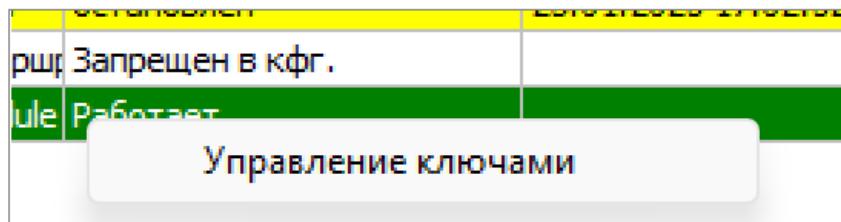


Рисунок 208 - Кнопка «Управление ключами»

Откроется окно «Список ключей»:

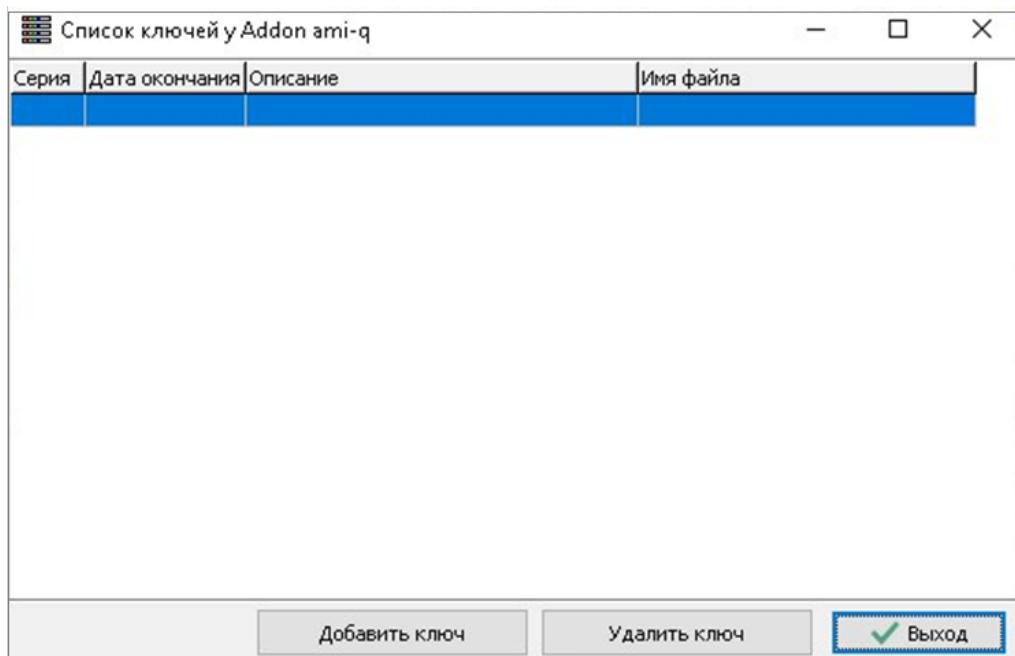


Рисунок 209 - Окно «Список ключей»

Для дальнейшей установки ключевых данных на ФПСУ-IP, администратор УА ФПСУ-IP должен их получить, и, нажав кнопку «Добавить ключ» и вызвав стандартное окно выбора каталога, указать УА ФПСУ-IP путь к ним.

После выбора файла с ключевыми данными, УА предложит ввести пароль:

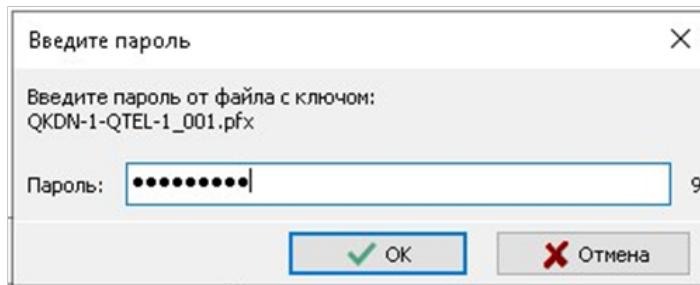
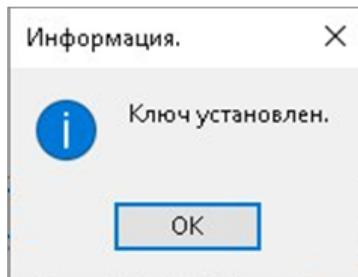


Рисунок 210 - Окно ввода пароля

После ввода пароля и нажатия кнопки «OK» ключевые данные будут установлены на ФПСУ-IP, при этом на экран будет выведено соответствующее информационное окно:

**Рисунок 211 - Сообщение об установке ключевых данных**

Сведения о добавленных ключевых данных отобразятся в окне «Список ключей»:

Список ключей у Addon ami-q			
Серия	Дата окончания	Описание	Ин
1	02.12.2024	QKDN-1-QTEL-1	аг

At the bottom of the window are three buttons: 'Добавить ключ' (Add key), 'Удалить ключ' (Delete key), and 'Выход' (Exit) with a green checkmark icon.

Рисунок 212 - Окно со списком ключей

Для удаления установленных на ФПСУ-IP ключевых данных следует выбрать ключ в списке и нажать кнопку «Удалить ключ».

14. 3. 3. Дистанционная установка/удаление ключевых данных ФПСУ-IP/Клиентов

Для осуществления этой операции на компьютере УА ФПСУ-IP должно быть установлено устройство чтения ТМ-идентификаторов. Чтобы установить или удалить

ключевые данные клиентов с ФПСУ-IP, в режиме ручного управления необходимо выбрать в списке доступных операций команду «ЦГКК: Установка/удаление ключей» в разделе «Ключи»:

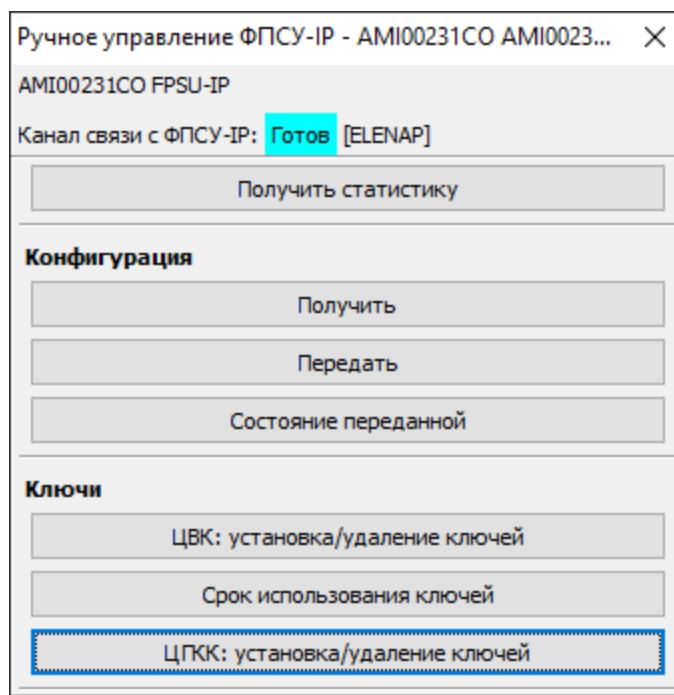


Рисунок 213 - Ручное управление ФПСУ-IP

На экране появится окно, содержащее список установленных на ФПСУ-IP общесистемных ключей Криптосетей Клиентов. Если строка помечена символом «√» – это означает, что ключи зарегистрированы на ФПСУ-IP и используются при описании правил работы клиентов. Такие ключи можно удалить только после того, как удалены описатели всех логических групп, принадлежащих данной Криптосети (подробнее см. документ «Криптотомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4.0.1. Руководство администратора ФПСУ-IP»). Если ключи не используются в конфигурации ФПСУ-IP, их можно удалить с помощью клавиши «Del» или выбора соответствующей кнопки «Удалить текущий ».

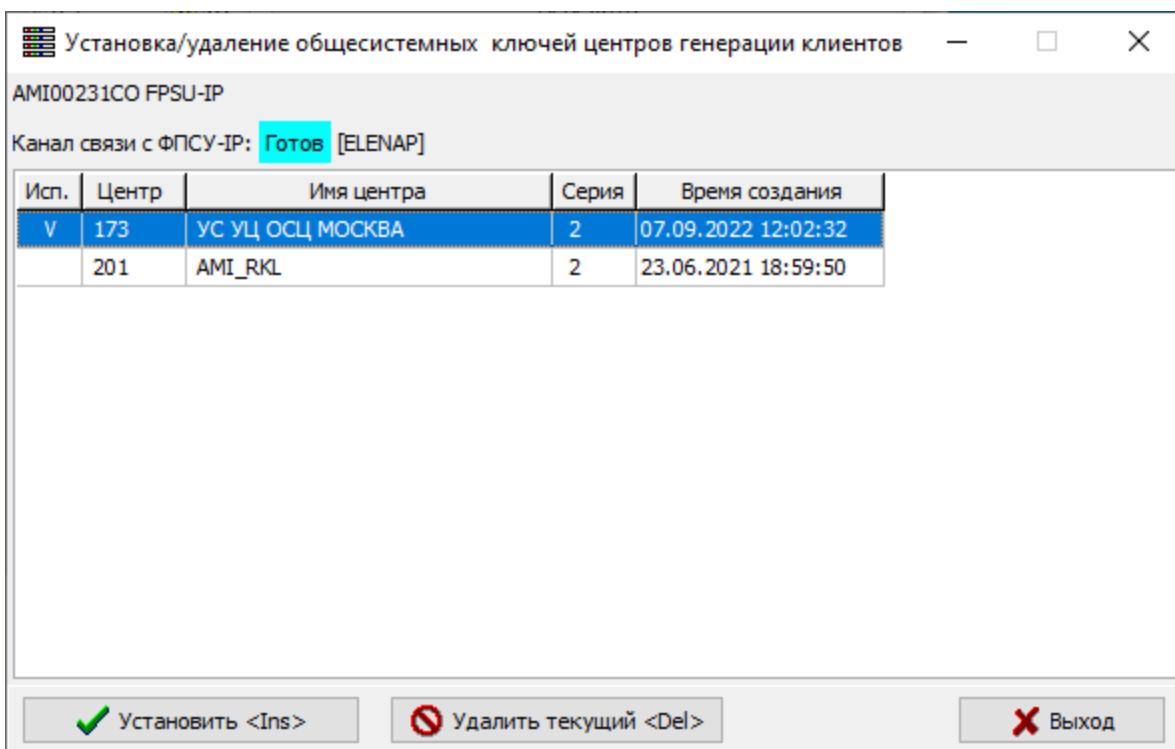


Рисунок 214 - Окно управления ключами ЦГКК

Для установки новых ключей необходимо нажать кнопку «Установить <Ins>» или клавишу «*Ins*», после чего на экран будут последовательно выдаваться приглашения на прижатие к считывающему контактному устройству всех ТМ-идентификаторов, на которых хранятся общесистемные ключи. По мере предъявления ТМ-идентификаторов индикаторы готовности в нижней части экрана будут меняться с «–» на «+». Когда установка будет закончена и появится приглашение убрать ТМ-ключи, следует нажать кнопку «Выход».

14. 4. Синхронизация времени

Синхронизация времени на подконтрольных ФПСУ-IP с текущим временем УА ФПСУ-IP требуется в тех случаях, когда:

- установленные на ФПСУ-IP правила фильтрации пакетов используют зависящие от времени и даты параметры;
- Администратор УА ФПСУ-IP при передаче измененной конфигурации и дополнений/изменений программного обеспечения задает время их активизации на ФПСУ-IP;
- подсистемы регистрации и статистики подконтрольных ФПСУ-IP должны работать

по единому с администратором времени.

УА ФПСУ-IP поддерживает возможность синхронизации времени на подконтрольных ФПСУ-IP с текущим временем УА ФПСУ-IP как в ручном, так и в автоматическом режимах. Для осуществления этих операций администратору УА ФПСУ-IP при регистрации на ФПСУ-IP должно быть локальным администратором ФПСУ-IP предоставлено право на изменение времени.

Для немедленной синхронизации времени ФПСУ-IP с текущим временем УА ФПСУ-IP необходимо выйти в режим ручного управления и выбрать в списке доступных операций окна «Ручное управление ФПСУ-IP» команду «Установить время» в разделе «Управление ФПСУ-IP».

Если не последует сообщений о неполадках, время на ФПСУ-IP будет установлено в соответствии с текущим временем УА ФПСУ-IP, о чем будет выдано служебное сообщение «Время установлено».

Автоматическая синхронизация времени указывается в параметрах взаимодействия ФПСУ-IP с УА ФПСУ-IP (см. пункт «Установка параметров взаимодействия ФПСУ-IP с УА ФПСУ-IP»).

14. 5. Срок использования ключей

Появление всплывающего служебного сообщения «На ФПСУ-IP требуется обновить ключ» означает, что срок действия одного или нескольких ключей на ФПСУ-IP с указанным в сообщении серийным номером закончился, и требуется замена ключевых данных:

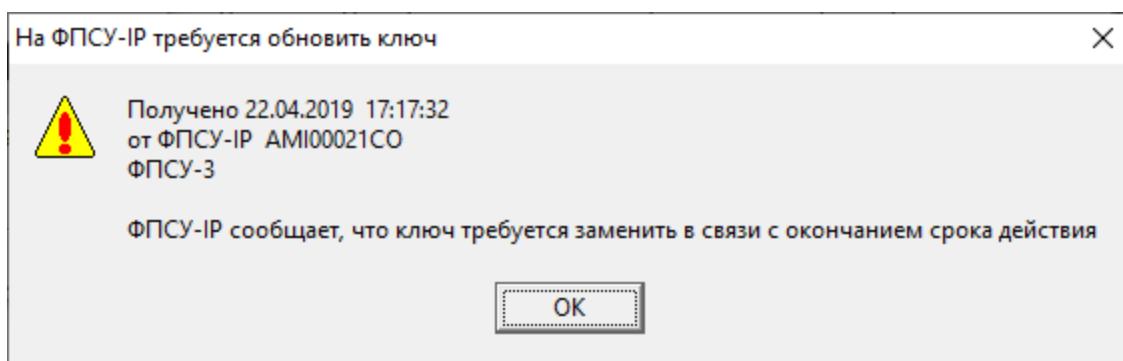


Рисунок 215 - Оповещение

Подробную информацию о том, у каких ключей на ФПСУ-IP закончились сроки действия, можно посмотреть в ручном управлении ФПСУ-IP, по команде «Срок использования ключей»:

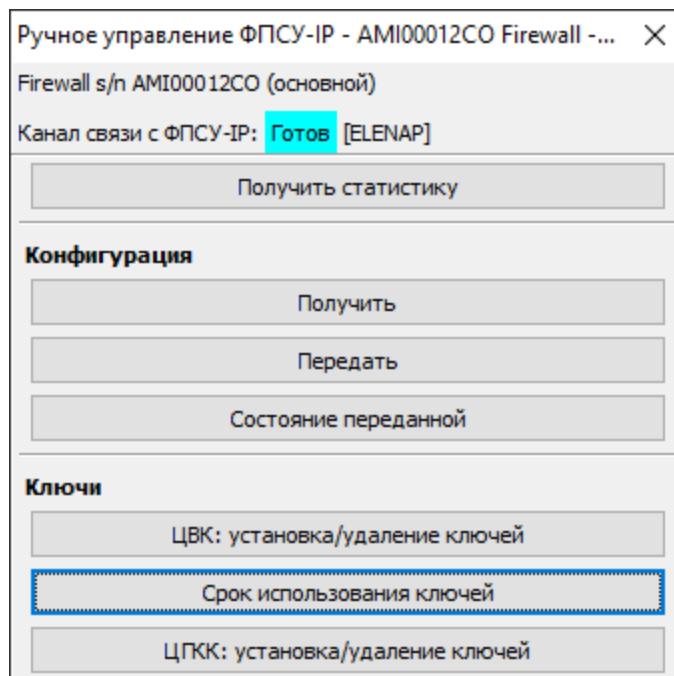


Рисунок 216 - Ручное управление

Будет выдано справочное окно, в котором находится полученный от ФПСУ-IP список установленных на том ключевых данных, где можно посмотреть на список ключей и их состояние.

Для ускорения оценки состояния ключевых данных, строки списка отмечаются разными цветами:

- зеленый – все в порядке, ключевые данные используются в пределах срока действия;
- красный – срок действия ключевых данных закончился, требуется смена;
- белый – на ключевые данные при генерации не были установлены сроки действия.

Установленные ключи и их срок действия на ФПСУ-IP AMI00012CO Firewall						
Сигнал	Тип ключа	Ключ	Дата создания	Дата истечения	Дата сигнализации	Повтор через
	Парно-выборочный ключ	криптосеть:AMID ключ:2 серия:5 тип:KC1				
	Парно-выборочный ключ	криптосеть:AMIK ключ:1 серия:1 тип:KC3	06.12.2022	07.03.2024	06.02.2024	2
	Ключ хранения					
▶	Ключ горячего резервирования	Регистрация на комплексе: 09.09.2020 13:26:48	09.09.2020	08.12.2021	08.11.2021	1

Рисунок 217 - Список и состояние ключевых данных на ФПСУ-IP

14. 6. Установка дополнений и изменений на ФПСУ-IP

К дополнениям и изменениям относятся новые (усовершенствованные) версии программного обеспечения ФПСУ-IP, его отдельные модули и т.д., полученные от поставщика ФПСУ-IP или напрямую от Разработчика (ООО «АМИКОН»).

Операция по дистанционной установке обновления ПО ФПСУ-IP доступна администратору УА ФПСУ-IP только в том случае, если при регистрации на ФПСУ-IP он получил от локального администратора ФПСУ-IP соответствующие права.

В режиме ручного управления выбранным ФПСУ-IP необходимо нажать кнопку «Передать изменения/дополнения» раздела «Изменения/дополнения». В появившемся окне выбора следует указать каталог, в котором находятся файлы обновления ПО ФПСУ-IP.

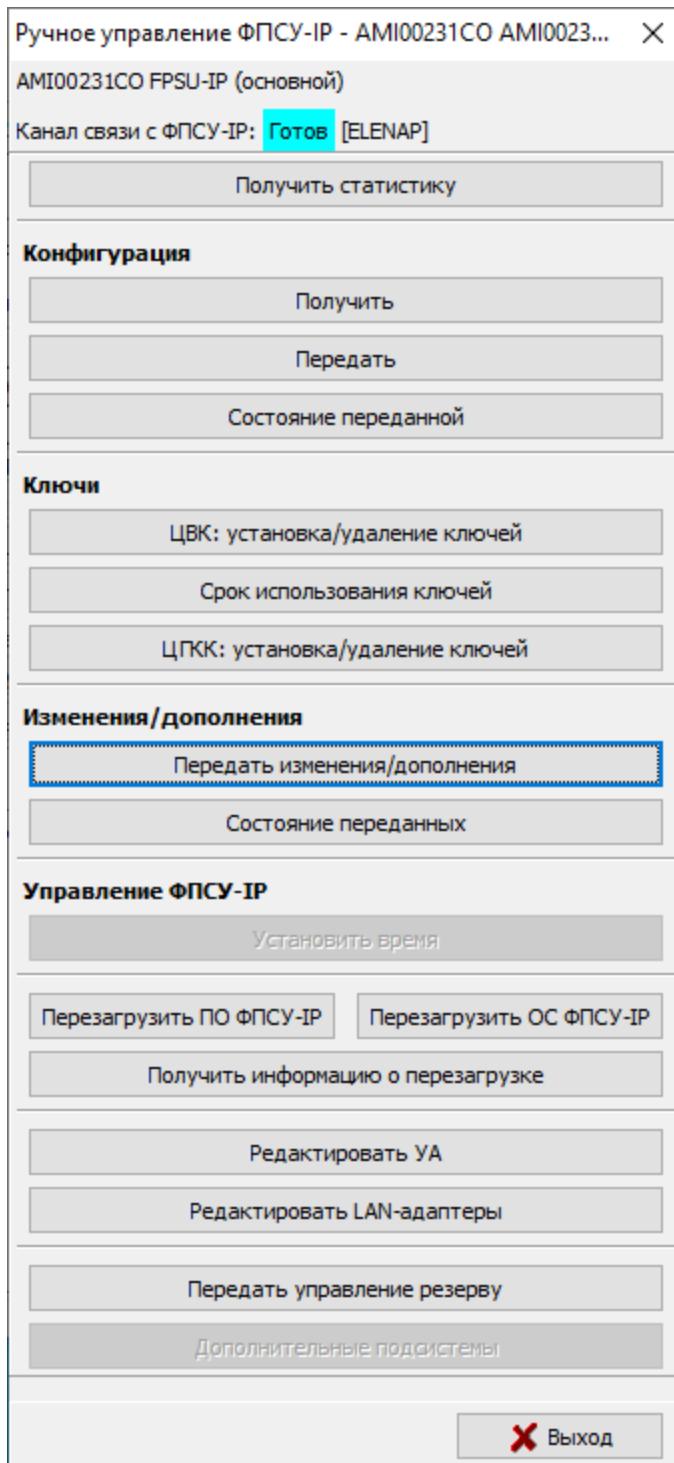


Рисунок 218 - Ручное управление ФПСУ-IP

Если в указанном каталоге содержатся файлы, относящиеся к программному обеспечению ФПСУ-IP (файлы с расширением «.UP0» и «.UPD»), УА ФПСУ-IP выдаст на

экран их список, отображающий дату и время выпуска обновления, и аннотацию к нему:

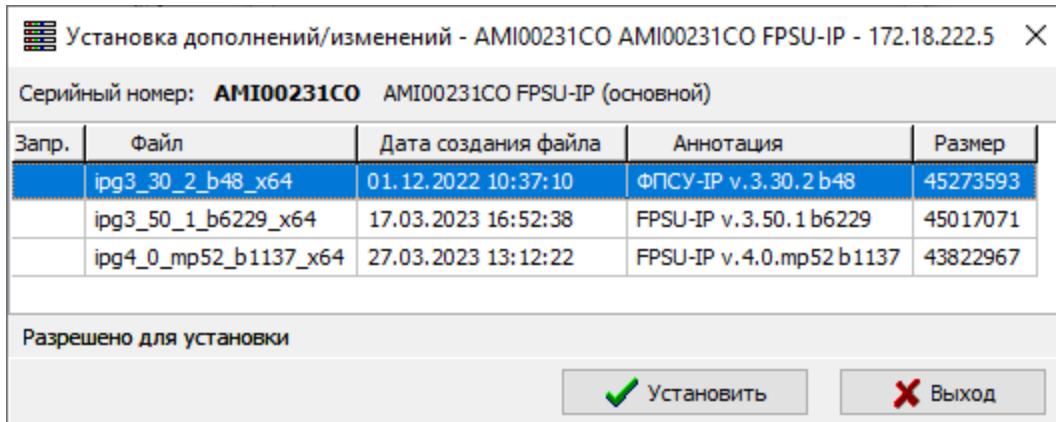


Рисунок 219 - Обнаруженные обновления ПО ФПСУ-IP

Устанавливаемое обновление необходимо отметить курсором и нажать клавишу «Enter» или кнопку «Установить». После ряда служебных сообщений о передаче файла обновления на экране появится запрос времени активации, то есть времени, когда переданное обновление ПО должно вступить в силу на ФПСУ-IP.

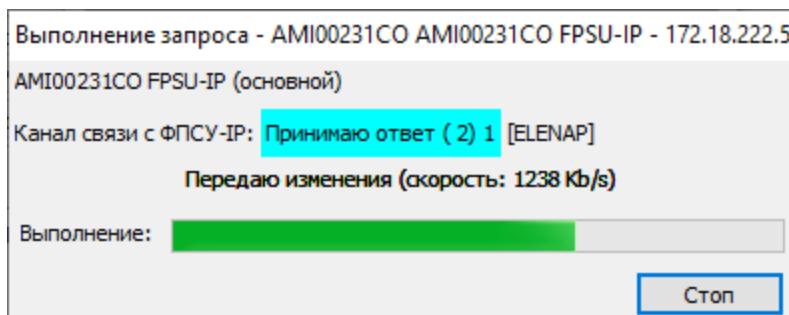


Рисунок 220 - Передача на ФПСУ-IP файла с обновлением ПО

Далее следует ввести дату и время активации и выбрать команду «Установить».

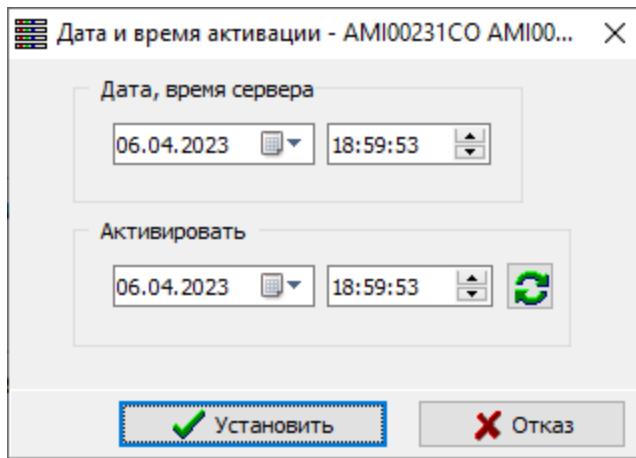


Рисунок 221 - Установка времени активации обновления

При активации переданного обновления будет использована дата и время ФПСУ-IP, а не время на компьютере УА ФПСУ-IP.

Дальнейшее управление пересланным обновлением, выбор и изменение времени активации, отмена установки обновления происходит так же, как и управление переданной конфигурацией (см. пункт «Дистанционная установка конфигурации на ФПСУ-IP»).

Активацию обновления можно отменить по кнопке «Стоп».

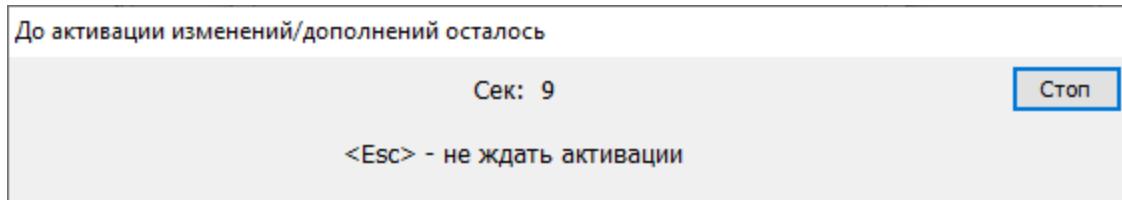


Рисунок 222 - Сообщение об активации обновления

Далее на экран будет выдано сообщение о запросе результата активации обновления на ФПСУ-IP. После установки обновления произойдет перезагрузка ФПСУ-IP и, как следствие, переключение канала связи с ФПСУ-IP в нерабочее состояние.

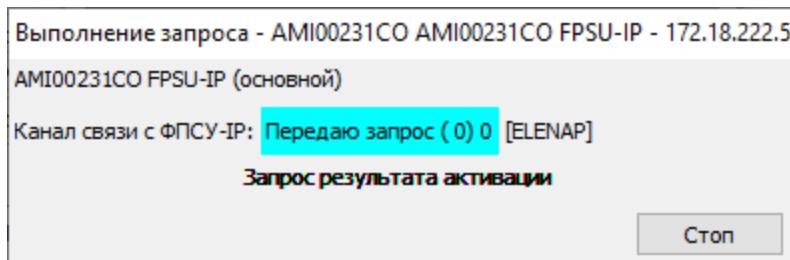


Рисунок 223 - Запрос результата активации с ФПСУ-IP

После восстановления связи УА с ФПСУ-IP будет выдано сообщение о результате активации обновления.

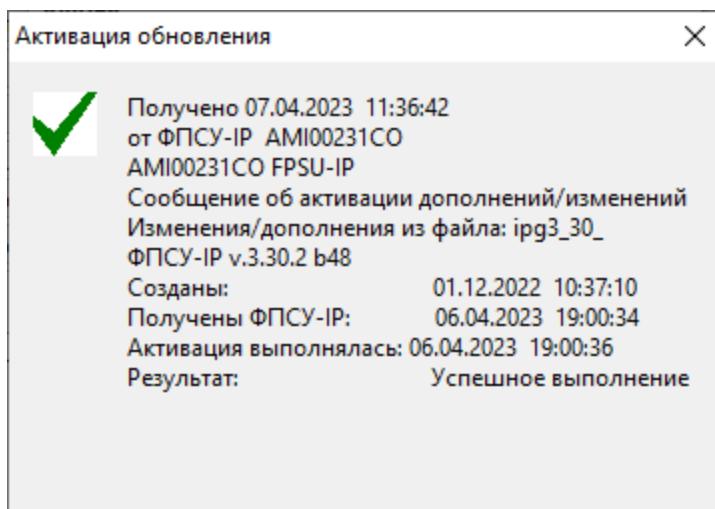


Рисунок 224 - Запрос результата активации с ФПСУ-IP

14. 7. Дистанционная перезагрузка ФПСУ-IP

Для того чтобы перезагрузить ФПСУ-IP, необходимо выйти в режим ручного управления и выбрать в списке доступных операций окна «Ручное управление ФПСУ-IP» раздел «Управление ФПСУ-IP».

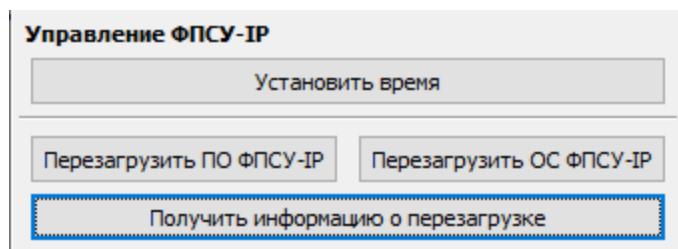


Рисунок 225 - Раздел Управление ФПСУ - IP

Кнопка «Перезагрузить ПО ФПСУ-IP», расположенная в этом разделе, позволяет перезапустить исполняемый файл.

Кнопка «Перезагрузить ОС ФПСУ», так же расположенная в этом разделе, позволяет произвести мягкий рестарт ОС с загрузкой нового ядра и стартом ОС с нуля.

По нажатию кнопки «Получить информацию о перезагрузке» вызывается справочное окно о времени включения и непрерывной работы ФПСУ-IP, и общее количество перезагрузок ФПСУ-IP с указанием времени последней перезагрузки.

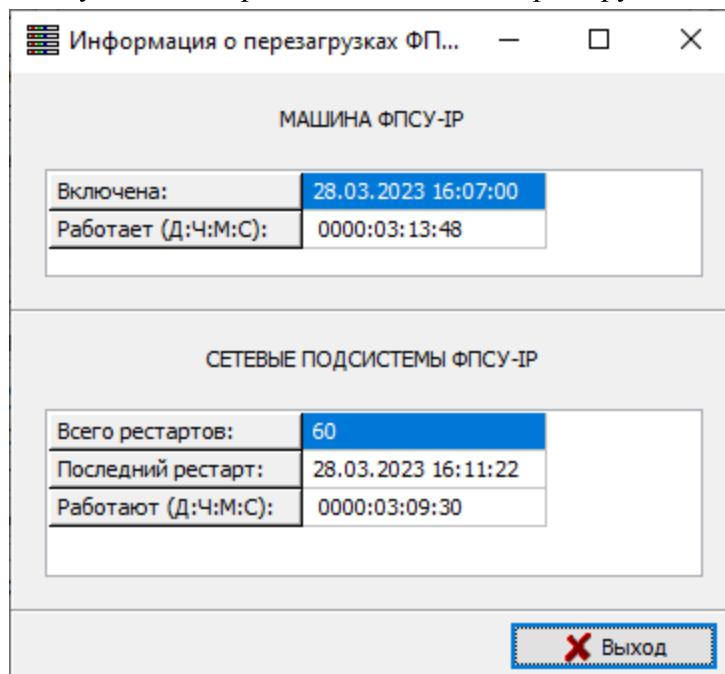


Рисунок 226 - Информация о перезагрузках ФПСУ-IP

14.7.1. Дистанционная перезагрузка ФПСУ-IP

Для того чтобы перезагрузить ФПСУ-IP путем перезапуска исполняемого файла, необходимо выйти в режим ручного управления и выбрать в списке доступных операций окна «Ручное управление ФПСУ-IP» команду «Перезагрузить ПО ФПСУ-IP» раздела Управление ФПСУ-IP. Через несколько секунд после подтверждения выполнения будет произведена перезагрузка ФПСУ-IP.

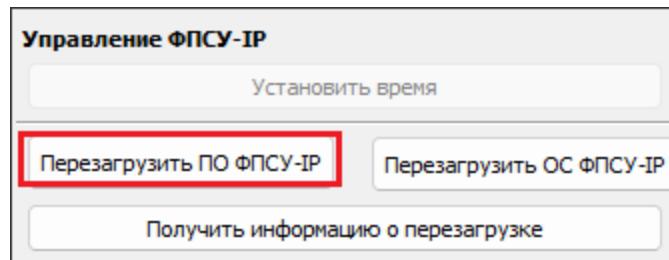


Рисунок 227 - Раздел Управление ФПСУ - IP

14. 7. 2. Дистанционная перезагрузка ОС ФПСУ-IP

Для того чтобы перезагрузить ОС ФПСУ-IP (произвести мягкий рестарт ОС с загрузкой нового ядра и стартом ОС с нуля), необходимо выйти в режим ручного управления и выбрать в списке доступных операций окна «Ручное управление ФПСУ-IP» команду «Перезагрузить ОС ФПСУ-IP» раздела «Управление ФПСУ-IP». Через несколько секунд после подтверждения выполнения будет произведена перезагрузка ОС ФПСУ-IP.

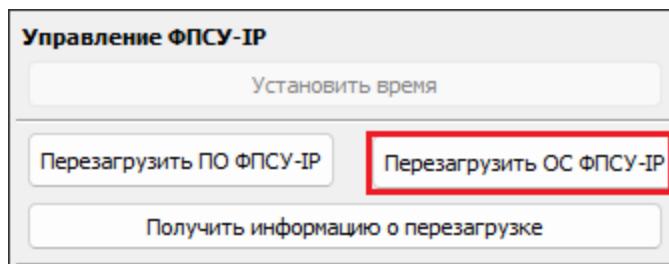


Рисунок 228 - Раздел «Управление ФПСУ - IP»

15. Резервирование и восстановление работы УА ФПСУ-IP

В УА ФПСУ-IP администратору доступны несколько механизмов резервирования, предназначенных для быстрого восстановления рабочего режима УА ФПСУ-IP при отказах операционной системы или аппаратного обеспечения.

Для обеспечения минимальных потерь при сбоях:

1. После установки или изменения параметров администратора следует сохранять ключ УА на внешний носитель и/или надежный файловый сервер, обновлять дубликат VPN-Key/UA (см. пункт Резервирование VPN-Key/UA);
2. После проведения первоначальной настройки УА ФПСУ-IP, а именно:
 - регистрации ФПСУ-IP и установки их рабочих параметров (см. пункт Регистрация ФПСУ-IP в УА ФПСУ-IP);
 - установки параметров мониторинга (см. пункт Настройка пороговых значений по умолчанию);
 - установки параметров автоматической выгрузки статистики в архив (см. пункт Перемещение статистики в архив);сделать резервную копию настроек УА ФПСУ-IP (см. пункт Резервирование рабочих установок УА ФПСУ-IP) и регулярно обновлять её.

15.1. Резервирование рабочих установок УА ФПСУ-IP

После первоначальной настройки УА ФПСУ-IP рекомендуется выполнить резервирование произведённых установок для быстрого восстановления УА ФПСУ-IP по отношению к задачам мониторинга и удаленного управления ФПСУ-IP.

Восстановление утраченного в результате сбоя списка зарегистрированных ФПСУ-IP может быть затянутой во времени задачей, если открытые ключи ФПСУ-IP приходится получать заново.

Для быстрой повторной регистрации ФПСУ-IP на УА ФПСУ-IP возможны следующие способы резервирования:

- создание полной резервной копии УА ФПСУ-IP;
- резервирование описателей отдельных ФПСУ-IP. Резервируются открытые ключи ФПСУ-IP, его IP адрес, параметры мониторинга и снятия статистики, пороговые значения сигнализации событий.

15.1.1. Создание резервной копии УА ФПСУ-IP

Создание резервной копии предназначено для быстрого восстановления работоспособности УА ФПСУ-IP. Резервируются все внесённые настройки и параметры работы УА ФПСУ-IP (кроме собранной статистики), параметры и полученные с ФПСУ-IP конфигурации. Из этого архива можно восстановить сохраненную конфигурацию УА ФПСУ-IP как для рабочей версии УА ФПСУ-IP, так и для новой, только что установленной версии.

Для включения режима автоматического создания резервных копий необходимо:

1. Выбрать команду главного меню УА ФПСУ-IP «Параметры → Резервная копия → Параметры создания резервной копии БД».
2. В открывшемся окне «Параметры резервной копии БД Wradm» следует выбрать каталог для сохранения резервных копий (подкаталоги формата «wrc_ГГММДД_ЧЧММ» УА ФПСУ-IP будет создавать сама), и включить опцию «Создавать резервную копию автоматически при выходе из программы».

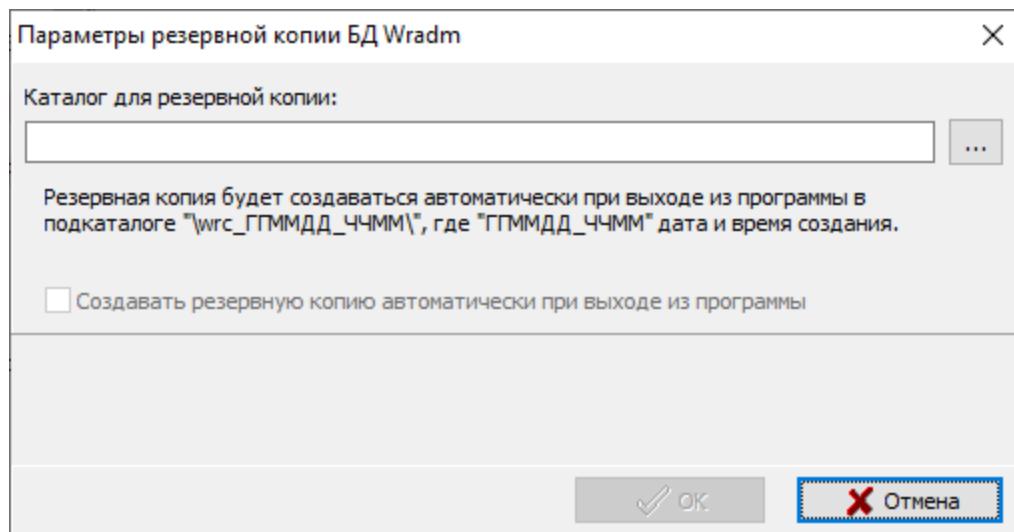


Рисунок 229 -Выбор каталога для сохранения резервной копии

3. Для подтверждения внесённых изменений следует нажать кнопку «OK».

Настройка автоматического создания резервных копий базы данных УА ФПСУ-IP завершена.

При создании резервной копии выбирается каталог, в котором создаются подкаталоги с именем формата wrc_ГГММДД_ЧЧММ, где ГГ — последние две цифры года создания архива, ММ — месяц, ДД — день месяца, ЧЧММ — час и минута создания архива.

Каждая новая резервная копия создаётся в новом каталоге при завершении работы с УА ФПСУ-IP.

Кроме автоматического создания резервной копии при выходе из программы, администратор УА ФПСУ-IP может создать резервную копию вручную.

Для создания отдельной резервной копии УА ФПСУ-IP до выхода из программы, необходимо выполнить команду главного меню УА ФПСУ-IP «Параметры → Резервная копия → Создать резервную копию БД». В появившемся окне следует подтвердить необходимость создания резервной копии УА ФПСУ-IP в указанном каталоге.

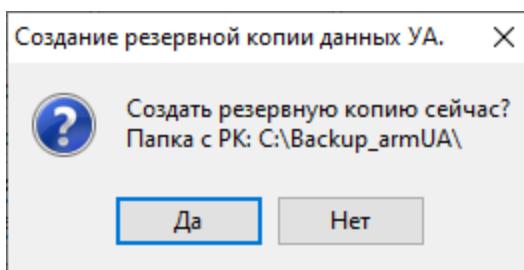


Рисунок 230 - Создание резервной копии по запросу администратора УА ФПСУ-IP

После создания резервной копии будет выдано служебное оповещение об успешном создании резервной копии, либо ошибка с причиной ошибки создания резервной копии.

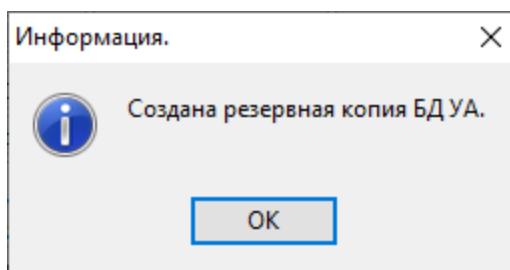


Рисунок 231 - Служебное оповещение

15. 1. 2. Резервирование описателей отдельных ФПСУ-IP

Кроме создания полного архива УА ФПСУ-IP, возможно сохранение описателей отдельных ФПСУ-IP в файлы. В этом случае сохраняются открытые ключи ФПСУ-IP, и настройки их работы с УА ФПСУ-IP (Временные диапазоны работы, типы собираемой статистики, периодичность опросов системы мониторинга и статистики, пороговые значения для отправления оповещений от данного ФПСУ-IP, IP-адрес управляемого ФПСУ-IP).

Для сохранения описателей ФПСУ-IP в файлы следует выделить его в окне списка и выполнить команду главного меню «ФПСУ-IP» → «Выгрузить описатели ФПСУ-IP». Далее необходимо выбрать каталог, в который требуется поместить резервируемые описатели.

Администратор УА ФПСУ-IP может выполнить резервирование нескольких ФПСУ-IP одновременно, отметив строкой выбора в окне списка те ФПСУ-IP, описатели которых требуется резервировать. Выбор более одного описателя в окне списка осуществляется удерживанием нажатыми клавиш «Ctrl» или «Shift» с последующим выбором новых ФПСУ-IP в списке с помощью левой клавиши мыши или кнопок стрелок навигации клавиатуры.

Для восстановления сохраненных таким образом описателей зарегистрированных ФПСУ-IP следует:

- выполнить команду главного меню «ФПСУ-IP» → «Загрузить описатели ФПСУ-IP»;
- в появившемся стандартном окне выбора каталога найти и указать каталог, в котором хранится резервная копия описателя ФПСУ-IP;
- УА ФПСУ-IP восстановит те ФПСУ-IP, чьи описатели были в указанном каталоге. Для тех ФПСУ-IP, которые уже зарегистрированы в УА ФПСУ-IP, будет выдана пометка «Дубль», и данные из резервной копии устанавливаться не будут.

15. 2. Восстановление в случае повторной установки ПО УА ФПСУ-IP

В случае повторной установки программного обеспечения УА ФПСУ-IP для полного восстановления существовавших ранее настроек необходимо:

1. Выполнить установку УА ФПСУ-IP (см. пункт «Панель инструментов»);
2. Запустить УА ФПСУ-IP;
3. Выполнить, если требуется, восстановление VPN-Key/UA с помощью ключа УА или воспользоваться дубликатом USB-ключа для запуска УА ФПСУ-IP (см. подраздел «Создание дубликата VPN-Key/UA»);
4. После запуска УА ФПСУ-IP выполнить команду главного меню «Параметры» → «Резервная Копия» → «Восстановить БД из резервной копии». Откроется стандартное меню выбора каталога, в котором следует указать, где находится резервная копия базы данных УА ФПСУ-IP.
5. Появится служебное сообщение, в котором требуется подтвердить запрос администратора на восстановление базы данных УА ФПСУ-IP из резервной копии. Нажать кнопку «Да» для продолжения.

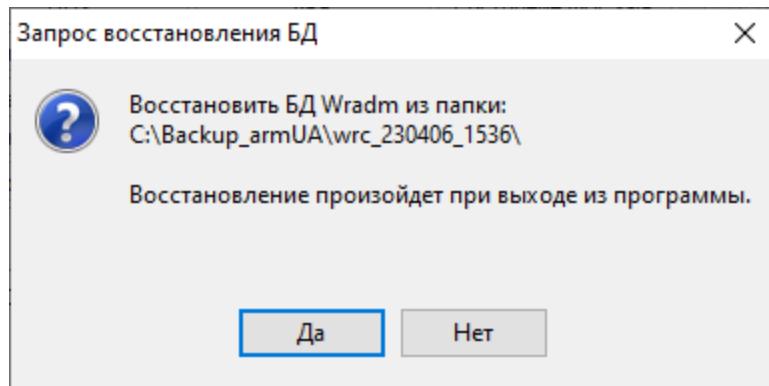


Рисунок 232 - Подтверждение восстановления настроек УА ФПСУ-IP из резервной копии

6. Появится служебное окно с предупреждением о завершении работы УА ФПСУ-IP перед выполнением восстановления, в котором необходимо нажать кнопку «OK» для продолжения.
7. Будет запущена процедура восстановления базы данных из резервной копии и выполнен выход из программы УА ФПСУ-IP. После выхода из программы необходимо запустить её самостоятельно.

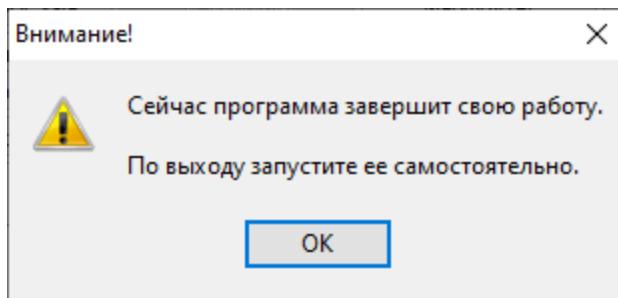


Рисунок 233 - Успешное восстановление настроек из резервной копии

Восстановление базы данных УА ФПСУ-IP из резервной копии завершено. Поскольку конфигурации управляемых ФПСУ-IP не сохраняются в резервной копии УА ФПСУ-IP, для дальнейшей работы с ними следует загрузить конфигурации с ФПСУ-IP напрямую или из заранее сделанной резервной копии конфигураций (см. пункт «Загрузка конфигурации ФПСУ-IP на УА ФПСУ-IP»).

16. Управление и мониторинг ФПСУ-IP

Одной из основных функций УА ФПСУ-IP является мониторинг, который заключается в проведении опроса состояния ФПСУ-IP и отображении полученной информации одновременно по событиям на всех ФПСУ-IP на экран монитора в виде служебных оповещений, записей окна состояния, изменения строки состояния. УА ФПСУ-IP производит анализ полученных от ФПСУ-IP данных с целью выдачи администратору графической и звуковой сигнализации на происходящие на ФПСУ-IP события.

Мониторинг ФПСУ-IP осуществляется как в автоматическом режиме с задаваемыми частотами опроса, так и в режиме непосредственного соединения с ФПСУ-IP по команде администратора УА ФПСУ-IP. Право на опрос состояния ФПСУ-IP предоставляется всем зарегистрированным на нём администраторам УА ФПСУ-IP.

Ряд событий на подконтрольных ФПСУ-IP, требующих графической и/или звуковой сигнализации по получении данных мониторинга, задается администратором (выбирается из предлагаемого списка). Для каждого типа событий могут быть установлены отдельные виды звуковой сигнализации.

16. 1. Контроль состояния ФПСУ-IP

Для оперативного контроля состояния ФПСУ-IP, УА ФПСУ-IP предоставляет администратору список команд-запросов, которые могут быть посланы ФПСУ-IP после установления VPN-туннеля. Запросы отправляются нажатием соответствующей кнопки панели мониторинга:

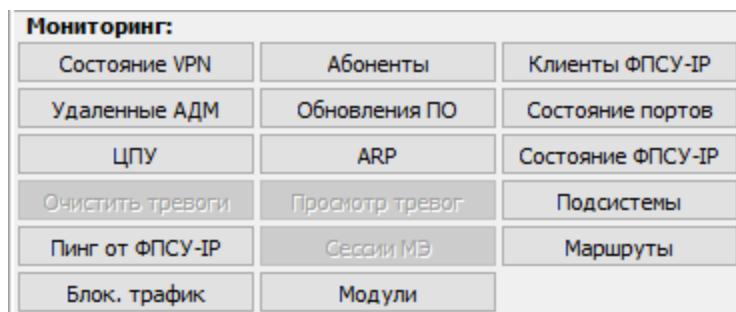


Рисунок 234 - Команды мониторинга

16. 1. 1. Опрос состояния VPN-туннелей с другими ФПСУ-IP

Для непосредственного опроса выбранного в окне списка ФПСУ-IP с целью получения информации о текущем состоянии его VPN-туннелей с другими ФПСУ-IP

необходимо нажать кнопку «Состояние VPN».

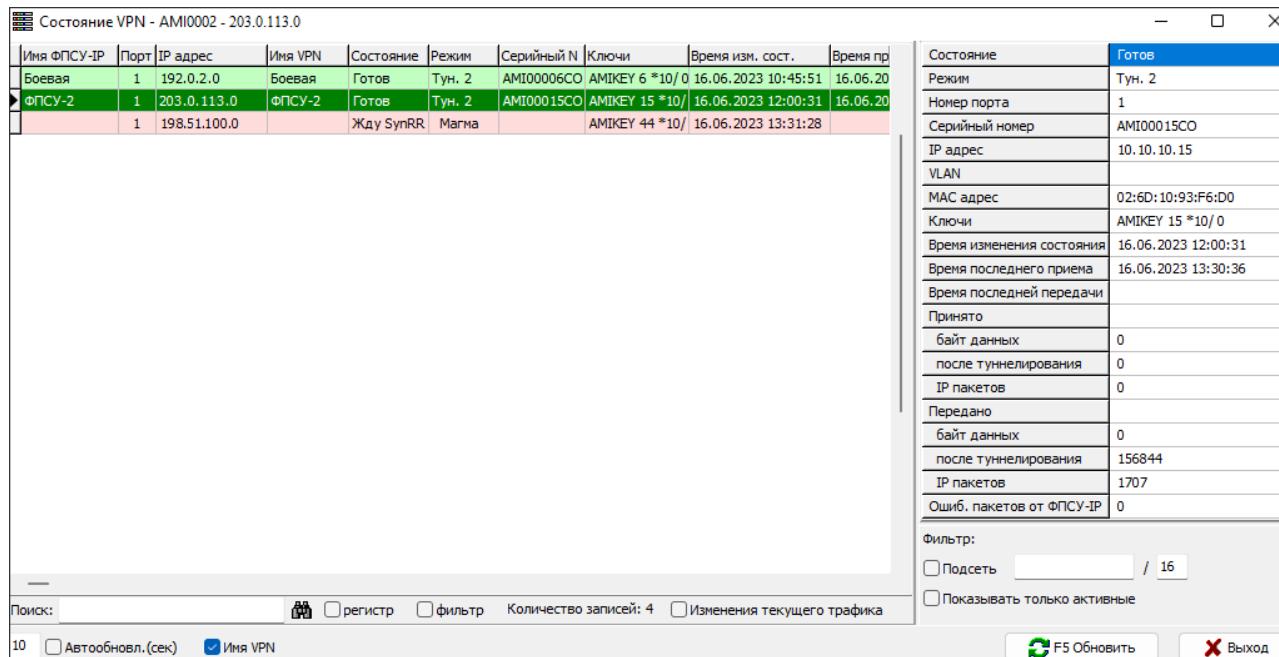


Рисунок 235 - Состояние VPN-туннелей

По активизации этой команды открывается информационное окно, содержащее список ФПСУ-IP, работающих в текущий момент времени с выбранным ФПСУ-IP. Для каждого ФПСУ-IP из списка отображаются:

- имя ФПСУ-IP;
- порт ФПСУ-IP, со стороны которого находится ФПСУ-IP из списка;
- IP-адрес;
- текущее состояние туннеля, при этом в данной графе может отображаться следующая информация:
 - Готов - туннель работоспособен;
 - Не готов прием - прием данных от другого ФПСУ-IP невозможен;
 - Не готова передача - передача данных другому ФПСУ-IP невозможна;
 - Не готовы прием/передача - прием и передача данных другому ФПСУ-IP невозможна;
 - Жду ARP - прием и передача данных абонентов невозможны, маршрут до удаленного ФПСУ-IP неизвестен (в частности, неизвестен MAC-адрес сетевого устройства, которому требуется передать фрейм для дальнейшей

маршрутизации);

- Жду SynRR - прием и передача данных абонентов невозможны, ожидается разрешение синхронизации от удаленного ФПСУ-IP. Отображается в случаях ошибок с парно-выборочными ключами на текущем или удаленном ФПСУ-IP (например, не согласованность конфигураций ФПСУ-IP в используемых номерах ключевых данных, серии или криптосети; ошибки чтения файла с ключевыми данными). Также отображается когда по указанному IP-адресу находится не ФПСУ-IP, а другое устройство, с которым невозможно установить VPN-туннель;
 - Жду SynOK - прием и передача данных абонентов невозможна, ожидается синхронизация с удаленным ФПСУ-IP;
 - Ожидание подтверждения сеансового ключа - ожидается подтверждение на выданный удаленному ФПСУ-IP сеансовый открытый ключ.
- режим передачи данных абонентов через VPN-туннель, при этом в данной графе может отображаться следующая информация:

Пометка	Дополнение	Означает
Тун.		установленный туннель с шифрованием на Магма МГМ (например, «Тун. 2 Магма МГМ»);
Сжат.		сжатие данных;
Версия криптоалгоритма, по которому осуществляется шифрование:		
	""	0
	П	1
	2	2
	3	3
U		признак взаимодействия ФПСУ-IP по протоколу UDP;

Магма, Магма МГМ		вид шифра, устанавливающий работу ФПСУ-IP с ФПСУ-IP в режиме шифрования по заданному алгоритму;
QKD		признак установленного туннеля на квантовых ключах (например, «Тун. 2 QKD Магма МГМ»);
HYB		признак установленного гибридного туннеля в обычном режиме;
HYBQKD		признак установленного гибридного туннеля на квантовых ключах.

Следует иметь в виду, что туннель без шифрования будет подзначен сиреневым цветом.

- серийный номер ФПСУ-IP, с которым установлено соединение;
- ключи, используемые для установления соединения;
- время последнего изменения состояния туннеля, время последнего приема и передачи данных между ФПСУ;
- количество переданных байт и IP-пакетов;
- количество ошибок при передаче пакета.

Возможен фильтр списка отображаемых «партнёров» ФПСУ-IP по диапазону IP-адресов и указанной маске, а также автоматическое обновление отображаемого списка через указанное количество секунд (по умолчанию — 10).

«F5 Обновить» – нажатие кнопки осуществляет внеочередной запрос УА ФПСУ-IP к ФПСУ-IP, обновляя полученную от него информацию мониторинга. Кнопка доступна только при установленном соединении с ФПСУ-IP.

Установка флага «Имя VPN» добавляет для отображения колонку с именами VPN. .

16. 1. 2. Получение информации о работе абонентов

Для получения информации о состоянии работы абонентов и клиентов ФПСУ-IP следует нажать кнопку «Абоненты» панели команд. Когда соединение будет установлено, на экран будет выдано окно, содержащее список пар работающих абонентов (описываемых IP-адресами) и подробную информацию о состоянии работы пары абонентов из текущей

строки.

Если в списке пар абонентов в колонке «Ош.» (Ошибка) стоит знак «+», это означает, что в работе абонентов есть неполадки. Более подробная информация о работе выбранной пары абонентов находится в нижней части информационного окна. Информация о последнем отказе содержится в нижней области окна, в поле «Ошибка».

Для каждого абонента из пары, отмеченной строкой выбора, указываются порт подконтрольного ФПСУ-IP, со стороны которого работает абонент, IP-адрес ФПСУ-IP, через который абонент работает с ФПСУ-IP, а также информация о передаваемых данных.

Ош.	Акт.	Абонент 1	Абонент 2	Порт 1	Порт 2	Данные аб. 1	Данные аб. 2	Пакет
► 1	+	77.234.200.226	192.168.20.49	1	2	0	166,1041 М	
2	+	104.16.249.249	77.108.111.101	1	2	10,837 М	0	
2	+	142.250.74.174	77.108.111.101	1	2	32,1006 М	0	
1	+	77.234.200.226	192.168.1.106	1	2	0	2,169 М	
1	+	193.47.33.135	192.168.1.99	1	2	0	73,912 М	
0	+	87.245.145.6	192.168.0.1	1	2	0	1,006 М	
2	+	87.245.145.6	77.108.111.101	1	2	7,384 М	0	
1	+	104.16.249.249	192.168.20.49	1	2	0	1,115 М	
0	+	78.25.76.162	192.168.1.107	1	2	0	50400	
0	+	193.47.33.135	77.108.111.101	1	2	45,871 М	0	
0	+	Леонид Муравьев	192.168.1.99	1	2	5,1041 М	19,989 М	
0	+	77.234.200.226	77.108.111.101	1	2	97,370 М	0	
0	+	Демидов_Моб	192.168.0.13	1	2	10,218 М	290,354 М	
0	+	Пичугина Елена	192.168.1.111	1	2	28,878 М	206,709 М	
0	+	51.178.91.235	77.108.111.101	1	2	7705	0	
0	+	51.178.91.235	192.168.20.20	1	2	0	4917	
0	+	31.172.70.24	192.168.20.20	1	2	0	819065	
0	+	Данышов_Моб	192.168.0.64	1	2	3,950 М	3,1012 М	
0	+	Данышов_Моб	192.168.0.72	1	2	51605	38413	
0	+	Срапиль	192.168.0.3	1	2	99	310	
1	-	77.108.111.101	108.177.14.113	1	1	0	0	
1	+	31.172.70.24	77.108.111.101	1	2	1620	0	

Помимо основного списка, в окне есть фильтр на текущий список, позволяющий устанавливать различные параметры для отображения клиентов. Внизу расположены кнопки для обновления информации и выхода из окна.

Рисунок 236 - Абоненты ФПСУ-IP

Чтобы обновить полученные от ФПСУ-IP сведения, следует нажать кнопку «F5 Обновить» или установить флаг «Автообновление», указав интервал времени, через который будут производиться повторные запросы.

Причины отказов передачи пакета могут быть следующими:

«Нет памяти для обработки пакета» — недостаточно оперативной памяти для обработки пакета;

«Неправильный IP адрес» — неверен IP-адрес отправителя (широковещательный);

«Пакет слишком короткий» — ошибка формата пакета;

«MAC-адрес станции совпадает с адресом ФПСУ-IP» — MAC-адрес отправителя равен MAC-адресу LAN-плат ФПСУ;

«Отправитель не зарегистрирован на ФПСУ-IP» — IP-адрес отправителя пакета не прописан в конфигурации;

«Получатель не зарегистрирован на ФПСУ-IP» — IP-адрес получателя пакета не описан в конфигурации;

«Запрет работы» — отказ в доступе (запрет работы);

«Абонент должен работать \"Через ФПСУ-IP\"» — абонент должен работать через ФПСУ;

«Удаленный ФПСУ-IP не работает», — удаленный ФПСУ-IP не работает;

«Маршрут неизвестен» — неизвестен MAC-адрес получателя;

«Запрет межсетевым экраном по интерфейсам доступа» — запрет по параметрам доступа;

«Запрет по режиму работы с партнером»

«Обращение с неподдерживаемым протоколом» — обращение к ФПСУ-IP не поддерживаемым протоколом;

«Сбой LAN карты» — сбой LAN-адаптера;

«Запрещено межсетевым экраном по таблице взаимосвязей» — запрет по таблице взаимосвязей;

«Длина фрагмента > 65536» — длина фрагмента больше допустимой;

«Необходима фрагментация, но установлен запрет» — необходима фрагментация;

«Абонент не должен работать через ФПСУ-IP» — абонент не должен работать в режиме ретрансляции;

«Запрет доступа по TCP/UDP портам» — запрет доступа по TCP/UDP портам;

«Запрет доступа по SourceRoute» — запрет доступа по SourceRoute;

«Неправильный список опций IP пакета» — ошибки в списке опций IP пакета;

«Ошибочный пакет от ФПСУ-IP» — ошибочный пакет от ФПСУ;

«Ошибочный REDIRECT-пакет» — ошибочный пакет переадресации;

«Ложный ФПСУ» — станция пытается подменить ФПСУ-IP;

«Фрагмент не кратен 8» — по сети на ФПСУ пришел пакет неправильной длины;"

«Ошибка сериализации» — обнаружено дублирование серийного номера на двух разных ФПСУ;

«Мост: Длинный пакет» — в режиме моста по сети от ФПСУ пришел пакет неправильной длины;

«Клиент не соединен» — отсутствие подключения клиента;

«Запрет доступа клиента к абоненту» — установлен запрет на доступ клиентов к абоненту;

«Запрет доступа клиента к клиенту» — установлен запрет на доступ клиентов;

«Не установлен туннель между ФПСУ-IP» — не установлено соединение с ФПСУ-IP;

«Ошибочный пакет от клиента» — от клиента получен пакет с ошибкой.

16. 1. 3. Получение информации о работе клиентов

Для получения информации о Клиентах, работающих через ФПСУ-IP, следует выбрать ФПСУ-IP в окне списка, и нажать кнопку «Клиенты ФПСУ-IP» панели команд. Когда соединение будет установлено, на экран будет выдано информационное окно, содержащее данные о подключенных в данный момент к ФПСУ-IP клиентах:

- имя и номер, данные клиенту при генерации его ключей;
- IP-адрес клиента в защищённом IP-фрагменте, присвоенный ему администратором ФПСУ-IP;
- номер порта ФПСУ-IP, со стороны которого работает клиент;
- количество байт данных, принятых от клиента и переданных ему с ФПСУ-IP.

Для выделенного клиента списка в окне справа отображаются дополнительные сведения:

- дата и время открытия туннеля - соединения клиента с ФПСУ-IP;
- системные идентификаторы (номер центра, номер группы и номер клиента в группе);
- количество пакетов, принятых от клиента и переданных ему с ФПСУ-IP;
- дата и время последнего обмена данными между ФПСУ-IP и клиентом;

- реальный IP-адрес, с которого работает клиент;
 - MAC-адрес клиента.

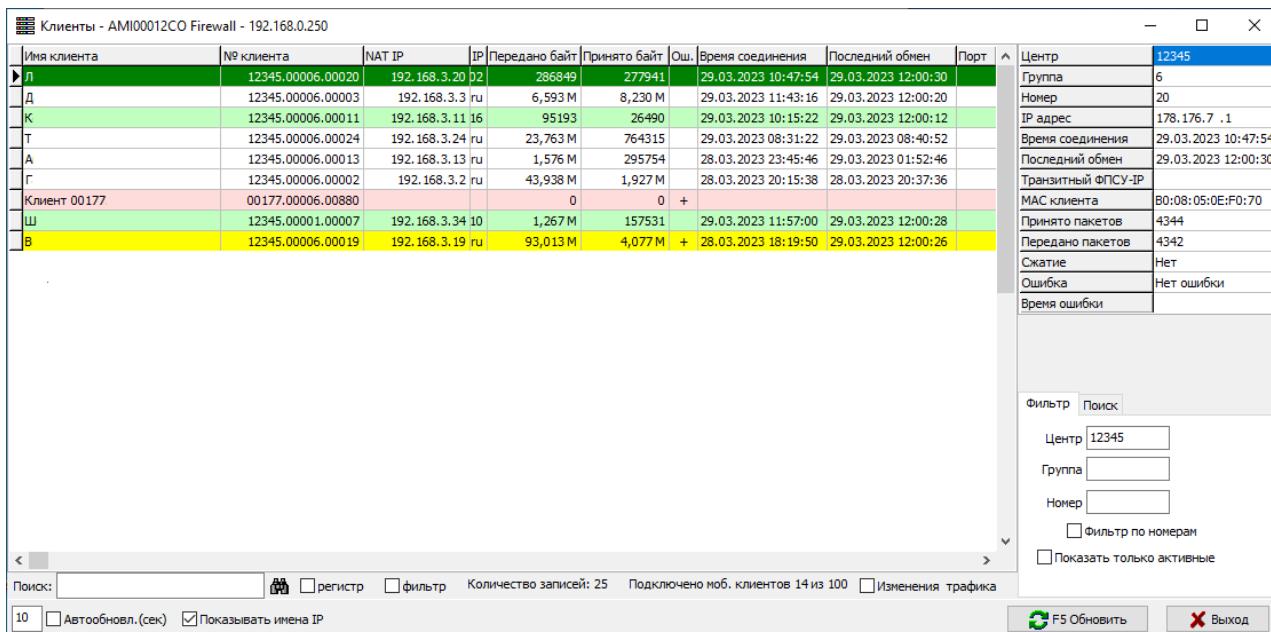


Рисунок 237 - Клиенты ФПСУ-IP

Чтобы обновить полученные от ФПСУ-IP сведения, следует нажать кнопку «F5 Обновить» или установить флаг «Автообновление», указав интервал времени, через который будут производиться повторные запросы. Осуществляется фильтрация по составному номеру клиента.

Подцветка клиентов в списке означает следующее:

- красный цвет - невозможность соединения ввиду ошибки/ошибок;
 - желтый - наличие установленного соединения с ошибкой;
 - зеленый - установленное соединение с клиентом;
 - белый - клиент отсоединен.

Установка флага «Показать только активные» приводит к тому, что в интерфейсе просмотра данных ФПСУ-IP/Клиентов, передаваемых через ФПСУ-IP, запрашиваются и отображаются данные только тех клиентов, которые в настоящий момент соединены с ФПСУ-IP. Эта настройка аналогична описанной в пункте «Дополнительные настройки интерфейса УА ФПСУ-IP».

Следует учитывать, что в случае отображения всех клиентов в списке, отсоединенные клиенты будут показываться до момента перезагрузки ФПСУ-IP.

16. 1. 4. Получение информации о работе администраторов УА ФПСУ-IP

Для получения информации об администраторах УА ФПСУ-IP, зарегистрированных на выбранном в окне списка ФПСУ-IP, следует нажать кнопку «Удаленные АДМ» панели команд. Когда соединение будет установлено, на экран будет выдано окно, отображающее текущее состояние и результаты последних действий администраторов УА ФПСУ-IP.

Чтобы обновить полученные от ФПСУ-IP сведения, необходимо нажать кнопку «F5 Обновить» или установить флаг «Автообновление», указав интервал времени, через который будут производиться повторные запросы.

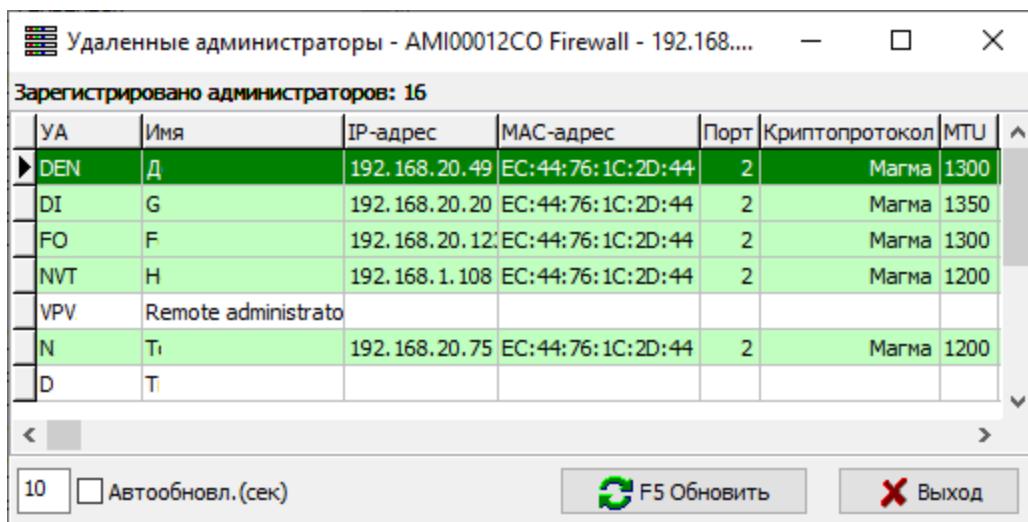


Рисунок 238 - Окно мониторинга состояния администраторов УА ФПСУ-IP

16. 1. 5. Получение информации об изменениях программного обеспечения

Для получения данных об установках и изменениях программного обеспечения на ФПСУ-IP, следует выбрать в окне списка ФПСУ-IP и нажать кнопку «Обновления ПО» панели команд. Появится информационное окно, отображающее состояние обновлений ПО на выбранном ФПСУ-IP. По умолчанию список выводится в порядке установленных обновлений, вверху - самое первое установленное обновление, внизу - самое последнее.

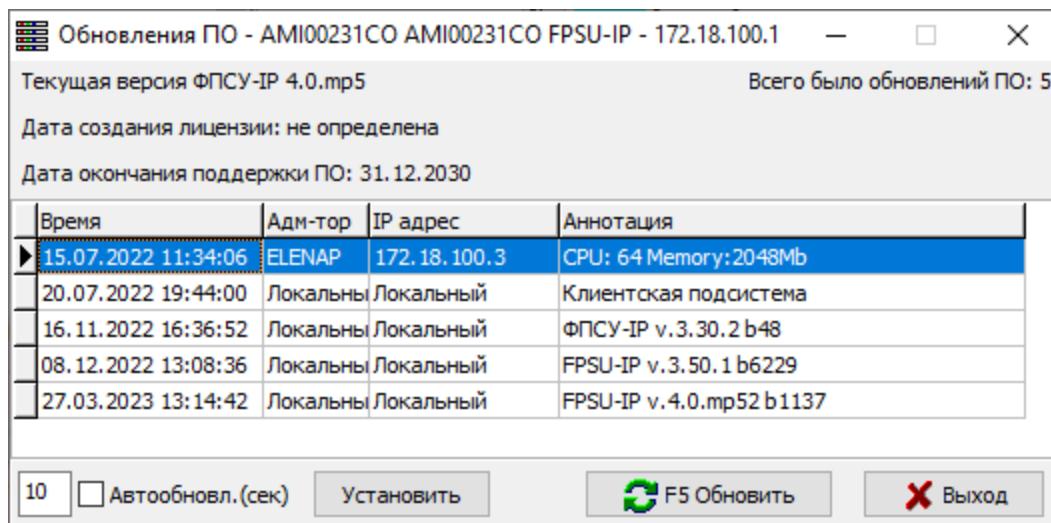


Рисунок 239 - Сведения по обновлениям ПО

В окне отображаются дата и время установок дополнительного или обновлённого ПО, имя администратора, который осуществлял установку, его IP-адрес и описание установленного ПО.

В поле «Аннотация» первого по времени установленного обновления выводимый текст изменяется на полученную в последнем запросе к ФПСУ-IP информацию о количестве оперативной памяти на ФПСУ-IP (число после слова "Memory:" в мегабайтах) и задействованных ядрах (число после слова «CPU»).

Чтобы обновить полученные от ФПСУ-IP сведения, необходимо нажать кнопку «F5 Обновить» или установить флаг «Автообновление», указав интервал времени, через который будут производиться повторные запросы.

16. 1. 6. Получение информации о состоянии портов

Для просмотра событий на портах ФПСУ-IP необходимо нажать кнопку «Состояние портов» панели команд, после чего в случае успешной установки туннеля с ФПСУ-IP на экран будет выдано соответствующее информационное окно.

The screenshot shows a window titled 'Состояние портов - AMI00012CO Firewall - 192.168.0.250'. It displays two tabs for ports: '1' and '2'. The '1' tab is selected. The table contains the following data:

Параметр порта	1	2
Link	Up	Up
Speed	1000 Мб/с FD	1000 Мб/с FD
IP	77.108.111.101	192.168.0.250
Mask	255.255.255.0	255.255.255.0
MAC	02:6D:10:92:22:10	02:6D:10:92:22:11
+ Кол-во VLAN	2	1
Прием, Мбит/с	0,844	0,261
Передача, Мбит/с	0,471	0,619
Прием, пак/с	625	271
Передача, пак/с	426	470
Принято ARP	185	11621
Отправлено ARP	489	54245
Принято ошибочных ARP	0	6
Ошибка при отправке ARP	3	10
Отказано в приеме ARP	1072	248546
Принято IP	45776168	33221764
Отправлено IP	34076068	45045091
Принято ошибочных IP	0	0
Ошибка при отправке IP	0	0
Отказано в приеме IP	168154	110273
Пропущено на приеме IP	0	27
Неподдерж. фреймы	0	0

At the bottom, there are buttons for 'Auto-refresh (sec)' (10), 'Reset counters' (highlighted in blue), 'F5 Refresh', and 'Exit'.

Рисунок 240 - Мониторинг состояния портов ФПСУ

Окно разделено на две половины, в каждой из которых отображается состояние одного из портов ФПСУ-IP, используемых для связи локальных подсетей и передачи пакетов абонентов. Выводимые параметры разбиты на три группы.

Первая группа содержит сведения о конфигурационных установках порта - параметрах используемого сетевого адаптера, Ethernet- и IP-адресах порта, маске подсети, связанной с портом; а также о скорости передачи данных по порту в Мбит/с.

Вторая и третья группа отображает статистику событий на сетевом адаптере с момента запуска подсистемы фильтрации. Они содержат сведения о количестве поступивших на сетевой адаптер по сети пакетов различных протоколов (до фильтрации),

переданных с этого адаптера в сеть пакетах различных протоколов, отвергнутых пакетах (не прошедших фильтрацию или по причине неполадок сетевого уровня) и пакетах, содержащих ошибки кадрового уровня.

Кнопка «Сбросить счётчики» предназначена для дистанционного обнуления отображаемых в окне счётчиков (на подконтрольном ФПСУ-IP) с целью, например, проведения контрольных замеров в дальнейшем.

Чтобы обновить полученные от ФПСУ-IP сведения, следует нажать кнопку «F5 Обновить» или установить флаг «Автообновление», указав интервал времени, через который будут производиться повторные запросы.

16. 1. 7. Получение информации о загрузке процессора ФПСУ-IP

Для того чтобы соединиться с ФПСУ-IP и получить данные о текущей загрузке его процессоров, необходимо выбрать ФПСУ-IP в списке главного окна УА ФПСУ-IP и нажать кнопку «ЦПУ» панели команд. В случае успешной установки туннеля появится окно, отображающее график загрузки ЦПУ в процентах. Масштаб шкалы времени можно увеличивать и уменьшать при помощи кнопок [–] и [+].

Максимальная с момента запуска ФПСУ-IP нагрузка указывается в соответствующей информационной строке окна. Чтобы обновить полученные от ФПСУ-IP сведения, следует нажать кнопку «F5 Обновить» или установить флаг «Автообновление», указав интервал времени, через который будут производиться повторные запросы.

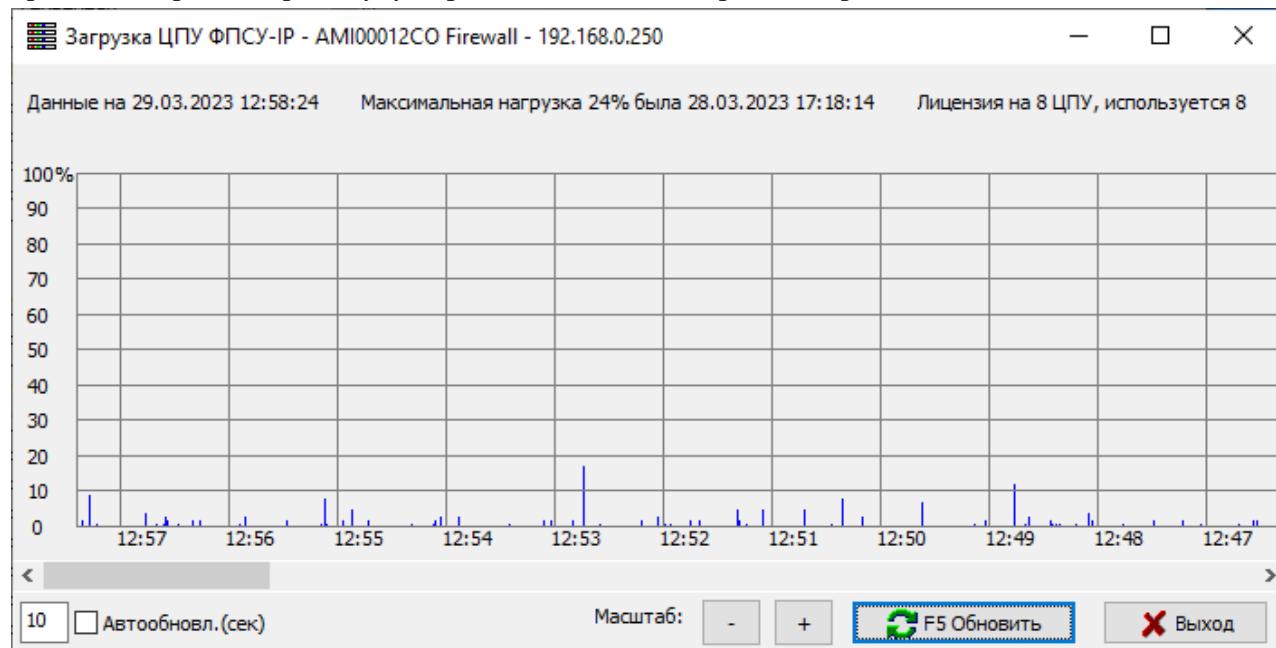
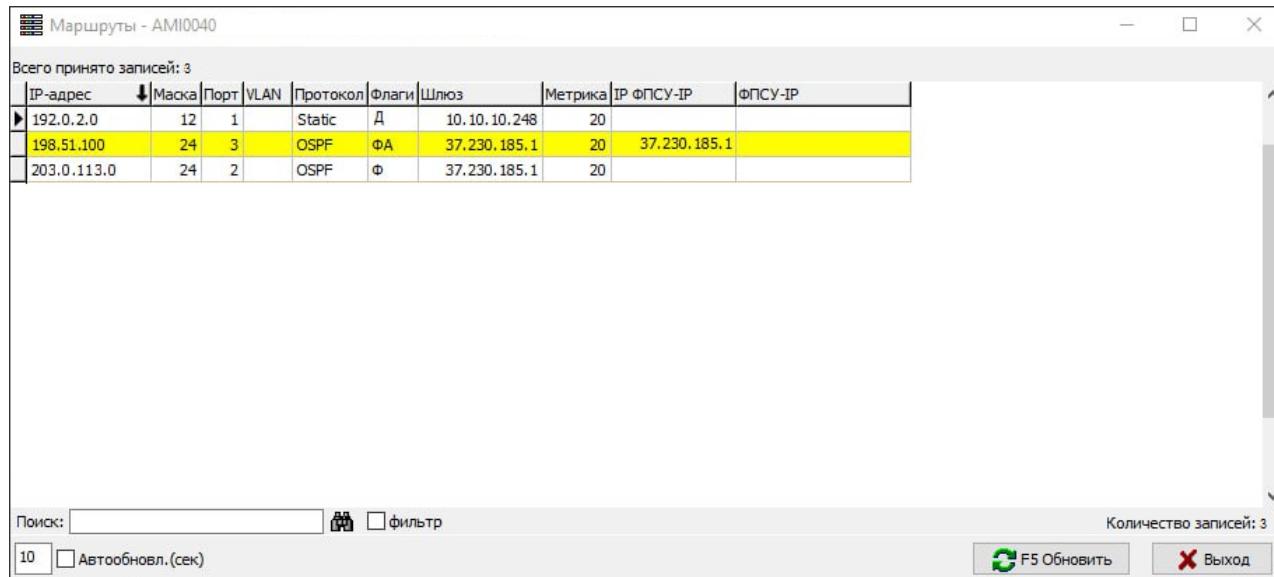


Рисунок 241 - Мониторинг загрузки ЦПУ

16. 1. 8. Получение информации о маршрутах

Для того чтобы просмотреть маршруты соединения ФПСУ-IP, необходимо выбрать ФПСУ-IP в списке главного окна УА ФПСУ-IP и нажать кнопку «Маршруты» панели команд. Данная опция доступна для ФПСУ-IP начиная с версии 4.



The screenshot shows a window titled 'Маршруты - AMI0040'. At the top, it displays 'Всего принято записей: 3'. Below is a table with the following data:

IP-адрес	Маска	Порт	VLAN	Протокол	Флаги	Шлюз	Метрика	IP ФПСУ-IP	ФПСУ-IP
192.0.2.0	12	1		Static	Д	10.10.10.248	20		
198.51.100	24	3		OSPF	ФА	37.230.185.1	20	37.230.185.1	
203.0.113.0	24	2		OSPF	Ф	37.230.185.1	20		

At the bottom, there are search and filter fields ('Поиск:', 'фильтр'), a refresh button ('F5 Обновить'), and an exit button ('Выход').

Рисунок 242 - Маршруты ФПСУ-IP

В строке маршрута выводятся следующие сведения:

- адрес сети или узла назначения;
- маска сети назначения;
- номер порта ФПСУ-IP, являющийся шлюзом;
- описатель VLAN;
- протокол маршрутизации:
 - статический маршрут (Static);
 - маршрут, установленный во время загрузки (BOOT);
 - BGP;
 - OSPF;
- флаги;
- шлюз, обозначающий IP-адрес порта ФПСУ-IP или маршрутизатора в сети, на который необходимо отправить пакет, следующий до указанного адреса назначения;
- метрика;

- IP ФПСУ-IP;
- ФПСУ-IP.

16. 1. 9. Просмотр ARP-таблиц

Для получения сведений о состоянии ARP-таблиц на портах ФПСУ-IP, следует выбрать его в окне списка, и нажать кнопку «ARP» панели команд. Когда соединение с ФПСУ-IP будет установлено, на экране появится окно просмотра ARP-записей.

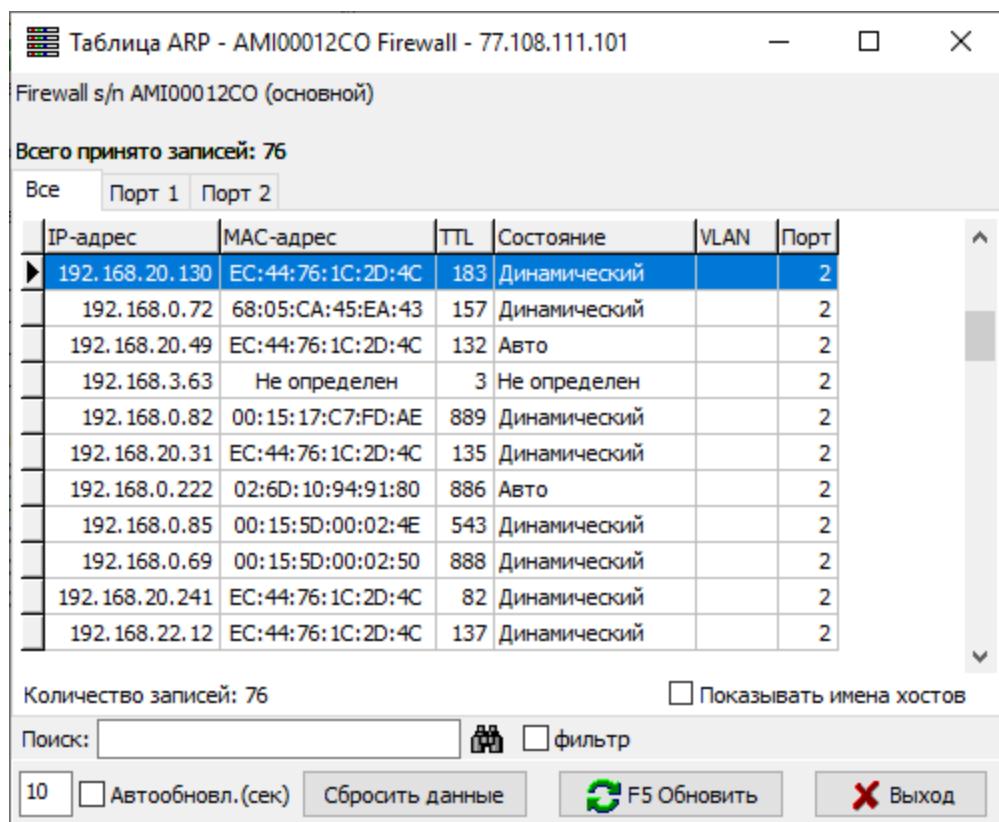


Рисунок 243 - Мониторинг ARP-таблиц

Каждая запись таблицы имеет следующий формат:

IP-адрес, для которого ищется ARP-адрес	MAC-адрес (если найден)	Время в секундах, оставшееся до вытеснения записи из списка (TTL)	Состояние работы	VLAN
---	-------------------------	---	------------------	------

Работа прокола ARP может находиться в следующих состояниях (последнее поле):

- Поиск - начата процедура определения MAC-адреса IP-абонента;

- Не определен - процедура поиска закончилась отрицательно;
- Динамический - MAC-адрес для соответствующего IP-адреса определён.

Чтобы обновить полученные от ФПСУ-IP сведения, следует нажать кнопку «F5 Обновить» или установить флаг «Автообновление», указав интервал времени, через который будут производиться повторные запросы. Кнопка «Сброс данных» позволяет заново начать на ФПСУ-IP процедуру поиска адресов для абонентов списка.

Переключиться на просмотр ARP-таблицы другого порта ФПСУ-IP можно при помощи вкладки с названием порта верхней части окна (Порт 1/Порт 2).

16. 1. 10. Просмотр статистики ФПСУ-IP

Статистическую информацию по работе выбранного в окне списка ФПСУ-IP можно получить, нажав кнопку «Статистика ФПСУ-IP» панели команд. Необходимо, чтобы между УА ФПСУ-IP и ФПСУ-IP было установлено успешное соединение, на УА ФПСУ-IP была настроена БД статистики, включен сбор статистики ФПСУ-IP, подробнее см. пункт «Получение статистической информации».

В открывшемся окне выбора статистических данных, запрашиваемых с ФПСУ-IP, необходимо установить условия поиска: необходимые типы и подтипы данных и значения интервалов даты и времени. С помощью кнопок «Сегодня 0 часов» и «Сейчас» можно быстро установить время съёма информации за текущие сутки.

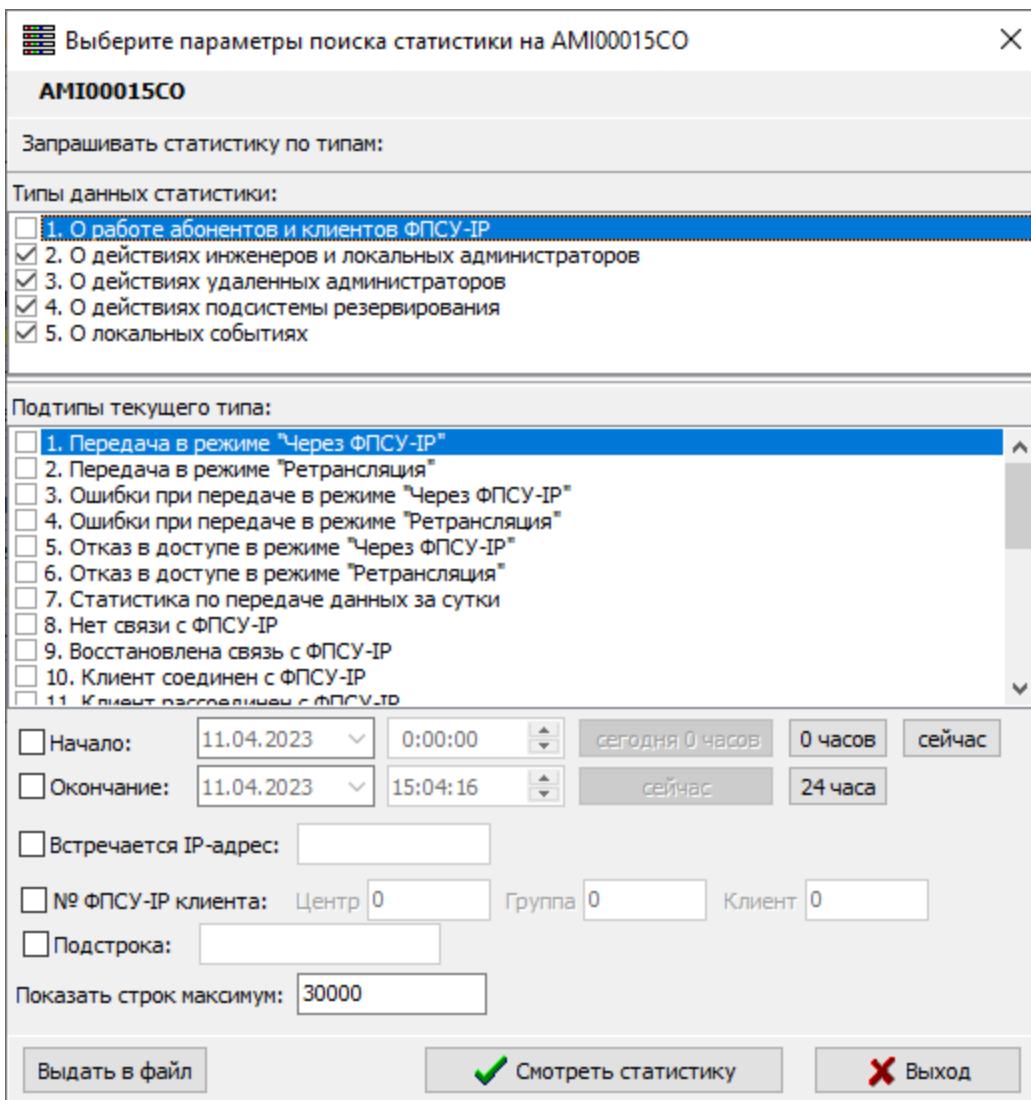


Рисунок 244 - Окно выбора типов и времени запрашиваемой вручную статистики

После выбора требуемых параметров необходимо нажать кнопку «Смотреть статистику», или «Выход» для отмены процедуры запроса.

В отдельном окне выводятся записи статистики в хронологическом порядке с датой и типом события.

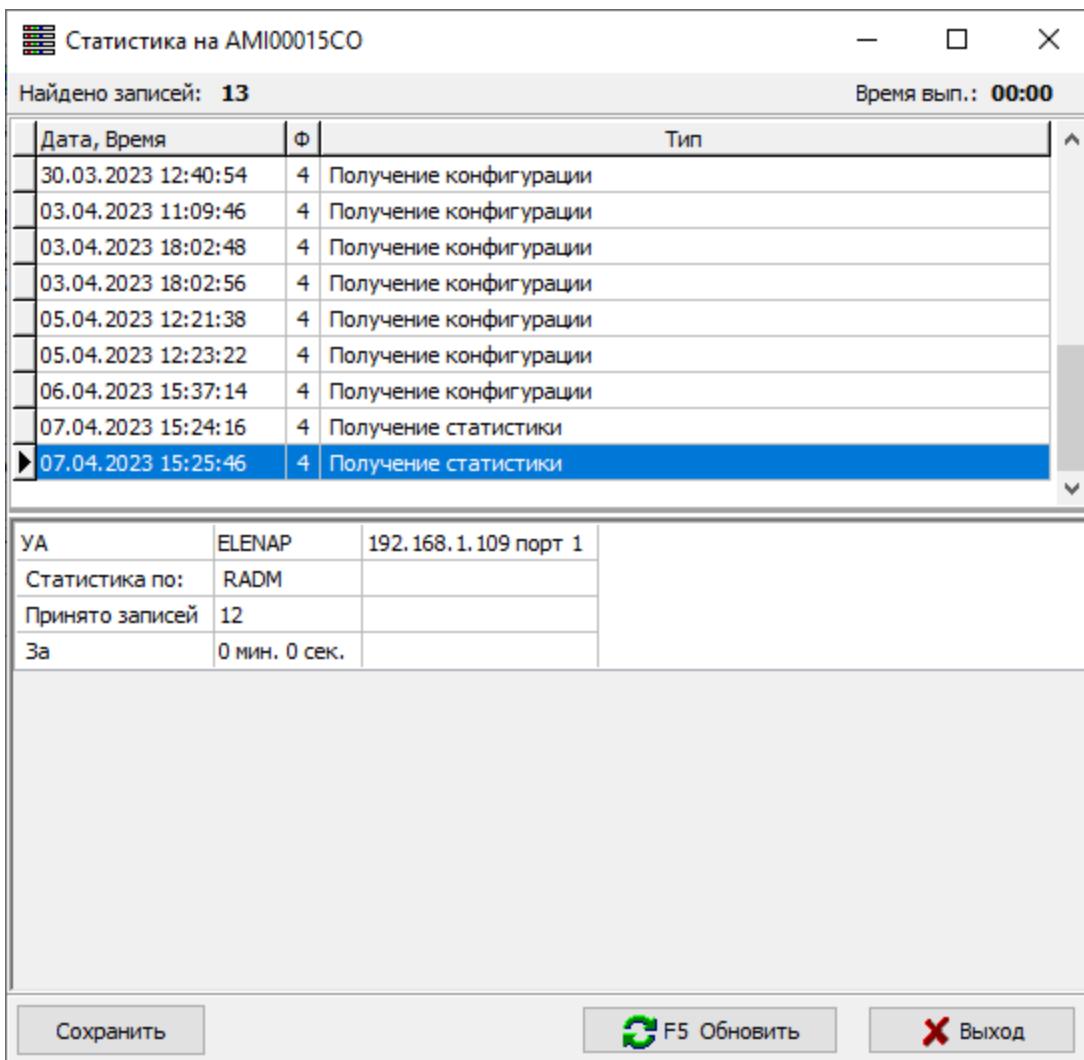


Рисунок 245 - Окно просмотра статистики

16. 1. 11. Дистанционный запуск ping на управляемом ФПСУ-IP

Под управлением УА ФПСУ-IP ФПСУ-IP отправляет эхо-запрос заданному хосту для проверки соединения с помощью команды ping, а также для определения трассировки маршрута с помощью команды traceroute. Данные команды запускаются дистанционно на управляемом ФПСУ-IP.

Для тестирования соединения ФПСУ-IP с заданным хостом, следует выбрать ФПСУ-IP в окне списка, и нажать кнопку «Пинг от ФПСУ-IP» панели команд.

На экран будет выдано окно для отправления эхо-запроса указанному хосту:

- в поле «IP-адрес» требуется задать IP-адрес хоста для отправки ему эхо-запроса;

- в поле «Количество» указывается количество передаваемых эхо-пакетов;
- установленный флаг «Traceroute» позволяет получить трассировку маршрута до указанного хоста, показывает время прохождения пакетов до промежуточных и конечного хостов;
- в поле «TTL» указывается время жизни отправляемого эхо-пакета;
- установленный флаг «Показывать имена хостов» рядом с IP-адресом добавляет имя хоста в системе доменных имён, если его удается получить. Запрос разрешения имён отправляется с компьютера, на котором установлен УА ФПСУ-IP.

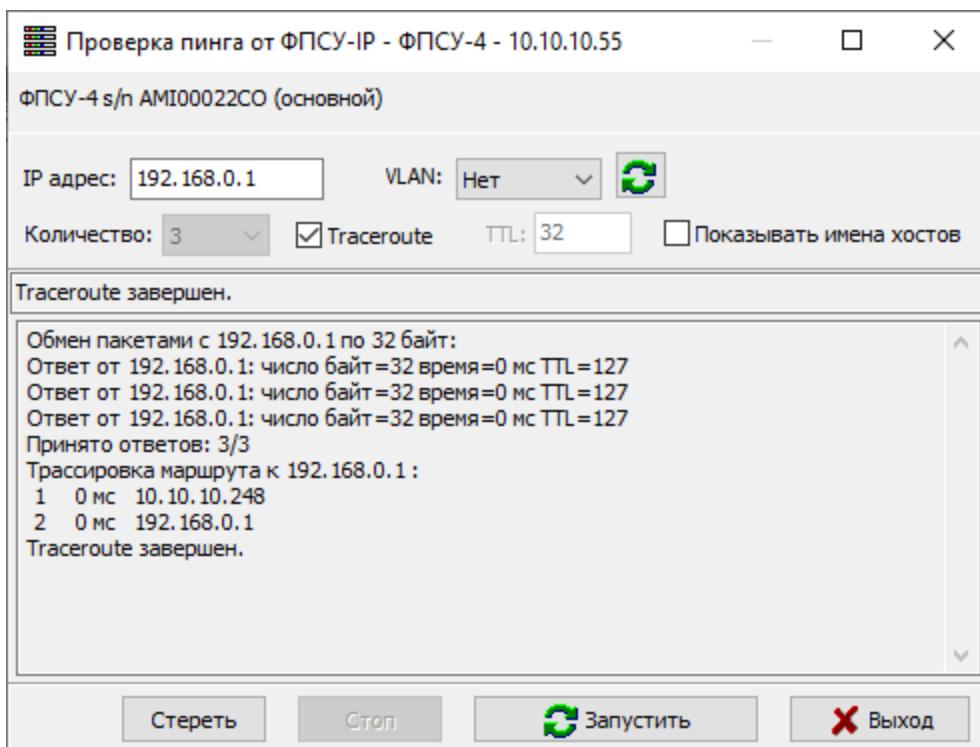


Рисунок 246 - Результат выполнения утилиты ping и traceroute

По нажатию кнопки «Запустить» в информационном поле отобразится результат работы утилиты ping или, в случае установленного флага «Traceroute», утилиты traceroute.

16. 1. 12. Мониторинг сессий МЭ

Для получения данных о сессиях ФПСУ-IP, следует выбрать в окне списка ФПСУ-IP и нажать кнопку «Сессии МЭ» панели команд. Появится информационное окно, отображающее соединения на выбранном ФПСУ-IP. По каждому соединению на экран будет выдана информация о:

- правилах МЭ;
- IP-адресах инициатора и получателя соединения;
- портах инициатора и получателя соединения;
- используемом протоколе;
- таймауте и длительности соединения;
- объёме и скорости передачи данных.

The screenshot shows a software interface titled 'Сессии межсетевого экрана - AMI00012CO Firewall - 192.168.0.250'. It displays a table of network sessions with columns: Правило (Rule), Инициатор (Initiator), Получатель (Recipient), Из IP порта (From IP port), В IP порт (To IP port), Протокол (Protocol), Из LAN порта (From LAN port), В LAN порт (To LAN port), Таймаут (Timeout), Длительность (Duration), От инициатора байт (Bytes from initiator), and several other columns for recipient and duration. A context menu is open on the right side of the table, listing options like Internet_All, Инициатор (Initiator), Получатель (Recipient), Из IP порта (From IP port), В IP порт (To IP port), Протокол (Protocol), Из LAN порта (From LAN port), В LAN порт (To LAN port), Таймаут (Timeout), Длительность (Duration), От инициатора байт (Bytes from initiator), От получателя байт (Bytes to initiator), От инициатора пак. (Packets from initiator), От получателя пак. (Packets to initiator), Состояние (State), Передача Kb/s (Transmission Kb/s), and Прием Kb/s (Receipt Kb/s). At the bottom of the window, there are search fields, filter checkboxes, and buttons for Refresh (F5) and Exit.

Рисунок 247 - Сессии МЭ

Информация о сессиях преобразуется с помощью опций:

- «Автообновление» позволяет обновлять полученные от ФПСУ-IP сведения с заданным интервалом. Для этого следует установить флаг «Автообновление», указав интервал времени, через который будут производиться повторные запросы.
- Установленный флаг «Показывать имена хостов» в столбцах таблицы «Инициатор», «Получатель» вместо IP-адреса позволяет отображать имя хоста в системе доменных имён, если его удается получить. Запрос разрешения имён отправляется с компьютера, на котором установлен УА ФПСУ-IP.
- Установленный флаг «Имена портов TCP/UDP» в столбцах таблицы «Из IP-порта», «В IP-порт» вместо номера порта позволяет отображать имя сервиса, который

использует этот порт.

- Кнопка «F5 Обновить» позволяет администратора УА вручную запросить новые сведения от ФПСУ-IP.

Для поиска сессий может быть применен фильтр, содержит следующие опции:

- Поле для ввода информации и кнопка «Поиск следующего»  позволяет задать в поле текстовую или цифровую информацию для поиска. Поиск ведется по всем столбцам таблицы, в записи таблицы искомый текст ищется как подстрока. По кнопке «Поиск следующего» происходит переход к следующей найденной записи, удовлетворяющей введённой информации.
- Установленный флаг «Регистр» позволяет искать искомый текст с учётом регистра введённых символов.
- Установленный флаг «Фильтр» оставляет в таблице только записи, удовлетворяющие условию поиска. Если в поле ввода вносится новая информация, то для обновления поиска следует снять флаг и повторно его установить.

Для частичного мониторинга и может быть применен запрос с фильтром, при котором задается диапазон IP-адресов или диапазон номеров клиентов ЦГКК. Запрос с фильтром выполняется быстрее, чем полный запрос всех сессий с ФПСУ-IP.

Установленный флаг «Запрос с фильтром» позволяет использовать дополнительные фильтры.

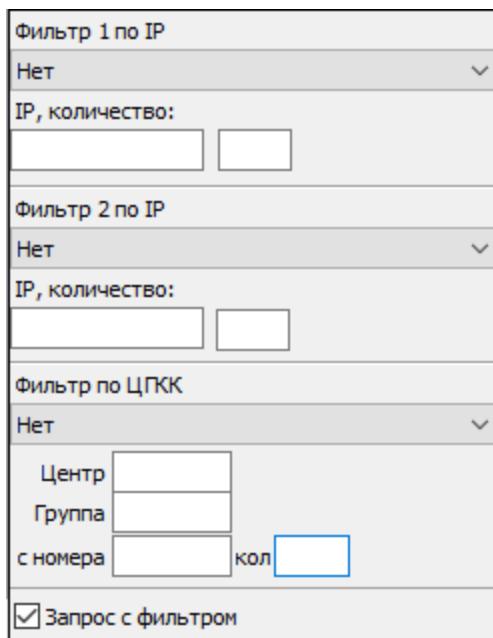


Рисунок 248 - Опции запроса с фильтром

Для фильтра по диапазону IP-адресов следует в поле «Фильтр %N% по IP» выбрать столбец таблицы, в котором будет производиться поиск IP-адресов. Диапазон IP-адресов задается первоначальным IP-адресом и количеством последующих IP-адресов, включая первоначальный, в полях «IP, количество».

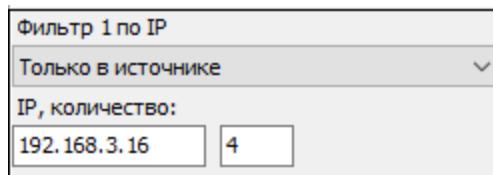


Рисунок 249 - Пример фильтра

На рисунке выше приведен пример задания фильтра для поиска сессий с IP-адресами 192.168.3.16 - 192.168.3.19 в столбце таблицы «Инициатор».

Фильтр по диапазону номеров клиентов ЦГКК позволяет выбрать столбец таблицы в поле «Фильтр по ЦГКК», в котором будет производиться поиск сессий клиентов ЦГКК. В полях «Центр», «Группа» задаются номера центра и группы ЦГКК. В поле «С номера» задается номер клиента, с которого начинается диапазон, в поле «Количество» - количество номеров диапазона, включая первый номер диапазона.

Флаги «Фильтр» и «Запрос с фильтром» могут применяться как по отдельности, так и совместно.

Контекстное меню содержит следующие команды:

- «Открыть правило в конфигурации...» - открывает окно правил трафика конфигурации ФПСУ-IP; позволяет изменять правила в конфигурации ФПСУ-IP;
- «Найти в абонентах...» - открывает окно «Абоненты» с выделенной парой абонентов;
- «Пинг...» - открывает окно проверки эхо-запроса и запускает тест соединения выбранного хоста с помощью команды ping (см. пункт «Дистанционный запуск ping на управляемом ФПСУ-IP»);
- «Блокировка» - позволяет заблокировать/разблокировать выбранное соединение.

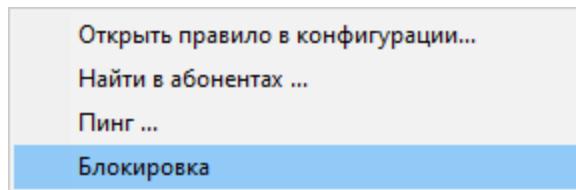


Рисунок 250 - Контекстное меню

16. 1. 13. Мониторинг заблокированного трафика

Для получения сведений о заблокированном на ФПСУ-IP трафике, а также для временного блокирования трафика без внесения изменений в конфигурацию ФПСУ-IP, следует выбрать ФПСУ-IP в окне списка, и нажать кнопку «Блокировать трафик» панели команд, если трафик уже блокируется ФПСУ-IP. В случае успешного установления соединения между УА ФПСУ-IP и ФПСУ-IP, на экран будет выведено информационное окно, отображающее тип и значение трафика, временной период блокировки.

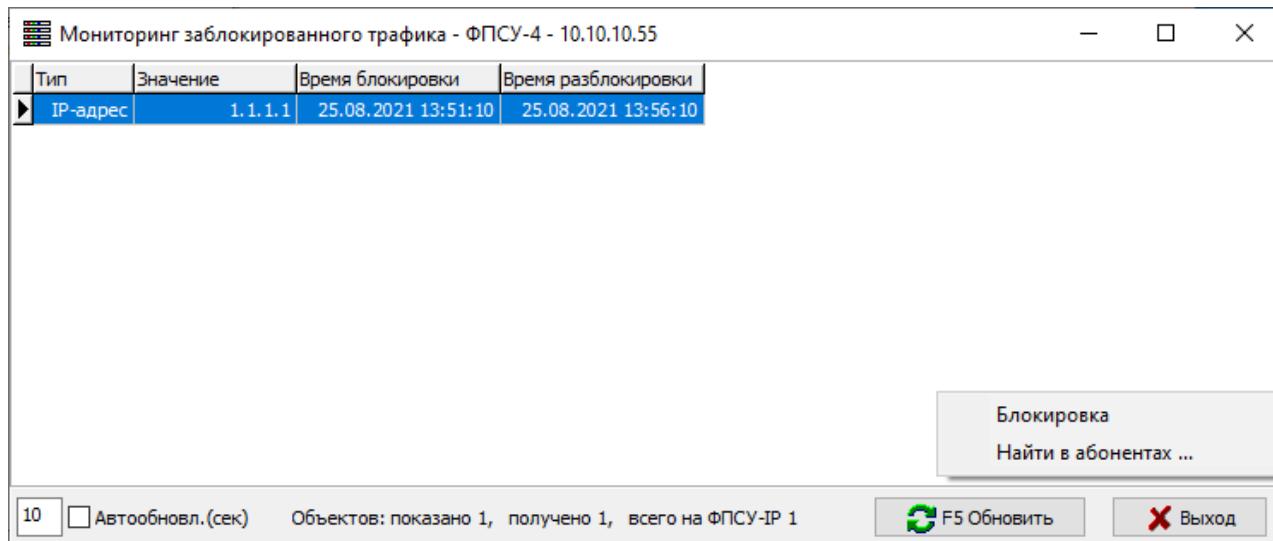


Рисунок 251 - Мониторинг заблокированного трафика

Чтобы обновить полученные от ФПСУ-IP сведения, следует нажать кнопку «F5 Обновить» или установить флаг «Автообновление», указав интервал времени, через который будут производиться повторные запросы.

По нажатию правой кнопки мыши в строке списка отображается контекстное меню с командой «Блокировка», если список блокировок не пустой, доступна команда «Найти в абонентах ...».

При необходимости блокирования трафика администратором УА ФПСУ-IP должны быть соблюдены условия:

- в конфигурации ФПСУ-IP в параметрах доступа должен быть включен «Flood control»;
- для выбранного ФПСУ-IP должен быть включен межсетевой экран и отображаться на панели информации знаком .

По команде «Блокировка» откроется окно, в котором для блокирования трафика требуется:

- выбрать один из типов трафика, чаще хост или подсеть;
- задать значение или список значений для выбранного типа;
- установить период времени блокировки или разблокировки.

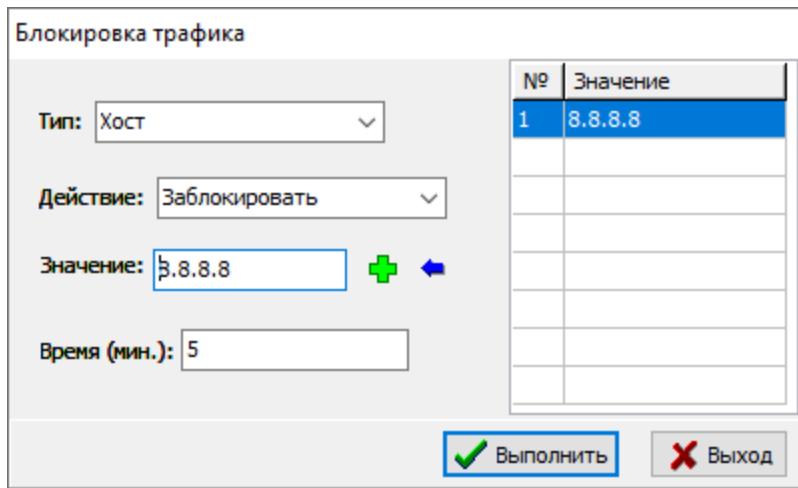


Рисунок 252 - Блокировка трафика

По нажатию кнопки «Выполнить» на экран выдается сообщение о результате выполнения операции и заблокированный трафик добавляется в список, разблокированный трафик из списка удаляется. Для возврата в окно мониторинга требуется нажать кнопку «Выход».

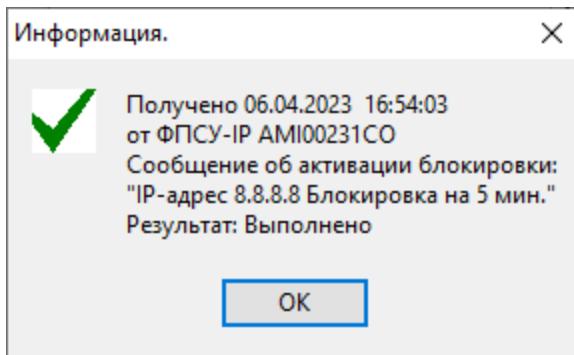


Рисунок 253 - Информационное сообщение

По команде «Найти в абонентах ...» открывается окно «Абоненты» (см. пункт «Получение информации о работе абонентов»).

16. 1. 14. Состояние ФПСУ-IP

Краткую информацию по работе выбранного в окне списка ФПСУ-IP можно получить, нажав кнопку «Состояние ФПСУ-IP» панели команд. В случае успешного установления соединения между УА ФПСУ-IP и ФПСУ-IP, на экран будет выведено информационное окно:

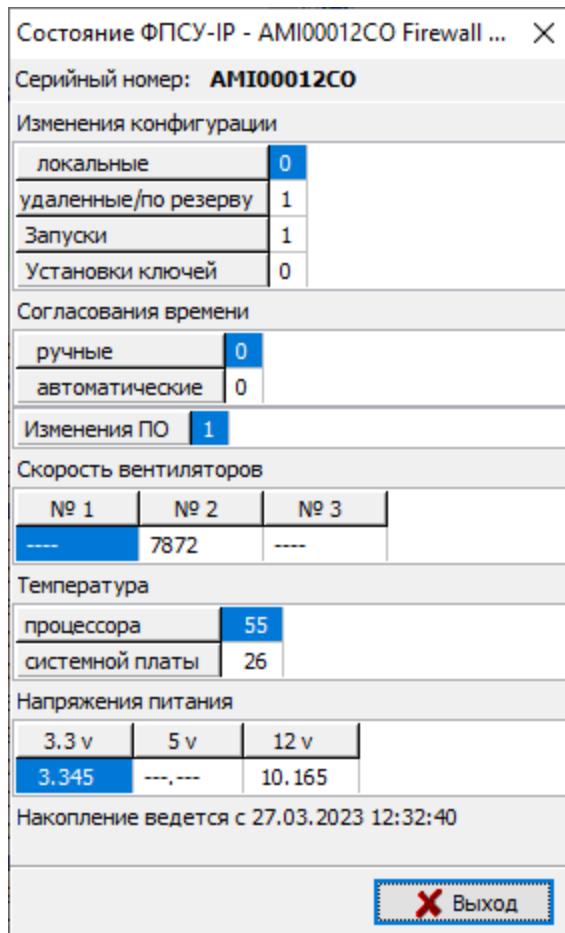


Рисунок 254 - Общая статистика по работе ФПСУ-IP

В этом окне находится краткий отчёт об изменениях конфигурации ФПСУ-IP, программного обеспечения, даты и времени, а также состояние аппаратной части — скорость вращения вентиляторов, температура и напряжение.

16. 2. Запрос с ФПСУ-IP по SNMP

Для мониторинга ФПСУ-IP используется протокол SNMP. В УА ФПСУ-IP встроен SNMP-менеджер, позволяющий получать данные с ФПСУ-IP в виде иерархической (древовидной) структуры MIB-базы.

В MIB-базе хранится информация обо всех управляемых объектах (параметрах, настройках) ФПСУ-IP. К записям можно обратиться через идентификаторы объектов OID и по имени объекта OID.

Для каждой версии ФПСУ-IP различается список объектов, определенных в MIB-

базе. Если для данной версии ФПСУ-IP объект не определен, то в описании объекта будет ошибка «Параметр не найден».

Для получения данных с ФПСУ-IP необходимо выбрать пункт меню «Операции» → «Запрос с ФПСУ-IP по SNMP».

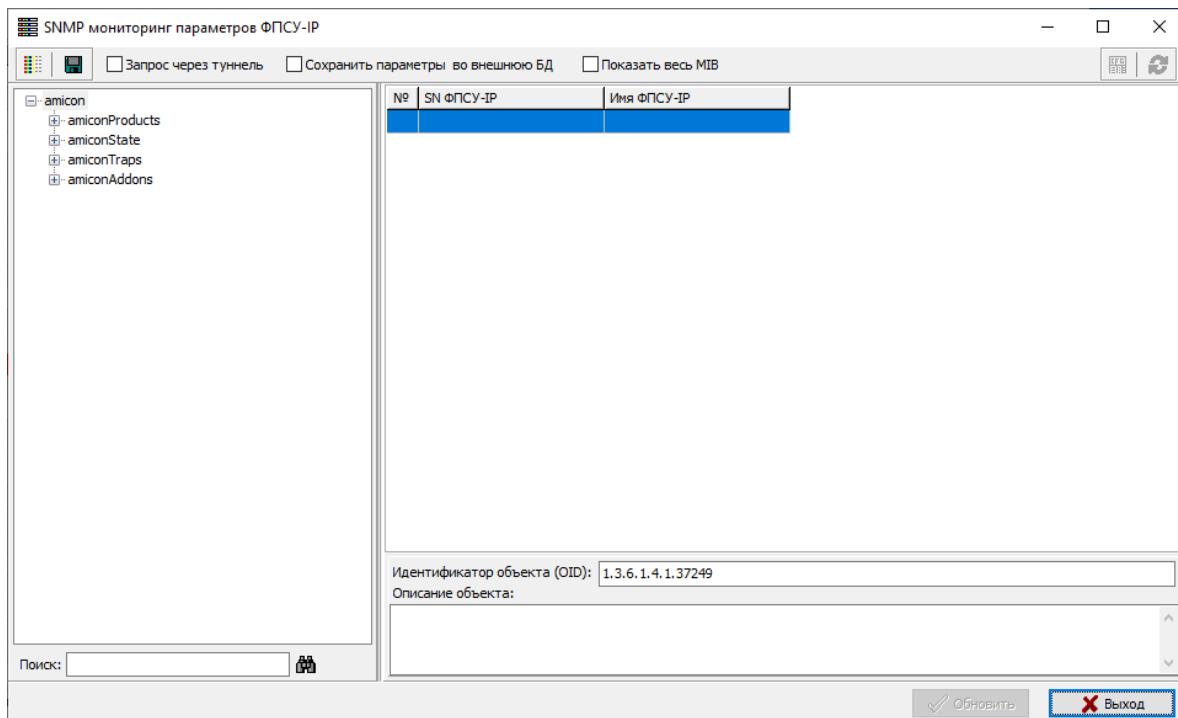


Рисунок 255 - SNMP мониторинг параметров ФПСУ-IP

В области слева отображается дерево объектов МИВ-базы.

Кнопка в верхнем левом углу «Выбор ФПСУ» позволяет выбрать ФПСУ-IP для мониторинга.

Кнопка в верхнем левом углу «Сохранить результат» позволяет сохранить запрошенные данные в буфер обмена, в текстовый файл, в файл формата csv.

При установке флага «Запрос через туннель» SNMP сообщения от ФПСУ-IP будут отправлены по защищенному соединению через VPN-туннель «УА-ФПСУ-IP» (применяется для ФПСУ-IP версии 3.30.1 и выше).

При установке флага «Сохранить параметры во внешнюю БД» параметры будут сохраняться во внешнюю БД, в этом случае в базе будет отображаться изображение аппаратной платформы ФПСУ-IP.

При установке флага «Показать весь МИВ» база МИВ будет отображаться в виде полной

иерархической структуры, начиная с первого уровня.

В верхнем правом углу окна кнопки «Редактировать выбранную кфг» и «Загрузить выбранную кфг с ФПСУ» позволяют не выходя из настроек сменить/задать пароль SNMP.

16. 3. Работа с квантовым дополнением

Начиная с 4-й версии, ФПСУ-IP поддерживает работу с устройствами квантового распределения ключей (квантовая криптографическая система выработки и распределения ключей), реализующими использующий квантовые явления метод распределения симметричных ключей между узлами сети связи (сеть передачи данных, состоящая из связанных квантовыми туннелями узлов).

При установке квантового соединения используются следующие виды туннелей:

- Служебный туннель – криптографически защищенное соединение (туннель) между двумя смежными в рамках квантовой сети ФПСУ-IP, в рамках которого осуществляется обмен служебными данными между соседними устройствами СВКРК в процессе выработки квантовых ключей. Служебные данные используются для синхронизации случайных последовательностей между соседними устройствами СВКРК.
- Квантовый туннель – защищенное имитовставкой и шифрованием виртуальное соединение (туннель), организованное между ФПСУ-IP с использованием полученных от соседних устройств СВКРК квантовых ключей или с использованием полученных от промежуточного узла квантово-защищенных ключей (секретных ключей, используемых для построения квантового туннеля между несмежными ФПСУ-IP квантовой сети и переданных на них через квантовые туннели).
- Квантово-сервисный туннель – защищенное имитовставкой и шифрованием виртуальное соединение (туннель), организованное между ФПСУ-IP с использованием полученных от соседних устройств СВКРК квантовых ключей. Квантово-сервисный туннель предназначен для передачи квантово-защищенных ключей (КЗК) между смежными ФПСУ-IP в рамках квантовой сети/
- Гибридный туннель – криптографически защищенное соединение (туннель) между двумя ФПСУ-IP, которому разрешено шифровать передаваемую информацию как на основе квантовых ключей (в случае их наличия), так и на основе полученных от ЦВК ключей. Квантовые ключи считаются более приоритетными, как только на ФПСУ-IP появляются квантовые ключи, шифрование в гибридном туннеле переходит на них.

Информация по работе с устройствами квантового распределения ключей в УА ФПСУ-IP отображается в окнах «Состояние VPN» и «Модули», вызываемыми одноименными кнопками блока команд (см. раздел «Панель команд»).

Нажатие кнопки «Состояние VPN» выводит на экран окно, отображающее состояние VPN-туннелей для выбранного ФПСУ-IP. При этом в графе «Режим» квантовый и квантово-сервисный туннели будут помечены сокращением «QKD», а гибридный - сокращением «HYB».

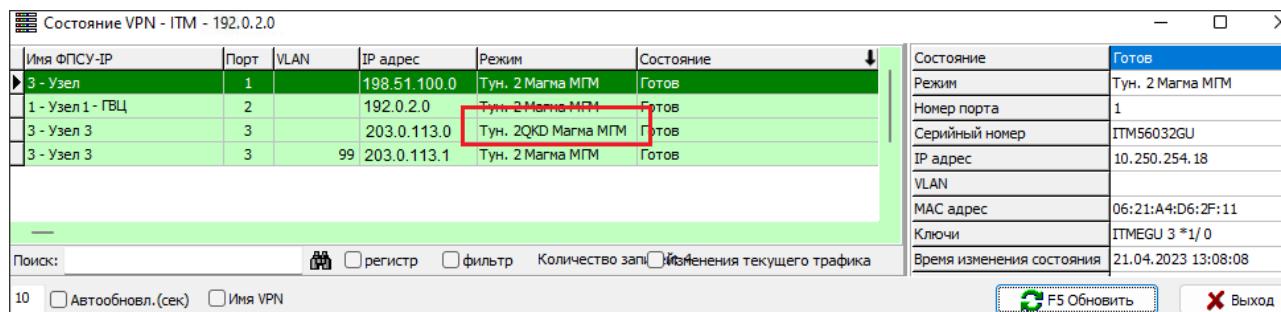


Рисунок 256 - Состояние VPN с отображением квантового туннеля

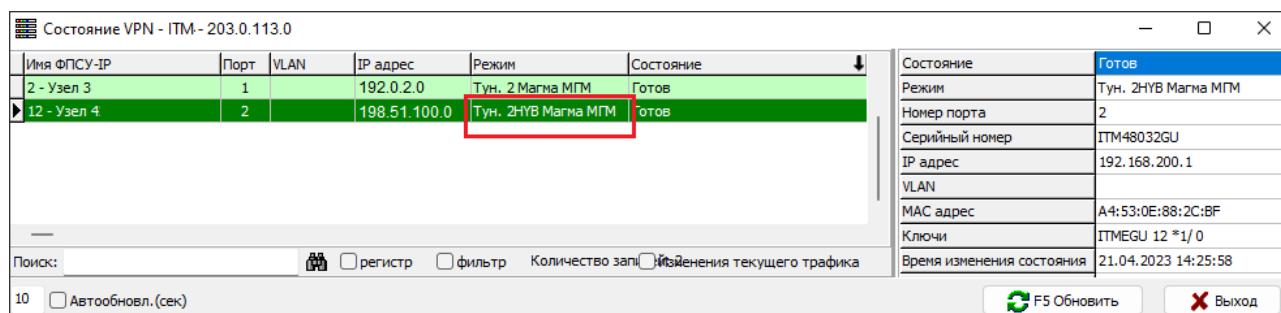


Рисунок 257 - Состояние VPN с отображением гибридного туннеля

Нажатие кнопки «Модули» открывает окно просмотра и диагностики работы подключенных модулей. По кнопке «Диагностика» окна «Модули» предоставляется возможность просмотреть различные виды диагностических данных для квантовых модулей.

Рядом с кнопкой «Диагностика» расположено меню дополнительных команд, позволяющее просматривать различные диагностические данные, необходимые для работы с квантовым адоном. В настоящий момент предусматривается возможность просмотра следующих видов информации:

- Общая информация.
- Диагностика СВКРК.

- Диагностика абонентских подключений.
- Диагностика клиентского режима.
- Диагностика ошибок.

Для последовательного переключения между указанными диагностическими окнами необходимо выбрать в выпадающем списке пункта «Следующий диагн. экран» и нажать кнопку «Команда», после чего нажать кнопку «Диагностика».

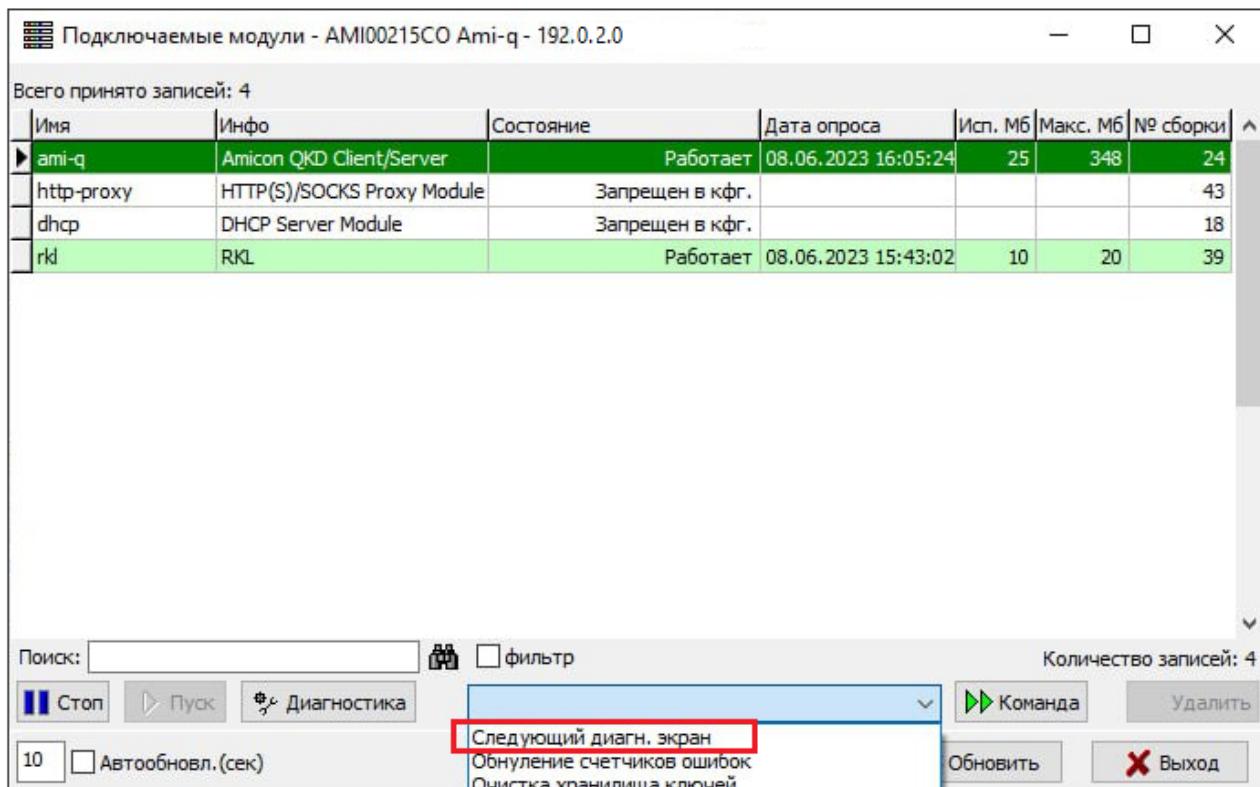


Рисунок 258 - Диагностика

На рисунке ниже представлено диагностическое окно СВКРК, открывающееся по кнопке «Диагностика» окна «Модули»:

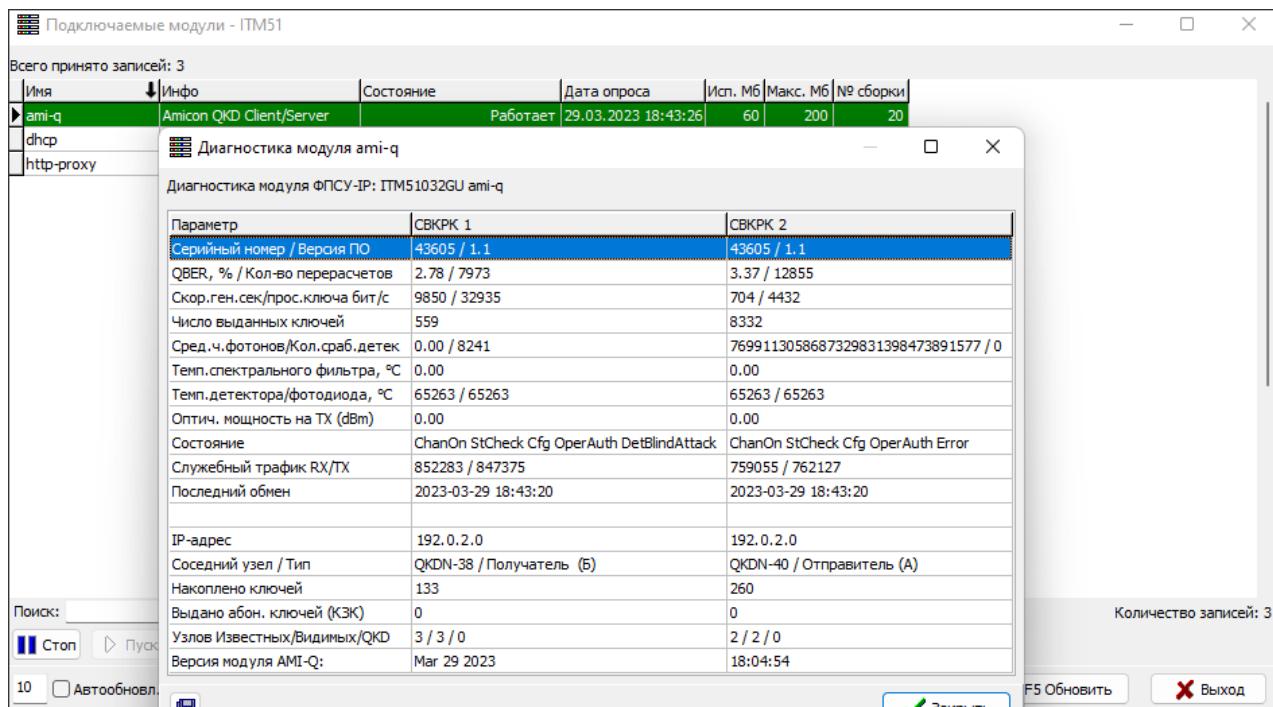


Рисунок 259 - Модули

В данном окне для модуля am-i-q отображается информация по подключенными к ФПСУ-IP устройствам СВКРК (устройства квантовой криптографической системы выработки и распределения ключей разработки ООО «СМАРТС-Кванттелеком»). Если записи пустые, то следует проверить подключение устройства СВКРК к ФПСУ-IP.

Описание выданных на ФПСУ-IP от устройств СВКРК параметров рекомендуется смотреть к документации на устройство СВКРК.

Для каждого подключенного СВКРК отображается в соответствующем ему столбце следующая информация:

- Серийный номер устройства СВКРК и версия его программного обеспечения;
- QBER, %, коэффициент квантовых ошибок по битам (описание допустимых значений параметра см. в руководстве на СВКРК);
- Скорость просеивания ключей для получения секретного квантового ключа (описание допустимых значений параметра см. в руководстве на СВКРК);
- Число выданных квантовых ключей;
- Среднее число фотонов и количество срабатываний детектора фотонов;
- температура детектора и оптического модуля (описание допустимых значений

параметра см. в руководстве на СВКРК);

- оптическая мощность приема и передачи в канале между устройствами СВКРК (описание допустимых значений параметра см. в руководстве на СВКРК);
- слово состояния (описание значений параметра см. в руководстве на СВКРК);
- служебный трафик RX/TX между устройствами СВКРК, прием и передача;
- дата последнего обмена между устройствами СВКРК.

Со строки «IP-адрес» указывается хранящаяся на ФПСУ-IP информация:

- IP-адрес устройства СВКРК;
- зарегистрированные за соседним узлом тип и номер узла в квантовой сети;
- счетчики полученных от устройства СВКРК квантовых ключей, накопленных на ФПСУ-IP на текущий момент;
- количество выданных другим абонентам квантово-защищенных ключей;
- общее сведение о количестве узлов в квантовой сети;
- версия модуля AMI-Q, дополнения, обеспечивающего поддержку работы ФПСУ-IP с устройствами СВКРК и построения VPN-туннелей на квантовых и/или квантово-защищенных ключах.

16.4. Настройка пороговых значений по умолчанию

Чтобы выбрать ряд событий на ФПСУ-IP, о которых УА ФПСУ-IP будет оперативно оповещать администратора, настраивается система пороговых значений, по достижению которых ФПСУ-IP будет отправлять УА ФПСУ-IP заданное оповещение.

Для удобства управления может быть сначала задана стандартная схема оповещений, которая потом может быть распространена на все зарегистрированные ФПСУ-IP. Для настройки пороговых значений по умолчанию, необходимо выполнить команду главного меню «Параметры» → «Пороговые значения по умолчанию...». На экране появится окно, содержащее список событий, на которые может быть выдана графическая и звуковая сигнализация, и поля для ввода количественных или временных параметров.

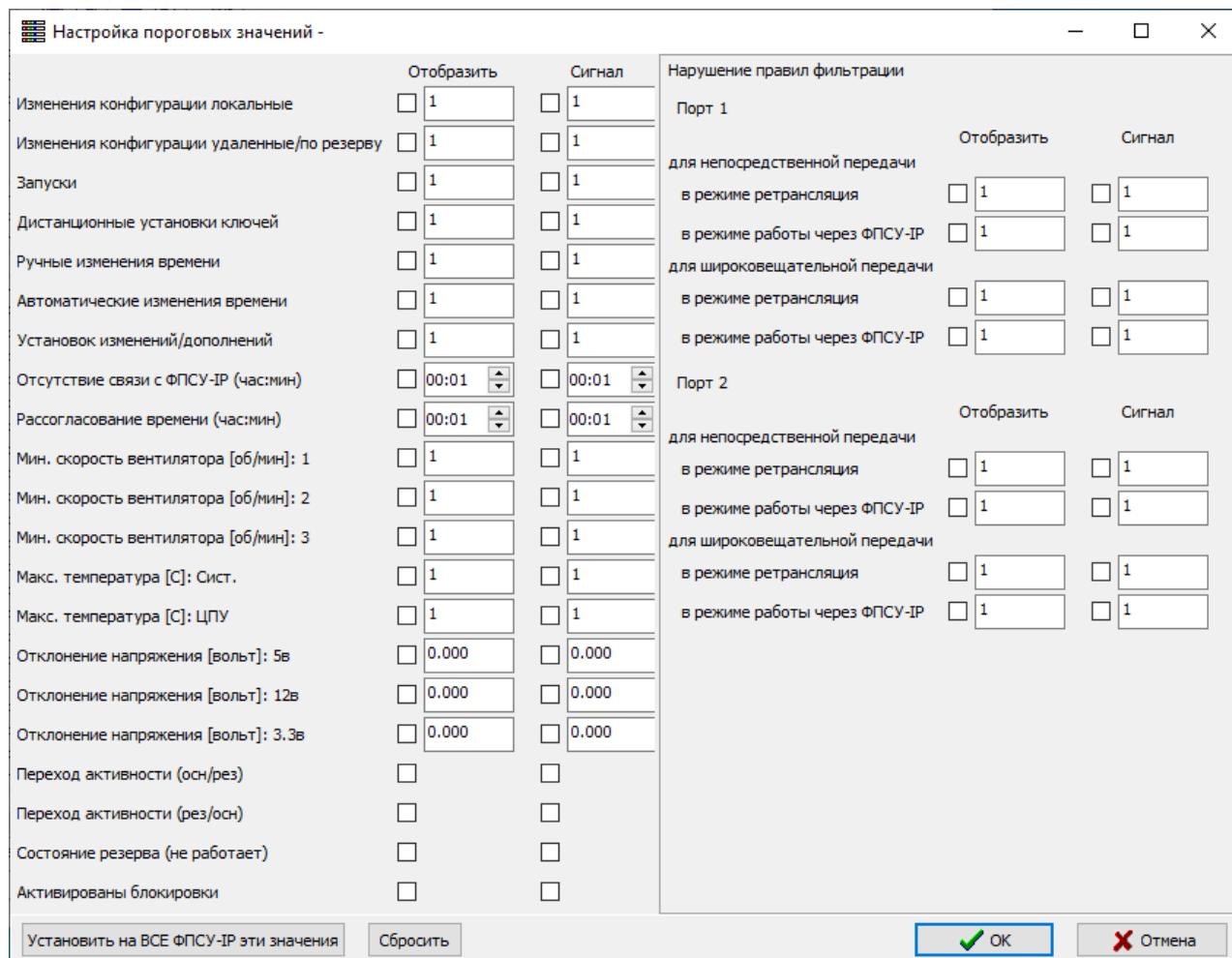


Рисунок 260 - Настройка пороговых значений по умолчанию

В колонку «Отобразить» необходимо ввести количество событий или период времени, по истечении которых последует графическая сигнализация - на изображении ФПСУ-IP в списке будет отображаться восклицательный знак. Чтобы сделать режим отображения каждого события активным, необходимо установить флаг в соответствующей строке.

В колонку «Сигнал» следует проставить количество событий или период времени, по истечении которых УА ФПСУ-IP выдаст звуковое сообщение. Звуковые оповещения выбираются в окне установки сигналов пороговых значений, вызываемое командой главного меню «Параметры» → «Сигналы пороговых значений...».

Включение режимов сигнализации на количество нарушений правил фильтрации, превышающее задаваемое пороговое значение, производится отдельно для каждого из портов ФПСУ-IP (логические номера портов выдаются в соответствии с конфигурацией

ФПСУ-IP).

Оперативная графическая и звуковая реакция УА ФПСУ-IP может быть запрограммирована на следующие события:

- перезапуск подсистемы фильтрации ФПСУ-IP;
- нарушение правил фильтрации на каждом из портов ФПСУ-IP как для индивидуальных IP-пакетов, так и для широковещательных передач;
- изменение конфигурации как локальными, так и администраторами УА ФПСУ-IP;
- дистанционная установка ключевых данных;
- дистанционное изменение времени вручную или в результате автокоррекции;
- установка изменений/дополнений к ПО ФПСУ-IP;
- отсутствие связи с ФПСУ-IP в течение некоторого времени;
- рассогласование текущего времени УА ФПСУ-IP и ФПСУ-IP;
- изменение аппаратных характеристик ФПСУ-IP: снижение скорости вентиляторов, повышение температуры процессора и системной платы, отклонение напряжений системного блока;
- изменение статуса резервирования.

Кнопка «Установить на ВСЕ ФПСУ-IP эти значения» устанавливает выставленные параметры пороговых значений на все ФПСУ-IP, зарегистрированные в УА ФПСУ-IP.

Внимание! Такая установка перезапишет ранее произведенные индивидуальные настройки на всех ФПСУ-IP!

Кнопка «Сбросить» снимает отметки о всех событиях в данном окне.

16. 4. 1. Установка типов сигналов о событиях

УА ФПСУ-IP позволяет для каждого вида событий на ФПСУ-IP назначить разные оповещения: уникальный звуковой сигнал, запуск указанной программы, отправку сообщения на почту.

Для установки типов сигналов необходимо выполнить команду главного меню «Параметры → Сигналы пороговых значений...». На экране монитора появится окно «Сигналы событий мониторинга», содержащее список событий, идентичный списку из окна «Настройка пороговых значений».

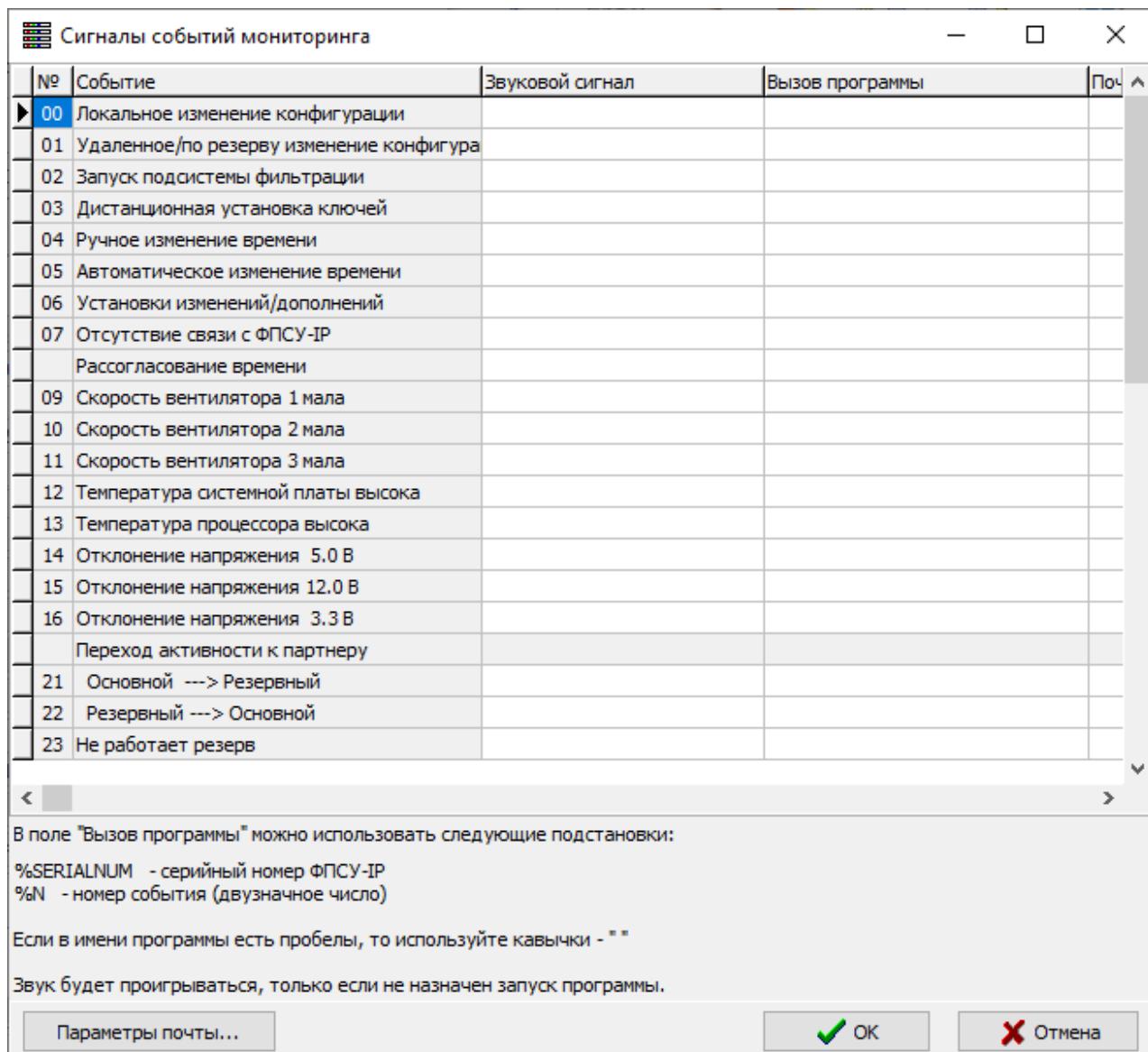


Рисунок 261 - Сигналы событий мониторинга

Для установки звукового оповещения необходимо выбрать отслеживаемое событие из списка и два раза нажать левой клавишей мыши поле строки события «Звуковой сигнал». УА ФПСУ-IP предложит выбрать сигнал оповещения из списка звуковых файлов, которые хранятся в подкаталоге Sound основного каталога УА ФПСУ-IP. Поддерживаемые форматы звуковых файлов — .MIDI, .WAV.

При наступлении каждого вида событий из списка может быть запущена какая-либо сторонняя программа. Полное имя программы (содержащее путь к ней) указывается для выбранного события, в поле «Вызов программы» строки, например «C:\ARM SCRIPTS\TimeAlert.bat».

В командной строке могут быть использованы подстановочные параметры «%SERIALNUM» и «%N», которые при вызове программы будут заменены на серийный номер ФПСУ-IP (на котором произошло событие) и номер события соответственно. Подстановочные параметры вводятся в поле «Вызов программы».

Для отправки сообщения на электронную почту при наступлении события, следует указать в поле «Почта» строки события электронный адрес. Чтобы УА ФПСУ-IP смог отправлять сообщения на адрес электронной почты, требуется выполнить предварительную настройку параметров почты УА ФПСУ-IP.

Для установки параметров почты УА ФПСУ-IP, необходимо нажать кнопку «Параметры почты» окна сигналов событий мониторинга. В появившемся окне настроек требуется указать следующие параметры:

- SMTP сервер;
- Порт сервера;
- Отправитель;
- Пользователь;
- Пароль.

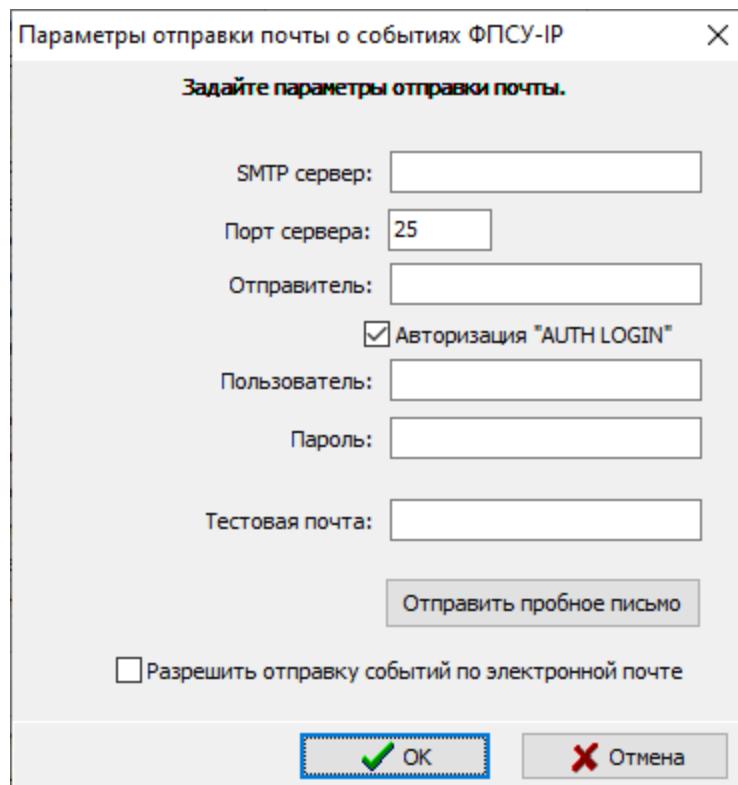


Рисунок 262 - Установка параметров почты УА ФПСУ-IP

Внимание! Очередь на передачу писем не сохраняется от сессии к сессии УА ФПСУ-IP, при перезапуске УА ФПСУ-IP не доставленные сообщения пропадают. Доставка почты получателю о событиях на ФПСУ-IP не гарантируется ввиду возможности сбоев или недоступности почтового сервера.

16. 4. 2. Настройка пороговых значений на ФПСУ-IP

Если для отдельных ФПСУ-IP требуются специальные настройки пороговых значений, отличные от настроек по умолчанию, администратор может их внести для каждого такого ФПСУ-IP самостоятельно.

Для этого следует в окне списка выбрать ФПСУ-IP, для которого требуется изменить пороговые значения по умолчанию, и нажать кнопку «Пороговые значения» панели команд.

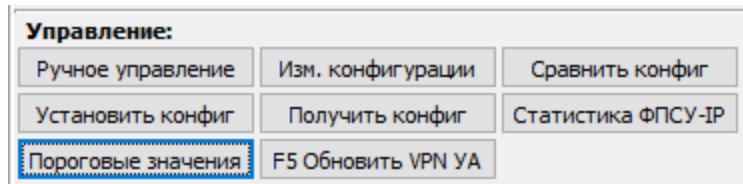


Рисунок 263 - Кнопка «Пороговые значения» панели команд

Будет вызвано служебное окно настройки пороговых значений выбранного ФПСУ-IP, аналогичное окну настроек значений по умолчанию. Администратор УА ФПСУ-IP в нем может внести специальные настройки пороговых значений.

Для обратной установки специальных параметров в значения по умолчанию, следует нажать кнопку «Установить в значения по умолчанию».

Настройка	Отобразить	Сигнал
Изменения конфигурации локальные	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Изменения конфигурации удаленные/по резерву	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Запуски	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Дистанционные установки ключей	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Ручные изменения времени	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Автоматические изменения времени	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Установок изменений/дополнений	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Отсутствие связи с ФПСУ-IP (час:мин)	<input type="checkbox"/> 00:01	<input type="checkbox"/> 00:01
Рассогласование времени (час:мин)	<input type="checkbox"/> 00:01	<input type="checkbox"/> 00:01
Мин. скорость вентилятора [об/мин]: 1	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Мин. скорость вентилятора [об/мин]: 2	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Мин. скорость вентилятора [об/мин]: 3	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Макс. температура [С]: Сист.	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Макс. температура [С]: ЦПУ	<input type="checkbox"/> 1	<input type="checkbox"/> 1
Отклонение напряжения [вольт]: 5в	<input type="checkbox"/> 0.000	<input type="checkbox"/> 0.000
Отклонение напряжения [вольт]: 12в	<input type="checkbox"/> 0.000	<input type="checkbox"/> 0.000
Отклонение напряжения [вольт]: 3.3в	<input type="checkbox"/> 0.000	<input type="checkbox"/> 0.000
Переход активности (осн/рез)	<input type="checkbox"/>	<input type="checkbox"/>
Переход активности (рез/осн)	<input type="checkbox"/>	<input type="checkbox"/>
Состояние резерва (не работает)	<input type="checkbox"/>	<input type="checkbox"/>
Активированы блокировки	<input type="checkbox"/>	<input type="checkbox"/>

Нарушение правил фильтрации

Порт 1

Настройка	Отобразить	Сигнал
для непосредственной передачи	<input type="checkbox"/> 1	<input type="checkbox"/> 1
в режиме ретрансляция	<input type="checkbox"/> 1	<input type="checkbox"/> 1

Порт 2

Настройка	Отобразить	Сигнал
для непосредственной передачи	<input type="checkbox"/> 1	<input type="checkbox"/> 1
в режиме ретрансляция	<input type="checkbox"/> 1	<input type="checkbox"/> 1

Рисунок 264 - Настройка пороговых значений на отдельном ФПСУ-IP

16. 5. Сообщения от ФПСУ-IP

Отдельный журнал ведется относительно сообщений, отправляемых ФПСУ-IP к УА ФПСУ-IP. Окно со списком таких сообщений вызывается командой главного меню «Вид → Сообщения от ФПСУ-IP...», и содержит следующую информацию:

- поле «Посл. серийный №», в котором отображается серийный номер ФПСУ-IP, отправившего сообщение;
- тип полученного сообщения;
- количество сообщений;
- дата и время получения УА ФПСУ-IP сообщения.

Сообщения от ФПСУ-IP			
Посл. серийный №	Тип сообщения	Количество	Время
AMI00231CO	Перекл. Основной <-- Резервный	1	07.04.2023 14:10:24
AMI00231CO	Перекл. Основной --> Резервный	1	07.04.2023 13:53:28
AMI00231CO	Дамп памяти на ФПСУ-IP	1	07.04.2023 13:49:40
AMI00231CO	Активация обновления	1	07.04.2023 11:36:42

Серийный №	Имя ФПСУ-IP	Тип сообщения	Время
AMI00231CO	AMI00231CO FPSU-IP	Перекл. Основной <-- Резервный	07.04.2023 14:10:24

Подробно

Перекл. Основной <-- Резервный
Получено 07.04.2023 14:10:24
от ФПСУ-IP AMI00231CO
AMI00231CO FPSU-IP
01.04.2023 04:57:20
произошло переключение ФПСУ-IP
в направлении Резервный ---> Основной
Дополнительная информация:

Рисунок 265 - Окно списка сообщений от ФПСУ-IP

В нижней части окна выводится подробный текст сообщения, присланный ФПСУ-IP на УА ФПСУ-IP.

Кнопка очищает весь список сообщений от ФПСУ-IP.

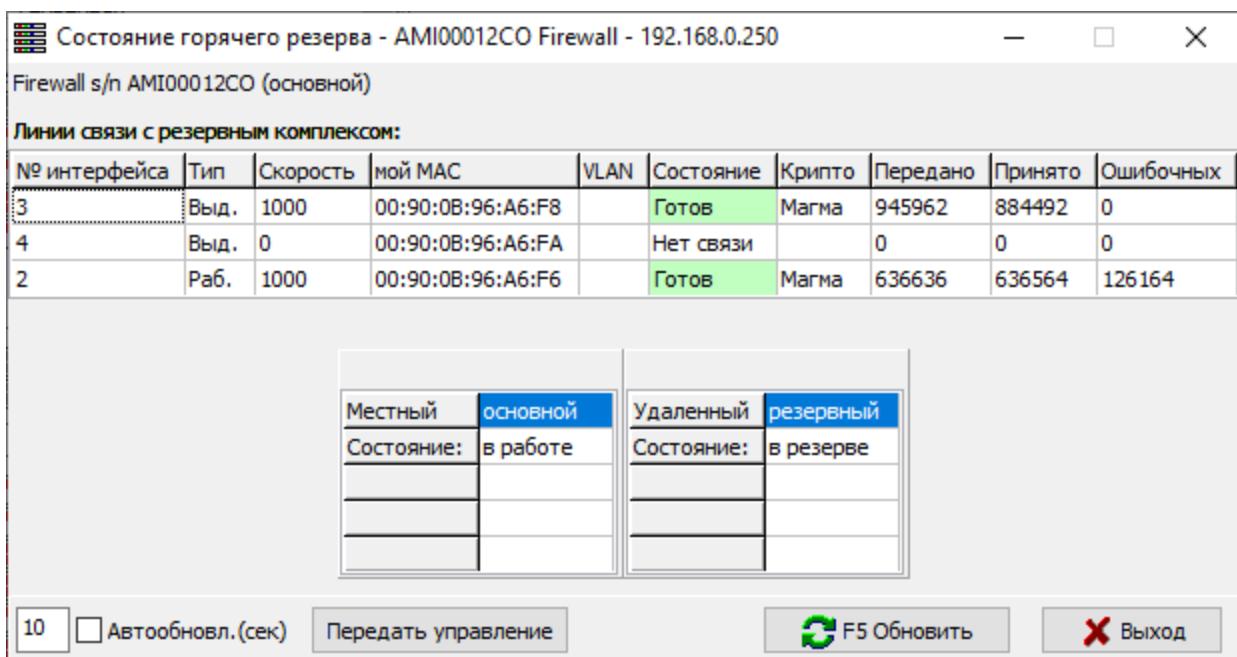
16. 6. Получение данных о состоянии «горячего» резервирования

Для просмотра состояния «горячего» резервирования на выбранном ФПСУ-IP, следует нажать кнопку панели команд.

| Работает | **R** Основной | Резерв | работает |

Рисунок 266 - Состояние подсистемы горячего резерва

На экран будет выдано информационное окно, в верхней строке которого содержатся сведения об установках порта резервирования выбранного ФПСУ-IP и о скорости передачи данных по порту в Мбит/с. В таблице отображается регистрационная информация об обмене данными через порт.

**Рисунок 267 - Состояние подсистемы горячего резерва**

В столбце состояние отображается состояние VPN-туннеля «горячего резерва» (защищённого канала связи между ФПСУ-IP и его партнёром по резервированию). Туннель может находиться в следующих состояниях:

- «Устанавливается» - начал процесс установки туннеля.
- «Готов» - туннель установлен и по нему происходит обмен служебной информацией.
- «Нет связи» - канал связи между двумя ФПСУ-IP не установлен физически (ФПСУ-IP выключен, соединительный кабель не подключен или неисправен и т.д.) или на партнёре горячего резерва не запущена подсистема фильтрации.
- «Нет связи (не согласован ключ)» - канал связи не может быть установлен по причине ошибки аутентификации, необходимо переустановить ключи горячего

резерва.

- «Нет связи (ошибка установки)» - канал связи не может быть установлен по причине ошибочных установок (например, различных MAC-адресов для одноимённых портов ФПСУ-IP).

Далее выводятся данные о состоянии ФПСУ-IP и его партнёра горячего резерва (если он на связи с выбранным ФПСУ-IP): текущее время, функциональный статус («основной» или «резервный»), аппаратный адрес портов резервирования, текущее состояние каждого ФПСУ-IP в процессе резервирования («в работе» или «в резерве»), а также оценка их работоспособности.

Чтобы обновить полученные от ФПСУ-IP сведения, следует нажать кнопку «F5 Обновить» или выставить флагок «Автообновление», указав интервал времени, через который будут производиться повторные запросы.

Чтобы изменить функциональный статус ФПСУ-IP, необходимо войти в режим ручного управления ФПСУ-IP и нажать на кнопку «Передать управление резерву».

16. 7. Диагностика ошибок с помощью mlog

Зарегистрированные события на ФПСУ-IP могут быть выданы в текстовом формате. Подпрограмма mlog записывает события в журнал, который может быть использован для диагностики и выявления ошибок при старте ФПСУ-IP, запуске аддонов, установлении соединений, установлении туннелей с другими ФПСУ, подключении Клиентов и при других событиях ФПСУ.

Подпрограмма mlog.dsr доставляется на ФПСУ следующими способами:

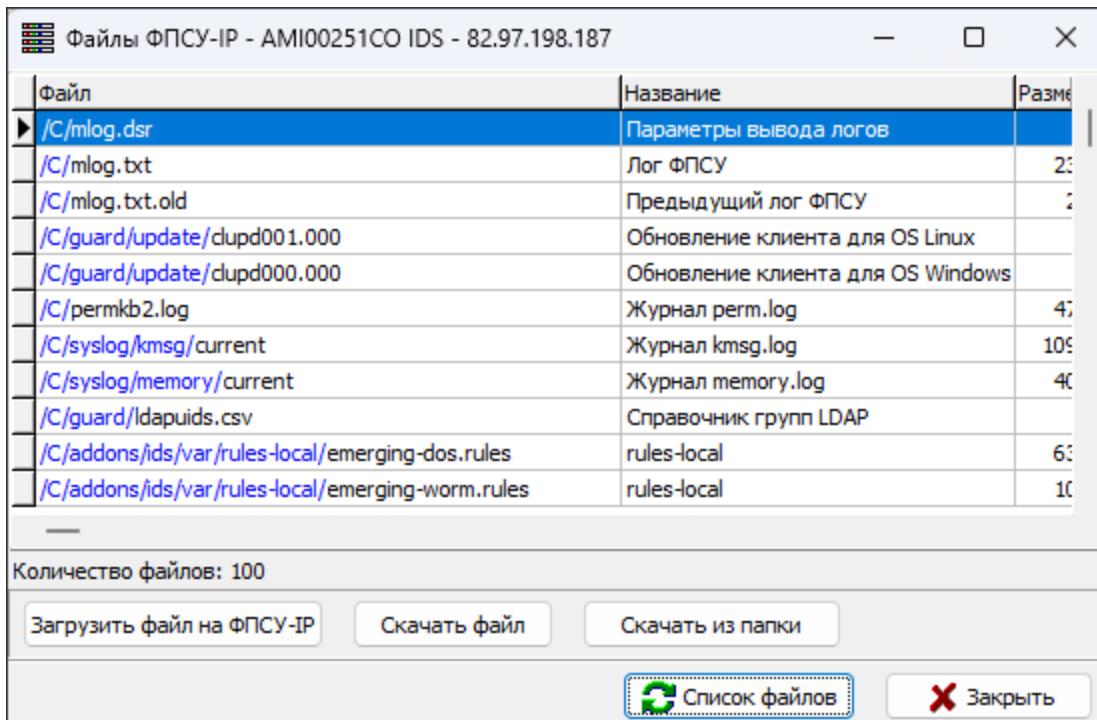
- подключением к USB-порту ФПСУ-IP USB-носителя с утилитой mlog.dsr в корне;
- загрузкой на ФПСУ-IP утилиты mlog.dsr через программу «Удаленный администратор ФПСУ» по кнопке «Файлы» на панели команд.

Для ФПСУ-IP версии 4.0 базовая версия утилиты mlog уже загружена в память ФПСУ-IP в «/C», в этом случае загрузка через программу УА ФПСУ не требуется.

Запись журнала ведется в файл mlog.txt, данная запись называется текущим логом. После начала записи лога существующий файл mlog.txt становится предыдущим логом и изменяет название на mlog.txt.old, при этом новый вывод mlog становится текущим.

Для записи лога с помощью УА ФПСУ-IP необходимо выполнить следующие действия:

1. На панели команд нажать кнопку «Файлы». Проверить количество необходимой информации в базовом файле mlog.dsr.

**Рисунок 268 - Состояние подсистемы горячего резерва**

2. Выполнить перезагрузку ФПСУ-IP нажатием кнопки «Перезагрузить ОС ФПСУ-IP» (см. п. «Дистанционная перезагрузка ОС ФПСУ-IP»).
3. После перезагрузки ФПСУ-IP информация будет записана в лог ФПСУ. Повторная перезагрузка позволит обновить файл mlog.txt.

После повторной перезагрузки ФПСУ-IP в окне «Файлы ФПСУ-IP» необходимо выбрать mlog.txt и нажать на кнопку «Скачать файл». В дальнейшем предоставляется возможность передать полученный файл в службу технической поддержки.

Для получения дополнительной информации служба технической поддержки дополняет файл mlog.dsr необходимыми параметрами и передает его пользователю. В этом случае необходимо дополнить последовательность действий следующими:

4. В окне «Файлы» выбрать /C/mlog.dsr и нажать на кнопку «Загрузить файл на ФПСУ-IP». Далее в стандартном окне выбора необходимо указать путь к полученному файлу и подтвердить его установку на ФПСУ.
5. Выполнить перезагрузку ФПСУ-IP нажатием кнопки «Перезагрузить ОС ФПСУ-IP» (см. п. «Дистанционная перезагрузка ОС ФПСУ-IP»).
6. После перезагрузки ФПСУ-IP информация будет записана в лог ФПСУ. Повторная перезагрузка позволит обновить файл mlog.txt.

После повторной перезагрузки ФПСУ-IP в окне «Файлы ФПСУ-IP» необходимо выбрать mlog.txt и нажать на кнопку «Скачать файл».

17. Ключи УА

17. 1. Управление VPN-Key/UA

Во время работы с УА ФПСУ-IP администратор может получить справочную информацию о подключенном VPN-Key/UA, выполнив команду главного меню «Ключ УА» → «Информация о USB-ключе и лицензии...».

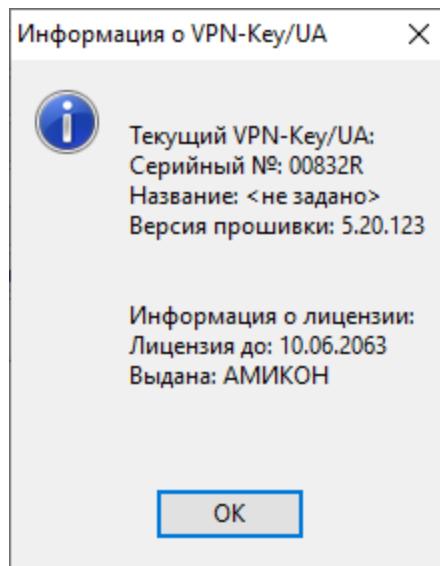


Рисунок 269 - Информация о VPN-Key/UA

Кроме того, администратору предоставляется возможность добавить необязательное текстовое имя VPN-Key/UA, которое будет хранится только на УА ФПСУ-IP, выполнив команду главного меню «Ключ УА» → «Задать имя текущего ключа...».

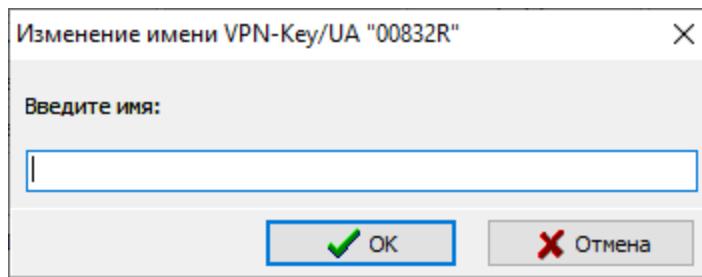


Рисунок 270 - Задание текстового имени VPN-Key/UA

17. 1. 1. Работа УА ФПСУ-IP с несколькими VPN-Key/UA

УА ФПСУ-IP поддерживает режим работы с несколькими VPN-Key/UA одновременно. При этом потребуется вводить PIN-коды всех устройств во время запуска УА ФПСУ-IP.

При одновременной работе с несколькими VPN-Key/UA, администратор УА ФПСУ-IP может выбирать, из какого VPN-Key/UA брать данные для установления защищенного соединения с ФПСУ-IP. По умолчанию, соединение будет устанавливаться с помощью того VPN-Key/UA, PIN-код которого первым был затребован при запуске УА ФПСУ-IP.

Для изменения порядка соединения с ФПСУ-IP при одновременном использовании нескольких VPN-Key/UA, необходимо выполнить команду основного меню «Ключ УА» → «Используемые УА». Появится окно привязки учетной записи администратора к ФПСУ-IP, в котором можно выбрать, какие администраторы УА ФПСУ-IP будут работать с какими ФПСУ-IP.

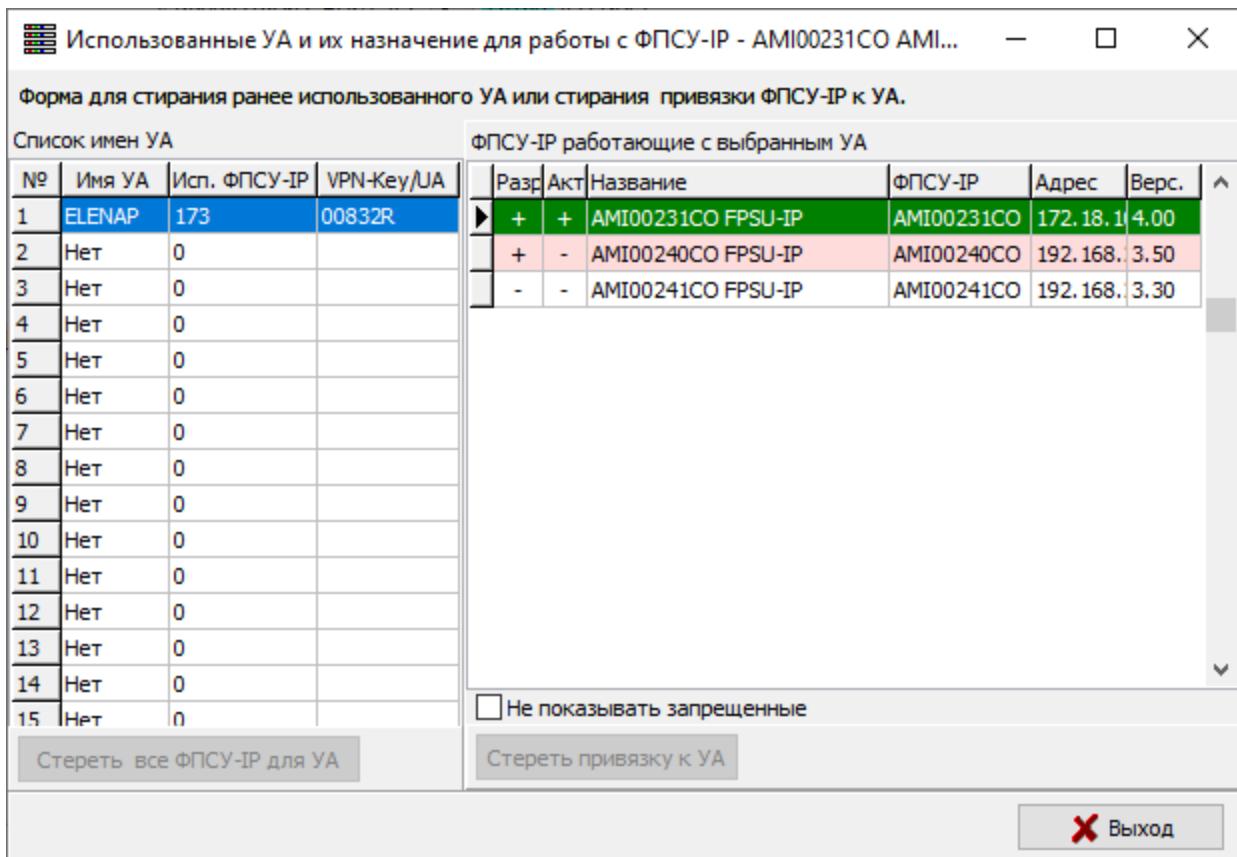


Рисунок 271 - Выбор администраторов УА ФПСУ-IP

17. 1. 2. Пересоздание ключевых данных администратора УА ФПСУ-IP

Администратор УА ФПСУ-IP может посмотреть текущие параметры VPN-Key/UA и привязанной к нему учетной записи администратора УА ФПСУ-IP, выполнив команду основного меню «Ключ УА»→«Просмотр/изменение ключа УА».

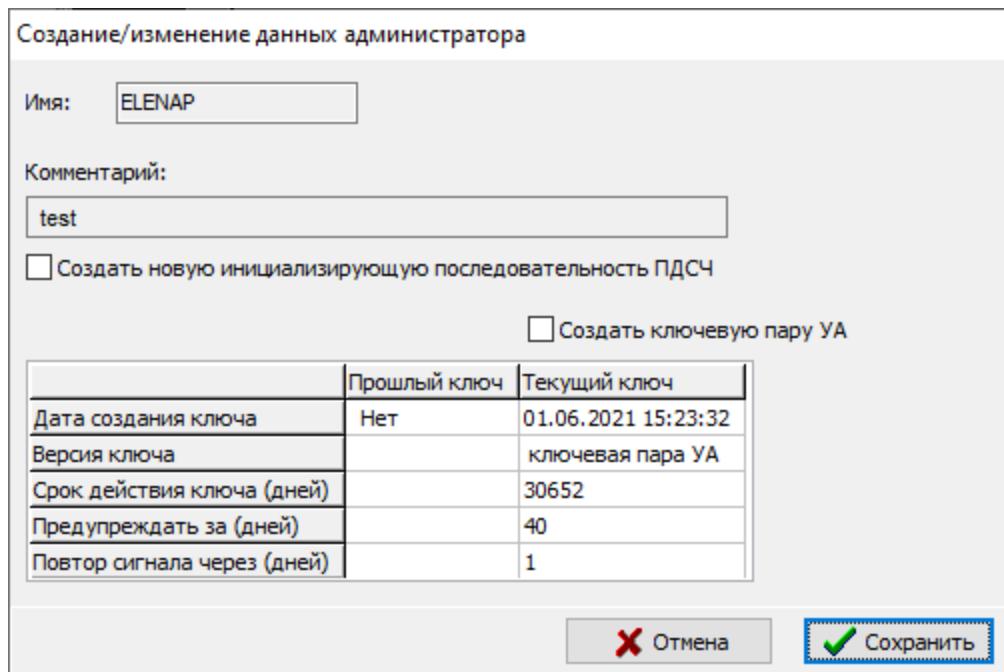


Рисунок 272 - Создание/изменение ключа УА

В открывшемся окне будут указаны имя администратора, комментарий к нему, дата создания ключа (для предыдущих версий) и ключевой пары УА ФПСУ-IP, а также срок действия ключей ключевой пары.

Для пересоздания ключевых данных необходимо установить флаг «Создать ключевую пару УА» и нажать кнопку «Сохранить».

17. 1. 3. Управление доступом к базе данных УА ФПСУ-IP

База данных УА ФПСУ-IP хранится на внутреннем накопителе рабочей станции в зашифрованном состоянии. Доступом к базе данных УА ФПСУ-IP по умолчанию управляет первый администратор УА ФПСУ-IP, созданный при первом запуске (см. пункт «Первоначальная настройка УА ФПСУ-IP (с VPN-Key/UA)»).

Переход в окно управления ключом шифрования базы данных УА ФПСУ-IP осуществляется по команде главного меню «Ключ УА» → «Доступ УА к ключу шифрования БД».

В открывшемся окне можно посмотреть, каким администраторам УА ФПСУ-IP уже был предоставлен доступ к базе данных данного УА ФПСУ-IP (по умолчанию там будет одна запись с именем администратора УА ФПСУ-IP, созданным при первом запуске УА ФПСУ-IP).

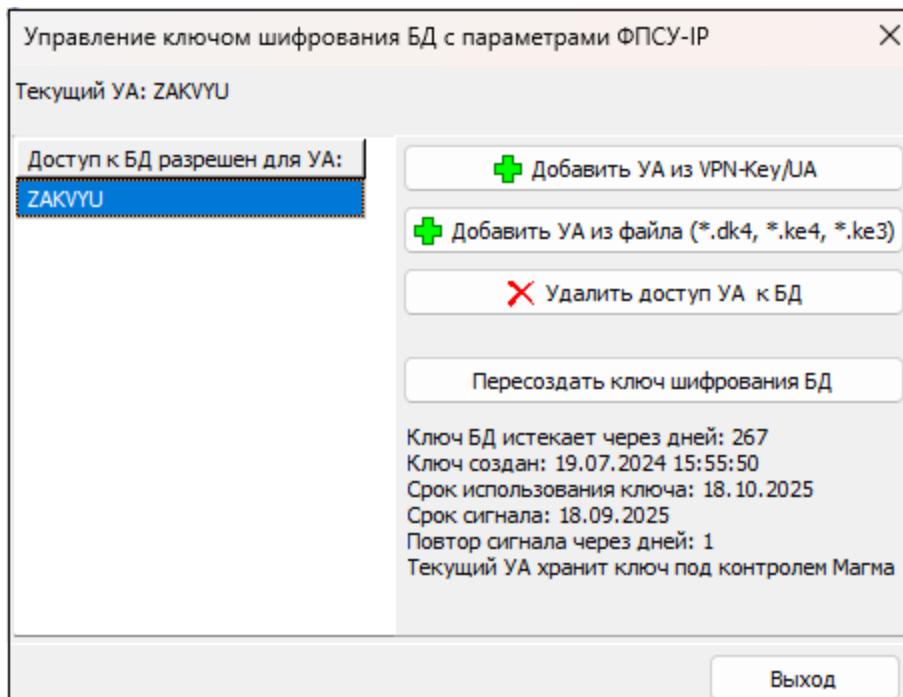


Рисунок 273 - Окно управления ключом шифрования БД УА ФПСУ-IP

Доступ к базе данных УА ФПСУ-IP может быть предоставлен другим администраторам УА ФПСУ-IP, с помощью командных кнопок «Добавить УА из VPN-Key/UA» и «Добавить УА из файла».

Команда «Добавить УА из VPN-Key/UA» добавляет доступ к базе данных учетной записи администратора УА ФПСУ-IP, чей VPN-Key/UA сейчас подключен к УА ФПСУ-IP.

Команда «Добавить УА из файла» требует указать файл со служебными данными администратора УА ФПСУ-IP, находящийся в файле. Этот файл должен быть получен от другого администратора УА ФПСУ-IP заранее.

Команда «Пересоздать ключ шифрования» используется для повторного создания ключа шифрования базы данных УА ФПСУ-IP, по причине истечения срока действия предыдущего ключа или его компрометации. По вызову команды, интерфейс УА ФПСУ-IP предупреждает, что при этой операции потребуется повторно зарегистрировать всех остальных администраторов УА ФПСУ-IP.

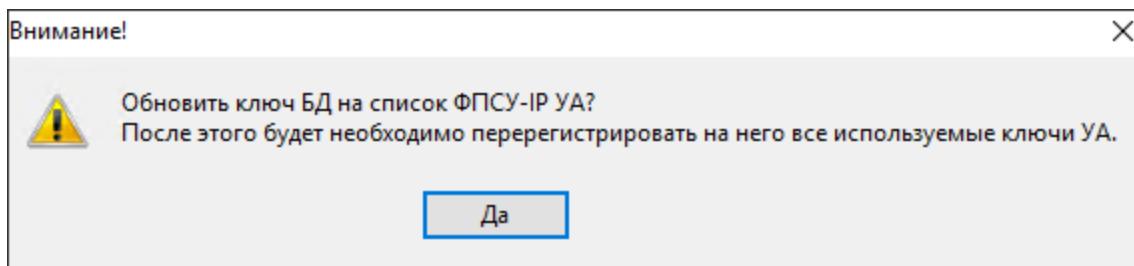


Рисунок 274 - Пересоздание ключа шифрования БД

Регистрация администратора из файла.

Для регистрации или перерегистрации после смены ключа шифрования БД администратора УА ФПСУ-IP в окне управления ключом шифрования БД УА ФПСУ-IP следует выбрать команду «Добавить УА из файла (*.dk, *.ke4, *.ke3)». Откроется стандартное окно выбора файла, следует выбрать файл .dk, .ke4 или .ke3.

На экран будет выдано окно со списком найденных файлов с ключами.

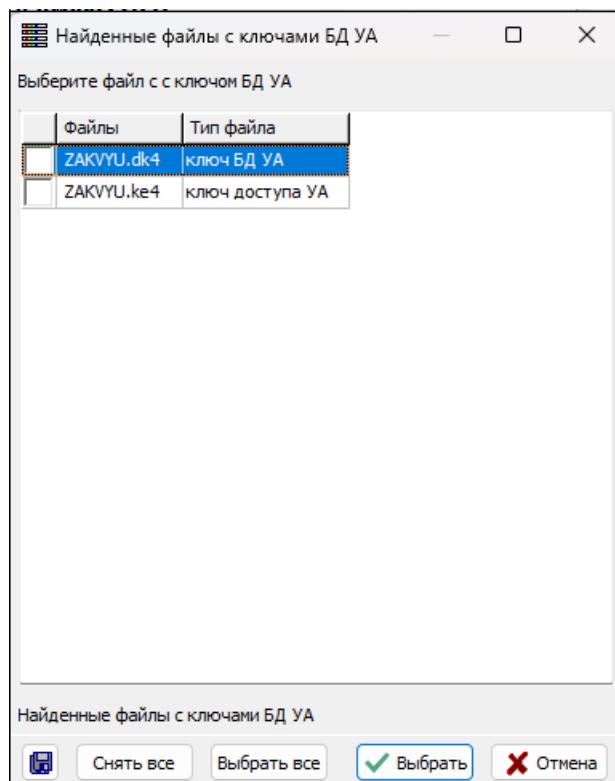


Рисунок 275 - Список файлов с ключами

В списке в строке с файлом регистрируемого администратора следует установить флаг

и нажать кнопку «Да». Регистрировать администраторов можно списком, отметив соответствующие файлы.

На экран будет выдано окно для подтверждения разрешения доступа к БД параметров ФПСУ-IP, следует разрешить доступ, нажав кнопку «Да».

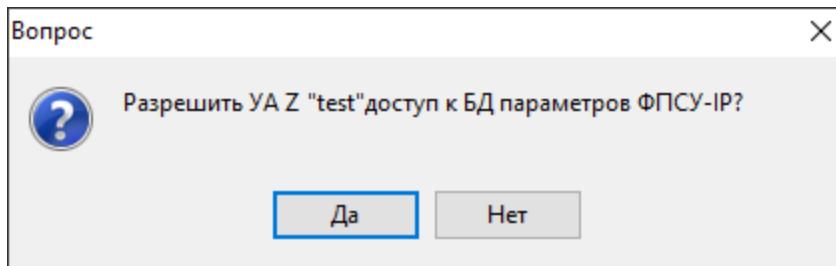


Рисунок 276 - Подтверждение доступа

В окне управления ключом шифрования БД УА ФПСУ-IP в списке администраторов отобразится зарегистрированный администратор.

17. 1. 4. Управление паролями

Для использования VPN-Key/UA с УА ФПСУ-IP требуется ввод специального пароля доступа к устройству.

VPN-Key/UA для УА ФПСУ-IP имеет две учетные записи с паролями доступа: «Пользователь», имеющий непривилегированные права на эксплуатацию VPN-Key/UA, и «Администратор», который может вносить изменения в конфигурацию VPN-Key/UA.

Для смены пароля учетной записи подключенного VPN-Key/UA необходимо:

1. Выполнить команду главного меню «Ключ УА» → «Изменить пароль пользователя USB-ключа» для смены пароля учетной записи «Пользователь» VPN-Key/UA (или команду «Ключ УА» → «Изменить пароль администратора USB-ключа» для смены пароля учетной записи «Администратор» VPN-Key/UA);
2. При появлении служебного сообщения «Изменение пароля USB ключа» убедиться в том, что к компьютеру подключен только один VPN-Key/UA и подтвердить начало операции смены пароля устройства.
3. Ввести текущий пароль учетной записи и нажать кнопку «OK»;
4. Установить новый пароль учетной записи VPN-Key/UA (длиной от 6 до 16 символов), дважды повторив его ввод, и нажать кнопку «OK»;
5. Нажать кнопку «OK» в появившемся окне «Пароль успешно изменен!».

Процедура смены пароля завершена.

По умолчанию, пароли для каждой учетной записи установлены в значения «1111» или «111111». После проведения этапа первоначальной настройки (см. раздел «Начало работы с УА ФПСУ-IP») УА ФПСУ-IP потребует сменить предустановленные пароли VPN-Key/UA. Действия по смене пароля идентичны описанным выше, начиная с п. 2.

17. 1. 5. Резервирование VPN-Key/UA

Для устранения последствий отказов работы, поставляемого с УА ФПСУ-IP VPN-Key/UA (следует иметь в виду что в случае отказа USB-ключа, УА ФПСУ-IP не сможет запуститься!), предусмотрено два механизма резервирования: восстановление с помощью специального файла — ключа УА, и запись данных УА в другой VPN-Key/UA.

Внимание! Для обеспечения возможности восстановления работы в случае программных или аппаратных ошибок, рекомендуется резервировать VPN-Key/UA хотя бы одним из перечисленных способов.

17. 1. 5. 1. Создание дубликата VPN-Key/UA

Создание дубликата VPN-Key/UA – запись системных данных администратора УА ФПСУ-IP (имени, ключа УА) в VPN-Key/UA с другим серийным номером. В этом случае при выходе из строя основного VPN-Key/UA, администратор сможет запустить УА ФПСУ-IP с помощью запасного, добавив в подкаталог LIC соответствующую лицензию (см. подраздел «Первый запуск УА ФПСУ-IP с VPN/Key UA»).

Для создания дубликата следует выполнить команду главного меню «Ключ УА» → «Записать УА из USB-ключа в USB-ключ». УА ФПСУ-IP предложит извлечь основной USB-ключ, и вставить тот, который требуется сделать запасным.

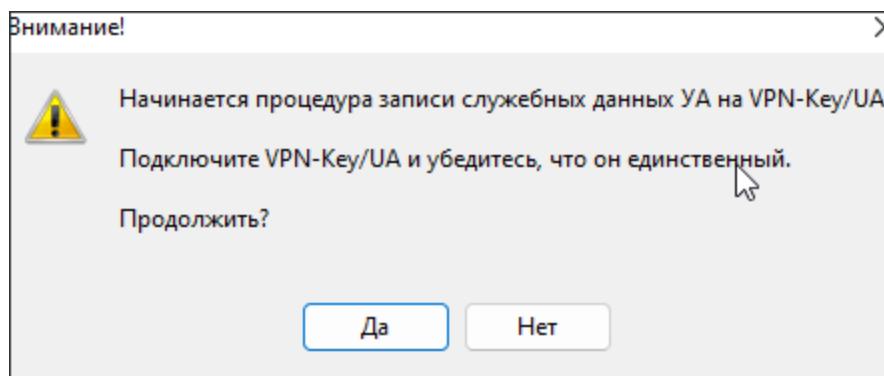
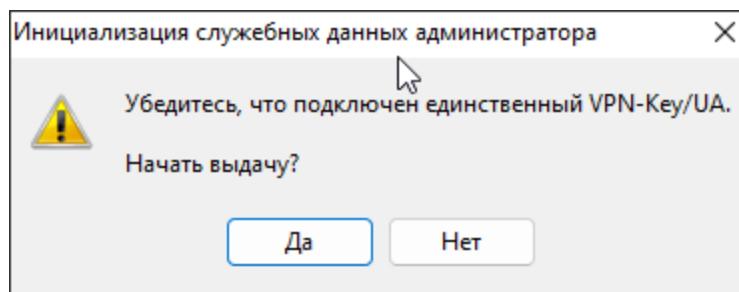


Рисунок 277 - Создание дубликата USB-ключа

После подключения к USB-порту VPN-Key/UA, который будет выполнять роль запасного, необходимо подтвердить начало выполнения инициализации копии ключа, нажав кнопку «Да».

Для подтверждения создания дубликата ключа необходимо нажать кнопку «Да» в новом служебном окне:

**Рисунок 278 - Подтверждение записи**

При успешном опросе ключа и нахождения корректного файла лицензии (см. подраздел «Первый запуск УА ФПСУ-IP с VPN/Key UA»), УА ФПСУ-IP предложит ввести PIN-код администратора VPN-Key/UA, которое будет выполнять роль запасного. После ввода PIN-кода необходимо нажать кнопку «OK». Если ввод PIN-кода осуществлён верно, в подключенный VPN-Key/UA будут записаны системные параметры администратора УА ФПСУ-IP. Далее необходимо извлечь подключенный VPN-Key/UA и вставить исходный USB-ключ администратора УА ФПСУ-IP. Процедура создания дубликата завершена, созданным USB-ключом можно будет воспользоваться при отказе основного.

17. 1. 5. 2. Резервирование с помощью ключа УА

Второй способ резервирования VPN-Key/UA предусматривает запись системных параметров администратора УА ФПСУ-IP в специальный файл — «Ключ УА», который служит специальным средством восстановления.

Для резервирования с помощью ключа УА требуется сначала сохранить его в файл для дальнейшего хранения на надежном носителе. При отказе основного VPN-Key/UA и отсутствии дубликата, с помощью файла ключа УА можно записать системную информацию администратора УА ФПСУ-IP на «чистый», не инициализированный ранее для этого администратора, USB-ключ.

Для выдачи ключа УА в файл следует выбрать команду меню «Ключ УА» → «Записать ключ УА в файл (*.ke4)». Последует вызов стандартного окна выбора каталога для выдачи файла ключа УА на внутренний накопитель или на внешний носитель.

ВНИМАНИЕ! Файл с открытым ключом не защищен от копирования и ответственность за его хранение и защиту от НСД несет администратор УА ФПСУ-IP!

Для восстановления с помощью файла ключа УА необходимо:

- при работе с VPN-Key/UA подключить новый VPN-Key/UA к USB порту компьютера, а лицензию на его использование поместить в подкаталог LIC рабочего каталога УА ФПСУ-IP;
- запустить УА ФПСУ-IP и ввести PIN-код пользователя подключенного VPN-Key/UA;
- УА ФПСУ-IP обнаружит отсутствие ключа УА в устройстве, и предложит инициализировать устройство заново;

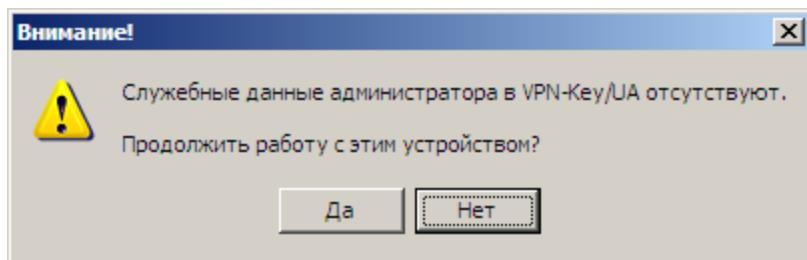


Рисунок 279 - Обнаружен VPN-Key/UA без данных администратора УА ФПСУ-IP

- на экран будет выведено окно установки параметров администратора УА ФПСУ-IP, в котором необходимо нажать на кнопку «Загрузить с диска» и указать в появившемся стандартном окне выбора каталога сохранённый ранее файл с ключом УА;

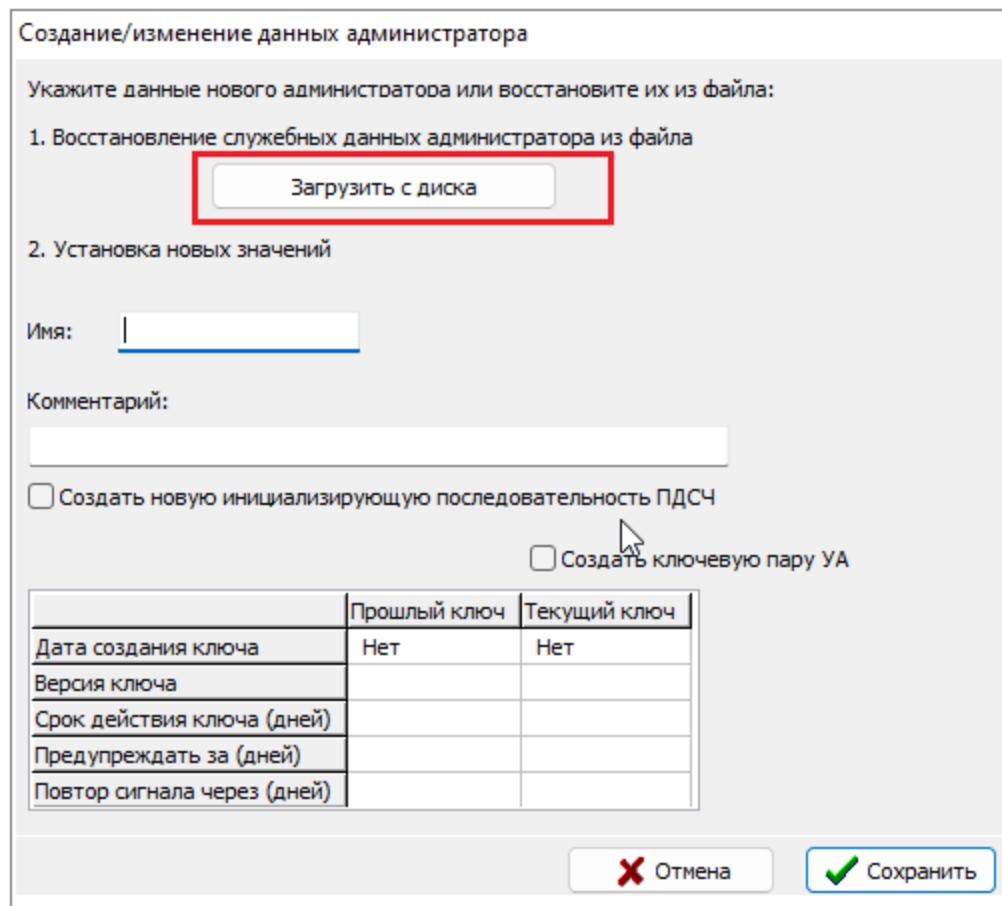


Рисунок 280 - Восстановление VPN-Key/UA с помощью ключа УА

- выбрав файл с ключевыми данными администратора УА ФПСУ-IP (файл с расширением «.ke2» или «.ke3»), подтвердить загрузку с указанного файла ключа УА. УА ФПСУ-IP выдаст параметры, найденные в файле ключе УА (имя и комментарий сохранённого в нём администратора УА ФПСУ-IP). Для подтверждения выбора необходимо нажать «Да»;
- в появившемся окне проверить ещё раз найденные параметры, и нажать кнопку «Сохранить» для начала записи найденных параметров в VPN-Key/UA;

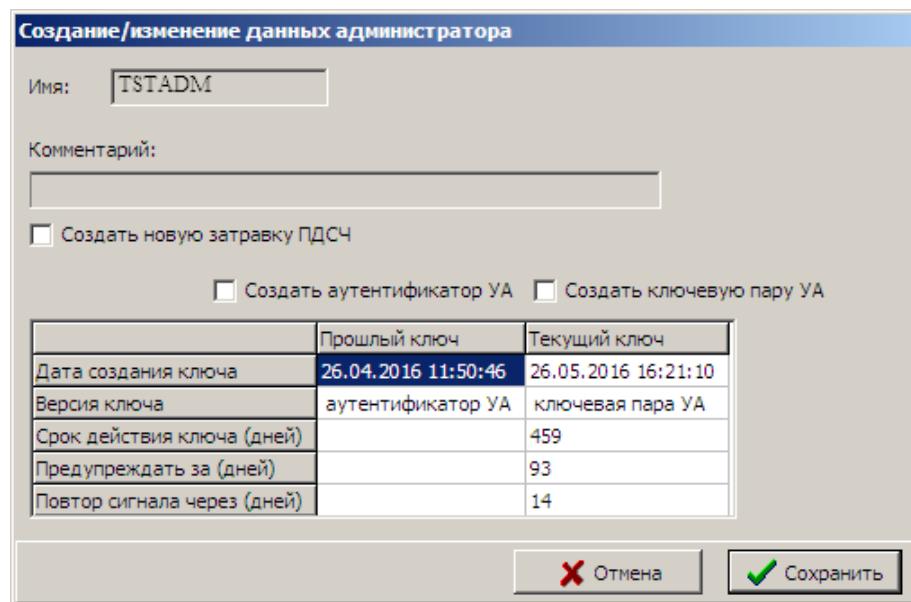


Рисунок 281 - Подтверждение загруженных данных

- перед записью потребуется провести повторную инициализацию датчика случайных чисел, как при создании администратора УА ФПСУ-IP (см. пункт «Первоначальная настройка УА ФПСУ-IP (с VPN-Key/UA)»);

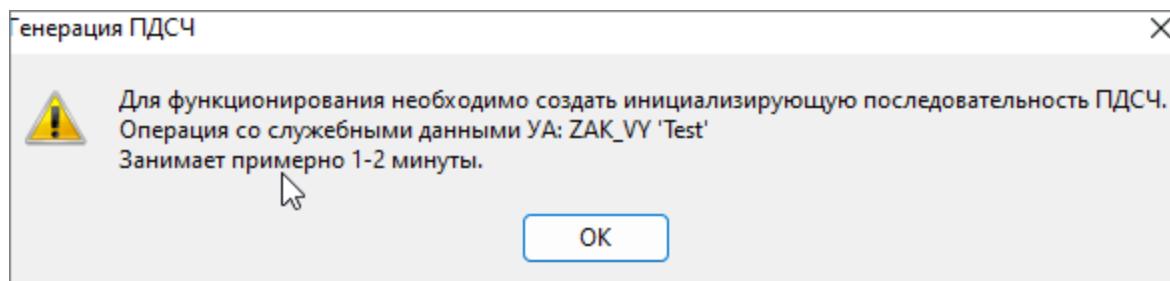


Рисунок 282 - Требуется инициализация датчика случайных чисел

- после инициализации датчика случайных чисел необходимо проверить, что в данный момент к USB-порту компьютера подключен единственный VPN-Key/UA, и нажать кнопку «Да» в появившемся служебном окне;

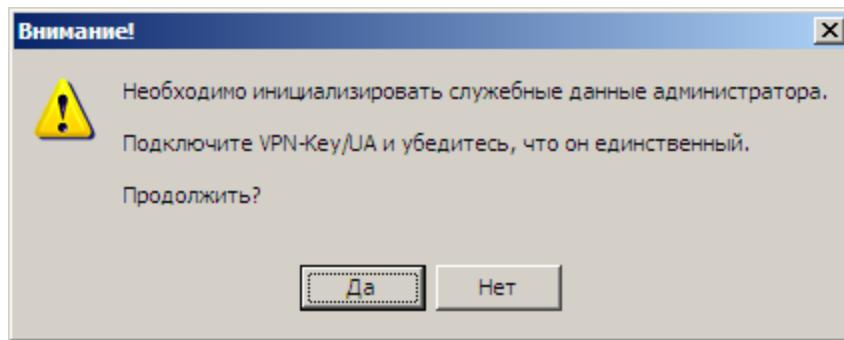


Рисунок 283 - Запись ключа УА в VPN-Key/UA

- УА ФПСУ-IP запросит PIN-код администратора для записи данных в VPN-Key/UA, и после его корректного ввода ключ будет инициализирован, по завершении будет выдано оповещение «Служебные данные администратора записаны в VPN-Key\UA».

Процедура восстановления VPN-Key/UA администратора УА ФПСУ-IP завершена, USB-ключом можно пользоваться в штатном режиме после перезапуска УА ФПСУ-IP.

17. 1. 6. Управление ключевыми данными администратора (при работе с VPN-Key)

Для управления ключами УА, записанными в VPN-Key/UA, следует использовать следующие команды меню «Ключ УА»:

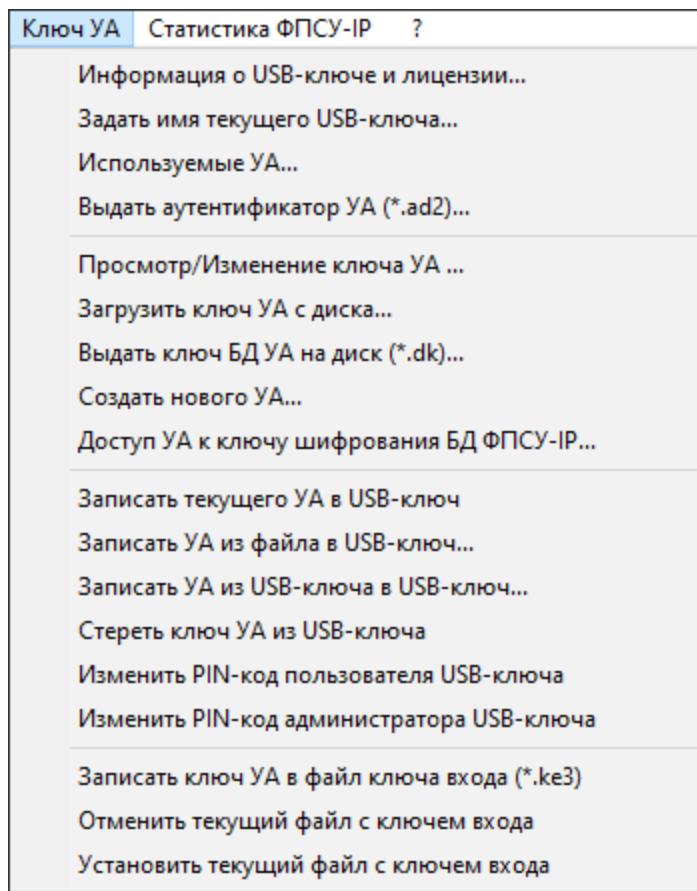


Рисунок 284 - Команды меню «Ключ УА»

- «Записать текущего УА в USB-ключ».

При одновременной работе с несколькими VPN-Key/UA, администратор УА ФПСУ-IP может свои данные записать в новый VPN-Key/UA. Для этого необходимо оставить подключенным к USB порту компьютера только один VPN-Key/UA, в которое будет записываться ключ текущего администратора УА ФПСУ-IP, и далее производить запись.

- «Записать УА из файла в USB-ключ».

Для записи ключа администратора УА ФПСУ-IP из файла следует в открывшемся стандартном окне выбрать файл с ключевыми данными формата .ke2 подключить к USB порту компьютера VPN-Key/UA, в который будет записываться выбранный ключ администратора УА ФПСУ-IP, и далее производить запись.

- «Записать УА из USB-ключа в USB-ключ».

Создание дубликата ключа администратора УА ФПСУ-IP подробно изложено в

пункте «Создание дубликата VPN-Key/UA».

- «Стереть ключ УА из USB-ключа».

Для очистки ключевых данных на VPN-Key/UA следует воспользоваться данной командой.

17.2. Управление ключевыми данными администратора УА ФПСУ-IP (без VPN-Key/UA)

Для управления ключами УА, записанными в VPN-Key/UA, следует использовать следующие команды меню «Ключ УА»:

- «Просмотр/Изменение ключа УА». Предназначена для просмотра текущих параметров ключа УА и привязанной к нему учетной записи администратора УА ФПСУ-IP (см. п. «Пересоздание ключевых данных администратора УА ФПСУ-IP»);
- «Загрузить ключ УА с диска». Предназначена для загрузки ключа администратора УА ФПСУ-IP из файла в VPN-Key/UA (или файл с ключом - см. п. «Загрузка ключа администратора УА ФПСУ-IP с диска»);
- «Создать нового УА». Предназначена для установки параметров администратора УА ФПСУ-IP (см. п. «Изменение параметров работы УА ФПСУ-IP»);
- «Доступ УА к ключу шифрования БД ОК ФПСУ-IP». Предназначена для управления доступом администраторов УА ФПСУ-IP к базе данных УА ФПСУ-IP (см. п. «Управление доступом к базе данных УА ФПСУ-IP»);
- «Записать ключ УА в файл (*.ke4)». Предназначена для выдачи ключа администратора УА ФПСУ-IP на любой носитель (см. п. «Выдача ключа администратора УА ФПСУ-IP в файл»);
- «Отменить текущий файл с ключом входа». Предназначена для поддержки файла ключа входа;
- «Установить файл с ключом входа». Предназначена для поддержки файла ключа входа.

17.2.1. Выдача ключа администратора УА ФПСУ-IP в файл

Ключ администратора УА ФПСУ-IP может быть выдан на любой носитель для хранения и возможности резервирования VPN-Key/UA с помощью ключа администратора УА ФПСУ-IP (подробнее в пункте «Резервирование с помощью ключа УА») или переноса на другой УА ФПСУ-IP. Для этого необходимо выбрать пункт меню «Ключ УА» → «Записать

ключ УА в файл (*.ke4)» и ввести пароль текущего администратора УА ФПСУ-IP. В случае работы с VPN-Key/UA требуется, чтобы VPN-Key/UA был подключен к USB-порту. Далее в открывшемся стандартном окне указать путь к директории, в которой необходимо сохранить файл. Файл нужного формата будет сохранен.

17. 2. 2. Загрузка ключа администратора УА ФПСУ-IP с диска

Ключ администратора УА ФПСУ-IP может быть загружен с диска в VPN-Key/UA.

Для загрузки ключа администратора УА ФПСУ-IP из файла с внутреннего накопителя в VPN-Key/UA необходимо выбрать пункт меню «Ключ УА» → «Загрузить ключ УА с диска» и в открывшемся стандартном окне указать путь к директории, в которой расположен файл с ключевыми данными. Отобразится окно с найденными файлами ключа администратора УА ФПСУ-IP, в котором следует выбрать файл по нажатию кнопки «Да».

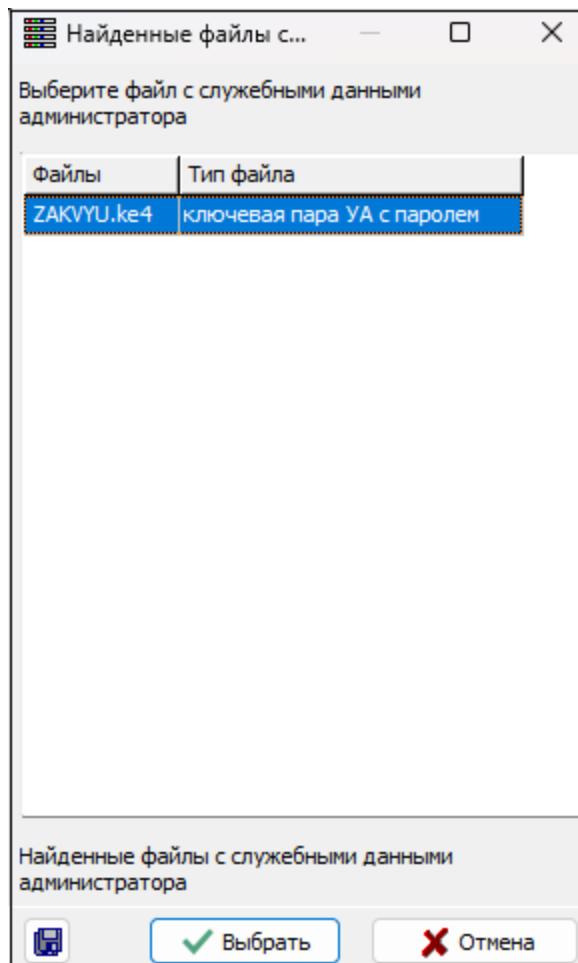


Рисунок 285 - Файлы с ключами администратора УА ФПСУ-IP

На экран будет выдано сообщение о загрузке ключевой пары в VPN-Key/UA, следует подтвердить действие по нажатию кнопки «Да».

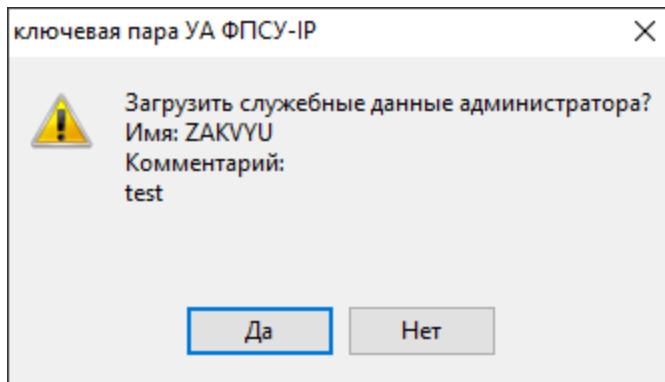


Рисунок 286 - Загрузка ключа администратора УА ФПСУ-IP

Дальнейшие действия с ключевыми данными осуществляются как при создании ключевых данных администратора УА ФПСУ-IP (подробнее в пункте «Пересоздание ключевых данных администратора УА ФПСУ-IP»).

17. 2. 3. Выдача ключа для подключения к внешней БД

Использование внешней БД позволяет синхронизировать изменения описателей ФПСУ-IP с разных УА ФПСУ-IP.

Подключение к внешней БД осуществляется по ключу шифрования БД администратора УА ФПСУ-IP. Для выдачи ключа шифрования БД на носитель необходимо выполнить команду главного меню «Ключ УА» → «Выдать ключ БД УА на диск», в открывшемся стандартном окне следует выбрать диск и каталог, в который будет выдан файл с ключом формата .dk.

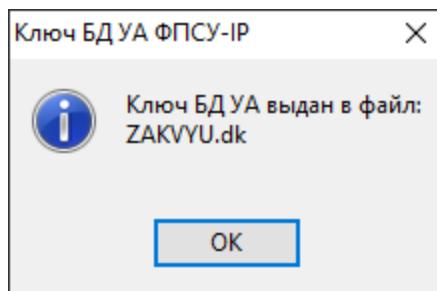


Рисунок 287 - Выдача ключа БД администратора УА ФПСУ-IP в файл

Дальнейшие действия с ключом производит администратор внешней БД ФПСУ-IP.

После того, как администратор УА ФПСУ-IP зарегистрирован в внешней БД, на УА ФПСУ-IP требуется настроить доступ к файлу внешней БД. На панели информации следует нажать кнопку  «Внешняя БД», откроется окно с настройками. В качестве примера на рисунке ниже приведены настройки подключения.

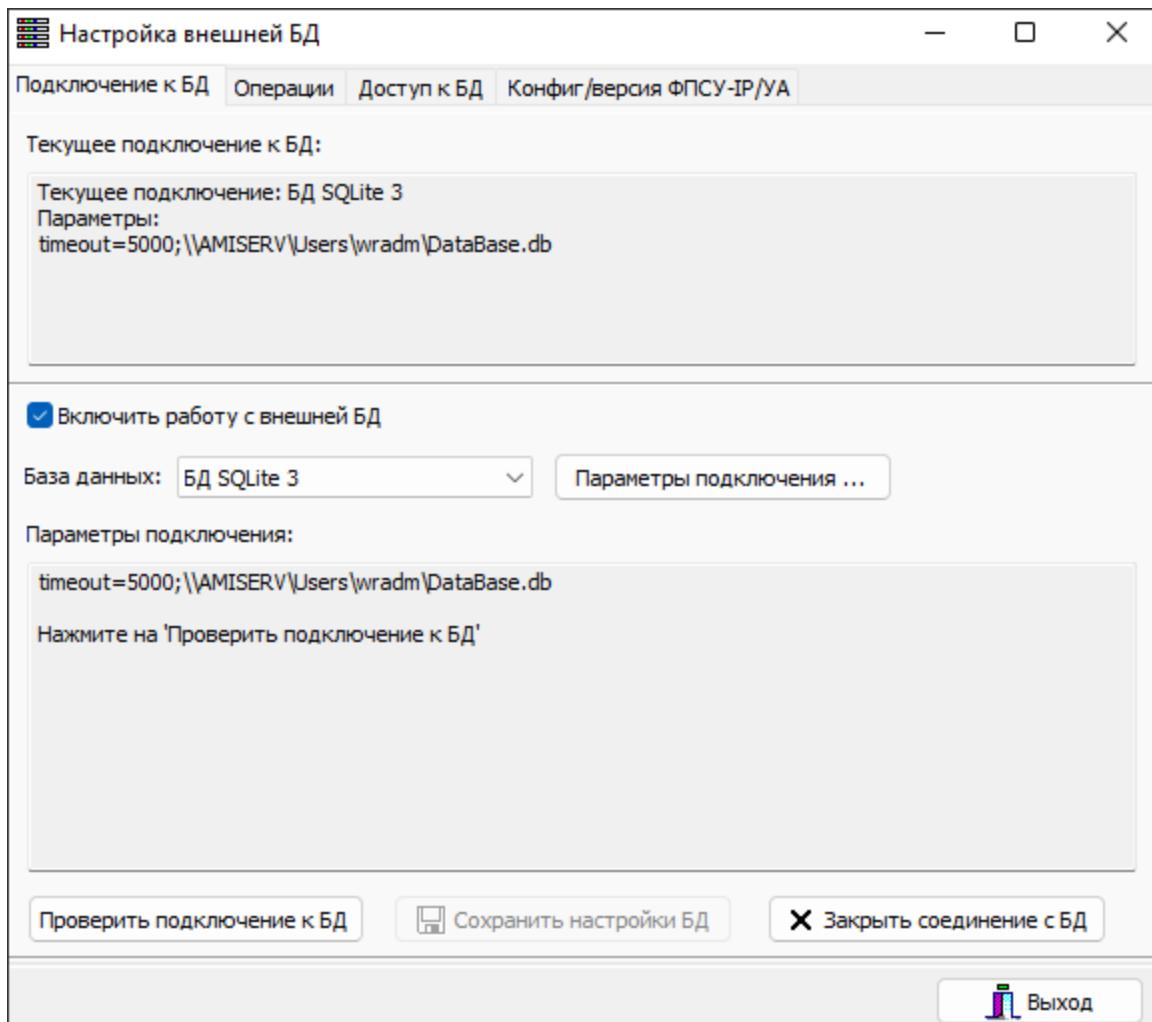


Рисунок 288 -Настройка доступа к файлу внешней БД

18. Работа со внешними базами данных

Внешняя БД является централизованным хранилищем описателей ФПСУ-IP при многопользовательской работе (одновременной работы нескольких пользователей УА ФПСУ-IP). Внешняя БД для УА ФПСУ-IP является местом хранения информации, расположенным на компьютере (сервере), доступ к которому осуществляется через сеть. Работа с внешней базой данных осуществляется по технологии «Клиент-Сервер». Клиентом является ПО «Удаленный администратор ФПСУ-IP», установленный на компьютере пользователя. Сервером является внешняя БД.

Для работы с внешней базой данных необходимо наличие в каталоге «LIC» файла лицензии-расширения для работы с сетевыми базами данных (файлы в каталог «LIC» могут быть скопированы или добавлены с использованием окна «Управление лицензиями», см. п. «Лицензирование»). В случае отсутствия лицензии для работы с сетевыми базами данных работа со внешними БД будет невозможна.

В разделе приведены сведения о настройке подключения ко внешней БД и особенности взаимодействия ФПСУ-IP со внешней БД.

18. 1. Настройка подключения ко внешней БД

Все настройки внешней БД осуществляются в одноименном окне, открывающемся по нажатию кнопки  в окне «Удаленный администратор «ФПСУ-IP»:

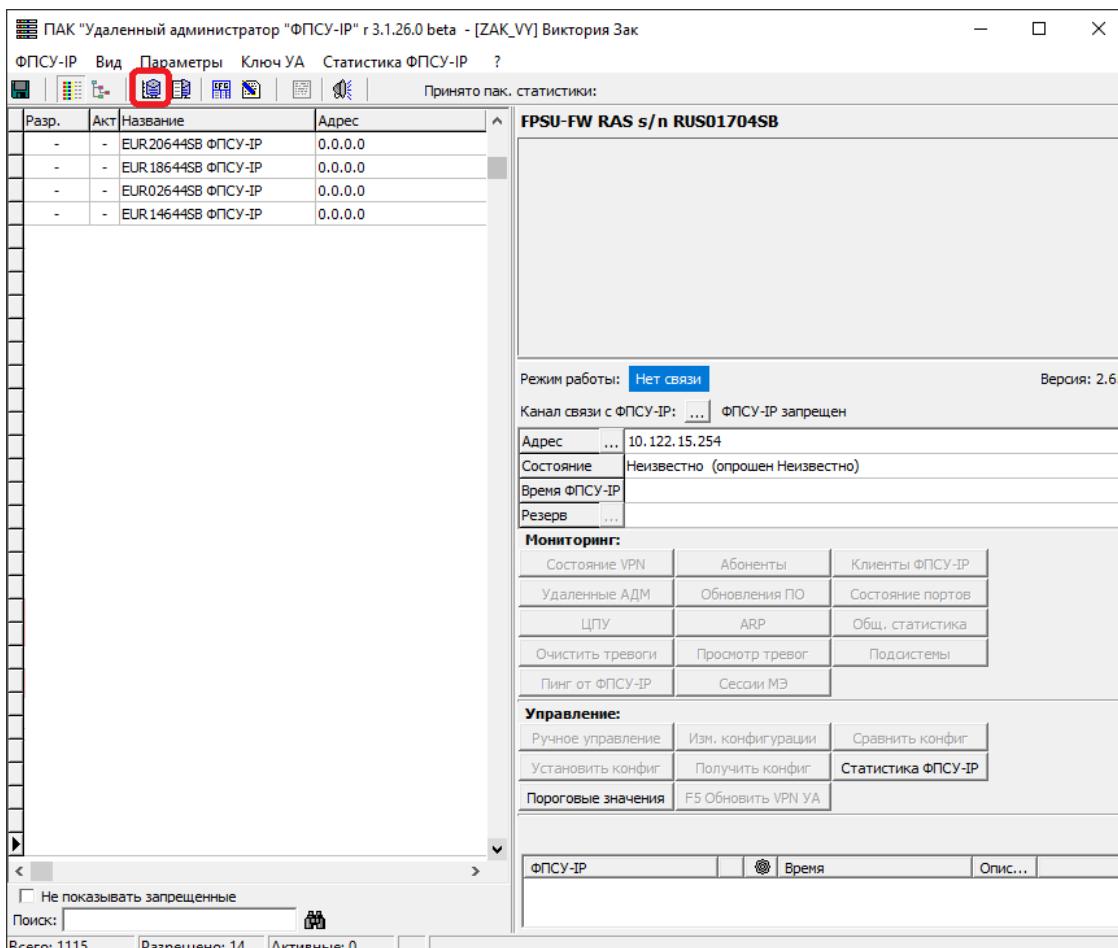


Рисунок 289 – Основное окно программы

Следует иметь в виду, что в случае отсутствия лицензии для работы с сетевыми базами данных (см. п. «Лицензирование») кнопка «Внешняя БД» на панели инструментов отображаться не будет.

Окно «Настройки внешней БД» включает в себя четыре вкладки, в которых производятся те или иные действия, связанные с настройками БД:

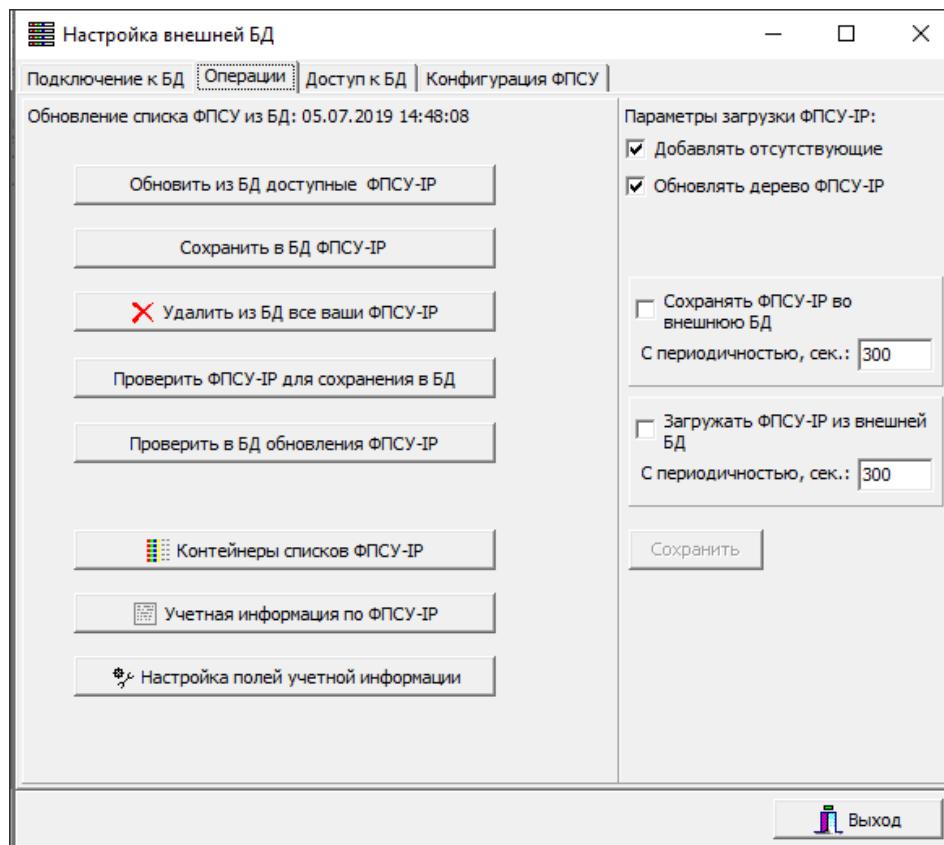


Рисунок 290 – Окно настроек внешней БД

18. 1. 1. Первое подключение к БД

После первого нажатия кнопки «Внешняя БД» откроется окно «Настройки внешней БД» с пустыми установками по умолчанию. В верхней части вкладки «Подключение к БД» открывшегося окна отображается текущее состояние настроек базы данных, ниже находятся поле выбора базы данных, кнопка её настройки «Параметры подключения», и кнопка тестирования корректности настроек «Проверить подключение к БД»:

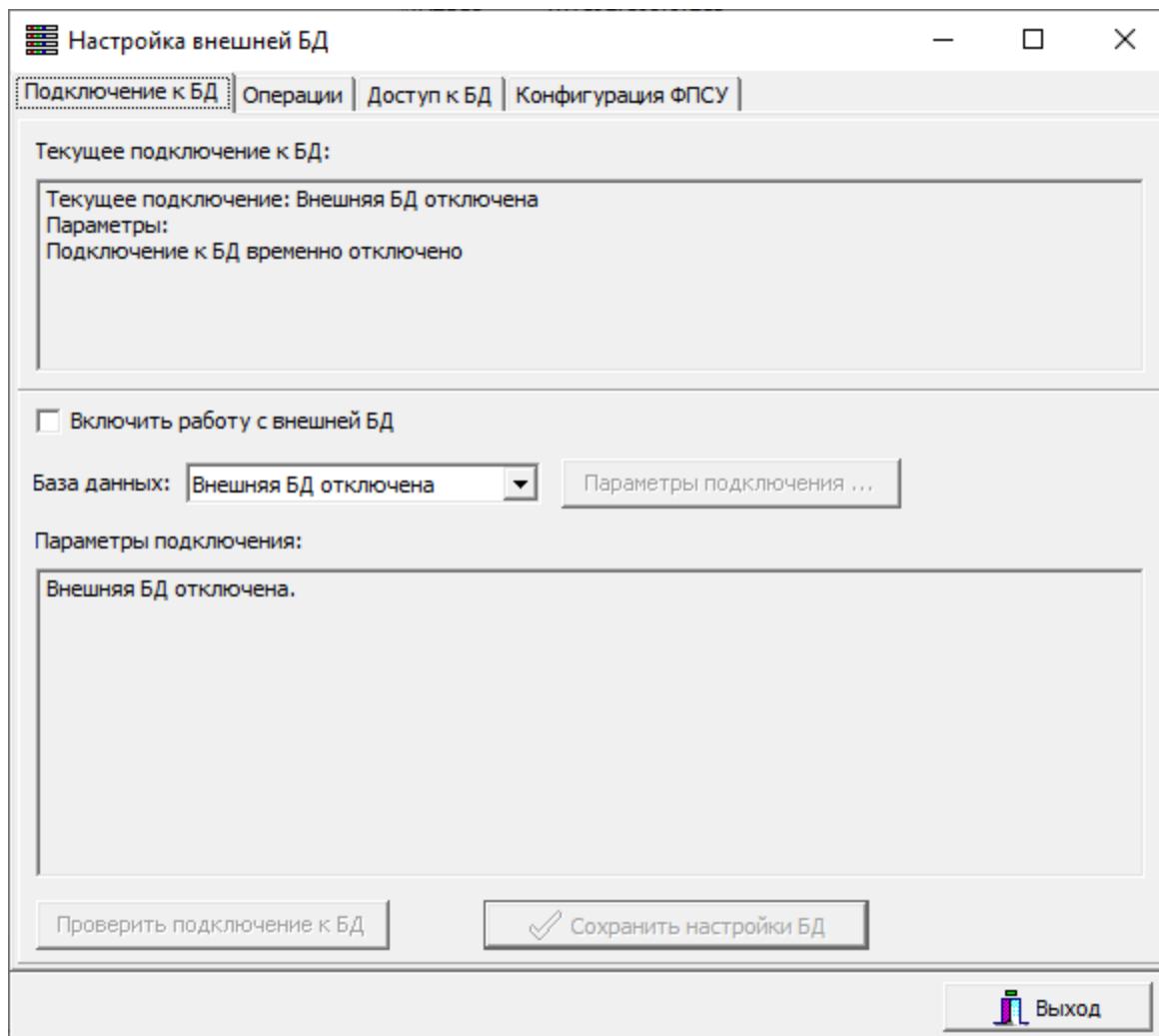


Рисунок 291 – Настройки подключения ко внешней БД по умолчанию

Для первоначального подключения ко внешней БД следует:

- установить флаг «Включить работу со внешней БД»;
- выбрать тип внешней базы данных в поле «База данных»;
- указать сетевой путь ко внешней БД, предоставленный администратором внешней БД;
- проверить подключение, нажав одноименную кнопку;
- сохранить настройки БД.

18. 1. 1. Особенности работы со внешними БД PostgreSQL

После нажатия кнопки «Внешняя БД» откроется окно «Настройки внешней БД».

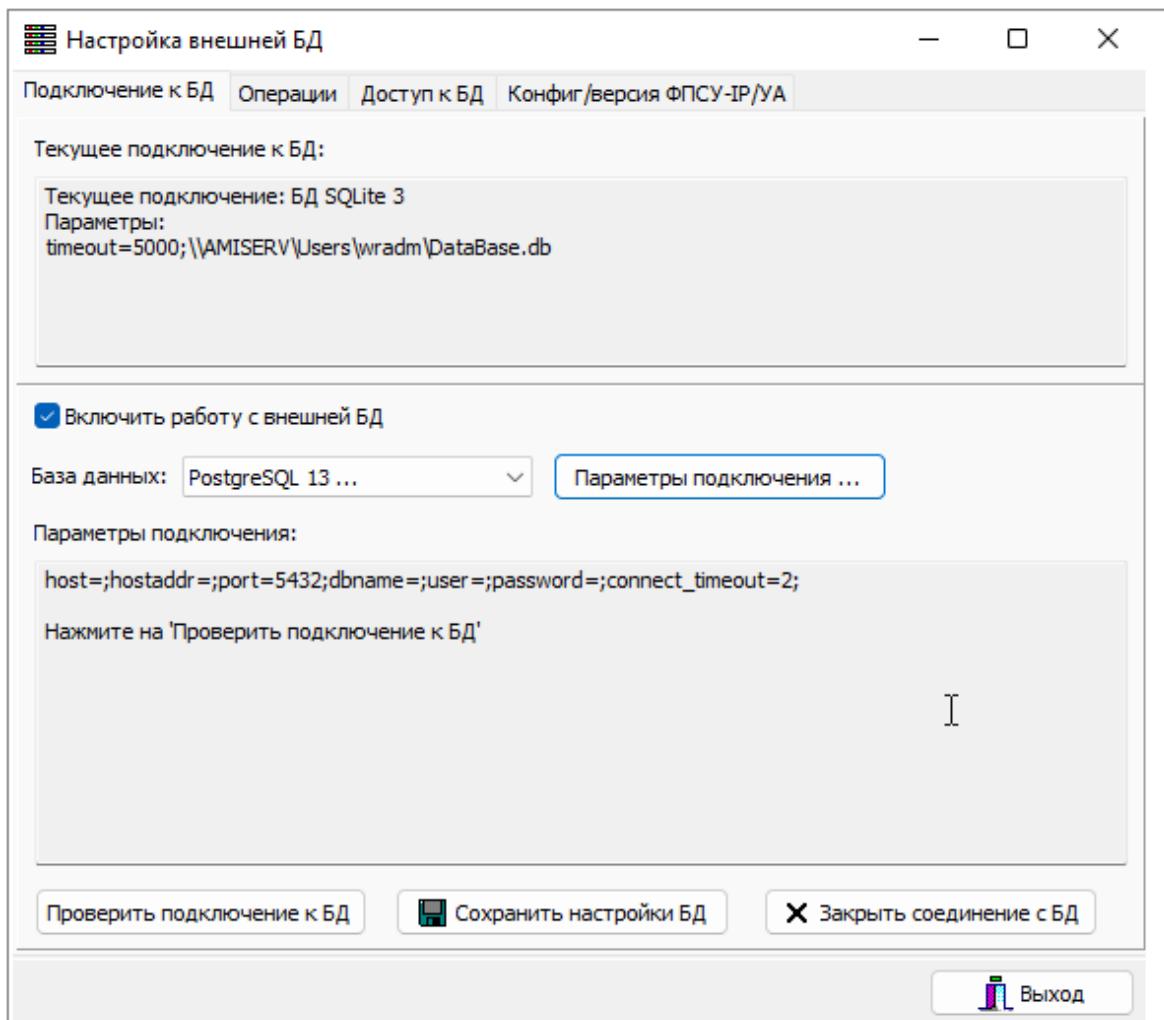


Рисунок 292 – Настройки подключения ко внешней БД

Для подключения ко внешней БД PostgreSQL следует:

- установить флаг «Включить работу со внешней БД»;
- выбрать тип «PostgreSQL 13...» в поле «База данных»;
- нажать кнопку «Параметры подключения» и в открывшемся окне ввести следующие параметры:
 - ✓ host: наименование хоста;
 - ✓ hostaddr: сетевой адрес хоста;
 - ✓ port: порт, который слушает БД (по умолчанию 5432);
 - ✓ dbname: имя БД;
 - ✓ user: имя пользователя БД (по умолчанию postgres);

- ✓ **password:** пароль, созданный для пользователя при создании БД;
- ✓ **connect_timeout:** превышение лимита времени соединения с БД в секундах (по умолчанию 2).

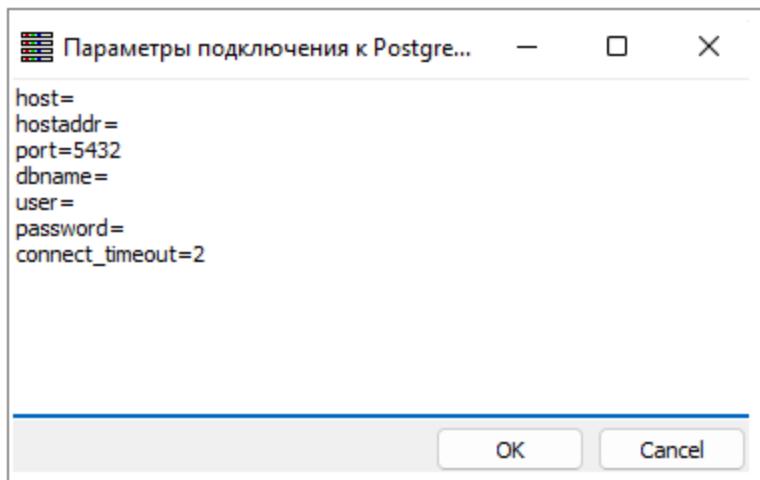


Рисунок 293 – Настройки подключения ко внешней БД

- проверить подключение, нажав одноименную кнопку;
- сохранить настройки БД.

Внимание! В случае отсутствия активной работы с БД в течение 15 минут соединение с ней будет принудительно прервано и автоматически восстановлено при следующем обращении к БД.

Следует иметь в виду, что для корректной работы со внешней БД PostgreSQL из УА необходимо, чтобы при создании новой базы данных в PGAdmin были заданы следующие параметры:

- ENCODING = 'WIN1251'
- TEMPLATE = template0
- COLLATION = 'Russian_Russia.1251'
- CHARACTER TYPE = 'Russian_Russia.1251'

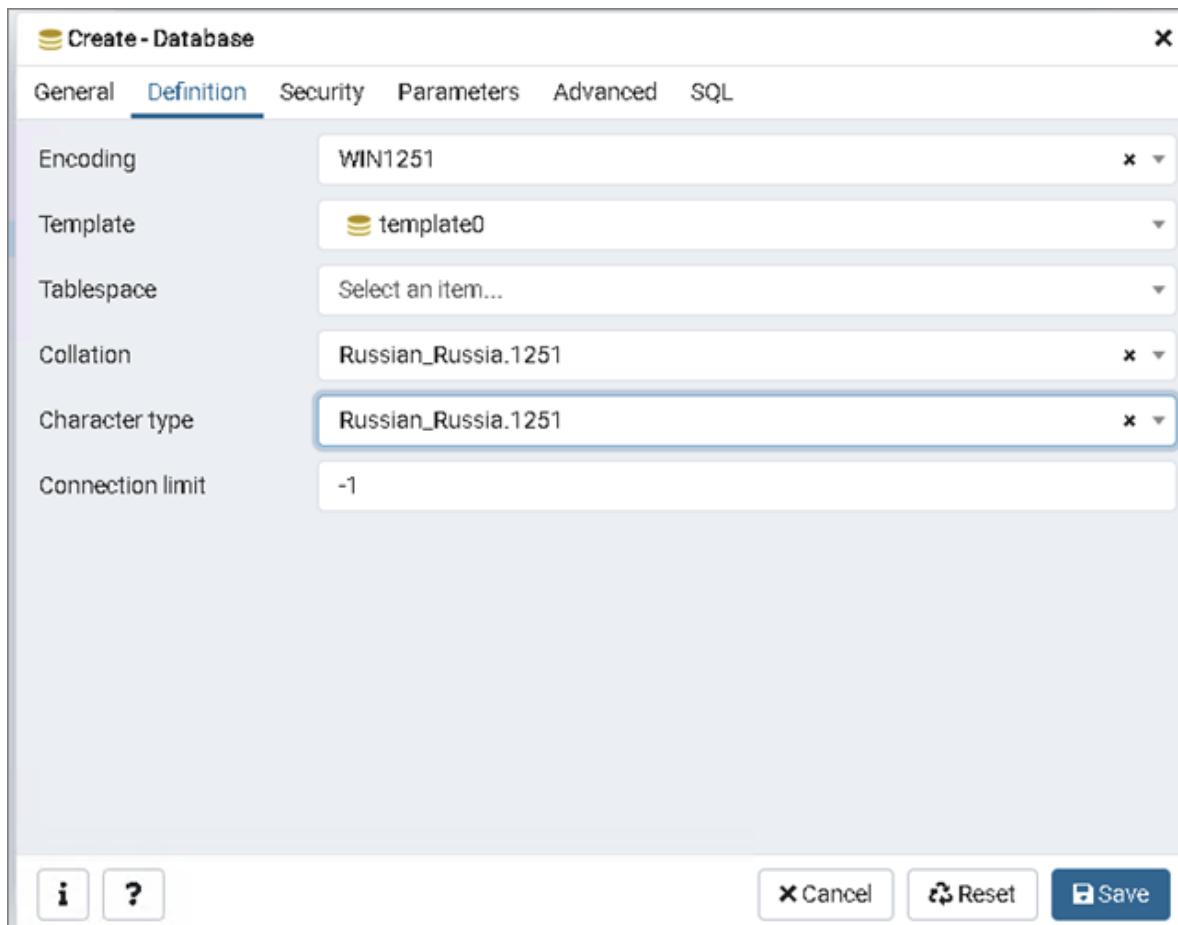


Рисунок 294 – Настройки БД при ее создании в PGAdmin

18. 1. 2. Повторное подключение ко внешней БД

Для включения возможности связи со внешней БД необходимо перейти во вкладку «Подключение к БД» и установить флаг «Включить работу со внешней БД».

Для работы с нужной внешней БД необходимо нажать кнопку «Параметры подключения», найти и выбрать необходимую БД и нажать кнопку «Сохранить».

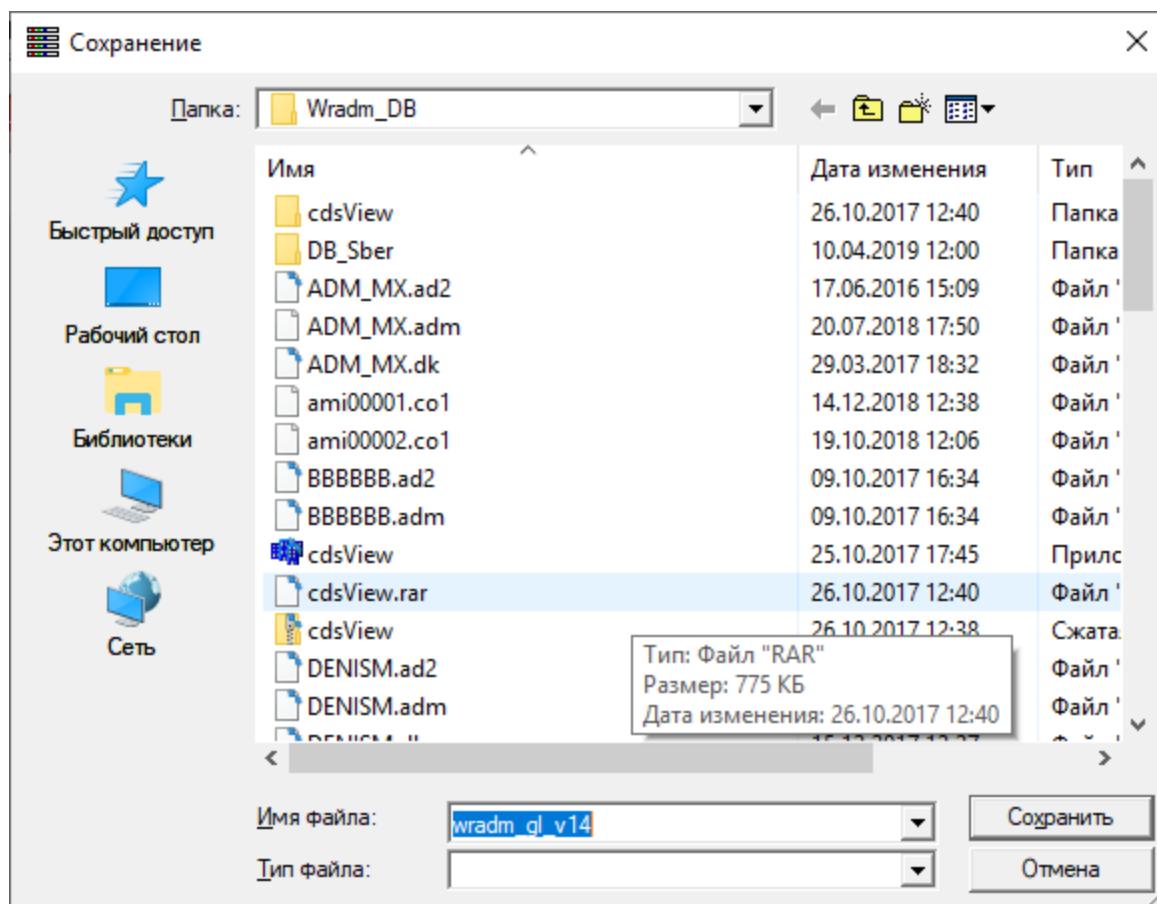


Рисунок 295 – Окно выбора пути к базе данных

После выбора пути к необходимой внешней БД, он отобразится в поле «Параметры подключения». Для продолжения работы необходимо нажать кнопку «Проверить подключение к БД».

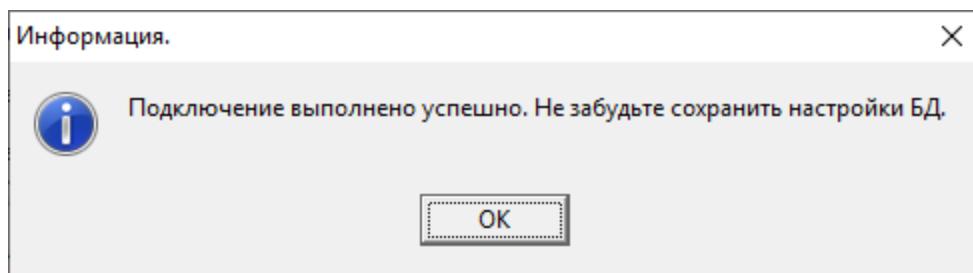


Рисунок 296 – Подключение выполнено успешно

Система выдаст сообщение об успешной проверке подключения, после чего необходимо будет сохранить настройки БД, нажав одноименную кнопку.

18. 1. 3. Отключение работы со внешней БД

Отключение от внешней БД так же производится в окне «Подключение к БД». Работу со внешней БД можно отключить двумя способами.

1. Временно. Для этого необходимо снять флаг «Включить работу со внешней БД», при этом в поле «Параметры подключения» будет выведено следующее сообщение: «Подключение к БД временно отключено Нажмите на 'Проверить подключение к БД'». Для продолжения работы необходимо нажать кнопку «Проверить подключение к БД» в окне настроек внешней БД. Система выдаст сообщение об успешной проверке подключения, после чего необходимо будет сохранить настройки БД, нажав одноименную кнопку. Система выдаст сообщение, представленное на рисунке ниже.

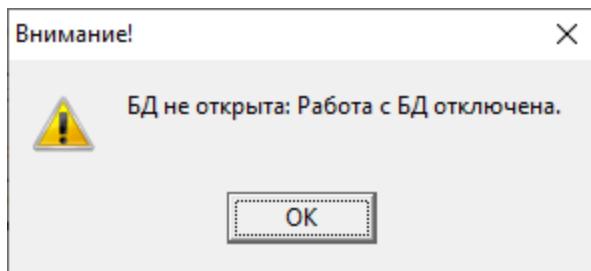


Рисунок 297 – Сообщение об отключении работы с БД

При этом в поле «Параметры соединения» появится следующее сообщение: «\\путь к базе\xxx Подключение к БД временно отключено». Для включения работы с БД необходимо установить флаг «Включить работу со внешней БД».

2. Постоянно (удалить путь к БД). Для этого из выпадающего в поле «База данных» списка необходимо выбрать пункт «Внешняя БД отключена».

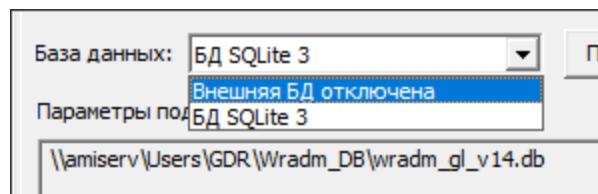


Рисунок 298 – Отключение БД

При этом в поле «Параметры отключения» отобразится следующее сообщение: «Внешняя БД отключена.». После сохранения настроек БД путем нажатия одноименной кнопки, внешняя БД будет полностью отключена. Для повторного подключения необходимо заново подключиться к нужной внешней БД (раздел «Первое подключение к БД»).

18. 1. 4. Доступ ко внешней БД

Для получения тех или иных возможностей при работе со внешней БД администратору внешней БД необходимо перейти во вкладку «Доступ к БД» и создать список профилей тех пользователей УА ФПСУ-IP, которые будут иметь доступ ко внешней БД, а так же наделить их соответствующими правами.

Профили пользователей УА ФПСУ-IP создаются из либо из файла (с расширением *.dk или *.ke), формируемого удаленным администратором для работы со внешней БД (пункт «Выдать ключ БД УА на диск...» меню «Ключ УА» основного окна), или при помощи данных из VPN-Key/UA. Изначально существует одна запись, созданная при первом запуске УА ФПСУ-IP и отображающей данные самого администратора внешней БД.

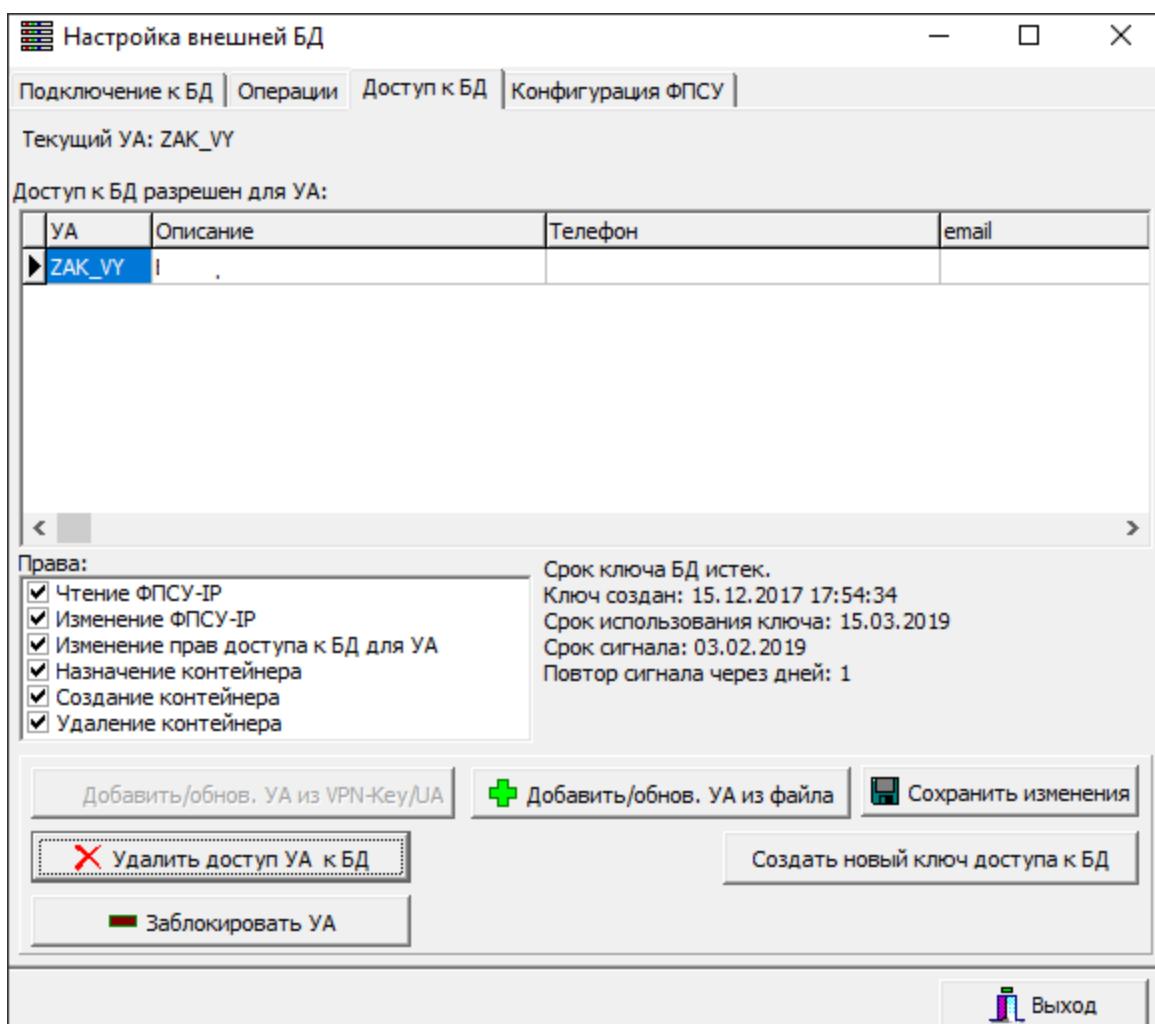


Рисунок 299 – Список пользователей УА ФПСУ-IP, которым разрешен доступ ко внешней БД

Все изменения, производимые в этой вкладке, необходимо сохранять путем нажатия на кнопку «Сохранить изменения».

18. 1. 4. 1. Добавление или обновление УА при помощи файла

Кнопка «Добавить УА из файла» требует указать файл с данными пользователя УА ФПСУ-IP. Этот файл должен быть получен от другого пользователя УА ФПСУ-IP заранее.

Для того, чтобы создать профиль нового пользователя УА ФПСУ-IP при помощи файла, необходимо нажать кнопку «Добавить/обнов. УА из файла». В открывшемся окне следует выбрать путь к каталогу, в котором хранятся файлы (с расширением *.dk или *.ke). Система откроет окно, в котором отобразит все файлы с ключами БД УА ФПСУ-IP.

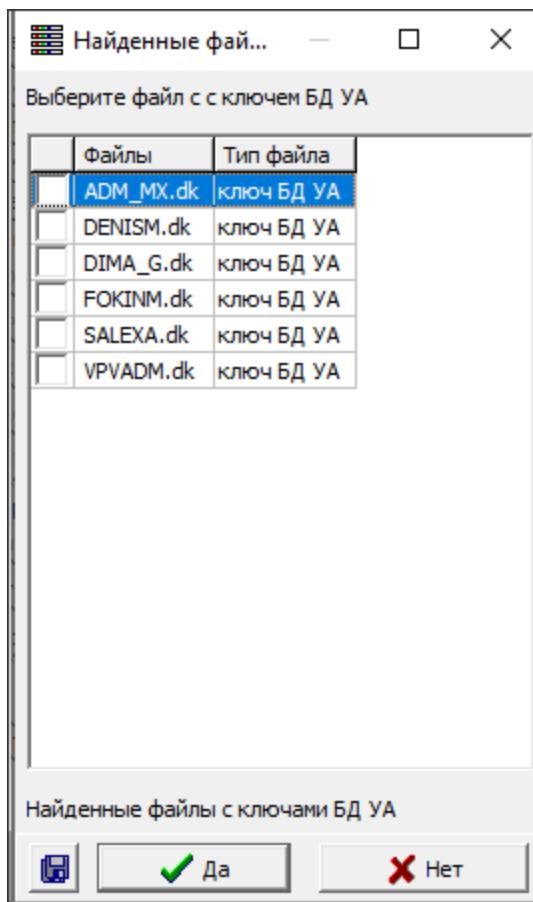


Рисунок 300 – Список ключей БД УА ФПСУ-IP

В открывшемся списке необходимо установить флаги для выбора файлов с ключами БД УА ФПСУ-IP. После нажатия кнопки «Да» выбранные файлы будут добавлены в БД. Соответственно, всем пользователям УА ФПСУ-IP - владельцам этих ключей - будет разрешен доступ к БД с правами на выполнение определенных действий. По умолчанию УА

создаются с теми правами, которые прописаны в загружаемом файле. В дальнейшем администратор внешней базы данных сможет изменить их путем установки или снятия флагов в поле «Права».

Перед тем, как добавить найденных пользователей в список, система выведет сообщение о разрешении доступа выбранным УА:

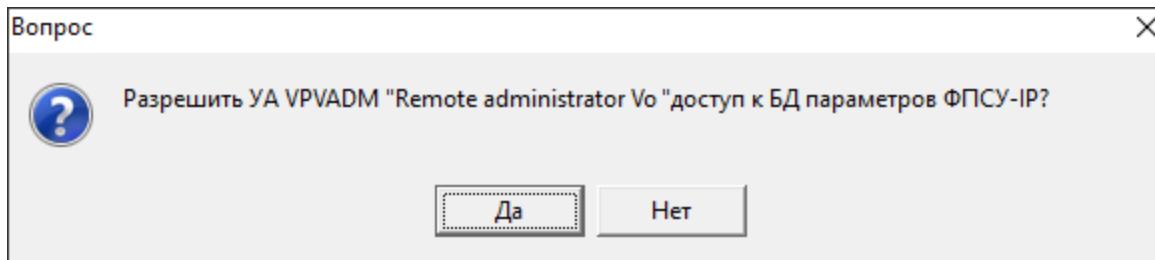


Рисунок 301 – Запрос разрешения доступа для УА к параметрам БД

После нажатия «Да» выбранному пользователю УА ФПСУ-IP будет предоставлен доступ к базе данных параметров ФПСУ-IP, и он отобразится в общем списке.

18. 1. 4. 2. Добавление или обновление УА при помощи VPN-key/UA

Нажатием кнопки «Добавить УА из VPN-Key/UA» инициируется предоставление доступа к базе данных учетной записи пользователя УА ФПСУ-IP, чей VPN-Key сейчас подключен к УА ФПСУ-IP.

Для того, чтобы создать нового профиль нового пользователя УА ФПСУ-IP при помощи устройства VPN-Key/UA, необходимо подключить устройство VPN-Key/UA и нажать кнопку «Добавить УА из VPN-Key/UA». Система выдаст сообщение об обнаруженном VPN-Key/UA и запрос на ввод текущего PIN-кода пользователя УА ФПСУ-IP:

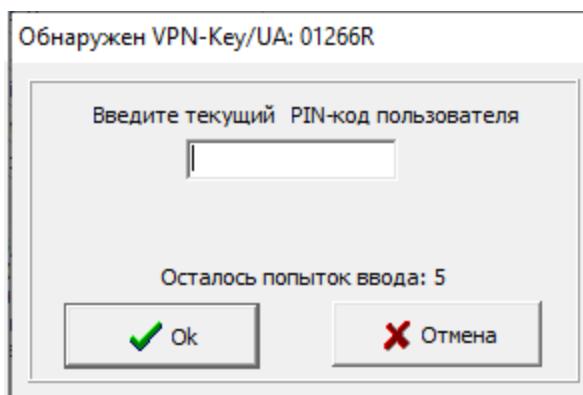


Рисунок 302 – Запрос на ввод текущего PIN-кода

После корректного ввода PIN-кода и нажатия кнопки «OK» система выдаст запрос на предоставление доступа пользователю УА ФПСУ-IP ко внешней БД:

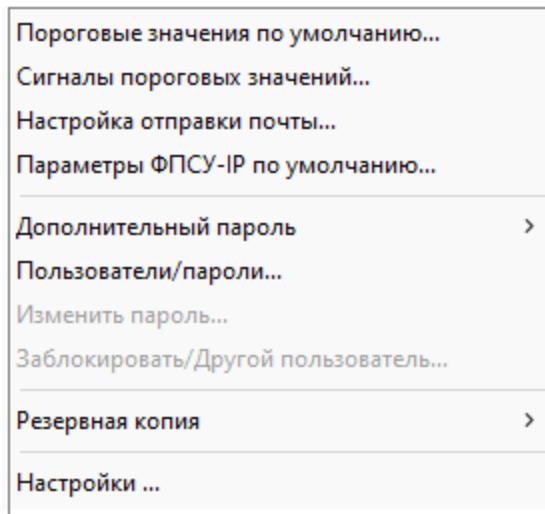


Рисунок 303 – Запрос на предоставление доступа ко внешней БД

После нажатия кнопки «Да» пользователю УА ФПСУ-IP будет предоставлен доступ к базе данных параметров ФПСУ-IP, и он отобразится в общем списке.

18. 1. 4. 3. Изменение прав доступа УА к БД

Администратор внешней БД имеет право на изменение прав доступа к БД для пользователей УА ФПСУ-IP. Доступ может быть предоставлен на:

- чтение ФПСУ-IP (ситуация, в которой запись о параметрах ФПСУ-IP забирается на УА ФПСУ-IP, после чего удаленный администратор может просматривать описатель);
- изменение параметров ФПСУ-IP (ситуация, в которой запись о параметрах ФПСУ-IP забирается на УА ФПСУ-IP, после чего удаленный администратор может просматривать и редактировать описатель);
- назначение контейнера тому или иному удаленному администратору для работы;
- создание контейнера;
- удаление контейнера.

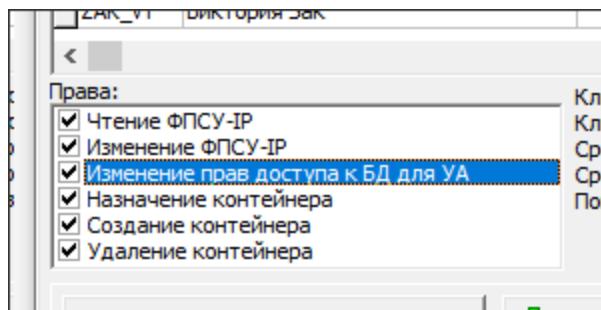


Рисунок 304 – Права доступа к БД для УА

18.1.4.4. Удаление доступа УА к БД

Если необходимо удалить доступ пользователя УА ФПСУ-IP к базе данных, следует выбрать запись из списка и нажать кнопку «Удалить доступ УА к БД». Система выдаст уточняющее сообщение:

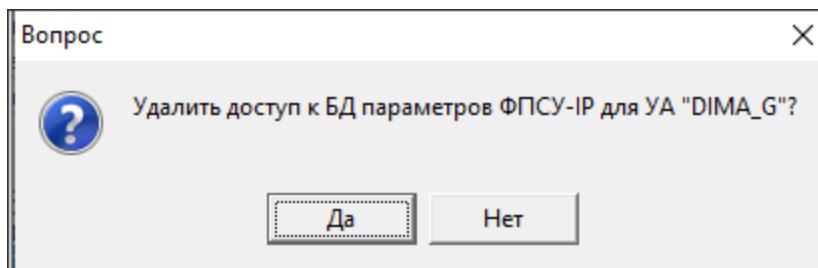


Рисунок 305 – Запрос на удаление доступа

После подтверждения действия пользователь УА ФПСУ-IP будет удален из списка.

18.1.4.5. Блокировка доступа УА к БД

При необходимости можно заблокировать пользователю УА ФПСУ-IP доступ к базе данных, не удаляя его из списка. Для этого необходимо выбрать запись и нажать кнопку «Заблокировать УА». Система выдаст следующее сообщение:

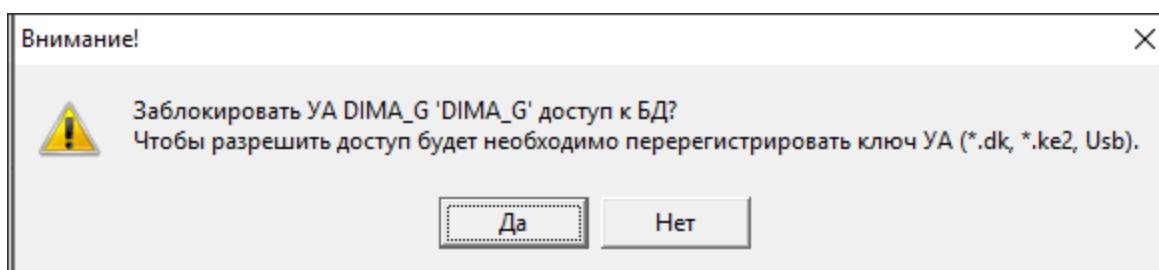


Рисунок 306 – Запрос о блокировке УА

После подтверждения данного действия доступ выбранного пользователя УА ФПСУ-IP к БД будет приостановлен.

18.1.4.6. Создание нового ключа доступа к БД

Ключ доступа к БД, на основе которого создаются файлы с ключами доступа УА, создается администратором, у которого есть возможность изменения прав доступа к БД для УА (установлен одноименный флаг). Кнопка «Создать новый ключ УА» во вкладке «Доступ к БД» окна «Настройка внешней БД» используется для повторного создания ключа шифрования базы данных УА ФПСУ-IP по причине истечения срока действия предыдущего ключа или его компрометации.

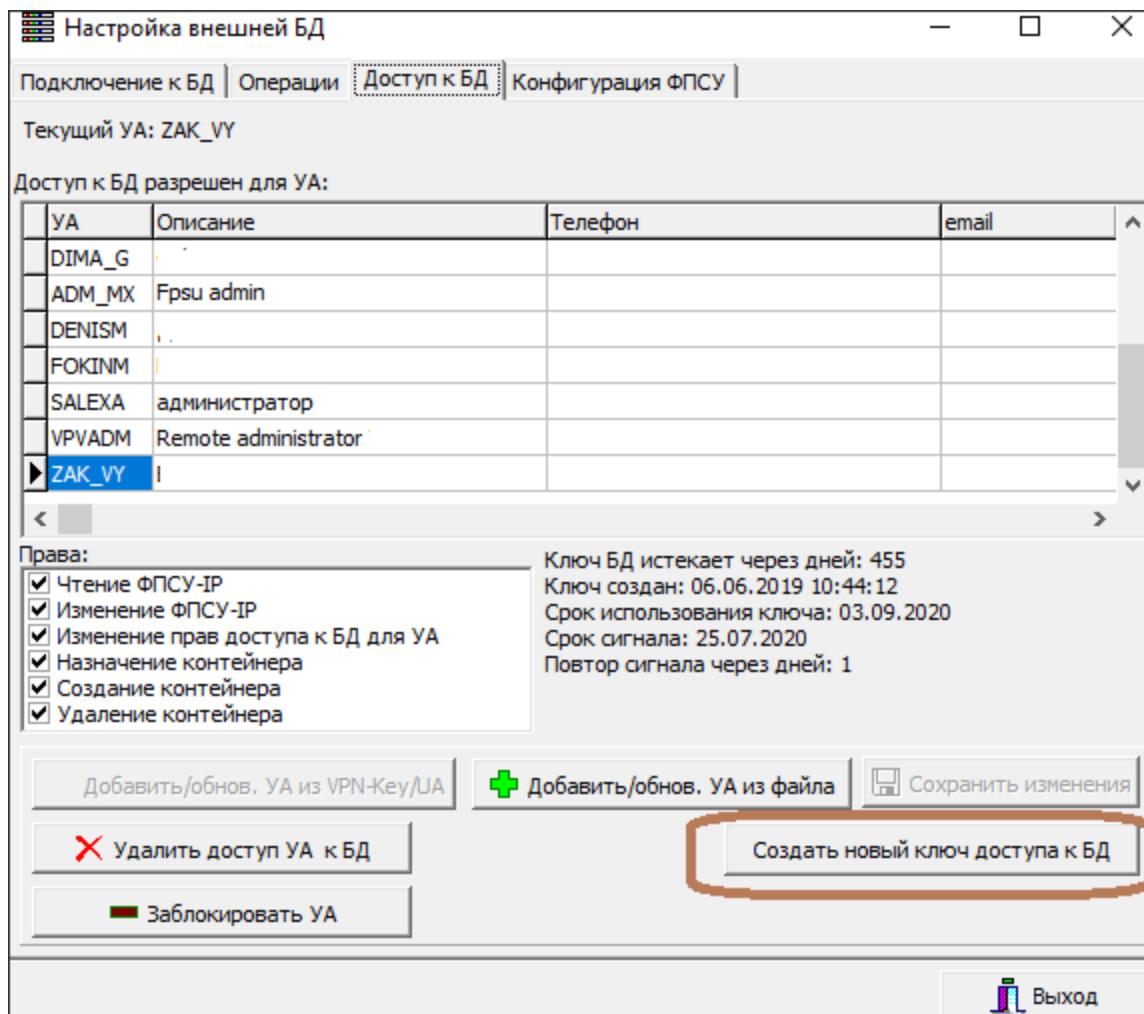


Рисунок 307 – Начало создания нового ключа к БД

По нажатию этой кнопки система выдаст предупреждение о том, что все используемые ключи пользователей УА ФПСУ-IP после обновления необходимо будет

перерегистрировать:

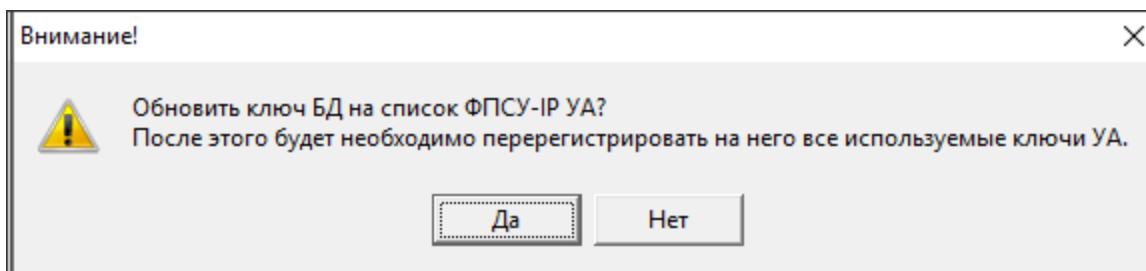


Рисунок 308 – Предупреждение о возможной необходимости перерегистрации используемых ключей

После нажатия кнопки «Да» на экран будет выведено окно, предназначенное для установки ключа шифрования базы данных. В нем необходимо установить:

- срок действия ключа в днях (по умолчанию 455);
- количество дней до истечения срока действия ключа, за которое программа будет выводить предупреждение об этом (по умолчанию 40);
- временной интервал (в днях), по прошествии которого сигнал будет повторен.

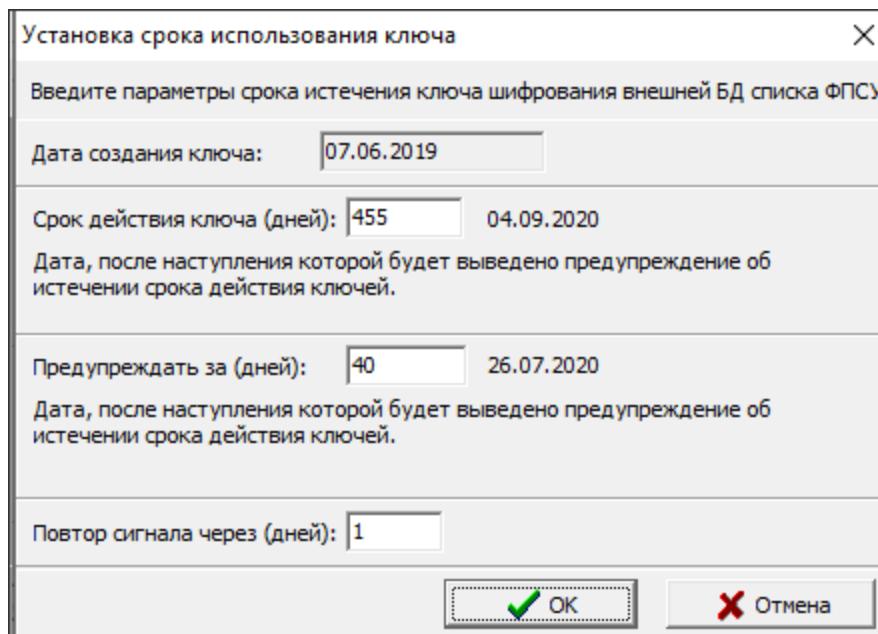


Рисунок 309 – Установка срока использования ключа

По нажатию кнопки «OK» ключ будет обновлен. Система выдаст следующее сообщение:

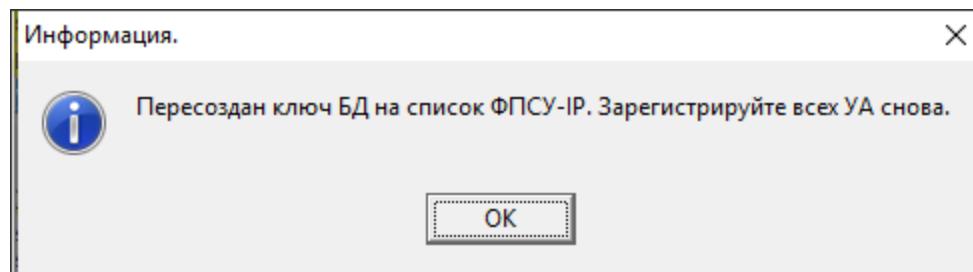


Рисунок 310 – Сообщение о пересоздании ключа

18.1.4.7. Обновление ключей УА

После обновления основного ключа доступа к БД необходимо повторно зарегистрировать всех остальных пользователей УА ФПСУ-IP. В списке пользователей УА ФПСУ-IP, которым разрешен доступ к БД, эти УА будут подзвучены желтым:

Рисунок 311 – Список УА, подлежащих повторной регистрации

Обновить данные можно либо путем, описанным в разделе «Добавление или обновление УА при помощи файла», либо путем, описанным в разделе «Добавление или обновление УА при помощи VPN-key/UA». При этом на последнем шаге система выдаст следующее сообщение:

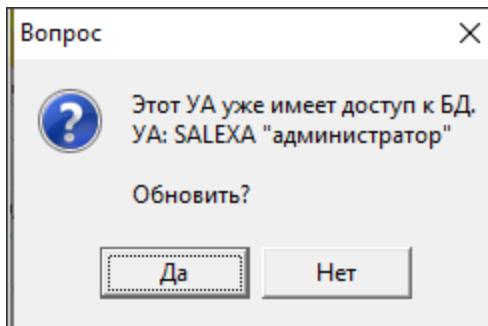


Рисунок 312 – Запрос необходимости обновления ключа УА

После нажатия кнопки «Да» пользователю УА ФПСУ-IP будет повторно предоставлен доступ к БД, в общем списке он будет отображаться на белом фоне. После нажатия

18. 1. 5. Операции с внешней БД

Во вкладке «Операции» окна «Настройки внешней БД» предоставляется возможность настроить операции, доступные при работе со внешней БД через систему удаленного администрирования ФПСУ-IP.

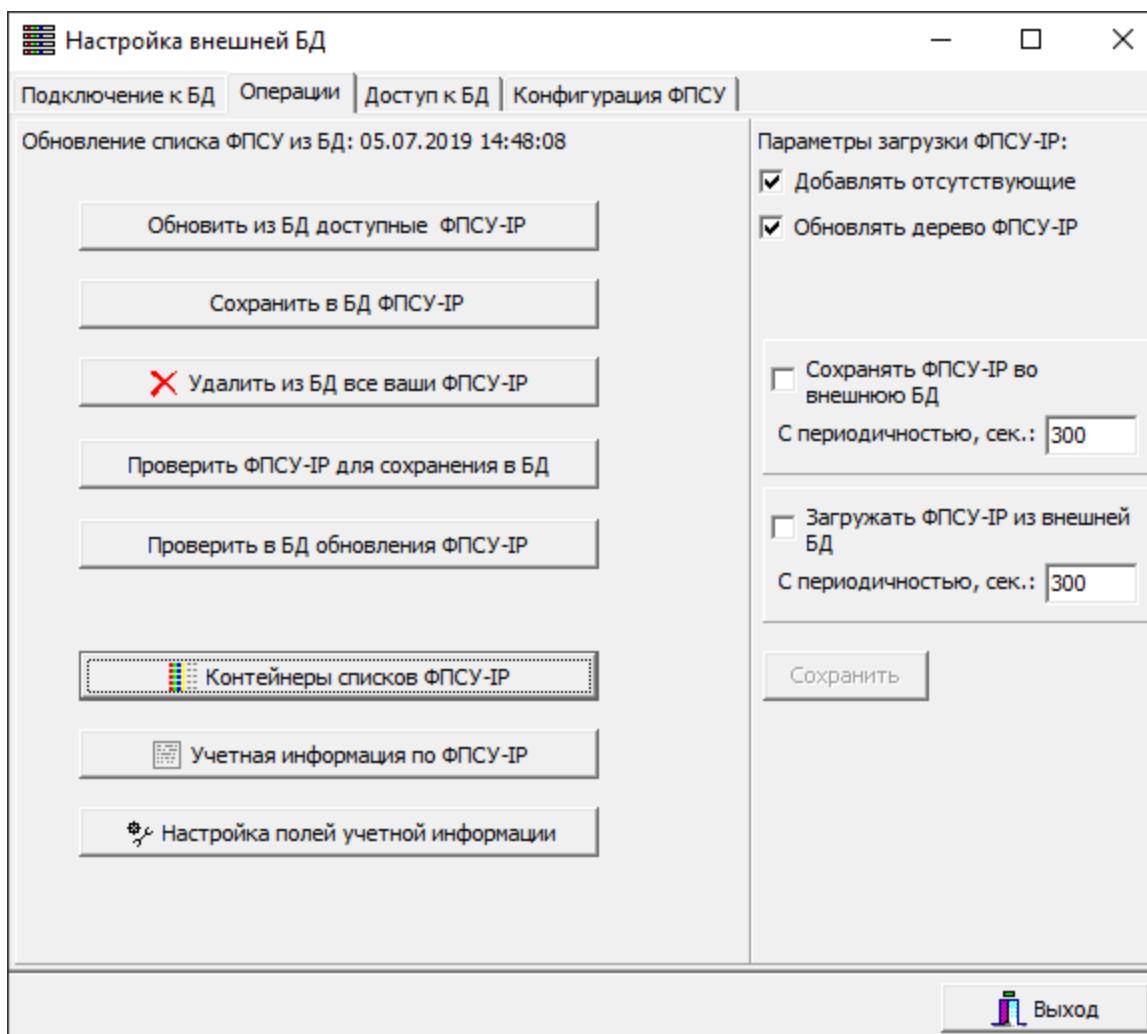


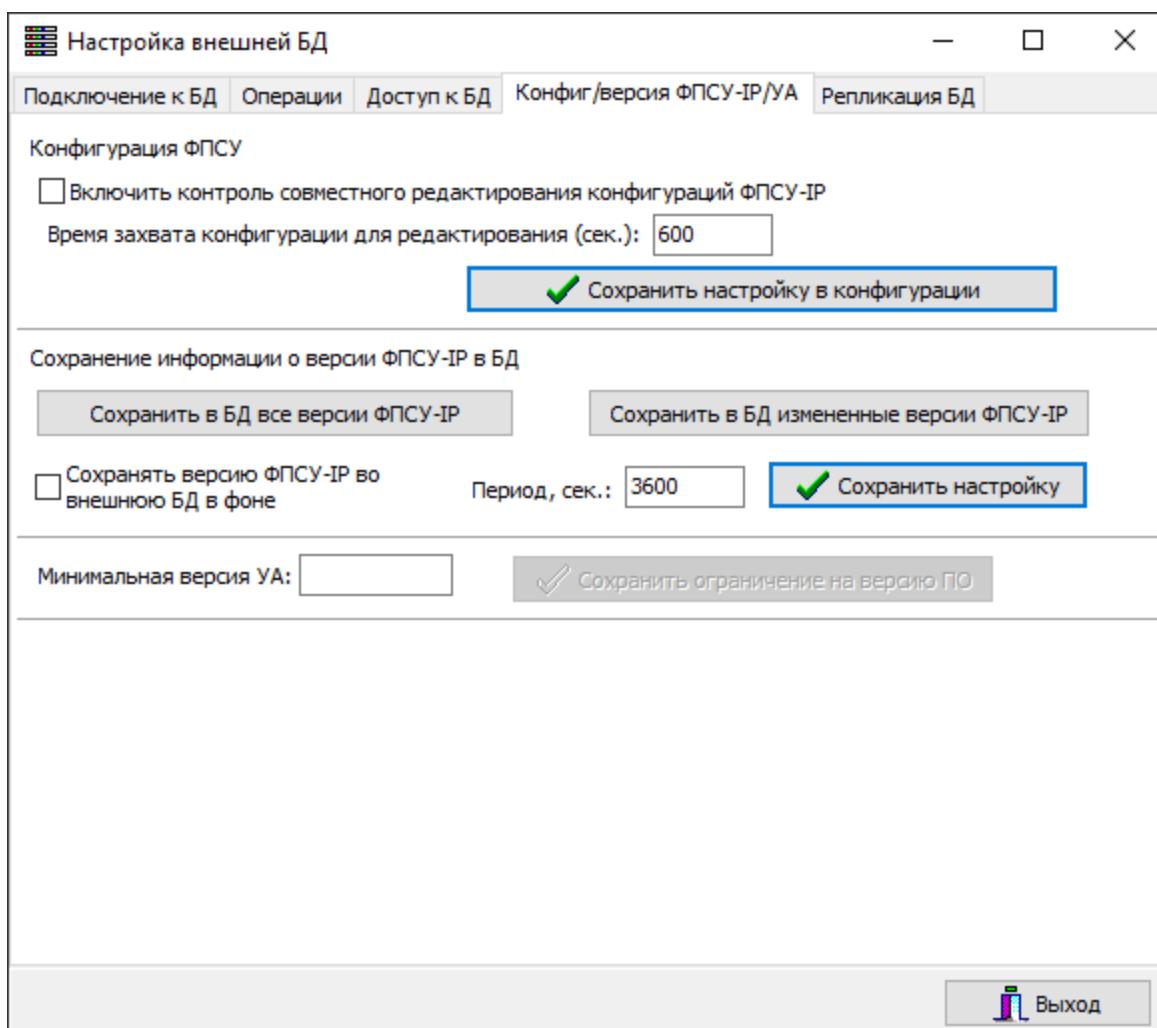
Рисунок 313 - Операции со внешней БД

Кроме того, во вкладке «Операции» окна «Настройки внешней БД» предоставляется возможность установить временные интервалы, по истечению которых все изменения ФПСУ-IP, внесенные на УА ФПСУ-IP, будут сохраняться во внешнюю БД, и/или загружаться из внешней БД. Данные действия осуществляются путем установки одноименных флагов и задания временных интервалов, по умолчанию установленных в 300 секунд. Так же можно изменить параметры загрузки ФПСУ-IP путем установки или снятия флагов в соответствующей части окна.

- 18. 1. 5. 1. Обновление параметров ФПСУ-IP из внешней БД**
- 18. 1. 5. 2. Сохранение ФПСУ-IP в БД**
- 18. 1. 5. 3. Проверка обновлений ФПСУ-IP во внешней базе данных**

18.1.5.4. Проверка наличия изменений параметров ФПСУ-IP**18.1.5.5. Контейнеры списков ФПСУ-IP****18.1.5.5.1. Изменение прав доступа на контейнер****18.1.5.5.2. Заполнение контейнера****18.1.5.6. Конфигурация ФПСУ-IP**

Если существует возможность одновременной работы нескольких пользователей УА ФПСУ-IP с одной ФПСУ-IP, необходимо включить контроль совместного редактирования конфигураций. Для этого во вкладке «Конфигурация ФПСУ» необходимо установить соответствующий флаг и выставить время захвата конфигурации (по умолчанию 600 секунд), после чего нажать на кнопку «Сохранить настройку в конфигурации».

**Рисунок 314 – Включение контроля совместного редактирования конфигураций**

После установки этих настроек при редактировании параметров ФПСУ-IP одним пользователем и попытке одновременного подключения для редактирования этих же параметров другим, система выдаст предупреждение о захвате конфигурации. При этом одновременная работа пользователей блокироваться не будет.

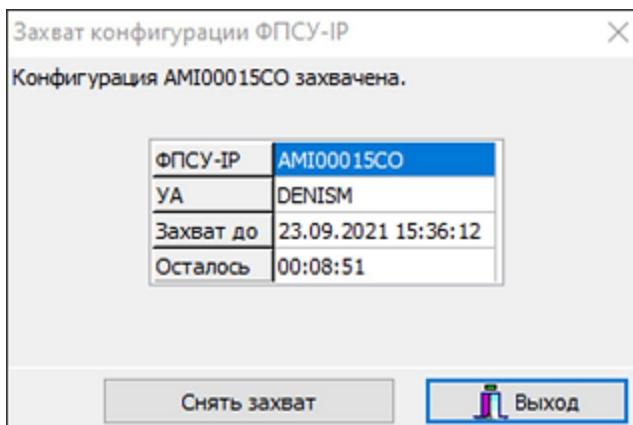


Рисунок 315 – Предупреждение о захвате конфигурации

В случае, если изменение конфигурации инициировано одновременно двумя пользователями, пользователю, вносящему изменения вторым, будет также выдано предупреждение о недавнем изменении конфигурации:

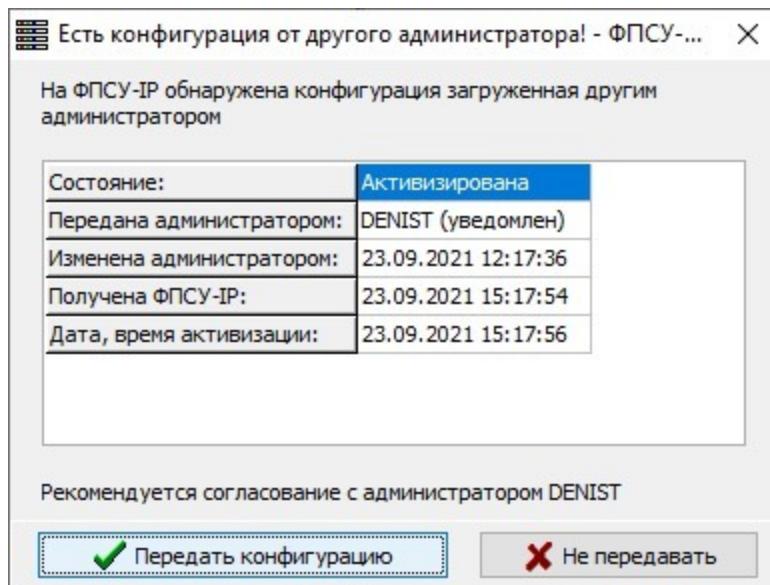


Рисунок 316 – Предупреждение при одновременном редактировании конфигурации двумя администраторами

Для автосохранения информации о версиях ФПСУ-IP в БД установить флаг

«Сохранять версию ФПСУ-IP во внешнюю БД в фоне» и задать период сохранения, после чего нажать на кнопку «Сохранить настройку».

Версии ФПСУ-IP могут быть сохранены по запросу с помощью опций «Сохранить в БД все версии ФПСУ-IP» и «Сохранить в БД измененные версии ФПСУ-IP».

18.1.6. Учетная информация по ФПСУ-IP

Учетная информация по ФПСУ-IP представляет собой данные об IP-адресах, а также дополнительные сведения о ФПСУ-IP, которые пользователи УА ФПСУ-IP могут вносить по кнопке «Показ учетной информации по ФПСУ-IP»:

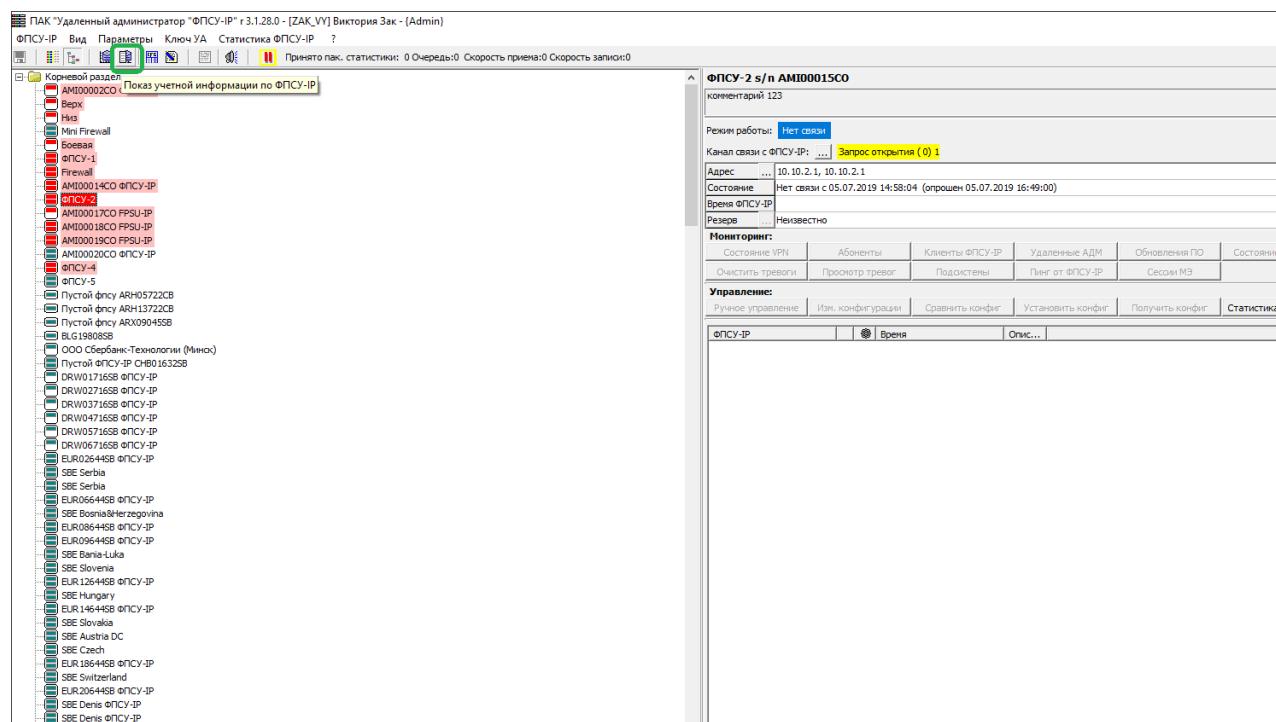


Рисунок 317 – Настройка внешней БД

По нажатию этой кнопки открывается окно, в котором пользователь ФПСУ-IP может вносить те или иные необходимые сведения по выбранному в общем списке ФПСУ-IP:

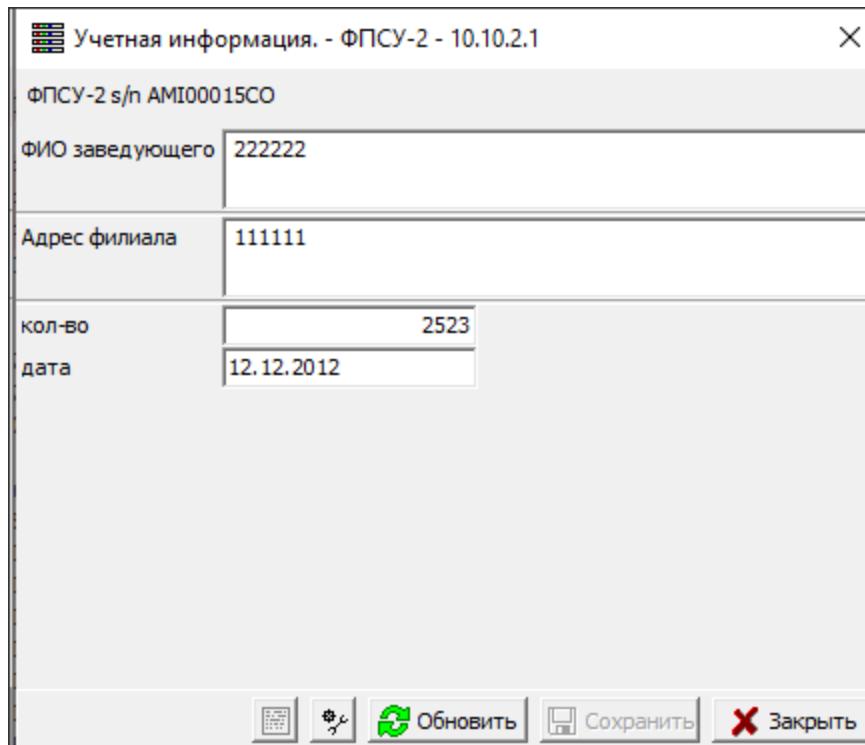


Рисунок 318 – Окно ввода дополнительной (учетной) информации

Список дополнительных полей, в которые можно вводить информацию о ФПСУ-IP, составляется администратором внешней БД (раздел «Настройка полей учетной информации»).

18. 1. 6. 1. Просмотр дополнительной информации по ФПСУ-IP

18. 1. 6. 2. Настройка полей учетной информации

18. 2. Взаимодействие ФПСУ-IP со внешней БД

В основном окне УА ФПСУ-IP после изменения тех или иных параметров определенного ФПСУ-IP можно записать эти изменения во внешнюю базу данных. Так же возможно обновить параметры выбранного ФПСУ-IP в соответствии со сведениями, сохраненными в базе данных.

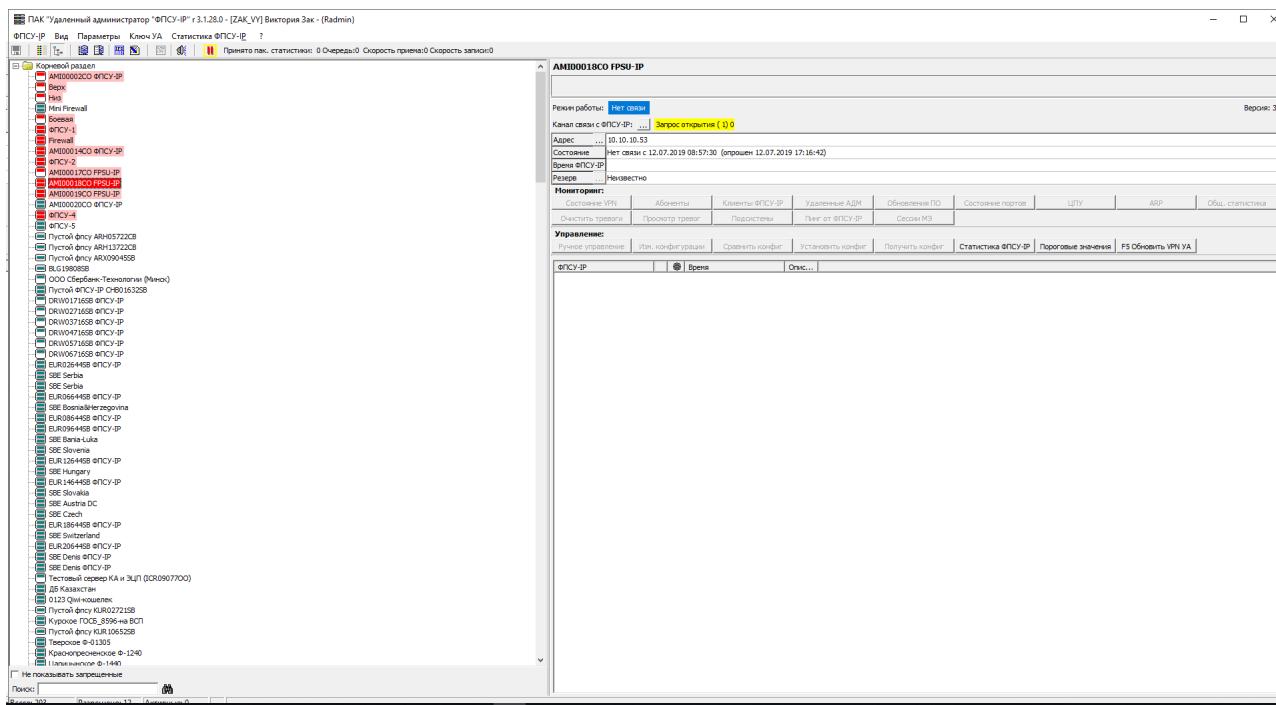


Рисунок 319 – Основное окно программы

18. 2. 1. Обновление ФПСУ-ИР из внешней БД

Для того, чтобы обновить параметры одного ФПСУ-IP в соответствии со сведениями, сохраненными во внешней БД, необходимо выбрать запись в общем списке основного окна программы и из выпадающего по нажатию правой клавиши мыши списка выбрать пункт «Обновить ФПСУ-IP из внешней БД».

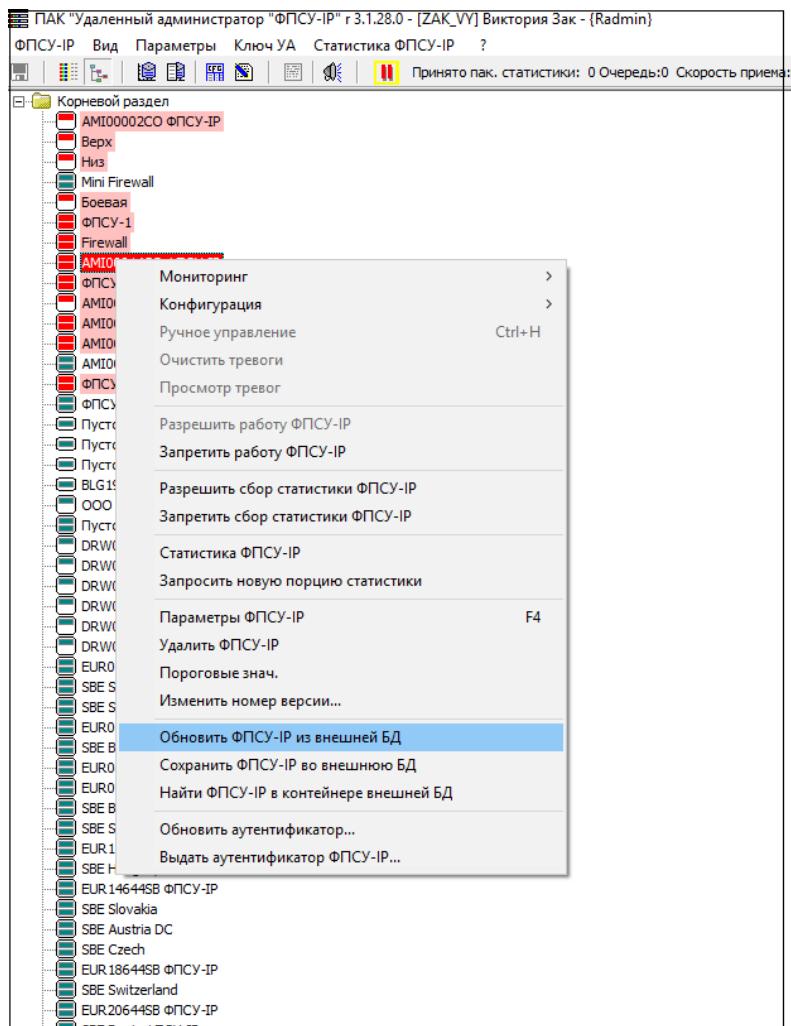


Рисунок 320 – Выбор пункта контекстного меню

Система выдаст следующее сообщение:

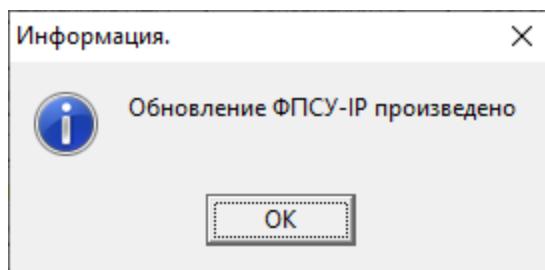


Рисунок 321 – Сообщение об обновлении ФПСУ-IP

В том случае, если параметры ФПСУ-IP совпадают с сохраненными во внешней БД, на экран будет выведено следующее сообщение:

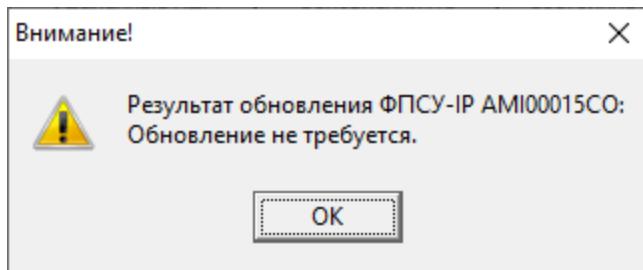


Рисунок 322 – Обновление не требуется

18. 2. 2. Сохранение ФПСУ-IP во внешней БД

Для того, чтобы сохранить измененные параметры одного ФПСУ-IP во внешней БД, необходимо выбрать запись в общем списке основного окна программы и из выпадающего по нажатию правой клавиши мыши списка выбрать пункт «Сохранить ФПСУ-IP во внешнюю БД».

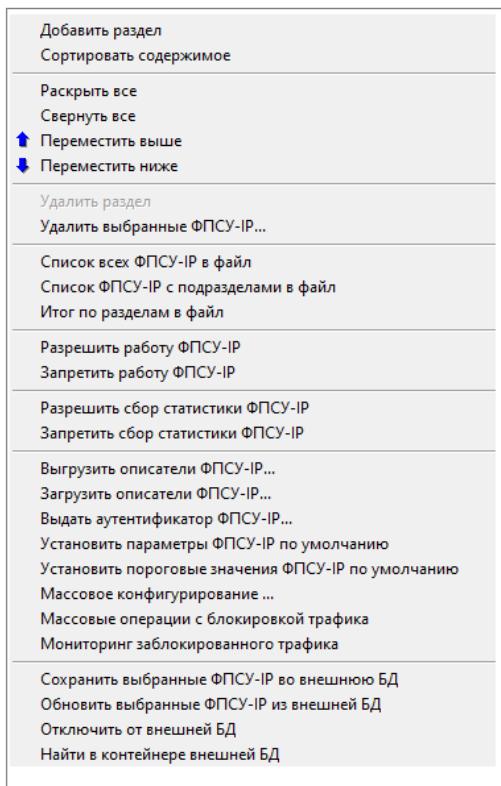


Рисунок 323 – Выбор пункта контекстного меню

Система выдаст следующее сообщение:

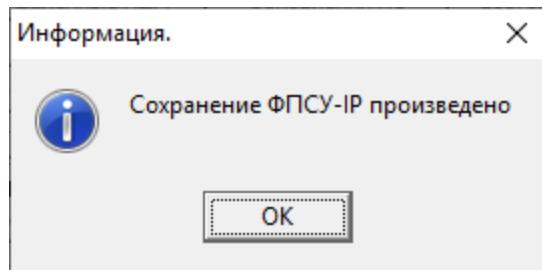


Рисунок 324 – Сохранение ФПСУ-IP произведено

19. Управление статистикой ФПСУ-IP

УА ФПСУ-IP позволяет получать, просматривать и обрабатывать статистическую информацию о работе подконтрольных ФПСУ-IP, которая хранится локально на ФПСУ-IP (см. документ «Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4.0.1. Руководство администратора ФПСУ-IP»).

Администратору УА ФПСУ-IP могут быть предоставлены следующие данные:

- о соединениях абонентов и клиентов с ФПСУ-IP (передача данных в открытом виде и через VPN-туннель, ошибки при передаче, отказ в доступе, отсутствие связи, статистика передачи данных за сутки);
- о работе локальных администраторов (запуск компьютера ФПСУ-IP, начало и окончание работы ФПСУ-IP, регистрация ТМ-идентификаторов и их удаление, изменение параметров конфигурации ФПСУ-IP, установка изменений или дополнений к программному обеспечению ФПСУ-IP, регистрация администраторов УА ФПСУ-IP и т.д.);
- о работе администраторов УА ФПСУ-IP (получение статистических данных и правил фильтрации ФПСУ-IP, изменение текущего времени ФПСУ-IP, дистанционная установка изменений или дополнений к программному обеспечению и т.д.);
- о работе подсистемы резервирования (синхронизация данных).

Статистические записи предоставляются администратору с указанием времени и даты события, вида события, а также адресов абонентов, объема передаваемой информации и других необходимых данных.

Статистическая информация о работе абонентов и клиентов ФПСУ-IP предоставляется любому зарегистрированному этим ФПСУ-IP администратору, а данные о работе локальных и удаленных администраторов может получить только тот администратор УА ФПСУ-IP, которому такое право локальным администратором предоставлено специально.

УА ФПСУ-IP содержит средства сортировки и поиска регистрационных записей по задаваемым администратором условиям: типам событий, произошедших на конкретных ФПСУ-IP, а также по времени их возникновения.

Для оптимизации использования свободного пространства памяти внутреннего накопителя, УА ФПСУ-IP позволяет упаковывать (в собственном формате) и перемещать

регистрационные данные в файл архива.

Для работы с регистрационными данными ФПСУ-IP предназначена группа команд «Статистика ФПСУ-IP» главного меню УА ФПСУ-IP.

19. 1. Получение статистической информации

Статистическая информация может поступать в базу данных УА ФПСУ-IP различными способами:

- в процессе автоматического опроса ФПСУ-IP, если при их регистрации автоопрос статистики был разрешен и были установлены необходимые параметры опроса (см. раздел «Установка параметров взаимодействия ФПСУ-IP с УА ФПСУ-IP»);
- в режиме ручного управления отдельным ФПСУ-IP по сети;
- из архива, созданного УА ФПСУ-IP (или ранней DOS версией УА ФПСУ-IP) ранее.

Внимание! Для начала сбора статистики в базу данных УА ФПСУ-IP требуется включить режим сбора статистики с управляемых ФПСУ-IP. Для этого необходимо активировать переключатель главного меню «Статистика ФПСУ-IP» → «Включен сбор статистики ФПСУ-IP». Опция включения сбора статистики становится доступна только после настройки базы данных статистики (см. пункт «Настройка базы данных статистики УА ФПСУ-IP»), необходимо выключить флаг «Доступ к БД только чтение (просмотр статистики)». При этом в окне установки параметров ФПСУ-IP (см. пункт «Установка параметров взаимодействия ФПСУ-IP с УА ФПСУ-IP») следует настроить данные автоопроса статистики - задать интервал опроса, установить переключатель «Статистика разрешена», выбрать типы и подтипы статистики. Также в конфигурации ФПСУ-IP в общих параметрах должны быть отменены «Ограничения сбора статистики».

19. 1. 1. Автоматический сбор статистической информации

Для проведения автоматического сбора регистрационной информации подконтрольного ФПСУ-IP необходимо указать УА ФПСУ-IP при его регистрации, что автоопрос с целью получения статистики разрешен, и установить необходимые рабочие параметры: время начала и конца ежедневного опроса, период опроса, типы данных и др. (см. раздел «Установка параметров взаимодействия ФПСУ-IP с УА ФПСУ-IP»).

Следует обратить внимание, что независимо от того, какие данные заказаны к получению, ФПСУ-IP предоставит администратору только ту информацию, к которой он имеет доступ.

Текущее состояние работы УА ФПСУ-IP по автоматическому опросу статистики для выбранного в окне списка ФПСУ-IP можно просмотреть на панели информации напротив поля «Состояние VPN».

19. 1. 2. Получение статистики по сети по запросу администратора

Для получения статистики по запросу администратора с ФПСУ-IP необходимо выйти в режим ручного управления и нажать кнопку «Получить статистику» в разделе Статистика.

Появится окно выбора статистических данных, запрашиваемых с ФПСУ-IP, в котором необходимо установить условия поиска: необходимые типы и подтипы данных и значения интервалов даты и времени. С помощью кнопок «Сегодня 0 часов» и «Сейчас» можно быстро установить время съёма информации за текущие сутки.

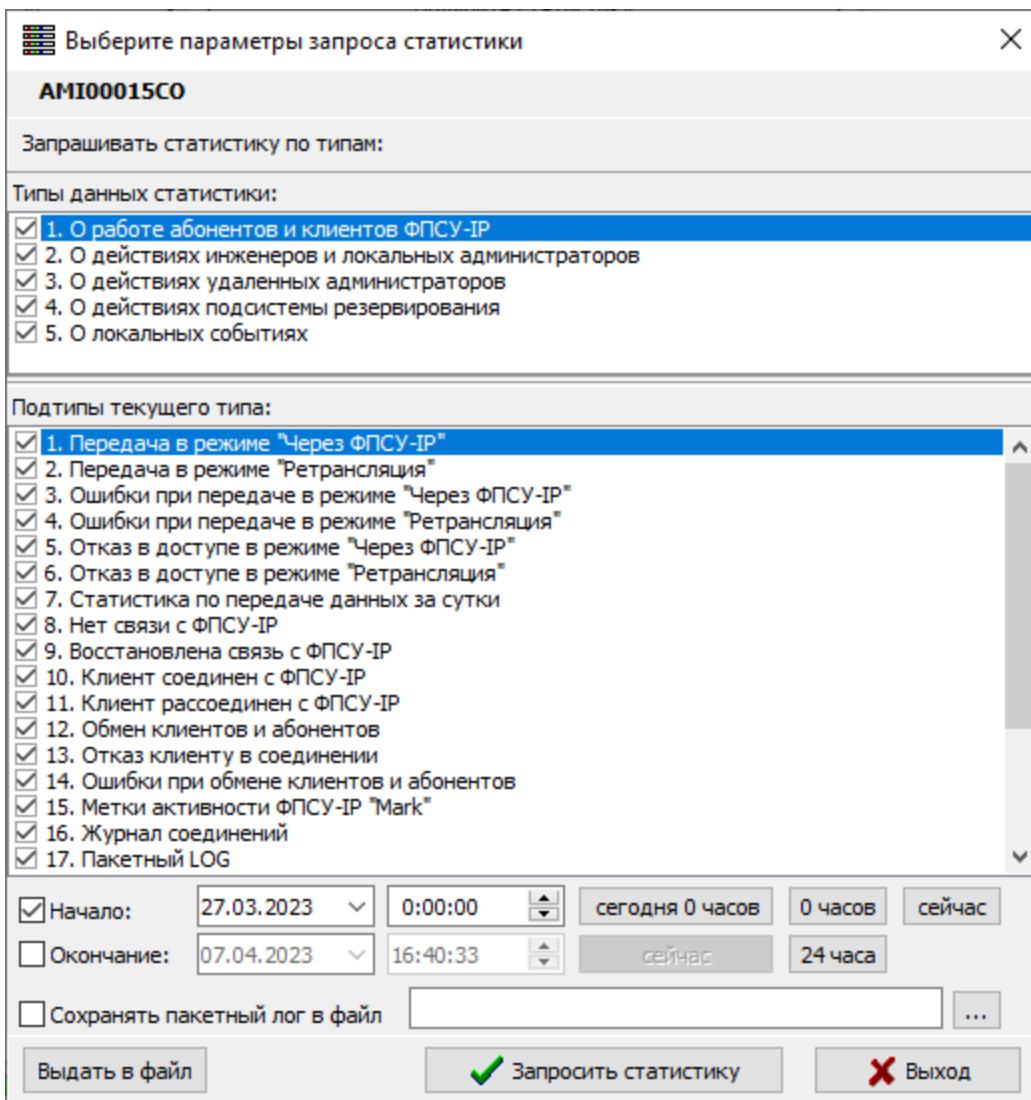


Рисунок 325 - Окно выбора типов и времени запрашиваемой вручную статистики

При установлении флага «Сохранять пакетный лог в файл» сохраняется дамп трафика в сокращенном виде в файл. Для сохранения дампа трафика необходимо, чтобы на ФПСУ-IP был включен межсетевой экран, в общих параметрах ФПСУ-IP было задано гарантированное логирование всех событий, собиралась статистика по пакетному логу.

После выбора требуемых параметров необходимо нажать кнопку «Запросить статистику» для опроса ФПСУ-IP, или «Выход» для отмены процедуры запроса. УА ФПСУ-IP при установленном туннеле запросит указанную информацию и загрузит в свою базу данных.

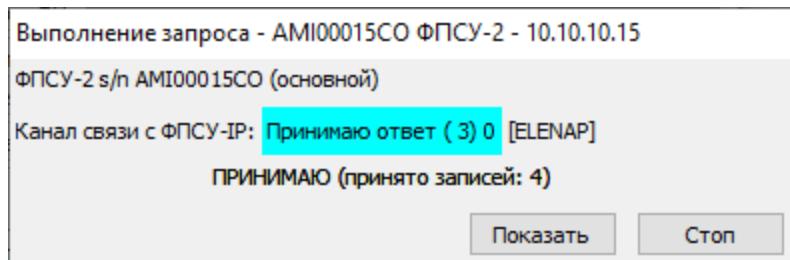


Рисунок 326 - Выполнение запроса статистики

После загрузки статистики на экран будет выдано сообщение с предложение просмотреть статистики.

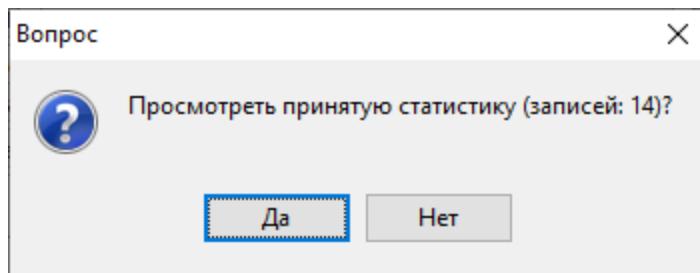


Рисунок 327 - Сообщение о просмотре статистики

В отдельном окне выводятся записи статистики в хронологическом порядке с датой и типом события.

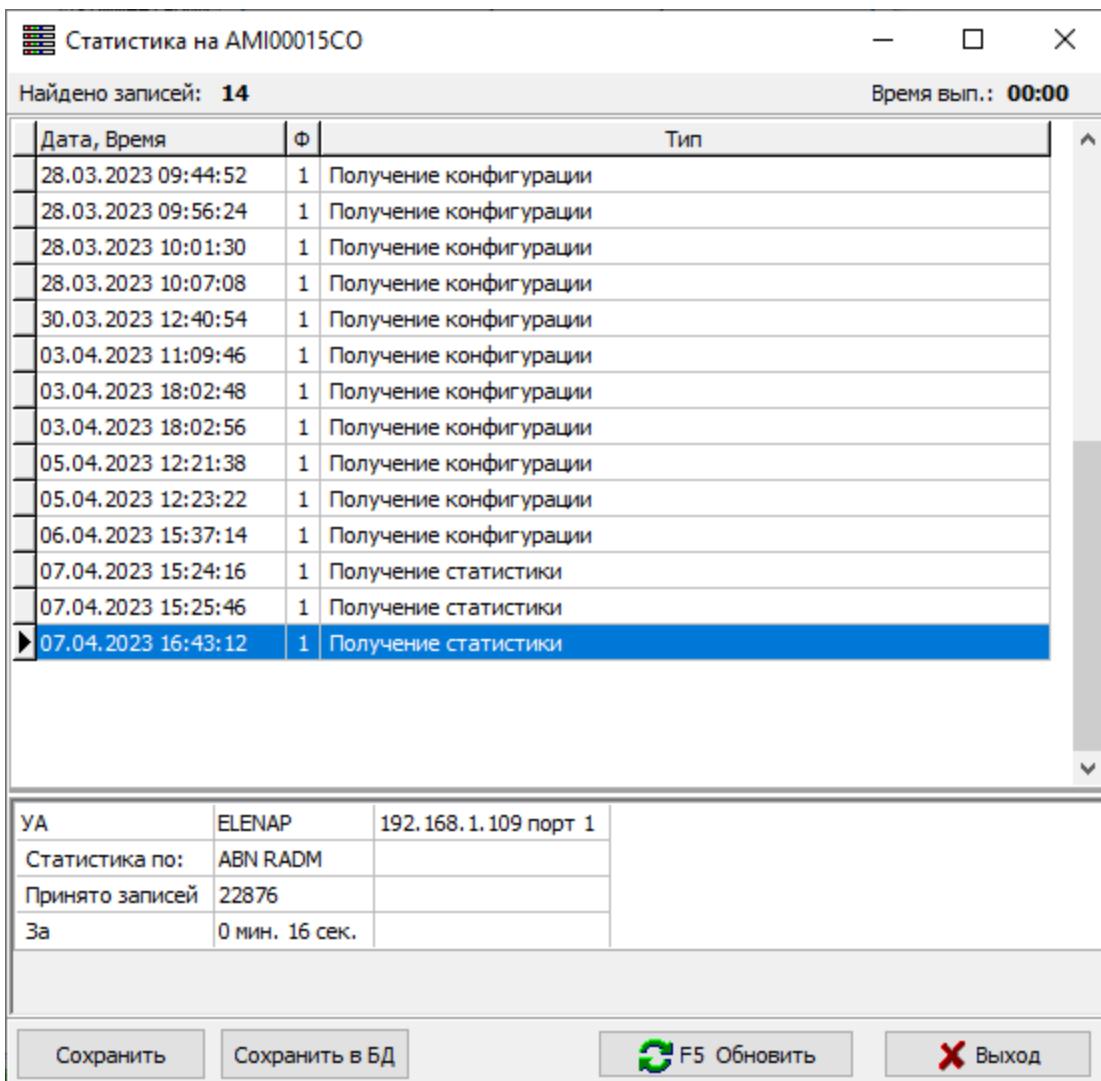


Рисунок 328 - Окно просмотра статистики

19. 1. 3. Загрузка статистической информации из DOS архива UA ФПСУ-IP

Загрузка статистики из DOS-архива предназначена для возможности работы с теми статистическими данными, которые были собраны предыдущей версией UA ФПСУ-IP, работающей в DOS-режиме.

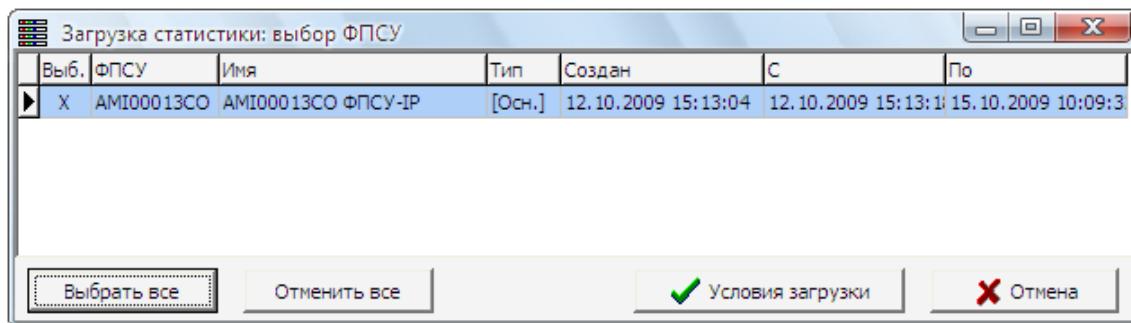


Рисунок 329 - Загрузка статистики из архива

Для переноса статистических данных из DOS-архива следует выполнить команду главного меню «Статистика ФПСУ-IP» → «Загрузить статистику из локальной копии», и в открывшемся окне выбрать каталог, в котором хранятся файлы DOS-архива, имеющиеся файлы с расширением «.STA». После нажатия кнопки «Выбор» открывается окно управления найденными в архиве записями статистики. В нем отображается список ФПСУ-IP, по которым в данном файле архива есть статистика, с указанием типа ФПСУ-IP (основной или резервный), даты создания архива, и диапазона дат записей статистики, хранящейся в нём.

Каждый ФПСУ-IP, статистику по которому требуется загрузить из DOS-архива в базу данных УА ФПСУ-IP, следует отметить мышью в поле «Выб.» или нажав клавишу «Пробел» при установленном напротив записи курсоре. Для загрузки статистики по всем ФПСУ-IP следует нажать кнопку «Выбрать все». Открывается окно выбора параметров загрузки, аналогичное окну при запросе статистики по команде администратора (см. пункт «Получение статистической информации»), в котором так же требуется указать типы забираемой статистики и подтвердить выбор нажатием кнопки «Запросить статистику».

19. 2. Просмотр накопленных статистических данных

Для просмотра регистрационных данных отдельного ФПСУ-IP, накопленных в базе данных УА ФПСУ-IP, требуется выбрать в окне списка ФПСУ-IP и нажать кнопку «Статистика ФПСУ-IP» панели команд.

Откроется служебное окно установки параметров просматриваемой статистики, в котором необходимо установить фильтры поиска: необходимые типы и подтипы данных и значения интервалов даты и времени.

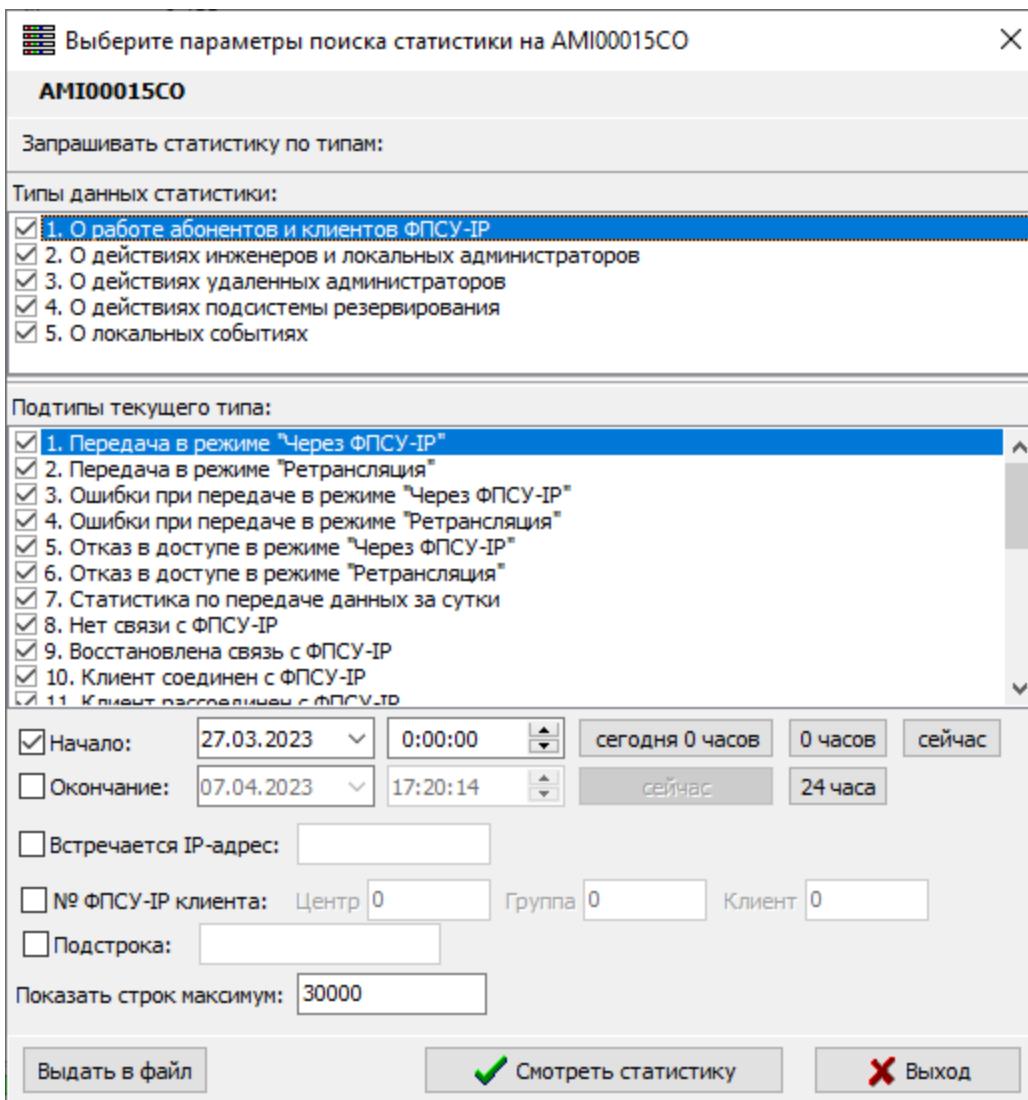


Рисунок 330 - Запрос на просмотр статистики

Поле «Встречается IP-адрес» позволяет сделать запрос по статистике работы через ФПСУ-IP отдельного абонента по известном IP-адресу.

Поле «№ ФПСУ-IP Клиента» позволяет сделать запрос по статистике работы через ФПСУ-IP отдельного Клиента по его известным системным данным номеру Криптосети, номеру группы и персональному номеру Клиента в группе.

Поле «Подстрока» позволяет сделать фильтр запроса по встречающемуся в записи статистики слову, например имени клиента.

Для просмотра статистики следует нажать кнопку «Смотреть статистику», или кнопку «Выход» для отмены запроса.

По окончании поиска по заданным условиям результат будет показан в информационном окне «Статистика». Регистрационные записи отображаются с указанием времени и даты события, вида события, а также адресов абонентов, объема передаваемой информации и других данных, выдаваемых в нижней части окна в виде комментария. Цифры слева вверху означают номер текущей записи (отмеченной строкой выбора) в списке и, справа, общее число записей в представленной выборке статистических данных.

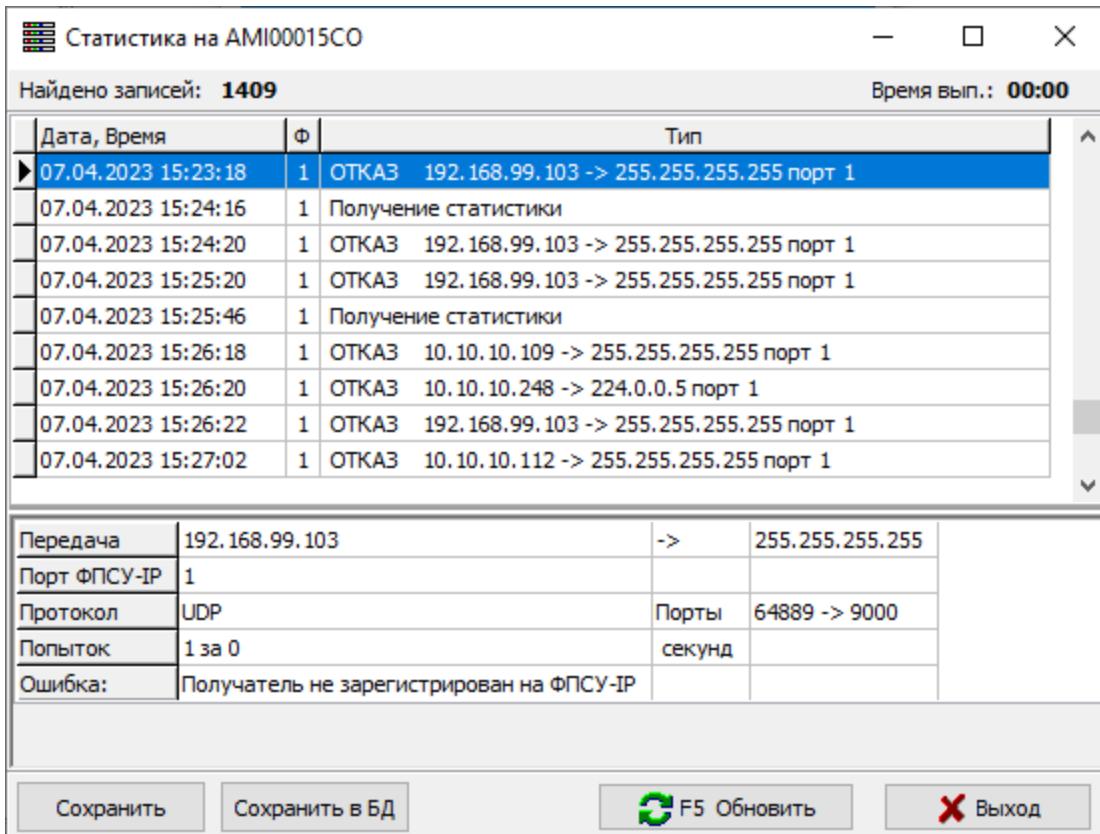


Рисунок 331 - Просмотр статистики

Кнопка «F5 Обновить» выполняет повторный запрос с последними указанными параметрами, и отображает новые записи статистики, которые могли попасть за прошедшее время под повторный запрос.

Регистрационная информация о работе абонентов может быть конвертирована УА ФПСУ-IP в файлы txt-формата для последующей обработки сторонними программами. Следует обратить внимание, что в txt-файлы будут выведены те данные, которые были выбраны из хранилища по заданным администратором условиям поиска.

19. 2. 1. Наблюдение за автоматическим сбором статистики

За ФПСУ-IP можно установить наблюдение. В случае превышения пороговых значений параметров ФПСУ-IP, сообщение от SMTP-сервера будет отправляться на указанную электронную почту.

Предварительно требуется задать пороговые значения параметров ФПСУ-IP (см. пункт «Настройка пороговых значений на ФПСУ-IP»).

Затем необходимо установить параметры почты. Необходимо выбрать пункт меню «Параметры» → «Настройка отправки почты». В открывшемся окне задать SMTP сервер, порт, отправителя, данные для авторизации, почту для отправки пробного письма.

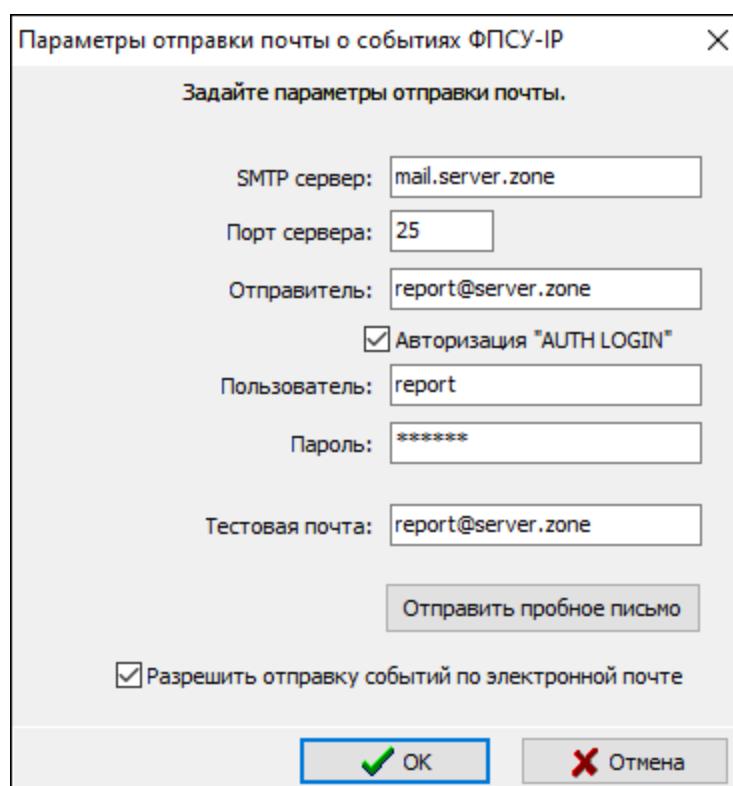


Рисунок 332 - Настройка отправки почты

19. 3. Перемещение статистики в архив

УА ФПСУ-IP содержит встроенный архиватор, позволяющий упаковывать регистрационные записи ФПСУ-IP (скимая их для дальнейшего хранения) в файлы внутреннего формата и перемещать в файл на внутреннем накопителе компьютера УА ФПСУ-IP администратора или на внешние носители.

Архивирование может производиться как в ручном, так и в автоматическом режимах (см. пункт «Получение статистической информации»).

19. 3. 1. Перемещение статистики в архив администратором

Чтобы переместить статистику в архивные файлы вручную, следует воспользоваться командой главного меню «Статистика ФПСУ-IP → Выгрузить БД статистики в архив».

Появится служебное окно подтверждения выполняемой операции, для запуска процесса архивации необходимо нажать кнопку «Да».

Следует обратить внимание, что в процессе архивирования статистические данные изымаются из базы данных и могут быть просмотрены только с помощью предварительной распаковки, описанной в подразделе «Просмотр статистики из архива».

В результате выполнения выгрузки базы данных, формируется файл архива и служебное оповещение о его месторасположении.

Файл архива помещается в подкаталог Stat рабочего каталога УА ФПСУ-IP, получает расширение «.DB» и название, состоящее из названия архивируемой базы данных, букв ARC (archive, архив), даты создания архива в формате ГГММДД, и порядкового номера создаваемого за указанные сутки архива (если создаётся несколько за один день).

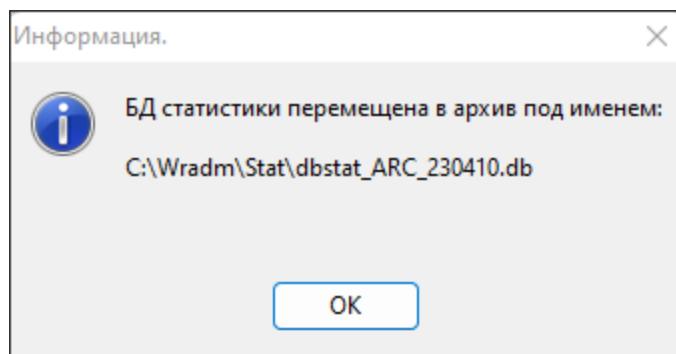


Рисунок 333 - Успешная архивация базы данных статистики

19. 3. 2. Автоматическое перемещение статистики в архив

Администратор может установить режим автоматического архивирования статистических данных одновременно для всех зарегистрированных у него ФПСУ-IP, воспользовавшись командой главного меню «Статистика ФПСУ-IP» → «Параметры архивации статистики». После выбора этой команды на экран будет выдано окно настроек, в поля которого следует ввести необходимые параметры автоматического архивирования.

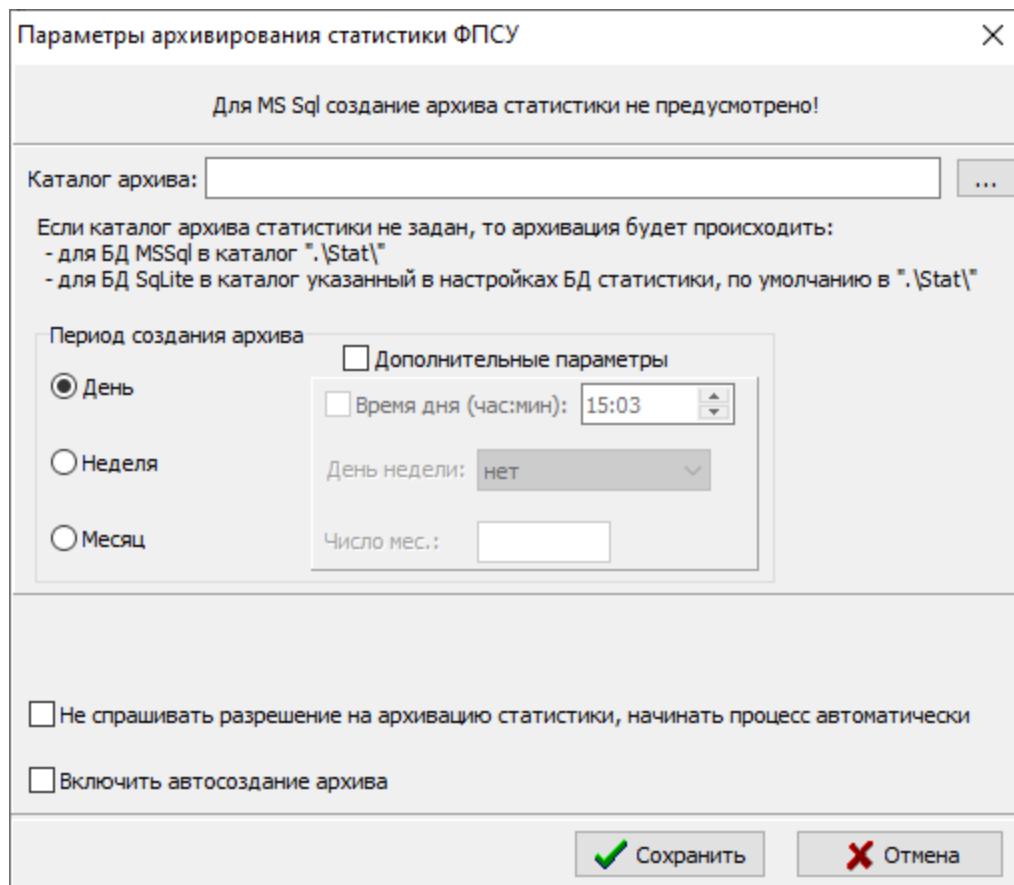


Рисунок 334 - Параметры автоматической архивации статистики

В окне настроек предоставляется возможность указать следующие параметры автоматической архивации:

- каталог, куда будут выгружаться файлы (если не указан, то архивация будет происходить в каталоги по умолчанию);
- период, с которым будет производиться автоматическое архивирование, начиная с текущего момента: раз в день, раз в неделю или раз в месяц. Опционально можно указать время, день недели (если выбран режим «раз в неделю») и число месяца, в который будет выполняться архивация.

Архив статистики будет создан, только если для ведения статистики настроена БД SQLite, для БД MSSql и PostgreSQL архив статистики не предусмотрен.

После осуществления всех установок следует установить флаг «Включить автосоздание архива» и нажать кнопку «Сохранить» для активации произведённых настроек.

19. 4. Просмотр статистики из архива

Из общей базы данных статистики УА ФПСУ-IP удаляется перемещаемая в архив статистика, в момент создания файла архива. Для просмотра помещенной в архив статистики необходимо выполнить команду главного меню «Статистика ФПСУ-IP» → «Просмотр статистики из архива». УА ФПСУ-IP вызовет стандартное окно выбора файла, в котором следует указать, статистику из какого именно архива-файла требуется просмотреть.

После выбора файла откроется окно уведомления о необходимости сканирования БД:

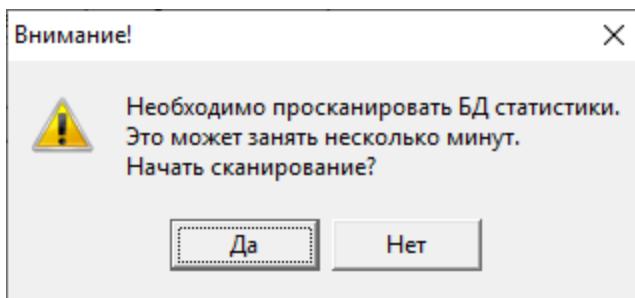


Рисунок 335 - Запрос начала сканирования

По нажатию кнопки «Да» на экран будет выведено служебное окно, содержащее список статистики с разбиением на ФПСУ-IP, к которым эта статистика относится. Просматривать одновременно можно статистику только по одному ФПСУ-IP.

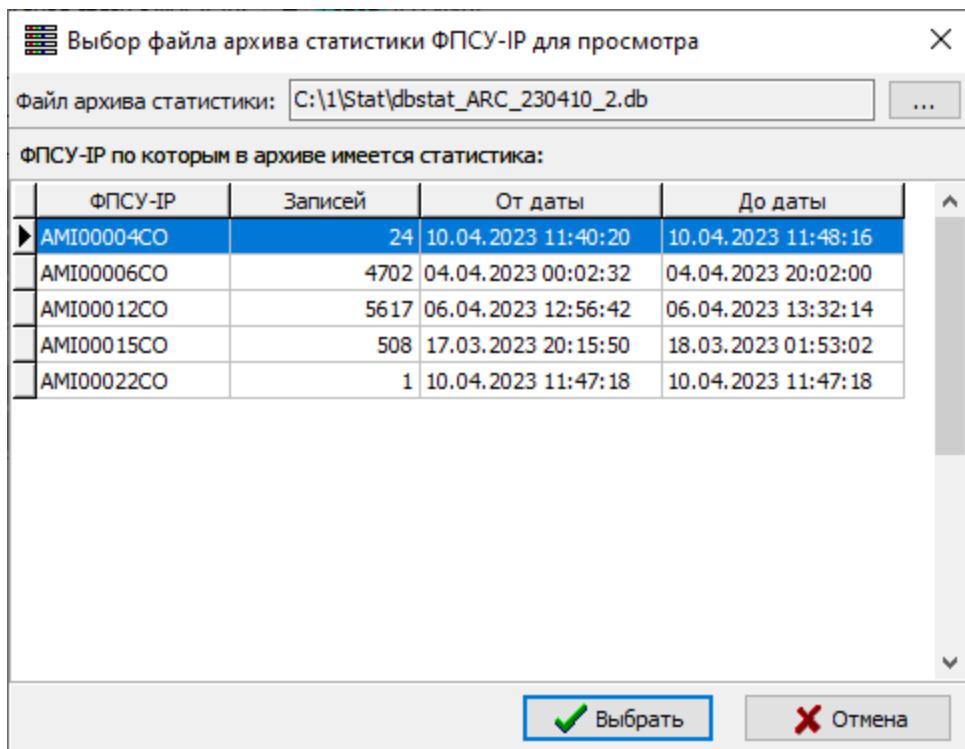


Рисунок 336 - Выбор просмотра статистики ФПСУ-IP из сохранённого архива

После выбора ФПСУ-IP, статистику по работе которого требуется посмотреть, необходимо нажать кнопку «Выбрать» для перехода к окну поиска статистики. Дальнейшие действия аналогичны поиску статистики по ФПСУ-IP в базе данных УА ФПСУ-IP (см. подраздел «Просмотр накопленных статистических данных»).

20. Рекомендованные процедуры смены ключей УА

Срок действия ключевой информации отсчитывается с момента генерации ключевых данных и не должен превышать 15 месяцев. До истечения срока действия текущих ключевых данных требуется повторно сгенерировать и установить новые ключевые данные.

В частности, такой ключевой информацией являются ключ УА, ключ шифрование БД УА, ключ доступа УА ко внешней БД.

20. 1. Процедура смены ключа УА

На УА ФПСУ-IP поддерживается смена старого ключа УА на новый и передача на ФПСУ-IP нового ключа УА. Смену ключа УА следует осуществлять каждые 15 месяцев.

Администратор УА ФПСУ-IP создает новую ключевую пару УА для смены. Ключевая пара УА содержит «закрытый» ключ, записываемый на VPN-Key/UA и «открытый» ключ (далее ключ УА или открытый ключ), передаваемый на ФПСУ-IP.

Смена старого ключа на новый на ФПСУ-IP производится одним из двух способов:

- рекомендуемый: локальным администратором ФПСУ-IP. В этом случае процедура совпадает с регистрацией на ФПСУ-IP нового удаленного администратора (см. документ «Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4.0.1. Руководство администратора ФПСУ-IP»);
- дистанционно, другим администратором УА указанного ФПСУ-IP, при этом срок действия ключа, загружаемого на ФПСУ-IP, меняется на срок действия ключа администратора УА, который выполняет смену ключа. Этот вариант описывается ниже.

Для пересоздания или смены ключа УА администратор УА ФПСУ-IP создаёт ключевую пару УА (см. пункт «Пересоздание ключевых данных администратора УА ФПСУ-IP»), которая генерируется и записывается в виде файла формата *.AD2 или *.ADM. Файл с новым ключом УА следует передать администратору УА ФПСУ-IP, осуществляющему смену ключа на ФПСУ-IP.

Администратору УА ФПСУ-IP, осуществляющему смену ключа УА на ФПСУ-IP, необходимо:

1. В контекстном меню ФПСУ-IP выбрать команду «Ручное управление».

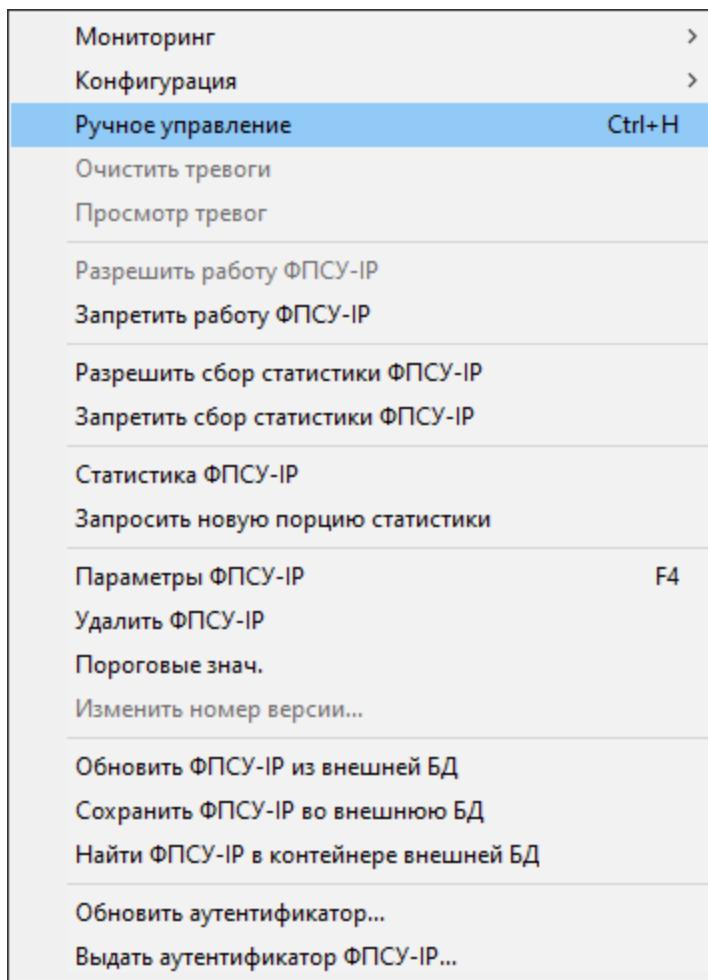


Рисунок 337 - Контекстное меню ФПСУ-IP

2. Откроется меню с командами ручного управления ФПСУ-IP. В разделе «Управление ФПСУ-IP» следует выбрать команду «Редактировать УА», откроется окно регистрации удаленных администраторов.

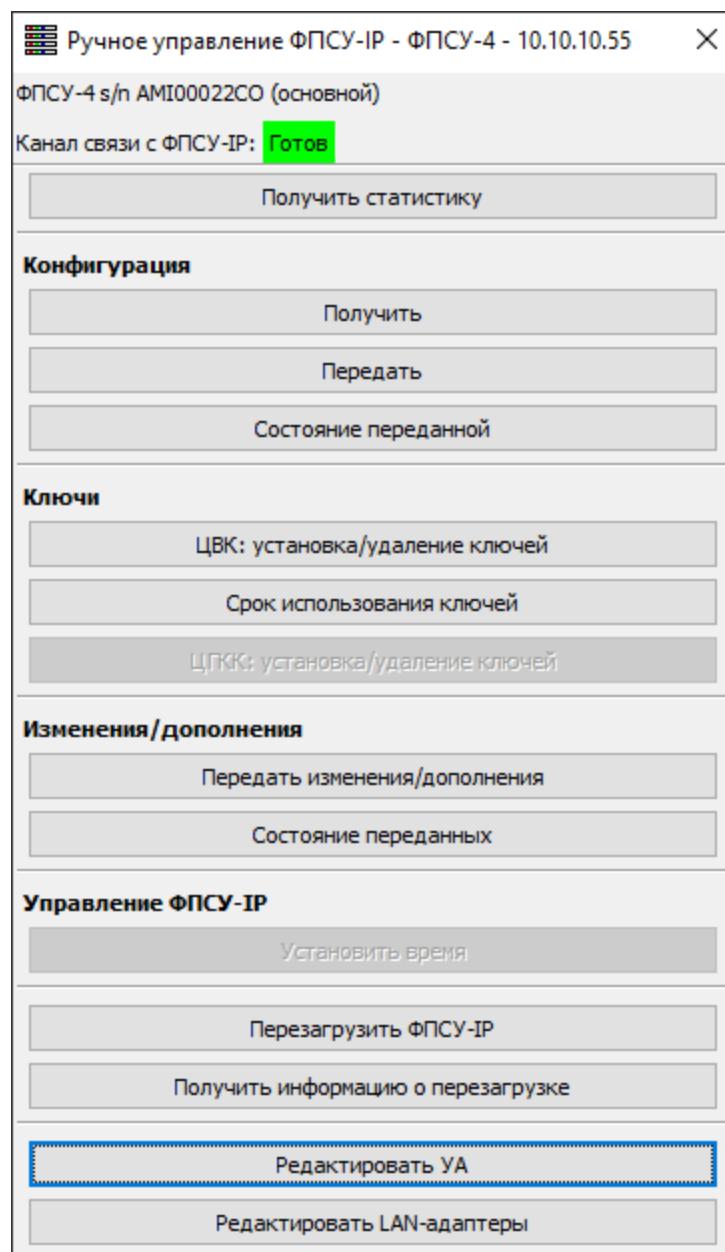


Рисунок 338 - Меню «Ручное управление»

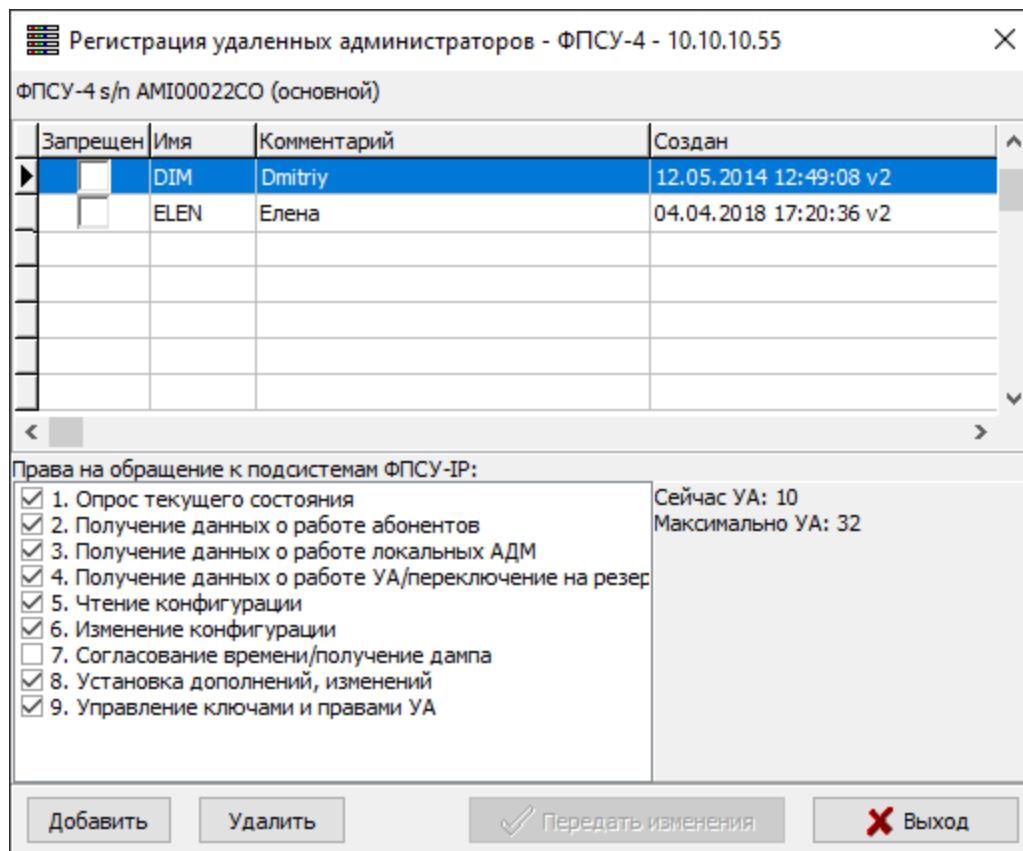


Рисунок 339 - Список удаленных администраторов ФПСУ-IP

3. Требуется проверить состояние флага «Согласование времени/получение дампа» у всех администраторов из списка. Право на согласование времени может быть выдано только одному администратору УА ФПСУ-IP. Флаг должен быть обязательно установлен у одного из администраторов УА ФПСУ-IP.

В случае, если флаг не установлен ни у одного из администраторов, передать изменения на ФПСУ-IP не удастся и на экран будет выдано сообщение:

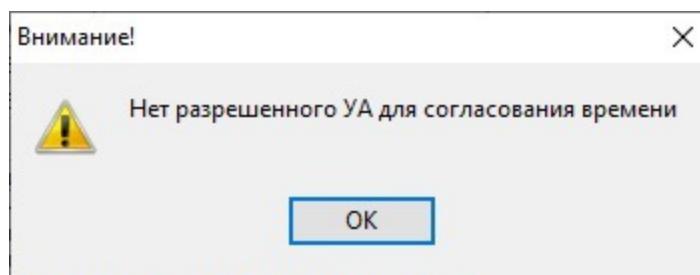


Рисунок 340 - Проблема при передаче изменений на ФПСУ-IP

4. У администратора УА ФПСУ-IP, производящего смену ключа, должно быть право «Управление ключами и правами УА» на выбранном ФПСУ-IP.
5. В окне регистрации удаленных администраторов в списке следует выбрать администратора УА ФПСУ-IP, которому требуется смена ключей.
6. Старый ключ УА должен быть предварительно удален с управляемого ФПСУ-IP. Следует нажать кнопку «Удалить», на экран будет выдано окно для подтверждения операции.

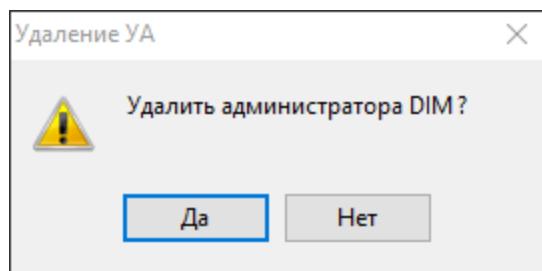


Рисунок 341 - Подтверждение операции

Следует нажать кнопку «Да» для подтверждения удаления старого ключа. Администратор УА ФПСУ-IP будет удален из списка администраторов.

7. Для загрузки нового ключа УА ФПСУ-IP в окне регистрации удаленных администраторов необходимо нажать кнопку «Добавить». Откроется стандартное окно выбора каталога, следует выбрать каталог с файлом *.AD2 или *.AD4.

На экран будет выдано окно с найденными открытыми ключами администратора УА ФПСУ-IP.

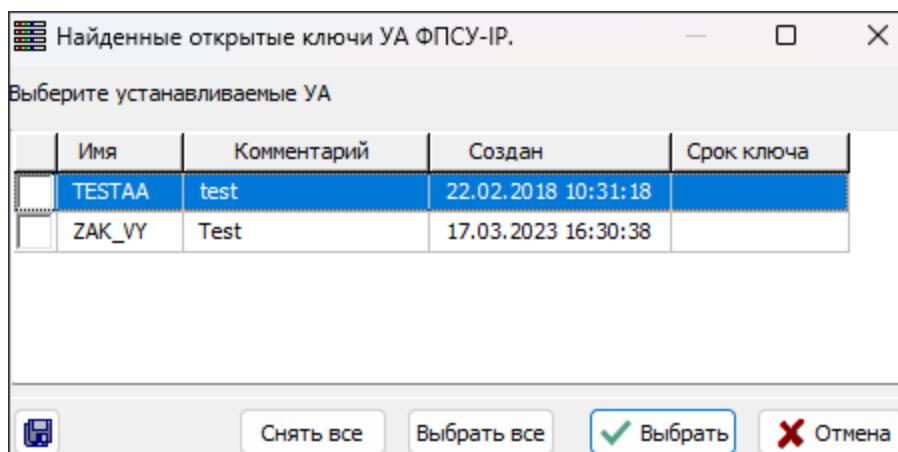


Рисунок 342 - Найденные открытые ключи УА ФПСУ-IP

8. В строке с открытым ключом администратора УА ФПСУ-IP следует установить флаг и нажать кнопку «Да». Новый ключ УА администратора будет установлен.
 9. Администратор УА ФПСУ-IP добавляется в список администраторов в статусе «Запрещен», необходимо снять флаг в строке с вновь добавленным администратором УА ФПСУ-IP и нажать кнопку «Передать изменения» для передачи нового ключа УА на ФПСУ-IP.

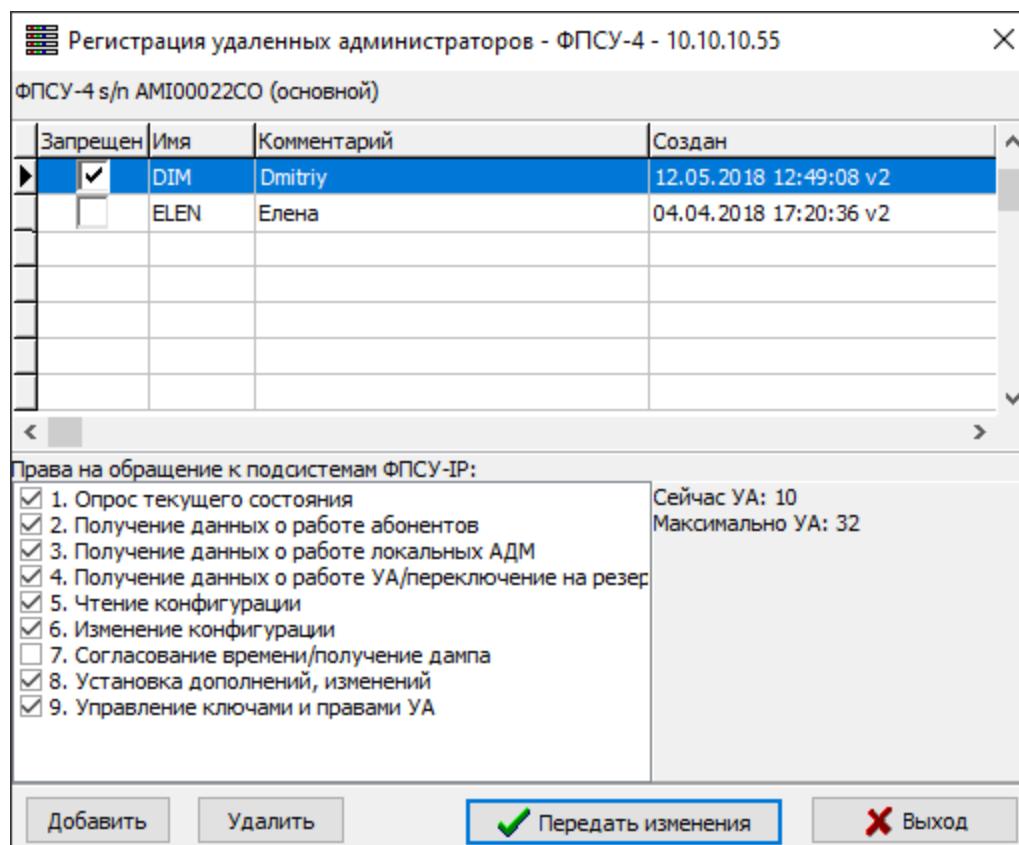


Рисунок 343 - Окно «Регистрация удаленных администраторов»

На экран будет выдано окно подтверждения операции, для обновления ключа УА администратора на ФПСУ-IP следует нажать кнопку «Да».

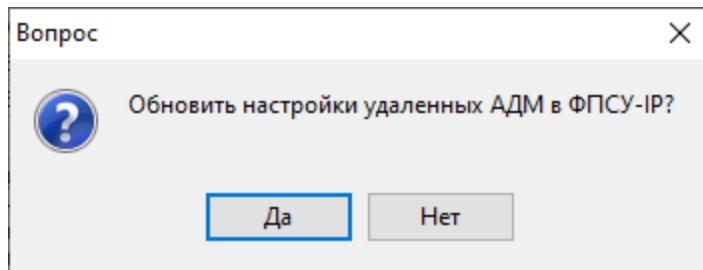


Рисунок 344 - Окно подтверждения операции

На время, пока информация на ФПСУ-IP будет обновляться, связь с ФПСУ-IP будет потеряна и на экран будет выдано сообщение:

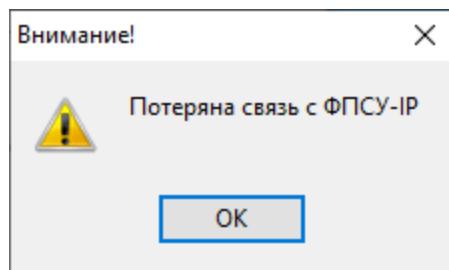


Рисунок 345 - Потеря связи с ФПСУ-IP

После того, как информация на ФПСУ-IP обновится на экран будет выдано сообщение об успешной смене ключа УА администратора на ФПСУ-IP.

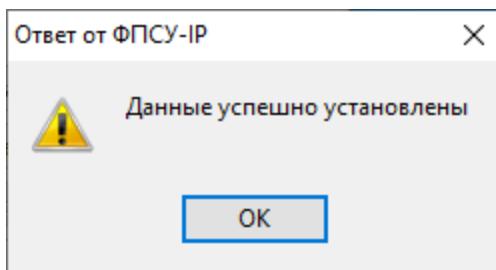


Рисунок 346 - Сообщение об успешной смене ключей

20. 2. Процедура смены ключа шифрования БД УА

В базе данных УА ФПСУ-IP (далее БД УА ФПСУ-IP) хранятся параметры управляемых ФПСУ-IP, зашифрованные на специальном ключе. Смену ключа шифрования БД УА ФПСУ-IP следует осуществлять каждые 15 месяцев.

Смену ключа шифрования БД УА может осуществлять первый администратор УА

ФПСУ-IP, созданный при первом запуске (см. пункт «Первоначальная настройка УА ФПСУ-IP (с VPN-Key/UA)»).

Для пересоздания или смены ключа шифрования БД УА необходимо:

1. Выбрать команду главного меню «Ключ УА» → «Доступ УА к ключу шифрования БД».
2. В открывшемся окне следует нажать кнопку «Пересоздать ключ шифрования БД».

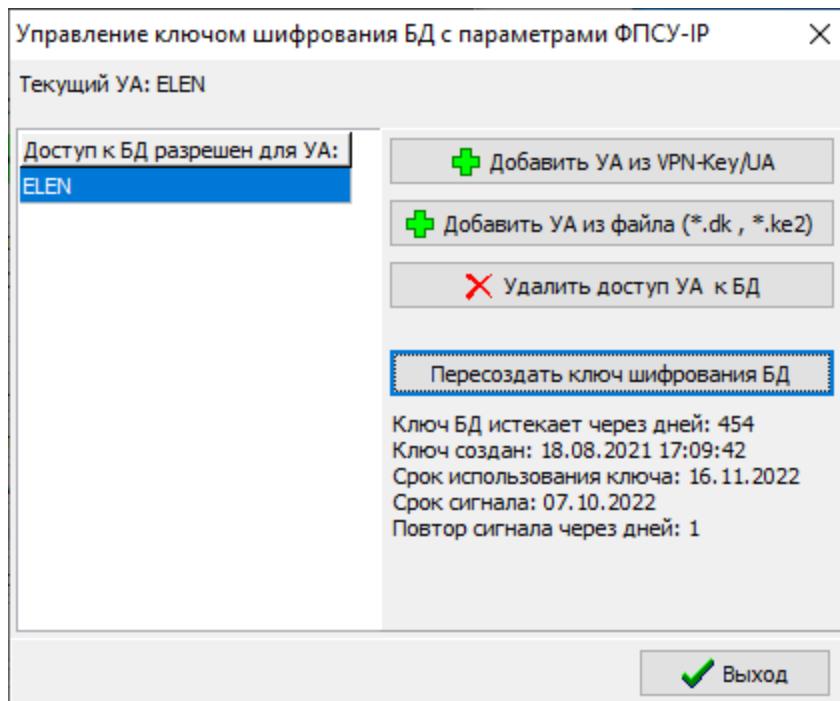


Рисунок 347 - Окно управления ключом шифрования БД

После пересоздании ключа шифрования БД УА потребуется повторно зарегистрировать всех остальных администраторов в БД параметров ФПСУ-IP. Регистрация администраторов осуществляется командами «Добавить УА из VPN-Key/UA», «Добавить УА из файла» (см. пункт «Управление доступом к базе данных УА ФПСУ-IP»).

3. На экран будет выдано окно для подтверждения пересоздания ключа шифрования БД УА, в котором следует нажать кнопку «Да».

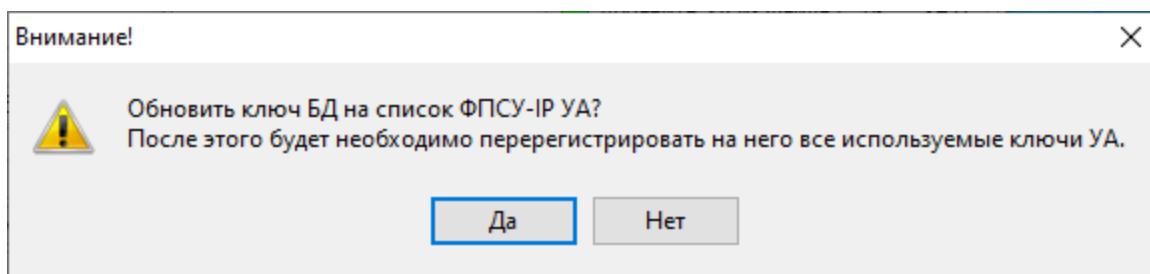


Рисунок 348 - Пересоздание ключа шифрования БД

4. На экран будет выдано окно установки срока использования ключа.

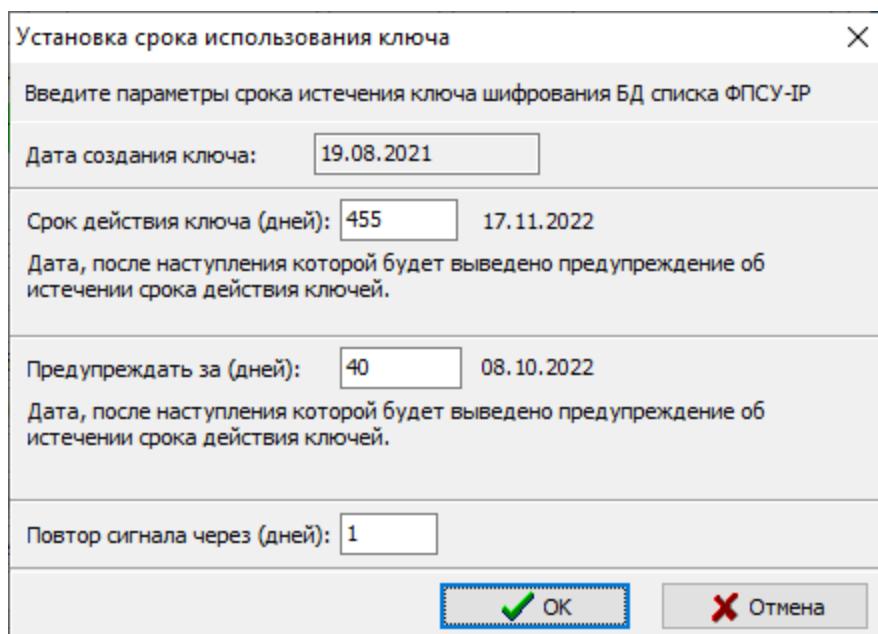


Рисунок 349 - Установка срока использования ключа

В открывшемся окне может быть изменен:

- срок действия ключа (по умолчанию 455 дней - 15 месяцев);
- срок, начиная с которого будет выдаваться предупреждения о необходимости смены ключа;
- периодичность оповещения.

По нажатию кнопки «OK» отобразится сообщение о пересоздании ключа шифрования БД УА.

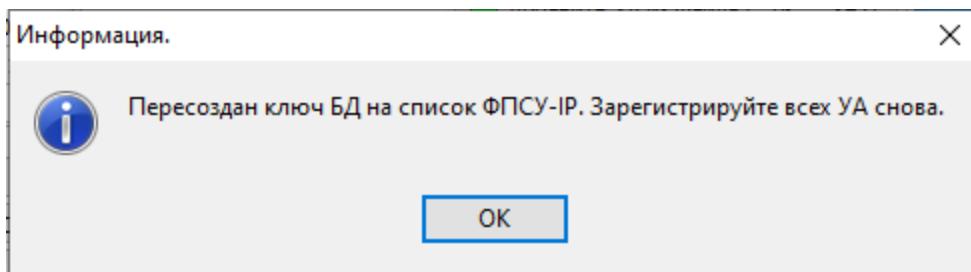


Рисунок 350 - Ключ шифрования БД пересован

В окне управления ключом шифрования БД УА ФПСУ-IP информация о ключе шифрования БД будет обновлена, а в списке администраторов, имеющих доступ к БД УА ФПСУ-IP, будет зарегистрирован только один администратор, производивший смену ключа шифрования БД. Остальных администраторов, которым ранее был разрешен доступ к БД параметров ФПСУ-IP, требуется повторно зарегистрировать (см. пункт «Управление доступом к базе данных УА ФПСУ-IP»).

20. 3. Процедура смены ключа доступа ко внешней БД

Для обновления или смены ключа доступа ко внешней БД на панели инструментов следует выбрать команду «Внешняя БД», . Откроется окно настройки внешней БД.

Администратор внешней БД, производящий смену ключа доступа ко внешней БД, должен обладать правом изменять права доступа к БД администраторов внешней БД (см. раздел «Работа со внешними базами данных»).

На вкладке «Доступ к БД» следует нажать кнопку «Создать новый ключ доступа к БД».

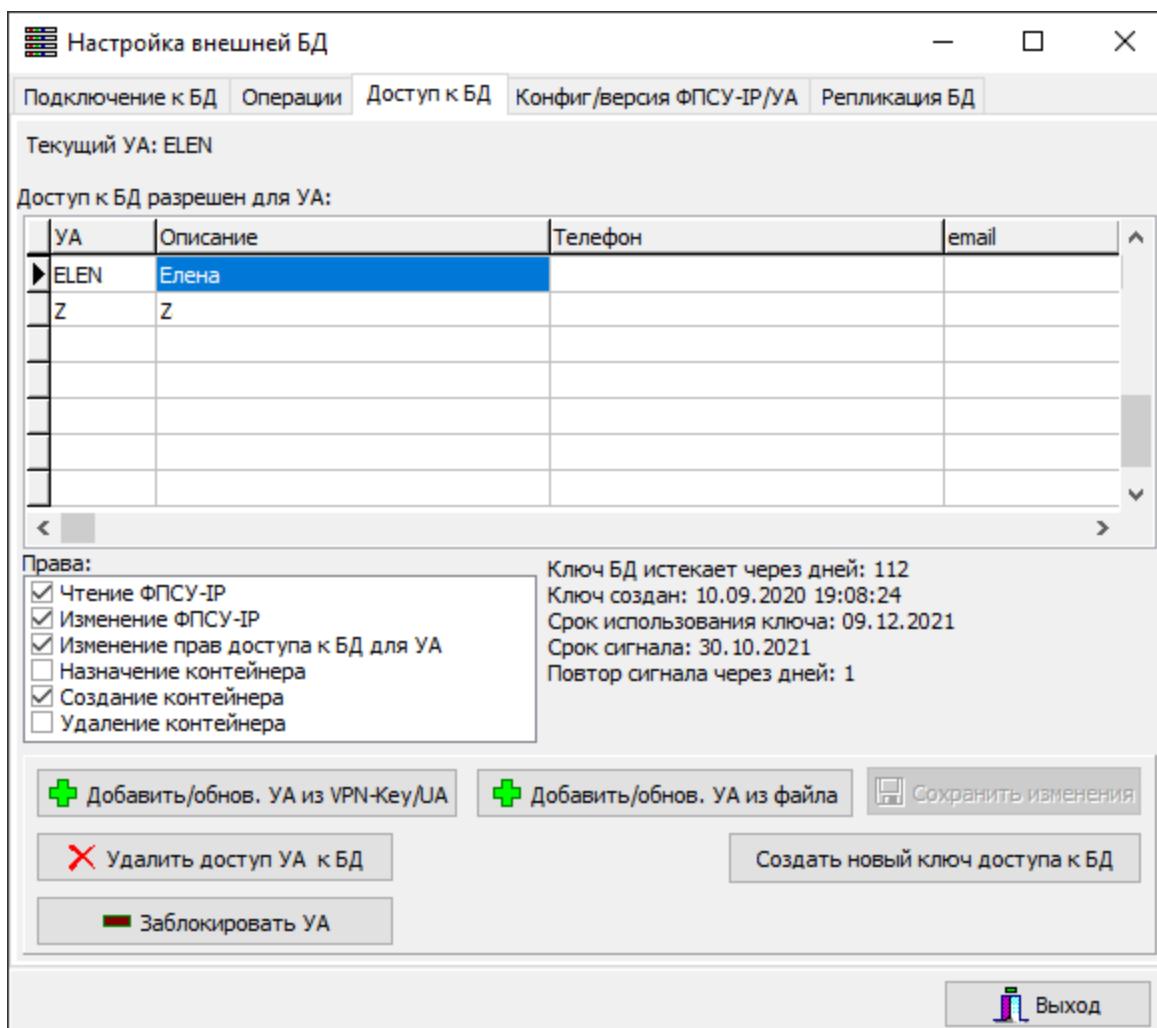


Рисунок 351 - Вкладка «Доступ к БД»

При обновлении ключа доступа ко внешней БД требуется повторно зарегистрировать всех остальных администраторов внешней БД, которым разрешен доступ к БД. При начале процедуры создания нового ключа на экран будет выдано сообщение:

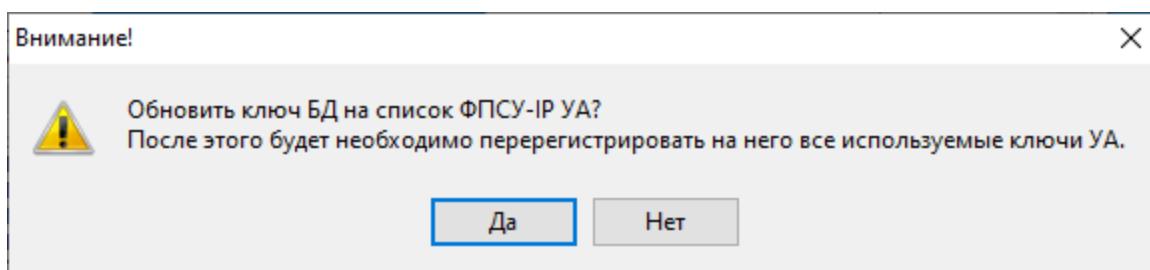


Рисунок 352 - Обновление ключа доступа к БД

Для подтверждения обновления ключа доступа ко внешней БД следует нажать кнопку «Да».

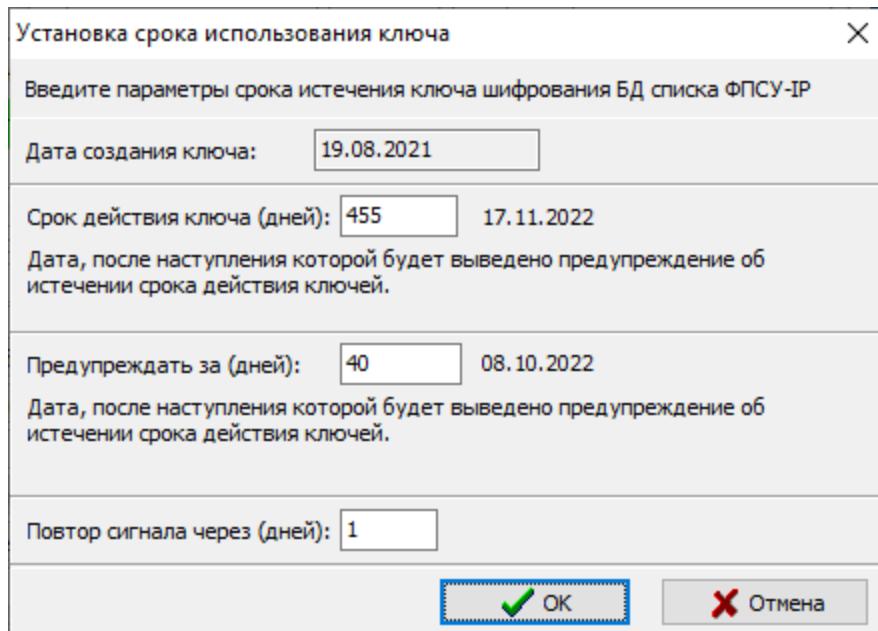


Рисунок 353 - Установка срока использования ключа

В открывшемся окне установки срока использования ключа может быть изменен:

- срок действия ключа (по умолчанию 455 дней - 15 месяцев);
- срок, начиная с которого будет выдаваться предупреждения о необходимости смены ключа;
- периодичность оповещения.

По нажатию кнопки «OK» отобразится сообщение о пересоздании ключа БД.

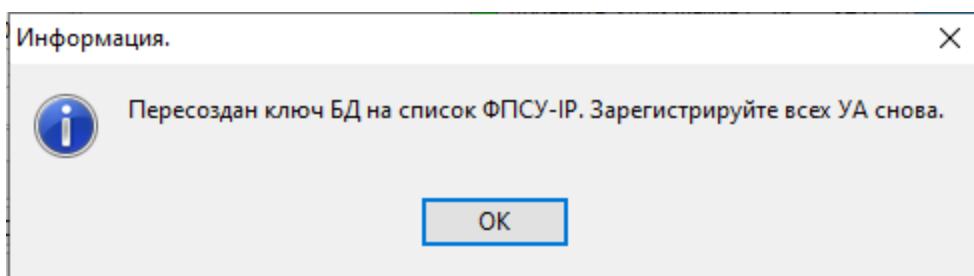


Рисунок 354 - Ключ доступа к БД обновлен

В информационном окне требуется нажать кнопку «OK».

На вкладке «Доступ к БД» обновится информация о ключе доступа ко внешней БД. Администратор внешней БД, производивший смену ключа доступа ко внешней БД, в списке администраторов будет отображаться белой строкой. Строки остальных администраторов внешней БД в списке будут отображаться желтым цветом. Всех администраторов УА в списке необходимо перерегистрировать (кроме текущего, который выполнил смену ключа доступа ко внешней БД).

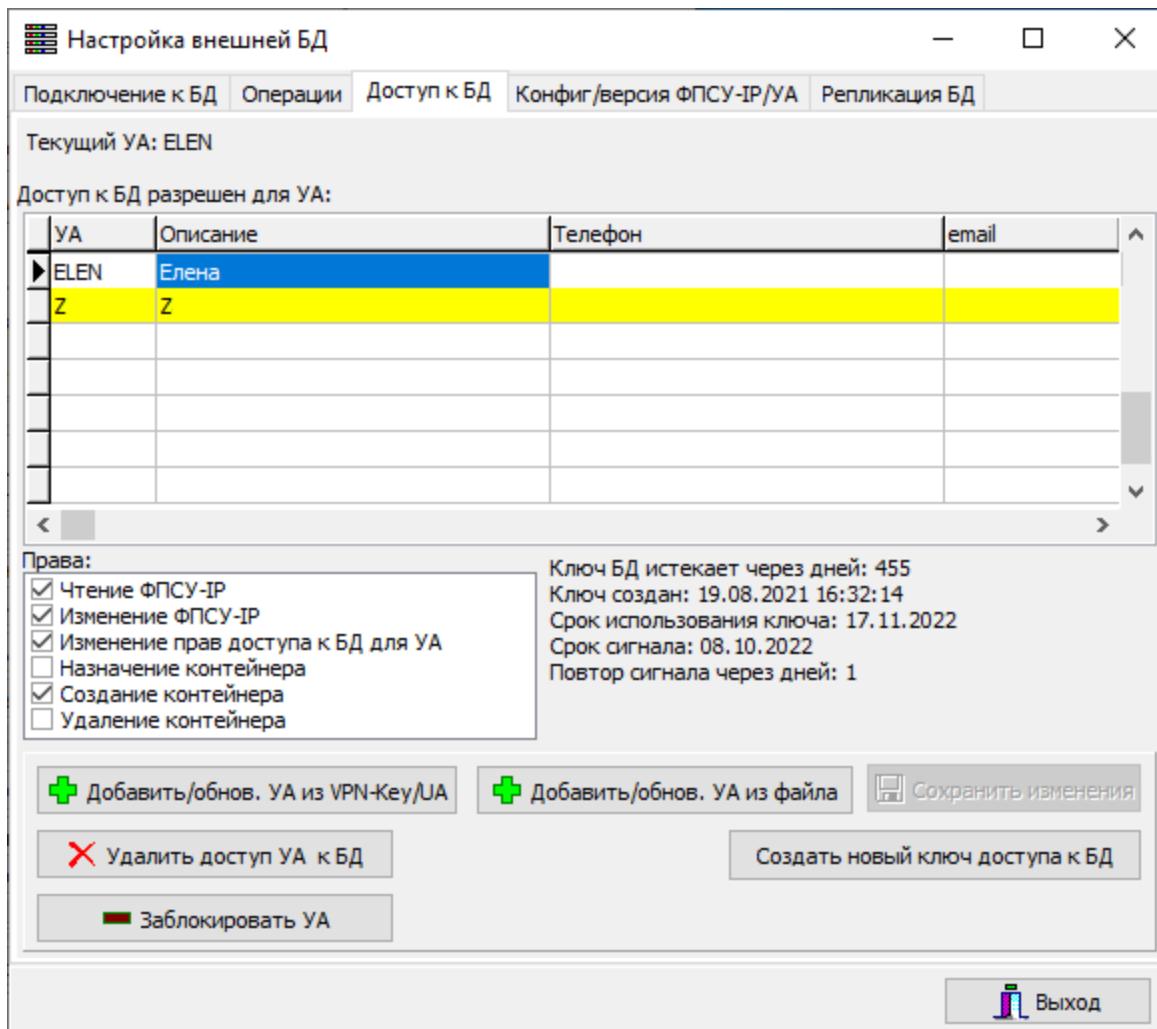


Рисунок 355 - Вкладка «Доступ к БД»

Перерегистрация администраторов внешней БД осуществляется командами «Добавить/обнов. УА из VPN-Key/UA», «Добавить/обнов. УА из файла» (см. раздел «Работа со внешними базами данных»).

21. Способы разрешения возможных проблем при работе УА ФПСУ-IP

Список возможных проблем при работе с УА ФПСУ-IP представлен в таблице ниже:

Сообщения от УА ФПСУ-IP	Возможные причины неполадок	Методы определения и/или устранения
Не найдена ни одна учетная лицензия УА ФПСУ-IP. Попробуйте ее найти через окно управления.	Отсутствие файла лицензии в каталоге «LIC».	Следует зайти в каталог «LIC» (например, через окно управления) и добавить нужную лицензию.
Текущая учетная лицензия не определена.	Файл лицензии создан с ошибкой.	Ошибка разбора файлов с лицензией.
Учетная лицензия закончилась. Для продолжения использования УА, рекомендуется ее обновить.	Срок лицензии истек.	Срок действия лицензии истек, следует её обновить.
Учетная лицензия XXX заканчивается через Y дней. Для продолжения использования УА, рекомендуется ее обновить.	Дату окончания поддержки истекает через 30 дней.	Срок лицензии истекает, следует её обновить.
Лицензия XXX на управление ФПСУ-IP закончилась. Для управления достаточным количеством ФПСУ-IP, рекомендуется ее обновить.	Срок лицензии на управление определенным количеством ФПСУ истек.	Срок лицензии на управление определенным количеством ФПСУ истек. Следует обновить лицензию.
Инициализирующая последовательность ПДСЧ не прошла проверку. Хотите ее	Инициализирующая последовательность ПДСЧ не прошла проверку	Следует переинициализировать последовательность ДСЧ.

пересоздать?		
Ошибка создания ключа шифрования БД.	Файл лицензии создан с ошибкой.	Следует заново создать ключ шифрования БД.
<p>Истек срок действия ключа УА X дней назад.</p> <p>Настоятельно рекомендуется обновить ключ и перерегистрировать его на всех ФПСУ-IP.</p> <p>При создании нового ключа УА будут заново созданы:</p> <ul style="list-style-type: none"> - ключ доступа к БД (необходимо заново получить доступ к БД (локальной или внешней)); - ключ ПДСЧ (необходимо будет заново инициализировать датчик случайных чисел) 	Срок действия ключа УА истек.	Рекомендуется создать новый ключ УА.
<p>Срок действия ключа шифрования БД списка ФПСУ-IP истек дней назад: X</p> <p>Настоятельно рекомендуется обновить ключ.</p> <p>Не забудьте перерегистрировать на него все используемые ключи УА.</p> <p>Меню: \"Ключ УА\"->"Доступ УА к ключу шифрования БД\"->"Пересоздать ключ шифрования БД\"Локальная</p>	Срок действия ключа шифрования БД списка ФПСУ-IP истек.	Требуется обновить ключ шифрования БД УА и перерегистрировать на него все используемые ключи УА.

БД")		
<p>Срок действия ключа БД на список ФПСУ-IP УА истекает через дней: nnn</p> <p>Настоятельно рекомендуется до окончания срока обновить ключ.</p>	<p>Срок действия ключа БД на список ФПСУ-IP УА истекает.</p>	<p>Требуется обновить ключ шифрования БД УА до окончания срока его действия и перерегистрировать на него все используемые ключи УА.</p> <p>При этом будет необходимо зарегистрировать на новый ключ шифрования все используемые ключи УА.</p> <p>Повторное предупреждение будет через XXX дней.</p>
<ul style="list-style-type: none"> • При загрузке ключа УА возникла проблема: • При проверке VPN-Key/UA возникла проблема: <p>УА XXX не имеет права доступа к ключу шифрования БД</p>	<p>УА XXX не имеет права доступа к ключу шифрования БД.</p>	<p>Следует предоставить УА XXX права доступа к ключу шифрования БД.</p>
Ошибка загрузки параметров зарегистрированных ФПСУ-IP.	Вероятно, используются несовместимые версии программы или БД.	Если БД разрушена, то рекомендуется восстановить файл wradm.db из резервной копии.
<p>Обнаружены дублированные IP</p> <p>ФПСУ-IP с дублированным IP</p>	Обнаружены ФПСУ-IP с дублированным IP-адресом.	

Превышено ограничение на количество активных соединений с ФПСУ-IP. Сейчас разрешено: NNN Из них имеется лицензия на XXX соединений	Лицензия имеется на меньшее количество ФПСУ-IP, чем разрешено.	
Для нового логина в VPN-Key/UA нужен пароль от 6 до 16 символов	При попытке обновления пароля было введено менее 6 или более 16 символов.	Следует ввести нужное количество символов для нового пароля.
Устройство VPN-Key/UA не обнаружено. Хотите загрузить ключ УА из файла или создать новый?	При подключенном VPN-Key/UA может означать отсутствие в каталоге «LIC» соответствующего VPN-Key/UA файла лицензии на его использование.	Следует загрузить ключ УА из файла или создать новый ключ.
Файл XXX с ключом УА не загружен.	Настройка на файл с ключом УА сброшена.	
Проверка структуры УА не пройдена.	Содержимое ключа некорректно.	Необходимо скопировать файл с ключом УА из резервной копии и повторить проверку или создать нового УА.
Информация в файле с ключом испорчена.	Содержимое файла некорректно.	
Не открылся файл БД; Ошибка чтения файла БД; Не открылась БД 'IPGADMB'.	У пользователя недостаточно прав доступа к каталогу Администратора ФПСУ-IP.	Предоставить пользователю необходимые права.

Кроме того к возможным проблемам относится компроментация ключей для связи с ФПСУ-IP и для доступа к БД администратора.

При компроментации ключей для связи с ФПСУ-IP необходимо произвести следующие действия:

Компрометация ключа для связи с ФПСУ-IP (секретного ключа УА ФПСУ-IP) возможна при хранении на отчуждаемых носителях. В этом случае необходимо немедленно выполнить следующий порядок действий:

1. Прекратить использование на УА ФПСУ-IP скомпрометированных ключей (сформировать новый ключ, см. пункты «Пересоздание ключевых данных администратора УА ФПСУ-IP» и «Первоначальная настройка УА ФПСУ-IP (с VPN-Key/UA)»);
2. Выполнить на всех ФПСУ-IP, использовавших канал связи, защищенный скомпрометированным ключом действия согласно правилам пользования на ФПСУ-IP;
3. Передать сформированный открытый ключ на ФПСУ-IP (см. пункты «Пересоздание ключевых данных администратора УА ФПСУ-IP» и «Первоначальная настройка УА ФПСУ-IP (с VPN-Key/UA)»).

При компроментации ключей доступа к базе данных администратора необходимо произвести следующие действия:

Компрометация ключа возможна при хранении на отчуждаемых носителях. В этом случае необходимо немедленно выполнить следующий порядок действий:

1. Считать скомпрометированными открытые ключи ФПСУ-IP, доступ к которым на УА ФПСУ-IP осуществляется с использованием скомпрометированных ключей доступа;
2. Прекратить использование на УА ФПСУ-IP скомпрометированных открытых ключей ФПСУ-IP (удалить открытые ключи ФПСУ-IP из базы данных, см. пункт «Удаление описателей ФПСУ-IP из списка»);
3. Выполнить на всех ФПСУ-IP, использовавших канал связи, защищенный с использованием скомпрометированных открытых ключей, действия согласно правилам пользования на ФПСУ-IP;
4. Зарегистрировать нового администратора на УА ФПСУ-IP и создать новую базу данных, сформировать новые ключи для связи с ФПСУ-IP и передать открытый ключ на ФПСУ-IP.

В процессе работы УА ФПСУ-IP изменение ряда параметров самого УА ФПСУ-IP или учетной записи администратора УА ФПСУ-IP требует специальных действий или решений.

