



ViPNet Administrator Центр управления сетью

Руководство администратора

ФРКЕ.00006-05 32 01



Версия 3.2

© 1991 – 2012 ОАО «ИнфоТекС», Москва, Россия.

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТекС».

ViPNet является зарегистрированной торговой маркой программного обеспечения, разрабатываемого ОАО «ИнфоТекС».

Все торговые марки и названия программ являются собственностью их владельцев.

ОАО «ИнфоТекС»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

E-mail: hotline@infotecs.ru

WWW: <http://www.infotecs.ru>

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	8
1 ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ПРОГРАММЫ ЦУС	11
1.1 Объединение Центров управления сетью разных сетей в иерархическую систему..	11
2 НОВЫЕ ВОЗМОЖНОСТИ	12
2.1 Версия 3.2.9	12
2.2 Версия 3.2.5	12
2.3 Версия 3.2.4	13
2.4 Версия 3.2.3	13
3 ОПИСАНИЕ ОСНОВНЫХ ПОНЯТИЙ	14
3.1 Топология сети	14
3.1.1 <i>Основные понятия сетевого уровня.....</i>	<i>14</i>
3.1.1.1 Сетевой Узел.....	14
3.1.1.2 Сетевая Группа.....	15
3.1.1.3 Сетевые Объекты	15
3.1.2 <i>Основные понятия прикладного уровня.....</i>	<i>15</i>
3.1.2.1 Прикладная задача.....	15
3.1.2.2 Пользователь (Абонент).....	15
3.1.2.3 Коллектив, тип коллектива и связь коллективов	16
3.1.2.4 Тип Коллектива	16
3.1.2.5 Связь Коллективов	16
3.1.2.6 Главный Коллектив.....	17
3.1.2.7 Открытые и Скрытые Коллективы	17
3.1.3 <i>Разграничение доступа к конфиденциальной информации</i>	<i>17</i>
3.2 Справочники для СУ.....	18
3.3 Организация межсетевого взаимодействия.....	19
4 УСТАНОВКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЦУС. СИСТЕМНЫЕ ТРЕБОВАНИЯ	19
5 ПОРЯДОК РАЗВЕРТЫВАНИЯ СЕТИ VIPNET.....	20
6 ОРГАНИЗАЦИЯ РАБОТЫ ИЕРАРХИЧЕСКОЙ СИСТЕМЫ ЦЕНТРОВ УПРАВЛЕНИЯ	21
СЕТЬЮ	
6.1 Организация иерархической системы ЦУС при первоначальном развертывании сетей ViPNET.....	21
6.2 Перевод действующих сетей ViPNET на использование иерархической системы ЦУС	23
6.3 Работа в головном ЦУС.....	24
6.3.1 <i>Распределение лицензий для сетей.....</i>	<i>24</i>
6.3.2 <i>Отправка (передача) файлов лицензий в подчиненные сети</i>	<i>24</i>
6.3.3 <i>Получение и просмотр отчетов из подчиненных сетей</i>	<i>25</i>

6.3.4	Обновление лицензии	25
7	ЗАПУСК ПРОГРАММЫ И ЗАВЕРШЕНИЕ РАБОТЫ С НЕЙ	25
8	ТИПОВОЙ ПОРЯДОК ПЕРВИЧНОЙ КОНФИГУРАЦИИ СЕТИ VIPNET	27
8.1	ГЕНЕРАЦИЯ СЕТЕВОЙ СТРУКТУРЫ.....	27
8.2	ГЕНЕРАЦИЯ ПРИКЛАДНОЙ СТРУКТУРЫ.....	30
8.3	ФОРМИРОВАНИЕ ЭКСПОРТА И ПОЛУЧЕНИЕ ИМПОРТА ДЛЯ ПЕРВОНАЧАЛЬНОГО ОБЕСПЕЧЕНИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ С ДРУГИМИ СЕТЯМИ VIPNET	34
8.4	КОНТРОЛЬ ПРАВИЛЬНОСТИ КОНФИГУРАЦИИ СИСТЕМЫ	36
8.5	ФОРМИРОВАНИЕ АДРЕСНЫХ СПРАВОЧНИКОВ, МАРШРУТНЫХ ТАБЛИЦ, СПРАВОЧНИКОВ ДЛЯ УКЦ 36	
8.6	РЕКОМЕНДАЦИИ ПО СОЗДАНИЮ АРХИВНЫХ КОПИЙ.....	36
9	ТИПОВОЙ ПОРЯДОК ДЕЙСТВИЙ ПРИ ПЕРЕКОНФИГУРАЦИИ СЕТИ VIPNET.....	37
10	РАЗБИЕНИЕ СЕТИ VIPNET НА САМОСТОЯТЕЛЬНЫЕ ПОДСЕТИ.....	38
11	ПОДСИСТЕМА АДРЕСНОЙ АДМИНИСТРАЦИИ СЕТИ.....	38
11.1	АДМИНИСТРАЦИЯ СЕТЕВОГО УРОВНЯ	38
11.1.1	Функциональное назначение	38
11.1.2	Диалоговая среда подсистемы адресной администрации.....	39
11.1.3	Окно Серверы-маршрутизаторы сети	40
11.1.4	Окно АП из области СМ	41
11.1.5	Окно межсерверных каналов, образованных данным СМ.....	43
11.1.6	Окно всех межсерверных каналов	43
11.1.7	Окно групп сетевых узлов, окно подгрупп группы СУ.....	44
11.1.8	Формирование таблиц маршрутизации	46
11.1.9	Вывод БД в текстовый файл	46
11.1.10	Окно Межсетевые каналы.....	46
11.1.11	Выход из подсистемы	47
11.2	АВТОМАТИЧЕСКАЯ ГЕНЕРАЦИЯ АДРЕСНОЙ СТРУКТУРЫ.....	47
11.2.1	Добавление абонентских пунктов с формированием имен по заданной маске 49	
11.3	ЗАДАНИЕ АДРЕСОВ СЕТЕВЫХ УЗЛОВ СЕТИ VIPNET ПРИ РАБОТЕ ЧЕРЕЗ ВНЕШНИЕ СЕТИ.....	50
11.4	ГРУППОВЫЕ ОПЕРАЦИИ С УЗЛАМИ	51
11.4.1	Создание сетевых узлов	51
11.4.2	Удаление абонентских пунктов.....	52
11.4.3	Изменение свойств абонентских пунктов.....	53
11.5	ПЕРЕНОС АБОНЕНТСКИХ ПУНКТОВ НА ДРУГОЙ СЕРВЕР-МАРШРУТИЗАТОР.....	54
11.6	ВОССТАНОВЛЕНИЕ БАЗЫ ДАННЫХ СЕТЕВЫХ УЗЛОВ	55
12	НАСТРОЙКИ ПО УМОЛЧАНИЮ	55

13	РЕГИСТРАЦИЯ АП И СМ В ПРИКЛАДНЫХ ЗАДАЧАХ	57
13.1	СПИСОК ПРИКЛАДНЫХ ЗАДАЧ ДЛЯ РЕГИСТРАЦИИ СУ	58
13.2	РЕКОМЕНДАЦИИ ПО РЕГИСТРАЦИИ СУ В РАЗЛИЧНЫХ ПРИКЛАДНЫХ ЗАДАЧАХ В ЗАВИСИМОСТИ ОТ ФУНКЦИОНАЛЬНОСТИ, КОТОРУЮ ДОЛЖНО ОБЕСПЕЧИВАТЬ ПО ViPNET НА ЭТИХ УЗЛАХ	68
13.3	ИНДИВИДУАЛЬНАЯ РЕГИСТРАЦИЯ АП В ЗАДАЧАХ	71
13.4	ГРУППОВАЯ РЕГИСТРАЦИЯ СУ (АП И СМ) В ПЗ.....	73
13.4.1	<i>Регистрация узлов в задаче “Защита трафика”</i>	<i>74</i>
13.4.2	<i>Регистрация СМ в задаче “Сервер IP-адресов”</i>	<i>75</i>
13.4.2.1	Задание IP-адресов	76
13.4.2.2	Включение функции Сервер открытого Интернета	76
13.4.2.3	Задание максимального числа адресов для туннелирования	76
13.4.2.4	Назначение резервного сервера IP-адресов для АП-терминала.....	76
13.4.2.5	Удаление резервного сервера для АП-терминала.....	78
13.4.3	<i>Регистрация СМ в задаче “ViPNet Cluster”.....</i>	<i>78</i>
13.4.4	<i>Регистрация АП в задаче “Деловая почта”.....</i>	<i>78</i>
13.4.5	<i>Регистрация в задаче “Центр регистрации”.....</i>	<i>79</i>
13.4.6	<i>Регистрация АП в задаче “Центр управления политиками”</i>	<i>80</i>
13.4.7	<i>Регистрация АП в задаче “Сервер мониторинга”</i>	<i>81</i>
13.4.8	<i>Регистрация АП в задачах “Терминал Спектр” и “Терминал Ареал-Сервис” ..</i>	<i>82</i>
13.4.9	<i>Регистрация АП в прикладной задаче « ViPNet Terminal»</i>	<i>84</i>
13.4.10	<i>Регистрация во всех остальных задачах</i>	<i>86</i>
13.5	ПОРЯДОК НАСТРОЙКИ РАЗЛИЧНЫХ ПАРАМЕТРОВ СЕТЕВЫХ УЗЛОВ.....	87
13.5.1	<i>Краткое описание формата строк, используемых для настройки</i>	<i>88</i>
13.6	РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ ПАРАМЕТРОВ СЕТЕВЫХ УЗЛОВ В ЗАВИСИМОСТИ ОТ ТРЕБУЕМОЙ КОНФИГУРАЦИИ.....	92
13.7	НАСТРОЙКА КООРДИНАТОРОВ.....	93
13.7.1	<i>Автоматическая настройка параметров подключения координатора к внешней сети 93</i>	
13.7.1.1	Настройка параметров подключения координатора без использования межсетевого экрана 93	
13.7.1.2	Настройка параметров подключения координатора через МЭ ViPNet-Координатор ... 93	
13.7.1.3	Настройка параметров соединения координатора через МЭ со статической трансляцией 94	
13.7.1.4	Настройка параметров соединения координатора через МЭ с динамической трансляцией 95	
13.7.2	<i>Настройка адресов доступа к координатору</i>	<i>96</i>
13.7.3	<i>Частичная настройка координатора</i>	<i>96</i>
13.7.4	<i>Настройка туннелируемых адресов на координаторе</i>	<i>97</i>
13.7.5	<i>Настройка параметров межсетевого экрана для всех абонентских пунктов координатора 97</i>	
13.7.6	<i>Настройка параметров доступа к терминальному серверу.....</i>	<i>98</i>

13.8	НАСТРОЙКА АБОНЕНТСКИХ ПУНКТОВ (АП)	99
14	РЕГИСТРАЦИЯ ТИПОВ КОЛЛЕКТИВОВ И ПОЛЬЗОВАТЕЛЕЙ.....	100
14.1	ФОРМИРОВАНИЕ ПРИКЛАДНОЙ СТРУКТУРЫ СЕТИ	100
14.2	РЕГИСТРАЦИЯ ТИПОВ КОЛЛЕКТИВОВ.....	100
14.2.1	<i>Регистрация нового типа коллектива</i>	101
14.2.2	<i>Удаление типа коллектива</i>	101
14.2.3	<i>Изменение имени и/или области действия типа коллектива</i>	101
14.2.4	<i>Изменение связей типа коллектива</i>	102
14.2.5	<i>Поиск по подстроке</i>	102
14.3	РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ	102
14.3.1	<i>Регистрация нового пользователя</i>	103
14.3.2	<i>Удаление пользователя</i>	103
14.3.3	<i>Изменение имени пользователя</i>	103
14.3.3.1	Назначение псевдонимов. Обеспечение сопряжения криптофункций с другими системами установления идентификаторов	103
14.3.4	<i>Изменение списка коллективов пользователя</i>	104
14.3.5	<i>Изменение атрибутов коллективов пользователей</i>	105
14.3.6	<i>Предоставление пользователю права электронной подписи</i>	105
14.3.7	<i>Поиск по подстроке</i>	105
14.4	СПИСКИ РАССЫЛКИ КОПИЙ ПИСЕМ.....	105
14.5	СПИСОК РАССЫЛКИ СОС	107
15	ОРГАНИЗАЦИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ	108
15.1	ЭКСПОРТ. ПРОСМОТР ВРЕМЕНИ ПОЛУЧЕНИЯ И ОБРАБОТКИ ЭКСПОРТА В ДОВЕРЕННЫХ СЕТЯХ VIPNET 110	
15.2	ИМПОРТ. ИНФОРМАЦИЯ О СТАТУСЕ И ВРЕМЕНИ ПРИНЯТОГО ИМПОРТА.....	114
15.3	НЕОБРАБОТАННЫЙ ИМПОРТ.....	115
16	ОБРАБОТКА ЗАПРОСОВ, ПОСТУПАЮЩИХ ИЗ ЦЕНТРА РЕГИСТРАЦИИ	116
17	РАСПРЕДЕЛЕНИЕ ЛИЦЕНЗИЙ ДЛЯ СЕТЕЙ	118
18	КОНТРОЛЬ ПРАВИЛЬНОСТИ КОНФИГУРАЦИИ СИСТЕМЫ	123
18.1	ПРОСМОТР КОНФИГУРАЦИИ СЕТИ	123
18.1.1	<i>Структура сети</i>	124
18.2	ПРОВЕРКА КОНФИГУРАЦИИ СЕТИ	125
19	ФОРМИРОВАНИЕ АДРЕСНЫХ СПРАВОЧНИКОВ, МАРШРУТНЫХ ТАБЛИЦ, СПРАВОЧНИКОВ ДЛЯ УКЦ.....	126
19.1	ФОРМИРОВАНИЕ ВСЕХ СПРАВОЧНИКОВ (ПУНКТ МЕНЮ "СФОРМИРОВАТЬ ВСЕ СПРАВОЧНИКИ") 126	
19.2	ПРОСМОТР И КОПИРОВАНИЕ СПРАВОЧНИКОВ АП (ПУНКТ МЕНЮ "СПРАВОЧНИКИ АП").....	126
19.3	КОПИРОВАНИЕ СПРАВОЧНИКОВ СМ (ПУНКТ МЕНЮ "СПРАВОЧНИКИ СМ")	129

19.4	ФОРМИРОВАНИЕ ФАЙЛОВ ДЛЯ СОЗДАНИЯ КЛЮЧЕЙ В УКЦ	130
19.4.1	Файлы для создания ключей сетевых узлов	130
19.4.2	Файлы для создания ключей пользователей	130
19.4.3	Файлы для создания дистрибутивов ключей	130
19.4.4	Компрометация ключей	131
19.4.5	Файлы для создания ключей узлов, связанных с другими сетями	131
20	РАБОТА С АРХИВАМИ КОНФИГУРАЦИЙ СЕТИ	131
21	УПРАВЛЕНИЕ СЕТЬЮ	132
21.1	ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ	132
21.2	ОТПРАВКА ИЗМЕНЕННЫХ ФАЙЛОВ (ПУНКТ МЕНЮ "ОТПРАВИТЬ ИЗМЕНЕННЫЕ ФАЙЛЫ")	132
21.2.1	Отправка справочников и маршрутных таблиц	134
21.2.2	Отправка ключевой информации	135
21.2.3	Отправка дистрибутивов ключей	136
21.2.4	Отправка Экспорта в другие ЦУС	136
21.3	УДАЛЕННОЕ ОБНОВЛЕНИЕ ПО ViPNET (ПУНКТ МЕНЮ "ОБНОВИТЬ ПО")	137
21.3.1	Варианты обновления и рекомендации по его проведению	138
21.3.1.1	Обновление ПО ViPNet на узлах с ОС Windows	138
21.3.1.2	Обновление ПО ViPNet на узлах с ОС Linux и мобильных устройствах	138
21.3.2	Обновление файла лицензии	139
21.4	ИЗМЕНЕНИЕ ПРИОРИТЕТА ОБРАБОТКИ УПРАВЛЯЮЩИХ КОНВЕРТОВ	139
21.5	НАСТРОЙКА ПУТЕЙ (ПУНКТ МЕНЮ "ПУТИ")	140
21.6	БАЗА ДАННЫХ ЗАПРОСОВ (ПУНКТ МЕНЮ "ЗАПРОСЫ И ОТВЕТЫ")	140
21.6.1	Просмотр ответа на запрос	142
21.6.2	Повторение запроса	142
21.6.3	Удаление запроса	142
21.6.4	Отправка подтверждений и откатов на запросы	143
21.6.5	Фильтрация и сортировка записей в базе запросов и ответов	143
21.6.6	Просмотр содержимого отправленного запроса	144
22	ДОПОЛНИТЕЛЬНЫЕ СЕРВИСНЫЕ ВОЗМОЖНОСТИ	144
22.1	ПРОСМОТР ИНФОРМАЦИИ О ЛИЦЕНЗИИ	144
22.2	КОНТЕКСТНО-ЧУВСТВИТЕЛЬНАЯ СПРАВКА	145
22.3	ПРОСМОТР ФАЙЛА	145
22.4	УДАЛЕНИЕ, КОПИРОВАНИЕ И ПЕРЕИМЕНОВАНИЕ ФАЙЛОВ	145
22.5	ВРЕМЕННЫЙ ВЫХОД В ОПЕРАЦИОННУЮ СИСТЕМУ	145
22.6	СМЕНА ВИДЕОРЕЖИМА	145

Введение

Пакет программ ViPNet Custom предоставляет возможность создания полностью защищенной от внешнего влияния и постороннего доступа информационной сети, которая через любые каналы связи, поддерживающие IP-протокол (телефонные с использованием служб удаленного доступа, выделенные, Интернет, локальные сети и др.) позволяет объединить все отделения, филиалы, отделы и конкретных лиц Вашей организации, Ваших партнеров в единую частную защищенную сеть.

Сеть не требует специального оборудования, рассчитана на обычные IBM-совместимые компьютеры, любые локальные IP-сети, любые способы подключения к сети: Ethernet, PPPoE через XDSL-подключение, PPP через подключение Dial-up или ISDN, устройства Wi-Fi, сеть сотовой связи GPRS или 3G.

Пакет программ ViPNet Custom предназначен для подготовки, передачи, хранения и обработки конфиденциальной информации, а в применении к IP-сетям является универсальным программным средством для создания виртуальных частных сетей (**Virtual Private Network - VPN**) любых конфигураций.

В пакете реализован комплекс программно-технических и организационных решений по защите информации и самой системы от несанкционированного доступа.

В пакет программ частной сети ViPNet могут входить следующие программные продукты:

ViPNet Administrator (обязательная административная программа), включающая

- * Центр Управления сетью
- * Удостоверяющий и Ключевой центр;

ViPNet Coordinator (устанавливается на координатор);

ViPNet Client (устанавливается на АП);

ViPNet CryptoService;

ViPNet Пункт регистрации;

другие прикладные программы.

Сеть ViPNet - это совокупность сетевых узлов (абонентских пунктов и координаторов).

Конфигурирование и управление сетью ViPNet происходит в программе ViPNet Administrator Центр управления сетью (далее ЦУС), которую описывает этот документ. Подробнее об основных функциях читайте в разделе 1.

При регистрации в ЦУС координатор наделяется функциями сервера-маршрутизатора (СМ). СМ обеспечивает маршрутизацию почтовых конвертов и управляющих сообщений при взаимодействии ЦУС, Ключевого центра и объектов сети между собой.

При построении VPN ViPNet координатор может быть зарегистрирован в дополнительных прикладных задачах и выполнять функции сервера со следующими возможностями:

Сервер IP-адресов, обеспечивающий:

- * регистрацию и предоставление информации о текущих IP-адресах и состоянии объектов корпоративной сети.

Сервер ViPNet Firewall, обеспечивающий:

- * Работу защищенных компьютеров локальной сети в VPN от имени одного адреса.
- * Туннелирование пакетов от заданных незащищенных компьютеров локальной сети.
- * Фильтрацию открытых пакетов в соответствии с заданной политикой безопасности.

- * Возможность работы защищенных компьютеров локальной сети через Firewall.

ViPNet-сервер открытого Интернета, обеспечивающий:

- * Возможность организации подключения части компьютеров локальной сети к Интернет **без их физического отключения от локальной сети организации.**

Программное обеспечение для реализации этих функций носит название ViPNet Coordinator. Функцию СМ выполняет программа ViPNet Coordinator MFTP, входящая в ViPNet Coordinator. Все остальные функции выполняет программа ViPNet Coordinator Монитор. Координатор может быть зарегистрирован и в других прикладных задачах.

Каждый абонентский пункт (АП) регистрируется в ЦУС на одном координаторе (Сервере-маршрутизаторе), который обеспечивает маршрутизацию почтовых пакетов сообщений от пользователя-отправителя к пользователю-получателю в соответствии с заданным сетевым адресом получателя и с учетом приоритетности сообщений. АП при передаче почтовых сообщений могут взаимодействовать и напрямую без СМ.

При построении VPN ViPNet АП должен быть зарегистрирован в конкретных прикладных задачах для возможности установки на нем соответствующего клиентского ПО (например, ViPNet Client, ViPNet CryptoService).

Для обеспечения взаимодействия между СУ необходимо задать связи.

Обо всем подробнее читайте далее. Данное руководство рекомендуется читать в следующем порядке:

1. Введение,
2. Раздел 2,
3. Раздел 4,
4. Раздел 7,
5. Раздел 8,
6. Раздел 5.

С остальными разделами можно знакомиться по мере необходимости.

Концепция защиты и разграничения доступа в сети ViPNet

В сети ViPNet используется интегрированная многоуровневая защита от несанкционированного доступа к сети и к конфиденциальной информации:

В почтовых приложениях "Виртуальной защищенной сети ViPNet" доступ к конфиденциальным документам в папках имеют только пользователи, владеющие соответствующей ключевой информацией и паролями. Каждому коллективу пользователей выделяются отдельные папки входящих и исходящих документов, защищенные от доступа пользователей, не входящих в данные коллективы. Установлением связей между коллективами достигается управление потоками информации. Имеются общие папки, доступ к которым определяется установлением соответствующих меток конфиденциальности (идентификаторов) каждому пользователю.

Доступ к другим информационным ресурсам через сетевые подключения разграничивается:

- * установленными связями между абонентскими пунктами;
- * индивидуальной парольной и ключевой информацией;
- * установлением различных критериев фильтрации как для защищенных, так и незащищенных соединений по всем значимым полям IP-пакета;
- * инкапсуляцией реальных IP-пакетов в специальные недоступные для чтения и значимой модификации пакеты, формируемые Драйвером сетевой защиты при установлении защищенных соединений;
- * внедрением в пакеты уникальных идентификаторов пользователей;

- * установлением меток времени, предотвращающих возможность повторения записанных пакетов за пределами заданного промежутка времени.

Пользователи не имеют возможность вносить изменения в адресные структуры и разрешенные им связи.

Корректировка и дистанционное обновление адресных справочников АП и СМ, маршрутных таблиц СМ, а также формирование части ключевой и парольной информации осуществляется только администраторами Виртуальной защищенной сети. Доступ к транспортным конвертам и канальным кадрам запрещен для всех категорий субъектов.

Информация в почтовых приложениях может предназначаться для пользователя, коллектива или узла, при этом:

- * Пользователь имеет доступ к информации (за исключением персональной ключевой информации), предназначенной для любого другого пользователя, зарегистрированного в тех же коллективах, что и данный пользователь; пользователь не имеет доступа к информации пользователей коллективов, в которых данный пользователь не зарегистрирован.
- * Пользователь имеет доступ к информации, предназначенной для любого коллектива, где зарегистрирован данный пользователь; пользователь не имеет доступа к информации коллективов, где пользователь не зарегистрирован,
- * Пользователь имеет доступ к информации, предназначенной для любого узла, в коллективе которого зарегистрирован данный пользователь; пользователь не имеет доступа к информации узлов, в коллективах которых данный пользователь не зарегистрирован,
- * Пользователь, желающий обеспечить защиту от доступа к своей информации со стороны других пользователей, должен быть зарегистрирован в некотором коллективе один.
- * Пользователь, коллектив или узел может получить (отправить) информацию только от (для) объектов, с которыми есть связь; связь между объектами одного уровня определяется наличием связи между соответствующими коллективами, заданной в Центре управления сетью.

Возможность доступа различных объектов к соответствующей информации определяется двумя Центрами, не имеющими возможность модифицировать полномочия в сети друг без друга, - Центром управления сетью (ЦУС) и Удостоверяющим и Ключевым центром (УКЦ) с использованием двух независимых средств:

- * Индивидуальных для каждого узла Адресных справочников доступа, модификация и формирование которых возможна только в программе ЦУС,
- * Наличием доступа каждого объекта только к той ключевой информации, сформированной Ключевым центром и недоступной для ЦУС, состав которой определен соответствующими Адресными справочниками доступа.

Информационная независимость объектов сети от Центров достигается формированием каждым объектом сети дополнительных ключей шифрования на принципах открытого распределения, не доступных Центрам. Достоверность открытой части ключа шифрования каждого объекта сети подтверждается электронной подписью пользователя, сформировавшего данный ключ.

Для каждого пользователя сети Ключевым центром или непосредственно самим пользователем в своей программе формируются закрытый и открытый ключи электронной подписи, используемые для подтверждения достоверности информации, автором которой является данный пользователь. Достоверность открытого ключа электронной подписи каждого пользователя подтверждается сертификатом (электронной подписью) администратора сети. При наличии межсетевого взаимодействия открытые ключи электронных подписей администраторов других сетей подтверждаются сертификатами администраторов данной

сети. Открытые ключи электронных подписей администраторов данной сети хранятся в ключах пользователя.

1 Основные функциональные возможности программы ЦУС

Программа Центр управления сетью (ЦУС) – это административная программа, которая входит в состав ПО ViPNet Administrator.

Программа Центр управления сетью (ЦУС) предназначена для создания инфраструктуры сети ViPNet, мониторинга и управления объектами сети.

Пользователя, отвечающего за конфигурирование и управление сетью ViPNet, будем называть администратором ЦУС (далее администратор). Для администратора ЦУС предназначено данное руководство.

Программа **Центр управления сетью** позволяет администратору выполнять следующие основные функции:

- регистрацию сетевых узлов (СУ) и пользователей сети ViPNet,
- регистрацию СУ в различных прикладных задачах ViPNet,
- задание полномочий и связей,
- задание IP-адресов и других сетевых параметров,
- формирование справочников СУ и справочников для Удостоверяющего и Ключевого центра (УКЦ),
- взаимодействие с УКЦ,
- взаимодействие с Центрами регистрации (обработка запросов из Центра регистрации);
- взаимодействие с ЦУС других сетей ViPNet для организации межсетевого обмена,
- контроль времени отправки экспорта, а также получения и обработки импорта в своей и других сетях,
- централизованную рассылку на СУ обновлений справочников и ключевой информации,
- централизованную рассылку на СУ обновления программного обеспечения ViPNet,
- управление конфигурацией СУ ViPNet.

Регистрация имен сетевых узлов и пользователей может быть произведена только с использованием букв русского или английского алфавита.

Конфигурирование сети ViPNet в ЦУС происходит в соответствии с имеющейся лицензией для данной сети (файл Infotecs.reg). В лицензии указаны различные параметры сети: название, номер сети, срок действия лицензии (при наличии ограничения на срок), ограничение на число СУ, пользователей, туннелируемых адресов и др. параметры структуры сети, которые разрешено задать в ЦУС данной сети. Также в лицензии указано ограничение на номер используемой версии ViPNet, список лицензированных прикладных задач и число СУ, которое можно зарегистрировать в каждой из задач.

Файлы лицензии (Infotecs.reg (необходим только для ЦУС) и Infotecs.re (необходим для ЦУС и остальных программ ViPNet)) включены в комплект поставки ПО ViPNet Custom или могут передаваться продавцом отдельно.

1.1 Объединение Центров управления сетью разных сетей в иерархическую систему

Центры управления сетью нескольких сетей ViPNet могут быть объединены в иерархическую систему Центров управления сетью. Это означает, что ЦУС какой-либо сети ViPNet (назовем такую сеть и ЦУС головными) может управлять Центрами управления сетью других сетей ViPNet (назовем такие сети и ЦУС подчиненными).

Необходимость в создании такой системы может потребоваться, например, в следующем случае:

Организация (как правило, с многочисленным количеством объектов, требующих сетевой защиты), имеющая основной офис и несколько удаленных филиалов, приобретает ПО ViPNet CUSTOM и планирует развернуть отдельные сети ViPNet для основного офиса и каждого филиала. Все сети ViPNet планируется связать между собой для осуществления межсетевого взаимодействия. При этом существует потребность из сети основного офиса управлять лицензиями на конфигурацию сетей ViPNet филиалов (в рамках лицензионных ограничений для всей организации) и контролировать текущую структуру сети филиалов.

Для объединения Центров управления сетью в иерархическую систему необходим специальный, общий файл лицензии. В этом файле указаны суммарные лицензионные ограничения на головную и подчиненные сети ViPNet, а также указаны номера головной и подчиненных сетей. Файл помещается в папку установки ЦУС, который планируется сделать головным.

Головной ЦУС в дополнении к основным функциям ЦУС обеспечивает следующие возможности:

Централизованное управление лицензиями своей сети и подчиненных сетей в рамках выданной общей лицензии.

Централизованный контроль количества использованных лицензий и структуры сети ViPNet в подчиненных сетях.

Подробнее об иерархической системе ЦУС читайте в разделе 6.

2 Новые возможности

2.1 Версия 3.2.9

Добавлены прикладные задачи *ViPNet Security Gateway*, *Coordinator KB 100*, *Coordinator KB 1000*, *Coordinator HW-VA* (см. п. 13.1).

Доработана функция, позволяющая создавать списки рассылки копий писем. Теперь возможность создавать списки рассылки копий по получателям писем отсутствует, списки рассылки копий можно формировать только по отправителям писем (см. п. 14.4).

В данной версии программы отсутствует возможность копирования минимального необходимого комплекта справочников для формирования сокращенного дистрибутива ключей в УКЦ. В дальнейшем эта возможность не будет поддерживаться.

2.2 Версия 3.2.5

Реализована возможность установки программного обеспечения ViPNet на мобильные устройства с операционной системой Android. В связи с этим название прикладной задачи *Клиент iOS* изменено на *VPN-клиент для мобильных устройств*. В данной задаче следует регистрировать абонентские пункты, которые будут работать на мобильных устройствах с операционными системами iOS и Android (см. п. 13.1).

Реализована возможность отправки обновлений справочников, ключей и программного обеспечения на абонентские пункты, зарегистрированные в прикладной задаче *VPN-клиент для мобильных устройств*.

Добавлена прикладная задача *Сервер мониторинга СБ РФ* (см. п. 13.1).

В окне *Управление внешними адресами* (см. п.11.3) отображаются только узлы своей сети, добавлена возможность поиска узлов.

Доработана функция переноса абонентского пункта на другой координатор (см. п. 11.5):

Если в течение заданного периода старого адреса от перенесенного абонентского пункта будут получены конверты, отправленные с нового адреса, использование старого адреса

будет прекращено. Все последующие обновления будут отправляться по новому адресу абонентского пункта.

При переносе на другой координатор сохраняются заданные IP-адреса абонентского пункта.

2.3 Версия 3.2.4

Добавлена прикладная задача **Координатор HW110** (см. п. 13.1).

Реализована возможность формирования имен абонентских пунктов по заданной маске при добавлении абонентских пунктов на существующий координатор в окне автоматической генерации подсетей (см. п. 11.2.1).

Реализована возможность группового переноса абонентских пунктов на другой координатор из основного окна программы с помощью меню **Службы > Адресная администрация** (см. п. 11.5).

Реализована возможность настройки полномочий пользователя и параметров доступа к терминальному серверу в прикладной задаче **ViPNet Terminal** (см. п. 13.4.9).

Реализована возможность группового изменения полномочий пользователей в прикладных задачах **Защита трафика, Деловая почта, КриптоСервис, Клиент iOS, ViPNet Terminal** (см. п. 13.4).

2.4 Версия 3.2.3

Добавлены прикладные задачи **Клиент iOS** и **Координатор HW100-СНВ** (см. п. 13.1).

Реализована возможность групповой регистрации сетевых узлов, редактирования и удаления абонентских пунктов (см. п. 11.4).

Произошли значительные изменения в меню программы:

В меню **Службы** переименованы следующие пункты:

- * Пункт Индивидуальная регистрация АП в ПЗ переименован в Индивидуальная регистрация АП в задачах.
- * Пункт Групповая регистрация СУ в ПЗ переименован в Групповая регистрация узлов в задачах.
- * Пункт Прикладная администрация переименован в Списки рассылки.
- * Пункт Необработанные запросы на регистрацию переименован в Обработка запросов на регистрацию.
- * Пункт Распределение лицензий переименован в Распределение лицензий для сетей.
- * Пункт Просмотр конфигурации переименован в Просмотр конфигурации сети.
- * Пункт Проверка конфигурации переименован в Проверка конфигурации сети.
- * Пункт Справочники для УКЦ переименован в Файлы для создания ключей в УКЦ.
- * Пункт Архивы баз данных переименован в Архив конфигураций сети.

Из меню **Сервис > Прикладная администрация** (в новой версии **Списки рассылки**) в меню **Сервис** перенесены следующие команды:

- * Регистрация типов коллективов.
- * Регистрация пользователей.

В меню **Службы > Справочники для УКЦ** (в новой версии **Файлы для создания ключей в УКЦ**) переименованы следующие пункты:

- * Пункт Справочники связей сетевых узлов переименован в Ключей узлов.
- * Пункт Справочники связей пользователей переименован в Ключей пользователей.
- * Пункт Справочники узлов, связанных с др. сетями переименован в Ключей узлов, связанных с другими сетями.

Из меню **Сервис > Справочники для УКЦ** (в новой версии **Файлы для создания ключей в УКЦ**) удален пункт **Дистрибутивы**, его подпункты перенесены на уровень выше и переименованы:

- * Дистрибутивов в минимальном объеме.
- * Дистрибутивов в полном объеме.

Из меню **Сервис > Просмотр конфигурации** (в новой версии **Просмотр конфигурации сети**) удален пункт **Структура сети**, его подпункты перенесены на уровень выше и переименованы:

- * Структура сети в широком формате.
- * Структура сети в узком формате.

В меню **Управление > Отправить измененные файлы** переименованы следующие пункты:

- * Пункт Справочники АП и СМ переименован в Справочники узлов.
- * Пункт Ключевые наборы для СУ переименован в Ключи узлов.
- * Пункт Индивидуальные ключи для пользователей переименован в Ключи пользователей.
- * Пункт Дистрибутивы ключей пользователей переименован в Дистрибутивы ключей.

Из меню **Управление > Обновить ПО** в меню **Управление > Отправить измененные файлы** перенесен пункт **Файл лицензии**.

3 Описание основных понятий

3.1 Топология сети

3.1.1 Основные понятия сетевого уровня

3.1.1.1 Сетевой Узел

Сетевой узел – это отдельный абонентский пункт или Сервер-маршрутизатор.

Каждый абонентский пункт (АП) для почтовых приложений подключается к одному Серверу-маршрутизатору (СМ), который обеспечивает маршрутизацию почтовых пакетов сообщений от пользователя-отправителя к пользователю-получателю.

Серверы-маршрутизаторы для обмена почтовой информацией могут соединяться между собой логическими каналами по произвольной схеме. Почтовые сообщения будут проходить от сервера к серверу по кратчайшему маршруту.

При построении VPN - сети взаимодействие абонентских пунктов с СМ, зарегистрированными в задачах защиты IP-трафика, и серверов между собой определяется связями, установленными в прикладной администрации.

3.1.1.2 Сетевая Группа

Несколько сетевых узлов могут быть объединены в сетевую группу.

Сетевая группа – это совокупность сетевых узлов, которые должны иметь возможность связываться друг с другом.

3.1.1.3 Сетевые Объекты

Сетевые объекты - это совокупность сетевых узлов и сетевых групп.

Каждый сетевой объект (узел или группа) имеет уникальный сетевой адрес.

Сетевой адрес имеет размер 8 байт. В него входят (слева направо):

поле селекторов	2 байта;
номер сети	2 байта;
номер СМ	2 байта;
номер АП в области данного СМ	2 байта;

Таким образом, структура сетевого адреса позволяет иметь до 65535 сетей ViPNet, не пересекающихся по сетевым адресам. В каждой сети может быть размещено до 65535 СМ, к каждому из которых может быть подключено до 65535 АП.

При продаже сетевого программного обеспечения сети ViPNet, включающего программу ЦУС, этой сети лицензируется уникальный номер.

Различные сети ViPNet могут взаимодействовать между собой после взаимного обмена необходимой сетевой и криптографической информацией.

Поле селекторов зарезервировано.

Наряду с сетевым адресом каждый сетевой объект (узел или группа) имеет уникальный 9-символьный шестнадцатеричный сетевой идентификатор. Первые 4 символа - шестнадцатеричный номер сети, следующие 4 символа - шестнадцатеричный идентификатор объекта в рамках сети, последний символ = '0' для сетевых узлов и '1' для сетевых групп.

В рамках одной сети сетевым объектам дается сквозная нумерация вне зависимости от принадлежности к конкретной области Сервера.

3.1.2 Основные понятия прикладного уровня

3.1.2.1 Прикладная задача

Прикладная задача (ПЗ) – это совокупность программных средств, предназначенных для решения целевых и служебных задач сети.

В настоящей версии поддерживаются следующие ПЗ: **Деловая почта, Центр управления сетью, Ключевой центр, Защита трафика, Сервер IP-адресов, Центр регистрации, Секретный диск** и др. Каждой ПЗ присвоен уникальный 4-символьный шестнадцатеричный идентификатор, который включается в транспортные конверты, генерируемые в рамках этих задач. Один сетевой узел ViPNet может быть зарегистрирован в нескольких прикладных задачах. По идентификатору ПЗ в транспортном конверте прикладная программа ViPNet определяет, что конверт адресован именно ей.

3.1.2.2 Пользователь (Абонент)

Абонентом (или пользователем) сети ViPNet называется владелец ключей пользователя для доступа в сеть. Пользователь несет всю полноту ответственности за действия, производимые в сети с использованием его ключей пользователя.

Имя пользователя (56 символов) должно быть уникальным в сети. При необходимости это имя можно изменять.

При регистрации пользователя автоматически создается уникальный 8-символьный шестнадцатеричный идентификатор пользователя.

Пользователь может регистрироваться в составе одного или нескольких коллективов на одном или нескольких сетевых узлах.

3.1.2.3 Коллектив, тип коллектива и связь коллективов

Отправителями и получателями почтовых сообщений в сети являются коллективы, в состав которых входят пользователи, имеющие одинаковые права. Поэтому на каждом сетевом узле (в том числе СМ) обязательно должен быть зарегистрирован хотя бы один коллектив, а в нем хотя бы один пользователь.

На одном сетевом узле (АП) может быть создано несколько различных коллективов, имеющих свои ключи для шифрования конфиденциальной информации.

Коллектив - это совокупность пользователей одного сетевого узла, имеющих одинаковые ключи для шифрования конфиденциальной информации.

Каждый коллектив имеет уникальный 13-символьный шестнадцатеричный идентификатор, составленный из 4-символьного шестнадцатеричного идентификатора типа коллектива и 9-символьного шестнадцатеричного идентификатора сетевого узла.

Включение пользователя в коллектив означает, что пользователь может расшифровать конфиденциальную информацию, отправленную этому коллективу или любому пользователю этого коллектива.

Коллектив появляется в адресных справочниках АП, если в нем зарегистрирован хотя бы один пользователь.

3.1.2.4 Тип Коллектива

Если на нескольких сетевых узлах должны быть коллективы с одинаковым именем и имеющих возможность связываться друг с другом, то такие сетевые узлы объединяются в одну сетевую группу, а на этой группе можно зарегистрировать один тип коллектива. Если тип коллектива зарегистрирован на одном АП, то этот тип коллектива совпадает с коллективом данного АП.

Тип коллектива (ТК) регистрируется на определенном одном сетевом объекте (узле или группе). Этот сетевой объект называется ОБЛАСТЬЮ ДЕЙСТВИЯ ТК.

При регистрации ТК ему автоматически выделяется уникальный 4-символьный шестнадцатеричный идентификатор. Это означает, что в сети допускается регистрация более 65 тыс. различных ТК.

Регистрация ТК на сетевой группе означает автоматическую регистрацию коллективов этого типа на всех узлах и подгруппах этой сетевой группы.

Это также автоматически означает, что коллектив определенного типа, действующий на одном сетевом объекте, имеет связь с любым коллективом этого же типа на любом другом сетевом объекте из области действия этого ТК.

3.1.2.5 Связь Коллективов

Связь между коллективами означает, что эти коллективы видят друг друга в адресных справочниках своих АП и могут связываться между собой с помощью зашифрованной связи на уникальных парных ключах, т.е. эту операцию могут осуществить любые пользователи, входящие в соответствующие коллективы.

Связь между коллективами означает также, что в ключах узлов, на которых зарегистрированы данные коллективы, будут присутствовать ключи транспортного уровня для связи между АП данных коллективов.

Для связи с СМ, на которых зарегистрированы данные АП, в ключи соответствующих узлов на ключи транспортного уровня заносятся автоматически.

В ключи узла АП с ЦУС автоматически, независимо от установленных связей, заносятся транспортные ключи для связи со всеми объектами сети (АП и СМ).

Связь между коллективами может появиться только, если они не пустые, то есть после регистрации в каждом из них хотя бы одного пользователя.

Связь между коллективами типа G1 с областью действия N1 и коллективами типа G2 с областью действия N2 автоматически означает, что коллектив типа G1 на любом сетевом объекте N1i из области действия группы N1, имеет связь с любым коллективом типа G2 на любом сетевом объекте N2j из области действия N2.

При регистрации ТК вводится имя длиной до 50 символов. Это имя должно быть уникальным в сети. По желанию это имя можно изменять.

Удаление ТК означает удаление его из каталога типов коллективов, а также удаление всех записей из каталога персональных списков коллективов этого типа.

При создании каталога типов коллективов в него автоматически включается ТК с идентификатором "0000", именем "Пользователь деловой почты" и областью действия "Вся сеть", имеющей идентификатор "0000".

Ключи коллектива этого типа используются для шифрования сообщений, адресуемых абонентскому пункту в целом, то есть всем пользователям данного АП.

3.1.2.6 Главный Коллектив

Если пользователь входит в несколько коллективов, то среди них всегда выделяется один коллектив, называемый главным.

Новые ключи пользователя отправляются только на тот АП, где зарегистрирован главный для данного пользователя коллектив. На другие АП ключи пользователя переносятся им самостоятельно.

3.1.2.7 Открытые и Скрытые Коллективы

Коллективы могут быть открытыми и скрытыми для данного пользователя.

Если коллектив определен как открытый для пользователя, то другие пользователи могут видеть его в этом коллективе в адресном справочнике АП.

Если коллектив определен как скрытый для пользователя, то другие пользователи не будут знать, что он входит в этот коллектив, хотя такому пользователю доступна вся информация, адресованная пользователям данного коллектива.

3.1.3 Разграничение доступа к конфиденциальной информации

Регистрацией коллективов на АП и пользователей в них обеспечивается возможность разграничения доступа к зашифрованной информации на различных АП.

В прикладной системе Деловой почты можно обеспечить неограниченное количество уровней доступа к конфиденциальной зашифрованной информации, хранящейся на АП и передаваемой по каналам связи.

С этой целью на каждом АП может быть зарегистрировано несколько разных коллективов, не имеющих доступа к конфиденциальной информации друг друга. В составе каждого коллектива регистрируются пользователи, имеющие одинаковый уровень доступа.

Если есть необходимость запретить доступ к конфиденциальной информации некоторого пользователя, то он должен присутствовать в каком-то коллективе один.

Каждый пользователь может быть зарегистрирован в одном или нескольких коллективах на одном или нескольких АП. В соответствии с этим пользователь получает на этих АП доступ к поступившей зашифрованной информации, предназначенной пользователям коллективов, в которых зарегистрирован данный пользователь, и не имеет доступа к зашифрованной информации других коллективов.

Этот пользователь имеет также доступ к поступившей зашифрованной информации, адресованной абонентским пунктам в целом, на которых он зарегистрирован.

Пользователь может быть зарегистрирован в каком-то коллективе явно, и тогда он виден в справочнике соответствующего коллектива. Однако некоторые пользователи могут быть зарегистрированы в каком-то коллективе и быть при этом скрытыми для него, то есть такие пользователи не видны в справочнике этого коллектива, но имеют доступ к засекреченной информации, адресованной этому коллективу. Эта возможность удобна для обеспечения доступа руководителя организации ко всей конфиденциальной информации некоторых АП.

Шифрование информации производится на ключах коллектива, куда входит пользователь.

Если пользователь зарегистрирован в нескольких коллективах, то шифрование информации производится на ключах некоторого одного коллектива, имеющего связь с выбранным адресатом. Выбор коллектива, на ключах которого будет производиться шифрование, осуществляется пользователем в программе Настройка параметров безопасности СУ на вкладке **Шифрование**. Таким образом, зашифрованную информацию на АП, где шифровалось сообщение, смогут прочитать только пользователи этого коллектива.

При рассылке новой ключевой информации для действующих пользователей ключи пользователей всегда высылаются на тот АП, где зарегистрирован главный для данного пользователя коллектив. Поэтому внимательно относитесь к регистрации главного коллектива для конкретного пользователя. Для работы на АП пользователя, для которого коллектив, зарегистрированный на этом АП, не является главным, пользователь должен приносить с собой ключи пользователя (каталог Key_Disk) с АП, где зарегистрирован главный для него коллектив.

При отправке зашифрованных документов производится их перешифрование на ключах в соответствии с выбранным адресом.

Регистрация пользователя в каких-то коллективах нескольких АП означает, что этот пользователь получает возможность войти в прикладную программу на данных АП и получить доступ к информации в соответствии с тем, как это указано выше.

3.2 Справочники для СУ

По окончании первоначального формирования структуры сети ViPNet и настройки различных параметров, а также после любых изменений в конфигурации сети, в ЦУС для всех новых узлов, а также узлов, которых коснулось изменения, должны быть сформированы специальные справочники – справочники сетевых узлов, справочники для УКЦ:

Справочники АП и СМ – набор защищенных файлов для соответствующего узла, определяющих:

- * список пользователей, которым разрешена работа на данном узле;
- * список коллективов пользователей данного узла;
- * список других узлов, пользователей и коллективов пользователей, с которыми разрешено защищенное взаимодействие с данного узла;
- * ограничения по режимам работы и права пользователей данного узла по изменению настроек на нем;
- * список приложений ПО ViPNet, использование которых разрешено на данном узле;
- * настройки данного узла для его работы в конкретных условиях TCP/IP сети.

В состав справочников СМ дополнительно входят маршрутные таблицы, которые определяют дальнейший маршрут почтовых конвертов, полученных данным СМ с других узлов.

Справочники для УКЦ – набор файлов, созданных ЦУС, на основании которых УКЦ формирует всю необходимую ключевую информацию для узлов и конкретных пользователей

сети ViPNet, обеспечивающую шифрование информации в соответствии с заданным адресным пространством для данного узла.

Справочники сетевых узлов, а также ключевая информация для каждого узла и пользователя входят в состав защищенных ключевых дистрибутивов пользователей, используемых для первоначального развертывания ПО ViPNet на СУ, и в дальнейшем после различных изменений обновляются дистанционно из ЦУС.

3.3 Организация межсетевого взаимодействия

Между двумя различными сетями ViPNet может быть организовано межсетевое взаимодействие. В этих целях в программе ЦУС предусмотрены специальные меры по формированию экспортных данных для ЦУС других сетей и импорта данных от других ЦУС.

Обмен информацией между пользователями двух различных сетей производится через один из СМ каждой сети, называемых шлюзовыми.

При формировании экспорта в программе ЦУС каждой сети указывается, какие коллективы, на каких АП должны взаимодействовать с пользователями другой сети. Указывается, какой из СМ данной сети является шлюзовым для другой сети. Эти данные оформляются в виде экспорта для другой сети. Одновременно в данные экспорта автоматически включаются все пользователи, зарегистрированные в экспортированных коллективах на выбранных АП.

Данные экспорта другой сети импортируются в базу данных ЦУС. В результате в списке коллективов данного ЦУС появляются коллективы из другой сети, зарегистрированные на АП внешней сети. В списке СМ появляется СМ другой сети.

Установив логический канал связи между импортированным СМ и своим СМ, переданным в качестве шлюзового в другую сеть, и установив связи между импортированными коллективами и коллективами своей сети, переданными в другую сеть, в каждом из ЦУС формируются абонентские справочники и маршрутные таблицы для своих АП и СМ, в которых видны пользователи другой сети. Если сторона, установившая связи своих коллективов с коллективами другой сети опять отправит экспорт в другую сеть, то эти связи также автоматически импортируются ЦУС другой сети.

После первоначального обмена данными экспорта и импорта дальнейшее обновление этих данных в обоих ЦУС производится автоматически по защищенным каналам связи при помощи транспортного модуля ViPNet MFTP.

Для обеспечения независимого криптографического межсетевого взаимодействия между криптографическими администрациями организуется обмен специальными межсетевыми мастер-ключами. Между каждой парой сетей могут быть как свои мастер-ключи, так и использоваться общие межсетевые мастер-ключи для связи со всеми сетями. Внутренний обмен осуществляется на основе своих мастер-ключей, независимых от межсетевых.

Возможны два способа генерации межсетевых мастер-ключей.

Пара межсетевых ключей формируется одним из Ключевых центров и передается другому.

В каждом из Ключевых центров формируется закрытая и открытая часть своего межсетевого ключа. Открытая часть передается в другую сеть. Мастер-ключ для связи с некоторой сетью образуется на основе своего секретного ключа и открытого ключа другой сети.

Сформировав межсетевые мастер-ключи, ключевая информация каждым из Ключевых центров формируется только для своих пользователей.

Сети, с которыми организовано межсетевое взаимодействие, называются доверенными сетями.

4 Установка программного обеспечения ЦУС. Системные требования

Программа ViPNet Центр управления сетью (ЦУС) входит в состав ПО ViPNet Administrator.

Минимальные требования к аппаратным средствам для установки ЦУСа следующие:

- Процессор — не менее Pentium IV.
- ОЗУ — не менее 512 МБайт (рекомендуется 1 Гбайт). ЦУС работает в режиме protected mode и использует до 16 Мбайт оперативной памяти.
- Свободное место на жестком диске — не менее 1 Гбайт.
- Операционная система — Windows XP SP3/Server 2003/ Vista SP2/Server 2008/Windows 7.

Внимание! ЦУС является DOS-приложением и может работать только под управлением 32-битных ОС Windows.

В случае установки ЦУСа совместно с программой ViPNet Удостоверяющий и ключевой центр на компьютере должна использоваться 32-битная ОС, при этом оперативная память должна быть не менее 1 Гбайт (рекомендуется 2 Гбайт).

Для работы ЦУС необходимо, чтобы максимальное число одновременно открытых файлов в сеансе MS-DOS составляло не менее 20. Это число задается строкой FILES=n в файле CONFIG.NT (он находится в каталоге %systemroot%\System32\) для операционных систем WINDOWS 2000/XP/Server 2003.

Инсталляция производится с инсталляционного комплекта ViPNet Administrator.

Данный инсталляционный комплект позволяет установить на один компьютер программу ЦУС и УКЦ (Удостоверяющий и Ключевой центр).

Перед установкой рекомендуется скопировать файлы лицензии infotecs.re, infotecs.reg в одну папку с программой установки setup.exe, тогда при установке они автоматически разложатся в нужные папки: infotecs.re, infotecs.reg – в папку установки ЦУС, infotecs.re – в папку установки УКЦ. В ином случае после установки ViPNet Administrator необходимо вручную разложить файлы лицензии в указанные выше папки.

Для установки комплекта необходимо запустить SETUP.EXE и далее действовать в соответствии с подсказками инсталлятора. Для обеспечения работы АП администратора нужно подготовить рабочее место администратора.

Подробную инструкцию по установке ViPNet Администратор и подготовке рабочего места администратора читайте в отдельном документе "[Инструкция по установке, запуску, удалению ViPNet Administrator](#)", имеющемся в инсталляционном комплекте.

5 Порядок развертывания сети ViPNet

Установка программного обеспечения и развертывание сети ViPNet должны осуществляться в следующей последовательности:

Установка программного обеспечения ЦУС и УКЦ в соответствии с инструкцией по установке и настройке рабочего места администратора.

Внимание! Если должна быть организована работа иерархической системы Центров управления сетью, то ознакомьтесь с разделом 6.

Формирование структуры сети ViPNet в соответствии с разделом 8 настоящего руководства.

Генерация ключевой информации и дистрибутивов в соответствии с руководством пользователя Удостоверяющего и Ключевого центра.

Установка программного обеспечения ViPNet Coordinator в соответствии с руководством Координатора.

Установка программного обеспечения ViPNet на АП в соответствии с руководством пользователя прикладной системы.

6 Организация работы иерархической системы Центров управления сетью

Центры управления сетью нескольких сетей ViPNet могут быть объединены в иерархическую систему Центров управления сетью. Это означает, что ЦУС какой-либо сети ViPNet (назовем такую сеть и ЦУС головными) может управлять Центрами управления сетью других сетей ViPNet (назовем такие сети и ЦУС подчиненными).

Для объединения Центров управления сетью в иерархическую систему необходимо:

Наличие специального файла лицензии (Infotecs.reg), где указаны суммарные лицензионные ограничения на головную и подчиненные сети ViPNet, а также номера головной и подчиненных сетей. Файл предназначен для ЦУС, который планируется сделать головным. Файлы лицензии для подчиненных ЦУС будут сделаны головным ЦУС после его установки.

Во всех сетях ViPNet, входящих в иерархическую систему, наличие установленной версии ЦУС не ниже 2.8 (11.1825).

Головной ЦУС помимо основных функций ЦУС обеспечивает следующие возможности:

Централизованное управление лицензиями своей сети ViPNet и подчиненных сетей в рамках выданной общей лицензии. Т.е. в головном ЦУС происходит распределение лицензий, прописанных в общем файле лицензии, по своей сети и подчиненным сетям, а затем централизованная отправка полученных файлов лицензии в подчиненные сети.

Централизованный контроль количества использованных лицензий и структуры сети ViPNet в подчиненных сетях. Т.е. подчиненные ЦУС при изменениях в структуре своей сети высылают соответствующие отчеты в головной ЦУС.

6.1 Организация иерархической системы ЦУС при первоначальном развертывании сетей ViPNet

Для того, чтобы развернуть иерархическую систему ЦУС в сетях ViPNet, требуется выполнить следующий порядок действий:

1. Начинать развертывание сети ViPNet необходимо с сети, которая планируется быть **головной**:

Установите ПО ViPNet Администратор версии не ниже 2.8 (11.1825) на компьютер администратора ЦУС головной сети (в соответствии с инструкцией по установке). Проверьте, что специальные файлы лицензии (с суммарными лицензионными ограничениями на головную и подчиненные сети ViPNet) помещены в папку установки ЦУС. Подготовку рабочего места администратора на данном этапе можно не производить.

Запустите ЦУС (см. п.7).

Распределите лицензии для своей сети. Для этого выберите пункт главного меню **Службы/Распределение лицензий для сетей**. В открывшемся окне **Распределение лицензий** (Рисунок 1) выберите строку с номером головной сети (в колонке **Статус** обозначена значением **Головная**) и нажмите кнопку **Лицензии**. Произведите настройки лицензии для своей сети, используя кнопку **Изменить**, в соответствии с разделом 17.

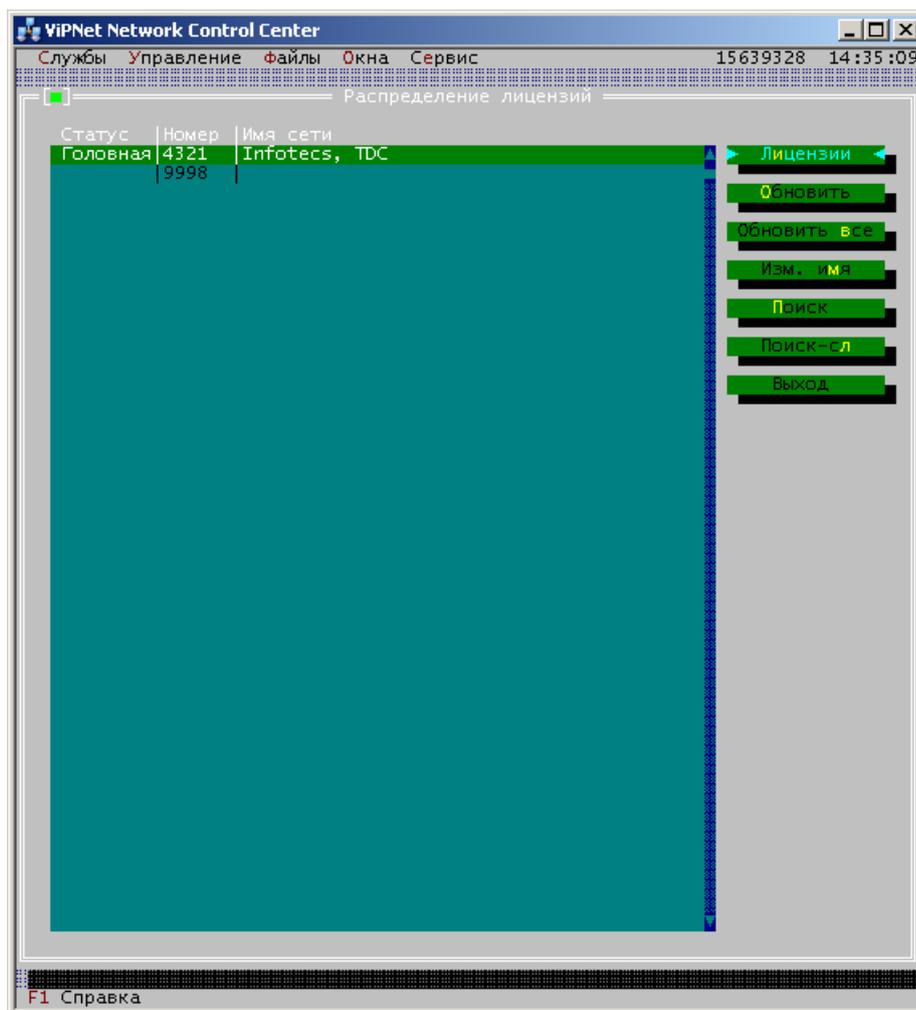


Рисунок 1

Если Вам уже известны параметры подчиненных сетей, то произведите настройки лицензии для подчиненных сетей. Распределите лицензии по сетям и задайте имена сетей. Для этого в окне **Распределение лицензий** (Рисунок 1) выберите строку с номером нужной сети и нажмите кнопку **Лицензии**. В открывшемся окне произведите настройки лицензии, используя кнопку **Изменить**, в соответствии с разделом 17. Задайте имя подчиненной сети, нажав кнопку **Изм. имя** в окне **Распределение лицензий** (Рисунок 1). Выполните эти действия для каждой подчиненной сети. После произведенных настроек сформируются файлы лицензии (infotecs.re, infotecs.reg) для подчиненных сетей, которые помещаются в экспорт для соответствующих сетей. Файлы лицензии нужно перенести в заданную папку для передачи в подчиненные сети при помощи пункта меню **Управление/Отправить измененные файлы/Экспорт** (кнопка **Перенести**, см. п. 21.2.4).

Передайте сформировавшиеся файлы лицензии каким-либо защищенным способом администраторам ЦУС подчиненных сетей, после чего они могут начать развертывание своих подчиненных сетей (см. ниже абзац 2).

Можно приступать к первичной конфигурации своей сети (см. п.8) и подготовке рабочего места администратора (в соответствии с инструкцией по установке).

2. После получения файлов лицензии от администратора ЦУС головной сети произведите развертывание **подчиненных** сетей ViPNet:

Установите ПО ViPNet Администратор версии не ниже 2.8 (11.1825) на компьютер администратора ЦУС подчиненной сети (в соответствии с инструкцией по установке). Проверьте, что новые файлы лицензии, переданные администратором ЦУС головной сети, помещены в папку установки ЦУС.

Запустите ЦУС и приступайте к первичной конфигурации сети (см. п.8) и подготовке рабочего места администратора (в соответствии с инструкцией по установке). Информацию о статусе сети и об используемой лицензии можно посмотреть с помощью пункта меню **Сервис/Лицензия** (см. п. 22.1).

6.2 Перевод действующих сетей ViPNet на использование иерархической системы ЦУС

Для того чтобы перевести несколько действующих сетей ViPNet (развернутых и функционирующих) на использование иерархической системы ЦУС, выполните следующие действия:

1. Установите ПО ViPNet Администратор версии не ниже 2.8 (11.1825) на компьютеры администраторов ЦУС головной и подчиненных сетей, которые планируется объединить в иерархическую систему ЦУС (в соответствии с инструкцией по установке).
2. Выполните нижеописанные действия на компьютере администратора ЦУС сети ViPNet, которая планируется быть **головной**:

Проверьте, что новые файлы лицензии (с суммарными лицензионными ограничениями на головную и подчиненные сети ViPNet) помещены в папку установки ЦУС или скопируйте их туда вручную.

Вместе с новыми файлами лицензии Вам могли быть переданы предыдущие версии файлов лицензии для всех существующих ранее сетей ViPNet, которые Вы переводите на использование иерархической системы ЦУС. Переданные файлы лицензии расположены в папке со следующей структурой: REGS\<номер сети>\Infotecs.reg. Скопируйте папку REGS и ее содержимое в папку установки ЦУС. Эта информация потребуется Вам для быстрого и удобного распределения лицензий по сетям ViPNet. Вы можете подготовить такую структуру самостоятельно, запросив у администраторов ЦУС всех сетей их текущие файлы лицензии из папки установки ЦУС, и поместив их в вышеуказанные папки.

Запустите ЦУС (см. п.7).

Распределите лицензии для своей и подчиненных сетей. Для этого выберите пункт главного меню **Службы/Распределение лицензий для сетей**. В открывшемся окне **Распределение лицензий** (Рисунок 1) выберите строку с номером нужной сети и нажмите кнопку **Лицензии**. Сначала произведите настройки для головной сети, затем для подчиненных. Головная сеть обозначена значением **Головная** в колонке **Статус**. Вы можете импортировать все лицензии из предыдущей версии Infotecs.reg каждой сети (REGS\<номер сети>\Infotecs.reg, который Вы ранее скопировали в папку установки ЦУС), нажав кнопку **Импорт лицензий**, или назначить лицензии вручную с помощью кнопки **Изменить**. Выполните действия в соответствии с разделом 17.

Замечание: При распределении лицензий, обеспечьте правильные ограничения лицензий для головной сети, чтобы они не были меньше уже использованного в головном ЦУС числа лицензий.

Если в Вашей сети уже было организовано межсетевое взаимодействие с подчиненными сетями, то в колонке **Имя сети** окна **Распределение лицензий** (Рисунок 1) будет отображаться имя сети из окна **Экспорт**. Вы можете сменить это имя, нажав кнопку **Изм. имя** (Рисунок 1).

После произведенных настроек сформируются файлы лицензии (infotecs.re, infotecs.reg) для подчиненных сетей, которые помещаются в экспорт для соответствующих сетей. Если межсетевое взаимодействие с подчиненными сетями установлено, то для передачи сформированных файлов лицензии в подчиненные сети отправьте экспорт в эти сети с помощью пункта меню **Управление/Отправить измененные файлы/Экспорт** (кнопка **Отправить**). Если межсетевое взаимодействие еще не установлено, то передайте сформированные файлы лицензии администраторам ЦУС подчиненных сетей каким-либо защищенным способом, предварительно перенеся их в заданную папку с помощью пункта меню **Управление/Отправить измененные файлы/Экспорт** (кнопка **Перенести**). Выполните эти действия в соответствии с разделом 21.2.4.

3. На компьютерах администраторов ЦУС **подчиненных** сетей ViPNet:

Запустите ЦУС. Если межсетевое взаимодействие с головной сетью установлено, то после получения импорта (с новыми файлами лицензии) из головной сети (см. п. 15), ЦУС автоматически перейдет на использование новой лицензии. Если межсетевое взаимодействие с головной сетью не установлено, то после получения файлов лицензии от администратора ЦУС головной сети скопируйте их в папку установки ЦУС и запустите ЦУС. Информацию о статусе сети и новой лицензии можно посмотреть с помощью пункта меню **Сервис/Лицензия** (см. п. 22.1).

6.3 Работа в головном ЦУС

После организации иерархической системы ЦУС для нескольких сетей в головном ЦУС появляются дополнительные возможности:

Распределение лицензий на свою (головную) и подчиненные сети (см. п.6.3.1).

Отправка лицензий в подчиненные сети (см. п.6.3.2).

Получение и просмотр отчетов из подчиненных сетей (см. п.6.3.3).

6.3.1 **Распределение лицензий для сетей**

Администратор головного ЦУС осуществляет распределение лицензионных ограничений по своей и подчиненным сетям в рамках общего файла лицензии, выданного на все сети иерархической системы. Тем самым администратор головного ЦУС создает файлы лицензии (infotecs.re, infotecs.reg) для каждой сети, которые в дальнейшем может изменять.

Для распределения лицензий выберите пункт главного меню **Службы/Распределение лицензий для сетей**. В открывшемся окне **Распределение лицензий** (Рисунок 1) для головной и подчиненных сетей назначьте лицензионные ограничения при помощи кнопки **Лицензии**, а для подчиненных сетей задайте также имена сетей при помощи кнопки **Изм. имя**.

Если для головного ЦУС изменился специальный файл лицензии и требуется обновить файлы лицензии в подчиненных сетях без перераспределения лицензионных ограничений (например, если в лицензии изменился только разрешенный номер версии используемого ПО ViPNet), то воспользуйтесь кнопками **Обновить** для подготовки файлов лицензии для выбранной сети или **Обновить все** – для всех подчиненных сетей.

Подробности распределения лицензий читайте в разделе 17.

После произведенных настроек будут сформированы файлы лицензии (infotecs.re, infotecs.reg) для тех сетей, лицензии которых изменялись.

Головной ЦУС автоматически перейдет на использование нового файла лицензии. Файлы лицензии для подчиненных сетей помещаются в экспорт для соответствующих сетей. Вы можете их отправить в ЦУС подчиненных сетей (см. п. 6.3.2).

6.3.2 **Отправка (передача) файлов лицензий в подчиненные сети**

После создания или изменения лицензий для подчиненных сетей администратору головного ЦУС необходимо их отправить в ЦУС подчиненных сетей.

Файлы лицензии отправляются в составе экспорта. Для отправки выберите пункт меню **Управление/Отправить измененные файлы/Экспорт**. Отправьте или перенесите экспорт в соответствии с разделом 21.2.4.

Если в какую-либо подчиненную сеть необходимо повторно отправить файлы лицензии (не изменяя их), то в окне **Экспорт**, доступном по пункту меню **Службы/Экспорт**, скопируйте файлы экспорта для данной сети (кнопка **Копировать**, см. п.15.1, **Копирование экспортных данных для сети**). Затем отправьте экспорт, как описано выше.

6.3.3 Получение и просмотр отчетов из подчиненных сетей

Администратор головного ЦУС может осуществлять централизованный контроль действий администраторов подчиненных ЦУС по конфигурированию сети. Централизованный контроль может быть осуществлен только после организации межсетевого взаимодействия с подчиненными сетями. Контроль осуществляется на основе следующей информации, поступающей из подчиненных ЦУС:

1. При изменениях в структуре подчиненной сети ЦУС подчиненной сети формирует отчеты о текущей конфигурации сети:

Отчет об использовании лицензии (текстовый файл st<номер сети>.ger) – в этом отчете отображается информация о лицензионных ограничениях и числе использованных лицензий в подчиненной сети. Информация, отображаемая в этом отчете, аналогична информации, получаемой для своей сети при использовании пункта меню **Сервис/Лицензия** (см. п. 22.1).

Отчет о структуре сети (текстовый файл sr<номер сети>.ger) – в этом отчете отображается информация о структуре сети и перечне прикладных задач, в которых зарегистрированы узлы сети. Информация, отображаемая в этом отчете, аналогична информации, получаемой для своей сети при использовании пункта меню **Службы/Просмотр конфигурации сети/Структура сети в узком формате** (см. п.18.1.1).

Данные отчеты поступают в головной ЦУС вместе с импортом из подчиненного ЦУС. После обработки импорта (см. п. 15.3) отчеты помещаются в подпапку папки установки ЦУС: REP\<номер сети>\<дата формирования отчетов>. **Замечание:** Если в один день придет несколько импортов с отчетами из одной и той же сети, то при сохранении очередных отчетов к имени папки с датой формирования отчетов будет добавляться расширение (например, 23012007, 23012007.1, 23012007.2).

Для просмотра отчетов используйте любой текстовый редактор. Для определения изменений в отчетах (добавление/удаление узла, регистрация узла в прикладной задаче и т.д.) необходимо использовать внешние средства сравнения текстовых файлов, например, Araxis Merge.

Замечание: Поскольку файлы в папке \REP постоянно накапливаются, рекомендуем регулярно отслеживать размер этой папки и при слишком большом размере папки переносить часть самых старых файлов на съемные диски (например, CD/DVD) или другие носители.

2. После отправки экспорта в подчиненный ЦУС информация о времени отправки, доставки и обработки последнего отправленного экспорта в подчиненном ЦУС отобразится в окне **Экспорт**. Для просмотра информации выберите пункт главного меню **Службы/Экспорт** (см. п. 15.1, **Просмотр времени получения и обработки экспорта в доверенных сетях ViPNet**).
3. После получения от головного ЦУС импорта с новыми файлами лицензии, ЦУС подчиненной сети автоматически высылает в головной ЦУС текущую информацию о числе использованных лицензий.

Факт получения отправленного экспорта подчиненным ЦУС, как было описано выше (2), можно проконтролировать в окне **Экспорт** (для соответствующей сети в колонке **Действие** должно отображаться значение **Принят**).

Убедившись, что экспорт был принят подчиненным ЦУС, можно посмотреть информацию о числе использованных лицензий. Для просмотра воспользуйтесь пунктом главного меню **Службы/Распределение лицензий для сетей**, в открывшемся окне для соответствующей подчиненной сети нажмите кнопку **Лицензии** и посмотрите информацию в колонке **Использовано** (Рисунок 53).

6.3.4 Обновление лицензии

После получения нового специального файла лицензии поместите его в папку установки ЦУС головной сети. Запустите ЦУС. Если лицензия была увеличена, то Вы можете распределять лицензии по сетям (своей и подчиненным) в пределах Вашей новой лицензии.

7 Запуск программы и завершение работы с ней

Запустить программу можно несколькими способами.

Способ 1:

1. Нажмите на кнопку **Пуск (Start)** на панели задач Windows и в появившемся меню Windows выберите пункт **Программы (Programs)**.
2. Затем выберите пункты, соответствующие ПО ViPNet Administrator ЦУС. По умолчанию это **ViPNet -> Administrator**, но, Вы могли изменить названия в процессе установки. Далее выберите пункт **ViPNet Центр Управления сетью**.

Способ 2:

Также для запуска ViPNet Administrator ЦУС можно использовать ярлык  на рабочем столе Windows, если в процессе установки Вы не отменили его создание.

Способ 3:

Можно запустить ViPNet Administrator ЦУС непосредственно из папки установки. Для этого откройте папку установки программы (по умолчанию C:\Program Files\InfoTeCS\ViPNet Administrator) в каком-либо файловом менеджере (например, Windows Commander, Windows Explorer и т.д.), и запустите файл _start.bat.

Замечание: В операционной системе Windows 7 возможны проблемы с отображением шрифтов в окне программы ViPNet Administrator ЦУС. Чтобы избежать этих проблем, выполните

следующие действия: щелкните ярлык  правой кнопкой мыши и в контекстном меню выберите пункт **Свойства**; в окне свойств откройте вкладку **Шрифт**; в списке **Шрифт** выберите пункт **Точечные шрифты** и нажмите кнопку **ОК**.

Другой способ решения проблемы – в свойствах ярлыка на вкладке **Совместимость** установить режим совместимости с Windows XP (пакет обновления 3).

Если ярлык ViPNet Administrator ЦУС не был создан, следует запускать программу с помощью файла _start.bat (для этого файла можно создать ярлык).

После первого запуска программы ЦУС появится окно настройки путей к папкам транспортного модуля и папкам обмена с УКЦ. Произведите соответствующие настройки (в соответствии с разделом 21.4).

Далее появится окно с настройками по умолчанию. Следует выбрать интересующие Вас настройки (в соответствии с разделом 11.4).

Далее можно приступать к работе в программе.

Замечание: В программе ViPNet Administrator ЦУС переключение клавиатуры с английской раскладки на русскую и наоборот осуществляется с помощью правой клавиши CTRL.

В ходе работы ЦУС автоматически создаются:

папка MAP, в которую записываются таблицы сетевой и межсетевой маршрутизации для Серверов-маршрутизаторов,

папка APDB, в которую записываются справочники для AP и CM,

папка ABN, в которую записываются справочники связей пользователей, используемые при создании ключей пользователей,

папка DB, в которой хранятся Базы Данных ЦУС,

папка NEW, а в ней подпапки APDB, ABN, EXPORT, в которых хранятся все новые файлы, появляющиеся после внесения каких-либо изменений в конфигурацию сети,

папка EXPORT, в которой в соответствующих подкаталогах хранятся необходимые данные для экспорта в другие сети ViPNet,

папка IMPORT, в которой помещаются экспортные данные из других сетей ViPNet,

папка R, в которой хранятся отправленные запросы,
папка S, в которой хранятся ответы на запросы,
папка ARC, в которой хранятся архивы баз данных ЦУС,
другие служебные папки.

Внимание! В рабочих папках ЦУС не следует создавать никаких личных папок.

Для завершения работы программы (выгрузки ее из памяти компьютера) выберите пункт главного меню **Файлы/Выйти**.

8 Типовой порядок первичной конфигурации сети ViPNet

В этом разделе по шагам описывается типовая схема первичной генерации сети. Для более подробной информации по каждому из шагов читайте последующие разделы руководства.

1. Шаг 1. Регистрация Серверов
2. Шаг 2. Регистрация абонентских пунктов
3. Шаг 3. Задание каналов между Серверами
4. Шаг 4. Регистрация сетевых групп
5. Шаг 5. Формирование таблиц маршрутизации
6. Шаг 6. Задание адресов сетевых узлов сети ViPNet при работе через внешние сети
7. Шаг 7. Регистрация АП и СМ в конкретных прикладных задачах
8. Шаг 8. Регистрация типов коллективов (ТК) на АП, СМ, сетевых группах
9. Шаг 9. Задание связей между коллективами
10. Шаг 10. Регистрация пользователей
11. Шаг 11. Установка атрибутов коллектива пользователя
12. Шаг 12. Задание адресов рассылки копий
13. Шаг 13. Первоначальное формирование Экспорта и получение Импорта
14. Шаг 14. Контроль правильности конфигурации системы
15. Шаг 15. Формирование адресных справочников, маршрутных таблиц, справочников для УКЦ

Далее следует более подробное описание этих шагов.

Замечание. При необходимости создания структуры сети, имена узлов которых могут быть заданы по определенному правилу, можно воспользоваться автоматической генерацией при помощи пункта меню **Службы/Адресная администрация/Автоматическая генерация...** (см. п. 11.2, стр.47).

16. Шаг 16. Формирование ключевой информации в программе УКЦ (читайте документацию ViPNet Administrator Удостоверяющий и ключевой центр, раздел **Создание ключевой информации при первоначальном развертывании сети**).

8.1 Генерация сетевой структуры

Генерация сетевой структуры осуществляется подсистемой адресной администрации ЦУС, вызываемой выбором пункта меню **Службы/Адресная администрация/Структура сети ViPNet**.

Описание этой подсистемы приведено в разделе 11 настоящего руководства.

Напомним основные определения.

Сетевой узел - это отдельный АП или СМ.

Сетевая группа - это совокупность сетевых узлов, которые должны иметь возможность связываться друг с другом.

Сетевые объекты - это совокупность сетевых узлов и сетевых групп.

Шаг 1. Регистрация Серверов

Выберите пункт меню **Серверы-маршрутизаторы** и нажмите **Enter**.

Если в сети пока не было Серверов, то появится строка ввода. Введите в этой строке имя Сервера и нажмите **Enter**. Появится окно со списком зарегистрированных Серверов.

Для регистрации второго Сервера нажмите клавиши **Alt+I**. В появившейся строке ввода введите имя второго Сервера и нажмите **Enter**. В списке Серверов появятся уже два имени.

Таким образом, Вы должны зарегистрировать все СМ Вашей сети.

ВНИМАНИЕ! Имена СМ не должны повторяться.

Шаг 2. Регистрация абонентских пунктов

Для подключения АП к какому-либо Серверу подведите курсор к имени этого СМ и нажмите **Enter**. Появится окно со списком всех сетевых узлов, входящих в область этого с Сервера. Первоначально в эту область входит только сам Сервер.

Для регистрации АП нажмите клавиши **Alt+I**. В появившейся строке ввода введите имя этого АП и нажмите **Enter**. Это имя добавится к списку АП данного Сервера.

Аналогичные операции выполните для подключения остальных АП, которые должны быть зарегистрированы на этом и других СМ.

ВНИМАНИЕ! Каждый АП может быть подсоединен только к одному Серверу.

Имена АП не должны повторяться.

Шаг 3. Задание каналов между Серверами

Подведите курсор к имени первого Сервера и нажмите клавиши **Alt+M**, а затем сделайте это же для второго Сервера. После того как два Сервера будут отмечены, нажмите клавиши **Alt+C** для задания канала между отмеченными Серверами. Нажав клавиши **Alt+Z** можно посмотреть список всех межсерверных каналов, имеющихся у текущего Сервера.

Внимание! Координатор, планируемый для использования в составе ПАК NME-RVPN ViPNet, должен иметь только один межсерверный канал.

Аналогичным образом задайте каналы между всеми Серверами.

Если у Вас один СМ, то этот шаг может быть пропущен.

Если у Вас несколько СМ, то Вы можете задавать любые каналы между СМ. Например, можно связать все СМ с одним центральным (схема "звезда"). В этом случае вся почтовая информация будет циркулировать через центральный СМ.

Если Вы свяжете каждый СМ с каждым, то информация между ними будет маршрутизироваться по кратчайшему маршруту.

Если Вы свяжете СМ по кольцу, то информация от СМ к СМ будет передаваться по этому кольцу в ближайшую сторону.

В последних двух случаях программа сообщит, что имеются циклы.

ВНИМАНИЕ! Проверьте, что все СМ логически связаны между собой, то есть от каждого СМ к каждому есть маршрут. Если не будет полной связности, программа предупредит Вас об этом.

Шаг 4. Регистрация сетевых групп

При необходимости следует зарегистрировать сетевые группы и включить в них определенные АП. В группы можно объединять АП, которые однозначно должны быть связаны друг с другом. Создание групп облегчит дальнейшие действия по генерации сети, но наличие их не обязательно. На группе можно зарегистрировать общий тип коллектива с одним названием,

например “Общий отдел”. В этом случае в справочниках всех АП появится коллектив с названием “Общий отдел”.

Внутри групп можно создать подгруппы АП.

Вернитесь в головное меню подсистемы адресной администрации, выберите пункт меню **Группы АП** и нажмите **Enter**.

Если в сети пока нет сетевых групп, то появится строка ввода. Введите в этой строке имя группы и нажмите **Enter**. Появится окно со списком зарегистрированных групп.

Для добавления новых групп используйте клавиши **Alt+I** или **Alt+O**.

Сделайте созданную группу текущей. Для этого нажмите клавиши **Alt+G**.

Вернитесь в головное меню подсистемы адресной администрации, выберите пункт меню **Серверы-маршрутизаторы** и нажмите **Enter**. Выберите Сервер, где есть АП из этой группы, и нажмите **Enter**. Нажмите клавишу **Ins**, находясь на строках, которые обозначают АП или сам СМ, входящие в создаваемую группу. Эти АП будут помечены символом “*” слева от имени. Кроме того, этим символом будут помечены СМ, в областях которых есть АП, входящие в текущую группу. Аналогично поступите для других Серверов, где есть АП или СМ, которые Вы хотите включить в созданную группу.

Аналогичные операции проделайте для регистрации всех создаваемых сетевых групп.

ВНИМАНИЕ! Имена сетевых групп не должны повторяться.

ВНИМАНИЕ! При необходимости удаления АП или СМ из текущей группы, на котором уже зарегистрированы пользователи, предварительно, выбрав пункт меню **Службы/Регистрация пользователей**, следует удалить все записи о включении пользователя в ТК на удаляемых сетевых узлах.

Шаг 5. Формирование таблиц маршрутизации

В соответствии с таблицами маршрутизации (маршрутными таблицами), которые формируются для каждого СМ, происходит процесс выбора оптимального пути для передачи почтовых конвертов между СУ в рамках одной или нескольких сетей ViPNet.

Данный шаг не является обязательным, поскольку выполняется автоматически на последующих этапах (при формировании всех справочников на шаге 15, п. 8.5), но его можно выполнить для проверки правильности созданной адресной структуры.

Вернитесь в головное меню подсистемы адресной администрации, выберите пункт меню **Выдать таблицы маршрутизации** и нажмите **Enter**.

ВНИМАНИЕ! Если Вы не обеспечили полной связности между СМ, то есть не существует между какими-либо СМ маршрута для прохождения информации, программа предупредит Вас об этом. Введите необходимые каналы.

Если программа выдала сообщение “*Имеются циклы*”, это означает, что имеется несколько возможных маршрутов между какими-либо СМ. В этом случае информация между этими СМ будет передаваться по кратчайшему маршруту между ними.

В подкаталоге \MAP рабочего каталога ЦУС будут сформированы таблицы маршрутизации.

Информацию о сформированной сетевой структуре Вашей сети можно получить в текстовом виде по ключу **Enter** в позиции **Вывод БД в текстовый файл**. Файл записывается в подкаталог \MAP рабочего каталога ЦУС.

Для завершения работы с подсистемой адресной администрации нажмите клавишу **Esc** или выберите пункт головного меню **Выход**.

Появится экран основной программы ЦУС.

Шаг 6. Задание адресов сетевых узлов сети ViPNet при работе через внешние сети

Для задания таких адресов следует выбрать пункт меню **Службы/Адресная администрация/Адреса во внешних сетях**. Появится диалоговое окно со списком всех узлов своей сети.

Выбрав нужный сетевой объект, нажмите кнопку **Адреса**. Появится окно, в котором Вы можете настроить адреса для выбранного сетевого узла.

Если на узлах сети используется Драйвер сетевой защиты ViPNet (ПО ViPNet Client или ViPNet Coordinator), то в этом окне адреса можно не задавать. Они автоматически попадут сюда при задании адреса в окне регистрации узла в задаче **Защита трафика**.

Вы можете задать IP-адреса сетевых узлов сети ViPNet, а также их SMTP-адреса. Заданные Вами адреса попадут в состав адресных справочников соответствующих сетевых узлов сети ViPNet.

Всегда достаточно задать адреса только СМ.

8.2 Генерация прикладной структуры

Напомним основные определения.

Коллектив - это совокупность пользователей одного сетевого узла, имеющих одинаковые ключи для шифрования конфиденциальной информации. Коллектив может состоять и из одного пользователя.

На одном АП может быть создано несколько различных коллективов, имеющих свои ключи для шифрования конфиденциальной информации.

Если на нескольких АП должны быть коллективы, имеющие одинаковые имя и возможность связываться друг с другом, то такие коллективы объединяются в один тип коллектива (ТК), который можно зарегистрировать на группе АП. Если тип коллектива зарегистрирован на одном АП, то этот тип коллектива совпадает с коллективом данного АП.

Регистрация коллектива данного типа на определенном сетевом узле осуществляется при регистрации типа коллектива на этом узле или сетевой группе, в которую входит этот узел.

Сетевой объект (АП, СМ или сетевая группа), на котором зарегистрирован тип коллектива, называется областью действия данного ТК.

Связь между коллективами означает, что они видны в справочниках друг друга и могут обмениваться информацией с помощью шифрованной связи на уникальном ключе, т.е. эту операцию могут осуществить любые пользователи, входящие в соответствующие коллективы.

Задание связей между коллективами определяется связями между типами коллективов. Задание связи между двумя типами коллективов автоматически означает наличие связи между любыми коллективами этих двух типов.

Шаг 7. Регистрация АП и СМ в конкретных прикладных задачах

Регистрация АП и СМ в конкретных прикладных задачах означает предоставление возможности установки на данном АП (СМ) соответствующих (одной или нескольких) прикладных задач (Деловая почта, Защита трафика и др.).

Если в окне настроек по умолчанию у Вас задана автоматическая регистрация в интересующих Вас задачах, то этот шаг можно выполнять не полностью. Необходимо только зарегистрировать один или два АП в задачах ЦУС и Ключевой центр, а также ввести все необходимые адреса для серверов IP-адресов.

Для регистрации АП в прикладной задаче выполните команду меню **Службы/ Индивидуальная регистрация АП в задачах**. Появится диалоговое окно со списком АП, зарегистрированных в различных прикладных задачах.

Для регистрации АП установите курсор на нужный АП и нажмите кнопку **Регистрация**. Появится окно со списком всех прикладных задач. Укажите задачи, в которых Вы регистрируете данный АП.

Регистрацию можно выполнить и выбрав пункт с конкретной прикладной задачей и добавив туда нужный узел.

Для регистрации СМ в задаче **Сервер IP-адресов** выполните команду меню **Службы/ Групповая регистрация узлов в задачах**, затем в появившемся окне выберите прикладную задачу **Сервер IP-адресов** и нажмите кнопку **Регистрация**. Появится диалоговое окно, в котором

можно добавить СМ, если он будет использоваться как Сервер IP-адресов. Если этот сервер должен использоваться как Сервер открытого Интернета, то нажмите кнопку **Сервер ОИ**. Если этот сервер должен туннелировать в защищенное соединение IP-пакеты от открытых компьютеров, то, нажав кнопку **Туннель**, задайте требуемое число адресов для туннелирования.

Нажав кнопку **IP-Адреса** в этом окне следует задать все необходимые адреса для серверов.

ВНИМАНИЕ! Для обеспечения установления соединения между узлами сети ViPNet и соединений с внешней сетью без каких-либо ручных настроек ПО ViPNet на самих сетевых узлах, рекомендуем произвести все необходимые настройки СУ в программе ViPNet ЦУС (настройка различных IP-адресов, типов МЭ, опций ViPNet и т.д.).

Для сетевых узлов можно настроить уровень полномочий. Уровень полномочий определяет допустимость различных действий пользователей по изменению настроек в ПО ViPNet на узле. По умолчанию присваивается уровень полномочий, указанный в окне настроек по умолчанию (пункт меню **Службы/Настройки по умолчанию**, см. п.11.4). Изменить уровень полномочий можно для узлов, зарегистрированных в ПЗ **Защита трафика, Деловая почта и КриптоСервис** из окна регистрации в соответствующей задаче при помощи кнопки **Полномочия**. Соответствие уровней полномочий функциональным возможностям программы описано в отдельном документе "[Классификация полномочий](#)".

Подробная информация о регистрации АП и СМ в конкретных прикладных задачах, изменении полномочий и о различных настройках сетевых узлов приведена в разделе **13**.

Шаг 8. Регистрация типов коллективов (ТК) на АП, СМ, сетевых группах

Выполните команду меню **Службы/Регистрация типов коллективов**. Появится диалоговое окно со списком зарегистрированных ТК.

Если в окне настроек по умолчанию задано **Автоматически создавать ТК и пользователя для нового узла**, то после регистрации узла в Адресной администрации здесь уже будет присутствовать коллектив с именем узла.

Для добавления нового ТК нажмите кнопку **Добавить**.

Появится строка ввода. Введите имя ТК и нажмите кнопку **Принять** или клавишу **Enter**. Появится окно со списком всех сетевых объектов сети (сетевых узлов и сетевых групп). Один из этих сетевых объектов надо выбрать в качестве области действия ТК. С помощью мыши или клавиш управления курсором выберите сетевой объект и нажмите кнопку **Принять** или клавишу **Enter**. ТК будет зарегистрирован.

ВНИМАНИЕ! На каждом сетевом узле (АП и СМ) должен быть зарегистрирован хотя бы один тип коллектива. При этом учитывайте, что при регистрации типа коллектива на сетевой группе этот тип коллектива автоматически регистрируется на каждом сетевом узле (АП или СМ) или подгруппе этой группы, и коллективы данного типа на каждом АП из данной сетевой группы получают возможность связываться друг с другом, то есть они все видны в своих справочниках и имеют ключи для конфиденциальной связи между собой.

Имена типов коллективов не должны повторяться.

Шаг 9. Задание связей между коллективами

Связи между коллективами определяются заданием связей между типами коллективов.

Если в окне **Настройки по умолчанию** установлены флажки **Автоматически связывать новый ТК со всеми другими ТК** и **Автоматически создавать ТК и пользователя для нового узла**, то после регистрации узла в Адресной администрации связи нового коллектива будут созданы автоматически (см. п. 11.4).

Для задания связей ТК подведите курсор к его имени и нажмите кнопку **Связи**. Появится окно со списком всех связей этого ТК. Первоначально этот список пуст.

Для добавления связи нажмите кнопку **Добавить**. Появится окно со списком всех ТК. Выберите один или несколько ТК и нажмите кнопку **Принять** или клавишу **Enter**.

Если есть необходимость управления Серверами чужих сетей коллектив, в который входит администратор (то есть зарегистрированный в задаче ЦУС), должен быть связан с коллективами, зарегистрированными на этих СМ.

Если Вы не желаете, чтобы ЦУС был виден в адресных справочниках других узлов своей сети, то коллектив ЦУС не следует связывать с коллективами этих узлов. Независимо от связей для обеспечения возможности управления узлами своей сети, вся необходимая ключевая информация для связи с узлами своей сети будет сформирована автоматически.

Коллективы АП с коллективами своего СМ, а также коллективы СМ, между которыми заданы логические каналы связи в адресной администрации, связывать нет необходимости, так как необходимые ключи для связи этих узлов появятся автоматически.

Если Вы желаете, чтобы абонентский пункт работал с несколькими серверами IP-адресов, то установите связи между соответствующими коллективами.

Шаг 10. Регистрация пользователей

Регистрация пользователя в каких-то коллективах одного или нескольких АП означает, что этот пользователь получает возможность войти в прикладную программу на данных АП и получить доступ к зашифрованной информации этих коллективов.

Напомним, что все пользователи одного коллектива на данном АП имеют одинаковые права доступа к зашифрованным документам, направленным любому пользователю данного коллектива на данном АП.

Если в окне настроек по умолчанию задано **Автоматически создавать ТК и пользователя для нового узла**, то после регистрации узла в Адресной администрации здесь уже будет присутствовать пользователь с именем этого узла.

Выполните команду меню **Службы/Регистрация пользователей**. Появится диалоговое окно со списком зарегистрированных пользователей.

Для добавления нового пользователя нажмите кнопку **Добавить**.

Появится строка ввода имени пользователя. Введите имя пользователя и нажмите кнопку **Принять** или клавишу **Enter**.

Появится окно со списком типов коллективов, в которые входит пользователь.

Для нового пользователя этот список первоначально пуст.

Для включения пользователя в коллектив какого-либо типа нажмите кнопку **Добавить**. Появится окно со списком ТК, зарегистрированных в сети.

Выберите ТК и нажмите кнопку **Принять** или клавишу **Enter**. Если область действия выбранного ТК - сетевая группа, а не отдельный сетевой узел, то появится окно со списком сетевых узлов, на которых зарегистрирован данный пользователь в коллективах данного типа. Для нового пользователя этот список первоначально пуст.

Для добавления сетевого узла нажмите кнопку **Добавить**. Появится окно со списком сетевых узлов, входящих в область действия выбранного ТК. Выберите сетевой узел и пометьте его нажатием клавиш «Пробел» или **Ins**.

Можно зарегистрировать пользователя на нескольких сетевых узлах из области действия ТК.

Аналогичными действиями можно зарегистрировать пользователя в любых других коллективах.

Если Вы желаете уже существующего пользователя зарегистрировать в новом коллективе, подведите курсор к имени пользователя и нажмите кнопку **Изм. ТК**. Появится окно со списком ТК, в которые входит пользователь.

Для включения пользователя в какой-либо ТК нажмите кнопку **Добавить** и проделайте те же действия, что и при регистрации нового пользователя.

ВНИМАНИЕ! На каждом сетевом узле Вашей сети (АП и СМ) в каждом коллективе должен быть зарегистрирован хотя бы один пользователь. Если на каком то сетевом узле ни одного пользователя зарегистрировано не будет, то связей с этим сетевым узлом установлено не будет.

Шаг 11. Установка атрибутов коллектива пользователя

Этот шаг выполняется одновременно с предыдущим при регистрации пользователей в конкретных коллективах.

Для каждого пользователя коллектив, в который он входит, может быть открытым или скрытым, главным или неглавным.

Если коллектив определен как открытый для пользователя, то другие пользователи могут видеть его в этом коллективе в адресных справочниках своих АП.

Если коллектив определен как скрытый для пользователя, то другие пользователи не будут знать, что он входит в этот коллектив, в то же время этот пользователь сможет прочитать любую зашифрованную информацию, адресованную пользователям этого коллектива.

Если пользователь входит в несколько коллективов, то среди них всегда выделяется один коллектив, называемый главным. Новые ключи пользователя отправляются только на тот АП, где зарегистрирован главный для данного пользователя коллектив. На другие АП ключи пользователя переносятся им самостоятельно.

При рассылке новой ключевой информации для действующих пользователей ключи пользователя всегда высылаются на тот АП, где зарегистрирован главный для данного пользователя коллектив. Поэтому внимательно относитесь к регистрации главного коллектива для конкретного пользователя. Для работы на АП пользователя, для которого коллектив, зарегистрированный на этом АП, не является главным, пользователь должен приносить с собой ключи пользователя (каталог Key_Disk) с АП, где зарегистрирован главный для него коллектив.

При регистрации нового пользователя первый коллектив, в который он включается, определяется как главный и открытый для этого пользователя.

Соответствующие ТК и сетевой узел помечаются слева символом “√”. Все остальные коллективы по умолчанию определяются как неглавные и скрытые (помеченные символом “⊗”).

Для того чтобы сделать неглавный коллектив главным, нужно подвести курсор к соответствующему имени ТК и нажать кнопку **Главный**. Выбранный ТК будет сделан главным (символ “√” переместится к этому ТК). Если область действия этого ТК – одиночный сетевой узел, этот узел автоматически будет назначен главным. Если область действия ТК – сетевая группа, главным сетевым узлом будет автоматически назначен первый узел в сетевой группе.

Если в качестве главного выбран ТК, областью действия которого является сетевая группа, можно изменить главный сетевой узел. Для этого подведите курсор к имени главного ТК и нажмите кнопку **Узлы**. Откроется окно со списком сетевых узлов данного ТК. Подведите курсор к имени сетевого узла, который Вы хотите сделать главным и нажмите кнопку **Главный**.

Внимание! Если требуется назначить главным сетевой узел, входящий в область действия неглавного ТК, сначала следует назначить этот ТК главным, а затем изменить главный сетевой узел. В противном случае возникнет ошибка выполнения программы.

Для того чтобы сделать открытый коллектив скрытым и наоборот, надо подвести курсор к соответствующему ТК и нажать кнопку **Открытый**. Если область действия этого ТК - одиночный сетевой узел, то соответствующий коллектив немедленно поменяет атрибут открытости на противоположный. Если область действия этого ТК - сетевая группа, то появится окно со списком сетевых узлов, на которых зарегистрирован данный пользователь в данном ТК. Подведите курсор к имени сетевого узла, для которого Вы хотите поменять атрибут открытости, и нажмите кнопку **Открытый**.

Для каждого коллектива возможно любое сочетание атрибутов “главный” и “открытый”. Однако только один коллектив для пользователя может быть главным.

Шаг 12. Задание адресов рассылки копий

Если у Вас есть необходимость для каких-то пар Отправитель-Получатель указать списки адресов, куда при отправлении почтового сообщения должны независимо от желания отправителя направляться копии сообщений, то выполните команду меню **Службы/Списки рассылки/Списки рассылки копий/По отправителям сообщений**. Появится диалоговое окно со списком отправителей, для которых заданы списки рассылки копий. Первоначально это окно пусто.

Для добавления нового отправителя нажмите кнопку **Добавить**.

Появится окно со списком всех АП Вашей сети.

Выберите один или несколько АП и нажмите кнопку **Принять** или клавишу **Enter**.

Для задания списка получателей, при адресации которым от имени некоторого АП должны формироваться копии в другие адреса, подведите курсор к имени этого АП, нажмите кнопку **Получатели**. Появится окно со списком АП-получателей.

Первоначально это окно пусто. Для добавления нового получателя нажмите кнопку **Добавить**. Появится окно со списком всех возможных АП-получателей.

Выберите один или несколько АП и нажмите кнопку **Принять** или клавишу **Enter**.

Подведите курсор к имени АП-получателя, нажмите кнопку **Добавить**. Появится окно со списком АП - получателей копий сообщений.

Первоначально это окно пусто. Для добавления нового получателя копий сообщений нажмите кнопку **Добавить**. Появится окно со списком всех АП - возможных получателей копий сообщений.

Выберите один или несколько АП и нажмите кнопку **Принять** или клавишу **Enter**.

Информация о необходимости формирования копий сообщений попадет в комплект справочник соответствующего АП.

Если у Вас есть необходимость для каких-то АП указать списки адресов, откуда копии отправленных почтовых сообщений должны независимо от желания отправителя направляться данному АП-получателю, то выполните команду меню **Службы/Списки рассылки/Списки рассылки копий/По получателям копий**. Появится диалоговое окно со списком получателей, для которых заданы списки отправителей сообщений, копии всех сообщений от которых должны отсылаться данному получателю. Первоначально это окно пусто.

Для добавления нового получателя нажмите кнопку **Добавить**.

Появится окно со списком всех АП Вашей сети.

Выберите один или несколько АП и нажмите кнопку **Принять** или клавишу **Enter**.

Для задания списка отправителей, копии всех почтовых писем от которых должны направляться также в адрес некоторого АП, подведите курсор к имени этого АП, нажмите кнопку **Отправители**. Появится окно со списком АП-отправителей.

Первоначально это окно пусто. Для добавления нового отправителя нажмите кнопку **Добавить**. Появится окно со списком всех возможных АП-отправителей.

Выберите один или несколько АП и нажмите кнопку **Принять** или клавишу **Enter**.

Таким образом Вы зададите список получателей копий, а для каждого получателя - список отправителей. Т.е. все почтовые сообщения от этих отправителей будут направляться также в адрес выбранного получателя копий.

Информация о необходимости формирования копий сообщений попадет в комплект справочников соответствующего АП-отправителя.

8.3 Формирование экспорта и получение импорта для первоначального обеспечения межсетевого взаимодействия с другими сетями ViPNet

Шаг 13. Первоначальное формирование Экспорта и получение Импорта

Для организации взаимодействия между различными сетями ViPNet предусмотрены процедуры обмена данными экспорта между ЦУС этих сетей. Экспортированные данные импортируются в ЦУС соответствующей сети.

При экспорте формируется ряд файлов, содержащих данные об экспортированных Вами СУ, коллективах и пользователях, данные об СМ Вашей сети, через который будет осуществляться взаимодействие с другой сетью. Кроме того, в УКЦ формируются и автоматически передаются в

ЦУС для экспорта файлы справочники сертификатов администраторов УКЦ и списки отозванных сертификатов пользователей Вашей сети.

При первичном обмене экспортом необходимо также в соответствии с руководством по УКЦ выработать общие межсетевые мастер-ключи. Далее, сформированные файлы экспорта необходимо передать каким-либо защищенным способом в ЦУС сети, с которой организуется межсетевое взаимодействие. Администратор той сети импортирует файлы экспорта в ЦУС своей сети и передает Вам файлы экспорта своей сети, которые Вам необходимо импортировать в ЦУС.

Формирование первичных данных для экспорта в другую сеть ViPNet осуществляется при выборе пункта меню **Службы/Экспорт**. На экране появится окно со списком сетей, для которых сформирован экспорт. Первоначально этот список пуст. Для добавления новой сети нажмите кнопку **Добавить**. Вам будет предложено ввести номер и наименование сети, для которой Вы хотите сформировать данные для экспорта. При этом будет создан подкаталог \EXPORT*<I>*, где *<I>* - номер сети, для которой формируется экспорт. **Для каждой сети, с которой Вы желаете работать, должен быть обязательно указан ее десятичный номер <I>**, например 5. По этому номеру будет осуществляться автоматический обмен данными с соответствующим ЦУС. Имя сети значения не имеет.

Далее можно действовать двумя способами:

Экспортировать сначала сетевые узлы, указав затем для экспорта ТК, зарегистрированные на них.

Либо экспортировать сначала типы коллективов, указав затем для экспорта СУ, которые входят в область действия данных коллективов.

Если Вы выбрали первый способ, то, установите курсор на добавленную сеть и нажмите кнопку **Узлы**. На экране появится окно экспортируемых СУ. Первоначально этот список пуст. Нажав кнопку **Добавить**, Вы можете добавить СУ из предложенного списка. Если на СУ зарегистрирован только один ТК, то больше никаких действий осуществлять не нужно, ТК экспортируются автоматически. Если на СУ зарегистрировано несколько ТК, то затем, установив курсор на добавленный СУ, нажмите кнопку **ТК** и выберите нужный ТК из предложенного списка. Предложены будут только коллективы, зарегистрированные на данном сетевом узле.

Если Вы выбрали второй способ назначения экспорта, то в окне со списком сетей, выбрав сеть, нажмите кнопку **ТК**, добавьте ТК, а затем нажав кнопку **Узлы**¹, добавьте соответствующие СУ.

После завершения формирования экспорта ТК и СУ в другую сеть Вам необходимо указать, через какой СМ Вашей сети будет осуществляться взаимодействие с данной сетью, т.е. нужно выбрать шлюзовой СМ.

Внимание! Координатор, планируемый для использования в составе ПАК NME-RVPN ViPNet, нельзя выбирать в качестве шлюзового СМ в другую сеть.

Установите курсор на нужную сеть в окне со списком сетей и нажмите кнопку **СМ-шлюз**. На экране появится окно со списком Серверов-маршрутизаторов Вашей сети. Один из них Вы должны выбрать в качестве шлюзового СМ, через который будет осуществляться обмен почтовой и управляющей информацией с выбранной сетью. Выбор осуществляется нажатием клавиши **Enter** или кнопки **Принять**.

Далее, нажав в окне со списком сетей кнопку **Копировать**, скопируйте экспорт данной сети в указанный Вами каталог. По умолчанию программа предлагает скопировать экспорт в каталог \NEW\EXPORT. Все файлы, появившиеся в каталоге, необходимо передать в ЦУС другой сети.

Аналогичные данные, полученные от администраторов ЦУС других сетей, следует поместить в подкаталог \IMPORT\NEW текущего каталога ЦУС.

Об изменениях в импорте программа предупреждает и предлагает обработать импорт сейчас или позднее из окна **Необработанный импорт** (см. п.15.3).

После обработки импорта в списке типов коллективов Вашего ЦУС появятся типы коллективов других сетей, зарегистрированных на СУ, которые должны взаимодействовать с Вашей сетью. В списке пользователей появятся пользователи из других сетей.

¹ Это нужно делать, только в случае, если в область действия ТК входит несколько СУ.

После получения и обработки импорта Вам необходимо в соответствии с разделом 8.2 (Шаг 9) установить необходимые связи импортированных коллективов другой сети с коллективами, которые Вы экспортировали в Вашу сеть.

После формирования экспорта в некоторую сеть и импорта данных из нее, необходимо выбрать пункт меню **Службы/Адресная администрация/Структура сети ViPNet/Межсетевые каналы** головного меню подсистемы.

В открывшемся окне обеспечивается установление логических каналов связи между шлюзовыми СМ Вашей и других сетей ViPNet. Для этого установите курсор на импортированный шлюзовой СМ и нажмите клавишу **Enter**, на экране появится список СМ Вашей сети. Выберите из списка СМ, который Вы выбрали в качестве шлюзового для данной сети, и нажмите клавишу **Enter**. Межсетевой канал между СМ двух сетей будет установлен. Аналогичную процедуру надо выполнить для всех импортированных шлюзовых СМ других сетей.

После того, как межсетевое взаимодействие будет установлено, обмен экспортом и импортом будет осуществляться автоматически по каналам связи сети ViPNet. Более подробно об экспорте и импорте читайте в разделе 15.

8.4 Контроль правильности конфигурации системы

Шаг 14. Контроль правильности конфигурации системы

Программа следит за правильностью конфигурации Вами системы и в случае ошибок сообщит Вам об этом. Вместе с тем некоторые ошибки могут быть выявлены только Вашим дополнительным контролем с использованием информационно-справочных пунктов меню **Службы/Просмотр конфигурации сети** (раздел 18, стр.123) и **Службы/Справочники АП/Просмотр** (раздел 19.2, стр. 126).

Общий контроль правильности конфигурации системы, который выявит возможные ошибки общего характера, можно провести, выбрав пункт меню **Службы/Проверка конфигурации сети**. Такой контроль система всегда проводит при формировании всех справочников (следующий шаг).

8.5 Формирование адресных справочников, маршрутных таблиц, справочников для УКЦ

Шаг 15. Формирование адресных справочников, маршрутных таблиц, справочников для УКЦ

После создания и конфигурирования сети ViPNet, сформируйте набор справочников, необходимый для обеспечения работы ПО ViPNet на СУ – адресные справочники для СУ, маршрутные таблицы для СМ, справочники для создания в УКЦ ключевой информации СУ.

Все необходимые справочники программа сформирует по команде **Службы/Сформировать все справочники** и запишет все новые файлы, появившиеся после последнего выполнения этой команды, в соответствующие подкаталоги APDB, ABN, EXPORT каталога \NEW рабочего каталога ЦУС и подкаталоги обмена с УКЦ.

При первом выполнении команды формирования справочников в эти каталоги будут помещены все файлы.

Данную команду следует всегда выполнять после внесения каких-либо изменений в конфигурацию сети.

Подробнее о формировании справочников читайте в разделе 19.1, стр.126.

8.6 Рекомендации по созданию архивных копий

Вся информация о сетевой структуре (базы данных сетевых узлов и сетевых групп, прикладных задач, коллективов и пользователей) содержится в каталоге DB, а также в каталогах EXPORT и IMPORT.

Для обеспечения возможности отката и для предотвращения потери жизненно важной информации настоятельно рекомендуется сохранять полный архив этих каталогов всегда, когда это предлагает программа.

Подробнее читайте в разделе 20.

9 Типовой порядок действий при переконфигурации сети ViPNet

В настоящем разделе изложен типовой порядок действий администрации сети при внесении в действующую сеть каких-либо изменений: регистрация или исключение СМ, АП, коллективов, пользователей, добавление или исключение связей и т.д.

1. В соответствии с разделами 11, 11.2, 13, 14 настоящего руководства внесите необходимые изменения в адресную или прикладную администрацию сети и убедитесь в их правильности.

ВНИМАНИЕ! Во избежание конфликтов при необходимости удаления АП или СМ из текущей группы предварительно, выбрав пункт меню **Службы/Регистрация пользователей**, следует удалить все записи о включении пользователя в ТК, зарегистрированный на этой группе, на удаляемых АП или СМ.

2. Если Вы организуете межсетевое взаимодействие с другой сетью, выполните действия в соответствии с разделом 15 настоящего руководства.
3. При помощи пунктов меню **Службы/Просмотр конфигурации сети** и **Службы/Справочники АП/Просмотр** в соответствии с разделами 18 и 19.2 убедитесь, что Вы внесли изменения, соответствующие поставленной цели, то есть во всех новых коллективах на всех АП зарегистрированы пользователи, установлены необходимые связи и т.д.
4. Выберите пункт меню **Службы/Сформировать все справочники**. Программа сформирует все абонентские справочники, маршрутные таблицы и справочники для УКЦ. После этого произведет поиск и запись в соответствующие подкаталоги каталога \NEW и в каталог обмена с УКЦ всех новых файлов.
5. Если Вы добавили пользователей на уже существующие СУ, то нужно скопировать справочники для УКЦ для того чтобы создать ключевые дистрибутивы для добавленных пользователей. Для этого выберите пункт меню **Службы/Файлы для оздания ключей в УКЦ/Дистрибутивов** и в соответствии с разделом 19.4.3 скопируйте справочники новых пользователей.
6. В Ключевом центре безопасности сформируйте всю необходимую новую ключевую информацию. Эта информация будет помещена в каталог обмена с УКЦ. Если были созданы новые сетевые узлы, то будут сформированы дистрибутивы ключей для пользователей на этих узлах (файлы *.DST). Эти дистрибутивы, а также пароли надо передать соответствующим пользователям. О формирование ключевой информации в программе УКЦ после изменений в конфигурации сети читайте документацию ViPNet Administrator Удостоверяющий и ключевой центр раздел **Рекомендации по созданию ключевой информации в связи с изменением структуры сети**).
7. Выберите пункт меню **Управление/Отправить измененные файлы/Справочники узлов** и отправьте в соответствии с разделом 21.2.1 справочники и маршрутные таблицы для существующих АП и СМ. Для новых АП и СМ отправку выполняйте после их установки.
8. Выберите пункт меню **Управление/Отправить измененные файлы/Ключи узлов** и **Управление/Отправить измененные файлы/Ключи пользователей** и отправьте в соответствии с разделом 21.2.2 новую ключевую информацию для пользователей существующих АП и СМ. Для новых АП и СМ отправку выполняйте после их установки.
9. Выберите пункт меню **Управление/Отправить измененные файлы/Экспорт** и отправьте в соответствии с разделом 21.2.4 новый Экспорт в другие ЦУС. Для новых только что добавленных сетей используйте кнопку **Копировать** (выбрав пункт меню **Службы/Экспорт**) для перемещения Экспорта в какой-либо каталог и передачи этой информации в соответствующие ЦУС каким-либо защищенным способом.
10. Если Вы хотите отправить на АП или СМ новое программное обеспечение, то выполните действия в соответствии с разделом 21.3.

11. Выберите пункт меню **Управление/Запросы и ответы** (раздел 21.6), проконтролируйте процесс получения новых файлов соответствующими адресатами и отправьте подтверждения необходимости обновления, если это требуется, и Вы их еще не отправляли.

10 Разбиение сети ViPNet на самостоятельные подсети

Если возникла необходимость разбить существующую сеть на отдельные сети, взаимодействующие на межсетевом уровне, то можно проделать следующую процедуру:

Приобрести у ОАО «ИнфоТекС» необходимое количество (N) программ ЦУС на требуемое число АП и СМ, то есть получить N файлов лицензии INFOTECS.REG и INFOTECS.RE.

Создать N копий своего ЦУС.

В каждой из копий войти в программу и удалить ненужные для данной сети, то есть не принадлежащие ей СМ, АП, сетевые группы, типы коллективов и пользователей. Выйти из программы.

Заменить в каждой из копий ЦУС файлы лицензии INFOTECS.REG и INFOTECS.RE на аналогичные файлы для соответствующей сети.

Запустить программу ЦУС и ответить “ДА” на вопросы об изменении номера сети.

Во всех программах в соответствии с разделом **15** сформировать экспорт и выйти из программы.

В каталоге \IMPORT\NEW каждого ЦУС поместить экспорт от всех остальных ЦУС.

В каждой программе ЦУС в соответствии с разделом **14.2** установить необходимые связи. В соответствии с разделом **18** убедиться в правильности конфигурации сети. Выбрать пункт меню **Службы/Архивы баз данных** и создать архив текущей базы данных.

Программы готовы к самостоятельному использованию. К инсталляционному комплекту каждого ЦУС добавьте из каталога \ARC последний архив, который должен быть помещен в аналогичный каталог после инсталляции программы ЦУС на месте. Этот архив после запуска программы должен быть восстановлен при помощи пункта меню **Службы/Архивы баз данных**.

В соответствии с руководством администратора Ключевого центра безопасности следует для модификации ключевой информации сформировать и обменяться межсетевыми ключами.

В каждой из сетей необходимо в соответствии с рекомендациями раздела 9 обновить всем своим АП, СМ и пользователям абонентские справочники, маршрутные таблицы и ключевую информацию.

11 Подсистема адресной администрации сети

11.1 Администрация сетевого уровня

11.1.1 Функциональное назначение

Подсистема адресной администрации решает следующие задачи:

1. Регистрация нового СМ в сети:

 задание (уникального) мнемонического имени (50 символов);

 выделение уникального номера СМ;

 выделение уникального идентификатора СМ.

2. Регистрация нового АП в сети:

- задание (уникального) мнемонического имени (50 символов);
 - подключение к определенному СМ (выделение индивидуального сетевого адреса);
 - выделение уникального идентификатора АП.
3. Регистрация новых сетевых групп (подгрупп) АП:
- задание (уникального) мнемонического имени (50 символов);
 - выделение уникального номера группы (сетевое адреса группы);
 - выделение уникального идентификатора группы.
4. Модификация состава сетевой группы (подгруппы) АП:
- включение в АП в группу;
 - удаление АП из группы.
5. Удаление СМ, АП, групп АП.
6. Добавление/удаление межсерверного канала.
7. Добавление/удаление межсетевого канала.
8. Выдача справочной информации (количество АП, СМ, групп АП, каналов).
9. Формирование для Серверов-маршрутизаторов таблиц маршрутизации.
10. Выдача в текстовый файл содержимого БД подсистемы.
11. Контроль корректности БД подсистемы.

11.1.2 Диалоговая среда подсистемы адресной администрации

Работа с подсистемой адресной администрации производится в диалоговом режиме с использованием оконного интерфейса и системы выпадающих меню. Подсистема вызывается командой меню **Службы/Адресная администрация/Структура сети ViPNet**.

Нижняя строка экрана содержит контекстно-зависимую справочную информацию о некоторых активных клавишах клавиатуры, среди которых всегда присутствуют ключи:

Esc	используется для возврата в предыдущее состояние или меню;
F1	используется для выдачи контекстно-зависимой справки. Текст справки содержит перечень возможных действий и соответствующих ключей клавиатуры в текущем контексте.
Enter	используется при работе с меню для выбора (выполнения) действия, обозначенного в текущем пункте меню.

Предпоследняя строка экрана содержит имя текущей группы АП в виде “Тек. группа: имя” либо “Тек. группа: нет”. Включение АП в группу и удаление из группы производится по отношению к текущей группе.

Запросы для текстового ввода производятся через выпадающее окно запросов. При вводе текста в окне запроса используются стандартные клавиши редактирования. Клавиша **Esc** при работе в окне запросов интерпретируется как отказ от ввода, происходит возврат к предыдущему состоянию. Клавиша **Enter** служит для окончания ввода текста.

Окно запросов используется также для подтверждения предлагаемых действий (запросы типа Да/Нет), например, для подтверждения удаления сетевых объектов.

Для выдачи сообщений используется выпадающее окно сообщений.

Справочное окно подсистемы (в правом верхнем углу экрана) содержит следующую информацию:

номер сети (в заголовке окна);

версия ПО;

количество СМ в сети;

количество АП в сети;

количество межсерверных каналов;

количество сетевых групп АП;

сообщение о необходимости смены маршрутных таблиц, если производились изменения, требующие новой маршрутизации.

Главное меню подсистемы содержит следующие пункты:

Серверы-маршрутизаторы

Межсерверные каналы

Группы АП

Выдать таблицы маршрутизации

Вывод БД в текстовый файл

Межсетевые каналы

Выход

11.1.3 Окно Серверы-маршрутизаторы сети

Вход в данное окно (Рисунок 2) происходит по клавише **Enter** из пункта **Серверы-маршрутизаторы** головного меню подсистемы.

Кн	Г Имя	Номер	АП	МСК	Идент	Сост
	SIA Ip address manager	00001	00002	00012	00010	Вкл
	Сервер_TEST	00029	00002	00001	00287	Вкл
	Центральный СЕРВЕР ДВ рег	00028	00003	00001	00262	Вкл
	WEB-сервер ГНИВЦ ГТК Росс	00025	00002	00001	00260	Вкл
	Центральный СЕРВЕР ИВО ВС	00027	00008	00017	00217	Вкл
	Борзинская таможня_СЕРВЕР	00012	00006	00001	00127	Вкл
	Бурятская таможня_СЕРВЕР	00013	00003	00001	00128	Вкл
	Братская таможня_СЕРВЕР	00014	00006	00001	00129	Вкл
	Тувинская таможня_СЕРВЕР	00015	00004	00001	00130	Вкл

Рисунок 2

Верхняя строка в окне **Серверы-маршрутизаторы** содержит сокращенные названия следующих полей (колонок):

“Кн”

поле отметки для образования канала. Отметки “*->” и “->” в поле “Кн” появляются и исчезают по нажатию **Alt+M** и обозначают два СМ, между которыми канал при нажатии **Alt+C** создается канал. Отметка “*->” сохраняется при нажатии **Alt+M** на строке любого другого СМ, тогда как отметка “->” при нажатии **Alt+M** перемещается на новую позицию. Отметки “Кн” сохраняются только на время сеанса.

“Г”	поле признака (“*”) наличия одного или нескольких АП, входящих в текущую группу, в области данного СМ.
“Имя”	поле имени СМ. При длине имени СМ, превышающем длину данного поля в окне СМ, в окне СМ выводится начало имени, а полностью имя СМ выводится в нижней части окна.
“Номер”	поле сетевого номера СМ.
“АП”	поле, в которое выводится количество АП для каждого СМ. Для любого СМ АП с номером 0 соответствует самому СМ, поэтому значение данного поля всегда больше нуля.
“МСК”	поле, в которое выводится количество межсерверных каналов между данным СМ и другими СМ.
“Идент”	поле идентификатора СМ.
“Сост.”	поле, в которое выводится состояние (Вкл/Выкл) СМ. Этот признак в данной версии не используется.

Активные ключи:

ESC	возврат в головное меню подсистемы.
ENTER	переход в окно со списком АП текущего СМ.
Alt+I	создание нового СМ за текущей позицией в окне СМ. Имя СМ вводится по запросу. Производится контроль уникальности имени, при конфликте выдается сообщение.
Alt+0 (ноль)	создание нового СМ в начальной позиции окна СМ. Имя СМ вводится по запросу. Производится контроль уникальности имени, при конфликте выдается сообщение.
Alt+D	удаление текущего СМ. После подтверждения действия, удаляется текущий СМ и все АП из его области. Все АП из области СМ удаляются из групп АП. Удаляются все каналы между данным СМ и другими СМ.
Alt+E	редактирование имени СМ в окне запросов. Производится контроль уникальности нового имени; при конфликте выдается сообщение и сохраняется прежнее имя.
Alt+M	включение/выключение отметки “Кн”.
Alt+C	образование канала между двумя отмеченными СМ. Если такой канал уже существует-выдается сообщение.
Внимание! Координатор, планируемый для использования в составе ПАК NME-RVPN ViPNet, должен иметь только один межсерверный канал.	
Alt+Z	переход в окно межсерверных каналов данного СМ.
Alt+S	переключение состояния (Вкл/Выкл) текущего СМ.
Alt+F	найти СМ по подстроке имени,
Alt+N	найти следующий СМ по подстроке имени,
F1	вывод текста справки.

11.1.4 Окно АП из области СМ

Вход в данное окно для конкретного СМ производится по клавише **Enter** из окна **Серверы-маршрутизаторы** (Рисунок 3).

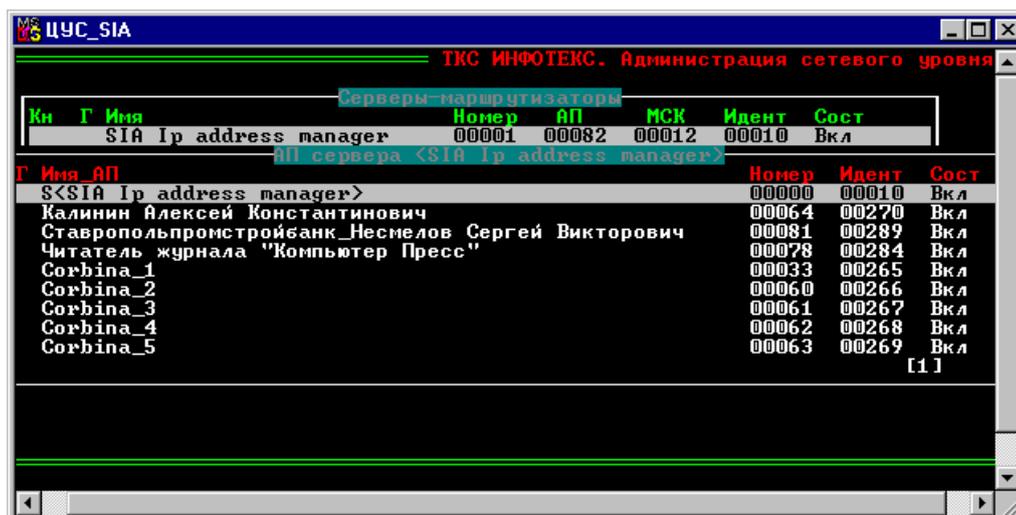


Рисунок 3

Верхняя строка в окне со списком АП содержит сокращенные названия следующих полей (колонок):

“Г”	поле признака (“*”) вхождения АП в текущую группу.
“Имя_АП”	поле имени АП.
“Номер”	поле сетевого номера АП в области СМ.
“Идент”	поле идентификатора АП.
“Сост”	поле, в которое выводится состояние (Вкл/Выкл) АП. Этот признак в настоящей версии не используется.

Активные ключи:

ESC	возврат в окно СМ.
Alt+I	добавление нового АП в конец списка. Имя АП вводится по запросу. Производится контроль уникальности имени, при конфликте выдается сообщение.
Alt+D	удаление текущего АП. После подтверждения действия, удаляется текущий АП. АП удаляется из групп АП.
Alt+E	редактирование имени АП в окне запросов. Производится контроль уникальности нового имени; при конфликте выдается сообщение и сохраняется прежнее имя.
Alt+S	переключение состояния (Вкл/Выкл) текущего АП.
Alt+F	найти АП по подстроке имени.
Alt+N	найти следующий АП по подстроке имени.
Ins	добавление АП к текущей группе, если данный АП не входил в нее. Если текущая группа является подгруппой, то проверяется, что данный АП входит в опорную группу. Если это условие нарушено - выдается сообщение.
Del	удаление АП из текущей группы, если данный АП входит в нее. АП удаляется также из всех вложенных в текущую группу подгрупп.
Home	перейти к первому АП.
F2	перейти к последнему АП.
F1	вывод текста справки.

ВНИМАНИЕ! Во избежание конфликтов при необходимости удаления АП или СМ из текущей группы предварительно, выбрав пункт меню *Службы/Регистрация пользователей*, следует

удалить все записи о включении пользователя в ТК, зарегистрированный на этой группе, на удаляемых АП или СМ.

11.1.5 Окно межсерверных каналов, образованных данным СМ

Вход в данное окно для конкретного СМ происходит по нажатию клавиш **Alt+Z** из окна *Серверы-маршрутизаторы* (Рисунок 4).

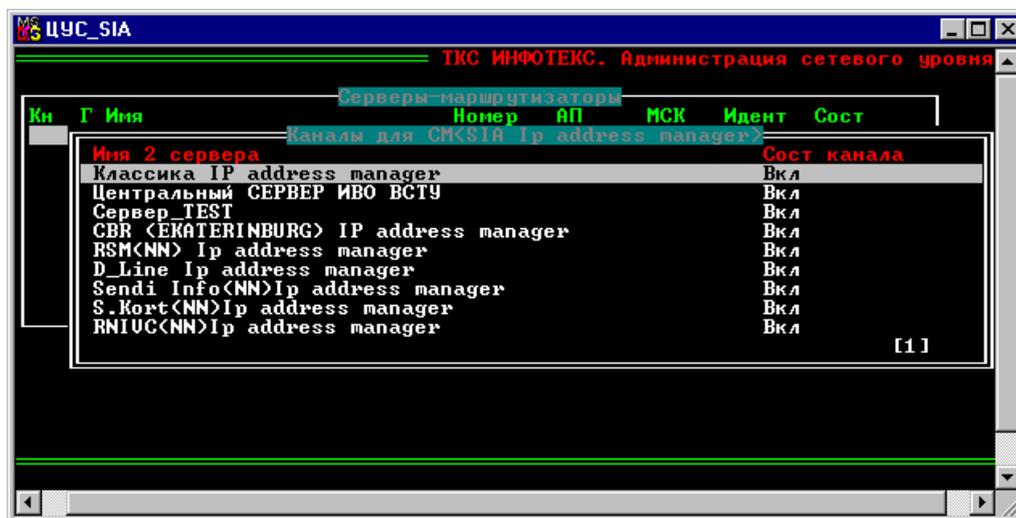


Рисунок 4

Верхняя строка в окне содержит сокращенные названия следующих полей (колонок):

- “Имя 2 Сервера” поле имени второго СМ, образующего канал.
- “Сост канала” поле, в которое выводится состояние (Вкл/Выкл). Этот признак в настоящей версии не используется.

Активные ключи:

- ESC** возврат в головное меню подсистемы.
- Alt+D** удаление канала в текущей позиции окна.
- Alt+S** переключение состояния (Вкл/Выкл) текущего канала.
- Alt+F** найти СМ по подстроке имени.
- Alt+N** найти следующий СМ по подстроке имени.
- F1** вывод текста справки.

11.1.6 Окно всех межсерверных каналов

Вход в окно всех межсерверных каналов происходит по клавише **Enter** из пункта *Межсерверные каналы* головного меню подсистемы (Рисунок 5).

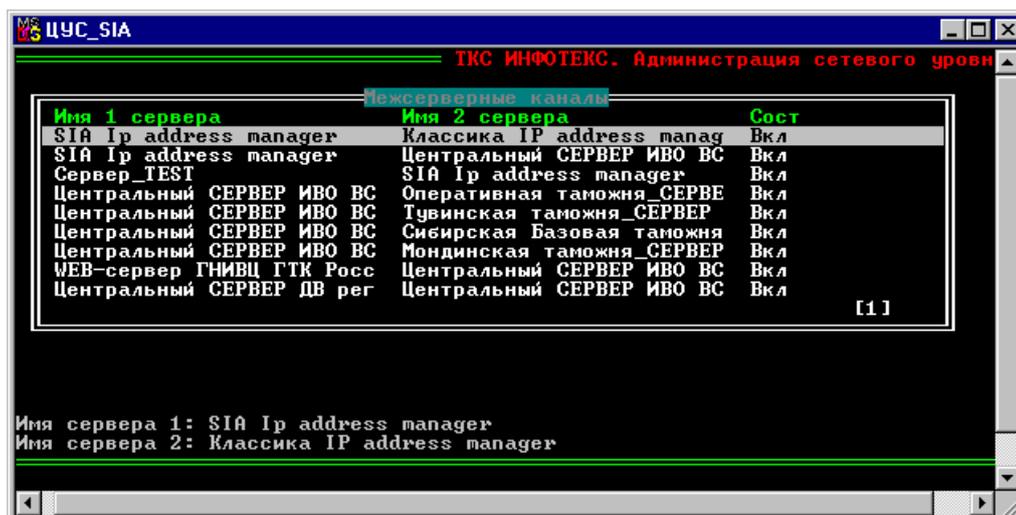


Рисунок 5

Верхняя строка в окне содержит сокращенные названия следующих полей (колонок):

- “Имя 1 Сервера” поле имени первого СМ, образующего канал. Если имя СМ превышает длину поля, то выводится его начало. Полностью имя СМ выводится в нижней части окна.
- “Имя 2 Сервера” поле имени второго СМ, образующего канал. Если имя СМ превышает длину поля, то выводится его начало. Полностью имя СМ выводится в нижней части окна.
- “Сост” поле, в которое выводится состояние (Вкл/Выкл) канала. Этот признак в настоящей версии не используется.

Активные ключи:

- Esc** возврат в головное меню подсистемы.
- Alt+D** удаление канала в текущей позиции окна.
- Alt+S** переключение состояния (Вкл/Выкл) текущего канала.
- Alt+F** найти СМ по подстроке имени.
- Alt+N** найти следующий СМ по подстроке имени.
- F1** вывод текста справки.

11.1.7 Окно групп сетевых узлов, окно подгрупп группы СУ

Вход в окно групп первого уровня происходит по клавише **Enter** из пункта **Группы АП** головного меню подсистемы. Переход в окно подгрупп некоторой группы (подгруппы) производится по клавише **Enter** из соответствующего строки окна групп АП предыдущего уровня (Рисунок 6).

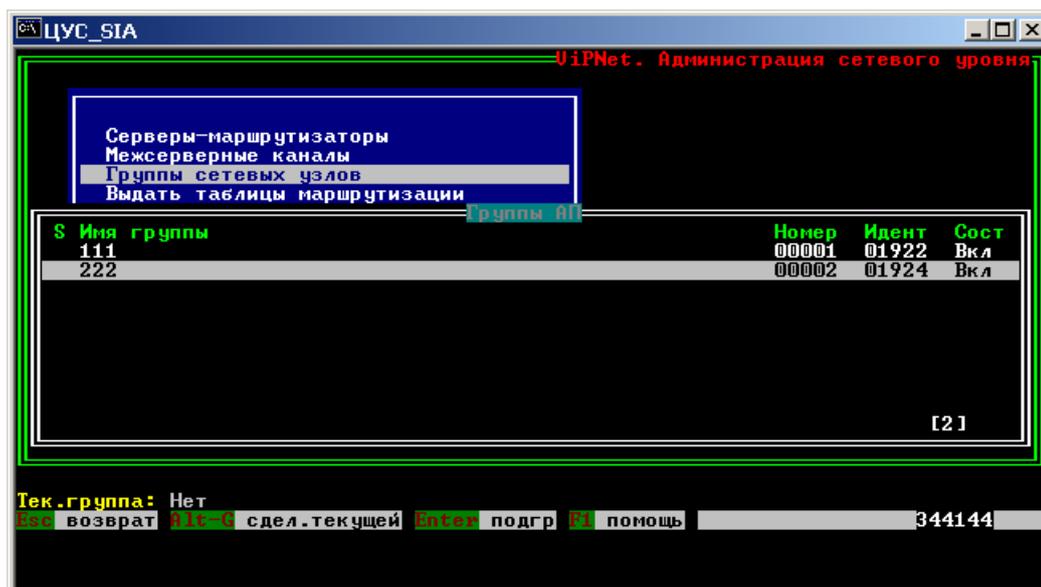


Рисунок 6

Заголовок окна имеет название **Группы AP** при работе с меню групп первого уровня либо **Подгруппы <имя опорной группы>** при работе в меню подгрупп указанной группы.

Верхняя строка в окне содержит сокращенные названия следующих полей (колонок):

- “S” поле отметки (“>”) наличия подгрупп.
- “Имя группы” поле имени группы.
- “Номер” поле сетевого номера группы.
- “Идент” поле идентификатора группы.
- “Сост” поле, в которое выводится состояние (Вкл/Выкл) группы. Этот признак в настоящей версии не используется.

Активные ключи:

- Esc** возврат в предыдущее меню.
- Enter** переход в окно подгрупп текущей группы. Если данная группа не имеет подгрупп, то предлагается ввести имя первой подгруппы. Производится контроль уникальности имени; при конфликте выдается сообщение и переход в окно подгрупп не выполняется.
- Alt+I** создание новой группы за текущей позицией окна. Имя группы вводится по запросу. Производится контроль уникальности имени, при конфликте выдается сообщение.
- Alt+O** создание новой группы в начальной позиции окна. Имя группы вводится по запросу. Производится контроль уникальности имени, при конфликте выдается сообщение.
- Alt+D** удаление группы в текущей позиции окна. После подтверждения действия, удаляется данная группа и все ее подгруппы. Все AP, входившие в состав данной группы и/или ее подгрупп, выводятся из их состава.
- Alt+E** редактирование имени группы в окне запросов. Производится контроль уникальности нового имени; при конфликте выдается сообщение и сохраняется прежнее имя.
- Alt+G** группа в текущей позиции окна объявляется текущей группой, ее имя отображается в предпоследней строке экрана как имя текущей группы.
- Alt+N** отменяется определение текущей группы; предпоследняя строка экрана отображает отсутствие текущей группы.

- Alt+S** переключение состояния (Вкл/Выкл) группы в текущей позиции окна. Этот признак в настоящей версии не используется.
- F1** вывод текста справки.

Существует априорная сетевая группа с именем “Вся сеть” и идентификатором ‘0000’. В эту сетевую группу входят все сетевые объекты сети.

11.1.8 Формирование таблиц маршрутизации

Генерация таблиц маршрутизации для всех СМ производится выбором пункта меню **Выдать таблицы маршрутизации**. В результате в подкаталоге \MAP рабочего каталога ЦУС будут созданы маршрутные таблицы.

Если Вы не обеспечили полной связности между СМ, то есть не существует между какими-либо СМ маршрута для прохождения информации, программа предупредит Вас об этом. Введите необходимые каналы.

Если программа выдала сообщение “*Имеются циклы*”, это означает, что имеется несколько возможных маршрутов между какими-либо СМ. В этом случае информация между этими СМ будет передаваться по кратчайшему маршруту между ними.

11.1.9 Вывод БД в текстовый файл

По клавише **Enter** в позиции **Вывод БД в текстовый файл** производится запрос имени файла выдачи в окне запросов (если файл с данным именем уже есть, запрашивается подтверждение действия), после чего производится вывод в текстовом виде информации, имеющейся в БД ЦУС сети, в указанный файл. Файл помещается в каталог \MAP.

11.1.10 Окно Межсетевые каналы

Вход в окно межсетевых каналов происходит по клавише **Enter** из пункта **Межсетевые каналы** головного меню подсистемы (Рисунок 7).

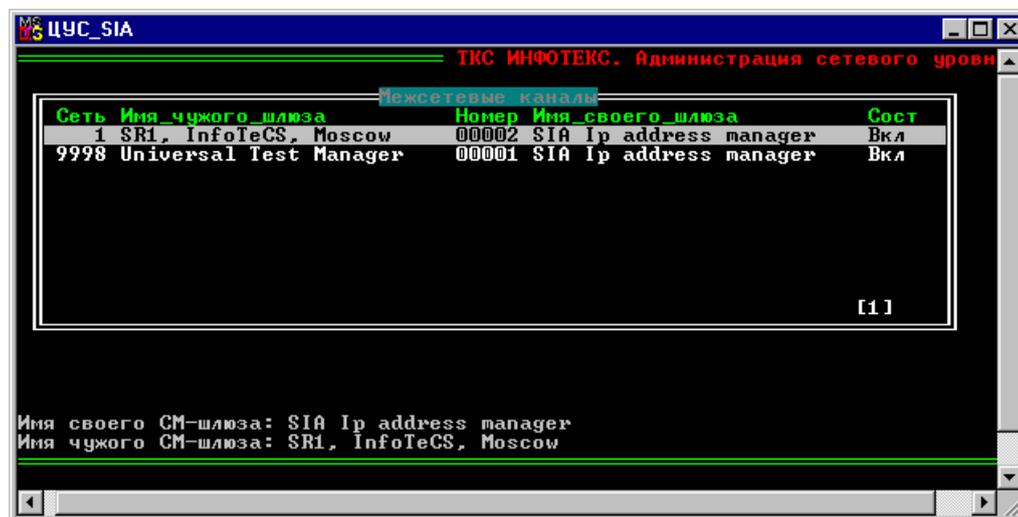


Рисунок 7

В этом окне обеспечивается установление логических каналов связи между шлюзовыми СМ Вашей и других сетей ViPNet. Для этого установите курсор на импортированный шлюзовой СМ и нажмите клавишу **Enter**, на экране появится список СМ Вашей сети. Выберите из списка СМ, который Вы выбрали в качестве шлюзового для данной сети, и нажмите клавишу **Enter**. Межсетевой канал между СМ двух сетей будет установлен. Аналогичную процедуру надо выполнить для всех импортированных шлюзовых СМ других сетей.

Верхняя строка в окне содержит сокращенные названия следующих полей (колонок):

“Сеть”	поле номера другой сети.
“Имя чужого шлюза”	поле имени шлюзового СМ другой сети.
“Номер”	поле сетевого номера шлюзового СМ своей сети.
“Имя своего шлюза”	поле имени шлюзового СМ своей сети.
“Сост”	поле, в которое выводится состояние (Вкл/Выкл) межсетевого канала. Этот признак в настоящей версии не используется.

Активные ключи:

Esc	возврат в предыдущее меню.
Enter	переход в окно выбора шлюзового СМ своей сети для образования канала с другой сетью.
Alt+D	удаление межсетевого канала.
Alt+S	переключение состояния (Вкл/Выкл) текущего канала.
Alt+F	найти СМ по подстроке имени.
Alt+N	найти следующий СМ по подстроке имени.
F1	вывод текста справки.

11.1.11 Выход из подсистемы

Выход из подсистемы производится либо по клавише **Esc** в головном меню подсистемы, либо выбором пункта **Выход** головного меню. Все произведенные во время сеанса изменения сохраняются в БД ЦУС сети. При выходе из подсистемы вырабатывается код возврата и файл изменений для прикладной администрации ЦУС.

11.2 Автоматическая генерация адресной структуры

При необходимости можно автоматически создать одну или несколько подсетей с заданным количеством сетевых узлов, имена которых будут заданы по определенному правилу. Также можно добавить на существующий сервер-маршрутизатор несколько абонентских пунктов, имена которых будут сформированы по заданной маске (см. п. 11.2.1).

Для этого следует воспользоваться пунктом меню **Службы > Адресная администрация > Автоматическая генерация** (Рисунок 8)

Перед началом генерации следует настроить правила для автоматических действий при создании нового сетевого узла, используя пункт меню **Службы > Настройки по умолчанию** (п. 11.4).

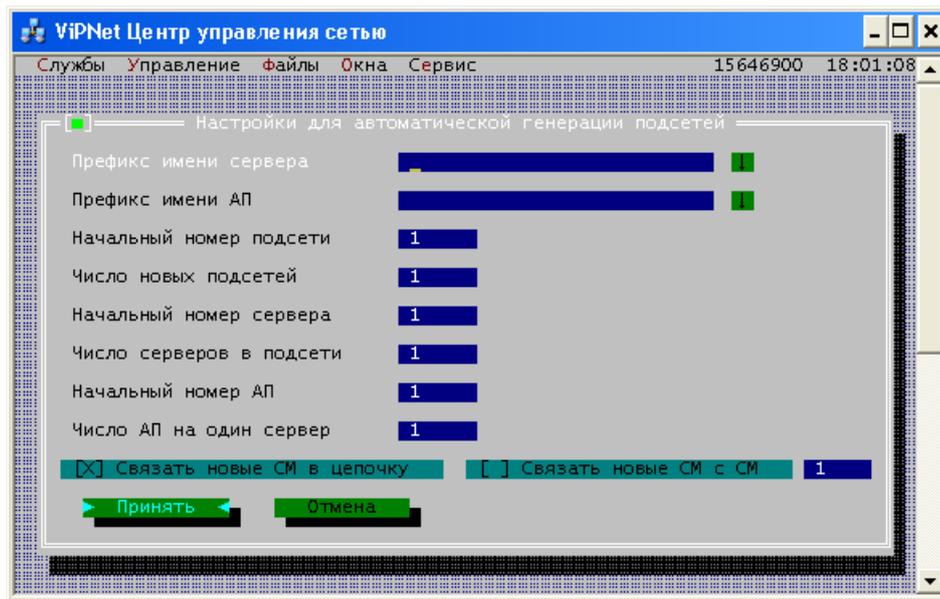


Рисунок 8

Подсеть состоит из заданного количества серверов-маршрутизаторов, на каждом из которых зарегистрировано заданное количество абонентских пунктов. Можно представить подсеть как один из отделов компании.

Для автоматической генерации подсетей задайте следующие параметры:

Префикс имени сервера — сгенерированное имя координатора будет содержать этот префикс и некоторый уникальный номер.

Префикс имени АП — сгенерированное имя АП будет содержать этот префикс и некоторый уникальный номер.

Начальный номер подсети — используется для генерации уникального номера подсети.

Число новых подсетей.

Начальный номер сервера — используется для генерации уникального номера координатора.

Число серверов в подсети. Если задано число серверов в подсети, равное нулю, то генерируются новые АП для СМ с заданным начальным номером.

Начальный номер АП — используется для генерации уникального номера АП.

Число АП на один новый сервер.

Связать новые СМ в цепочку — этот флажок используется для обеспечения межсерверных каналов связи между новыми СМ по цепочке: 1-2, 2-3, 3-4 и т.д., при этом первый из этой цепочки связывается с последним из ранее существующих СМ.

Связать новые СМ с СМ — этот флажок используется для обеспечения межсерверных каналов связи между новыми СМ и СМ, номер которого указан в этом параметре.

При выборе данного способа связывания СМ необходимо в поле справа задать номер координатора, который будет играть роль опорного СМ. Номер опорного СМ можно определить, используя пункт меню **Службы > Адресная администрация > Структура сети ViPNet > Серверы-маршрутизаторы**, номер отображается в колонке **Номер**.

Следует иметь в виду, что координаторы нуждаются в обеспечении межсерверных каналов связи между собой. В сети должен быть путь от любого координатора к каждому другому. Без такой связности будет невозможно создать все необходимые справочники связей. Для создания связей между генерируемыми координаторами используйте флажки **Связать новые СМ в цепочку** и **Связать новые СМ с СМ**. Эти флажки могут быть установлены одновременно.

Замечание: При добавлении нового пользователя по умолчанию устанавливается признак, что данный пользователь имеет право электронной подписи (в файле \DB\defset.txt значение параметра ASIGN=1). Если необходимо, чтобы для новых пользователей не предоставлялось право подписи, установите в файле DB\defset.txt значение параметра ASIGN=0. Это нужно сделать перед автоматической генерацией подсетей.

Укажите необходимые параметры и нажмите кнопку **Принять**, в соответствии с заданными параметрами будут сформированы новые сетевые узлы и межсерверные каналы связи.

Сгенерированное имя Координатора будет выглядеть следующим образом: <КоординаторПрефикс>_<Номер подсети>_<Номер Координатора>.

Сгенерированное имя АП будет выглядеть следующим образом: <АППрефикс>_<Номер подсети>_<Номер Координатора>_<Номер АП>.

11.2.1 Добавление абонентских пунктов с формированием имен по заданной маске

Для группового добавления абонентских пунктов на существующий сервер-маршрутизатор выполните следующие действия:

1. Выберите пункт меню **Службы > Адресная администрация > Автоматическая генерация**.
2. В окне **Настройки для автоматической генерации подсетей** задайте следующие параметры:

В поле **Префикс имени АП** введите маску для формирования имен абонентских пунктов.

Маска имени состоит из произвольной строки и выражения вида $%0Nd$, которое задает формат номера абонентского пункта. Здесь:

- * $%$ — обязательный служебный символ.
- * 0 — указывает, что номер абонентского пункта должен быть дополнен слева нулями до указанного числа знаков (если задано N). Чтобы номер АП был дополнен слева пробелами, опустите символ 0 , то есть введите $%Nd$.
- * N — число знаков в номере абонентского пункта.
- * d — обязательный символ, который указывает, что номер абонентского пункта имеет десятичный формат.

Пример маски имени: *New Client %04d*.

В поле **Начальный номер сервера** введите номер СМ, на который нужно добавить новые абонентские пункты. Номер сервера можно определить с помощью пункта меню **Службы > Адресная администрация > Структура сети ViPNet > Серверы-маршрутизаторы**, номер отображается в колонке **Номер**.

В поле **Число серверов в подсети** введите 0.

В поле **Начальный номер АП** укажите начальный номер для подстановки в маску имени абонентского пункта.

В поле **Число АП** на один сервер задайте количество абонентских пунктов, которые нужно создать.

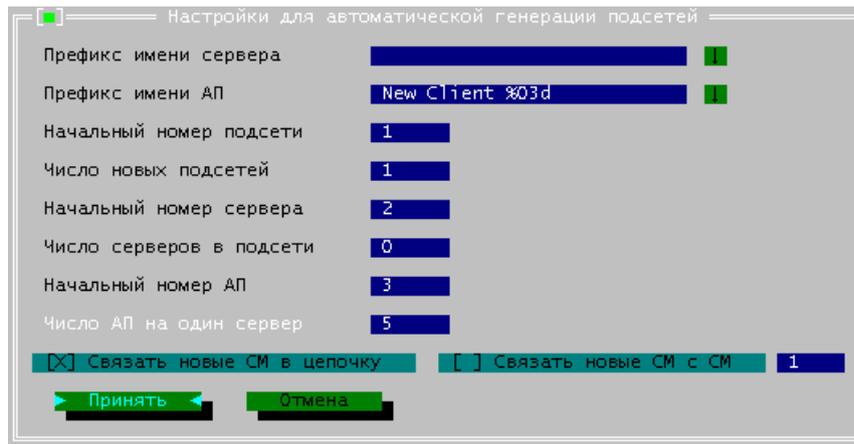


Рисунок 9

3. Нажмите кнопку **Принять**, будут созданы новые абонентские пункты.

Например, если задано добавить 5 абонентских пунктов с начальным номером 3 и маской имени *New Client %03d*, будут созданы абонентские пункты с именами *New Client 003*, *New Client 004* и так далее.

11.3 Задание адресов сетевых узлов сети ViPNet при работе через внешние сети

Вы можете задать IP-адреса сетевых узлов сети ViPNet, а также их SMTP-адреса. Заданные Вами адреса попадут в адресные справочники.

Всегда достаточно задать адреса только СМ.

Если узлы сети зарегистрированы в задачах **Защита трафика** или **Сервер IP-адресов**, то в этом окне в поле IP адреса задавать не нужно. Они автоматически попадут сюда при задании адреса в окне регистрации узла в задаче **Защита трафика** или **Сервер IP-адресов**.

Для задания таких адресов следует выбрать пункт меню **Службы/Адресная администрация/Адреса во внешних сетях**. Появится диалоговое окно со списком всех узлов своей сети (Рисунок 10).

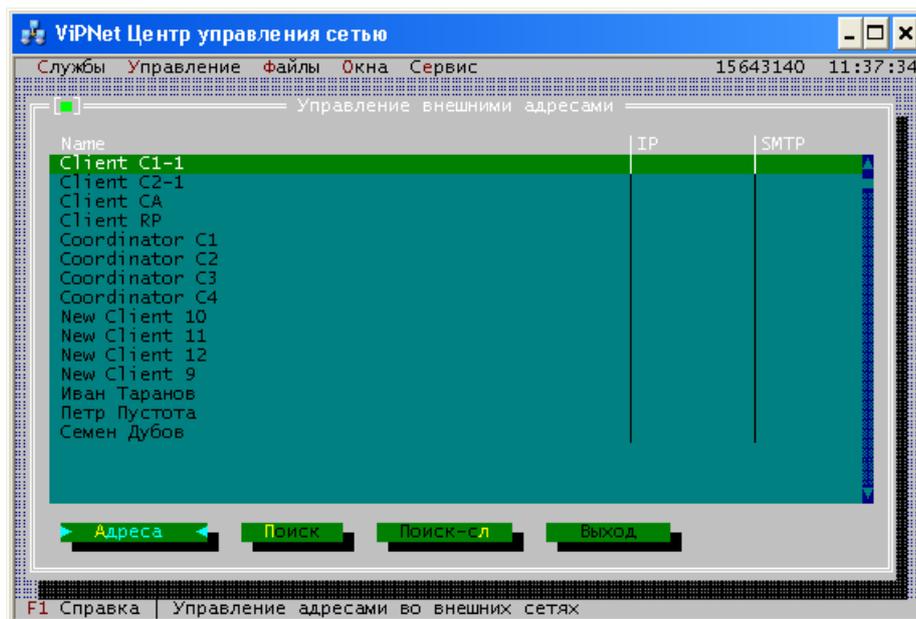


Рисунок 10

Установив курсор с помощью мыши или клавиш управления курсором на нужный сетевой объект, нажмите кнопку **Адреса**. Появится окно (Рисунок 11), в котором Вы можете настроить адреса для выбранного сетевого узла в соответствующей почтовой системе.

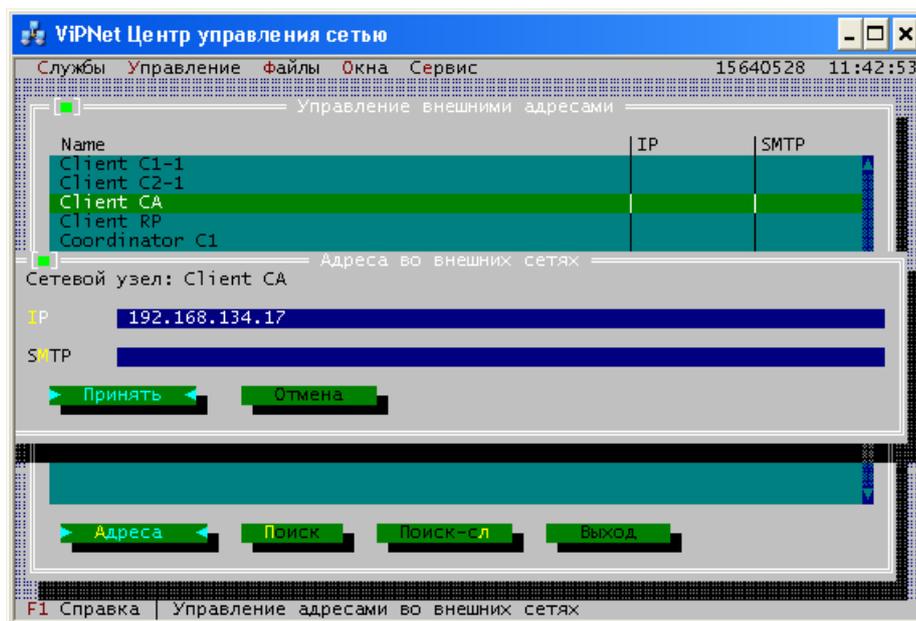


Рисунок 11

Введя адреса сетевого узла в соответствующих почтовых сетях, нажмите кнопку **Принять**. Несколько IP-адресов вводятся через «;». Заданные Вами адреса будут занесены в рассылаемый справочник.

11.4 Групповые операции с узлами

Групповые операции с сетевыми узлами включают:

создание сетевых узлов;

удаление абонентских пунктов;

изменение имен абонентских пунктов и перенос абонентских пунктов между серверами.

Необходимые параметры для выполнения групповых операций задаются с помощью внешних файлов auto.gen, auto.del, auto.upd.

11.4.1 Создание сетевых узлов

С помощью групповой операции можно создать новые серверы-маршрутизаторы и межсерверные каналы между ними, а также абонентские пункты на новых или существующих серверах-маршрутизаторах.

Для регистрации новых сетевых узлов выполните следующие действия:

1. Создайте текстовый файл с именем auto.gen.
2. Внесите в файл информацию о сетевых узлах, которые требуется создать, и сохраните файл. Формат файла auto.gen описан ниже.

Внимание! Если файл содержит кириллические символы, он должен быть сохранен в кодировке DOS.

3. Поместите созданный файл в папку \NCC (рабочая папка ЦУС).
4. В Центре управления сетью выберите пункты меню **Службы > Адресная администрация > Групповая регистрация узлов**.

5. На вопрос о сохранении архива базы данных и об обработке файла auto.gen ответьте **Да**.
Будут созданы заданные сетевые узлы.

Файл auto.gen имеет следующий формат:

```
S:<пробел><имя нового сервера 1>
A:<пробел><имя АП 1 на сервере 1>
A:<пробел><имя АП 2 на сервере 1>
.....
S: <пробел><имя нового сервера N>
A:<пробел><имя АП 1 на сервере N>
A:<пробел><имя АП 2 на сервере N>
.....
C:
G:
V:<пробел><номер опорного СМ>
N:<пробел><номер существующего сервера X>
A:<пробел><имя АП 1 на сервере X>
A:<пробел><имя АП 2 на сервере X>
.....
N:<пробел><номер существующего сервера Z>
A:<пробел><имя АП 1 на сервере Z>
A:<пробел><имя АП 2 на сервере Z>
```

Строки файла auto.gen имеют следующее значение:

S: — создать новый сервер-маршрутизатор.

N: — указать существующий сервер-маршрутизатор для создания абонентских пунктов.

A: — создать абонентский пункт на указанном новом или существующем сервере-маршрутизаторе.

Внимание! При задании имен следует учитывать, что длина имени не должна превышать 50 символов. Иначе имя будет обрезано.

Для создания межсерверных каналов следует использовать одну из следующих строк:

C: — связать новые серверы каналами в цепочку.

G: — связать все новые серверы каналами друг с другом.

V: — связать новые серверы с заданным опорным СМ. Заданный в строке V: опорный СМ должен быть предварительно зарегистрирован в ЦУС. Номер сервера можно найти в окне **ViPNet. Администрация сетевого уровня > Серверы-маршрутизаторы**.

11.4.2 Удаление абонентских пунктов

Для группового удаления абонентских пунктов выполните следующие действия:

1. Создайте текстовый файл с именем auto.del.
2. Внесите в файл имена абонентских пунктов, которые требуется удалить, и сохраните файл. Формат файла auto.del описан ниже.
Внимание! Если файл содержит кириллические символы, он должен быть сохранен в кодировке DOS.
3. Поместите созданный файл в папку \NCC (рабочая папка ЦУС).
4. В Центре управления сетью выберите пункты меню **Службы > Адресная администрация > Групповое удаление АП.**
5. На вопрос о сохранении архива базы данных и об обработке файла auto.del ответьте **Да**. Заданные абонентские пункты будут удалены.

В файл auto.del следует записывать имена абонентских пунктов для удаления, каждое имя в отдельной строке:

```
<имя абонентского пункта 1>  
<имя абонентского пункта 2>  
.....  
<имя абонентского пункта N>
```

11.4.3 Изменение свойств абонентских пунктов

С помощью групповой операции можно удалить или переименовать абонентские пункты, а также перенести абонентские пункты на другие серверы-маршрутизаторы.

Для группового изменения свойств абонентских пунктов выполните следующие действия:

1. Создайте текстовый файл с именем auto.upd.
2. Внесите в файл информацию об абонентских пунктах, которые требуется переименовать, перенести или удалить, и сохраните файл. Формат файла auto.upd описан ниже.
Внимание! Если файл содержит кириллические символы, он должен быть сохранен в кодировке DOS.
3. Поместите созданный файл в папку \NCC (рабочая папка ЦУС).
4. В Центре управления сетью выберите пункты меню **Службы > Адресная администрация > Групповое обновление АП.**
5. На вопрос о сохранении архива базы данных и об обработке файла auto.upd ответьте **Да**. Будут выполнены заданные действия.

Файл auto.upd имеет следующий формат:

```
U:<пробел><десятичный идентификатор АП><пробел><новое имя АП>  
U:<пробел><десятичный идентификатор АП><пробел><новое имя АП>  
.....  
M:<пробел><десятичный идентификатор АП><пробел><номер сервера>  
M:<пробел><десятичный идентификатор АП><пробел><номер сервера>  
.....  
D:<пробел><десятичный идентификатор АП для удаления>  
D:<пробел><десятичный идентификатор АП для удаления>
```

.....

Строки файла auto.gen имеют следующее значение:

U: — изменить имя абонентского пункта.

M: — перенести абонентский пункт на указанный сервер.

D: — удалить абонентский пункт.

Идентификатор абонентского пункта можно найти в окне **ViPNet. Администрация сетевого уровня > АП сервера <имя сервера>**. Идентификатор следует указывать в пятизначном формате или дополнить до пяти символов пробелами справа.

Номер сервера можно найти в окне **ViPNet. Администрация сетевого уровня > Серверы-маршрутизаторы**.

11.5 Перенос абонентских пунктов на другой сервер-маршрутизатор

При управлении защищенной сетью ViPNet может возникнуть необходимость переноса абонентских пунктов с одного сервера-маршрутизатора на другой.

Чтобы абонентский пункт начал работу с новым сервером-маршрутизатором, нужно отправить на абонентский пункт обновление справочников и ключей. Доставку справочников и ключей обеспечивает сервер-маршрутизатор, однако сначала абонентский пункт не может принимать обновления от своего нового сервера. Поэтому в течение некоторого времени после переноса требуется отправлять все обновления на абонентский пункт по старому адресу, то есть через старый сервер-маршрутизатор.

Период использования старого адреса можно задать в окне **Настройки по умолчанию** (см. п. 12). Если в течение заданного периода использования старого адреса от перенесенного абонентского пункта будут получены конверты, отправленные с нового адреса, данный абонентский пункт будет удален из списка перенесенных АП. Все последующие обновления будут отправляться по новому адресу абонентского пункта.

Для переноса абонентских пунктов на другой сервер-маршрутизатор выполните следующие действия:

1. Выберите пункт меню **Службы > Адресная администрация > Перенос АП на другой СМ**.
2. В окне **Выберите новый координатор для АП** укажите координатор, на который требуется перенести абонентские пункты, и нажмите кнопку **Принять**.

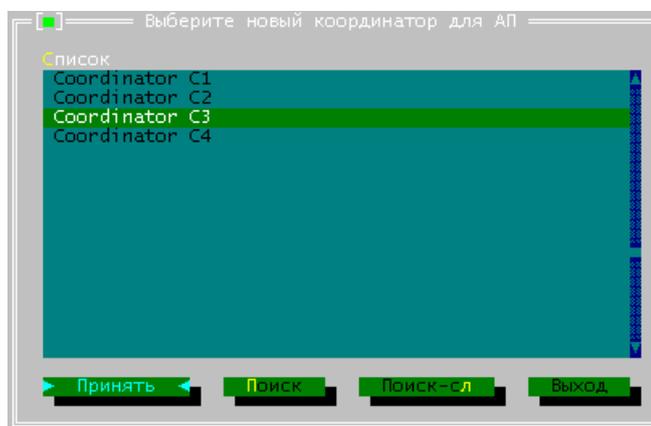


Рисунок 12

3. В окне **Составьте список АП для переноса** нажмите кнопку **Добавить**.

4. В окне **Выберите АП** укажите один или несколько абонентских пунктов, затем нажмите кнопку **Принять**. Для выделения абонентских пунктов используйте клавишу «пробел».
5. Добавив в список нужные абонентские пункты, в окне **Составьте список АП для переноса** нажмите кнопку **Перенести**.

Выбранные абонентские пункты будут перенесены на указанный ранее сервер-маршрутизатор.

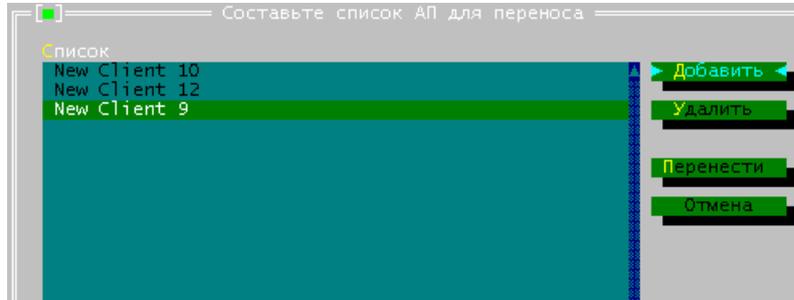


Рисунок 13

6. Сформируйте справочники, затем в программе ViPNet Удостоверяющий и ключевой центр создайте новые ключи для сетевых узлов, участвующих в изменении структуры сети. Перенесите созданные ключи в ЦУС.
7. Отправьте новые справочники и ключи одновременно на все сетевые узлы, участвующие в изменении структуры сети (см п. 21.2). Не рекомендуется отправлять обновления только для серверов-маршрутизаторов или только для перенесенных абонентских пунктов. При отправке обновлений обязательно укажите отложенное время вступления изменений в действие.

Внимание! Если требуется, чтобы изменения вступили в действия как можно раньше, отправьте немедленное обновление на серверы-маршрутизаторы, а обновление ключей на перенесенных абонентских пунктах выполните с помощью дистрибутивов ключей.

11.6 Восстановление базы данных сетевых узлов

Если при выборе пункта меню **Службы > Адресная администрация > Структура сети ViPNet** появляется сообщение «СБОЙ АРХИВА ИЛИ ОШИБКА СИСТЕМЫ», для восстановления базы данных сетевых узлов выполните следующие действия:

1. Выберите пункт меню **Службы > Адресная администрация > Восстановление базы данных узлов**.
2. В окне сообщения о восстановлении базы данных выберите **Да**. База данных будет восстановлена на основании текущих данных. Успех данной операции не гарантирован и зависит от того, насколько сильно была испорчена база данных. Если результат восстановления вас не устраивает, то рекомендуется восстановить одно из предыдущих стабильных состояний базы данных из архива.

12 Настройки по умолчанию

Это окно предназначено для автоматизации регистрационных действий в программе ЦУС (Рисунок 14).

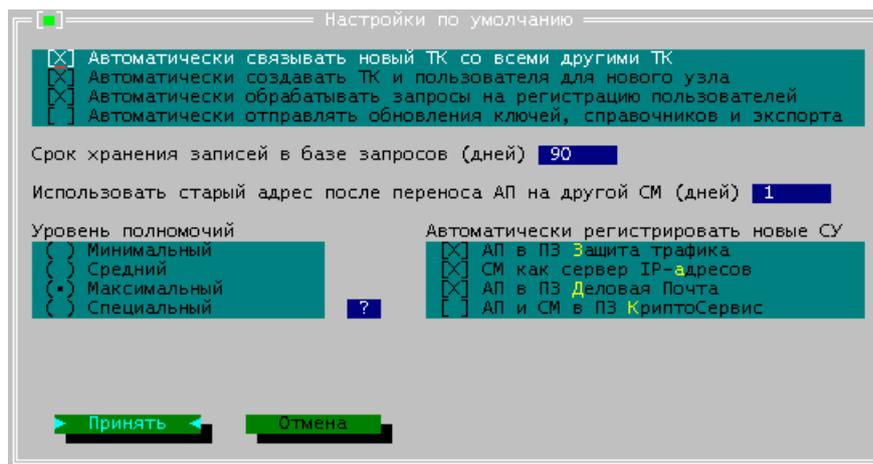


Рисунок 14

Это окно появляется при первом запуске ЦУС после инсталляции. В дальнейшем его можно открыть по команде меню **Службы/Настройки по умолчанию**.

В этом окне можно настроить правила для некоторых автоматических действий при создании нового сетевого узла:

Автоматическое установление связей вновь создаваемых коллективов со всеми существующими (подробнее см. ниже в этом разделе). По умолчанию опция выключена.

Автоматическое создание коллектива и пользователя при создании нового узла с именем этого узла. По умолчанию опция включена.

Автоматическую регистрацию вновь созданных СУ в нужных прикладных задачах. Список прикладных задач зависит от лицензии.

Установку уровня полномочий узла. По умолчанию установлен средний уровень полномочий.

Автоматическая обработка запросов на регистрацию пользователей из программы Центр Регистрации (подробнее см. ниже в этом разделе).

Автоматическая отправка обновления ключей, справочников и экспорта (подробнее см. ниже в этом разделе).

Также в этом окне можно задать следующие параметры:

Срок хранения записей в базе запросов — все записи, хранящиеся в базе дольше заданного срока, будут удаляться. По умолчанию установлено значение 90 дней. Базу запросов можно просмотреть, используя пункт меню **Управление -> Запросы и ответы** (п. 21.6).

Использовать старый адрес после переноса АП на другой СМ — период времени (в днях) после переноса, в течение которого обновления будут отправляться на абонентский пункт через старый сервер-маршрутизатор (см. п. 11.5). Допустимые значения параметра — от 1 до 30 дней.

Скажем несколько слов об опции **Автоматически связывать новый ТК со всеми другими ТК**. Данная опция по умолчанию отключена, так как наличие флажка в данной опции может привести к чрезмерному количеству связей. Мы настоятельно не рекомендуем использовать эту опцию в большой сети (с многими сотнями сетевых узлов). Вряд ли можно представить, что каждый узел в большой сети действительно должен быть связан со всеми другими. Если это будет сделано, тогда каждый клиент столкнется с очень длинным (и едва управляемым) списком доступных получателей. Помимо этого, значительно увеличится сетевой трафик, так как каждый раз при изменении структуры сети ViPNet (сетевые узлы могут добавляться, перемещаться и так далее)

десятки или сотни мегабайтов ключей узлов и справочников будут отправлены во все точки сети. Рекомендуется включать эту опцию только в маленьких сетях (с числом сетевых узлов, не превышающих нескольких десятков). Число связей ТК может быть ограничено файлом лицензии.

В зависимости от способа создания типа коллектива и настроек ЦУС, данная опция может обрабатываться по-разному:

Если в окне **Настройки по умолчанию** включена опция **Автоматически связывать новый ТК со всеми другими ТК** и в файле \DB\defset.txt указан параметр LNUGA=0 (по умолчанию):

- * Если новый ТК создан вручную, тогда он будет связан со всеми другими ранее созданными ТК. При этом программа выдаст предупреждение, и администратор сможет решить, требуется ли выполнять автоматическое связывание в каждом определенном случае.
- * Если новый ТК создан в процессе автоматической генерации сетевых узлов, то в пределах каждой создаваемой подсети все новые ТК будут связаны друг с другом. Подробнее см. в п. **Автоматическая генерация** (п.11.2).
- * Если несколько новых ТК были автоматически созданы после ручного добавления сетевых узлов в одном сеансе работы Адресной администрации (см. опцию **Автоматически создавать ТК и пользователя для нового узла**), то эти ТК будут связаны друг с другом и только друг с другом.

Если в окне **Настройки по умолчанию** включена опция **Автоматически связывать новый ТК со всеми другими ТК** и в файле \DB\defset.txt указан параметр LNUGA=1, то новый ТК будет автоматически связан со всеми существующими ТК.

Опция **Автоматически обрабатывать запросы на регистрацию пользователей** по умолчанию выключена. Это означает, что все новые запросы из Центра регистрации программа ЦУС будет сохранять в специальной папке, которая будет сканироваться каждые 2 секунды. Эти запросы можно просмотреть и обработать в специальном окне, которое можно открыть из пункта меню **Службы/Обработка запросов на регистрацию** (подробнее см. п. 16). При включении опции все запросы на регистрацию пользователя, поступающие из Центра регистрации, будут обрабатываться автоматически.

Опция **Автоматически отправлять обновления ключей, справочников и экспорта** по умолчанию выключена. При ее включении ЦУС раз в 1 минуту проверяет, есть ли обновления ключей узлов. Если обновления есть, то ЦУС автоматически формирует конверты для ВСЕХ имеющихся в данный момент обновлений: ключей узлов, ключей пользователей, справочников и экспорта. При этом задается текущее время обновления, и сразу отправляются подтверждения.

13 Регистрация АП и СМ в прикладных задачах

Регистрация абонентских пунктов и координаторов (СМ) в конкретных прикладных задачах является обязательной процедурой в процессе генерации сети. Эта процедура определяет, какие прикладные программы ViPNet могут быть установлены на том или ином сетевом узле.

Если в настройках по умолчанию (см. п. 11.4) задана регистрация в каких-либо задачах, то при создании нового АП или координатора такая регистрация произведется автоматически.

Возможность регистрации нужного числа узлов в конкретных задачах определяется файлом лицензии, предоставляемым ОАО «ИнфоТекС» при поставке ЦУС.

ВНИМАНИЕ! Если какой-либо СУ не будет зарегистрирован ни в одной прикладной задаче, то он не появится в абонентских справочниках.

При регистрации в ПЗ по умолчанию присваивается уровень полномочий, указанный в окне настроек по умолчанию (пункт меню **Службы/Настройки по умолчанию**, см. п.11.4)). Уровень полномочий определяет допустимость различных действий пользователей по изменению настроек в ПО ViPNet на узле. Изменить уровень полномочий можно для узлов, зарегистрированных в ПЗ **Защита трафика, Деловая почта и КриптоСервис**. Соответствие уровней полномочий

функциональным возможностям программы описано в отдельном документе "[Классификация полномочий](#)".

В разделе 13.1 приведен полный список задач, поддерживаемых ЦУС.

В разделе 13.2 даны рекомендации по регистрации СУ в различных ПЗ.

Внимание! Если сетевые узлы зарегистрированы в ПЗ *ViPNet SDK*, *КриптоСервис* или *Криптофайл*, то для них должно выполняться следующее условие: каждый пользователь должен быть зарегистрирован только в одном единственном типе коллектива, областью действия которого является один единственный сетевой узел.

Помимо регистрации в прикладных задачах (ПЗ) Вы можете производить различные настройки СУ – настраивать IP-адреса, полномочия, туннелируемые адреса (только для координаторов) и др.

Для регистрации СУ (АП и координаторов) в ПЗ, а также для настройки различных параметров СУ, используйте пункт главного меню **Групповая регистрация узлов в задачах** (см. раздел 13.4).

Для регистрации АП в ПЗ используйте пункт главного меню **Службы/ Индивидуальная регистрация АП в задачах** (см. раздел 13.3). В этом меню Вы не сможете задать никаких настроек АП.

Для обеспечения установления соединения между узлами сети ViPNet и соединений с внешней сетью без каких-либо ручных настроек ПО ViPNet на самих сетевых узлах, рекомендуем произвести все необходимые настройки для координатора и при необходимости для АП в программе ViPNet ЦУС (настройка различных IP-адресов, типов МЭ, опций ViPNet и т.д.). Рекомендации по таким настройкам приведены в разделе 13.5.

13.1 Список прикладных задач для регистрации СУ

В настоящей версии ПО ЦУС возможна регистрация АП и СМ в следующих прикладных задачах (Таблица 1):

Таблица 1

№ п/п	Название ПЗ	Идентификатор ПЗ	Тип СУ (АП и/или СМ)	Примечание
1.	Деловая почта	0000 и 0015	только АП	На СУ, зарегистрированных в этой задаче, будет работать программа ViPNet Client Деловая почта. Для каждого из зарегистрированных СУ можно задать уровень полномочий: минимальный, средний, максимальный или специальный
2.	Центр управления сетью	0004	только АП	Только один АП в локальной сети может быть зарегистрирован в этой прикладной задаче. Для осуществления функций управления сетью и обеспечения взаимодействия ЦУС разных сетей не забудьте зарегистрировать какой-либо АП в этой задаче.
3.	Ключевой центр	0008	только АП	Только один АП в локальной сети может быть зарегистрирован в этой прикладной задаче. Для осуществления функций управления сетью и обеспечения взаимодействия ключевых центров разных сетей не забудьте зарегистрировать какой-либо АП в этой задаче.

№ п/п	Название ПЗ	Идентификатор ПЗ	Тип СУ (АП и/или СМ)	Примечание
4.	Защита трафика	0017	АП или СМ	<p>На АП, зарегистрированных в этой задаче, будет работать программа ViPNet Монитор.</p> <p>Регистрация СМ в этой задаче требуется только для возможности изменять уровень полномочий.</p> <p>При регистрации СУ в задаче защиты IP-трафика есть возможность ввести несколько IP-адресов для каждого из зарегистрированных СУ, а также настроить дополнительные специальные параметры, позволяющие автоматически настроить узлы для их работы в сети.</p> <p>Кроме того, можно задать для каждого из зарегистрированных СУ уровень полномочий при защите IP-трафика: минимальный, средний, максимальный или специальный.</p>
5.	Сервер IP-адресов	001A	только СМ	<p>На СМ, зарегистрированных в этой задаче, будет работать программа ViPNet Coordinator Монитор и осуществляться функции Сервера IP-адресов и Сервера ViPNet Firewall.</p> <p>При регистрации СМ в этой задаче есть возможность задать несколько IP-адресов для каждого из зарегистрированных СМ, а также настроить дополнительные специальные параметры, позволяющие автоматически настроить узлы для их работы в сети.</p> <p>Настройки полномочий для координатора производятся в задаче Защита трафика, после предварительной регистрации его в этой задаче.</p> <p>Для каждого сервера можно задать число туннелируемых адресов. Суммарное число адресов не может превосходить число, заданное в лицензии.</p>
6.	Сервер Открытого Интернета	001С	только СМ	<p>Для осуществления функций Сервера Открытого Интернета зарегистрируйте СМ в этой задаче.</p> <p>В этой задаче может быть зарегистрирован только СМ, зарегистрированный в одной из задач: Сервер IP-адресов, Coordinator HW1000, Coordinator HW2000 или Coordinator HW-VPNМ.</p>
7.	Секретный диск	001E	АП или СМ	<p>На СУ, зарегистрированных в этой задаче, будет работать программа SafeDisk, интегрированная с ViPNet.</p>
8.	Центр регистрации	001D	только АП	<p>На АП, зарегистрированных в этой задаче, будет работать программа ViPNet Центр регистрации. Для каждого ЦР можно задать ограничения на количество запросов на дистрибутивы и запросов на сертификаты.</p>

№ п/п	Название ПЗ	Идентификатор ПЗ	Тип СУ (АП и/или СМ)	Примечание
9.	Центр управления политиками	000С	только АП	<p>На АП, зарегистрированных в этой задаче, будет работать программа ViPNet Policy Manager. Для каждого Центра управления политиками безопасности (ЦУПБ) можно задать список управляемых узлов (домен).</p> <p>ЦУПБ может находиться на том же АП, что и ЦУС.</p> <p>АП нельзя регистрировать в этой задаче, если он входит в домен какого-либо ЦУПБ.</p>
10.	КриптоСервис	0020	АП или СМ	<p>На СУ, зарегистрированных в этой задаче, будет работать программа ViPNet CryptoService, а также можно будет работать с набором криптофункций на базе криптопровайдера Домен К – ViPNet SDK. Можно задать для каждого из зарегистрированных СУ уровень полномочий: минимальный, средний, максимальный или специальный.</p>
11.	ViPNet SDK	0029	АП или СМ	<p>На СУ, зарегистрированных в этой задаче, можно будет работать с набором криптофункций на базе криптопровайдера Домен К – ViPNet SDK.</p>
12.	ViPNet Failover	0025	только СМ	<p>На СМ, зарегистрированных в этой задаче, будет работать функционал резервирования серверов Linux.</p> <p>Эту задачу можно регистрировать только для СМ, уже зарегистрированных в задачах Сервер IP-адресов, Coordinator HW1000, Coordinator HW2000 или Coordinator HW-VPNМ.</p>
13.	Терминал Навигатор	002E	только АП	<p>На АП, зарегистрированном в этой задаче, будет работать ПО ViPNet Клиент Монитор для терминала Навигатор АСУ «Экспресс-3» со специализированными для этой задачи настройками. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика.</p>
14.	Терминал Спектр	002F	только АП	<p>На АП, зарегистрированном в этой задаче, будет работать ПО ViPNet Linux для терминала Спектр АСУ «Экспресс-3» со специализированными для этой задачи настройками. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется.</p> <p>Для АП существует возможность задать резервный сервер IP-адресов.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика.</p>

№ п/п	Название ПЗ	Идентификатор ПЗ	Тип СУ (АП и/или СМ)	Примечание
15.	Терминал Ареал-Сервис	0030	только АП	<p>На АП, зарегистрированном в этой задаче, будет работать ПО ViPNet Linux для терминала Ареал-Сервис АСУ «Экспресс-3» со специализированными для этой задачи настройками. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется.</p> <p>Для АП существует возможность задать резервный сервер IP-адресов.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика.</p>
16.	ИСУ Магистраль	0031	только АП	<p>На АП, зарегистрированном в этой задаче, будет работать ПО ViPNet Клиент Монитор для индивидуальной справочной установки Магистраль АСУ «Экспресс-3» со специализированными для этой задачи настройками. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика.</p>
17.	ИСУ Спектр	0034	только АП	<p>На АП, зарегистрированном в этой задаче, будет работать ПО ViPNet Linux для индивидуальной справочной установки Спектр АСУ «Экспресс-3» со специализированными для этой задачи настройками. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика.</p>
18.	ИСУ Навигатор	0033	только АП	<p>На АП, зарегистрированном в этой задаче, будет работать ПО ViPNet Клиент Монитор для индивидуальной справочной установки Навигатор АСУ «Экспресс-3» со специализированными для этой задачи настройками. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика.</p>
19.	ViPNet Cluster	0032	только СМ	<p>На СМ, зарегистрированном в этой задаче, будет работать функционал ViPNet Cluster под ОС Windows. Для каждого кластера можно задать число элементов. Суммарное число элементов не может превосходить число, заданное в лицензии.</p>

№ п/п	Название ПЗ	Идентификатор ПЗ	Тип СУ (АП и/или СМ)	Примечание
20.	Web-шлюз	002С	только СМ	На СМ, зарегистрированном в этой задаче, будет запускаться программа ViPNet Web Gate под ОС Linux. Для каждого Web-шлюза можно задать число адресов. Суммарное число адресов не может превосходить число, заданное в лицензии.
21.	АРМ мониторинга	0036	только АП	На АП, зарегистрированном в этой задаче, будет запускаться апплет мониторинга АСУ «Экспресс-3».
22.	ИСУ Видеотон	0037	только АП	На АП, зарегистрированном в этой задаче, будет работать ПО ViPNet Клиент Монитор для индивидуальной справочной установки Видеотон АСУ «Экспресс-3» со специализированными для этой задачи настройками. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется. Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика .
23.	Сервис публикации	0038	только АП	На АП, зарегистрированном в этой задаче, будет работать программа ViPNet Publication Service.
24.	Блок сопряжения УФС	0039	только АП	На АП, зарегистрированном в этой задаче, будет работать ПО ViPNet Linux для блока сопряжения УФС АСУ «Экспресс-3» со специализированными для этой задачи настройками. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется. Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика .
25.	Сервер SGA	003A	только СМ	Для СМ (только для Linux), зарегистрированного в этой задаче, разрешен мониторинг со стороны абонентских пунктов, зарегистрированных в задаче Клиент SGA . Начиная с версии Linux-координатора 3.5.1, регистрация в этой задаче не требуется.
26.	Клиент SGA	003B	только АП	На абонентском пункте, зарегистрированном в этой задаче, будет запускаться апплет мониторинга ViPNet-координатора.
27.	Coordinator KB 1000	002D	только СМ	Координатор (СМ), зарегистрированный в этой задаче, сможет работать в составе ПАК ViPNet Coordinator KB 1000. Задание IP-адресов, туннелируемых IP-адресов и специальных параметров в этой задаче осуществляются так же, как в задаче Сервер IP-адресов .

№ п/п	Название ПЗ	Идентификатор ПЗ	Тип СУ (АП и/или СМ)	Примечание
28.	ИТТС Трансинфосеть	003D	только АП	<p>На АП, зарегистрированном в этой задаче, будет работать ПО ViPNet Клиент Монитор для информационно-транзакционного терминала самообслуживания Трансинфосеть АСУ «Экспресс-3» со специализированными для этой задачи настройками. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика.</p>
29.	Сервер TLS	003C	АП или СМ	<p>На СУ, зарегистрированных в этой задаче, будет обеспечена поддержка серверной компоненты протокола TLS (Transport Layer Security).</p>
30.	ИСУ Трансинфосеть	003F	только АП	<p>На АП, зарегистрированном в этой задаче, будет работать ПО ViPNet Client Монитор для индивидуальной справочной установки Трансинфосеть АСУ «Экспресс-3» со специализированными для этой задачи настройками. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика.</p>
31.	Coordinator HW100-A	0040	только СМ	<p>Координатор (СМ), зарегистрированный в этой задаче, сможет работать в составе ПАК ViPNet Coordinator HW100.</p> <p>Координатор, зарегистрированный в этой задаче, нельзя регистрировать ни в одной другой задаче, кроме задач Сервер Открытого Интернета и Агент мониторинга.</p> <p>Координатор, зарегистрированный в этой задаче, не выполняет функцию сервера-маршрутизатора почтовых сообщений.</p> <p>Ограничения на число туннелируемых адресов определяются условиями поставки.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же, как в задаче Сервер IP-адресов.</p>

№ п/п	Название ПЗ	Идентификатор ПЗ	Тип СУ (АП и/или СМ)	Примечание
32.	Coordinator HW100-B	0041	только СМ	<p>Координатор (СМ), зарегистрированный в этой задаче, сможет работать в составе ПАК ViPNet Coordinator HW100.</p> <p>Координатор, зарегистрированный в этой задаче, нельзя регистрировать ни в одной другой задаче, кроме задач Сервер Открытого Интернета и Агент мониторинга.</p> <p>Координатор, зарегистрированный в этой задаче, не выполняет функцию сервера-маршрутизатора почтовых сообщений.</p> <p>Ограничения на число туннелируемых адресов определяются условиями поставки.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же, как в задаче Сервер IP-адресов.</p>
33.	Coordinator HW100-C	0042	только СМ	<p>Координатор (СМ), зарегистрированный в этой задаче, сможет работать в составе ПАК ViPNet Coordinator HW100.</p> <p>Координатор, зарегистрированный в этой задаче, нельзя регистрировать ни в одной другой задаче, кроме задач Сервер Открытого Интернета и Агент мониторинга.</p> <p>Координатор, зарегистрированный в этой задаче, выполняет функцию сервера-маршрутизатора почтовых сообщений.</p> <p>Ограничения на число туннелируемых адресов определяются условиями поставки.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же, как в задаче Сервер IP-адресов.</p>
34.	Криптофайл	0043	только АП	<p>На АП, зарегистрированном в этой задаче, будет запускаться ПО ViPNet CryptoFile.</p>
35.	Coordinator HW1000	0044	только СМ	<p>Координатор (СМ), зарегистрированный в этой задаче, сможет работать в составе ПАК ViPNet Coordinator HW1000.</p> <p>Координатор, зарегистрированный в этой задаче, нельзя регистрировать ни в одной другой задаче, кроме задач ViPNet Failover, Сервер Открытого Интернета и Агент мониторинга.</p> <p>Задание IP-адресов, туннелируемых IP-адресов и специальных параметров в этой задаче осуществляются так же, как в задаче Сервер IP-адресов.</p>

№ п/п	Название ПЗ	Идентификатор ПЗ	Тип СУ (АП и/или СМ)	Примечание
36.	Coordinator HW2000	0045	только СМ	<p>Координатор (СМ), зарегистрированный в этой задаче, сможет работать в составе ПАК ViPNet Coordinator HW2000.</p> <p>Координатор, зарегистрированный в этой задаче, нельзя регистрировать ни в одной другой задаче, кроме задач ViPNet Failover, Сервер Открытого Интернета и Агент мониторинга.</p> <p>Задание IP-адресов, туннелируемых IP-адресов и специальных параметров в этой задаче осуществляются так же, как в задаче Сервер IP-адресов.</p>
37.	Сервер мониторинга StateWatcher	0047	только АП	<p>На АП, зарегистрированном в этой задаче, будет работать система мониторинга сетевых узлов ViPNet StateWatcher. На сетевых узлах будет разрешен мониторинг только с тех АП, которые зарегистрированы в этой задаче.</p> <p>Для АП, зарегистрированном в этой задаче, можно задать число узлов мониторинга и число дочерних серверов мониторинга.</p>
38.	КриптоСервис Linux	0048	АП или СМ	<p>На СУ, зарегистрированных в этой задаче, можно будет работать с набором криптофункций ViPNet SDK Linux.</p>
39.	ViPNet Terminal	0049	только АП	<p>На АП, зарегистрированном в этой задаче, будет работать ПАК ViPNet Terminal. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика.</p>
40.	ТТР Спектр	004A	только АП	<p>На АП, зарегистрированном в этой задаче, будет работать ПО ViPNet Client Монитор для терминала «ТТР Спектр» АСУ «Экспресс-3» со специализированными для этой задачи настройками. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Защита трафика.</p>

№ п/п	Название ПЗ	Идентификатор ПЗ	Тип СУ (АП и/или СМ)	Примечание
41.	Coordinator HW-VPNМ	004B	только СМ	<p>Координатор (СМ), зарегистрированный в этой задаче, сможет работать в составе ПАК ViPNet Coordinator HW-VPNМ.</p> <p>Координатор, зарегистрированный в этой задаче, нельзя регистрировать ни в одной другой задаче, кроме задач ViPNet Failover, Сервер Открытого Интернета и Агент мониторинга.</p> <p>Задание IP-адресов, туннелируемых IP-адресов и специальных параметров в этой задаче осуществляются так же как в задаче Сервер IP-адресов.</p>
42.	Агент мониторинга	004E	только СМ	<p>На координаторе (СМ), зарегистрированном в этой прикладной задаче, будет работать программное обеспечение ViPNet Monitoring Agent.</p>
43.	VPN-клиент для мобильных устройств	004F	только АП	<p>На АП, зарегистрированном в этой задаче, может работать ПО ViPNet Client iOS или ViPNet Client Android. Если АП зарегистрирован в этой задаче, то регистрация его в других задачах не требуется.</p> <p>Задание IP-адресов и уровня полномочий в этой задаче осуществляются так же, как в задаче Защита трафика.</p>
44.	Coordinator HW100-СНВ	0050	только СМ	<p>Координатор (СМ), зарегистрированный в этой задаче, сможет работать в составе ПАК ViPNet Coordinator HW100.</p> <p>Координатор, зарегистрированный в этой прикладной задаче, автоматически считается зарегистрированным в задачах КриптоСервис Linux, Деловая почта и Диспетчер.</p> <p>Координатор, зарегистрированный в этой задаче, выполняет функцию сервера-маршрутизатора почтовых сообщений.</p> <p>Ограничения на число туннелируемых адресов определяются условиями поставки.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же, как в задаче Сервер IP-адресов.</p>

№ п/п	Название ПЗ	Идентификатор ПЗ	Тип СУ (АП и/или СМ)	Примечание
45.	Coordinator HW110	0051	только СМ	<p>Координатор (СМ), зарегистрированный в этой задаче, сможет работать в составе ПАК ViPNet Coordinator HW110.</p> <p>Координатор, зарегистрированный в этой задаче, нельзя регистрировать ни в одной другой задаче, кроме задачи Агент мониторинга.</p> <p>Координатор, зарегистрированный в этой задаче, выполняет функцию сервера-маршрутизатора почтовых сообщений.</p> <p>Ограничения на число туннелируемых адресов определяются условиями поставки.</p> <p>Задание IP-адресов и специальных параметров в этой задаче осуществляются так же, как в задаче Сервер IP-адресов.</p>
46.	Сервер мониторинга СБ РФ	0052	только АП	На абонентском пункте, зарегистрированном в этой прикладной задаче, будет работать программное обеспечение ViPNet Monitoring Server.
47.	ViPNet Security Gateway	0053	только СМ	<p>На абонентском пункте, зарегистрированном в этой задаче, может работать ПО ViPNet Security Gateway.</p> <p>Задание IP-адресов, туннелируемых IP-адресов и специальных параметров в этой задаче осуществляются так же, как в задаче Сервер IP-адресов.</p>
48.	Coordinator KB 100	0054	только СМ	<p>Координатор (СМ), зарегистрированный в этой задаче, сможет работать в составе ПАК ViPNet Coordinator KB 100.</p> <p>Задание IP-адресов, туннелируемых IP-адресов и специальных параметров в этой задаче осуществляются так же, как в задаче Сервер IP-адресов.</p>
49.	Coordinator HW-VA	0055	только СМ	<p>Координатор (СМ), зарегистрированный в этой задаче, может быть развернут на виртуальной машине с помощью программного обеспечения ViPNet Coordinator HW-VA.</p> <p>Координатор, зарегистрированный в этой задаче, нельзя регистрировать ни в одной другой задаче, кроме задач ViPNet Failover, и Сервер Открытого Интернета.</p> <p>Задание IP-адресов, туннелируемых IP-адресов и специальных параметров в этой задаче осуществляются так же, как в задаче Сервер IP-адресов.</p>
50.	Сервер TSP/OCSP	0056	только АП	На абонентском пункте, зарегистрированном в этой задаче, будет работать программное обеспечение ViPNet CA Service, выполняющее функции TSP/OCSP-сервера.

Для удобства описания, прикладные задачи *Терминал Навигатор*, *Терминал Спектр*, *Терминал Ареал-Сервис*, *ИТТС Трансинфосеть*, *ИСУ Трансинфосеть*, *ИСУ Магистраль*, *ИСУ Навигатор*, *ИСУ Спектр*, *ИСУ Видеотон*, *ТТР Спектр* и *Блок сопряжения УФС* будем называть прикладными задачами для терминалов АСУ «Экспресс-3».

Для расширения функциональных характеристик ViPNet сети реализована возможность взаимодействия между собой абонентских пунктов с установленными на них разными прикладными программами (Деловая почта и Диспетчер). При этом следует иметь в виду следующее **ограничение**:

Прикладная программа «Диспетчер» может принимать почту от прикладной программы «Деловая почта» и наоборот, только, если АП с «Диспетчером» не зарегистрирован также и в задаче *Деловая почта* и наоборот. Если какие-то АП зарегистрированы в обеих задачах, то каждая из задач на этих АП может взаимодействовать только с одноименной задачей.

13.2 Рекомендации по регистрации СУ в различных прикладных задачах в зависимости от функциональности, которую должно обеспечивать ПО ViPNet на этих узлах

Рекомендации по регистрации СМ в различных прикладных задачах в зависимости от функциональности, которую должен обеспечивать ViPNet-координатор:

Функциональность, которую должен обеспечивать ViPNet-координатор, определяется Центром управления сетью путем регистрации СМ (координатора) в соответствующей прикладной задаче (ПЗ). При создании, координатор регистрируется в ПЗ, указанных в окне настроек по умолчанию (пункт меню *Службы/Настройки по умолчанию*, см. п.11.4)).

Для того чтобы на СУ работало ПО ViPNet Coordinator, и ViPNet-координатор осуществлял функции защиты IP-трафика (Сервера IP-адресов и Сервера ViPNet Firewall), а также функции Сервера маршрутизатора почтовых и управляющих сообщений, зарегистрируйте этот координатор в ПЗ *Сервер IP-адресов*.

Если ViPNet-координатор должен также обеспечить туннелирование открытых пакетов в защищенное соединение для отдельных незащищенных компьютеров (без ПО ViPNet), то следует указать для этого координатора максимальное число адресов для туннелирования. Максимальное число адресов для туннелирования задается в окне регистрации в ПЗ *Сервер IP-адресов* (см. п. 13.4.2).

Для того чтобы на ViPNet-координаторе работало ПО ViPNet Cluster (под ОС Windows) необходимо дополнительно (к ПЗ *Сервер IP-адресов*) зарегистрировать этот координатор в задаче *ViPNet Cluster* и задать для него максимальное число элементов кластера.

Для обеспечения работы ПАК ViPNet Coordinator KB 100/1000 зарегистрируйте этот координатор в ПЗ *Coordinator KB 100/1000*. При этом один и тот же координатор нельзя регистрировать в задаче *Сервер IP-адресов* и *Coordinator KB 100/1000*.

Для обеспечения работы ПАК ViPNet Coordinator HW100 следует зарегистрировать координатор в задаче *Coordinator HW100-A, B или C*.

Замечание: На координаторе, зарегистрированном в задаче *Coordinator HW100-A* или *B*, не следует регистрировать АП (в адресной администрации), если АП должны иметь возможность обмениваться почтовыми сообщениями с другими АП. Такое ограничение связано с тем, что координатор, зарегистрированный в задаче *Coordinator HW100-A* или *B*, не выполняет функцию сервера-маршрутизатора почтовых сообщений.

Для обеспечения работы ПАК ViPNet Coordinator HW1000 или ПАК ViPNet Coordinator HW2000 следует зарегистрировать координатор в задаче *Coordinator HW1000* или *Coordinator HW2000* соответственно.

Замечание: При регистрации координатора в прикладных задачах *Coordinator KB 100/1000* и задачах *Coordinator HW100/1000/2000/VPNM* происходит автоматическая отмена регистрации этого координатора во всех прикладных задачах, в которых он был зарегистрирован ранее (кроме задач *Агент мониторинга* и *ViPNet Failover* для совместимых задач).

ViPNet-координатор, работающий под ОС Linux, может осуществлять также функции резервирования серверов, для этого необходимо дополнительно (к ПЗ **Сервер IP-адресов**, **Coordinator HW1000**, **Coordinator HW2000** или **Coordinator HW-VPNМ**) зарегистрировать его в задаче **ViPNet Failover**.

Для того чтобы на координаторе работала программа ViPNet Web Gate под ОС Linux необходимо зарегистрировать его в ПЗ **Сервер IP-адресов** и **Web-шлюз**.

Для того чтобы ViPNet-координатор осуществлял функции Сервера Открытого Интернета, необходимо этот координатор зарегистрировать в следующих ПЗ: **Сервер IP-адресов** и **Сервер Открытого Интернета**. Регистрация в задаче **Сервер Открытого Интернета** производится в окне регистрации в задаче **Сервер IP-адресов**.

При регистрации в ПЗ **Сервер IP-адресов** координатору присваивается максимальный уровень полномочий. Если необходимо изменить уровень полномочий, то дополнительно такой координатор нужно зарегистрировать в задаче **Защита трафика**, т.к. настройки полномочий для координатора производятся в этой задаче (см. п. 13.4.1). При регистрации в ПЗ **Защита трафика** координатору присваивается уровень полномочий, указанный в окне настроек по умолчанию (пункт меню **Службы/Настройки по умолчанию**, см. п.11.4)).

Если координатор должен осуществлять функции только Сервера маршрутизатора почтовых и управляющих сообщений (для обеспечения функционирования сети защищенных почтовых сообщений), то достаточно зарегистрировать его в ПЗ **КриптоСервис**. В этом случае на координаторе должна быть установлена и запущена программа ViPNet CryptoService (для возможности осуществлять запуск ViPNet MFTP и производить централизованное обновление справочно-ключевой информации). На таком координаторе можно работать с набором криптофункций на базе криптопровайдера Домен К (ViPNet SDK). Также в задаче **КриптоСервис** Вы можете произвести изменение полномочий для СМ, если это необходимо. Если координатор одновременно зарегистрирован в задачах **КриптоСервис** и **Защита трафика**, то для обеих задач следует задавать одинаковые полномочия.

Для того чтобы на координаторе можно было работать с набором криптофункций на базе криптопровайдера Домен К (ViPNet SDK), зарегистрируйте координатор в задаче **ViPNet SDK** или **КриптоСервис**.

Для того чтобы на координаторе обеспечивалась поддержка серверной компоненты протокола TLS (Transport Layer Security), необходимо зарегистрировать координатор в задаче **Сервер TLS**. Также этот координатор должен быть зарегистрирован в задаче **КриптоСервис**.

Внимание! Если сетевые узлы зарегистрированы в ПЗ **ViPNet SDK** или **КриптоСервис**, то для них должно выполняться следующее условие: каждый пользователь должен быть зарегистрирован только в одном единственном типе коллектива, областью действия которого является один единственный сетевой узел.

Для того чтобы на координатор можно было использовать в качестве агента системы мониторинга абонентских пунктов ViPNet Monitoring System, необходимо зарегистрировать координатор в прикладной задаче **Агент мониторинга**.

Для того чтобы можно было осуществлять мониторинг координатора при помощи апплета мониторинга ViPNet-координатора, необходимо дополнительно (к ПЗ **Сервер IP-адресов**) зарегистрировать координатор в задаче **Сервер SGA**. **Внимание!** Начиная с версии Linux-координатора 3.5.1, регистрация в этой задаче не требуется.

Рекомендации по регистрации АП в различных прикладных задачах:

Для того чтобы на АП работало ПО ViPNet Client (т.е. работали модули Монитор и Деловая почта) необходимо этот АП зарегистрировать в следующих ПЗ: **Защита трафика** (для обеспечения работы ViPNet Client Монитор), **Деловая почта** (для обеспечения работы ViPNet Client Деловой почта).

Для того чтобы на АП работало ПО ViPNet Administrator необходимо этот АП зарегистрировать в следующих ПЗ: **Ключевой центр**, **ЦУС**. На АП администратора необходимо также

установить ПО ViPNet Client, поэтому зарегистрируйте этот АП в соответствующих ПЗ (см. выше).

Для того чтобы на АП работала программа ViPNet SafeDisk, интегрированная с ViPNet, необходимо зарегистрировать этот АП в задаче **Секретный диск**. СМ также может быть зарегистрирован в этой задаче.

Для того чтобы на АП работала программа ViPNet Registration Point необходимо зарегистрировать этот АП в задаче **Центр регистрации**.

Для того чтобы на АП работала программа ViPNet Policy Manager, необходимо зарегистрировать этот АП в задаче **Центр управления политиками**.

Для того чтобы на АП работала программа ViPNet Publication Service необходимо зарегистрировать этот АП в задаче **Сервис публикации**.

Для того чтобы на АП работала программа ViPNet CryptoService необходимо зарегистрировать этот АП в задаче **КриптоСервис**. В этом случае на АП можно работать с набором криптофункций на базе криптопровайдера Домен К (ViPNet SDK). Если АП одновременно зарегистрирован в задачах **КриптоСервис** и **Защита трафика**, то для обеих задач следует задавать одинаковые полномочия.

Для того чтобы на АП работала программа ViPNet CryptoFile необходимо зарегистрировать этот АП в задаче **Криптофайл**, а также в задаче **КриптоСервис**.

Для того чтобы на АП можно было работать с набором криптофункций на базе криптопровайдера Домен К (ViPNet SDK), а также если нет необходимости производить централизованное обновление справочно-ключевой информации, то необходимо зарегистрировать АП в задаче **ViPNet SDK**.

Для того, чтобы на АП обеспечивалась поддержка серверной компоненты протокола TLS (Transport Layer Security), необходимо зарегистрировать АП в задаче **Сервер TLS**. Также этот АП должен быть зарегистрирован в задаче **КриптоСервис**.

Внимание! Если сетевые узлы зарегистрированы в ПЗ **ViPNet SDK**, **КриптоСервис** или **Криптофайл**, то для них должно выполняться следующее условие: каждый пользователь должен быть зарегистрирован только в одном единственном типе коллектива, областью действия которого является один единственный сетевой узел.

Регистрировать АП в одной из задач для терминалов АСУ «Экспресс-3» требуется для возможности работы ПО ViPNet Client на соответствующем терминале АСУ «Экспресс-3». В других задачах регистрировать не требуется. Для каждого вида терминала ViPNet Client имеет специализированные настройки, зависящие от выбранной ПЗ. Для узлов, зарегистрированных в задачах терминалов АСУ «Экспресс-3», кроме задач **Терминал Спектр**, **Терминал Ареал-Сервис**, **ИТТС Трансинфосеть**, **ИСУ Трансинфосеть**, отключена функция отправки удаленного обновления ПО ViPNet, файла Infotecs.re, адресных справочников и ключей, т.к. в ПО ViPNet для этих терминалов не реализована возможность принятия обновлений.

Для узлов, зарегистрированных в задачах терминалов АСУ «Экспресс-3» **Терминал Спектр** или **Терминал Ареал-Сервис**, существует возможность задать резервный сервер IP-адресов (см. п. 13.4.2.4).

Для того, чтобы на АП можно было запускать апплет мониторинга ViPNet-координатора, его необходимо дополнительно (к ПЗ **Защита трафика**) зарегистрировать в задаче **Клиент SGA**.

Для того, чтобы на АП можно было запускать апплет мониторинга АСУ «Экспресс-3», его необходимо зарегистрировать в задаче **АРМ мониторинга**.

Для того, чтобы на АП можно было запускать систему мониторинга сетевых узлов ViPNet StateWatcher, его необходимо зарегистрировать в задаче **Сервер мониторинга** (см. п. 13.4.7).

13.3 Индивидуальная регистрация АП в задачах

Для регистрации АП в прикладной задаче выберите команду меню **Службы/ Индивидуальная регистрация АП в задачах** (Рисунок 15):

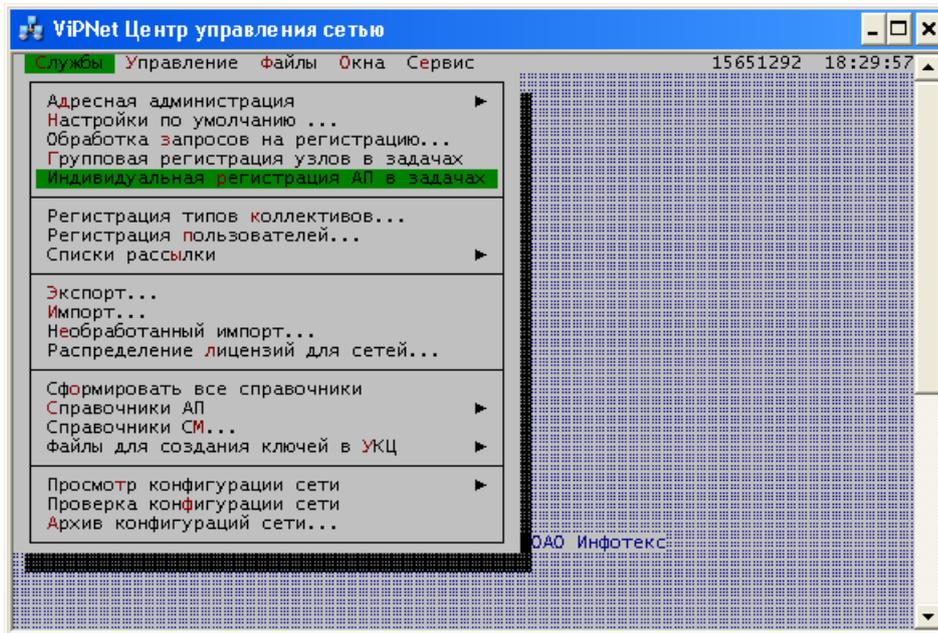


Рисунок 15

При выполнении команды меню **Индивидуальная регистрация АП в задачах** появится диалоговое окно со списком АП, зарегистрированных в различных прикладных задачах (Рисунок 16).

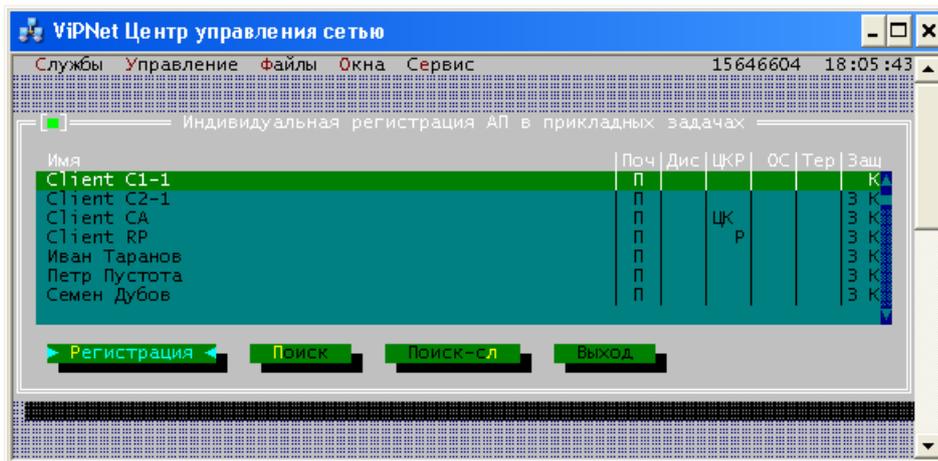


Рисунок 16

Наличие регистрации в какой-либо задаче отображается различными буквами в соответствующей колонке:

Колонка **Поч**

- * П – Деловая почта
- * V – ViPNet SDK

Колонка **Дис**

- * Д – Диспетчер

Колонка **ЦКР**

- * **Ц** – ЦУС
- * **К** – УКЦ
- * **Р** – Центр регистрации
- * **П** – Центр управления политиками безопасности

Колонка **ОС** отражает **S**, если используется операционная система Solaris

Колонка **Тер** отражает задачи терминалов

- * **N** – Терминал Навигатор
- * **S** – Терминал Спектр
- * **A** – Терминал Ареал-Сервис
- * **m** – ИСУ Магистраль
- * **n** – ИСУ Навигатор
- * **s** – ИСУ Спектр
- * **v** – ИСУ Видеотон
- * **U** – Блок сопряжения УФС
- * **I** – ИТТС Трансинфосеть
- * **i** – ИСУ Трансинфосеть

Колонка **Защ**

- * **З** – Защита трафика
- * **К** – КриптоСервис
- * **С** – Секретный диск

Для регистрации какого-либо АП, выберите его и нажмите кнопку **Регистрация**. Появится окно со списком прикладных задач, лицензированных для данного ЦУС (Рисунок 17).

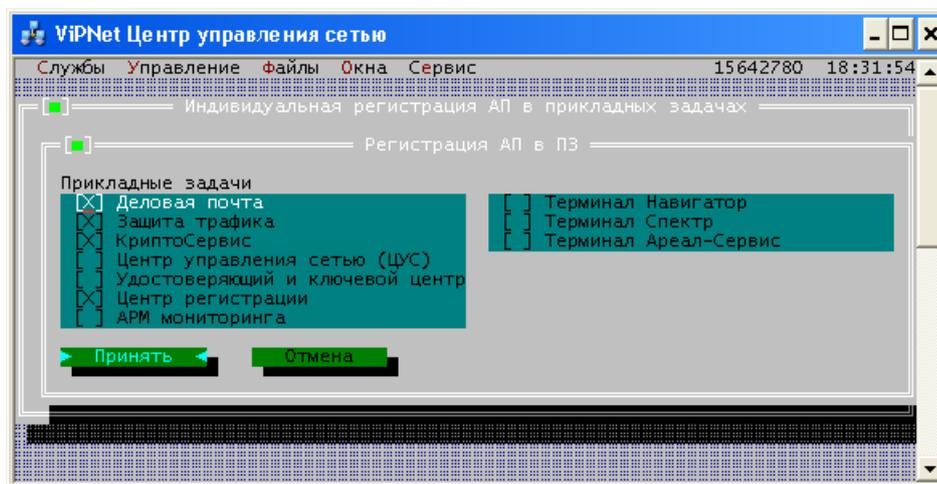


Рисунок 17

Для регистрации АП с помощью мыши или клавиши «Пробел» поставьте крестик напротив прикладной задачи, в которой хотите зарегистрировать выбранный АП.

Если Вам нужно произвести дополнительные настройки СУ, то воспользуйтесь групповой регистрацией СУ в ПЗ (см. п.13.4).

13.4 Групповая регистрация СУ (АП и СМ) в ПЗ

Для регистрации СУ (СМ или АП) в прикладной задаче выберите команду **Групповая регистрация узлов в задачах** (Рисунок 18).

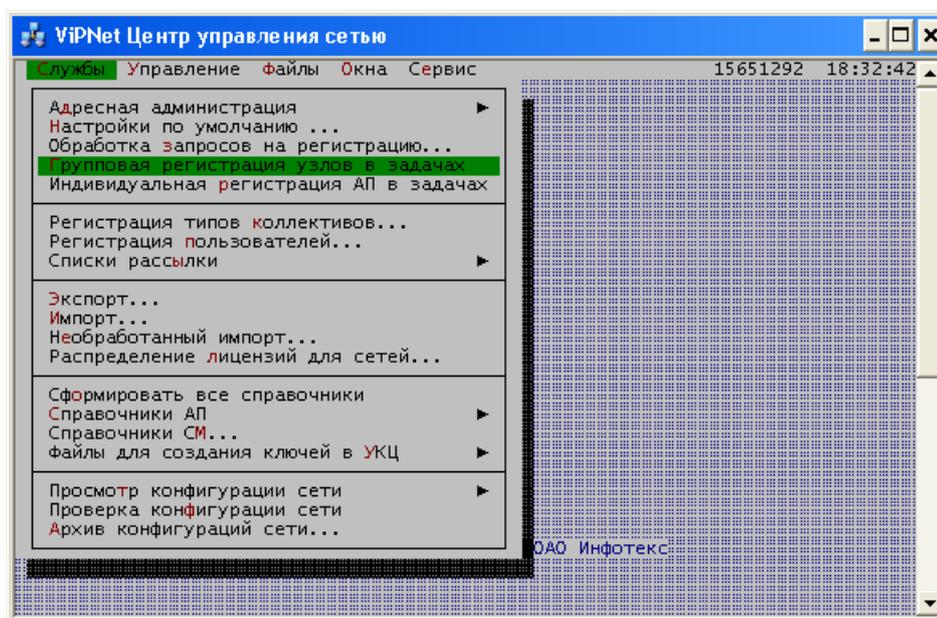


Рисунок 18

При выполнении команды меню **Групповая регистрация узлов в задачах** появится диалоговое окно (Рисунок 19), в котором в колонке **Прикладная задача** выводится список ПЗ, на которые есть разрешение в файле лицензии; в колонке **Использовано** указано количество использованных лицензий для выбранной ПЗ, в колонке **Лицензия** указано разрешенное количество лицензий для выбранной ПЗ.

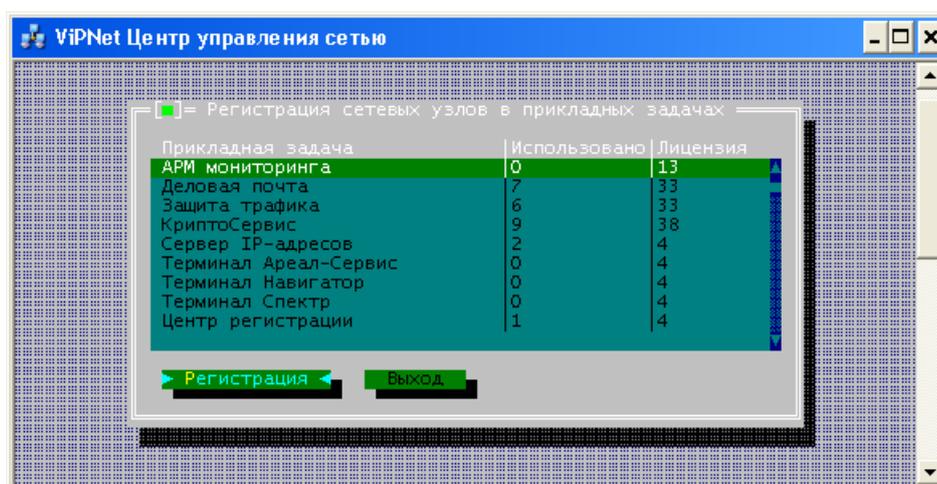


Рисунок 19

Выберите прикладную задачу, в которой хотите зарегистрировать СУ, и нажмите кнопку **Регистрация**. Появится окно со списком СУ, зарегистрированных в выбранной ПЗ (или пустое, если ни один узел еще не зарегистрирован в выбранной задаче) (Рисунок 20).

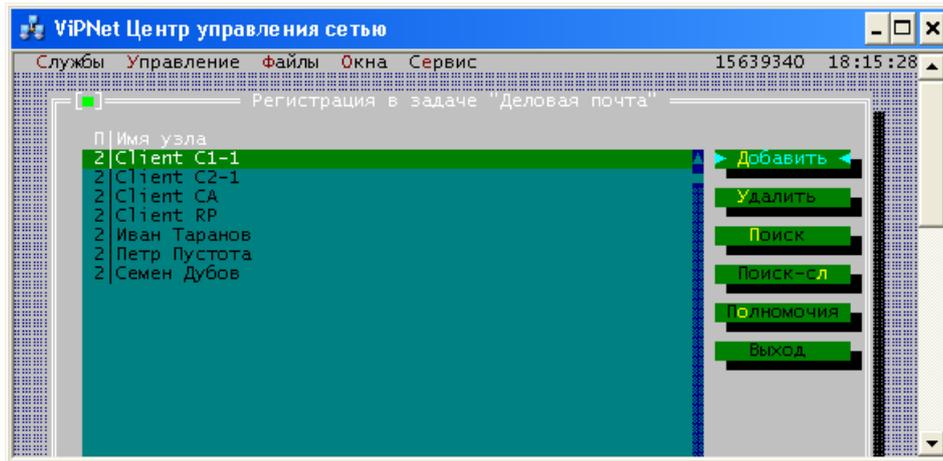


Рисунок 20

В этом окне Вы можете добавить (кнопка **Добавить**) или удалить СУ (кнопка **Удалить**). Кнопка **Выйти** используется для выхода из окна.

Для СУ, зарегистрированных в задачах **Защита трафика**, **Деловая почта**, **КриптоСервис**, **VPN-клиент для мобильных устройств** в окне регистрации в соответствующей задаче Вы можете произвести настройки полномочий пользователя (см. п. 13.4.1, 13.4.4).

Для СУ, зарегистрированных в задачах **Защита трафика**, **Сервер IP-адресов**, **Coordinator HW100-A, B, C**, **Coordinator HW1000**, **Coordinator HW2000**, **Coordinator HW-VPNM**, задачах для терминалов АСУ «Экспресс-3» Вы можете произвести дополнительные настройки различных параметров (IP-адресов и др.), см. п. 13.4.1, 13.4.2. Для координаторов, зарегистрированных в задачах **Coordinator HW1000** или **Coordinator HW2000**, **Coordinator HW-VPNM** можно задать максимальное число адресов для туннелирования.

Для координаторов, зарегистрированных в задаче **ViPNet Cluster**, можно задать число элементов кластера (см. п. 13.4.3).

Для координаторов, зарегистрированных в задаче **Web-шлюз**, можно задать число адресов.

Для АП, зарегистрированных в задаче **Центр регистрации**, можно задать ограничения на количество запросов на дистрибутивы и запросов на сертификаты (см. п. 13.4.5).

Для АП, зарегистрированных в задаче **Центр управления политиками**, можно задать список управляемых узлов (домен), см. п. 13.4.6.

Для АП, зарегистрированном в задаче **Сервер мониторинга**, можно задать число узлов мониторинга и число дочерних серверов мониторинга (см. п. 13.4.7).

Более подробно об этом читайте далее.

13.4.1 Регистрация узлов в задаче «Защита трафика»

Зарегистрировать АП в задаче **Защита трафика** можно обоими способами, указанными в разделах 13.3 и 13.4. Однако СМ можно зарегистрировать в задаче **Защита трафика** только из окна регистрации узла в этой задаче (см. раздел 13.4). Откроется окно **Регистрация в задаче «Защита трафика»** (Рисунок 21).

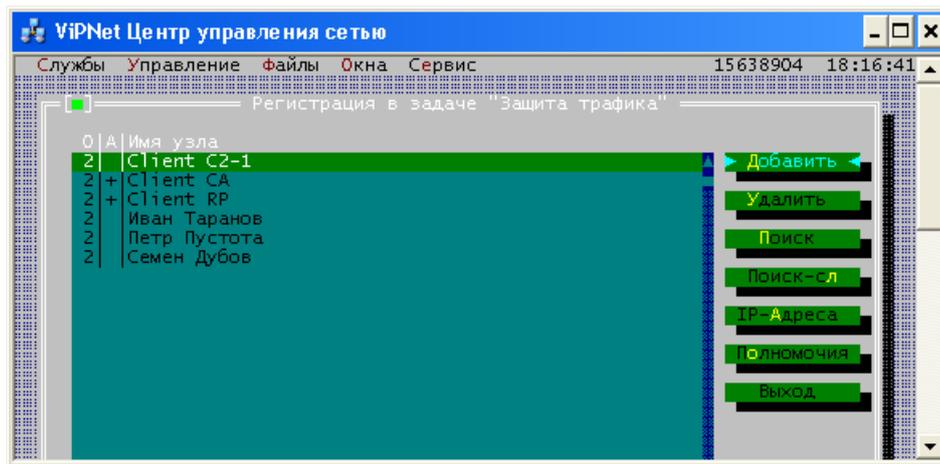


Рисунок 21

Для регистрации узла необходимо нажать кнопку **Добавить** и из предложенного списка СУ выбрать нужные, затем нажать кнопку **Принять**.

Нажав кнопку **IP-Адреса**, можно для конкретного узла произвести различные настройки (задать один или несколько IP-адресов, и т.д.). Однако задавать IP-адреса имеет смысл только для координаторов в окне регистрации в задаче **Сервер IP-адресов** (за исключением некоторых случаев, описанных ниже в разделе 13.8). Адреса друг друга АП узнают в процессе работы.

В прикладной задаче **Защита трафика** можно задать уровень полномочий пользователя для того или иного сетевого узла. Уровень полномочий определяет допустимость различных действий пользователей по изменению настроек в ViPNet Монитор и ViPNet MFTP на данном узле. По умолчанию присваивается уровень полномочий, указанный в окне настроек по умолчанию (пункт меню **Службы > Настройки по умолчанию**, см. п. 12).

Чтобы изменить уровень полномочий для одного или нескольких сетевых узлов, выберите эти узлы в списке и нажмите кнопку **Полномочия** (для выделения сетевого узла используйте клавишу «пробел»). В окне **Выбор уровня полномочий** установите один из четырех уровней: **Минимальный**, **Средний**, **Максимальный** и **Специальный**. При выборе пункта **Специальный** введите символ, обозначающий нужный уровень полномочий, в предусмотренное для это поле. Соответствие уровней полномочий функциональным возможностям программы описано в отдельном документе «Классификация полномочий».

Для удаления регистрации в данной задаче выберите один или несколько сетевых узлов и нажмите кнопку **Удалить**.

13.4.2 Регистрация СМ в задаче «Сервер IP-адресов»

В этой задаче могут быть зарегистрированы только СМ (Рисунок 22). Для регистрации сервера необходимо нажать кнопку **Добавить** и из предложенного списка СМ выбрать нужные, затем нажать кнопку **Принять**.

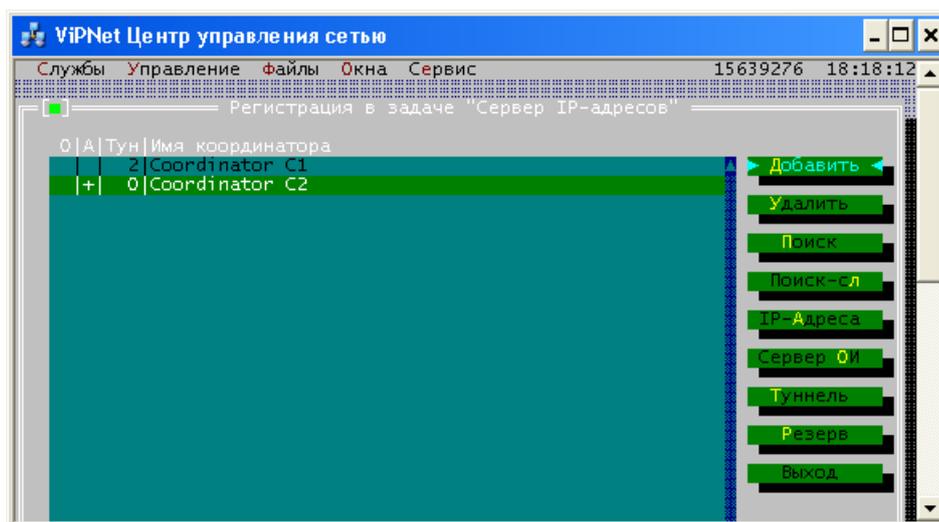


Рисунок 22

Удаление регистрации в прикладной задаче:

Для удаления регистрации в данной задаче необходимо выбрать нужные АП и нажать кнопку **Удалить**.

13.4.2.1 Задание IP-адресов

Нажав кнопку **IP-Адреса**, можно для выбранного сервера произвести различные настройки (задать один или несколько IP-адресов, и т.д.). После задания адресов в колонке **А** появится "+". При задании адресов следует руководствоваться правилами, описанными ниже в разделе 13.5 и его подразделах. Рекомендуем произвести все необходимые настройки в программе ViPNet ЦУС, чтобы избежать дополнительных ручных настроек на каждом СУ сети.

13.4.2.2 Включение функции Сервер открытого Интернета

Если сервер будет использоваться как Сервер открытого Интернета, то следует нажать кнопку **Сервер ОИ** (Рисунок 22), после подтверждения включения функции Сервер открытого Интернета в колонке **О** появится "+". Для отмены регистрации в задаче Сервер Открытого Интернета, нажмите эту кнопку еще раз.

Замечание: На координаторе, осуществляющем функции Сервера Открытого Интернета, не следует регистрировать АП (в адресной администрации), если АП должны взаимодействовать с другими АП сети ViPNet.

13.4.2.3 Задание максимального числа адресов для туннелирования

Если сервер должен обеспечивать туннелирование трафика открытых компьютеров локальной сети, то следует нажать кнопку **Туннель** и задать максимальное число адресов, которое может туннелироваться данным ViPNet-координатором. Это число появится в колонке **Тун**. По умолчанию в колонке **Тун** отображается 0, что означает, что ViPNet-координатор не будет осуществлять туннелирование. Если число туннелируемых адресов превышает 999, то в колонке **Тун** отображается "****".

13.4.2.4 Назначение резервного сервера IP-адресов для АП-терминала

Для абонентских пунктов, зарегистрированных в прикладных задачах **Терминал Спектр** или **Терминал Ареал-Сервис**, существует возможность задать резервный сервер IP-адресов.

Резервный сервер IP-адресов используется в следующем случае: Если АП-терминалу по каким-либо причинам перестает быть доступным его основной сервер IP-адресов, то АП-терминал переходит на использование другого сервера IP-адресов, заданного в ЦУС в качестве резервного. Для каждого АП-терминала можно задать только один резервный сервер IP-адресов. В качестве

резервного сервера IP-адресов может быть выбран сервер IP-адресов своей или доверенной сети. Для того чтобы сервер IP-адресов стал резервным для АП необязательно задавать между ними связи по типу коллектива.

Если сервер своей или доверенной сети должен выполнять функции резервного сервера IP-адресов для каких-либо абонентских пунктов, то выберите сервер и нажмите кнопку **Резерв** (Рисунок 22). Кнопка доступна только в случае, если есть ненулевое число лицензий на прикладные задачи **Терминал Спектр** или **Терминал Ареал-Сервис**. Откроется окно со списком абонентских пунктов, для которых сервер уже назначен резервным.

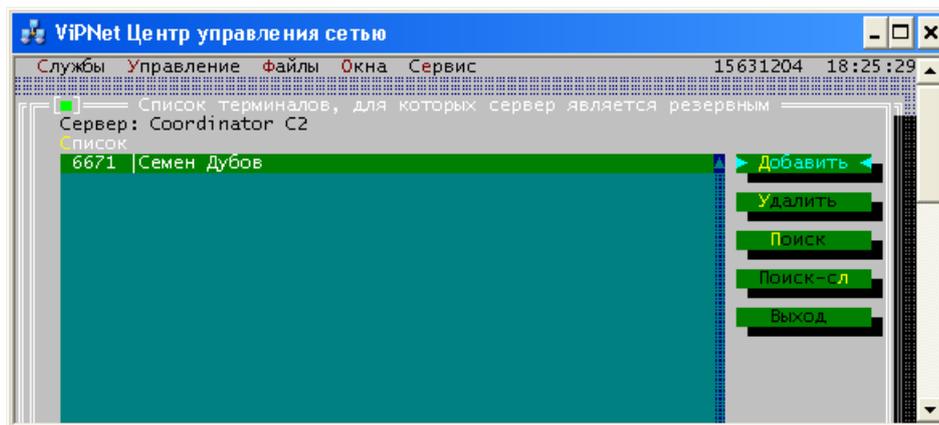


Рисунок 23

Если таких абонентских пунктов нет, то список будет пустым (Рисунок 23). Для добавления абонентского пункта нажмите кнопку **Добавить**, откроется окно со списком доступных для выбора абонентских пунктов (Рисунок 24), удовлетворяющих следующим условиям:

- АП зарегистрирован в задачах Терминал Спектр или Терминал Ареал-Сервис;
- АП не является абонентским пунктом, зарегистрированным на выбранном сервере;
- для АП еще не назначен резервный сервер IP-адресов.

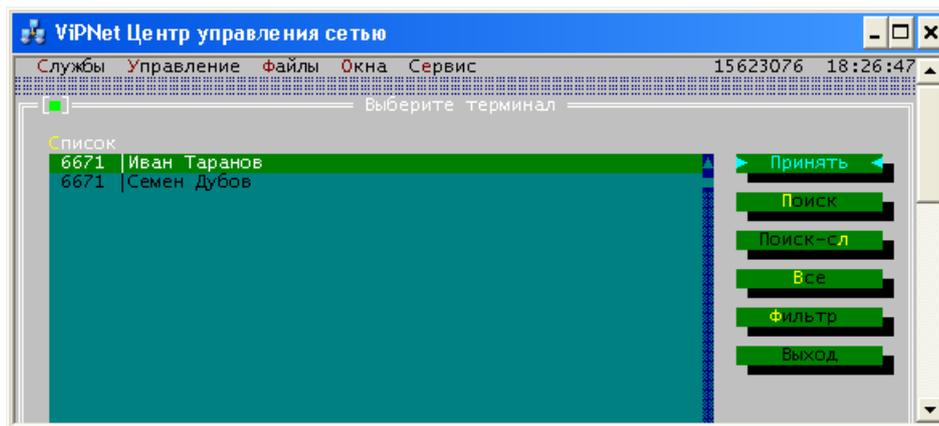


Рисунок 24

Выберите один или несколько АП-терминалов и нажмите кнопку **Принять**. АП отобразятся в окне **Список терминалов, для которых сервер является резервным** (Рисунок 23), что означает назначение выбранного сервера резервным сервером для этих АП.

Сменить резервный сервер Вы можете из окна регистрации в прикладной задаче **Терминал Спектр** или **Терминал Ареал-Сервис** (см. п.13.4.8).

Существует альтернативный способ задания резервного сервера IP-адресов (см. п.13.4.8).

13.4.2.5 Удаление резервного сервера для АП-терминала

Для того чтобы удалить резервный сервер для АП-терминала в окне регистрации в задаче **Сервер IP-адресов** (Рисунок 22) выберите сервер, который является резервным для АП-терминала, и нажмите кнопку **Резерв**. В открывшемся окне **Список терминалов, для которых сервер является резервным** (Рисунок 23) выберите АП-терминал и нажмите кнопку **Удалить**. После подтверждения удаления резервный сервер для выбранного АП-терминала будет удален.

13.4.3 Регистрация СМ в задаче «ViPNet Cluster»

В этой задаче могут быть зарегистрированы только СМ. Для регистрации воспользуйтесь пунктом меню групповой регистрации (см. раздел 13.4). Откроется окно **Регистрация в задаче «ViPNet Cluster»** (Рисунок 28).

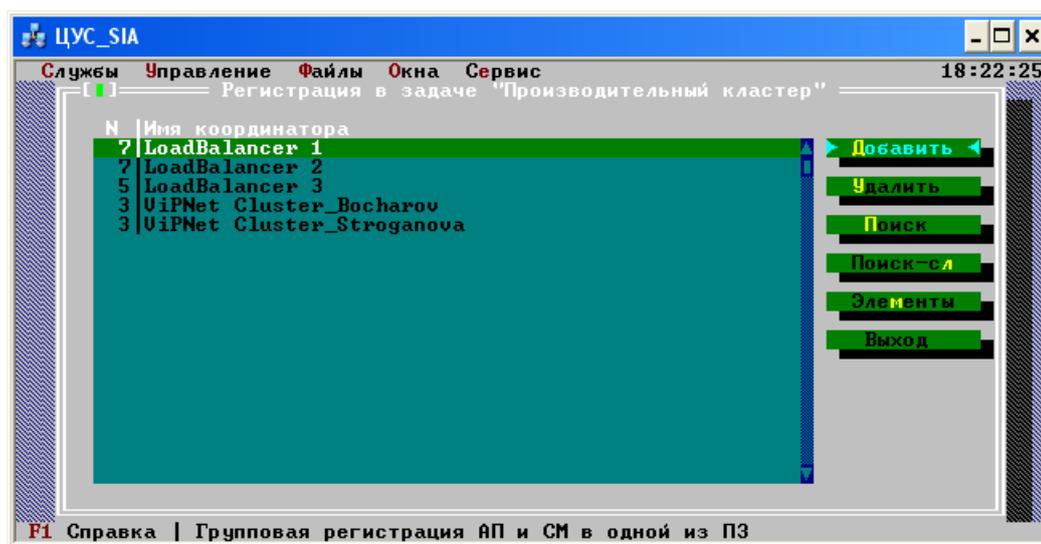


Рисунок 25

Для регистрации координатора необходимо нажать кнопку **Добавить** и из предложенного списка координаторов выбрать нужные, затем нажать кнопку **Принять**.

Для удаления регистрации в данной задаче необходимо выбрать нужные координаторы и нажать кнопку **Удалить**.

Чтобы задать максимальное число элементов кластера, выберите в списке нужный координатор и нажмите кнопку **Элементы**. В открывшемся окне укажите максимальное число элементов кластера. Максимальное число элементов кластера появится в колонке **N**.

Суммарное число элементов не может превосходить заданное в лицензии.

13.4.4 Регистрация АП в задаче «Деловая почта»

В этой ПЗ регистрируется только АП. Зарегистрировать АП в задаче **Деловая почта** можно обоими способами, указанными выше в разделах 13.3 и 13.4. Однако, если требуется задать полномочия для использования Деловой почты, нужно воспользоваться пунктом меню групповой регистрации (см. раздел 13.4). Откроется окно **Регистрация в задаче «Деловая почта»** (Рисунок 26).

Для регистрации узла необходимо нажать кнопку **Добавить** и из предложенного списка СУ выбрать нужные, затем нажать кнопку **Принять**.

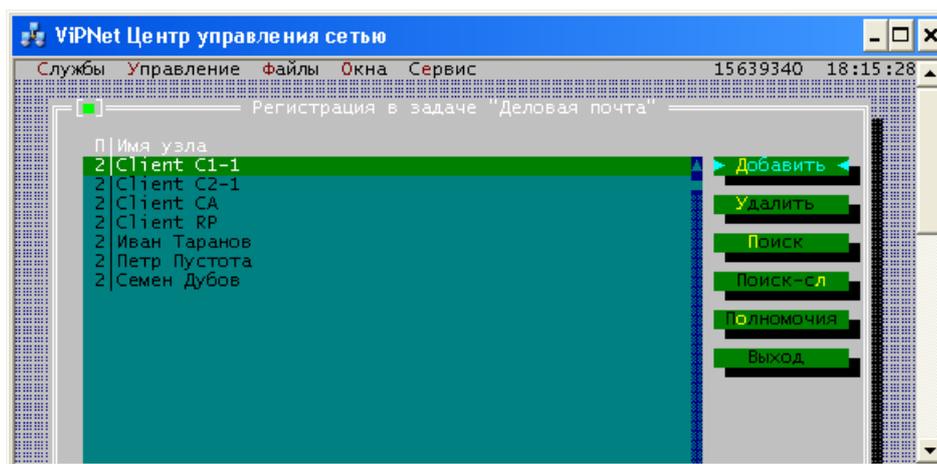


Рисунок 26

В прикладной задаче **Деловая почта** можно задать уровень полномочий пользователя для того или иного сетевого узла. Уровень полномочий определяет допустимость различных действий пользователей по изменению настроек в ViPNet Монитор и ViPNet MFTP на данном узле. По умолчанию присваивается уровень полномочий, указанный в окне настроек по умолчанию (пункт меню **Службы > Настройки по умолчанию**, см. п. 12).

Чтобы изменить уровень полномочий для одного или нескольких сетевых узлов, выберите эти узлы в списке и нажмите кнопку **Полномочия** (для выделения сетевого узла используйте клавишу «пробел»). В окне **Выбор уровня полномочий** установите один из четырех уровней: **Минимальный**, **Средний**, **Максимальный** и **Специальный**. При выборе пункта **Специальный** введите символ, обозначающий нужный уровень полномочий, в предусмотренное для это поле. Соответствие уровней полномочий функциональным возможностям программы описано в отдельном документе «Классификация полномочий».

Для удаления регистрации в данной задаче выберите один или несколько сетевых узлов и нажмите кнопку **Удалить**.

13.4.5 Регистрация в задаче «Центр регистрации»

В этой ПЗ регистрируется только АП. Зарегистрировать АП в задаче **Центр регистрации** можно обоими способами, указанными выше в разделах 13.3 и 13.4. Однако, если требуется задать ограничения на число запросов на дистрибутивы и сертификаты для пользователей, нужно воспользоваться пунктом меню групповой регистрации (см. раздел 13.4). Откроется окно **Регистрация в задаче «Центр регистрации»** (Рисунок 27).

Для регистрации узла необходимо нажать кнопку **Добавить** и из предложенного списка СУ выбрать нужные, затем нажать кнопку **Принять**.

Далее в этом окне выбрать ЦР, в котором Вы хотите ввести (или изменить) ограничения на количество запросов, нажать кнопку **Запросы**. Появится окно для ввода количества запросов на дистрибутивы и сертификаты (десятичные числа больше нуля) (Рисунок 27). Задайте нужные значения ограничений. Если ограничений на сертификаты нет (суммарное количество сертификатов внешних и внутренних пользователей не ограничено), то введите **-1** (минус единица). Если требуется полностью запретить создание запросов на сертификаты и (или) дистрибутивы в Центре регистрации, то введите **0**.

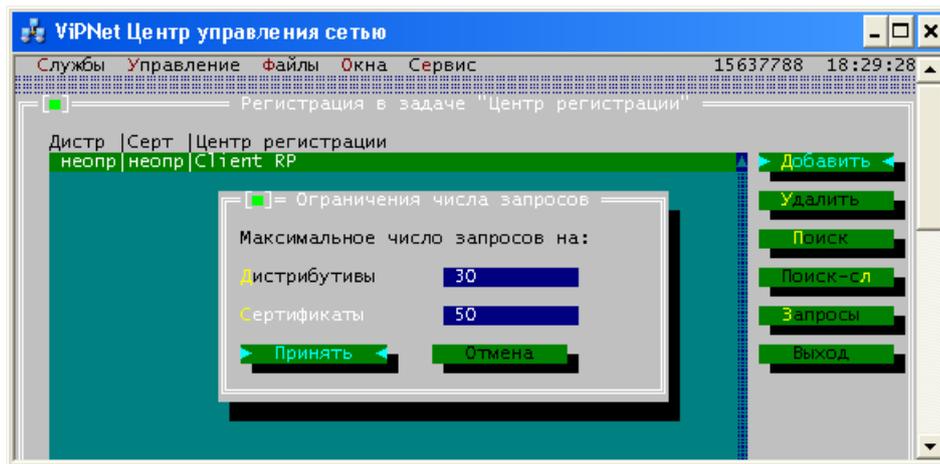


Рисунок 27

Далее нажать кнопку **Принять**. Заданные ограничения появятся в колонках **Дистр** и **Серт**, если не исчерпано общее количество для всех ЦР.

Замечание: Если в лицензии Вашей сети существуют ограничения на число сертификатов, то обязательно задайте ограничения на число запросов из Центра регистрации, чтобы избежать неожиданного завершения общего числа лицензий на сертификаты. При достижении максимального числа лицензий на сертификаты, запросы, поступившие из Центра регистрации, будут отклонены.

Для удаления регистрации в данной задаче необходимо выбрать нужные СУ и нажать кнопку **Удалить**.

13.4.6 Регистрация АП в задаче «Центр управления политиками»

В этой ПЗ регистрируется только АП. Зарегистрировать АП в задаче **Центр управления политиками** можно обоими способами, указанными выше в разделах 13.3 и 13.4. Однако для того, чтобы задать список управляемых узлов (домен) для Центра управления политиками безопасности (ЦУПБ), нужно воспользоваться пунктом меню групповой регистрации (см. раздел 13.4). Откроется окно **Регистрация в задаче «Центр управления политиками»** (Рисунок 28).

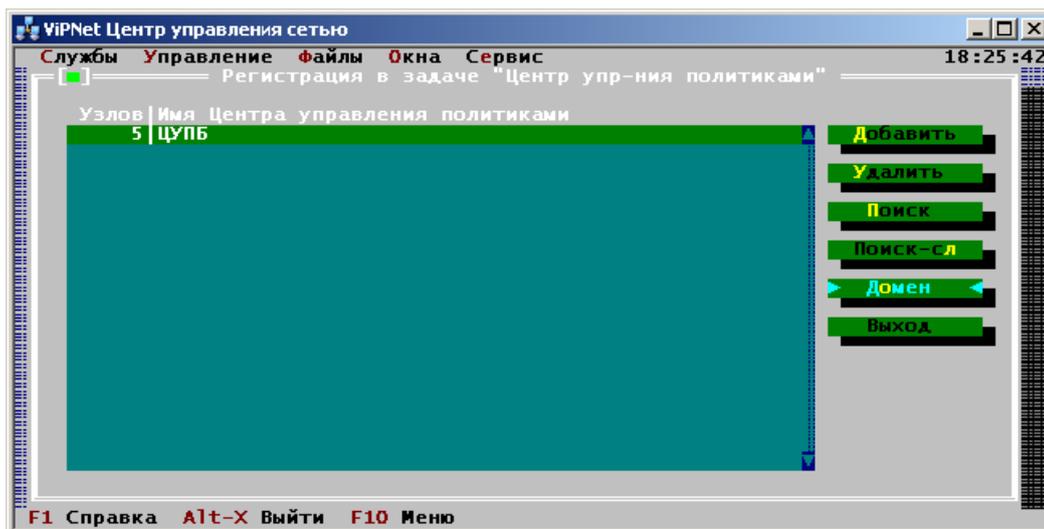


Рисунок 28

Для регистрации узла необходимо нажать кнопку **Добавить** и из предложенного списка СУ выбрать нужные, затем нажать кнопку **Принять**.

Для удаления регистрации в данной задаче необходимо выбрать нужные СУ и нажать кнопку **Удалить**.

Чтобы задать список узлов (домен), которыми может управлять некоторый ЦУПБ, выберите в списке нужный ЦУПБ и нажмите кнопку **Домен**. Появится окно со списком узлов, входящих в домен этого ЦУПБ (Рисунок 29).

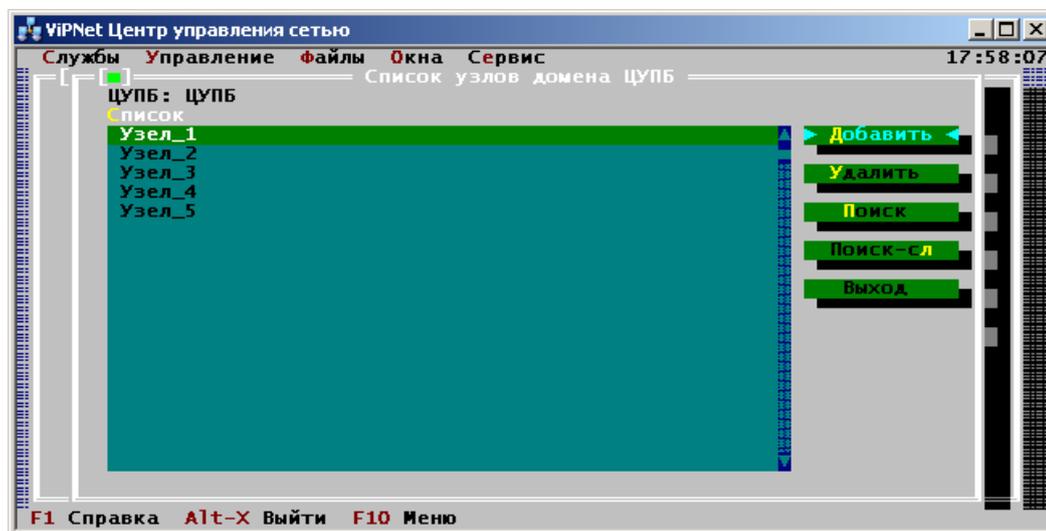


Рисунок 29

Для изменения домена используйте кнопки **Добавить** и **Удалить**, чтобы добавить/удалить узлы в/из домена. В домен нельзя включить:

- узлы, зарегистрированные в задаче *Центр управления политиками*;
- узлы, зарегистрированные в задачах терминалов;
- узлы, входящие в другие домены.

После изменения домена в колонке **Узлов** появится количество узлов, входящих в домен данного ЦУПБ, если не исчерпано общее количество управляемых узлов для всех ЦУПБ.

13.4.7 Регистрация АП в задаче "Сервер мониторинга"

В этой ПЗ регистрируются только АП. Для регистрации АП в задаче **Сервер мониторинга** нужно воспользоваться пунктом меню групповой регистрации (см. раздел 13.4). Откроется окно **Регистрация в задаче "Сервер Мониторинга"** (Рисунок 30).

Для регистрации узла необходимо нажать кнопку **Добавить** и из предложенного списка СУ выбрать нужные, затем нажать кнопку **Принять**.

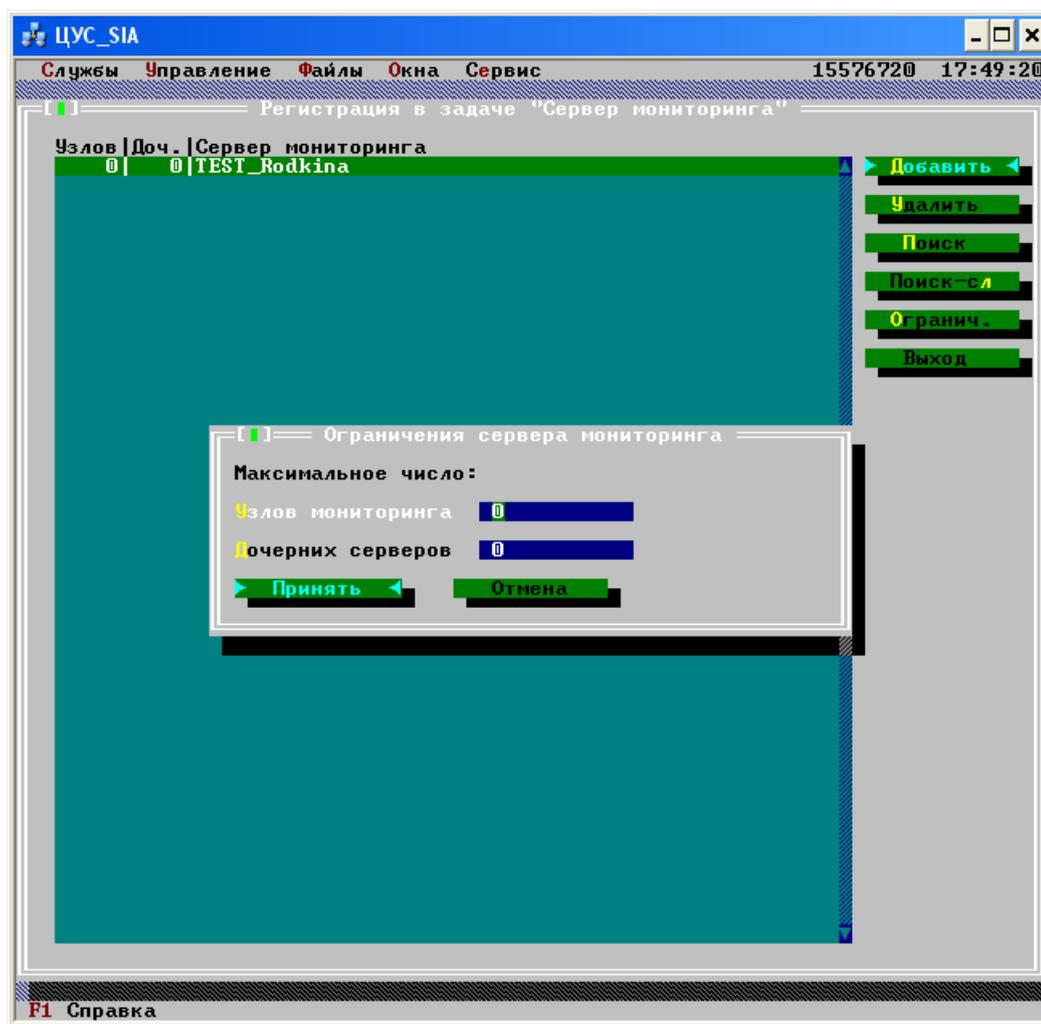


Рисунок 30

Чтобы задать ограничения сервера мониторинга, выберите в списке нужный сервер мониторинга и нажмите кнопку **Огранич.**. Появится окно для ввода максимального числа узлов мониторинга и дочерних серверов (Рисунок 30). По умолчанию в этих параметрах установлено значение 0. Это означает, что не разрешено ни одного узла мониторинга и дочернего сервера. Задайте нужные значения ограничений. Суммарное число узлов мониторинга, назначенных для всех Серверов Мониторинга, не должно превышать максимальное число узлов мониторинга в лицензии для Вашей сети. Суммарное число дочерних серверов мониторинга, назначенных для всех Серверов Мониторинга, не должно превышать максимальное число дочерних серверов мониторинга в лицензии для Вашей сети.

Далее нажмите кнопку **Принять**. Заданные ограничения появятся в колонках **Узлов** и **Доч.**, если не исчерпано общее количество для всех Серверов Мониторинга в лицензии для Вашей сети.

Для удаления регистрации в данной задаче необходимо выбрать нужные СУ и нажать кнопку **Удалить**.

13.4.8 Регистрация АП в задачах "Терминал Спектр" и "Терминал Ареал-Сервис"

В этих задачах могут быть зарегистрированы только АП. Для регистрации АП необходимо нажать кнопку **Добавить** (Рисунок 31) и из предложенного списка абонентских пунктов выбрать нужные АП, затем нажать кнопку **Принять**.

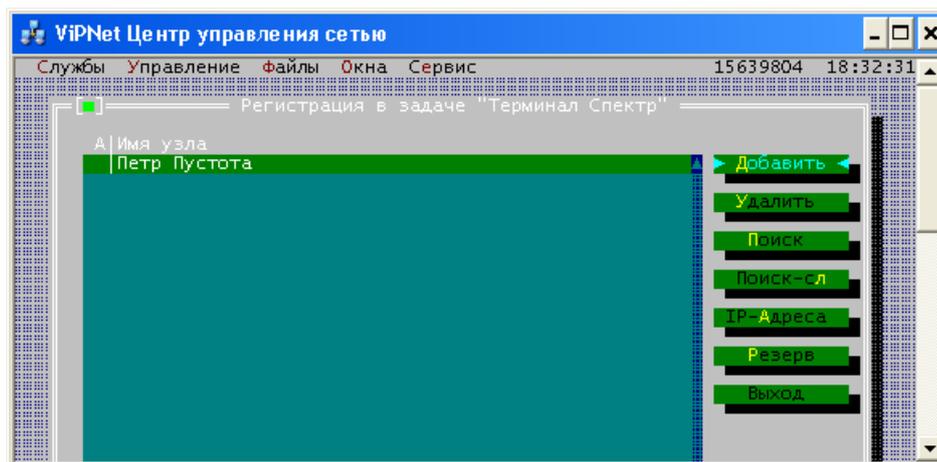


Рисунок 31

Удаление регистрации в прикладной задаче:

Для удаления регистрации в данной задаче необходимо выбрать нужные СУ и нажать кнопку **Удалить**.

Задание IP-адресов:

Нажав кнопку **IP-Адреса**, можно для выбранного АП произвести различные настройки (задать один или несколько IP-адресов, и т.д.). После задания адресов в колонке **А** появится "+". При задании адресов следует руководствоваться правилами, описанными ниже в разделе 13.5 и его подразделах. Рекомендуем произвести все необходимые настройки в программе ViPNet ЦУС, чтобы избежать дополнительных ручных настроек на каждом СУ сети.

Задание резервного сервера IP-адресов:

Для абонентских пунктов, зарегистрированных в прикладных задачах **Терминал Спектр** или **Терминал Ареал-Сервис**, существует возможность задать резервный сервер IP-адресов.

Для задания резервного сервера IP-адресов в окне регистрации в прикладной задаче **Терминал Спектр** или **Терминал Ареал-Сервис** выберите АП и нажмите кнопку **Резерв** (Рисунок 31). Если для АП резервный сервер IP-адресов еще не был выбран, то появится окно со списком серверов IP-адресов (т.е. координаторов, зарегистрированных в прикладной задаче **Сервер IP-адресов**) своей и доверенных сетей, кроме сервера, на котором зарегистрирован выбранный АП (Рисунок 32). Один из серверов Вы можете выбрать в качестве резервного сервера IP-адресов.

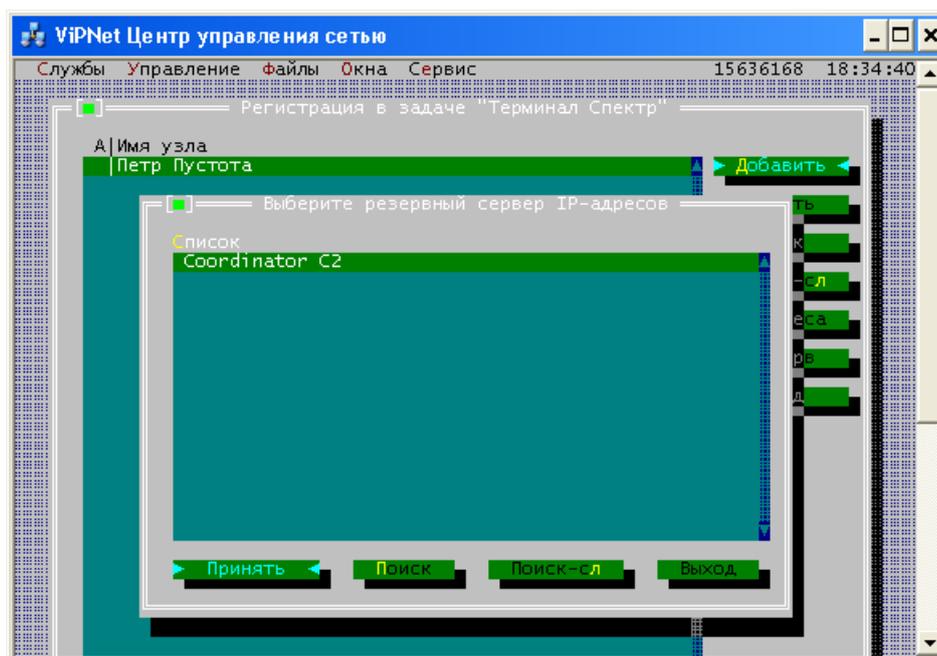


Рисунок 32

Выберите сервер и нажмите кнопку **Принять**. Выбранный сервер станет резервным для АП.

Смена резервного сервера:

Если резервный сервер IP-адресов уже был выбран, то при нажатии на кнопку **Резерв** появится сообщение с именем этого сервера и будет предоставлена возможность сменить сервер при помощи кнопки **Сменить сервер** (Рисунок 33).

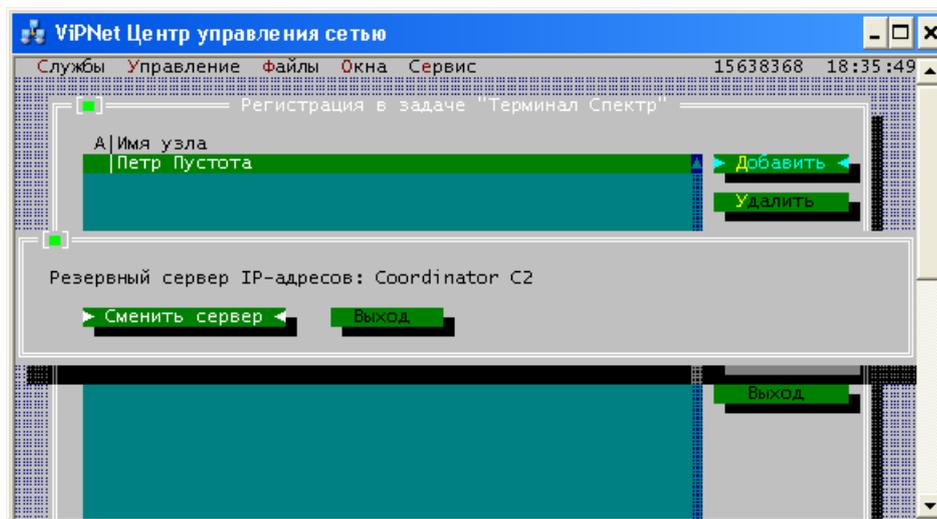


Рисунок 33

Резервный сервер IP-адресов можно настроить и из окна регистрации в задаче **Сервер IP-адресов** (см. п. 13.4.2.4). Из этого же окна можно удалить резервный сервер для АП (см. п. 13.4.2.5).

13.4.9 Регистрация АП в прикладной задаче «ViPNet Terminal»

В данной прикладной задаче могут быть зарегистрированы только абонентские пункты. Для регистрации абонентских пунктов в задаче нажмите кнопку **Добавить**, выберите нужные АП из предложенного списка, затем нажмите кнопку **Принять**.

Чтобы отменить регистрацию абонентских пунктов в данной задаче, выбрать нужные АП в списке и нажмите кнопку **Удалить**.

Задание IP-адресов:

Нажав кнопку **IP-Адреса**, можно задать для выбранного абонентского пункта параметры доступа к терминальному серверу. Для этого в список IP-адресов добавьте строку вида:

T:protocol:address, где:

protocol — протокол доступа к терминальному серверу. Допустимые значения: **rdp**, **citrix**, **http**, **https**.

address — адрес терминального сервера.

Если параметр **protocol** имеет значение **rdp** или **citrix**, в качестве значения параметра **address** можно указать IP-адрес, DNS-имя или идентификатор сетевого узла терминального сервера. Например: **T:rdp:1A0F000A**.

Если параметр **protocol** имеет значение **http** или **https**, в качестве значения параметра **address** следует указать адрес URL. Например: **T:http:server.ru/app** или **T:http://server.ru/app**.

Адрес терминального сервера может быть задан на сервере-маршрутизаторе терминала (см. п. 13.7.6), при этом приоритет имеет адрес, настроенный в прикладной задаче «ViPNet Terminal».

Рекомендуется также добавить в список IP-адресов строку **DYN:SRV**, чтобы настроить терминал для работы с использованием типа межсетевого экрана **C динамической трансляцией адресов**.

Задание уровня полномочий пользователя:

Для абонентских пунктов, зарегистрированных в прикладной задаче ViPNet Terminal, можно задать уровень полномочий при доступе к терминальному серверу по протоколам ICA (Citrix) и HTTP(S), а также разрешить или запретить перенаправление различных устройств при работе в терминальной сессии.

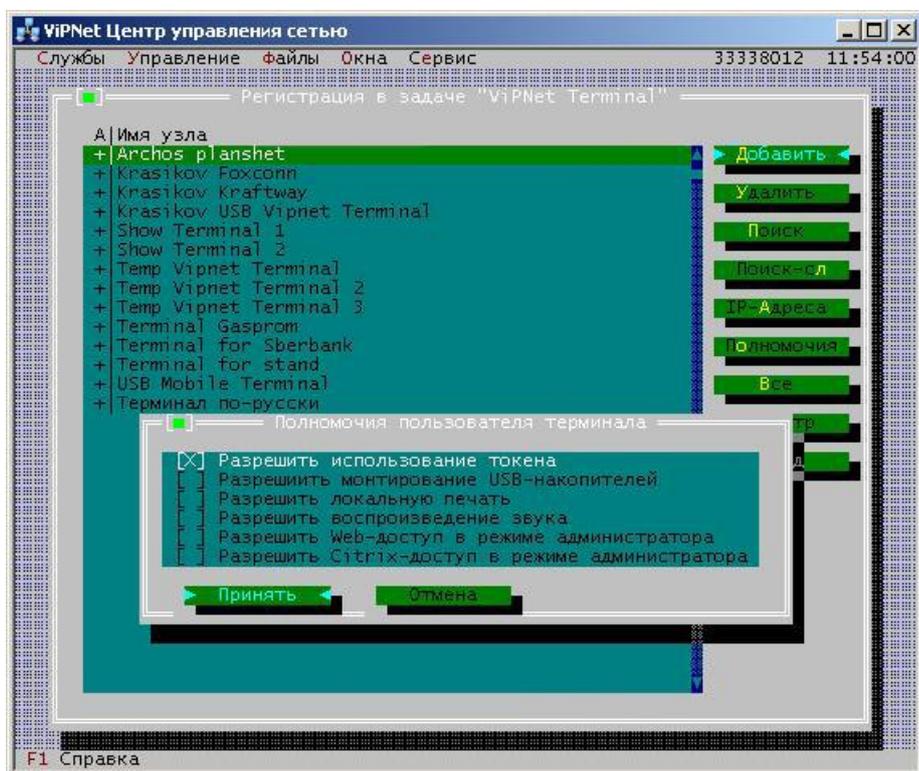


Рисунок 34

Чтобы задать уровень полномочий, выберите в списке один или несколько абонентских пунктов и нажмите кнопку **Полномочия**. В окне **Полномочия пользователя терминала** установите или снимите нужные флажки:

Разрешить использование токена — для использования устройств аутентификации. По умолчанию включено.

Разрешить монтирование USB-накопителей — для использования съемных USB-накопителей, подключенных к терминалу. По умолчанию отключено.

Разрешить локальную печать — для использования принтера, подключенного к терминалу. По умолчанию отключено.

Разрешить воспроизведение звука — для воспроизведения звука на терминале. По умолчанию отключено.

Разрешить Web-доступ в режиме администратора — полномочия администратора при подключении по протоколам HTTP и HTTPS. По умолчанию отключено.

В режиме администратора можно открыть несколько окон браузера, доступны меню и адресная строка. В режиме пользователя открывается только одно окно браузера в полноэкранный режим, меню и адресная строка недоступны.

Разрешить Citrix-доступ в режиме администратора — полномочия администратора при подключении по протоколу ICA (Citrix). По умолчанию отключено.

В режиме администратора на терминале локально запускается клиент Citrix, в котором можно задать терминальные серверы и настроить параметры подключения. В режиме пользователя выполняется автоматическое подключение к удаленному рабочему столу по протоколу ICA.

Задав необходимые полномочия, нажмите кнопку **Принять**.

13.4.10 Регистрация во всех остальных задачах

Для регистрации АП в какой-либо задаче из неописанных выше, Вы можете выбрать любой из способов, указанных выше в разделах 13.3 и 13.4.

Для регистрации СМ, или если для СУ необходимо задать полномочия или другие параметры, нужно воспользоваться способом из раздела 13.4, т.е.:

выбрать пункт меню Службы/Групповая регистрация узлов в задачах,

выбрать прикладную задачу,

в открывшемся окне для регистрации узла нажать кнопку **Добавить**,

из предложенного списка СУ выбрать нужные СУ,

нажать кнопку **Принять**.

Внимание! Если сетевые узлы зарегистрированы в ПЗ **ViPNet SDK**, **КриптоСервис** или **Криптофайл**, то для них должно выполняться следующее условие: каждый пользователь должен быть зарегистрирован только в одном единственном типе коллектива, областью действия которого является один единственный сетевой узел.

В окне для регистрации узла для разных задач можно настроить следующее:

Для задачи **КриптоСервис** можно задать полномочия, аналогично п. 13.4.4.

Для АП, зарегистрированных в задаче **Секретный диск**, уровень полномочий совпадает с полномочиями в задаче **Защита трафика**. Если АП не зарегистрирован в задаче **Защита трафика**, то полномочия максимальные. Для СМ, зарегистрированных в задаче **Секретный диск** уровень полномочий всегда максимальный.

Для задач терминалов АСУ «Экспресс-3», **Coordinator HW100-A, B, C**, **Coordinator HW1000**, **Coordinator HW2000** можно задать различные дополнительные настройки (см. далее, п. 13.5). Для

координаторов, зарегистрированных в задачах **Coordinator HW1000** или **Coordinator HW2000**, можно задать максимальное число адресов для туннелирования (см. п. 13.4.2.3).

Для задачи **Web-шлюз** можно задать число адресов, нажав кнопку **Адреса**.

13.5 Порядок настройки различных параметров сетевых узлов

После того, как структура Вашей сети сформирована, Вы можете производить настройки двух групп параметров сетевых узлов:

Настройку параметров подключения узлов к сети:

- * Настройку IP-адресов и DNS-имен сетевых узлов.
- * Выбор сервера IP-адресов для АП.
- * Настройку параметров работы СУ через межсетевой экран.

Задание IP-адресов туннелируемых координаторами ресурсов.

Настройки могут производиться для узлов, зарегистрированных в задачах: **Защита трафика**, **Сервер IP-адресов**, **Coordinator HW100-A, B, C**, **Coordinator HW1000**, **Coordinator HW2000**, задачах для терминалов АСУ «Экспресс-3».

Эти настройки необходимы для обеспечения установления соединения между узлами сети ViPNet и соединений с внешней сетью без каких-либо ручных настроек ПО ViPNet на самих сетевых узлах. Рекомендуем произвести все настройки в программе ViPNet ЦУС, чтобы избежать ручных настроек на каждом сетевом узле сети.

В процессе эксплуатации сети ViPNet, настройки можно изменять. Также предоставляется возможность указать конфигурации СУ, в которые должны быть загружены новые настройки.

Внимание! Если в процессе эксплуатации сети ViPNet в программе ЦУС были изменены настройки СУ – параметры подключения СУ и/или его туннелируемые адреса, то при обновлении справочников на узлах сети, измененные настройки всегда заменяют настройки этого СУ из соответствующей группы параметров, заданные на узлах вручную. Например, если в ЦУС Вы изменили только список туннелируемых ресурсов для некоторого координатора, то новый список применится на всех узлах. При этом настройки из другой группы параметров заменены не будут.

Настройки задаются путем добавления специальных строк для записей сетевых узлов.

Для настройки параметров сетевых узлов откройте окно регистрации в соответствующей задаче при помощи команды меню **Службы/Групповая регистрация узлов в задачах**. Далее выберите название прикладной задачи:

для настройки ViPNet Coordinator Монитор на координаторе нужно выбрать прикладную задачу **Сервер IP-адресов**.

для настройки ViPNet Client Монитор на АП нужно выбрать прикладную задачу **Защита трафика**.

для настройки ViPNet Client Монитор на АП, зарегистрированном в одной из задач для терминалов АСУ «Экспресс-3», нужно выбрать прикладную задачу с соответствующим названием.

для настройки ViPNet Coordinator HW100 на координаторе нужно выбрать прикладную задачу **Coordinator HW100-A, B, C**.

для настройки ViPNet Coordinator HW1000 или ViPNet Coordinator HW2000 на координаторе нужно выбрать прикладную задачу **Coordinator HW1000** или **Coordinator HW2000** соответственно.

Затем нажмите кнопку **Регистрация**.

В открывшемся окне выберите СУ и нажмите кнопку **IP-адреса**. Появится окно **IP-адреса** (Рисунок 35).

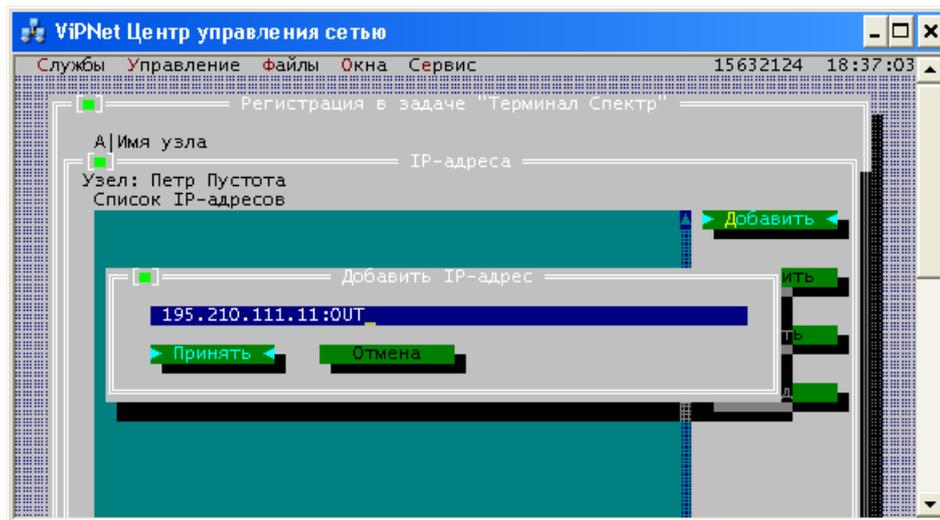


Рисунок 35

В этом окне нажмите кнопку **Добавить**, затем в появившейся строке ввода (Рисунок 35) введите необходимую строку настроек и нажмите **Принять**.

Рекомендации по настройке параметров сетевых узлов при помощи специальных строк читайте в разделе 13.6. Краткое описание формата строк приведено в п. 13.5.1.

Вы можете добавить нужное количество строк, каждый раз выполняя команду **Добавить**. Все добавленные строки отобразятся в окне **IP-адреса**.

В этом же окне параметры можно изменить (кнопка **Изменить**) или удалить (кнопка **Удалить**).

13.5.1 Краткое описание формата строк, используемых для настройки

В этом разделе приведено краткое описание форматов строк, которые могут быть заданы в ЦУС для обеспечения различных автоматических настроек ПО ViPNet на сетевых узлах. Заданные строки помещаются в состав адресных справочников сетевого узла.

О настройке параметров сетевых узлов при помощи этих строк читайте в разделе 13.6.

Внимание! Все параметры строки указываются друг за другом без пробелов.

Строки, определяющие адреса и порты UDP:

№	Формат строки	Пример строки	Описание
1.	АДРЕС	195.210.139.67	Строка определяет реальный IP-адрес компьютера.
2.	АДРЕС:ПОРТ:FIX	195.210.139.67:4321 или 195.210.139.67:OUT или 195.210.139.67:4321:FIX	Строка определяет: <ul style="list-style-type: none"> АДРЕС – IP-адрес доступа к сетевому узлу через межсетевой экран. ПОРТ – порт доступа к сетевому узлу через межсетевой экран. Параметр ПОРТ может иметь определенный номер порта или значение OUT . OUT – порт доступа по умолчанию – 55777. <ul style="list-style-type: none"> Параметр :FIX является необязательным параметром. Наличие :FIX означает, что на сетевом узле в программе ViPNet Монитор при выборе типа МЭ Со статической трансляцией адресов зафиксирован внешний IP-адрес доступа через МЭ, указанный в параметре АДРЕС.

3.	E:АДРЕС1- АДРЕС2:ПОРТ:FIX	E:195.210.139.44- 195.210.135.56:OUT	<p>Строка задается только для координатора. Строка используется для автоматической настройки из ЦУС параметров подключения координатора к сети.</p> <p>Строка определяет:</p> <ul style="list-style-type: none"> • АДРЕС1 – IP-адрес внешнего сетевого интерфейса координатора. • АДРЕС2 – IP-адрес доступа к координатору через МЭ. Значение АДРЕС2 должно быть равно 0.0.0.0, если данный параметр неизвестен или в нем нет необходимости. • ПОРТ – порт доступа к координатору через МЭ. Параметр ПОРТ может иметь определенный номер порта или значение OUT. OUT – порт доступа по умолчанию – 55777. • Параметр :FIX является необязательным параметром. Наличие :FIX означает, что на сетевом узле в программе ViPNet Coordinator Монитор при выборе типа МЭ Со статической трансляцией адресов зафиксирован внешний IP-адрес доступа через МЭ, указанный в параметре АДРЕС2. Если значение АДРЕС2 равно 0.0.0.0, то параметр :FIX использовать нельзя. <p>Для координатора строка такого формата должна быть только одна.</p>
4.	DNS://DNS- имя:ПОРТ	DNS://www.infotecs- vpn.info:OUT	<p>Строка задается в случае, если собственный адрес узла или адрес МЭ, который он использует, динамически меняется.</p> <p>Параметр :ПОРТ – необязательный.</p> <ul style="list-style-type: none"> • Если :ПОРТ не задан, то строка DNS://DNS-имя задает собственное DNS-имя узла. • Если :ПОРТ задан, то строка DNS://DNS-имя:ПОРТ задает DNS-имя и порт доступа через МЭ.
5.	S:АДРЕСА	S:178.136.121.10 S:178.136.121.12- 178.136.121.33 S:178.136.121.56- 178.136.122.212 S:178.136.122.215; 178.136.122.218	<p>Строка задается только для координатора.</p> <p>Строка определяет туннелируемые адреса координатора:</p> <p>АДРЕСА – туннелируемые адреса координатора задаются в виде адреса или диапазона адресов в одной или нескольких строках, начинающихся с S:.</p> <p>Адреса и диапазоны можно задавать одной строкой, разделяя их "точкой с запятой" (;).</p>

Специальные строки:

Строки для групповой настройки параметров абонентских пунктов координатора, который является для них сервером IP-адресов. Строки задаются только для координаторов.

№	Формат строки	Описание
1.	NOPROXY_AP	Наличие такой настройки у ViPNet-координатора означает, что на

		абонентских пунктах, для которых данный координатор является сервером IP-адресов, после установки и запуска ViPNet Client Монитор, по умолчанию выберется работа без использования МЭ.
2.	REQUEST_AP	Наличие такой настройки у ViPNet-координатора означает, что на абонентских пунктах, для которых данный координатор является сервером IP-адресов, после установки и запуска ViPNet Client Монитор, по умолчанию задается вопрос о желании использовать данный координатор в качестве МЭ. При отказе, на АП будет выбрана работа без использования МЭ.
3.	DYN_AP:SRV	Наличие такой настройки у ViPNet-координатора означает, что на абонентских пунктах, для которых данный координатор является сервером IP-адресов, после установки и запуска ViPNet Client Монитор, по умолчанию будет выбрано использование МЭ С динамической трансляцией адресов . Параметр :SRV является необязательным параметром. Наличие :SRV означает, что весь трафик АП с внешними узлами будет направляться только через данный ViPNet-координатор.
4.	STAT_AP	Наличие такой настройки у ViPNet-координатора означает, что на абонентских пунктах, для которых данный координатор является сервером IP-адресов, после установки и первого запуска ViPNet Client Монитор, будет выбрано использование МЭ Со статической трансляцией адресов .

Строки для индивидуальной настройки сетевых узлов. Индивидуальные настройки имеют приоритет перед групповыми настройками.

1.	NOPROXY	Строка задается только для АП. Наличие такой настройки у АП означает, что на этом АП в ViPNet Client Монитор будет выбрана работа без использования МЭ.
2.	PROXY	Строка задается только для АП. Наличие такой настройки у АП означает, что на этом АП в ViPNet Client Монитор должен быть выбран в качестве МЭ – ViPNet-координатор .
3.	REQUEST	Строка задается только для АП. Наличие такой строки у АП означает, что на АП, при первом запуске ViPNet Client Монитор задается вопрос о желании использовать в качестве МЭ ViPNet-координатор.
4.	DYN:SRV	Наличие такой настройки у сетевого узла означает, что на этом узле (АП или координаторе) в программе ViPNet Монитор будет выбрано использование МЭ С динамической трансляцией адресов . Параметр :SRV является необязательным параметром. Наличие :SRV означает, что весь трафик АП с внешними узлами будет направляться только через выбранный координатор для организации входящих соединений. Для координатора эта строка действует только при наличии строки формата Е:АДРЕС1-АДРЕС2:ПОРТ:FIX .
5.	NODYN	Строка задается только для АП. Наличие такой настройки у АП означает, что на этом АП в ViPNet Client Монитор не будет выбрано использование МЭ С динамической трансляцией адресов .
6.	TIMEOUT:N	Наличие такой настройки у сетевого узла означает, что на сетевом узле в

		<p>программе ViPNet Монитор, в случае использования МЭ С динамической трансляцией адресов, период опроса координатора для обеспечения пропускания входящего трафика будет равен N секундам.</p> <p>Например, TIMEOUT:40</p> <p>Отсутствие данной строки у сетевого узла означает, что период опроса равен 25 секундам.</p>
7.	STAT:ПОРТ	<p>Строка задается только для АП.</p> <p>Наличие такой настройки у АП означает, что на этом АП в ViPNet Client Монитор будет выбрано использование МЭ Со статической трансляцией адресов.</p> <p>Параметр :ПОРТ является необязательным параметром. Параметр указывается, если к данному АП доступ осуществляется через порт, отличный от порта с номером 55777.</p>
8.	PRID=ID	<p>ID – идентификатор ViPNet-координатора.</p> <p>Наличие такой настройки у сетевого узла означает, что данный узел будет использовать координатор с указанным идентификатором для работы с узлами, находящимися во внешней сети.</p> <p>Для АП строку следует задавать, если в качестве такого координатора нужно выбрать иной координатор, чем сервер IP-адресов этого АП.</p>
9.	IPID=ID	<p>Строка задается только для АП.</p> <p>ID – идентификатор ViPNet-координатора.</p> <p>Наличие такой строки у абонентского пункта означает, что на АП в качестве сервера IP-адресов будет выбран координатор с указанным идентификатором.</p> <p>Строку следует задавать, если для АП в качестве сервера IP-адресов нужно выбрать иной координатор, чем по умолчанию. По умолчанию сервером IP-адресов для АП является координатор, на котором этот АП зарегистрирован в ЦУС.</p>

Выбор на СУ конфигурации программы ViPNet Монитор для загрузки настроек:

Параметры, заданные при помощи строк, могут быть применены на сетевых узлах для разных конфигураций программы ViPNet Монитор.

Если перед строкой не указан символ **KNо:**, то строка должна быть загружена для всех конфигураций программы ViPNet Монитор на компьютере.

Для некоторых специальных конфигураций можно сделать отдельное обновление. Сейчас есть две такие конфигурации для каждого пользователя: **Основная** и **Открытый Интернет**.

Номера конфигураций имеют смысл только для существующей на узле конфигурации. Если такой конфигурации нет, то строка игнорируется.

Если требуется обеспечить обновление некоторой строки только для конкретной конфигурации, то в начале такой строки следует указать **KNо:**, где **№** может принимать значение 0 или 1:

K0: – строка действует на основные конфигурации всех пользователей узла.

K1: – строка действует на конфигурации **Открытый Интернет** всех пользователей узла.

Например:

K1:АДРЕС:ПОРТ

– означает, что данная строка должна загрузиться только для конфигурации **Открытый Интернет**. Конкретно этой строкой может быть задано, что данный АП в конфигурации **Открытый Интернет** должен использовать в качестве МЭ ViPNet-координатор, имеющий адрес "АДРЕС".

Или:

K1:NOPROXY_ AP

– это означает, что АП в конфигурации **Открытый Интернет** не будет использовать в качестве МЭ ViPNet-координатор, являющийся его сервером IP-адресов.

13.6 Рекомендации по настройке параметров сетевых узлов в зависимости от требуемой конфигурации

Все форматы строк, использованные ниже, описаны в п. 13.5.1.

Информацию о параметрах СУ (адресах, МЭ и параметрах настроек ПО ViPNet) Вы можете получить у сетевого администратора Вашей организации.

Задавать IP-адреса и DNS-имена необходимо, как правило, только для ViPNet-координаторов, причем DNS-имена имеет смысл задавать для координаторов, имеющих динамически изменяющийся IP-адрес.

Если для координаторов планируется автоматически установить определенные параметры работы с внешней сетью, то для таких координаторов следует обязательно задать все адреса доступа и специальные строки в соответствии с разделом 13.7.1 (в зависимости от способа подключения к внешней сети). Для правильных автоматических настроек параметров работы с внешней сетью, для координатора необходимо задать весь требуемый набор строк.

Если координаторы планируется настраивать вручную непосредственно на самом узле, то для таких координаторов необходимо и достаточно задать все адреса доступа к координатору, чтобы другие узлы смогли соединиться с ним. В этом случае произведите настройки в соответствии с разделом 13.7.3.

Если координатор должен осуществлять туннелирование открытых ресурсов, то для того чтобы не производить ручные настройки туннелируемых адресов непосредственно на координаторах, выполните настройки этих адресов в соответствии с разделом 13.7.4.

На АП настройки строк и адресов следует выполнять в следующих ситуациях:

По умолчанию сервером IP-адресов и межсетевым экраном для АП является координатор, на котором этот АП зарегистрирован в ЦУС. Таким образом, АП будет иметь указанные настройки, если для АП не заданы никакие строки, как для групповой настройки, так и для индивидуальной. Об адресах и настройках других узлов АП узнают автоматически после соединения со своим сервером IP-адресов.

Если все или большинство АП, зарегистрированных в ЦУС на одном и том же координаторе, являющемся их сервером IP-адресов, должны быть настроены иным способом, чем по умолчанию, то для таких АП нужно произвести общую настройку на их координаторе с помощью специальных строк. Выполните настройки в соответствии с описанием, приведенном в разделе 13.7.5.

Если для отдельных АП требуется задать другие настройки, то нужно произвести индивидуальные настройки каждого АП с помощью специальных строк в соответствии с описанием, приведенном в разделе 13.8.

Замечание: Информацию о способах подключения узлов к внешней сети и параметрах настройки работы с сетью Вы можете прочитать в документации к ПО ViPNet Coordinator и ViPNet Client.

13.7 Настройка Координаторов

13.7.1 Автоматическая настройка параметров подключения координатора к внешней сети

Внимание! Для правильных автоматических настроек параметров работы с внешней сетью, для координатора необходимо задать весь требуемый набор строк.

13.7.1.1 Настройка параметров подключения координатора без использования межсетевого экрана

Если координатор имеет непосредственное подключение к внешней сети, т.е. может быть доступен напрямую со стороны любых других СУ, например, имеет публичный адрес, то для такого координатора следует настроить подключение без использования межсетевого экрана.

Для координатора произведите следующие настройки:

1. Задайте все доступные адреса сетевых интерфейсов координатора:

Если адреса статические, то задайте строки в формате:

АДРЕС, например, 195.210.139.67.

Если адреса динамически меняются, то координатор должен быть зарегистрирован на DNS-сервере. Задайте DNS-имя в строке формата:

DNS://DNS-имя, например, DNS://www.infotecs-vpn.info.

При таких настройках на координаторе в программе ViPNet Coordinator Монитор будет установлен режим работы без использования МЭ (в окне **Настройки** флажок **Использовать межсетевой экран** снят). ViPNet-координатор сам может быть использован в качестве МЭ другими узлами.

13.7.1.2 Настройка параметров подключения координатора через МЭ ViPNet-Координатор

Если координатор будет использовать в качестве МЭ другой ViPNet-координатор, то для координатора произведите следующие настройки:

1. Задайте все доступные адреса сетевых интерфейсов координатора:

Если адреса статические, то задайте строки в формате:

АДРЕС, например, 195.210.139.67.

Если адреса динамически меняются, то координатор должен быть зарегистрирован на DNS-сервере. Задайте DNS-имя в строке формата:

DNS://DNS-имя, например, DNS://www.infotecs-vpn.info.

2. Задайте параметры подключения координатора через МЭ **ViPNet-координатор** в строке формата:

E:АДРЕС1-АДРЕС2:ПОРТ (такая строка должна быть только одна), где

В поле **АДРЕС1** указывается реальный адрес внешнего сетевого интерфейса координатора. Если задать адрес в данной строке, то этот адрес можно не задавать в строке формата **АДРЕС** на предыдущем шаге.

В поле **АДРЕС2** укажите значение 0.0.0.0, т.к. при настройке подключения координатора через МЭ **ViPNet-координатор** этот параметр не используется.

В поле **ПОРТ** укажите значение **OUT**, что означает номер порта 55777, или при необходимости любой другой номер порта.

3. Задайте ViPNet-координатор, который будет использоваться в качестве МЭ, в строке формата: **PRID=ID**, где

ID - идентификатор координатора, выполняющего функции МЭ. Идентификатор координатора Вы можете посмотреть при помощи команды меню **Службы/Просмотр конфигурации сети/Структура сети в узком формате**. Откроется отчет о структуре сети, отсортированный по номерам сети, координаторам и зарегистрированным на них АП. Этот отчет автоматически сохраняется в файле STRUCT.REP рабочего каталога ЦУС. В открывшемся окне или в файле STRUCT.REP найдите имя нужного координатора, и в строке **СМ**: в последней колонке посмотрите значение идентификатора.

При таких настройках на координаторе в программе ViPNet Coordinator Монитор в окне **Настройки** будет автоматически установлен тип МЭ **ViPNet-координатор** и выбран указанный координатор.

13.7.1.3 Настройка параметров соединения координатора через МЭ со статической трансляцией

Если координатор будет использовать в качестве МЭ некоторое устройство (или МЭ), на котором доступна настройка статических правил трансляции адресов, то для координатора произведите следующие настройки:

1. Задайте все доступные адреса сетевых интерфейсов координатора:

Если адреса статические, то задайте строки в формате:

АДРЕС, например, 195.210.139.67.

Если адреса динамически меняются, то координатор должен быть зарегистрирован на DNS-сервере. Задайте DNS-имя в строке формата:

DNS://DNS-имя, например, DNS://www.infotecs-vpn.info.

2. Задайте параметры подключения координатора через МЭ со статической трансляцией адресов в строке формата:

E:АДРЕС1-АДРЕС2:ПОРТ:FIX (такая строка должна быть только одна), где

В поле **АДРЕС1** указывается реальный адрес внешнего сетевого интерфейса координатора. Если задать адрес в данной строке, то этот адрес можно не задавать в строке формата **АДРЕС** на предыдущем шаге.

В поле **АДРЕС2** указывается адрес МЭ, через который будет осуществляться доступ к координатору со стороны внешних узлов.

Если адрес динамически меняется, то в поле **АДРЕС2** укажите значение 0.0.0.0, а адрес доступа задайте при помощи другой строки формата:

DNS://DNS-имя:ПОРТ, где

DNS-имя задает DNS-имя МЭ, **:ПОРТ** – см. ниже.

Если координатор имеет несколько адресов доступа с различных сетевых узлов, то остальные адреса Вы можете задать при помощи дополнительных строк (см. п. 13.7.2).

В поле **ПОРТ** указывается номер порта, который задан в настройках МЭ для обеспечения доступа к координатору со стороны внешних узлов. Вы можете указать **OUT**, что означает номер порта 55777, или при необходимости любой другой номер порта.

Параметр **:FIX** является необязательным параметром. Укажите этот параметр, если следует зафиксировать внешний адрес доступа к координатору через межсетевой экран. В этом случае на координаторе в программе ViPNet Coordinator Монитор в окне **Настройки** установится флажок **Зафиксировать внешний адрес доступа через межсетевой экран**.

Замечание: Указывать параметр **:FIX** рекомендуется только в случаях, когда все внешние узлы должны направлять свои IP-пакеты непосредственно через указанный внешний адрес доступа к координатору.

При таких настройках на координаторе в программе ViPNet Coordinator Монитор в окне **Настройки** будет автоматически установлен тип МЭ **Со статической трансляцией адресов** и выбраны заданные параметры.

13.7.1.4 Настройка параметров соединения координатора через МЭ с динамической трансляцией

Если координатор будет использовать в качестве МЭ некоторое устройство (или МЭ), на котором затруднительно настроить статические правила трансляции, то для координатора произведите следующие настройки:

1. Задайте все доступные адреса сетевых интерфейсов координатора:

Если адреса статические, то задайте строки в формате:

АДРЕС, например, 195.210.139.67.

Если адреса динамически меняются, то координатор должен быть зарегистрирован на DNS-сервере. Задайте DNS-имя в строке формата:

DNS://DNS-имя, например, DNS://www.infotecs-vpn.info.

2. Задайте параметры подключения координатора через МЭ с динамической трансляцией адресов в строке формата:

E:АДРЕС1-АДРЕС2:ПОРТ (такая строка должна быть только одна), где

* В поле **АДРЕС1** указывается реальный адрес внешнего сетевого интерфейса координатора. Если задать адрес в данной строке, то этот адрес можно не задавать в строке формата **АДРЕС** на предыдущем шаге.

* В поле **АДРЕС2** указывается значение 0.0.0.0, т.к. при настройке подключения координатора через МЭ с динамической трансляцией этот параметр не используется.

* В поле **ПОРТ** указывается номер порта инкапсуляции пакетов в UDP-формат для данного координатора. Вы можете указать **OUT**, что означает номер порта 55777, или при необходимости любой другой номер порта. Если в локальной сети через данный МЭ будет работать несколько сетевых узлов, то для каждого узла рекомендуется задать свой порт.

3. Задайте координатор входящих соединений, который будет обеспечивать пропуск начального входящего трафика через МЭ, в строке формата:

PRID=ID, где

ID – идентификатор координатора, который будет использован в качестве координатора входящих соединений. Идентификатор координатора Вы можете посмотреть при помощи команды меню **Службы/Просмотр конфигурации сети/Структура сети в узком формате**. Откроется отчет о структуре сети, отсортированный по номерам сети, координаторам и зарегистрированным на них АП. Этот отчет автоматически сохраняется в файле STRUCT.REP рабочего каталога ЦУС. В открывшемся окне или в файле STRUCT.REP найдите имя нужного координатора и в строке **СМ:** в последней колонке посмотрите значение идентификатора.

4. Задайте строку для выбора типа МЭ **С динамической трансляцией адресов** в формате:

DYN:SRV, где

параметр **:SRV** является **необязательным** параметром и задается в случае необходимости, чтобы весь трафик с внешними узлами передавался только через координатор входящих соединений, заданный в строке формата **PRID=ID** на предыдущем шаге. При такой настройке на координаторе в программе ViPNet Coordinator Монитор в окне **Настройки** установится флажок **Любой трафик с внешними узлами направлять через ViPNet-координатор**.

Если требуется на координаторе в программе ViPNet Coordinator Монитор в окне **Настройки** изменить значение поля **Период опроса координатора для обеспечения пропускания входящего трафика через межсетевой экран** (по умолчанию установлено 25 секунд), то задайте строку в формате:

TIMEOUT:N, где

N – период опроса в секундах. Например, **TIMEOUT:40**. Координатор с указанным периодом будет производить отправку UDP-пакетов на свой координатор входящих соединений, чтобы поддерживать динамическое правило на NAT-устройстве в активном состоянии. Этот период может быть настроен индивидуально, однако установленный по умолчанию период в 25 секунд вполне достаточен для работы с большинством NAT-устройств. При изменении периода следует учитывать, что период опроса не должен превышать таймаут сохранности динамического правила на NAT-устройстве².

Отсутствие данной строки у сетевого узла означает, что период опроса равен 25 секундам.

При таких настройках на координаторе в программе ViPNet Coordinator Монитор в окне **Настройки** будет автоматически установлен тип МЭ **С динамической трансляцией адресов** и выбраны заданные параметры.

13.7.2 Настройка адресов доступа к координатору

Если координатор имеет несколько адресов доступа с различных сетевых узлов, то эти адреса Вы можете задать при помощи следующих строк:

Если адрес статический, то задайте строку формата:

АДРЕС:ПОРТ, где

АДРЕС – IP-адрес доступа к координатору через межсетевой экран, **ПОРТ** – порт доступа к сетевому узлу через межсетевой экран. Параметр **ПОРТ** может иметь определенный номер порта или значение **OUT**. **OUT** – порт доступа по умолчанию – 55777.

Если адрес динамически меняется, то задайте строку формата:

DNS://DNS-имя:ПОРТ, где

DNS-имя задает DNS-имя МЭ, а **:ПОРТ** задает порт доступа к координатору через МЭ. Параметр **:ПОРТ** может иметь определенный номер порта или значение **OUT**. **OUT** – порт доступа по умолчанию – 55777.

Внимание! Во всех строках формата **Е:АДРЕС1-АДРЕС2:ПОРТ:FIX**, **АДРЕС:ПОРТ** и **DNS://DNS-имя:ПОРТ** для одного координатора должен быть указан один и тот же порт.

Внешние узлы автоматически с учетом заданных метрик выберут доступный для них адрес.

13.7.3 Частичная настройка координатора

Если не требуется полностью автоматическая настройка координатора (т.е. предполагается, что оператор координатора самостоятельно произведет окончательную настройку), то для координатора добавьте следующие строки:

1. Задайте все адреса сетевых интерфейсов координатора:

Если адреса статические, то задайте строки в формате:

АДРЕС, например, 195.210.139.67.

Если адрес динамически меняется, то координатор должен быть зарегистрирован на DNS-сервере. Задайте DNS-имя в строке формата:

DNS://DNS-имя, например, DNS://www.infotecs-vpn.info.

² У разных NAT-устройств таймаут устанавливается разным, но обычно не менее 30 секунд.

2. Задайте внешние адреса и порт доступа к координатору через МЭ (ViPNet-координатор или другой) следующими способами:

Если адрес статический, то задайте строку формата:

АДРЕС:ПОРТ, где

АДРЕС – IP-адрес доступа к координатору через межсетевой экран, **ПОРТ** – порт доступа к сетевому узлу через межсетевой экран. Параметр **ПОРТ** может иметь определенный номер порта или значение **OUT**. **OUT** – порт доступа по умолчанию – 55777.

Если адрес динамически меняется, то задайте строку формата:

DNS://DNS-имя:ПОРТ, где

DNS-имя задает DNS-имя МЭ, а **:ПОРТ** задает порт доступа к координатору через МЭ. Параметр **:ПОРТ** может иметь определенный номер порта или значение **OUT**. **OUT** – порт доступа по умолчанию – 55777.

Если координатор имеет несколько адресов доступа с различных сетевых узлов, то можно задать несколько строк формата **АДРЕС:ПОРТ** и **DNS://DNS-имя:ПОРТ**. Однако во всех этих строках должен быть указан один и тот же порт.

Такие настройки используется программой ViPNet Монитор других сетевых узлов для обеспечения их первоначального доступа к настраиваемому координатору.

На координаторе в программе ViPNet Coordinator Монитор в окне **Настройки** нужно будет вручную выбрать параметры подключения координатора к внешней сети.

13.7.4 Настройка туннелируемых адресов на координаторе

Если координатор должен осуществлять туннелирование открытых ресурсов, то для того чтобы не производить ручные настройки туннелируемых адресов непосредственно на координаторе и других связанных с ним сетевых узлах (в программе ViPNet Монитор), выполните настройки туннелируемых адресов координатора в соответствии с этим разделом.

Задайте туннелируемые адреса координатора в формате:

S:АДРЕСА, где

параметр **АДРЕСА** – туннелируемые адреса координатора. Адреса можно задать в виде одного адреса или диапазона адресов. Адреса и диапазоны адресов можно задать в нескольких строках формата **S:АДРЕСА** или в одной строке, разделяя их "точкой с запятой" (;).

Например, **S:178.136.121.10**

S:178.136.121.12-178.136.121.33

S:178.136.121.56-178.136.122.212

S:178.136.122.215;178.136.122.218

При таких настройках на координаторе в программе ViPNet Coordinator Монитор в окне **Туннелируемые ресурсы** (по кнопке **IP-адреса**) отобразятся заданные туннелируемые адреса. Также эти адреса появятся в программе ViPNet Монитор (в окне **Правило доступа\Туннель** для записи этого координатора) всех сетевых узлов, с кем связан данный координатор.

13.7.5 Настройка параметров межсетевого экрана для всех абонентских пунктов координатора

Если для координатора больше не делать никаких настроек, кроме указанных выше (см. п.13.7.1, 13.7.3, 13.7.4), то на всех АП, зарегистрированных в ЦУС на этом координаторе, в программе ViPNet Client Монитор автоматически будет выбран этот координатор в качестве сервера IP-адресов и межсетевого экрана.

Если все или большинство АП, зарегистрированных на одном и том же координаторе, должны быть настроены иным способом, то следует произвести общую настройку на их координаторе с помощью специальных строк.

Для координатора добавьте одну из следующих строк:

Если на АП должно быть выбрано использование МЭ **С динамической трансляцией адресов**, то для его координатора следует задать специальную строку в формате **DYN_AP:SRV**.

Наличие такой настройки у ViPNet-координатора означает, что на абонентских пунктах, зарегистрированных на этом координаторе, после первого запуска ViPNet Client Монитор, по умолчанию будет выбрано использование МЭ **С динамической трансляцией адресов**.

Параметр **:SRV** является **необязательным** параметром. Наличие **:SRV** означает, что весь трафик с внешними узлами будет направляться только через свой сервер IP-адресов, т.е. на АП в программе ViPNet Client Монитор в окне **Настройки** будет автоматически установлен флажок **Любой трафик с внешними узлами направлять через сервер IP-адресов**.

Если на АП должно быть выбрано использование МЭ **Со статической трансляцией адресов**, то для его координатора следует задать специальную строку в формате **STAT_AP**. Наличие такой настройки у ViPNet-координатора означает, что на абонентских пунктах, зарегистрированных на этом координаторе, после первого запуска ViPNet Client Монитор, по умолчанию будет выбрано использование МЭ **Со статической трансляцией адресов**.

Если на АП должна быть выбрана работа без использования МЭ, то для его координатора следует задать специальную строку в формате **NOPROXY_AP**. Наличие такой настройки у ViPNet-координатора означает, что на абонентских пунктах, зарегистрированных на этом координаторе, после первого запуска ViPNet Client Монитор, по умолчанию выберется работа без использования МЭ.

Если необходимо, чтобы пользователь при первом запуске ViPNet Client Монитор сам выбрал, будет ли он использовать ViPNet-координатор в качестве МЭ или нет, следует задать специальную строку в формате **REQUEST_AP**. Наличие такой настройки у ViPNet-координатора означает, что на абонентских пунктах, зарегистрированных на этом координаторе, при первом запуске ViPNet Client Монитор, будет задан вопрос о желании использовать данный координатор в качестве МЭ. При отказе будет выбрана работа без использования МЭ.

Если для отдельных АП следует сделать исключение из этих правил, то произведите настройки специальных строк для каждого такого АП (см. раздел 13.8).

13.7.6 Настройка параметров доступа к терминальному серверу

Если на сервере-маршрутизаторе зарегистрированы абонентские пункты с прикладной задачей «ViPNet Terminal», для этих абонентских пунктов можно задать параметры доступа к терминальному серверу. Для этого в список IP-адресов координатора добавьте строку вида:

T:protocol:address, где:

protocol — протокол доступа к терминальному серверу. Допустимые значения: **rdp**, **citrix**, **http**, **https**.

address — адрес терминального сервера.

Если параметр **protocol** имеет значение **rdp** или **citrix**, в качестве значения параметра **address** можно указать IP-адрес, DNS-имя или идентификатор сетевого узла терминального сервера. Например: **T:rdp:1A0F000A**.

Если параметр **protocol** имеет значение **http** или **https**, в качестве значения параметра **address** следует указать адрес URL. Например: **T:http:server.ru/app** или **T:http://server.ru/app**.

13.8 Настройка абонентских пунктов (АП)

Как правило, задавать какие-либо адреса и другие специальные строки для АП нет необходимости. Об адресах и настройках других узлов АП узнают автоматически после соединения со своим сервером IP-адресов.

После установки и запуска ViPNet Client Монитор на АП, АП будет настроен по умолчанию или в соответствии со специальными строками, заданными для его сервера IP-адресов (см. п. 13.7.5).

Если для некоторых АП требуется задать другие настройки ViPNet Client Монитор, то возможны следующие варианты настроек:

1. Если на АП есть необходимость использовать в качестве сервера IP-адресов другой координатор (т.е. не тот, на котором данный АП зарегистрирован в ЦУС), то для АП следует задать строку в формате **IPID=ID**, где ID – идентификатор координатора, который будет использован в качестве сервера IP-адресов. Идентификатор координатора Вы можете посмотреть при помощи команды меню **Службы/Просмотр конфигурации сети/Структура сети в узком формате**. Откроется отчет о структуре сети, отсортированный по номерам сети, координаторам и зарегистрированным на них АП. Этот отчет автоматически сохраняется в файле STRUCT.REP рабочего каталога ЦУС. В открывшемся окне или в файле STRUCT.REP найдите имя нужного координатора и в строке **СМ:** в последней колонке посмотрите значение идентификатора выбранного координатора.
2. Если на АП должен быть выбран тип МЭ **ViPNet-координатор**, но в качестве МЭ необходимо использовать иной координатор, чем его сервер IP-адресов, то следует добавить строку формата **PRID=ID**, где ID – идентификатор координатора, который будет использован в качестве межсетевых экранов.
3. Если АП необходимо автоматически установить в иное состояние, чем по умолчанию или как это определено в специальных строках для его сервера IP-адресов (см. п. 13.7.5), то для такого АП следует задать одну или несколько специальных строк в формате:

STAT:ПОРТ – задайте, если на АП в ПО ViPNet Client Монитор требуется установить тип МЭ **Со статической трансляцией адресов**. Параметр **:ПОРТ** является необязательным параметром. Параметр указывается, если к данному узлу доступ осуществляется через порт, отличный от порта с номером 55777.

Если на АП в ViPNet Client Монитор требуется установить тип МЭ **Со статической трансляцией адресов** и зафиксировать внешний адрес доступа к АП через межсетевой экран, то задайте строку формата **АДРЕС:ПОРТ:FIX**, где **АДРЕС:ПОРТ** – это адрес и порт доступа к этому АП через МЭ. В поле **ПОРТ** должен быть указан номер порта, который задан в настройках МЭ для доступа к данному узлу. Если не требуется иное, то можно указать **OUT** (означает номер порта 55777). Параметр **:FIX** предназначен для фиксации внешнего адреса доступа через межсетевой экран. Т.е. на АП в окне **Настройки** установится флажок **Зафиксировать внешний адрес доступа через МЭ**.

Если адрес доступа к АП через МЭ динамически меняется и на АП в ViPNet Client Монитор требуется установить тип МЭ **Со статической трансляцией адресов**, то задайте строку формата **DNS://DNS-имя:ПОРТ**, где в поле **ПОРТ** должен быть указан номер порта, который задан в настройках МЭ для доступа к данному узлу. Если не требуется иное, то можно указать **OUT** (означает номер порта 55777).

DYN:SRV – задайте, если на АП в ViPNet Client Монитор требуется установить тип МЭ **С динамической трансляцией адресов**. Параметр **:SRV** является необязательным параметром. Если он задан, то на этом АП в окне **Настройки** будет установлен флажок **Любой трафик с внешними узлами направлять через сервер IP-адресов**.

Если требуется изменить **Период опроса сервера IP-адресов для обеспечения пропуска входящего трафика через МЭ** (по умолчанию – 25 сек), то также следует задать строку в формате **TIMEOUT:N**, где N – период опроса в секундах.

NODYN – задайте, если на координаторе абонентского пункта задана строка **DYN_АП**, а для этого АП требуется сделать исключение. В этом случае АП будет установлен в состояние по умолчанию или состояние, определенное другими специальными строками.

PROXY – задайте, если на АП в ViPNet Client Монитор требуется установить тип МЭ *ViPNet-координатор*, а в групповых настройках координатора этого АП задано иное.

REQUEST – задайте, если требуется, чтобы на АП при запуске ViPNet Client Монитор был задан вопрос о желании использовать в качестве МЭ ViPNet-координатор или работать без использования МЭ.

NO_PROXY – задайте, если требуется, чтобы АП работал без использования МЭ. Наличие такой настройки у АП означает, что на этом АП в ViPNet Client Монитор в окне *Настройки* будет выбрана работа без использования МЭ.

14 Регистрация типов коллективов и пользователей

14.1 Формирование прикладной структуры сети

Для формирования прикладной структуры сети ViPNet подразумевает решение следующих задач:

1. Регистрация типов коллективов на конкретных объектах сети (узлах и группах):
задание (уникального) мнемонического имени (50 символов);
выделение уникального идентификатора типа коллектива.
2. Регистрация нового пользователя в конкретных типах коллективов на конкретных узлах (АП и СМ) сети:
задание (уникального) мнемонического имени (50 символов);
выделение уникального идентификатора пользователя.
3. Установление связей между типами коллективов.
4. Регистрация АП в конкретных прикладных задачах.
5. Удаление пользователей и типов коллективов.

14.2 Регистрация типов коллективов

Выполните команду меню *Службы/ Регистрация типов коллективов*. Появится диалоговое окно со списком зарегистрированных ТК (Рисунок 36).

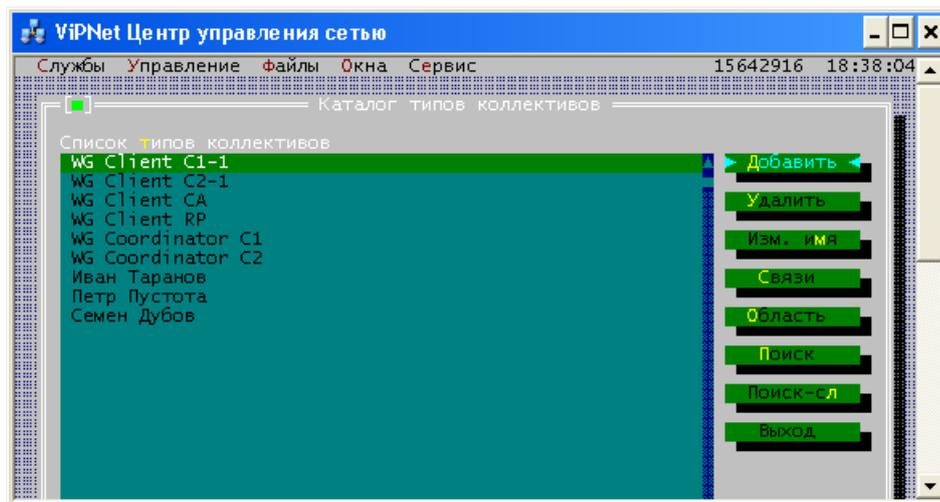


Рисунок 36

В этом окне доступны следующие функции:

Регистрация нового ТК.

Удаление ТК.

Изменение области действия ТК.

Изменение связей ТК.

Если программа выдает сообщения о невозможности открытия базы данных сетевых узлов, то, скорее всего, это означает, что в сети не зарегистрирован ни один сетевой узел. Войдите в адресную администрацию и выполните необходимые действия по созданию сетевой структуры.

14.2.1 Регистрация нового типа коллектива

Если в окне настроек по умолчанию задано **Автоматически создавать ТК и пользователя для нового узла**, то после регистрации узла в Адресной администрации здесь уже будет присутствовать коллектив с именем узла.

Для добавления нового ТК нажмите кнопку **Добавить**.

Появится строка ввода. Введите имя ТК и нажмите кнопку **Принять** или клавишу **Enter**. Появится окно со списком всех сетевых объектов сети (сетевых узлов (АП и СМ) и сетевых групп). Один из этих сетевых объектов надо выбрать в качестве области действия ТК. С помощью мыши или клавиш управления курсором выберите сетевой объект и нажмите кнопку **Принять** или клавишу **Enter**. ТК будет добавлен в каталог.

Зарегистрировать новый ТК можно только на одном сетевом объекте.

14.2.2 Удаление типа коллектива

Для удаления ТК подведите курсор к его имени, нажмите кнопку **Удалить** и ответьте “Да” на вопрос об удалении. Этот ТК будет удален из каталога ТК. Кроме того, будут удалены все записи о включении пользователей в коллективы этого типа. Если коллектив удаляемого типа был главным для какого-то пользователя и пользователь зарегистрирован, по крайней мере, в коллективе еще одного типа, то главным станет коллектив, в котором пользователь остался зарегистрированным.

14.2.3 Изменение имени и/или области действия типа коллектива

Для изменения имени ТК подведите курсор к его имени и нажмите кнопку **Изм. имя**. Появится строка ввода имени, в которой будет предложено отредактировать старое имя ТК. Нажатие любой нефункциональной клавиши очистит это имя. Для того чтобы это имя не очистилось, нажмите любую клавишу управления курсором. Если требуется изменить имя, то отредактируйте эту строку и нажмите кнопку **Принять** или клавишу **Enter**.

Чтобы узнать область действия уже зарегистрированного ТК, подведите курсор к его имени и нажмите кнопку **Область**.

Для изменения области действия ТК нажмите кнопку **Область** и затем **Сменить область**. Появится окно со списком всех сетевых объектов сети. Один из этих сетевых объектов можно выбрать в качестве новой области действия ТК. Для этого с помощью мыши или клавиш управления курсором выберите сетевой объект и нажмите кнопку **Принять** или клавишу **Enter**.

Если Вы не хотите изменять область действия ТК, то нажмите кнопку **Выйти** или клавишу **Esc**.

Если в ТК зарегистрированы пользователи, то поменять область действия ТК можно только в том случае, когда старая область – сетевой узел, а новая – узел или группа, включающая старый узел. В противном случае Вам потребуется удалить этот ТК и завести его заново. Либо предварительно убрать регистрацию пользователей в этом ТК. Естественно, что при этом придется заново регистрировать пользователей в коллективах этого типа.

При исключении какого-либо СУ из сетевой группы, на которой зарегистрирован некоторый ТК, автоматически удаляются все записи о регистрации пользователей в данном ТК на исключенном СУ.

Связи между ТК чужих сетей задать нельзя, так как это не входит в компетенцию данного ЦУС и может привести к конфликтам.

14.2.4 Изменение связей типа коллектива

Если в окне **Настройки по умолчанию** установлены флажки **Автоматически связывать новый ТК со всеми другими ТК** и **Автоматически создавать ТК и пользователя для нового узла**, то после регистрации узла в Адресной администрации связи нового коллектива будут созданы автоматически (см. п. 11.4).

Возможность задания нужного числа связей ТК определяется файлом лицензии, предоставляемым ОАО «ИнфоТекС» при поставке ЦУС.

Для изменения связей ТК подведите курсор к его имени и нажмите кнопку **Связи**. Появится окно со списком всех связей этого ТК. Первоначально этот список пуст.

Для добавления связи нажмите кнопку **Добавить**. Появится окно со списком всех ТК (за исключением тех, с которыми уже есть связи). Выберите один или несколько ТК и нажмите кнопку **Принять** или клавишу **Enter**.

Для удаления связи с некоторым ТК подведите курсор к имени этого ТК, нажмите кнопку **Удалить** и ответьте «Да» на вопрос об удалении связи.

Если список связей не пуст, то при нажатии кнопки **Добавить** появится окно, из которого можно сделать выбор: **"Добавить из списка всех ТК"** или **"Добавить из списка связей выделенного ТК"**. Последнюю возможность удобно использовать при задании однотипных связей для многих ТК.

14.2.5 Поиск по подстроке

Для поиска по подстроке нужного Вам ТК нажмите кнопку **Поиск** и введите подстроку.

Для поиска следующего ТК, в имя которого входит такая же подстрока, нажмите кнопку **Поиск-след.**

14.3 Регистрация пользователей

Выполните команду меню **Службы/Регистрация пользователей**. Появится диалоговое окно со списком зарегистрированных пользователей (Рисунок 37).

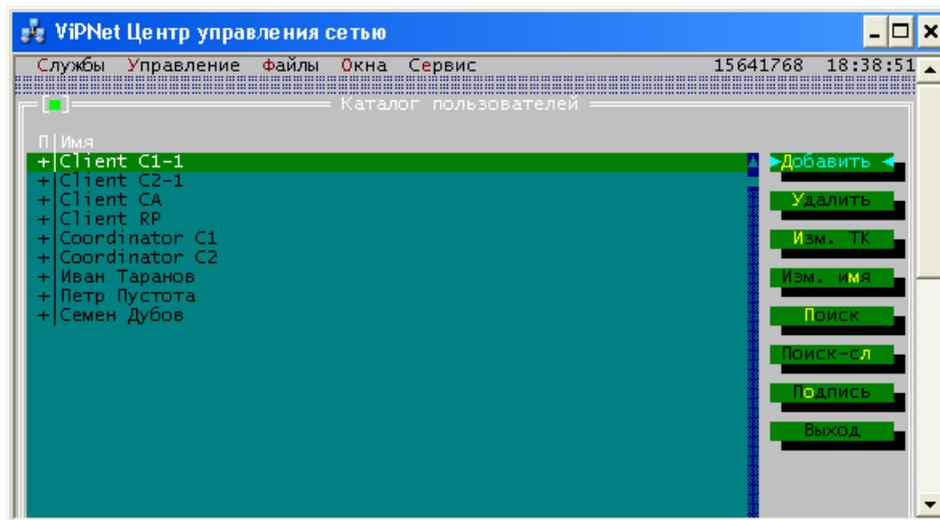


Рисунок 37

В этом окне доступны следующие функции:

Регистрация нового пользователя.

Удаление пользователя.

Изменение имени и/или списка коллективов пользователя.

Изменение атрибутов коллективов пользователя.

Предоставление пользователю права электронной подписи.

14.3.1 Регистрация нового пользователя

Если в окне настроек по умолчанию задано **Автоматически создавать ТК и пользователя для нового узла**, то после регистрации узла в Адресной администрации здесь уже будет присутствовать пользователь с именем этого узла.

Для добавления нового пользователя нажмите кнопку **Добавить**.

Появится строка ввода имени пользователя. Введите имя пользователя и нажмите кнопку **Принять** или клавишу **Enter**. Появится окно со списком типов коллективов, в которые входит пользователь. Для нового пользователя этот список первоначально пуст. Для включения пользователя в коллектив какого-либо типа нажмите кнопку **Добавить**. Появится окно со списком ТК, зарегистрированных в сети. С помощью мыши или клавиш управления курсором выберите ТК и нажмите кнопку **Принять** или клавишу **Enter**. Если область действия выбранного ТК - сетевая группа, а не отдельный сетевой узел, то появится окно со списком сетевых узлов, на которых зарегистрирован данный пользователь в коллективах данного типа. Для нового пользователя этот список первоначально пуст. Для добавления сетевого узла нажмите кнопку **Добавить**. Появится окно со списком сетевых узлов, входящих в область действия выбранного ТК. С помощью мыши или клавиш управления курсором выберите сетевой узел и пометьте его нажатием клавиш «Пробел» или **Ins**.

Можно зарегистрировать пользователя на нескольких сетевых узлах из области действия ТК.

Выбор всех сетевых узлов осуществляется нажатием кнопки **Все**. Для выбора сетевых узлов, в имени которых есть общая подстрока, нажмите кнопку **Фильтр**, введите общую подстроку и нажмите кнопку **Принять**.

Снять отметку с выбранного сетевого узла можно повторным нажатием клавиши **Ins**.

После выбора сетевых узлов нажмите кнопку **Принять** или клавишу **Enter**.

14.3.2 Удаление пользователя

Для удаления пользователя подведите курсор к его имени, нажмите кнопку **Удалить** и ответьте "Да" на вопрос об удалении. Далее задается вопрос, "**Считать ключи данного пользователя скомпрометированными**". Если этот пользователь считается скомпрометированным, то ответьте "Да", в этом случае пользователь удаляется, и после формирования всех справочников одновременно формируются справочники связей для создания в УКЦ новой ключевой информации, необходимой для восстановления работы сети.

14.3.3 Изменение имени пользователя

Если Вы хотите изменить имя пользователя, подведите курсор к имени пользователя и нажмите кнопку **Изменить имя**. Появится строка ввода имени пользователя, в которой будет предложено отредактировать старое имя пользователя. Нажатие любой нефункциональной клавиши очистит это имя. Для того чтобы это имя не очистилось, нажмите любую клавишу управления курсором. Отредактируйте эту строку и нажмите кнопку **Принять** или клавишу **Enter**.

14.3.3.1 Назначение псевдонимов. Обеспечение сопряжения криптофункций с другими системами установления идентификаторов

При нажатии на кнопку **Изменить имя** в каталоге пользователей для выбранного пользователя будет выведено окно **Имя и псевдонимы** (Рисунок 38), в котором с помощью кнопки **Добавить** поочередно можно создать псевдонимы для данного пользователя. Таким образом, в данном окне создается список псевдонимов для выбранного пользователя. Длина имени каждого псевдонима ограничена 245 символами. Все псевдонимы, добавляемые для одного пользователя, должны быть уникальны. Для изменения имени псевдонима используется кнопка **Изменить**, для удаления – **Удалить**. Для сохранения созданного списка псевдонимов для выбранного пользователя необходимо нажать **Принять**, если Вы решили отказаться от созданного только что списка, нажмите кнопку **Отмена**.

Внимание! Различным пользователям разрешается назначать одинаковые псевдонимы, однако, если эти пользователи зарегистрированы на АП, на которых зарегистрирована задача **ViPNet SDK** или **КриптоСервис**, то такие пользователи обязаны быть зарегистрированы в одном коллективе.

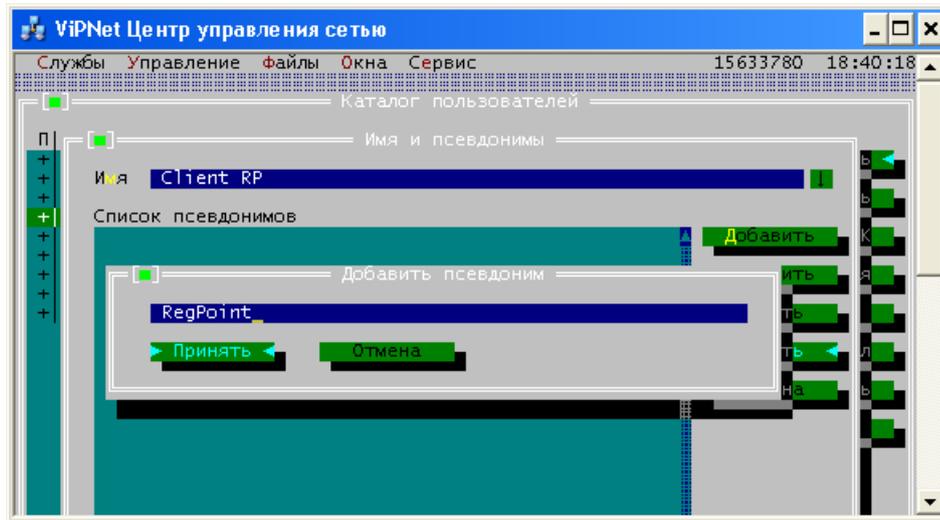


Рисунок 38

Все созданные псевдонимы пользователя попадут в состав справочников АП.

Данная функция полезна для обеспечения сопряжения криптофункций с другими системами установления идентификаторов. Так, для обеспечения шифрования при отправке сообщений из Microsoft Office Outlook или Microsoft Outlook Express с установленной программой ViPNet CryptoExtension необходимо сформировать список псевдонимов защищенных пользователей ViPNet, где псевдонимами будут являться адреса электронной почты (e-mail).

Замечание: Если импорт (п. 15) псевдонимов будет принят ЦУС, версии ниже 5.72-031, то импортируется только последний псевдоним из списка и его длина будет урезана до 80 символов.

14.3.4 Изменение списка коллективов пользователя

Если Вы хотите изменить список коллективов пользователя, подведите курсор к имени пользователя и нажмите кнопку **Изменить ТК**. Появится окно со списком ТК, в которые входит пользователь.

Для включения пользователя в какой-либо ТК нажмите кнопку **Добавить** и проделайте те же действия, что и при регистрации нового пользователя.

Для удаления пользователя из ТК подведите курсор к имени этого ТК, нажмите кнопку **Удалить** и ответьте "Да" на вопрос об удалении. Пользователь будет удален из всех коллективов этого типа на всех сетевых узлах, где он был зарегистрирован в этом ТК.

Для удаления пользователя из конкретного сетевого узла ТК или его регистрации на новом узле в данном ТК, область действия которого - сетевая группа, а не отдельный сетевой узел, подведите курсор к имени соответствующего типа коллектива и нажмите кнопку **Узлы**. Появится окно со списком сетевых узлов, на которых зарегистрирован данный пользователь в коллективах данного типа.

Для удаления - подведите курсор к имени сетевого узла, который Вы хотите удалить, нажмите кнопку **Удалить** и ответьте "Да" на вопрос об удалении. Пользователь будет удален из данного коллектива.

Для регистрации пользователя на новом узле в данном ТК нажмите кнопку **Добавить** и выберите интересующий Вас сетевой узел.

14.3.5 Изменение атрибутов коллективов пользователей

При регистрации нового пользователя первый коллектив, в который он включается, определяется как главный и открытый для этого пользователя. Соответствующие ТК и сетевой узел помечаются слева символом "√". Все остальные коллективы по умолчанию определяются как неглавные и скрытые (помеченные символом "☐").

Для того чтобы сделать неглавный коллектив главным, нужно подвести курсор к соответствующему имени ТК и нажать кнопку **Главный**. Выбранный ТК будет сделан главным (символ "√" переместится к этому ТК). Если область действия этого ТК – одиночный сетевой узел, этот узел автоматически будет назначен главным. Если область действия ТК – сетевая группа, главным сетевым узлом будет автоматически назначен первый узел в сетевой группе.

Если в качестве главного выбран ТК, областью действия которого является сетевая группа, можно изменить главный сетевой узел. Для этого подведите курсор к имени главного ТК и нажмите кнопку **Узлы**. Откроется окно со списком сетевых узлов данного ТК. Подведите курсор к имени сетевого узла, который Вы хотите сделать главным и нажмите кнопку **Главный**.

Внимание! Если требуется назначить главным сетевой узел, входящий в область действия неглавного ТК, сначала следует назначить этот ТК главным, а затем изменить главный сетевой узел. В противном случае возникнет ошибка выполнения программы.

Для того чтобы сделать открытый коллектив скрытым и наоборот, надо подвести курсор к соответствующему ТК и нажать кнопку **Открытый**. Если область действия этого ТК - одиночный сетевой узел, то соответствующий коллектив немедленно поменяет атрибут открытости на противоположный. Если область действия этого ТК - сетевая группа, то появится окно со списком сетевых узлов, на которых зарегистрирован данный пользователь в данном ТК. Подведите курсор к имени сетевого узла, для которого Вы хотите поменять атрибут открытости, и нажмите кнопку **Открытый**.

Для каждого коллектива возможно любое сочетание атрибутов "главный" и "открытый". Однако только один коллектив для пользователя может быть главным.

14.3.6 Предоставление пользователю права электронной подписи

При добавлении нового пользователя ему по умолчанию предоставляется право электронной подписи. В этом случае в УКЦ для пользователя будут созданы ключи электронной подписи.

Нажатием кнопки **Подпись** можно включать или отключить признак электронной подписи для каждого пользователя. Если пользователь имеет право электронной подписи, в колонке «П» перед именем пользователя отображается символ "+".

Для пользователей, генерируемых автоматически, можно задать значение признака электронной подписи. В файле DB\defset.txt значение параметра ASIGN=1 (по умолчанию) означает, что новые пользователи будут иметь право электронной подписи. Если ASIGN=0, то пользователи не будут иметь права подписи.

14.3.7 Поиск по подстроке

Для поиска по подстроке нужного Вам пользователя нажмите кнопку **Поиск** и введите подстроку.

Для поиска следующего ТК, в имя которого входит такая же подстрока, нажмите кнопку **Поиск-след**.

14.4 Списки рассылки копий писем

В программе существует возможность для каждой пары отправитель–получатель указать списки адресатов, которым при отправке писем в программе ViPNet Деловая почта должны независимо от желания отправителя направляться копии писем.

Для создания таких списков в меню **Службы** выберите **Списки рассылки/Список рассылки копий писем**. Откроется окно со списком абонентских пунктов, для которых заданы списки рассылки копий писем. Первоначально этот список пуст.

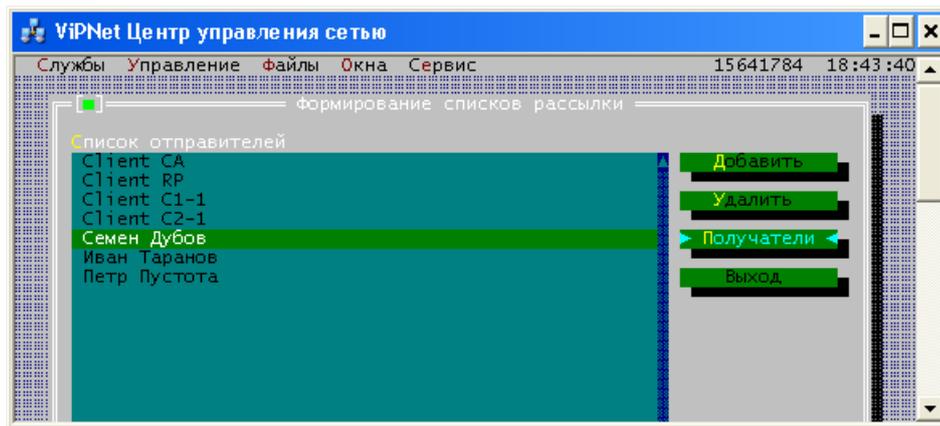


Рисунок 39

Для добавления нового отправителя нажмите кнопку **Добавить**. Появится окно со списком всех абонентских пунктов вашей сети. Выберите один или несколько абонентских пунктов и нажмите кнопку **Принять** или клавишу **Enter**.

Чтобы для определенного отправителя задать список получателей, при отправке писем которым должны автоматически формироваться копии другим адресатам, выберите отправителя и нажмите кнопку **Получатели**. Появится окно (Рисунок 40) со списком абонентских пунктов-получателей.

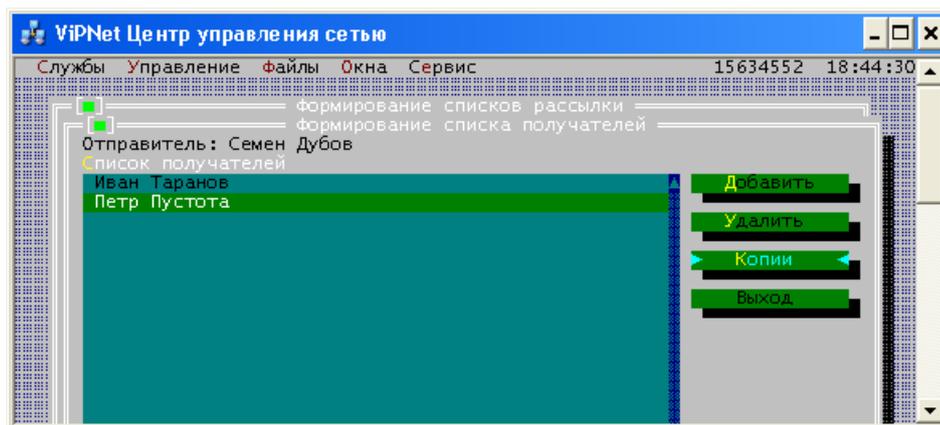


Рисунок 40

Первоначально это окно пусто. Для добавления нового получателя нажмите кнопку **Добавить**. Появится окно со списком всех возможных получателей.

Выберите один или несколько абонентских пунктов и нажмите кнопку **Принять** или клавишу **Enter**.

Подведите курсор к имени получателя, нажмите кнопку **Копии**. Появится окно (Рисунок 41) со списком получателей копий сообщений.

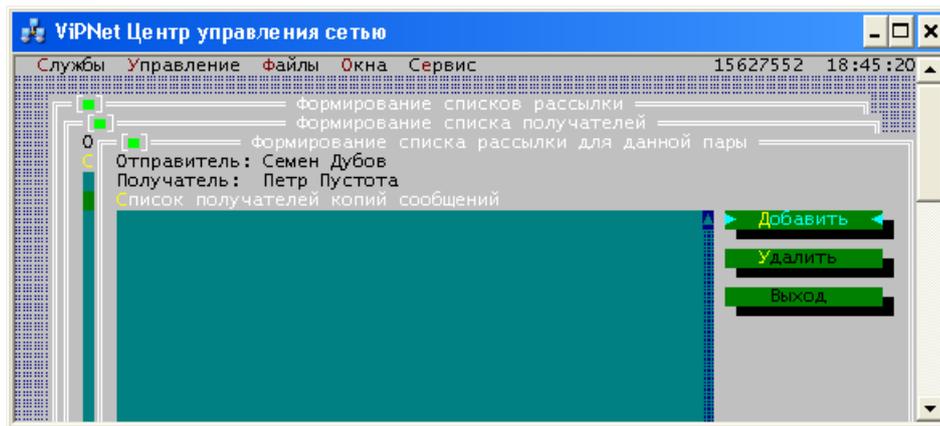


Рисунок 41

Первоначально это окно пусто. Для добавления нового получателя копий сообщений нажмите кнопку **Добавить**. Появится окно (Рисунок 42) со списком всех возможных получателей копий сообщений.

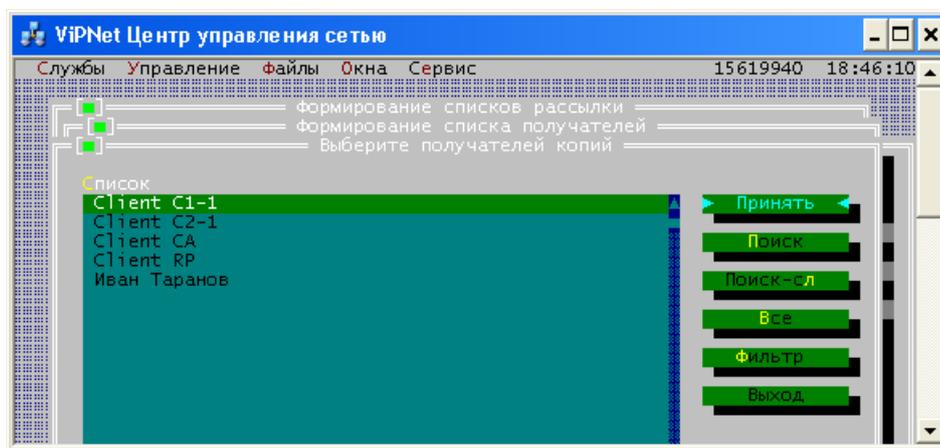


Рисунок 42

Выберите один или несколько абонентских пунктов и нажмите кнопку **Принять** или клавишу **Enter**.

В списках отправителей, получателей и получателей копий сообщений, нажав кнопку **Удалить**, можно удалить соответствующий АП из этих списков.

Информация о формировании копий сообщений попадет в комплект справочников соответствующего АП.

14.5 Список рассылки СОС

Список рассылки СОС предназначен для отправки списков отозванных сертификатов (СОС) на сетевые узлы, для которых необходимо гарантированное оперативное обновление СОС. При поступлении из программы ViPNet Удостоверяющий и ключевой центр обновленных СОС они автоматически отправляются на узлы из списка рассылки.

Внимание! Не следует добавлять в список рассылки СОС сетевые узлы, для которых не требуется оперативное обновление СОС. Для доставки СОС на все узлы сети ViPNet рекомендуется регулярно создавать обновления ключей в программе ViPNet Удостоверяющий и ключевой центр и опрашивать их на сетевые узлы (см. п. 21.2.2).

Для изменения списка рассылки СОС в меню **Службы** выберите **Списки рассылки/Список рассылки СОС** (Рисунок 43).

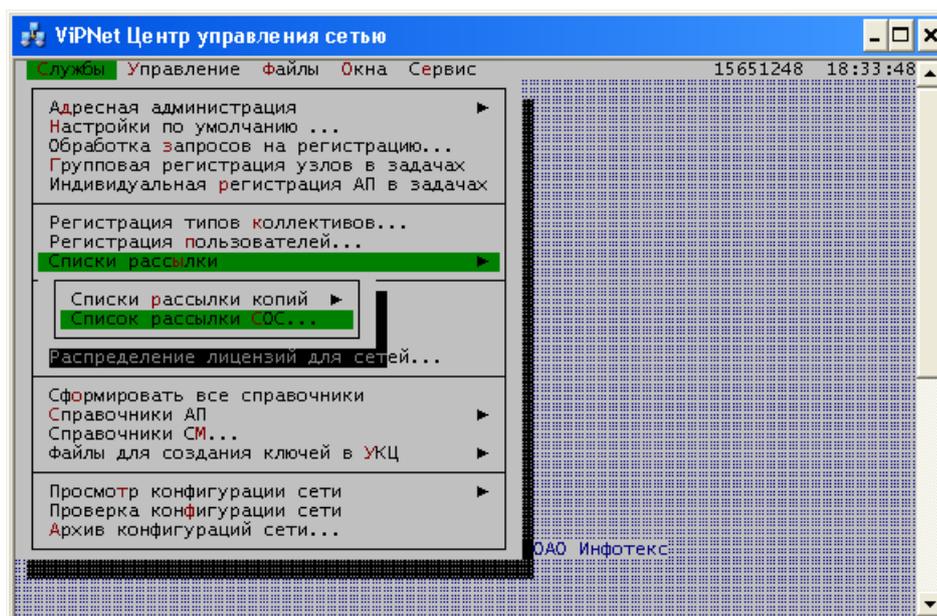


Рисунок 43

Появится диалоговое окно со списком АП для рассылки СОС (Рисунок 44). Первоначально это окно пусто. Для добавления нового АП нажмите кнопку **Добавить**. Появится окно со списком всех АП Вашей сети. Выберите один или несколько АП и нажмите кнопку **Принять** или клавишу **Enter**.

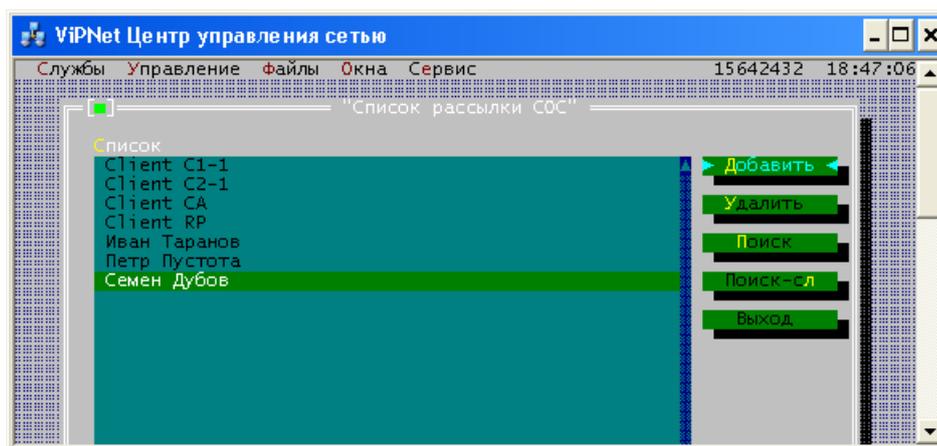


Рисунок 44

Программа ЦУС каждые 2 секунды сканирует каталог FOR_NCC\SIGN на предмет наличия файлов СОС. Если такие файлы есть, то они рассылаются на АП в соответствии со списком рассылки СОС, созданным Вами (Рисунок 44).

15 Организация межсетевого взаимодействия

Для организации взаимодействия между различными сетями ViPNet предусмотрены процедуры обмена данными экспорта между ЦУС этих сетей. Экспортированные данные импортируются в ЦУС соответствующей сети. Одновременно УКЦ должны выработать общие межсетевые мастер-ключи и обменяться ими (в соответствии с руководством по Ключевому центру), на базе которых будут созданы индивидуальные ключи для взаимодействия СУ разных сетей. После установления администратором связей с импортированными СУ из других сетей ViPNet, формирования и рассылки для своих СУ адресных справочников, новой ключевой информации, выработанной в УКЦ, пользователи данной сети получают возможность взаимодействовать с пользователями импортированных сетей.

1. Формирование первичных данных для экспорта

Формирование данных для экспорта в другую сеть ViPNet осуществляется при помощи пункта меню **Службы/Экспорт** (см. п. 15.1).

При экспорте формируется ряд файлов, содержащих данные об экспортированных Вами АП, коллективах и пользователях, данные об СМ Вашей сети, через который будет осуществляться взаимодействие с доверенной сетью. Кроме того, в УКЦ формируются и автоматически передаются в ЦУС для экспорта файлы справочники сертификатов администраторов УКЦ и списки отозванных сертификатов пользователей Вашей сети.

2. Передача файлов экспорта в доверенные сети

Сформированные файлы экспорта необходимо передать в ЦУС доверенной сети. При первоначальной организации межсетевое взаимодействия передайте файлы администраторам ЦУС соответствующих сетей каким-либо защищенным способом, предварительно перенеся их в заданный каталог (см. п. 21.2.4). Если уже установлено межсетевое взаимодействие, то эти файлы передаются автоматически по каналам связи сети ViPNet при выборе соответствующей команды ЦУС (**Управление > Отправить измененные файлы > Экспорт**, см.п. 21.2.4).

3. Получение и обработка импорта из доверенных сетей

Аналогичные экспортные данные, полученные от администраторов ЦУС доверенных сетей, следует поместить в каталог \IMPORT\NEW текущего каталога ЦУС (если не установлено межсетевое взаимодействие). Если уже установлено межсетевое взаимодействие, то эти файлы, поступившие по каналам связи сети ViPNet, автоматически попадают в каталог \IMPORT текущего каталога ЦУС.

Если уже установлено межсетевое взаимодействие, то отправка экспорта и получение импорта произойдет после запуска транспортного модуля ViPNet MFTP на Вашем АП.

Об изменениях в импорте программа предупреждает и предлагает обработать импорт сейчас или позднее (Рисунок 45).

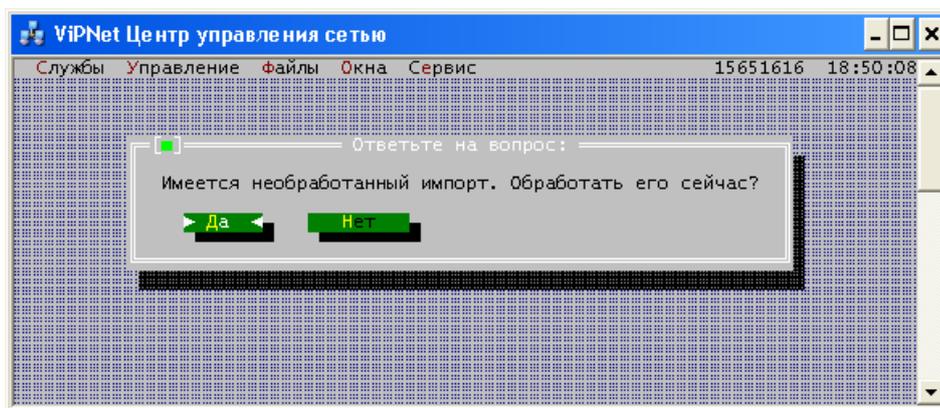


Рисунок 45

Обработка импорта происходит в окне **Необработанный импорт** (см. п. 15.3).

Замечание: Если Ваш ЦУС является подчиненным, а ЦУС сети, из которой пришел импорт головным, то в случае приема в составе импорта файлов лицензии, появится соответствующее сообщение о принятых файлах лицензии. Файлы лицензии обработаются автоматически (еще до обработки остального импорта) и подчиненный ЦУС перейдет на их использование. На экране откроется окно **Использование лицензии** (см. п. 22.1), где Вы сможете увидеть изменения в Вашей лицензии, произведенные в головном ЦУС.

Обработайте импорт в соответствии с п.15.3.

После получения и обработки импорта Вам необходимо в соответствии с разделом 14.2.4 установить необходимые связи импортированных коллективов другой сети с коллективами, которые Вы экспортировали в Вашу сеть. Если такие связи были установлены другой стороной, то эти действия не потребуются.

ВНИМАНИЕ! Если осуществляется первоначальная организация межсетевого взаимодействия, то не забудьте в соответствии с разделом 11.1.10 установить межсетевой канал

связи импортированного шлюзового СМ некоторой сети с одним из своих СМ, который Вы выбрали в качестве шлюзового для данной сети.

4. Прекращение межсетевого взаимодействия с сетью

Для прекращения межсетевого взаимодействия с сетью нужно удалить из списка экспорта в окне **Экспорт** (Рисунок 46). Выберите сеть в списке сетей и нажмите кнопку **Удалить**. Межсетевое взаимодействие будет прекращено. При этом будет удален подкаталог \EXPORT*<I>*.

15.1 Экспорт. Просмотр времени получения и обработки экспорта в доверенных сетях ViPNet

По команде меню **Службы/Экспорт** на экране появится окно (Рисунок 46) со списком доверенных сетей, для которых сформирован экспорт.

В этом окне можно формировать данные для организации межсетевого взаимодействия с различными сетями (1), а также отслеживать статус и время последнего отправленного экспорта (5).

1. Добавление новых сетей для организации межсетевого взаимодействия. Добавление СУ для экспорта в различные сети.

В основном, действия в этом окне нужно производить только при первоначальной организации межсетевого взаимодействия с какой-либо сетью. В дальнейшем, при задании связей ТК своей сети с ТК из другой сети, неэкспортированный ТК своей сети (с которым задана связь) будет попадать в экспорт автоматически. Если этот ТК зарегистрирован только на одном СУ, то СУ также попадет в экспорт автоматически. Ручное добавление СУ в экспорт потребуется, если ТК зарегистрирован на группе СУ, а также, если Вы экспортируете СУ и ТК в какую-либо сеть без задания связей с какими-либо узлами той сети.

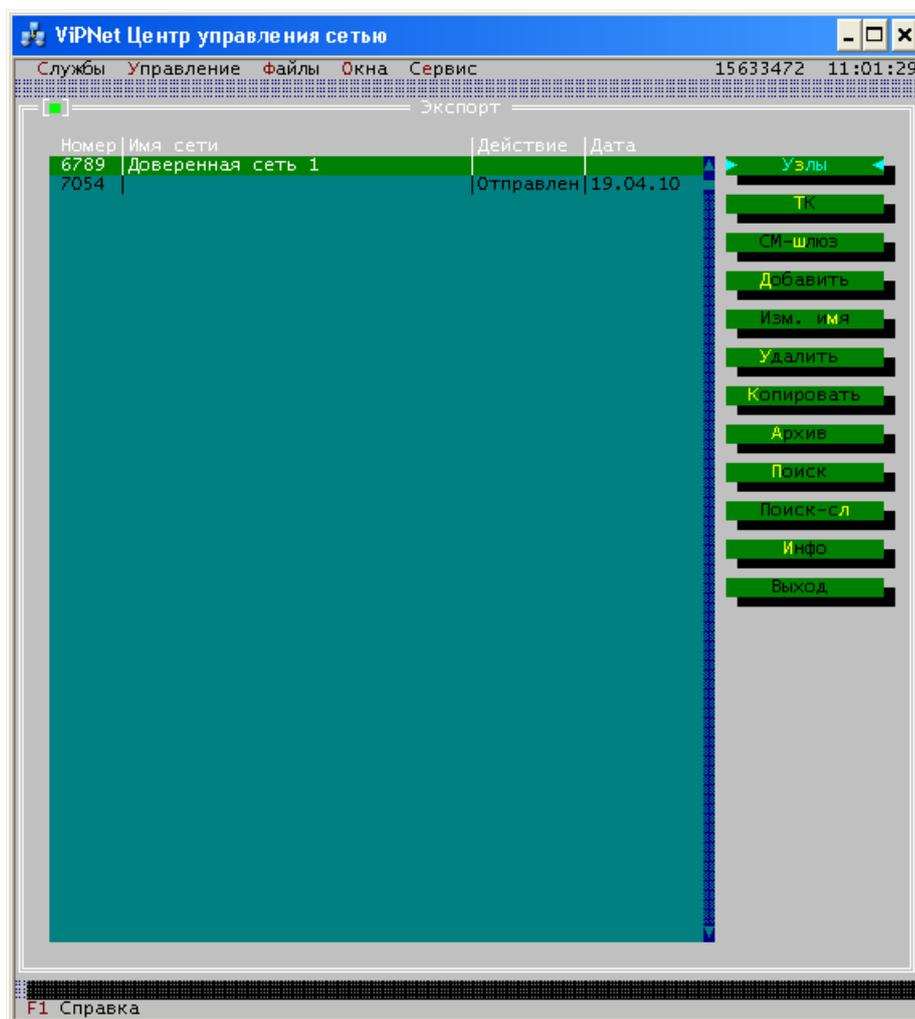


Рисунок 46

Первоначально этот список пуст. Для добавления новой сети нажмите кнопку **Добавить**. Вам будет предложено ввести номер и наименование сети, для которой Вы хотите сформировать данные для экспорта. При этом будет создан подкаталог \EXPORT*<I>*, где *<I>* - номер сети, для которой формируется экспорт. **Для каждой сети, с которой Вы желаете работать, должен быть обязательно указан ее десятичный номер <I>**, например 5. По этому номеру осуществляется автоматический обмен данными с соответствующим ЦУС. Имя сети значения не имеет. Но для удобства Вы можете задать имя сети, нажав кнопку **Изм. имя**.

Замечание: Если Ваш ЦУС является головным, а добавляемая сеть подчиненной, то информация об имени этой сети отобразится также в окне **Распределение лицензий** (см. п.17).

Для добавления в экспорт СУ можно действовать двумя способами:

Экспортировать сначала сетевые узлы, указав затем для экспорта ТК, зарегистрированные на них.

Экспортировать сначала типы коллективов, указав затем для экспорта АП, которые входят в область действия данных коллективов.

Если Вы выбрали первый способ, то, установите курсор на нужную сеть и нажмите кнопку **Узлы**. На экране появится окно экспортируемых СУ (Рисунок 47).

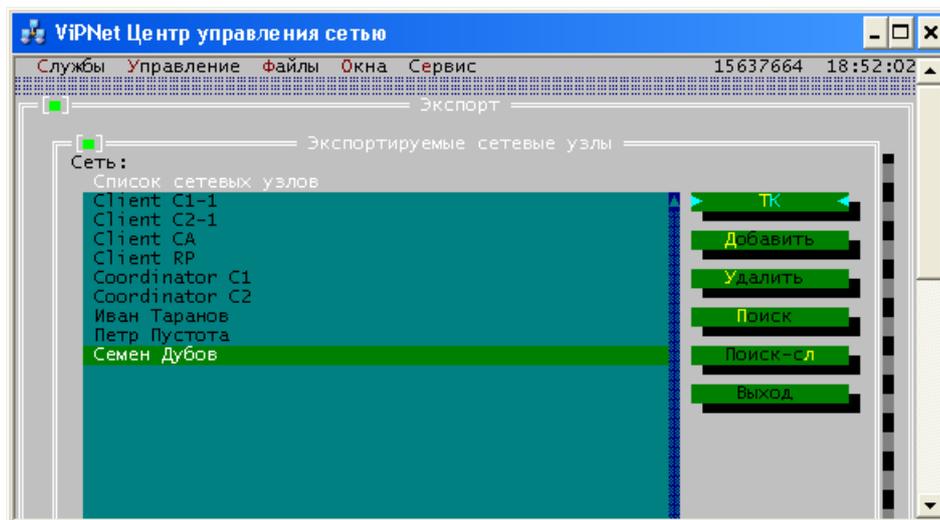


Рисунок 47

Первоначально этот список пуст. Нажав кнопку **Добавить**, Вы можете добавить СУ из предложенного списка. Если на СУ зарегистрирован только один ТК, то больше никаких действий осуществлять не нужно, ТК экспортируются автоматически. Если на СУ зарегистрировано несколько ТК, то затем, установив курсор на добавленный СУ, нажмите кнопку **ТК** и выберите нужные ТК из предложенного списка. Предложены будут только коллективы, зарегистрированные на данном сетевом узле.

Выбор ТК и СУ осуществляется путем отметки нужных объектов нажатием клавиши **Ins** и в завершении нажатием кнопки **Принять**.

Если Вы выбрали второй способ назначения экспорта, то в окне со списком сетей (Рисунок 46), выбрав нужную сеть, нажмите кнопку **ТК**, добавьте ТК. Если в область действия ТК входит только один СУ, то больше никаких действий осуществлять не нужно, СУ экспортируются автоматически. Если в область действия ТК входит несколько СУ, то затем, установив курсор на добавленный ТК, нажмите кнопку **Узлы** и выберите нужные СУ из предложенного списка.

После завершения формирования экспорта ТК и СУ в другую сеть Вам необходимо указать, через какой СМ Вашей сети будет осуществляться взаимодействие с данной сетью, т.е. нужно выбрать шлюзовой СМ (если он еще не был выбран и еще нет данных о шлюзовом СМ другой сети).

Внимание! Координатор, планируемый для использования в составе ПАК NME-RVPN ViPNet, нельзя выбирать в качестве шлюзового СМ в другую сеть.

Установите курсор на нужную сеть в окне со списком сетей и нажмите кнопку **СМ-шлюз** (Рисунок 46). На экране появится окно со списком Серверов-маршрутизаторов Вашей сети. Один из них Вы должны выбрать в качестве шлюзового СМ, через который будет осуществляться обмен почтовой и управляющей информацией с выбранной сетью. Выбор осуществляется нажатием клавиши **Enter** или кнопки **Принять**. Если СМ-шлюз уже был выбран, то по нажатию кнопки **СМ-шлюз**, программа сообщит имя этого шлюза и предоставит возможность его сменить (нажав кнопку **Сменить шлюз**).

Внимание! Если есть данные о шлюзовом СМ другой сети, то выбирать свой СМ-шлюз и задавать межсетевой канал следует в **Адресной администрации** в окне **Межсетевые каналы** (в соответствии с разделом 11.1.10). При нажатии на кнопку **СМ-шлюз** будет выдано соответствующее сообщение.

Далее, если Вы первоначально организуете межсетевое взаимодействие с какой-либо сетью, то, в окне со списком сетей установите курсор на нужную сеть и нажмите кнопку **Копировать** (Рисунок 46). По умолчанию программа предлагает скопировать экспорт в каталог `.NEW\EXPORT`. Вы можете указать другой каталог. Все файлы, появившиеся в каталоге, необходимо передать в ЦУС другой сети каким-либо защищенным способом.

Если межсетевое взаимодействие установлено, то при изменениях в экспорте, запустите формирование всех справочников (команда меню **Службы/Сформировать все справочники**), после чего Вы сможете отправить измененный экспорт в соответствующий ЦУС, выбрав пункт меню **Управление/Отправить измененные файлы/Экспорт**.

2. Копирование экспортных данных для сети

Воспользоваться кнопкой **Копировать** для какой-либо сети Вы можете также, если уже установлено межсетевое взаимодействие с сетью, но Вам по каким-то причинам необходимо отправить все экспортные данные в ЦУС этой сети. Для отправки воспользуйтесь пунктом меню **Управление/Отправить измененные файлы/Экспорт**.

3. Копирование экспортных данных в архив формата LZH

Копирование экспорта в архив формата LZH необходимо при установлении меж сетевого взаимодействия с сетью ViPNet OFFICE. Для установления такого взаимодействия администратор сети OFFICE отправляет администратору ЦУС первичный экспорт межсетевой информации. Администратор ЦУС должен обработать эту информацию, сформировать ответный экспорт и передать его в сеть OFFICE в виде архива LZH.

Чтобы скопировать экспортные данные в архив, в окне **Экспорт** выберите нужную доверенную сеть и нажмите кнопку **Архив**. В окне **Задайте каталог назначения** укажите папку, в которую будет скопирован архив (по умолчанию программа предлагает подпапку `\NEW\EXPORT`) и нажмите кнопку **Принять**. Файл формата LZH будет помещен в подпапку, имя которой совпадает с номером доверенной сети, для которой предназначен экспорт.

4. Удаление сети из экспорта для прекращения межсетевого взаимодействия с этой сетью

Для прекращения межсетевого взаимодействия с сетью сеть нужно удалить из списка экспорта (Рисунок 46). Выберите сеть в списке сетей и нажмите кнопку **Удалить**. Межсетевое взаимодействие будет прекращено. При этом будет удален подкаталог `\EXPORT\<I>`.

5. Просмотр времени получения и обработки экспорта в доверенных сетях ViPNet

После отправки экспорта в ЦУС какой-либо доверенной сети (с помощью пункта меню **Управление/Отправить измененные файлы/Экспорт** (кнопка **Отправить**, см. п. 21.2.4)) в окне **Экспорт** (Рисунок 48) для каждой такой сети отобразится информация о состоянии последнего отправленного экспорта в колонке **Действие**:

Отправлен – экспорт отправлен, но еще не принят ЦУС получателем.

Принят – экспорт принят ЦУС, но не обработан администратором (т.е. данные из Вашей сети не появились в базе данных ЦУС получателя).

Замечание: Если Ваш ЦУС является головным, а ЦУС сети, в который отправлен экспорт подчиненным, и в составе экспорта были отправлены файлы лицензии, то появление данного статуса дополнительно означает: файлы лицензии получены, и подчиненный ЦУС начал их использовать. В головной ЦУС была выслана информация об использовании лицензии в подчиненном ЦУС (эту информацию можно посмотреть в окне **Распределение лицензий** для соответствующей подчиненной сети (см. п. 17)).

Обработан – экспорт принят и обработан администратором.

Внимание! Значения **Принят** и **Обработан** появляются только в том случае, если ЦУС получатель имеет версию не ниже 2.8 (11.1825).

В колонке **Дата** отображается дата выполнения указанного в колонке **Действие** действия. Для просмотра более подробной информации о дате и времени отправки, приема и обработки экспорта нажмите кнопку **Инфо** (Рисунок 48).

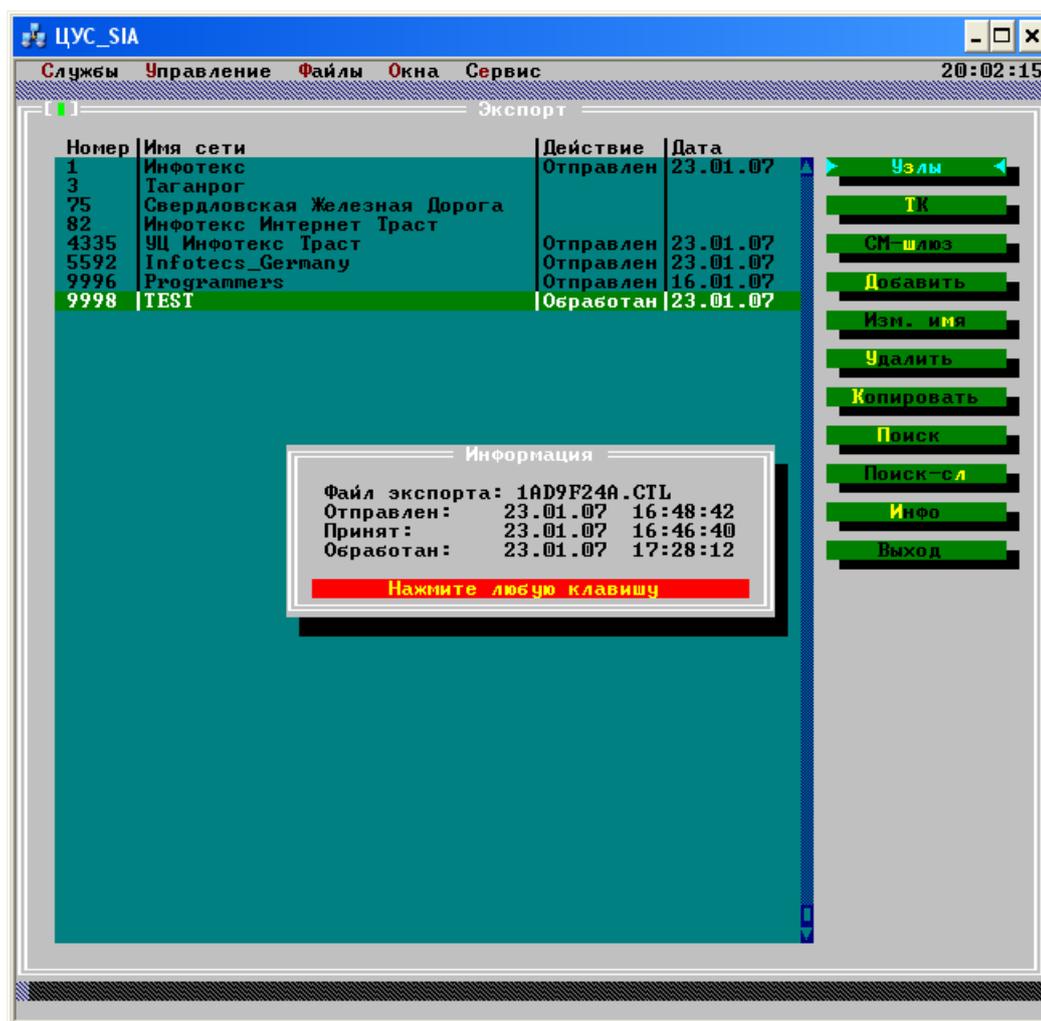


Рисунок 48

Для поиска по подстроке нужной Вам доверенной сети нажмите кнопку **Поиск** и введите подстроку.

Для поиска следующей доверенной сети, в имя которой входит такая же подстрока, нажмите кнопку **Поиск-сл**.

Для закрытия окна **Экспорт** нажмите кнопку **Выход**.

15.2 Импорт. Информация о статусе и времени принятого импорта

По команде меню **Службы/Импорт...** выводится окно со списком доверенных сетей (Рисунок 49).

В этом окне можно посмотреть и скопировать файлы импорта из доверенных сетей, а также посмотреть статус и время последнего принятого импорта.

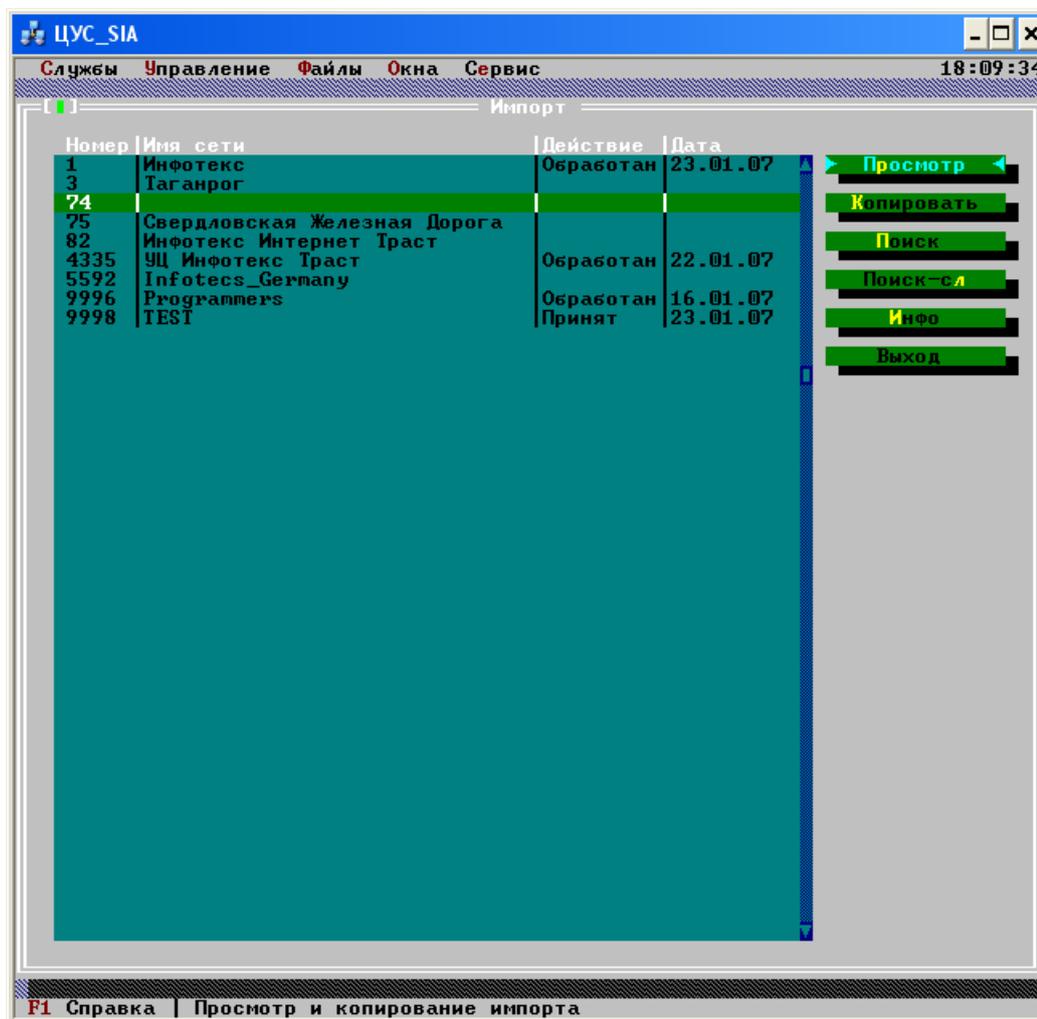


Рисунок 49

Для каждой сети из списка можно выполнить просмотр файлов импорта из данной сети (кнопка **Просмотр**) и копирование файлов импорта (кнопка **Копировать**).

Для поиска по подстроке нужной Вам доверенной сети нажмите кнопку **Поиск** и введите подстроку.

Для поиска следующей доверенной сети, в имя которой входит такая же подстрока, нажмите кнопку **Поиск-сл**.

После принятия импорта из ЦУС какой-либо доверенной сети в окне **Импорт** (Рисунок 49) для каждой такой сети отобразится информация о состоянии последнего полученного импорта в колонке **Действие**:

Принят – импорт принят ЦУС, но не обработан (т.е. данные из доверенной сети не появились в базе данных Вашего ЦУС). Вы можете его обработать в окне **Необработанный импорт** (см. п.15.3).

Замечание: Если Ваш ЦУС является подчиненным, а ЦУС сети, из которой пришел импорт головным, то в случае приема в составе импорта файлов лицензии, они

обработаются автоматически (еще до обработки остального импорта) и подчиненный ЦУС перейдет на их использование.

Обработан – импорт принят и обработан Вами (с помощью пункта меню **Службы/Необработанный импорт** (кнопка **Обработать**, см. п. 15.3).

В колонке **Дата** отображается дата выполнения указанного в колонке **Действие** действия. Для просмотра более подробной информации о дате и времени приема и обработки импорта нажмите кнопку **Инфо**.

15.3 Необработанный импорт...

Окно **Необработанный импорт** открывается, если при поступлении импорта Вы ответили **Да** на вопрос об обработке импорта сейчас. Если Вы ответили **Нет**, то это окно можно открыть по команде меню **Службы/Необработанный импорт...**

В этом окне выводится список доверенных сетей (Рисунок 50), от которых пришел импорт, но он еще не был обработан Вами.

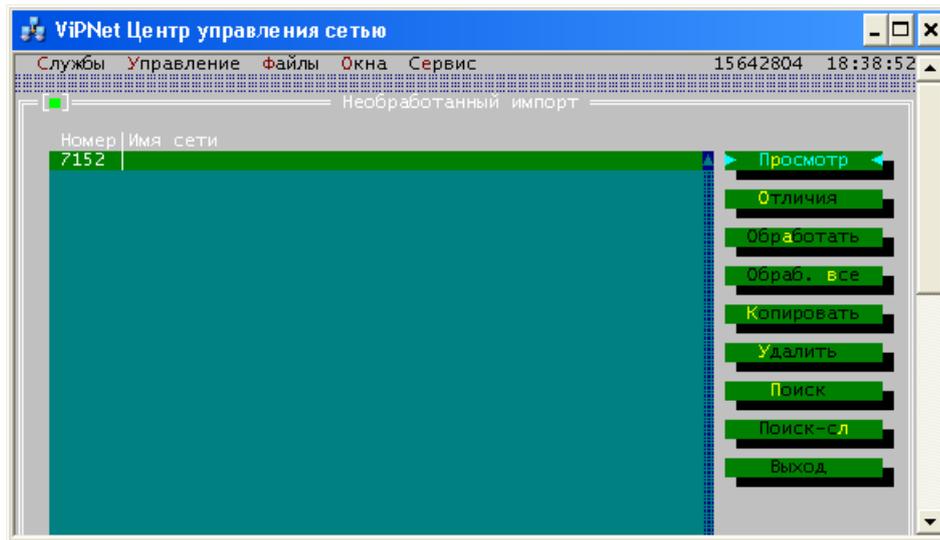


Рисунок 50

В этом окне имеется возможность:

посмотреть принятые файлы импорта от каждой сети (с помощью кнопки **Просмотр**);

посмотреть отличия принятых файлов импорта от имеющегося ранее обработанного импорта (с помощью кнопки **Отличия**);

обработать принятый импорт от выбранной доверенной сети (с помощью кнопки **Обработать**);

обработать весь (от всех сетей) необработанный импорт (с помощью кнопки **Обраб. все**);

После обработки импорта, в зависимости от изменений, пришедших из доверенной сети, появится соответствующее сообщение о дальнейших действиях администратора (сформировать справочники; если изменились файлы для УКЦ, то выполнить действия в УКЦ; и т.д.). В соответствующих окнах ЦУС отобразится новая информация (если она появилась), пришедшая из доверенной сети (например, о СУ, ТК, пользователях доверенных сетей, которые будут взаимодействовать с Вашей сетью).

Если Вы обработали ответный импорт из какой-либо сети для организации межсетевой связи импортированного шлюзового СМ с одним из своих СМ, который Вы выбрали в качестве шлюзового для Вашей сети. Соответствующая подсказка появится на Вашем экране. Задать межсетевой канал Вы можете в **Адресной администрации**, вызываемой

командой меню **Службы/Адресная администрация/Структура сети ViPNet**, в окне **Межсетевые каналы** в соответствии с разделом 11.1.10.

Замечание: Если Ваш ЦУС является головным, а ЦУС сети, из которой пришел импорт подчиненным, то при приеме в составе импорта файлов отчетов они будут помещены в подпапку REP\<номер сети>\<дата формирования отчетов> папки установки ЦУС после обработки импорта. Подробнее об отчетах читайте в п. 6.3.3.

Информация о статусе импорта, а также времени получения и обработки импорта появится в окне **Импорт**, доступном по пункту меню **Службы/Импорт** (см. п.15.2).

Информация об изменениях в последнем импорте сохраняется в файле Impdiff.rep в папке установки ЦУС. После обработки нового импорта информация переносится в файл Impdiff2.rep и там накапливается.

скопировать принятые файлы импорта от каждой сети в какой-либо каталог (с помощью кнопки **Копировать**)

удалить принятые файлы импорта от каждой сети (с помощью кнопки **Удалить**)

Для поиска по подстроке нужной Вам доверенной сети нажмите кнопку **Поиск** и введите подстроку.

Для поиска следующей доверенной сети, в имя которой входит такая же подстрока, нажмите кнопку **Поиск-сл.**

16 Обработка запросов, поступающих из Центра регистрации

ЦУС обрабатывает следующие запросы, поступающие из Центра регистрации:

1. Запросы на регистрацию пользователя в сети ViPNet и создание для него дистрибутива ключей (в том числе сертификата). При обработке такого запроса в ЦУС автоматически регистрируется сетевой узел, тип коллектива и пользователь, задаются связи с другими сетевыми узлами, а также производится регистрация сетевого узла в прикладных задачах согласно данным, указанным в запросе из Центра регистрации. Далее для УКЦ копируются справочники зарегистрированного сетевого узла для создания дистрибутива ключей. После получения из УКЦ дистрибутива ключей он отправляется в Центр регистрации автоматически без участия администратора ЦУС. Кроме того, ЦУС формирует справочники для сетевых узлов, с которыми были заданы связи зарегистрированного узла.
2. Запросы на обновление регистрационной информации о пользователе ViPNet. При обработке такого запроса в ЦУС автоматически изменяются данные о зарегистрированном сетевом узле (имя сетевого узла, типа коллектива, пользователя, связи с другими узлами, регистрация в прикладных задачах) согласно информации, указанной в запросе из Центра регистрации. Далее для УКЦ копируются справочники обновленного сетевого узла для создания дистрибутива ключей. После получения из УКЦ дистрибутива ключей он отправляется в Центр регистрации автоматически без участия администратора ЦУС. Кроме того, ЦУС формирует справочники для сетевых узлов, связи с которыми были добавлены или удалены при обновлении регистрационной информации сетевого узла в Центре регистрации.
3. Запросы на удаление информации о пользователе ViPNet. При обработке такого запроса в ЦУС удаляется вся информация о пользователе с заданным идентификатором. Причем, если на сетевых узлах и в типах коллективов, где зарегистрирован удаляемый пользователь, никаких других пользователей не зарегистрировано, то удаляются также эти сетевые узлы и типы коллективов. Кроме того, ЦУС сформирует справочники для узлов, с которыми был связан удаляемый узел.
4. Запросы на создание сертификата пользователя без регистрации пользователя в сети ViPNet (запросы для внешнего пользователя), запросы на обновление, отзыв, приостановку или возобновление действия сертификата внешнего пользователя или пользователя сети ViPNet. Такие запросы обрабатываются в ЦУС в автоматическом

режиме, т.е. запросы от Центра регистрации отправляются в УКЦ, а ответы из УКЦ отправляются обратно в Центр регистрации без участия администратора ЦУС.

По умолчанию, при поступлении какого-либо запроса из Центра регистрации он обрабатывается автоматически без участия администратора ЦУС.

Замечание: Если в лицензии Вашей сети существуют ограничения на число сертификатов, то при достижении максимального числа лицензий на сертификаты, запросы, поступившие из Центра регистрации, будут отклонены.

Для того чтобы можно было управлять процессом обработки запросов (из п. 1-3), поступающим из Центра регистрации, нужно отключить опцию **Автоматически обрабатывать запросы на регистрацию пользователей** в окне **Настройки по умолчанию** (см. п. 11.4).

При отключении этой опции все новые запросы из Центра регистрации отображаются в окне **Необработанные запросы от Центров регистрации** (Рисунок 51), открываемом по команде меню **Сервис\Обработка запросов на регистрацию**. Эти запросы можно просмотреть и обработать.

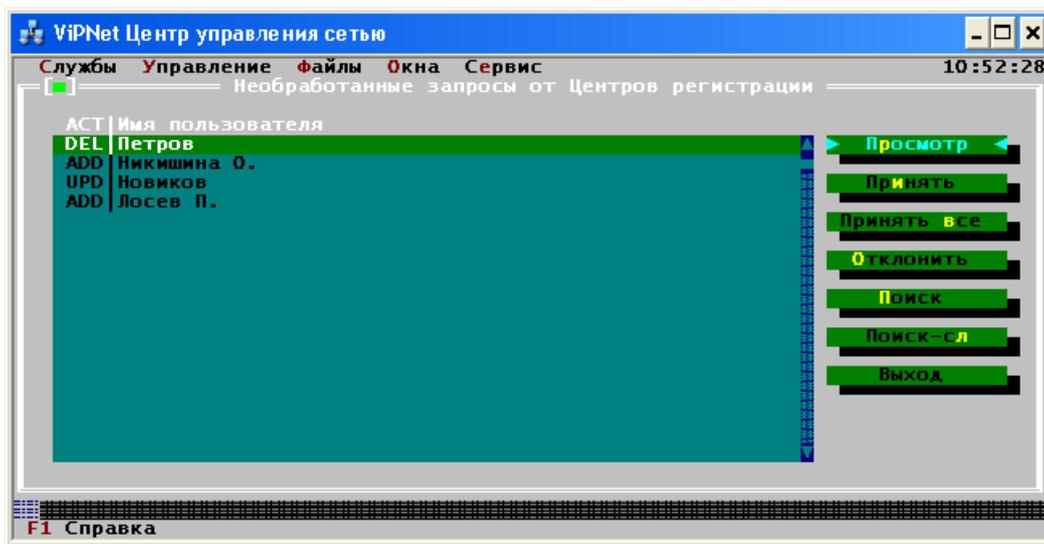


Рисунок 51

В данном окне для каждого запроса в списке отображается тип запроса, а также имя пользователя, параметры которого содержит запрос. Тип запроса отображается в графе **АСТ**. Существуют следующие типы запросов: ADD (зарегистрировать пользователя в ЦУС), UPD (обновить данные пользователя), DEL (удалить пользователя из ЦУС).

Для обработки запросов нужно воспользоваться кнопками окна. В окне присутствуют следующие кнопки:

Просмотр – просмотр запроса. Выбранный запрос отображается в текстовом виде.

Принять – принять запрос для обработки. Выбранный запрос принимается для дальнейшей обработки ЦУС.

Принять все – принять все запросы для обработки. Все необработанные запросы из списка принимаются для дальнейшей обработки ЦУС.

Отклонить – отклонить запрос. Запрос отклоняется, т.е. запрошенное из Центра регистрации действие осуществлено не будет. В ЦР отправляется квитанция о том, что запрос отклонен.

Поиск – поиск узла по подстроке имени узла.

Поиск-сл – поиск следующего запроса по той же подстроке (см. пред.).

Выход – закрыть окно. При этом, если есть принятые для обработки запросы, то задается вопрос **Обработать принятые запросы? При ответе "Нет" их можно будет обработать позже** (ответы Да, Нет). При ответе **Да** все запросы будут обработаны, т.е.

запрашиваемые из Центра регистрации действия будут выполнены (зарегистрирован пользователь, обновлены данные пользователя или пользователь удален из ЦУС в зависимости от типа запроса). При неуспешной обработке запроса ЦУС отправляет в ЦР квитанцию о том, что запрос не выполнен, т.е. отклонен. При ответе **Нет** запросы останутся необработанными.

При каждом старте программы ЦУС, а также один раз в час, ЦУС проверяет наличие новых и принятых запросов.

Если из ЦР поступили новые запросы, то ЦУС выведет сообщение: **Имеются необработанные запросы на регистрацию пользователей. Обработать их сейчас?** (ответы Да, Нет). При ответе **Да** откроется окно **Необработанные запросы от Центров регистрации** (Рисунок 51).

Если в ЦУС есть принятые запросы, но еще не обработанные, при этом новых запросов нет, то ЦУС выведет сообщение **Имеются принятые, но еще необработанные запросы на регистрацию пользователей. Обработать их сейчас?** (ответы Да, Нет). При ответе **Да** начнется обработка принятых запросов.

17 Распределение лицензий для сетей

Если ЦУС является головным (имеет соответствующий файл лицензии), то, при выборе пункта меню **Службы/Распределение лицензий для сетей** откроется окно **Распределение лицензий** (Рисунок 52) со списком сетей (головной и подчиненных).

Замечание: Если ЦУС не является головным, то данное окно недоступно.

В этом окне можно распределять лицензии из общего файла лицензии, на свою (головную) сеть и подчиненные сети, а также просматривать информацию о числе использованных в каждой сети лицензий.

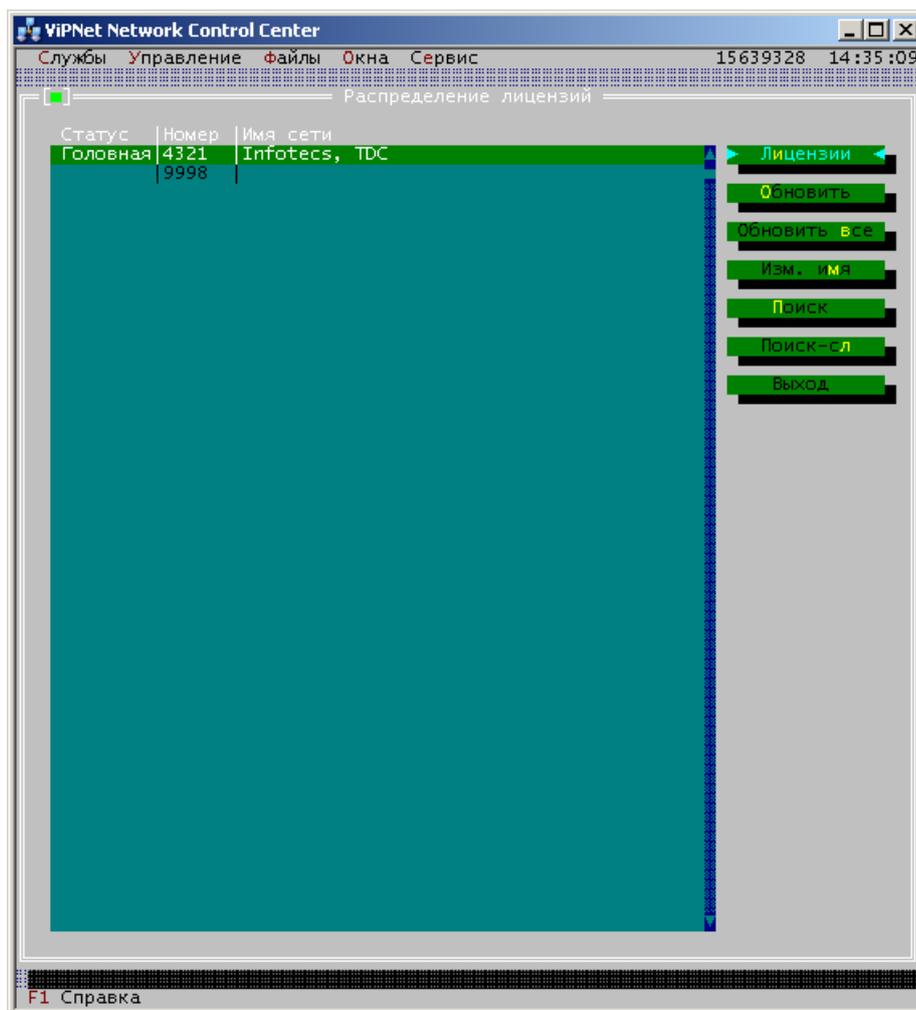


Рисунок 52

В окне **Распределение лицензий** отображается список сетей ViPNet (головная и подчиненные), входящие в иерархическую систему ЦУС, и заданные в общем файле лицензии (Infotecs.reg).

Для каждой сети отображается следующая информация:

Название колонки	Описание
Статус	Статус сети. Для головной сети в этой колонке отображается значение Головная , для подчиненных сетей ничего не отображается.
Номер	Номер сети, заданный в файле лицензии.
Имя сети	Имя сети. Имя головной сети берется из файла лицензии. Имя подчиненной сети может быть задано с помощью кнопки Изм. имя (Рисунок 52) или взято из колонки Имя сети окна Экспорт (если организовано межсетевое взаимодействие с сетью, см. п. 15.1). Имя подчиненной сети помещается в файл лицензии для подчиненной сети.

В окне **Распределение лицензий** доступны следующие действия:

1. Поиск сети

Для поиска по подстроке нужной Вам сети нажмите кнопку **Поиск** и введите подстроку имени или номера сети.

Для поиска следующей сети, в имя которой входит такая же подстрока, нажмите кнопку **Поиск-сл**.

6. Подготовка файлов лицензии для отправки в подчиненные сети без предварительного перераспределения лицензионных ограничений

Если для головного ЦУС изменился специальный файл лицензии, то может потребоваться обновить файлы лицензии в подчиненных сетях без перераспределения лицензионных ограничений. Такая ситуация может возникнуть, например, если в лицензии изменился только разрешенный номер версии используемого ПО ViPNet. Для подготовки файлов лицензии к отправке в подчиненные сети воспользуйтесь одной из следующих кнопок:

Обновить – подготовка файлов лицензии к отправке в выбранную подчиненную сеть.

Обновить все – подготовка файлов лицензии к отправке во все подчиненные сети.

При помощи этих кнопок Вы можете подготовить для отправки в подчиненные сети файлы лицензии даже в том случае, если они не менялись.

7. Изменение имени сети

Для задания или изменения имени подчиненной сети выберите сеть и нажмите кнопку **Изм. имя**. Если с этой сетью уже организовано межсетевое взаимодействие, то после изменения имени сети оно изменится и в окне **Экспорт** (см. п. 15.1).

8. Распределение лицензий и просмотр числа использованных лицензий

Для распределения лицензий выберите сеть и нажмите кнопку **Лицензии**. Откроется окно **Распределение лицензионных ограничений в сети** (Рисунок 53). В верхней части окна указано имя выбранной сети.

Лицензионное ограничение	Использовано	Назначено	Распределено	Максимально
=== Общие лицензионные ограничения ===				
Число координаторов	8	200	350	350
Число АП	64	5000	7000	7000
Число пользователей	88	10400	15400	15400
Число адресов туннелей	43	50	150	150
Число связей ТК	0	не огранич	не огранич.	не огранич.
Число элементов кластера	0	30	40	40
Число адресов Веб-шлюза	0	30	40	40
=== Максимальное число узлов в прикладных задачах ===				
КриптоСервис	12	13	23	23
Деловая почта	57	5000	7000	7000
Диспетчер	10	50	1050	1050
Центр регистрации	4	13	23	23
Секретный диск	12	13	23	23
Защита трафика	61	5000	7000	7000
Сервер IP-адресов	8	200	350	350
Кластер Linux	4	13	23	23
Solaris	1	3	5	14
Кластер Solaris	1	13	14	14
ViPNet SDK	7	13	19	19
Терминал Навигатор	1	13	16	16
Терминал Спектр	2	13	16	16
Терминал Ареал-Сервис	1	13	16	16
ИСУ Магистраль	0	1	4	16
Производительный кластер	0	3	4	4
Веб-шлюз	0	3	4	4
ИСУ Навигатор	0	13	16	16
ИСУ Спектр	0	13	16	16
UPN-координатор KB2	0	3	6	6
APM мониторинга	3	13	28	28
ИСУ Видеотон	0	9	10	10
Сервис публикации	0	5	7	10
Терминал УФС	0	5	5	10
Сервер SGA	0	1	1	2

Рисунок 53

В этом окне отображается список параметров лицензии и максимально допустимое число лицензий на них, заданных в общем файле лицензии, а также число распределенных лицензий, и число использованных и назначенных лицензий в выбранной сети.

Для каждого параметра лицензии отображается следующая информация (Рисунок 53):

Название колонки	Описание
Лицензионное ограничение	Название параметра лицензии, заданного в общем файле лицензии. Параметры лицензии разделены на 2 группы: Общие лицензионные ограничения , где перечислены ограничения на структуру сети, и Максимальное число узлов в прикладных задачах , где перечислены прикладные задачи, в которых можно регистрировать сетевые узлы. Эти параметры можно распределять по сетям (головной и подчиненным). Описание прикладных задач Вы найдете в п. 13.1.
Использовано	Число использованных лицензий в выбранной сети из числа назначенных (в колонке Назначено). Лицензии используются при конфигурировании сети ViPNet в ЦУС. Актуальная информация о числе лицензий, которые были использованы в подчиненном ЦУС, отображается только после получения подчиненным ЦУС (через каналы связи) экспорта с файлом лицензии .
Назначено	Число лицензий, которое назначено (разрешено) для использования в выбранной сети. Значение не огранич. означает, что параметр лицензии не имеет ограничения.
Распределено	Сумма назначенных (распределенных) администратором лицензий для всех сетей (головной и подчиненных) из числа общего лицензионного ограничения (в колонке Максимально). Значение не огранич. означает, что параметр лицензии не имеет ограничения.
Максимально	Максимально допустимое число лицензий, заданное в общем файле лицензии, которое можно распределить по сетям. Значение не огранич. означает, что параметр лицензии не имеет ограничения.

В окне **Распределение лицензионных ограничений в сети** (Рисунок 53) доступны следующие действия по изменению лицензии для выбранной сети:

а. Изменение лицензионных ограничений вручную

Для назначения (изменения) лицензионных ограничений для выбранной сети выберите параметр лицензии и нажмите кнопку **Изменить**, откроется окно для изменения ограничения параметра (Рисунок 54). Задайте значение и нажмите **Принять**.

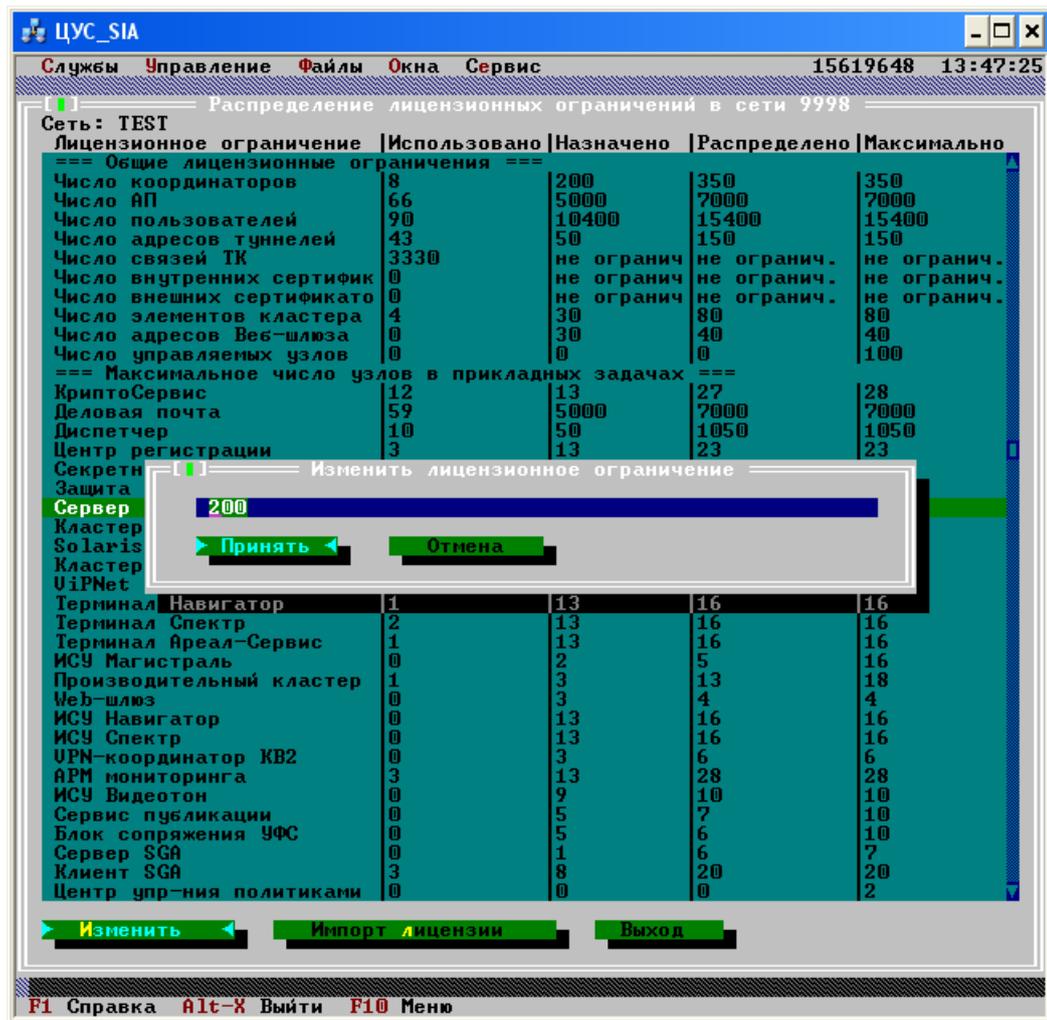


Рисунок 54

После ввода нового значения ЦУС проверяет, чтобы суммарное число распределенных значений для данного параметра по всем сетям (с учетом нового значения) не превосходило максимального значения, заданного в общем лицензионном файле (отображенного в колонке **Максимально**). Если проверка пройдет успешно, то введенное значение запишется в файл лицензии и отобразится в колонке **Назначено**. При этом в колонке **Распределено** для данного параметра изменится суммарное число распределенных значений по всем сетям. Если введенное значение слишком большое, то появится соответствующее сообщение и значение параметра не изменится. В этом случае введите меньшее число, чтобы уложиться в максимально возможное значение. Для задания всех лицензионных ограничений выполните указанные действия с каждым параметром лицензии из окна **Распределение лицензионных ограничений в сети** (Рисунок 54).

Если параметр общей лицензии не имеет лицензионных ограничений, то в колонке **Максимально** отображается значение **не огранич.** (например, параметр **Число связей ТК**, Рисунок 54). По умолчанию это значение записывается в файл лицензии для каждой сети (отображается в колонке **Назначено** и **Распределено**). При необходимости Вы можете изменить (кнопка **Изменить**) такой параметр на какое-нибудь ограничение, тогда в колонке **Назначено** и **Распределено** появятся соответствующие числа. Для возвращения к неограниченному значению параметра лицензии нажмите кнопку **Изменить** и в окне изменения ограничения параметра установите значение 0. Если требуется запретить создание внутренних и (или) внешних сертификатов, то в окне изменения ограничения соответствующего параметра установите значение -1.

в. Изменение лицензионных ограничений при помощи импорта из предыдущей версии файла лицензии

Вы можете импортировать все параметры лицензии из предыдущей версии файла лицензии Infotecs.reg для выбранной сети, нажав кнопку **Импорт лицензии**. Данное действие может

потребуется при переводе действующих сетей ViPNet (развернутых и функционирующих) на использование иерархической системы ЦУС. Для выполнения этого действия Infotecs.reg предыдущей версии должен находиться в папке REGS\<номер сети> папки установки ЦУС. Если файл найден, то появится вопрос **Импортировать лицензионные ограничения из файла REGS\<номер сети>infotecs.reg?** При положительном ответе лицензионные ограничения из файла отобразятся в окне **Распределение лицензионных ограничений в сети** (Рисунок 53) в колонке **Назначено**. Если при импорте для каких-то параметров лицензии суммарное число распределенных значений по всем сетям (с учетом нового значения) превысило максимальное значение, заданное в общем лицензионном файле (отображенное в колонке **Максимально**), то значение лицензионного ограничения для такого параметра лицензии не изменится. Если после импорта параметры лицензии не изменились, то появится соответствующее сообщение.

Для закрытия окна **Распределение лицензионных ограничений в сети** (Рисунок 53) нажмите кнопку **Выход**.

После произведенных настроек и выхода из окна будут сформированы файлы лицензии (infotecs.re, infotecs.reg) для тех сетей, лицензии которых изменялись.

Головной ЦУС автоматически перейдет на использование нового файла лицензии. Файлы лицензии для подчиненных сетей помещаются в экспорт для соответствующих сетей. Для передачи сформированных файлов лицензии в подчиненные сети отправьте экспорт в эти сети с помощью пункта меню **Управление/Отправить измененные файлы/Экспорт** (см. п. 21.2.4).

18 Контроль правильности конфигурации системы

Программа следит за правильностью конфигурации Вашей системы и в случае ошибок сообщит Вам об этом.

Вместе с тем, некоторые ошибки могут быть выявлены только Вашим дополнительным контролем с использованием информационно-справочных пунктов меню.

По команде меню **Службы/Просмотр конфигурации сети** Вам будет предоставлен выбор:

Выбор пользователей и ТК по сетевым объектам

Выбор пользователей и сетевых объектов по ТК

Структура сети

По команде меню **Службы/Проверка конфигурации сети** программа предоставит отчет об аномальных ситуациях.

18.1 Просмотр конфигурации сети

Выбрав пункт меню **Службы/Просмотр конфигурации сети/Выбор пользователей и ТК по узлам**, перед Вами появится список сетевых объектов (Рисунок 55).

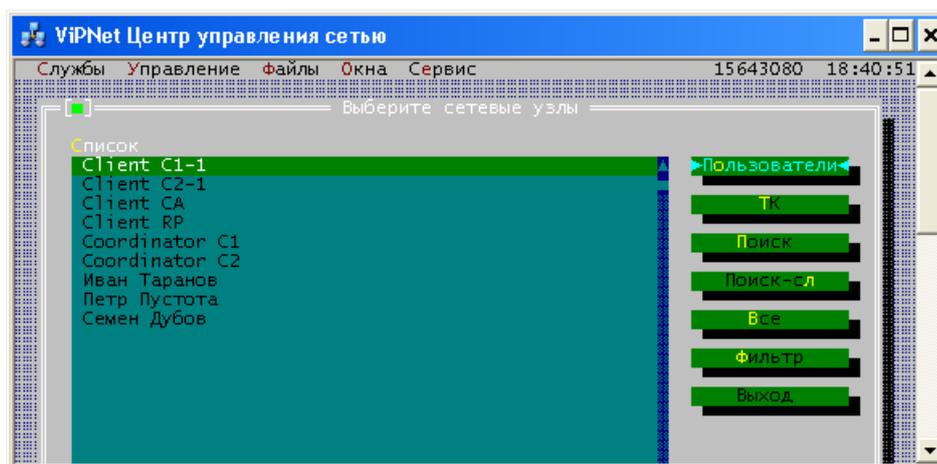


Рисунок 55

Выбрав интересующие Вас объекты, Вы можете:

Нажав кнопку **Пользователи**, просмотреть список пользователей, зарегистрированных на выбранных объектах. Убедитесь, что на всех АП и СМ зарегистрирован хотя бы один пользователь.

Нажав кнопку **ТК**, просмотреть список типов коллективов, зарегистрированных на выбранных объектах. Убедитесь, что на всех АП и СМ зарегистрирован хотя бы один ТК.

Выбрав пункт меню **Выбор пользователей и узлов по ТК** перед Вами появится список типов коллективов (Рисунок 56).

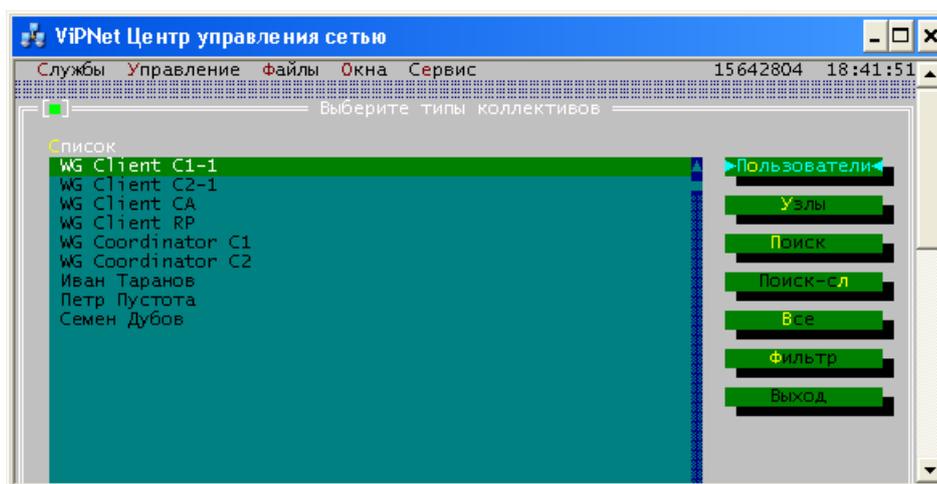


Рисунок 56

Выбрав интересующие Вас типы коллективов, Вы можете:

Нажав кнопку **Пользователи**, просмотреть список пользователей, зарегистрированных на выбранных типах коллективов. Убедитесь, что во всех ТК зарегистрирован хотя бы один пользователь.

Нажав кнопку **Узлы**, просмотреть список объектов сети (АП, СМ и группы), на которых зарегистрированы выбранные типы коллективов. Убедитесь, что каждый ТК зарегистрирован на предполагаемых Вами АП, СМ и группах. Убедитесь, что нет ТК, зарегистрированных одновременно на АП, СМ и группах.

18.1.1 Структура сети

Выбрав пункт меню **Службы/Просмотр конфигурации сети/Структура сети в широком формате** или **Структура сети в узком формате** на экране появится отчет о структуре сети,

отсортированный по номерам сети, координаторам и зарегистрированным на них АП. В этом отчете для каждого СУ отображается также перечень прикладных задач, в которых зарегистрированы узлы. Отчет может быть выведен в широком или узком формате соответственно. Этот отчет сохраняется в файле STRUCT.REP рабочего каталога ЦУС.

18.2 Проверка конфигурации сети

Выбрав пункт меню **Службы/Проверка конфигурации сети**, перед Вами появится список аномальных ситуаций, которые потенциально могут привести к проблемам при аутентификации и шифровании для созданной Вами конфигурации сети.

Вы увидите следующие списки (если они не пусты):

Список АП, не зарегистрированных ни в одной прикладной задаче.

Список АП, не имеющих ни одного пользователя.

Список АП своей сети, не зарегистрированных ни в одном ТК.

Список СМ своей сети, не имеющих ни одного пользователя.

Список ТК, не имеющих ни одной связи.

Список ТК, не имеющих ни одного пользователя.

Список АП, на которых не зарегистрирован ни один главный коллектив, ни для одного пользователя.

Список пользователей, не зарегистрированных ни в одном ТК.

Список СМ своей сети, не зарегистрированных ни в одном ТК.

Список выключенных СУ.

Список узлов, не управляемых ни одним ЦУПБ (если в сети зарегистрирован хотя бы один ЦУПБ).

Список ЦУПБ, не имеющих управляемых узлов.

Для каждой сети, в которую сформирован экспорт, Вы можете увидеть:

Не задан экспорт сетевых объектов.

Не задан экспорт ТК.

Не задан СМ-шлюз.

Список сетевых объектов, включенных в экспорт, но не входящих в область действия ни одного экспортированного ТК.

Список типов коллективов, включенных в экспорт, но в область действия которых не входит ни один сетевой объект.

Список своих ТК, имеющих связь с ТК данной сети, но не включенных в экспорт для данной сети.

Список не экспортированных ТК своей сети, но имеющих связь с ТК данной сети.

Список экспортируемых ТК, не имеющих на экспортируемых СО ни одного пользователя.

Список экспортируемых СО, не имеющих на экспортируемых ТК ни одного пользователя.

Фиксируются также события:

ни один АП не зарегистрирован в качестве ЦУС,

ни один АП не зарегистрирован в качестве Ключевого центра.

Внимательно просмотрите каждый список и, при необходимости, внесите в конфигурацию сети необходимые изменения.

Не все события, указанные в настоящих списках, означают, что Вы неправильно сформировали сеть. Например, Вы на сетевой группе из нескольких АП зарегистрировали тип коллектива и этот тип коллектива ни с кем не связали. Это означает, что Вами создана замкнутая группа, АП которой будут взаимодействовать только между собой. Такой тип коллектива появится в списке ТК, не имеющих ни одной связи, но ошибки здесь нет.

При выборе пункта меню **Сформировать все справочники** программа всегда проверяет возможные аномалии и выводит на экран указанные списки. После этой проверки программа предложит сформировать справочники. Более подробно о формировании всех справочников можно найти в главе 19.1.

При любом изменении конфигурации сети всегда полезно выполнить команду меню **Проверка конфигурации сети** и убедиться, что Вы не допустили ошибок.

Для контроля правильности установленных связей целесообразно также просмотреть справочники АП в соответствии с разделом 19.2 выбрав пункт меню **Просмотр**.

19 Формирование адресных справочников, маршрутных таблиц, справочников для УКЦ

В программе ЦУС формирование адресных справочников, маршрутных таблиц, файлов связей пользователей происходит **из меню** (см. раздел 19.1), а также **автоматически**, когда изменяется структура сети в связи с добавлением нового узла (коллектива, пользователя) при обслуживании запроса на создание дистрибутива из Центра Регистрации.

19.1 Формирование всех справочников (пункт меню "Сформировать все Справочники")

По команде **Службы/Сформировать все справочники** программа формирует абонентские справочники, маршрутные таблицы, справочники для создания ключей для тех узлов, параметры которых изменились. После этого производится поиск и запись в соответствующие подкаталоги АВН, АРДВ, EXPORT каталога \NEW рабочего каталога ЦУС и подкаталоги обмена с УКЦ всех новых файлов, появившихся после последнего выполнения этой команды.

Данную команду следует всегда выполнять после внесения каких-либо изменений в конфигурацию сети.

После формирования справочников на экране появится окно с информацией о новых файлах.

В каталоге обмена с УКЦ будут сформированы файлы, на основании которых УКЦ формирует всю необходимую ключевую информацию для узлов и конкретных пользователей сети ViPNet.

Для вновь созданных СУ ЦУС дополнительно поместит в каталог обмена с УКЦ комплект адресных справочников для создания в УКЦ дистрибутивов ключей (содержащих ключи и адресные справочники для каждого нового пользователя), необходимых для первичного запуска программного обеспечения ViPNet.

Выбрав пункт меню **Управление/Отправить измененные файлы**, Вы сможете осуществить рассылку обновленных справочников и ключей АП и СМ по соответствующим адресам или переместить их в указанные вами каталоги (см. п. 21.2).

19.2 Просмотр и копирование справочников АП (пункт меню "Справочники АП")

Программой Центра управления сетью для каждого АП формируются адресные справочники, определяющие возможности абонентского пункта по адресации корреспонденции.

По команде меню **Службы/Справочники АП** Вам будет предоставлен выбор:

Просмотр

Копирование

Выбрав пункт меню **Просмотр** (Рисунок 57), Вы сможете выбрать из списка интересующие Вас АП и просмотреть все установленные Вами связи в конкретной прикладной задаче этих АП. При просмотре конкретных справочников данный справочник формируется каждый раз заново и учитывает только что введенные Вами изменения.

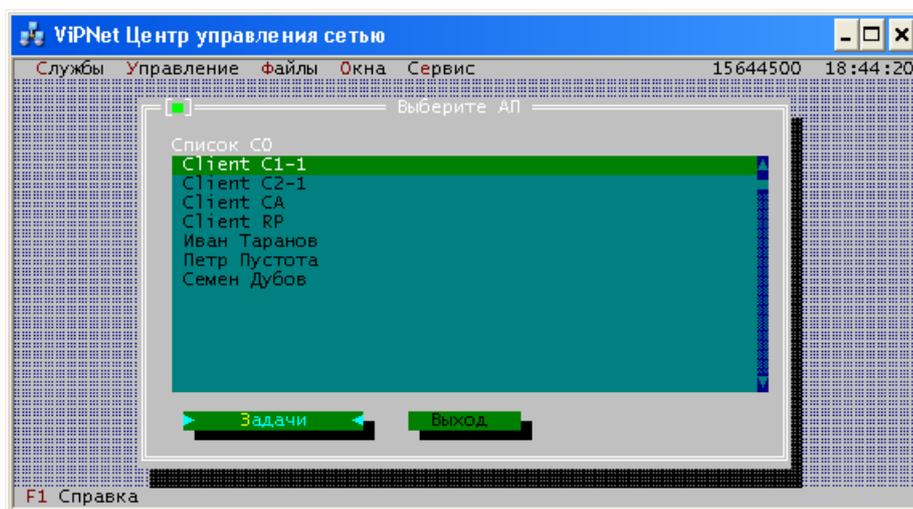


Рисунок 57

Установив курсор на интересующий Вас АП и нажав кнопку **Задачи**, Вы увидите список прикладных задач, в которых зарегистрирован выбранный АП (Рисунок 58).

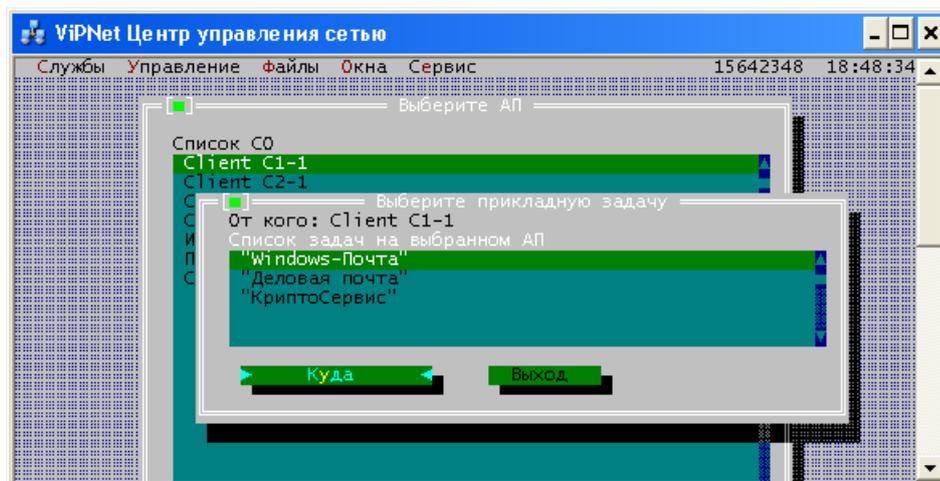


Рисунок 58

Если этот список пуст, это означает, что данный АП не зарегистрирован ни в одной из прикладных задач. В абонентских справочниках такой АП не появится.

Нажав кнопку **Куда**, Вы сможете просмотреть, с какими абонентскими пунктами связан выбранный АП в данной прикладной задаче, а также СМ, на котором зарегистрирован данный АП (Рисунок 59).

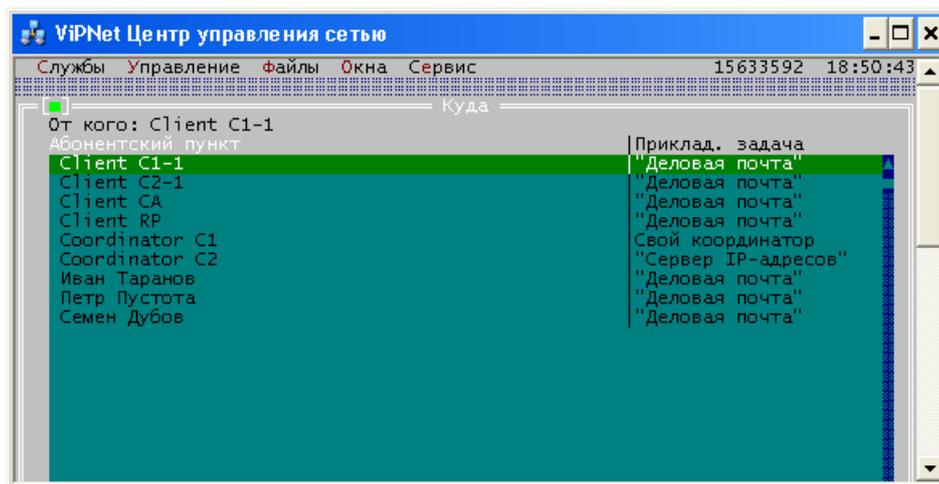


Рисунок 59

Если в этом списке не будет какого-то АП, это означает, что данный АП не зарегистрирован в соответствующей прикладной задаче или Вы не установили связь ни с одним коллективом на данном АП.

Выберите один из АП и нажмите кнопку **Копии**, перед Вами появится окно **Копии** со списком получателей копий сообщений от АП, указанного в строке **От кого:**, для АП, указанного в строке **Кому:**. Список получателей копий будет непустым, если он был задан для выбранной пары АП по команде меню **Службы/Списки рассылки/Списки рассылки копий** (см. п.14.4).

Выберите один из АП и нажмите кнопку **Кому**, перед Вами появится список коллективов, зарегистрированных на этом АП. (Рисунок 60)

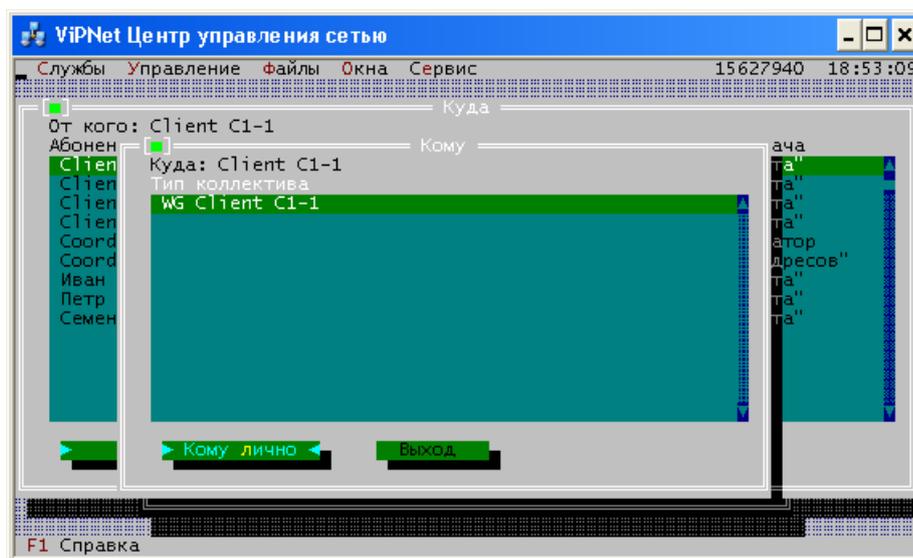


Рисунок 60

Если этот список окажется пуст, или в нем не будет какого-то коллектива, с которым Вы установили связь, это означает, что в этих коллективах не зарегистрированы пользователи.

Выбрав один из коллективов и нажав кнопку **Кому лично**, Вы узнаете список пользователей, зарегистрированных в данном коллективе (Рисунок 61).

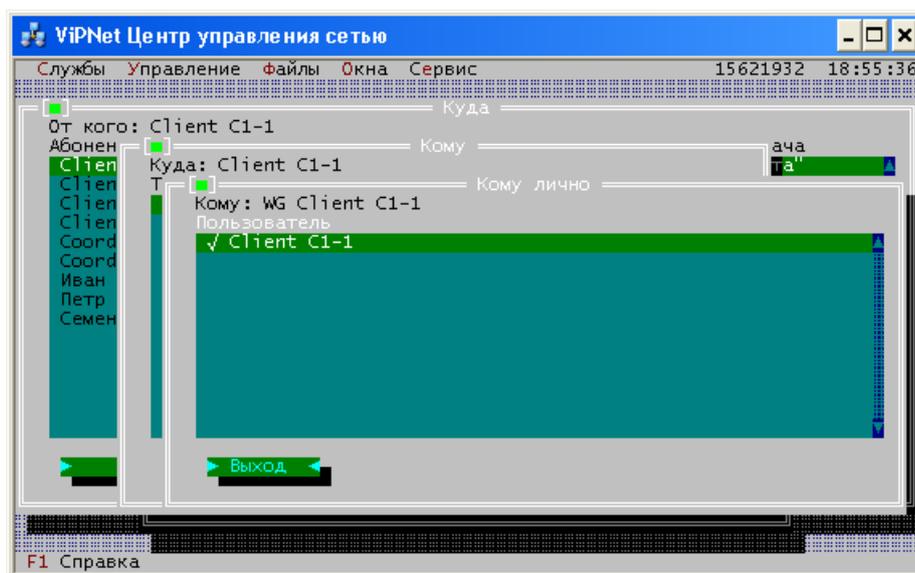


Рисунок 61

Если этот список пуст, это означает, что для всех пользователей, зарегистрированных в этом коллективе, данный коллектив является скрытым. Это может также обозначать, что Вы допустили ошибку и исключили данный абонентский пункт из сетевой группы, на которой зарегистрирован данный ТК, но не исключили из этого ТК на данном АП ранее зарегистрированных пользователей. Необходимо выбрать пункт меню **Службы/Регистрация пользователей** и сделать это.

Выбрав пункт меню **Копирование** (Рисунок 62), Вы сможете выбрать из списка интересующие Вас АП и скопировать выбранные справочники в заданный каталог.

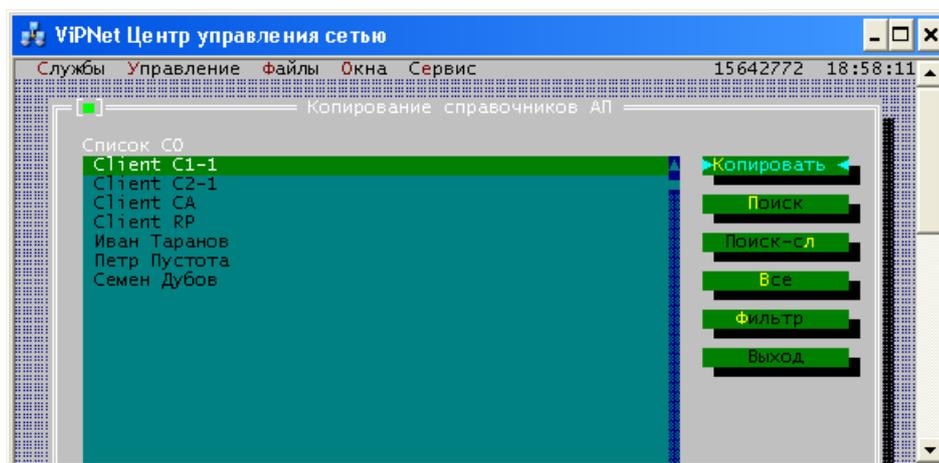


Рисунок 62

При нажатии кнопки **Копировать** по умолчанию предлагается скопировать справочники в каталог \NEW\APDB. Если Вы согласитесь с этим каталогом, то затем при помощи пункта меню **Управление/Отправить измененные файлы** сможете отправить выбранные справочники на соответствующие АП. Если укажите другой каталог то справочники перенесутся в подкаталог этого каталога с именем данного АП.

19.3 Копирование справочников СМ (пункт меню "Справочники СМ")

По команде меню **Службы/Справочники СМ** Вы сможете выбрать из списка интересующие Вас серверы и скопировать для них справочники и маршрутные таблицы в заданный каталог.

При нажатии кнопки **Копировать** по умолчанию предлагается скопировать справочники в каталог \NEW\APDB. Если Вы согласитесь с этим каталогом, то затем при помощи пункта меню

Управление/Отправить измененные файлы сможете отправить выбранные справочники на соответствующие СМ.

Если укажите другой каталог то справочники перенесутся в подкаталог этого каталога с именем данного СМ.

19.4 Формирование файлов для создания ключей в УКЦ

При выборе этого пункта меню появляется подменю, где можно выбрать и скопировать в каталог для УКЦ справочники связей СУ и пользователей, необходимые для создания в УКЦ ключевой информации, а также справочники для создания в УКЦ дистрибутивов ключей для выбранных пользователей.

Как правило, работа с пунктами этого меню не потребуется. Программа ЦУС сама во всех необходимых случаях помещает нужные файлы в соответствующие каталоги при формировании всех справочников (см. п. 19.1). Работа с этим меню может потребоваться в каких-либо нештатных ситуациях, например, когда по каким-то причинам требуется создать новую ключевую информацию для СУ, пользователя или создать новый дистрибутив ключей для существующего СУ. Также работа с этим меню потребуется при компрометациях (пункт меню **Службы/Файлы для создания ключей в УКЦ/Компрометация ключей**).

Замечание: Если запущена программа УКЦ, то при копировании справочников для УКЦ может возникнуть маловероятная ошибка копирования файла. Для того чтобы устранить эту ошибку, нужно закрыть программу УКЦ, повторить операцию в программе ЦУС и опять запустить УКЦ.

19.4.1 Файлы для создания ключей сетевых узлов

Для каждого сетевого узла формируется файл, где определены связи коллективов данного узла, со всеми другими коллективами и узлами, с которыми в программе ЦУС установили связи. Назовем эти файлы справочниками (файлами) связей сетевых узлов.

На основании этих файлов в Ключевом центре будет сформирована ключевая информация для каждого сетевого узла. Эта ключевая информация (зашифрована на ключах пользователя) размещается в подкаталоге STATION каталога, куда инсталлированы соответствующие программы на АП и координаторах.

Если требуется для каких-то СУ создать ключевую информацию в УКЦ, то воспользуйтесь пунктом меню **Службы/Файлы для создания ключей в УКЦ/Ключей узлов**. Перед Вами появится список зарегистрированных в сети абонентских пунктов и СМ. Выбрав нужные или все АП и СМ, Вы можете скопировать (с помощью кнопки **Копировать**) соответствующие справочники связей в каталог для УКЦ.

19.4.2 Файлы для создания ключей пользователей

Для каждого пользователя формируется файл, определяющий разрешенные связи для данного пользователя сети. Назовем эти файлы справочниками (файлами) связей пользователей. На основании этих файлов в Ключевом центре формируется ключевая информация для каждого пользователя.

Если требуется для каких-то пользователей создать ключевую информацию в УКЦ, то воспользуйтесь пунктом меню **Службы/Файлы для создания ключей в УКЦ/Ключей пользователей**. Перед Вами появится список зарегистрированных в сети пользователей. Отметив нужных пользователей, Вы можете скопировать (с помощью кнопки **Копировать**) соответствующие справочники связей в каталог для УКЦ.

19.4.3 Файлы для создания дистрибутивов ключей

Если новый узел только что создан в программе ЦУС, то ЦУС автоматически при формировании справочников помещает в каталог обмена с УКЦ комплект адресных справочников для создания в УКЦ дистрибутивов ключей для каждого нового пользователя, необходимых для первичного запуска программного обеспечения ViPNet.

Если требуется для каких-то пользователей сетевого узла создать в УКЦ дистрибутивы ключей, воспользуйтесь пунктом меню **Службы/Файлы для создания ключей в УКЦ/Дистрибутивы**, откроется список зарегистрированных в сети абонентских пунктов или абонентских пунктов и СМ. Выбрав нужные АП и СМ, вы можете скопировать соответствующие файлы для создания дистрибутивов ключей в папку обмена данными с УКЦ.

19.4.4 Компрометация ключей

Пункт меню **Службы/Файлы для создания ключей в УКЦ/Компрометация ключей** предназначен для формирования всех необходимых файлов для УКЦ в случае если произошла компрометация ключевой информации у одного из пользователей или всего сетевого узла в целом. В соответствии с сформированными файлами УКЦ произведет формирование новой ключевой информации, необходимой для восстановления работы сети.

Выбрав этот пункт меню, появятся два подменю **Выбор по сетевым узлам** и **Выбор по пользователям**. Если произошла компрометация ключей всех пользователей данного узла, то можно воспользоваться пунктом меню **Выбор по сетевым узлам**, в котором появится список узлов. При необходимости обозначить компрометацию ключей конкретного пользователя, следует воспользоваться пунктом меню **Выбор по пользователям**, где появится список пользователей.

Отметив пользователей или узлы с пользователями, которые считаются скомпрометированными, нажав кнопку **Компрометация**, будет запрошено подтверждение считать пользователей скомпрометированными, и после положительного ответа для УКЦ сформируются необходимые справочники.

19.4.5 Файлы для создания ключей узлов, связанных с другими сетями

При выборе пункта меню **Службы/Файлы для создания ключей в УКЦ/Ключей узлов, связанных с другими сетями** появляется окно со списком всех импортированных сетей.

Отметив нужные сети и нажав **Копировать** можно сразу сформировать необходимые справочники для создания в УКЦ ключевой информации для всех СУ, связанных с узлами выбранных сетей.

20 Работа с архивами конфигураций сети

Работа с архивами конфигураций сети ViPNet осуществляется в пункте меню **Службы/Архив конфигураций сети**. В данном пункте меню предоставляются следующие возможности:

Создать архив текущей конфигурации сети.

Восстановить одну из конфигураций сети.

Скопировать конфигурацию из архива в заданную папку.

Удалить какую-либо конфигурацию сети.

Архив конфигураций сети ViPNet создается в каталоге \ARC. В архив попадает содержимое следующих каталогов:

\DB,

\EXPORT,

\IMPORT,

Для работы с архивом выберите команду меню **Службы/Архив конфигураций сети**. По этой команде появится окно (Рисунок 63) со списком созданных ранее архивов.

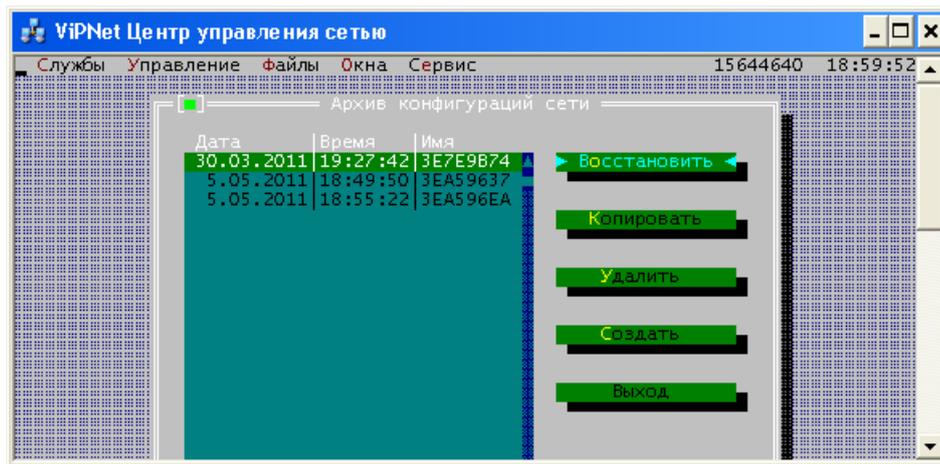


Рисунок 63

Чтобы восстановить конфигурацию, выберите ее и нажмите кнопку **Восстановить**.

При восстановлении текущая база данных ЦУС удаляется, поэтому перед восстановлением программа предложит Вам создать архив текущей базы данных ЦУС.

При нажатии кнопки **Удалить** будут удалены отмеченные конфигурации.

При нажатии кнопки **Создать** будет создан архив текущей конфигурации сети.

При нажатии кнопки **Копировать** будут скопированы отмеченные конфигурации в заданную папку.

Замечание: Поскольку конфигурации в каталоге VARC постоянно накапливаются, рекомендуем регулярно отслеживать размер каталога VARC и при слишком большом размере каталога переносить часть самых старых конфигураций на съемные диски (например, CD/DVD) или другие носители.

21 Управление сетью

21.1 Функциональное назначение

Подсистема управления работой сети решает следующие задачи:

1. Обновление в заданное время на объектах сети:

- адресных справочников на АП сети,
- маршрутных таблиц на СМ сети,
- ключевой информации на АП и СМ сети,
- дистрибутивы ключей пользователей,
- программного обеспечения на АП и СМ сети,

2. Отправка экспорта в другие сети ViPNet и прием импорта оттуда.

Отправка и получение запросов осуществляется после запуска программы транспортного модуля (ViPNet MFTP).

21.2 Отправка измененных файлов (пункт меню "Отправить измененные файлы")

При различных изменениях в структуре сети ЦУС формирует обновленные справочники СУ, а также, если изменения затрагивают другие сети ViPNet, то файлы для экспорта.

При различных изменениях ключевой информации в ЦУС от УКЦ через каталоги обмена для рассылки на СУ и автоматического обновления передаются:

- Специальные зашифрованные файлы с обновленными ключами пользователей и узлов;
- Сертификаты открытого ключа пользователей своей сети;
- Справочники сертификатов администраторов УКЦ доверенных сетей;
- Справочники отозванных сертификатов;
- Дистрибутивы ключей пользователей;
- Другие служебные файлы.

При поступлении файлов из УКЦ, программа предупредит Вас об этом и предложит отправить файлы на СУ. Если Вы согласитесь с предложением, то откроется окно отправки измененных файлов. Если Вы откажетесь, то можно отправить измененные файлы позже, выбрав соответствующий пункт меню.

Если из УКЦ поступили сертификаты ЭЦП пользователей, то ЦУС отправит их автоматически на нужный АП (без предупреждений).

Вход в подменю для отправки измененных файлов осуществляется по команде меню **Управление/Отправить измененные файлы** (Рисунок 64).

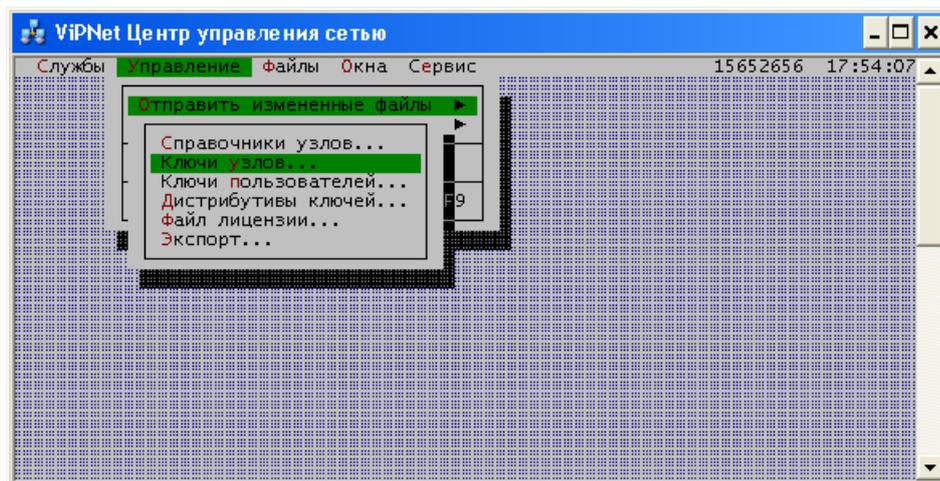


Рисунок 64

При выборе одного из пунктов этого подменю, если есть изменения в поступившем импорте от других сетей, то программа предупредит Вас об этом и предложит перед отправкой сформировать все справочники.

В этом подменю доступны следующие команды:

Справочники узлов — отправить на сетевые узлы или перенести в какой-либо каталог новые абонентские справочники и маршрутные таблицы.

Ключи узлов и **Ключи пользователей** — отправить на сетевые узлы или перенести в какой-либо каталог новые ключи узлов или ключи пользователей.

Дистрибутивы ключей — отправить на сетевые узлы или перенести в какой-либо каталог дистрибутивы ключей пользователей.

Файл лицензии — отправить на сетевые узлы файл infotecs.re.

Экспорт — Отправить в ЦУС другой сети ViPNet экспорт межсетевой информации.

Для входа в нужный пункт меню необходимо установить курсор на соответствующий пункт и нажать клавишу **Enter**.

При отправке измененных файлов на АП и СМ Вы должны указать дату и время, когда данные изменения необходимо произвести. После получения квитанций о доставке на АП или СМ новых файлов, если Вы сразу не отправили подтверждение, необходимо отправить (при помощи пункта меню **Управление/Запросы и ответы...**) дополнительное подтверждение о необходимости изменений. Если такое подтверждение на АП или СМ не поступит, то изменение произойдет после истечения заданного времени только после согласия с ним оператора на данном АП или СМ при очередном входе в соответствующую программу.

Запрос на изменение и подтверждение запроса можно отправлять одновременно.

Отправка файлов и получение произойдет после запуска транспортного модуля ViPNet MFTP.

21.2.1 Отправка справочников и маршрутных таблиц

Для отправки справочников и маршрутных таблиц войдите в пункт меню **Управление/Отправить измененные файлы/Справочники узлов**. На экране появится список АП и СМ Вашей сети, для которых есть новые справочники (Рисунок 65).

Перед отправкой Вы можете посмотреть справочники, которые будут отправлены СУ, для этого выберите АП или СМ и нажмите кнопку **Просмотр**. Откроется окно просмотра файлов.

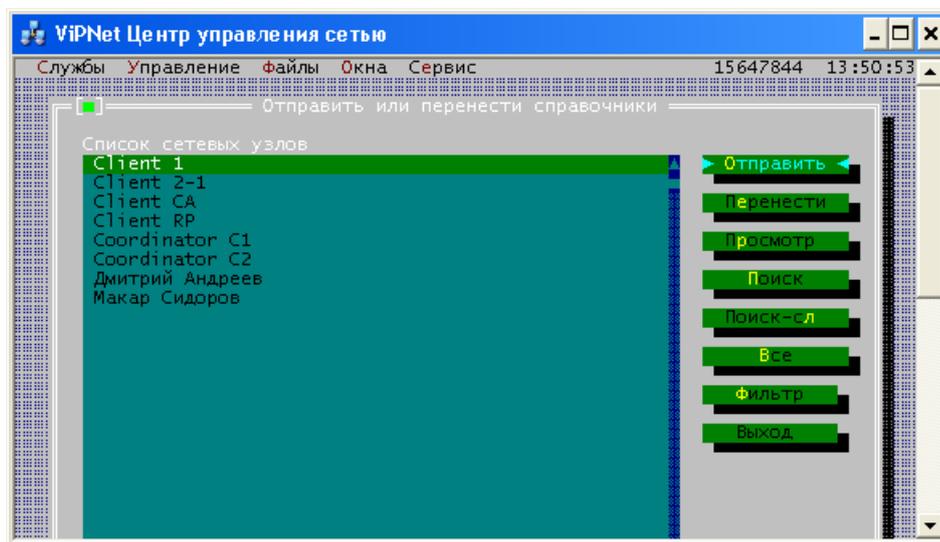


Рисунок 65

Выберите сетевые узлы, на которые требуется отправить справочники (чтобы выбрать все узлы в списке, нажмите кнопку **Все**), и нажмите кнопку **Отправить**. Откроется окно **Задайте параметры обновления**.

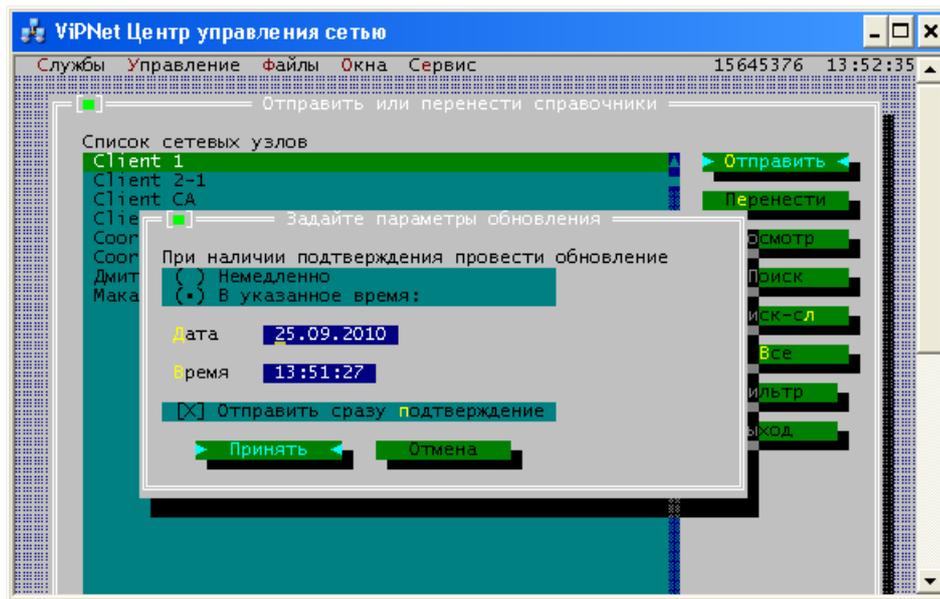


Рисунок 66

По умолчанию программа предлагает провести обновление немедленно, а также сразу отправить подтверждение обновления.

Если необходимо провести обновление в определенное время, выберите пункт **В указанное время** и в полях **Дата** и **Время** укажите дату и время обновления.

Если требуется, настройте опцию **Отправить сразу подтверждение**.

При включении опции **Отправить сразу подтверждение**, вместе с отправкой обновления произойдет отправка подтверждения обновления, тогда в назначенное время на СУ произойдет обновление.

Если Вы выключите опцию **Отправить сразу подтверждение**, то для того, чтобы на СУ произошло обновление, необходимо дополнительно отправить подтверждение обновления. Выключать эту опцию имеет смысл для тех сетевых узлов, для которых требуется обеспечить сначала доставку обновления до всех этих СУ, и только после этого разрешить на них обновление.

После нажатия кнопки **Принять** будут сформированы транспортные конверты, а отмеченные Вами запросы появятся в **Базе запросов и ответов** (см. п. 21.6), где Вы можете проконтролировать доставку конвертов адресату и прошло ли обновление. Отправка конвертов произойдет после запуска транспортного модуля.

Если Вы сразу не отправили подтверждение, то после получения квитанций о доставке на СУ обновлений, следует отправить дополнительное подтверждение о необходимости обновления при помощи пункта меню **Управление/Запросы и ответы** (см. п.21.6.4). Если такое подтверждение на СУ не поступит, то обновление произойдет после истечения заданного времени только после согласия с ним оператора на данном АП или СМ при очередном входе в соответствующую программу.

Если Вы не желаете отправлять какие-то справочники и таблицы для автоматического обновления, то для отмеченных АП и СМ нажмите кнопку **Перенести** и укажите каталог, куда должны быть перенесены отмеченные Вами справочники. При этом будут созданы подкаталоги, имена которых совпадают с идентификаторами отмеченных узлов.

21.2.2 Отправка ключевой информации

Для отправки измененных ключей выберите пункты меню **Управление/Отправить измененные файлы/Ключи узлов** и **Управление/Отправить измененные файлы/Ключи пользователей**.

Ключевая информация конкретного пользователя адресуется на тот АП или СМ, на котором зарегистрирован главный для этого пользователя коллектив.

Дальнейшая работа в этом пункте меню полностью аналогична работе в пункте меню **Управление/Отправить измененные файлы/Справочники узлов**.

Внимание! Не поддерживается отправка ключей пользователя на сетевые узлы ViPNet, работающие под управлением ОС Linux.

21.2.3 Отправка дистрибутивов ключей

Для отправки дистрибутивы ключей пользователей (файлов *.dst) выберите пункт меню **Управление/Отправить измененные файлы/Дистрибутивы ключей**.

Внимание! Дистрибутивы ключей пользователей можно отправить только на сетевые узлы ViPNet, работающие под управлением ОС Linux. При этом, если на сетевом узле был изменен пароль пользователя, отправленный на узел дистрибутив ключей не будет принят. На сетевых узлах ViPNet, работающих под управлением ОС Windows, обновление дистрибутивов ключей пользователей не обрабатывается.

Дальнейшая работа в этом пункте меню полностью аналогична работе в пункте меню **Управление/Отправить измененные файлы/Справочники узлов**.

21.2.4 Отправка Экспорта в другие ЦУС

Для отправки экспорта войдите в пункт меню **Управление/Отправить измененные файлы/Экспорт**. На экране появится список ЦУС доверенных сетей, для которых есть новые файлы (Рисунок 67).

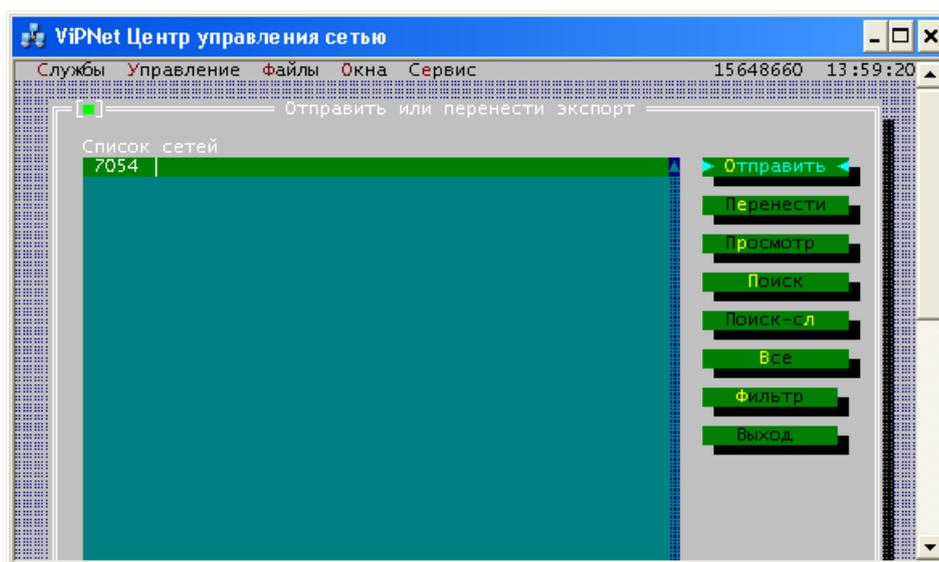


Рисунок 67

Перед отправкой Вы можете посмотреть файлы экспорта, которые будут отправлены в доверенные сети, для этого выберите сеть и нажмите кнопку **Просмотр**. Откроется окно просмотра файлов.

Если межсетевое взаимодействие с сетями установлено, то Вы можете отправить экспорт по каналам связи. Для отправки экспорта нажмите кнопку **Отправить**. Сформируются транспортные конверты, а отправленные Вами запросы появятся в **Базе запросов и ответов** (см. п. 21.6), где Вы можете проконтролировать доставку конвертов адресату. Отправка конвертов произойдет после запуска транспортного модуля (ViPNet MFTP). Информация о статусе и времени отправки, доставки и обработки экспорта в доверенных сетях появится в окне **Экспорт** (см. п. 15.1).

Если Вы не желаете отправлять Экспорт через транспортный модуль или межсетевое взаимодействие еще не установлено, то для отмеченных сетей нажмите кнопку **Перенести** и укажите каталог, куда должны быть перенесены отмеченные Вами файлы экспорта. Файлы перенесутся в заданный Вами каталог в подкаталоги с номерами сетей. Передайте файлы из каталогов администраторам ЦУС соответствующих сетей каким-либо защищенным способом.

21.3 Удаленное обновление ПО ViPNet (пункт меню "Обновить ПО")

ViPNet ЦУС предоставляет возможность администратору централизованно разослать на узлы сети ViPNet обновления программного обеспечения ViPNet – ViPNet Client, ViPNet Coordinator и ViPNet CryptoService.

Перед обновлением ПО ViPNet, если изменился файл лицензии (infotecs.re), то необходимо сначала обновить его на СУ сети. Для этого воспользуйтесь пунктом меню **Управление/Отправить измененные файлы/Файл лицензии** (см. п.21.3.2).

Для отправки нового программного обеспечения на АП или СМ войдите в пункт меню **Управление/Обновить ПО/Обновить ПО АП...** или **Управление/Обновить ПО/Обновить ПО СМ...**

Перед отправкой обновления обязательно прочитайте п. 21.3.1.

Выберите нужный архив (в соответствии с пунктом 21.3.1) и нажмите кнопку **Принять**. На экране появится список АП или СМ для выбора рассылки. Отметив те АП или СМ, на которых Вы хотите обновить ПО, следует нажать кнопку **Принять**. Откроется окно **Задайте параметры обновления** (Рисунок 68).

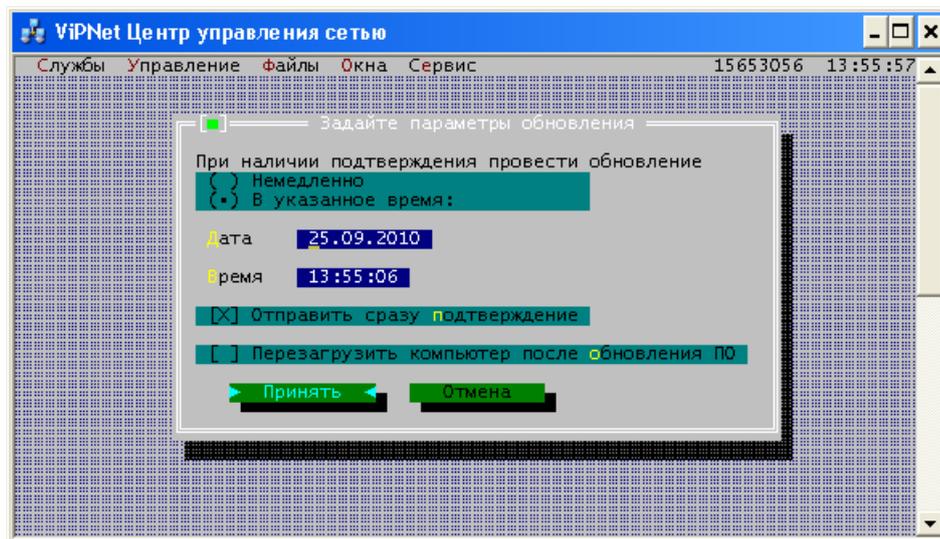


Рисунок 68

По умолчанию программа предлагает провести обновление немедленно, а также сразу отправить подтверждение обновления.

Если необходимо провести обновление в определенное время, выберите пункт **В указанное время** и в полях **Дата** и **Время** укажите дату и время обновления.

Если требуется, настройте опцию **Отправить сразу подтверждение**.

При включении опции **Отправить сразу подтверждение**, вместе с отправкой обновления произойдет отправка подтверждения обновления, тогда в назначенное время на СУ произойдет обновление.

Если Вы выключите опцию **Отправить сразу подтверждение**, то для того, чтобы на СУ произошло обновление, необходимо дополнительно отправить подтверждение обновления. Выключать эту опцию имеет смысл для тех сетевых узлов, для которых требуется обеспечить сначала доставку обновления до всех этих СУ, и только после этого разрешить на них обновление.

Далее при необходимости включите опцию **Перезагрузить компьютер после обновления ПО** для того, чтобы компьютер перезагрузился сразу после обновления ПО ViPNet (Рисунок 68). Эту опцию требуется обязательно включать при отправке обновления ПО ViPNet на координаторы, работающие без оператора (и если доступ к ним затруднен).

Если Вы при отправке обновления включите опцию **Перезагрузить компьютер после обновления ПО** (Рисунок 68), то в случае если на СУ потребуется перезагрузка компьютера,

программа выдаст соответствующее сообщение (с кнопками **ОК** – перезагрузить, **Отмена** – не перезагружать). Для того, чтобы обновление вступило в силу, необходимо перезагрузить компьютер (нажать кнопку **ОК**). Сообщение о перезагрузке появляется на 15 секунд. Если пользователь в течение этого времени не нажал ни на одну из кнопок, компьютер будет перезагружен.

Если Вы при отправке обновления опцию **Перезагрузить компьютер после обновления ПО** (Рисунок 68) не включите, то в случае если на СУ потребуется перезагрузка компьютера, программа выдаст соответствующее сообщение (с кнопками **ОК** – перезагрузить, **Отмена** – не перезагружать). Для того, чтобы обновление вступило в силу, необходимо перезагрузить компьютер (нажать кнопку **ОК**). Сообщение о перезагрузке появляется на 30 секунд. Если пользователь в течение этого времени не нажал ни на одну из кнопок, сообщение исчезнет с экрана компьютера, и ПО ViPNet перезапустится, при этом компьютер не перезагрузится. На экране появится сообщение о том, что прошло обновление и для того чтобы оно вступило в силу, компьютер следует перезагрузить. Это сообщение будет оставаться на экране, пока его не закроет пользователь. В этом случае пользователь должен перезагрузить компьютер вручную.

Далее нажмите **Принять**. После нажатия кнопки **Принять** будут сформированы транспортные конверты, а отмеченные Вами запросы появятся в Базе запросов и ответов (п. 21.6). Отправка конвертов произойдет после запуска транспортного модуля.

21.3.1 Варианты обновления и рекомендации по его проведению

Для удаленного обновления ПО ViPNet на сетевых узлах, используются различные комплекты обновлений в зависимости от операционной системы, установленной на СУ.

Если на СУ установлена ОС Windows, то рекомендации по обновлению ПО ViPNet на таких СУ читайте в п. 21.3.1.1.

Если на СУ установлена ОС Linux, то рекомендации читайте в п.21.3.1.2.

21.3.1.1 Обновление ПО ViPNet на узлах с ОС Windows

Внимание! Для обновления ПО ViPNet версии 2.8 до версии 3.1 обязательно прочитайте инструкцию по переходу на версию 3.1.

С помощью удаленного обновления версия ViPNet может быть обновлена только в рамках одного языка (т.е., например, если на СУ была установлена русская версия ПО ViPNet, то обновить ее можно только на русскую).

Удаленное обновление включает в себя следующие архивы для обновления различного ПО ViPNet на СУ:

driv_fsa.lzh – архив для обновления ПО ViPNet Client (обрабатывается программой Монитор и Деловая почта). Будут обновлены все ранее установленные на АП модули ПО ViPNet Client – Монитор и/или Деловая почта.

driv_fsn.lzh – архив для обновления ПО ViPNet Client, не содержащий модуля Контроль приложений.

driv_csa.lzh – архив для обновления ПО ViPNet Coordinator.

driv_csn.lzh – архив для обновления ПО ViPNet Coordinator, не содержащий модуля Контроль приложений.

clite_a.lzh – архив для обновления ПО ViPNet CryptoService.

ВНИМАНИЕ! Следите за правильностью присвоения начальной части имен указанным архивам. Если имя будет указано неверно, то обновления на СУ не произойдет, а поступивший архив будет удален.

21.3.1.2 Обновление ПО ViPNet на узлах с ОС Linux и мобильных устройствах

Удаленное обновление программного обеспечения ViPNet для узлов с операционной системой Linux и мобильных устройств с операционными системами iOS и Android включает в себя

следующие архивы: driv-*.lzh (динамический вариант) и driv-*-static.lzh (статический вариант), где * – параметры платформы, ОС и версии ПО ViPNet.

Для обновления ПО ViPNet на сетевых узлах с ОС Linux или мобильных устройствах необходимо выслать один из этих архивов.

ВНИМАНИЕ! Перед отправкой на сетевой узел архив нужно **ОБЯЗАТЕЛЬНО** переименовать в **driv.lzh**. Если имя будет указано неверно, то обновление на сетевом узле не произойдет.

21.3.2 Обновление файла лицензии

Внимание! На СУ файл лицензии необходимо обновить до установки новой версии ПО ViPNet на эти СУ.

Программа ЦУС позволяет произвести автоматическое обновление файла лицензии (infotecs.re) на всех СУ. Это может потребоваться, если в файле лицензии произошли какие-либо изменения. Предварительно поместите новый файл лицензии в каталог установки ЦУС. Для отправки выберите пункт меню **Управление/Отправить измененные файлы /Файл лицензии**.

Вам будет задан вопрос (Рисунок 69):

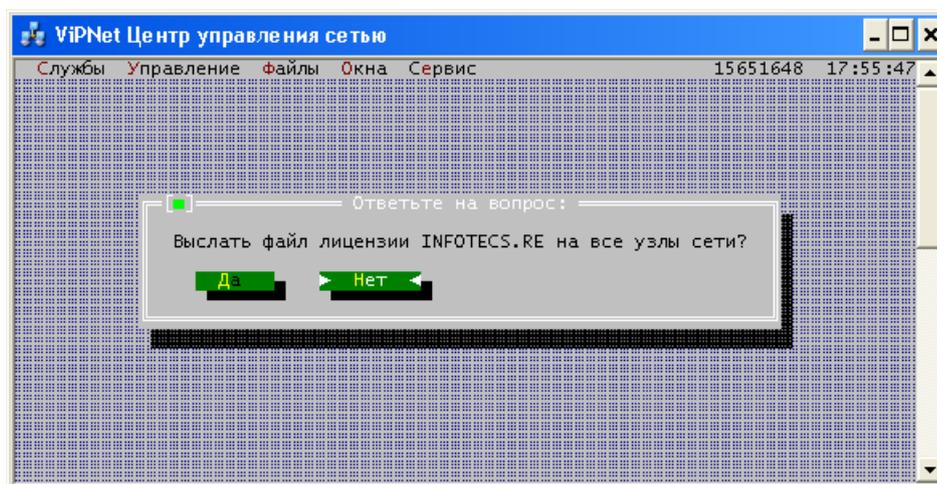


Рисунок 69

После положительного ответа на вопрос файл infotecs.re будет отправлен на ВСЕ СУ сети ViPNet.

21.4 Изменение приоритета обработки управляющих конвертов

При обновлении справочно-ключевой информации и программного обеспечения ViPNet на координаторах может поступать большое количество управляющих конвертов, формируемых ЦУС. Транспортные конверты обрабатываются модулем MFTP в соответствии с их приоритетом. По умолчанию управляющие конверты ЦУС имеют высокий приоритет, и при накоплении большой очереди из управляющих и прикладных конвертов обработка конвертов «Деловой почты» или «Файлового обмена» может сильно замедлиться.

Чтобы ускорить обработку прикладных конвертов, следует уменьшить приоритет управляющих конвертов, формируемых ЦУС. Настройка приоритета осуществляется с помощью параметра PRIOR в файле настроек NCC\DB\defset.txt. Если параметр PRIOR отсутствует в файле defset.txt, его следует туда добавить. После редактирования файла defset.txt необходимо перезапустить программу ЦУС.

Параметр PRIOR может принимать значения от 0 до 255. Чем выше значение, тем выше приоритет для управляющих конвертов.

Например, если необходимо, чтобы транспортный модуль MFTP обрабатывал конверты «Деловой почты» с более высоким приоритетом, чем управляющие конверты, нужно установить значение параметра PRIOR не выше чем 20.

Различных типы транспортных конвертов имеют следующий приоритет:

Конверты «Деловой почты»: 21.

Конверты «Файлового обмена»: 79.

Квитанции «Деловой почты» и «Файлового обмена»: 85.

Управляющие конверты (по умолчанию, если не задан параметр PRIOR): от 219 до 230.

21.5 Настройка путей (пункт меню "Пути")

Вход в данное окно осуществляется по команде меню **Управление/Пути**. На экране появится окно, в котором надо указать соответствующие пути (Рисунок 70).

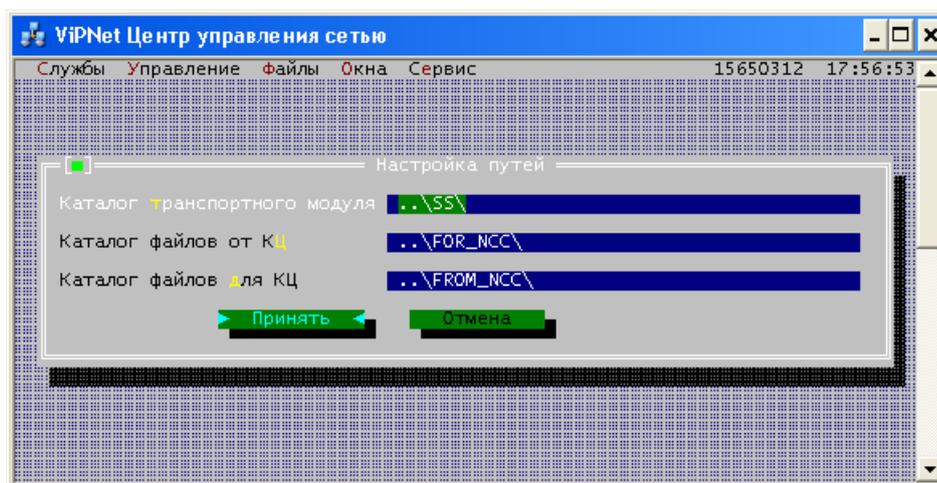


Рисунок 70

Вы должны указать пути к следующим каталогам:

каталог, где находится транспортный модуль АП, на котором установлена программа ЦУС (по умолчанию подкаталог `..\ss` каталога установки ViPNet Administrator), в этот каталог устанавливается программа ViPNet Client.

каталог, куда помещаются файлы с ключевой информацией, подготовленные в Ключевом центре (по умолчанию подкаталог `..\FOR_NCC` каталога установки ViPNet Administrator). При изменении этого каталога следует учитывать, что в настройках аналогичного каталога в УКЦ должен быть указан этот же каталог.

каталог, в который копируются файлы, предназначенные для Ключевого центра (по умолчанию подкаталог `..\FROM_NCC` каталога установки ViPNet Administrator). При изменении этого каталога следует учитывать, что в настройках аналогичного каталога в УКЦ должен быть указан этот же каталог.

21.6 База данных запросов (пункт меню "Запросы и ответы")

При выборе пункта меню **Управление/Запросы и ответы** Вы сможете просмотреть список запросов и ответов на СМ и АП с информацией о получателе, типе запроса, его статусе (запрос отправлен, получен ответ и т.д.), дате и времени отправки запроса и получения ответа, заданных дате и времени обновления ПО и др.

После выполнения этой команды перед Вами появится окно для настройки маски фильтра Базы запросов и ответов (раздел 21.6.5). Настройте фильтр по Вашему выбору и нажмите кнопку **Принять**. На экране появится окно, отображающее список удовлетворяющих фильтру запросов и ответов, отправленных и полученных программой ЦУС (Рисунок 71).

Ст	Получатель	Тип запроса	Д/В запроса	Д/В ответа
* Client RP		Отпр. подत्व. APZVZV	11.11 18:51	18.11 16:21
+R Client RP		Отпр. спр-ки APZVZV	11.11 18:51	18.11 17:01
+U Client CA		Отпр. спр-ки APKHVL	11.11 18:53	11.11 18:54
* Client CA		Отпр. подत्व. APKHVL	11.11 18:53	11.11 18:53
* Client RP		Отпр. подत्व. APZLVJ	11.11 18:53	18.11 16:21
+R Client RP		Отпр. спр-ки APZLVJ	11.11 18:53	18.11 17:01
+U Client CA		Отпр. спр-ки APZKGD	12.11 10:36	12.11 10:37
* Client CA		Отпр. подत्व. APZKGD	12.11 10:36	12.11 10:36
+R Client RP		Отпр. спр-ки APYWKG	12.11 10:36	18.11 17:01
* Client RP		Отпр. подत्व. APYWKG	12.11 10:36	18.11 16:21
* Client CA		Отпр. подत्व. APVGGF	12.11 10:39	12.11 10:39
+U Client CA		Отпр. спр-ки APVGGF	12.11 10:39	12.11 10:39
+R Client RP		Отпр. спр-ки APVEZJ	12.11 10:39	18.11 17:01
* Client RP		Отпр. подत्व. APVEZJ	12.11 10:39	18.11 16:21
+U Client CA		Отпр. спр-ки APKWYZ	15.11 18:18	15.11 18:20
* Client CA		Отпр. подत्व. APKWYZ	15.11 18:18	15.11 18:18
* Client RP		Отпр. подत्व. APDGVD	15.11 18:18	18.11 16:21
+U Client RP		Отпр. спр-ки APDGVD	15.11 18:18	18.11 17:01
Coordinator C1		Отпр. подत्व. KEAHEI	15.11 18:21	
+ Coordinator C1		Отпр. ключи KEAHEID	15.11 18:21	
+U Client CA		Отпр. ключи KEADDLY	15.11 18:21	15.11 18:22
* Client CA		Отпр. подत्व. KEADDL	15.11 18:21	15.11 18:21
* Client RP		Отпр. подत्व. KEAKZK	15.11 18:21	18.11 16:21
+U Client RP		Отпр. ключи KEAKZKH	15.11 18:21	18.11 17:01
+ Client 1		Отпр. ключи KEAKWKG	15.11 18:21	
Client 1		Отпр. подत्व. KEAKWK	15.11 18:21	
Макар Сидоров		Отпр. подत्व. KEANGV	15.11 18:21	
+ Макар Сидоров		Отпр. ключи KEANGVG	15.11 18:21	
+ Дмитрий Андреев		Отпр. ключи KEADDV	15.11 18:21	
Дмитрий Андреев		Отпр. подत्व. KEADFMK	15.11 18:21	
+ Coordinator C2		Отпр. ключи KEADFM	15.11 18:21	
Coordinator C2		Отпр. подत्व. KEADFM	15.11 18:21	
Client 2-1		Отпр. подत्व. KEAIWI	15.11 18:21	
+ Client 2-1		Отпр. ключи KEAIWII	15.11 18:21	
+U Client CA		Отпр. спр-ки APEDMF	18.11 17:03	18.11 17:04
* Client CA		Отпр. подत्व. APEDMF	18.11 17:03	18.11 17:03
* Client RP		Отпр. подत्व. ARMJEN	18.11 17:03	18.11 17:03
+U Client RP		Отпр. спр-ки ARMJEN	18.11 17:03	18.11 17:06

Рисунок 71

Верхняя строка в окне содержит сокращенные названия следующих полей (колонок):

“Ст” - статус отправленного запроса:

'U' означает, что запрос упакован (сформирован), но еще не отправлен;

'пробел' означает, что запрос отправлен, но ответ на него пока не получен;

'*' - ответ получен;

'√' - ответ (отчет по журналам, очередь, настройки Сервера и т. д.) просмотрен;

'П' - запрос отправлен повторно;

'+' - передано подтверждение на обновление файлов;

'A' - передано подтверждение на обновление ПО с автоматической перезагрузкой компьютера;

'!' - передан откат (отказ от обновления файлов);

'U' - обновление справочников, ключей или ПО прошло;

'R' - обновление справочников, ключей или ПО не прошло (был откат или другие причины);

Замечание. Статусы 'U' и 'R' указывают на успешное или неуспешное обновление файлов только в случае отправки справочников, ключей или ПО. При отправке другой информации, в том числе сертификатов и СОС, статусы 'U' и 'R' не отображаются.

'!' - на запрос получена квитанция "Управление запрещено";

- '?' - на запрос получена квитанция "Запрос искажен";
- '#' - на запрос получена квитанция "Неизвестная команда";
- 'N' - на запрос получена квитанция "Нет ключа";
- '%' - на запрос получена критическая транспортная квитанция;
- '@' - на СМ нет запрошенных файлов или они не изменились.

“Получатель”	имя получателя запроса.
“Тип запроса”	информация о типе направленного запроса: “Отправить ключи”, “Отправить справочники”, “Отправить экспорт”, “Отправить ПО” и др.
“Д/В запроса”	дата и время формирования запроса.
“Д/В ответа”	дата и время получения ответа.

Нажав кнопку **Инфо**, можно более подробно просмотреть информацию о получателе, типе запроса, статусе, дате и времени отправки выбранного запроса и ответа на него.

Нажав кнопку **Копировать**, можно скопировать выбранные конверты в заданную папку (по умолчанию предлагается папка COPYENV).

Нажав кнопку **Отчет** или клавишу **F2**, можно сохранить текущий отчет по базе данных запросов в файле.

21.6.1 Просмотр ответа на запрос

Установив курсор на интересующий Вас запрос и нажав кнопку **Просмотр**, Вы можете просмотреть полученный ответ.

Если запрос связан с отправкой какой-либо информации на СМ или АП, то, нажав кнопку **Просмотр**, Вы сможете просмотреть содержимое отправленного запроса.

После просмотра ответа на запрос, связанного с получением какой-либо информации, в поле “Ст” появится отметка '√'.

21.6.2 Повторение запроса

Если запрос уже отправлен, но ответ на него не получен, то, нажав кнопку **Повтор**, можно отправить этот запрос повторно. При этом в поле “Ст” появится признак 'П'.

Если ответ на запрос к СМ получен, то, нажав кнопку **Повтор**, можно сформировать новый запрос этого же типа и в этот же адрес.

Запрос на отправку ПО, ключей, справочников и таблиц можно повторить, даже если пришел ответ. При этом отправляется копия конверта, а в поле “Ст” появится признак 'П'.

Подтверждения и откаты можно повторять пока на них не придет ответ.

Отправка повторного запроса произойдет только после вызова транспортного модуля по клавишам **F7** или **F8**.

21.6.3 Удаление запроса

Для удаления отмеченных запросов следует нажать кнопку **Удалить**.

При удалении записи о запросе будут удалены ассоциированные с ним файлы запроса и ответа. Если конверт с запросом еще не отправлен, он также будет удален.

21.6.4 Отправка подтверждений и откатов на запросы

Подтверждения запроса требуют только запросы, для которых указано время их исполнения, то есть запросы на отправку ПО, ключей, справочников и таблиц. Только эти запросы можно откатить, то есть запретить их исполнение.

Подтвердить и откатить можно как запросы, на которые пришли квитанции о приеме, так и еще не отправленные или не доставленные запросы.

Откатить запрос можно, если не истекло время его исполнения.

После подтверждения запроса можно его откатить. Однако если на запрос сформирован Откат, то подтвердить его уже нельзя.

Для формирования Подтверждения или Отката следует установить курсор на соответствующий запрос или отметить несколько запросов и затем нажать кнопку **Подтверждение** или **Откат**. При этом в поле "Ст" соответствующих запросов появится отметка '+' или '-'.

Отправка Подтверждений и Откатов произойдет только после вызова транспортного модуля.

21.6.5 Фильтрация и сортировка записей в базе запросов и ответов

При нажатии кнопки **Фильтр/Сорт** на экране появится меню:

Фильтровать базу запросов,

Выбрать получателя,

Сортировать базу запросов.

Выбрав пункт **Фильтровать базу запросов**, можно задать фильтр базы запросов по дате формирования запроса, дате получения ответа, типу запроса, его статусу и типу отправленных файлов (Рисунок 72).

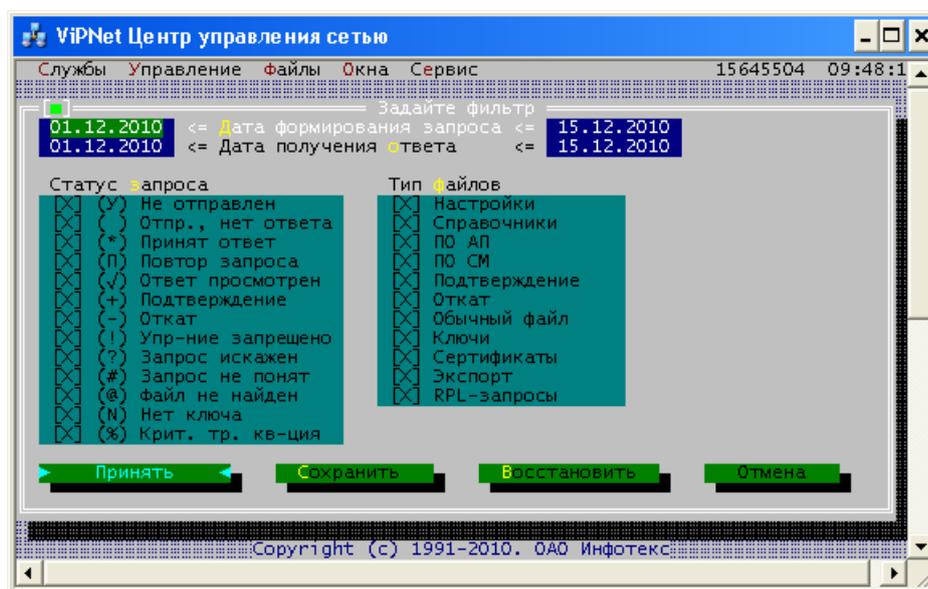


Рисунок 72

Выбрав фильтр и нажав кнопку **Сохранить**, можно запомнить под определенным именем файла наиболее часто используемые фильтры.

Нажав кнопку **Восстановить**, можно выбрать интересующий вас фильтр из сохраненных.

Отметка и снятие маски для участия в поиске на определенном поле фильтра осуществляется нажатием клавиши «Пробел» или мышью. Чтобы какое-то поле не участвовало в поиске, надо удалить в этом поле символ "X".

Например, если Вы хотите сохранить под именем APDB.CDB фильтр, позволяющий отобразить все запросы, подтверждения и откаты на обновление справочников АП, в колонке **Тип файла** оставьте отмеченными поля **Спр-ки и табл.**, **Подтверждение** и **Откат**.

Нажмите кнопку **Сохранить**, введите указанное имя и нажмите кнопку **Принять**.

Выбрав пункт меню **Выбрать получателя**, Вы сможете отфильтровать записи по конкретному сетевому узлу (АП или СМ).

Выбрав пункт меню **Сортировать базу запросов**, вы сможете выполнить сортировку базы запросов и ответов по выбранным полям:

по дате формирования запроса (по умолчанию),

по адресу получателя,

по статусу запроса,

по типу запроса.

21.6.6 Просмотр содержимого отправленного запроса

При необходимости просмотреть содержимое запросов, отправляемых в виде упакованных и зашифрованных файлов (так отправляются справочники, ПО и т.д.) можно при просмотре базы **Запросы и ответы** нажать кнопку **Просмотр**. Запрос будет расшифрован и его содержимое будет выведено в виде списка файлов. Каждый из этих файлов можно просмотреть на экране.

22 Дополнительные сервисные возможности

22.1 Просмотр информации о лицензии

По команде меню **Сервис/Лицензия** на экран будет выведена информация о лицензии, выданной Вашей сети, и о текущих параметрах использования этой лицензии по следующим элементам:

номер и название Вашей сети,

если сеть является подчиненной, то указывается номер головной сети,

версия ViPNet Administrator,

число использованных дней срока лицензии, если он ограничен,

число Серверов-маршрутизаторов,

число абонентских пунктов,

количество пользователей в сети,

число открытых адресов IP-сети, которое может туннелироваться в данной сети,

число элементов кластера, если лицензирована задача **ViPNet Cluster**,

число адресов Web-шлюза, если лицензирована задача **Web-шлюз**,

число связей ТК, которые возможно задать в сети, если они ограничены,

в случае ограничения количества сертификатов для внутренних и внешних пользователей будет указано количество изданных сертификатов/количество сертификатов, ограниченных лицензией (например, 55/100),

далее отображен список лицензированных прикладных задач и число узлов, которое позволяет зарегистрировать Ваша лицензия в каждой из задач, а также число уже зарегистрированных в каждой задаче узлов.

Эта информация сохраняется в файле Susp.ger в папке установки ЦУС.

22.2 Контекстно-чувствительная справка

Встроенная контекстно-чувствительная справочная информация появляется с помощью нажатия клавиши **F1**. Любой экран справочной информации может содержать одно или более ключевых слов (высвеченных элементов), по которым можно получить дополнительную справочную информацию, нажав клавишу **Enter**. Передвижение между ключевыми словами осуществляется с помощью клавиш **Tab**, **Shift+Tab**. Листание экрана осуществляется с помощью клавиш управления курсором. Клавиша **Alt+F1** показывает предыдущий экран справочной информации.

22.3 Просмотр файла

По команде **Файлы/Просмотреть файл** возникает диалоговое окно **Просмотр файла**. В этом диалоговом окне Вы должны выбрать имя текстового файла для просмотра. В окне **Просмотр файла** можно просматривать содержимое текстового файла. Для передвижения по файлу можно использовать мышь и линейки прокрутки или клавиши управления курсором:

Up	Передвижение экрана вверх на одну строку
Down	Передвижение экрана вниз на одну строку
Right	Передвижение экрана вправо на один столбец
Left	Передвижение экрана влево на один столбец
PgUp	Передвижение экрана вверх на одну страницу
PgDn	Передвижение экрана вниз на одну страницу
Home	Просмотр самого левого столбца файла
End	Просмотр самого правого столбца файла
Ctrl+PgUp	Просмотр начала файла
Ctrl+PgDn	Просмотр конца файла.

По клавише **F4** файл можно вывести на печать.

22.4 Удаление, копирование и переименование файлов

По команде **Файлы/Удалить файл...** вызывается диалоговое окно выбора имени файла, подлежащего удалению. По умолчанию для имен файлов предлагается маска *.*. Выбранный файл будет удален. Отменить удаление можно, нажав клавиши **Esc**, кнопку **Отмена** или закрывающую кнопку окна.

По команде **Файлы/Переименовать файл...** вызывается диалоговое окно выбора имени файла, подлежащего переименованию. По умолчанию для имен файлов предлагается маска *.*. После выбора файла вызывается окно ввода нового имени. Отменить переименование можно, нажав клавиши **Esc**, кнопку **Отмена** или закрывающую кнопку окна.

По команде **Файлы/Копировать файл...** вызывается диалоговое окно выбора имени файла, подлежащего копированию. По умолчанию для имен файлов предлагается маска *.*. После выбора файла вызывается строка ввода нового имени. Отменить копирование можно, нажав клавиши **Esc**, кнопку **Отмена** или закрывающую кнопку окна.

22.5 Временный выход в операционную систему

Выполнив команду **Файлы/ДОС**, оператор временно выходит из программы для того, чтобы выполнить некоторую команду DOS или запустить другую программу.

Для возвращения в программу надо набрать EXIT в ответ на приглашение DOS.

22.6 Смена видеорежима

По команде **Сервис/Видео режим...** вызывается диалоговое окно **Видео режим**.

В диалоговом окне **Видео режим** оператор может установить цветной или черно-белый режим вывода и переключить число строк с 25 на 43 для адаптера EGA или 50 для адаптера VGA. Изменения не влияют на экран до тех пор, пока диалоговое окно не будет закрыто кнопкой **Принять**.

При нажатии кнопки **Восстановить** будет восстановлен исходный видеорежим.