ACP Ideco 3

Руководство пользователя

http://www.ideco-software.ru

Автоматизированная система расчётов АСР Ideco 3
Руководство пользователя

Обратная связь

Если вы заметили ошибку в предлагаемой документации (быстрый запуск, руководство пользователя, online-справка или в readme файлах) или хотите высказать свои соображения по её содержанию, напишите нам по адресу docfeedback@ideco-software.ru.

http://www.ideco-software.ru
Дата редакции: июль 2010 года

Содержание

Часть I

1 Введение

Биллинговая система ACP Ideco 3

Автоматизированная система расчетов ACP Ideco - современная сертифицированная биллинговая система оптимально подходящая для небольших и средних Интернет-провайдеров, а также для офисных центров, гостиниц, ВУЗов и многих других.

Весь необходимый функционал для Интернет-провайдера

- Гибкие тарифы, возможность задавать стоимость в зависимости от подсетей, объема и времени суток, предоплаченный трафик
- Безлимитные тарифы возможность задавать скорость в зависимости от объема, времени суток и подсетей, ежедневная и ежемесячная абонентская плата
- Тарификация и отключение в реальном времени, рассылка предупреждений
- Поддержка NetFlow и RADIUS
- Поддержка SNMP, CoA, SSH, Telnet для управления сетевым оборудованием
- Полноценный сайт провайдера на CMS 1C-Bitrix
- Личный кабинет пользователя - статистика, смена тарифа и пароля, история операций, уведомления и др.
- Ведение лицевых счетов, договоров, финансовые операции, автоматическое формирование и печать документов, настройка шаблонов
- Карты оплаты для пополнения баланса, карты для анонимного разового подключения, карты с ограничением по времени для безлимитных тарифов
- Возможность иерархической группировки пользователей с большим уровнем вложенности
- Поддержка платежных систем: ОСМП, Город, RoboKassa, ComePay, QuickPay, RPS, SFOUR и другие
- Веб-интерфейс кассира
- Удобный графический интерфейс ACP Manager
- Возможность интеграции с внешними системами и 1С по различным протоколам
- Распределение полномочий дополнительным администраторам и операторам
- Поддержка СОРМ

- Возможность учета и списания дополнительных периодических услуг
- Хранение подробной статистики посещений в компактном формате, просмотр через личный кабинет, ТОП-100
- Поддержка маршрутизаторов и NAS-серверов: Ideco AS 3000, CISCO, SUN, MikroTik, D-Link, NSG, Revolution, Nomadix, PC router, Huawei, hotspot

Версия ACP Ideco 3 SoftRouter

Дополнительно включает в себя следующие возможности:

- Возможность работы без дополнительного маршрутизатора, сервер ACP Ideco 3 выступает маршрутизатором
- Авторизация пользователей по VPN-PPTP, PPPoE, L2TP, IP+MAC, IdecoAgent, веб-интерфейс
- Firewall, VPN, NAT, DNS, DHCP, FTP, интеллектуальный QoS, Shaper, NTPD
- Возможность установки до 3000 VPN соединений одновременно на один сервер
- Возможность иерархического распределения канала по тарифам в формате HTB rate & ceil
- Графики загруженности MRTG

Возможности для гостиниц, ВУЗов и офисных центров

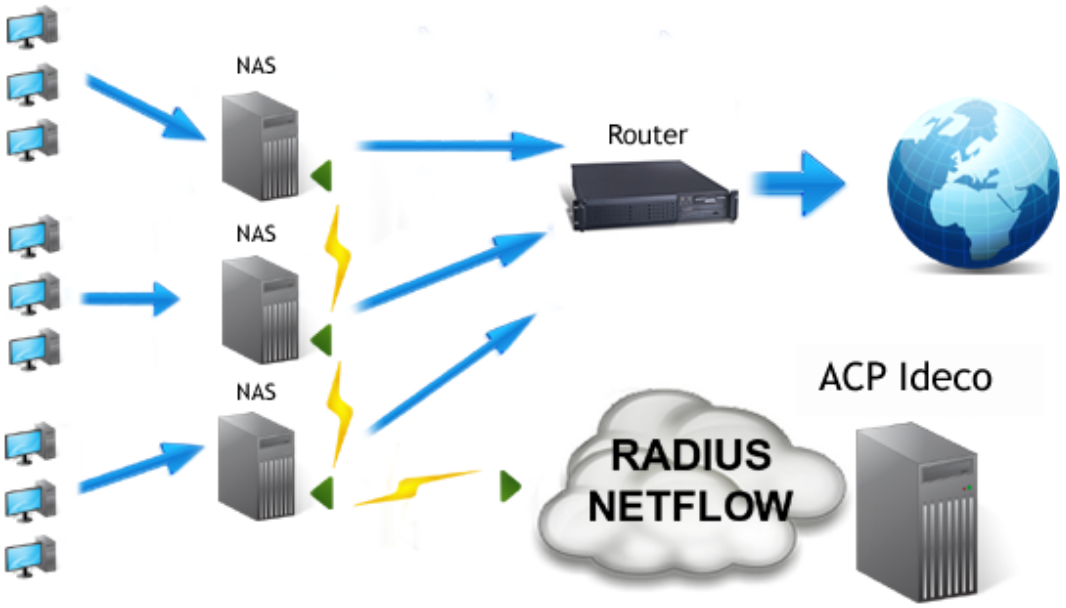
- Собственный почтовый сервер со встроенным антиспамом
- Веб-сервер, возможность кэширования трафика и антивирус
- Поддержка нескольких интернет каналов, резервирование и автоматическое переключение

Преимущества ACP Ideco 3

- Самая простая установка и управление из всех систем представленных на рынке. ACP Ideco 3 - полностью готовое решение, устанавливается с одного компакт диска на "пустой" компьютер и сразу готов к работе.
- Идеально подходит для начальных и средних провайдеров уровня города или района
- В базовую поставку включены все необходимые для работы функциональные модули
- Минимальные требования к сопровождению и квалификации технического персонала.
- Гибкая схема лицензирования. Возможность постепенного увеличения лицензии, вместе с ростом вашего бизнеса.
- Для начала работы не требуется дополнительного программного обеспечения и ОС.

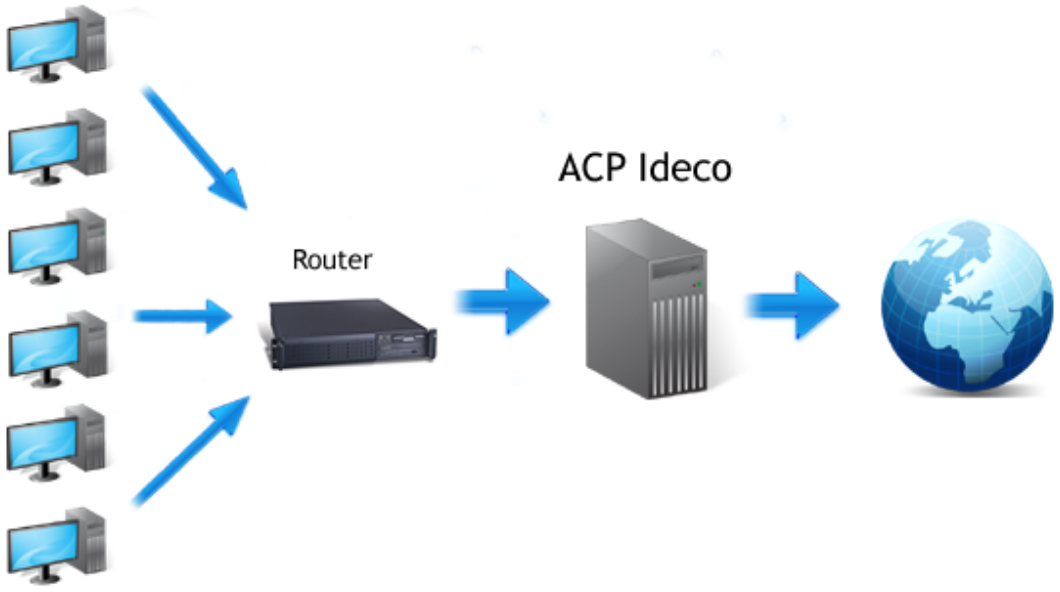
- В версии SoftRouter достаточно иметь сервер и канал подключения к вышестоящему провайдеру.
- Поддержка распределенных сетей, позволяет подключать до 100000 абонентов.
- Учет трафика и отключение абонентов в режиме реального времени.
- ACP Ideco 3 построена на базе ядра Linux, имеет беспрецедентную надежность, сравнимую с аппаратными решениями.
- Встроенный модуль отказоустойчивости восстановит систему даже в случае сбоя.
- Существует многоуровневая системы защиты сервера от внешних угроз.
- Бесплатная помощь в развертывании, демо-период 70 дней.

Схема использования ACP Ideco 3



Сеть провайдера разделена на IP-сегменты или VLAN, каждый из которых обслуживается Ideco AS 3000 или другим NAS-сервером или коммутатором. Интернет-трафик раздается при помощи маршрутизатора, установленного на границе с Интернетом. NAS-серверы или коммутаторы подключены к этому маршрутизатору. Авторизации и контроль трафика пользователей осуществляются при помощи технологий Radius и Netflow, запущенных на сервере Ideco ACP. Ideco ACP имеет возможность как принимать так и отсылать команды NAS серверам и коммутаторам по SNMP/Telnet/SSH/CoA. Таким образом, авторизация и учет трафика возлагается на ACP Ideco. С такой схемой построения сети возможно до 50000-100000 зарегистрированных пользователей; Ширина канала ограничена лишь пропускной способностью сети и возможностями маршрутизатора.

Схема использования ACP Ideco 3 SoftRouter в качестве шлюза



ACP Ideco 3 работает в качестве шлюза, устанавливается на границе между Интернет и локальной сетью. Весь интернет-трафик проходит через ACP Ideco что обеспечивает подсчет, блокирование и лимитирование скорости.

Возможности при такой схеме подключения:

- 7000 пользователей с авторизацией по IP и шириной канала до 400 МБит;
- 3000 пользователей с авторизацией по VPN/PPPoE одновременно и шириной канала до 300 МБит;
- Всего VPN пользователей может быть зарегистрировано до 7-15 тыс. с учетом коэффициента одновременности.

http://www.ideco-software.ru

Версия документа 1.07

Последние изменения: 01 июля 2010 г.

Часть II

2 Установка

В этом разделе описывается процесс установки сервера Ideco ACP.

2.1 Системные требования

Системные требования:

- Процессор Intel Pentium/Celeron/Dual-Core/Core 2 Duo/Xeon
- Системная плата на чипсете Intel.
- Память 512 Мб или больше.
- Жесткий диск объемом 80 Гб или больше с интерфейсом

SATA/SCSI, либо совместимый аппаратный RAID.

- Две сетевые карты. Рекомендуется карты на чипах

Broadcom, Intel, Realtek или D-Link (кроме DL-520 и DGE-528T).

Интегрированные сетевые карты на бюджетных материнских платах использовать не рекомендуется.

- CD-ROM или DVD-ROM с интерфейсом IDE, SATA или USB.
- Монитор.
- Клавиатура.

Замечания

- Нашим продуктом поддерживаются только процессоры фирмы Intel
- Не поддерживаются системные платы на чипсетах NVIDIA, VIA и ATI, процессоры AMD64.
- Для SATA дисков необходимо в BIOS включить режим IDE, Legacy или Compatible.
- Ядро сервера поддерживает более 4 Гб оперативной памяти (если это поддерживается вашей материнской платой). Для этого необходимо включать ядро PAE(setupbigmem), однако следует обратить внимание на то, что в данном режиме могут неверно работать некоторые драйвера.
- В зависимости от объема трафика и продолжительности хранения детализированной статистики, может потребоваться увеличение объема накопителя, или установка дополнительного. Для хранения данных встроенных сервисов (FTP, Web-сервер, почтовый сервер, прокси-сервер и др.) также может потребоваться дополнительное место.
- Для установки и работы Ideco ACP не требуется предустановленная ОС и дополнительное программное обеспечение. Ideco ACP устанавливается на выделенный сервер с загрузочного CD-R/RW, при этом автоматически создается файловая система и устанавливаются все необходимые компоненты.
- Для подключения к серверу достаточно стандартных программ ОС Windows, Linux или Mac OS X.
- При установке на компьютер с большим количеством ядер (больше 8), необходимо в биосе отключить HyperTraning, Virtualizationg Technology (может

быть VTX) и NXbit.

- Если памяти более 4Гб необходимо вместо setup вводить setupbigmem
- При установке на виртуальную машину необходимо вместо setup вводить setup100hz

2.2 Подготовка к установке

Ideco ACP устанавливается на отдельный компьютер с пустым жестким диском.

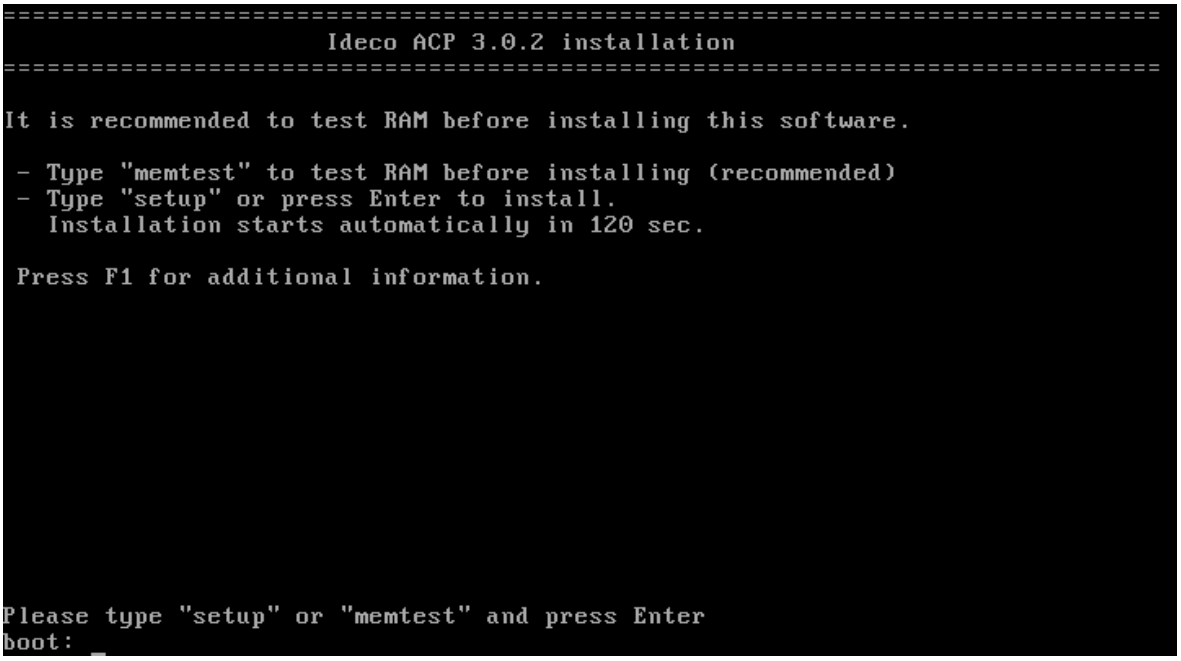
Этапы:

1. Скачайте файл ISO образа по ссылке, полученной после **заполнение формы** (http://ideco-software.ru/products/billing/bill_trial.aspx?type=Download&prod_ver=ACP3000), и сохранить его на жесткий диск. У скачанного образа проверьте контрольные суммы MD5, которые доступны на странице загрузки после заполнения формы.
2. С помощью CD-RW привода и программы для записи запишите ISO образ на чистый CD-R/RW диск. Большинство программ для записи распознают ISO-файлы.
3. Установите правильные время и дату в BIOS.
4. Записанный CD-R/RW вставьте в привод чтения компакт дисков компьютера, на который хотите установить Ideco ACP. Загрузитесь с этого загрузочного CD и следуйте дальнейшим пошаговым инструкциям появляющимся на экране.

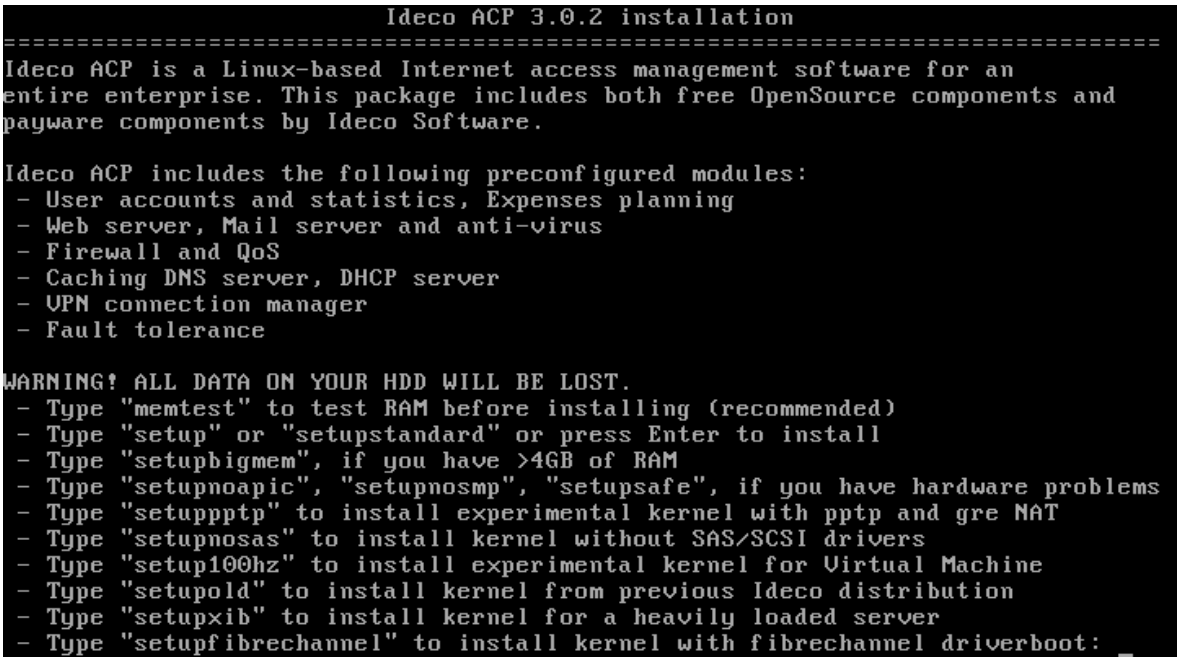
Примечание. На странице заполнения формы вам предварительно необходимо будет указать контактную информацию о себе, после станут доступны прямые ссылки на ISO образ. Там же будут указаны MD5 суммы для проверки скачиваемого файла на целостность данных после получения по сети. Настоятельно рекомендуется проверить скачанный образ на совпадение MD5 сумм со значениями на сайте.

2.3 Установка с диска. Мастер первоначальной настройки.

Диск с образом Ideco ACP 3.0 вставьте в привод чтения компакт-дисков сервера на котором требуется произвести установку. В параметрах BIOS компьютера вам надо выбрать загрузку с CD/DVD. При успешной загрузке с диска у вас на экране появится текстовая консоль с приглашением boot:. Для начала процесса установки напишите setup и нажмите Enter или просто нажмите Enter (параметр загрузчика "setup" уже выбран по умолчанию). Так же можно перед установкой запустить утилиту memtest для проверки оперативной памяти компьютера. В случае выбора memtest рекомендуем оставить компьютер на несколько часов для циклического прохождения синтетических тестов, например на ночь.

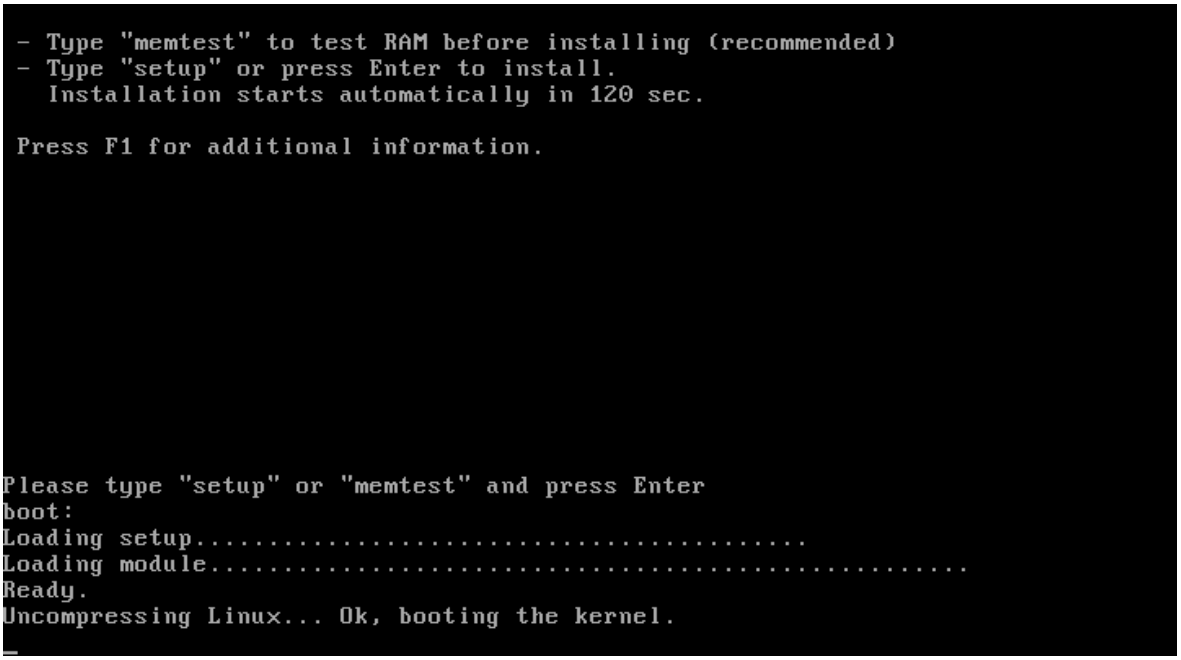


Нажмите F1 для получения справки по возможным режимам установки Ideco ACP. Обычно прибегать к этим режимам не приходится, используются они в случае если стандартный режим установки ("setup") не работает. За более подробной информацией обратитесь в отдел технической поддержки.

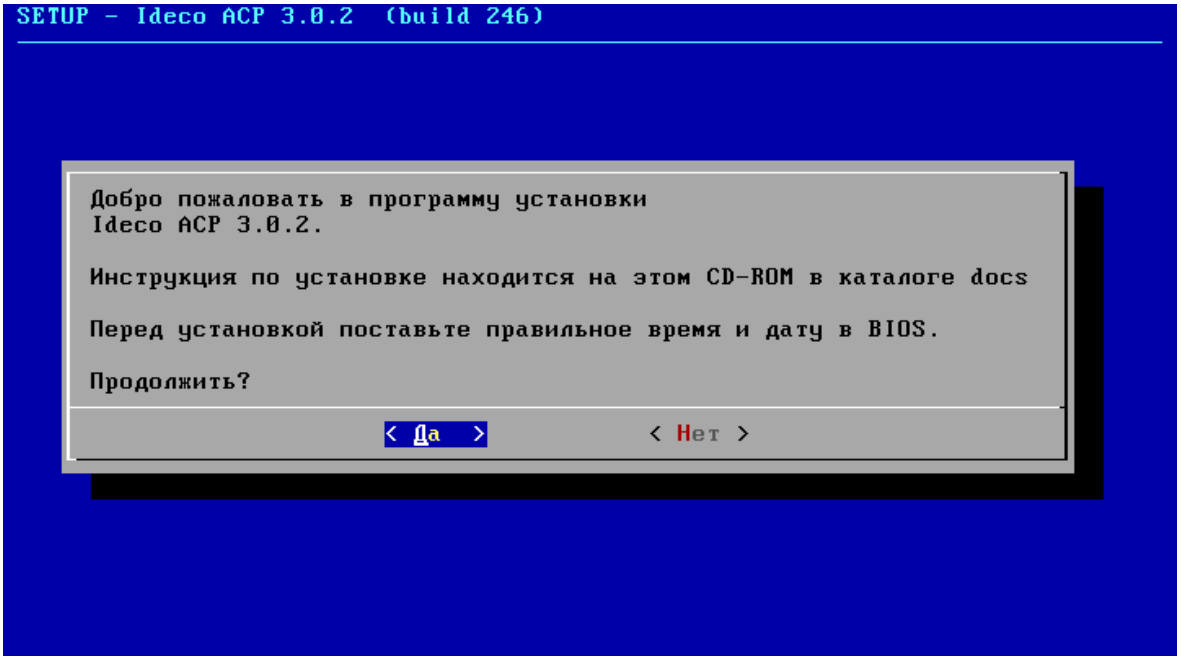


Выбрав режим установки в текстовой консоли загрузчика системы, вы увидите следующие строки на экране. Процесс распаковки ядра и установочной системы

(Uncompressing Linux) может занять достаточно долгое время (1-5 мин.)

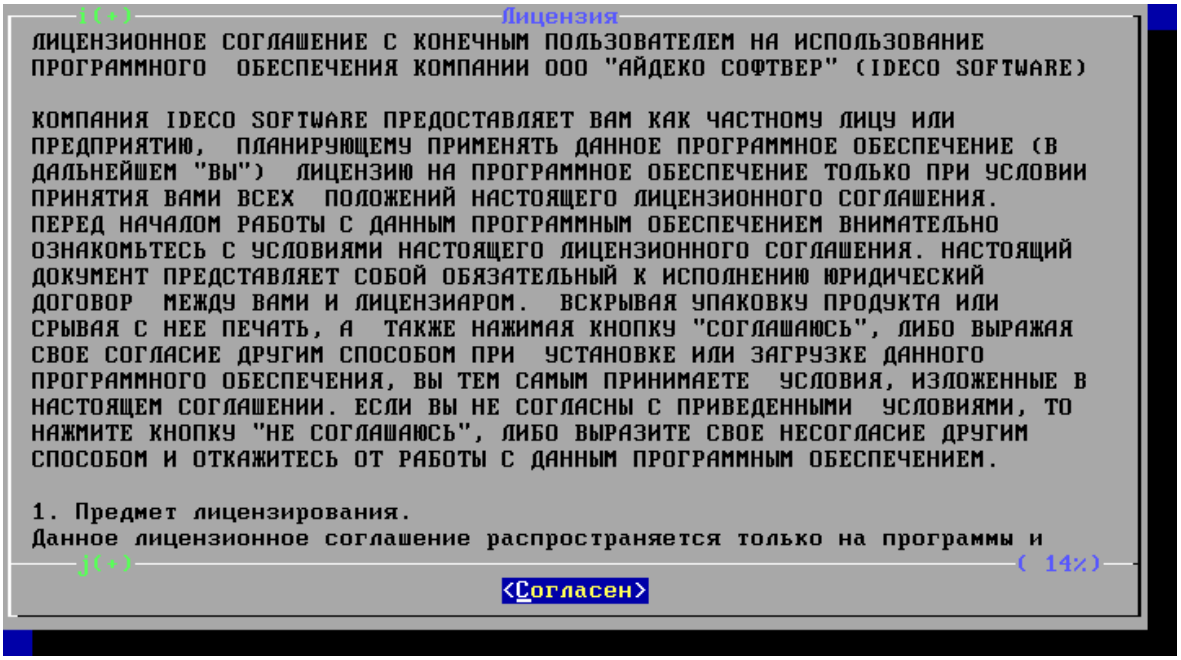


После загрузки системы будет запущен мастер установки с псевдографическим интерфейсом на синем фоне. Если время и прочие настройки в BIOS выставлены верно, то начинаем установку.

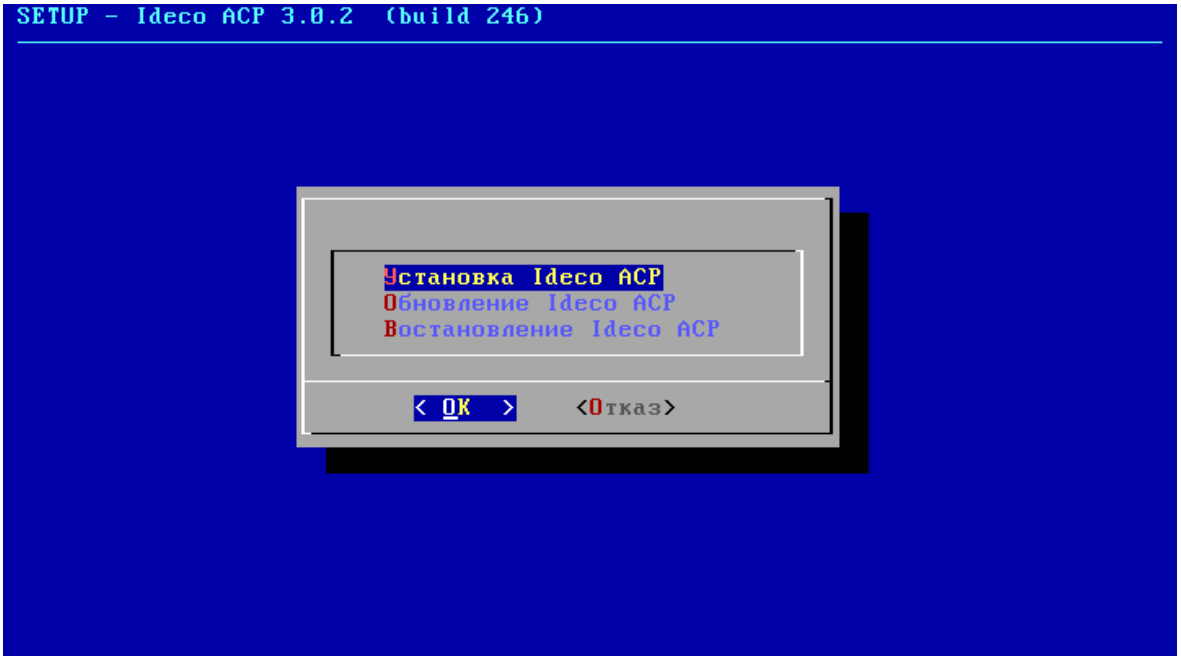


Прежде всего вам будет предложено ознакомиться с лицензионным соглашением

между нашей компанией и вами как конечным потребителем.

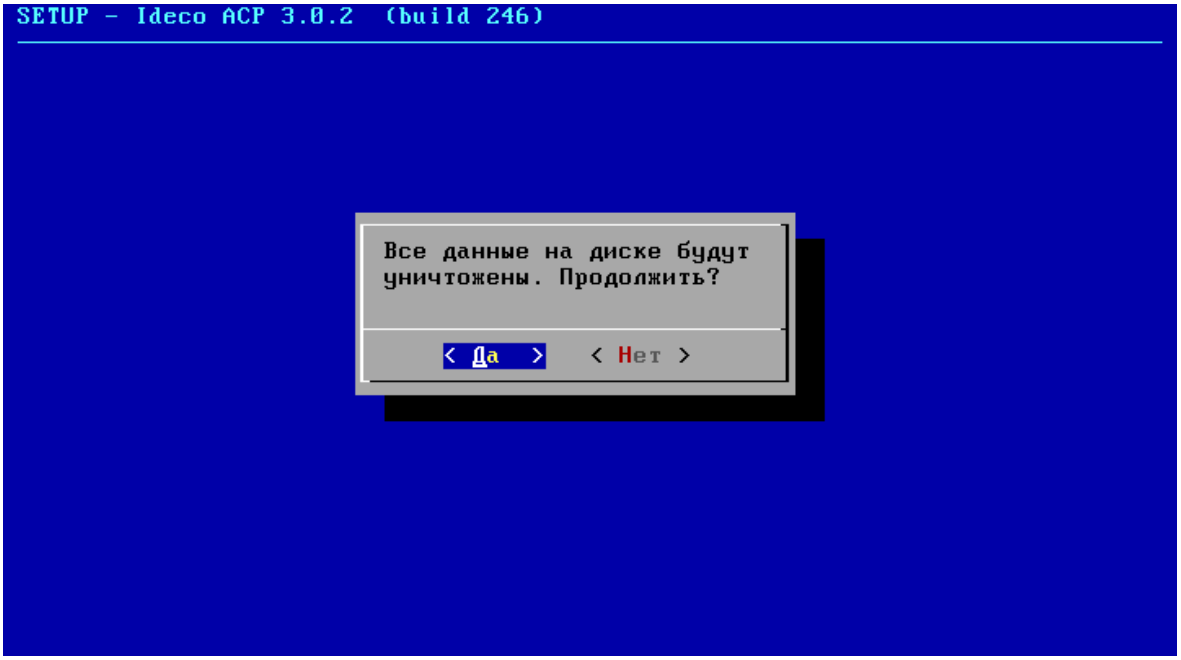


После ознакомления с лицензионным соглашением выберите "Установка Ideco ACP" для дальнейшей установки системы на жесткий диск с нуля. Так же в будущем вы сможете воспользоваться режимами Обновления и Восстановления системы.

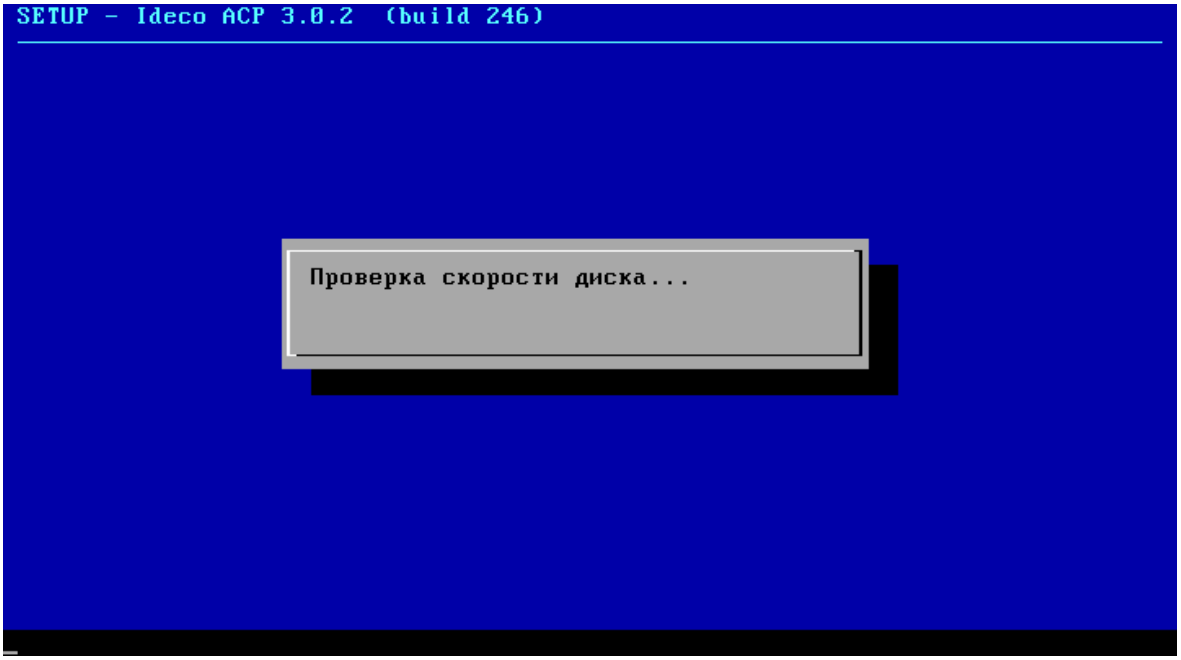


Выбрав установку с нуля ваши жесткие диски будут отформатированы, на них

будут созданы новые логические разделы и скопированы файлы системы, о чем вы будете предупреждены:

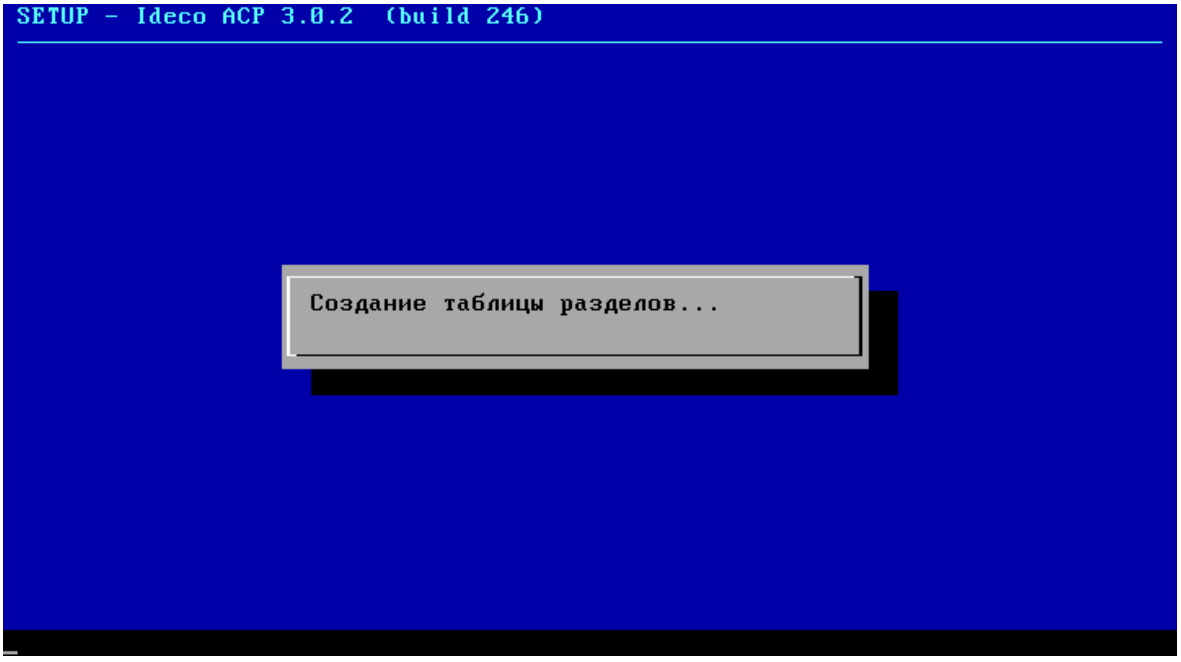


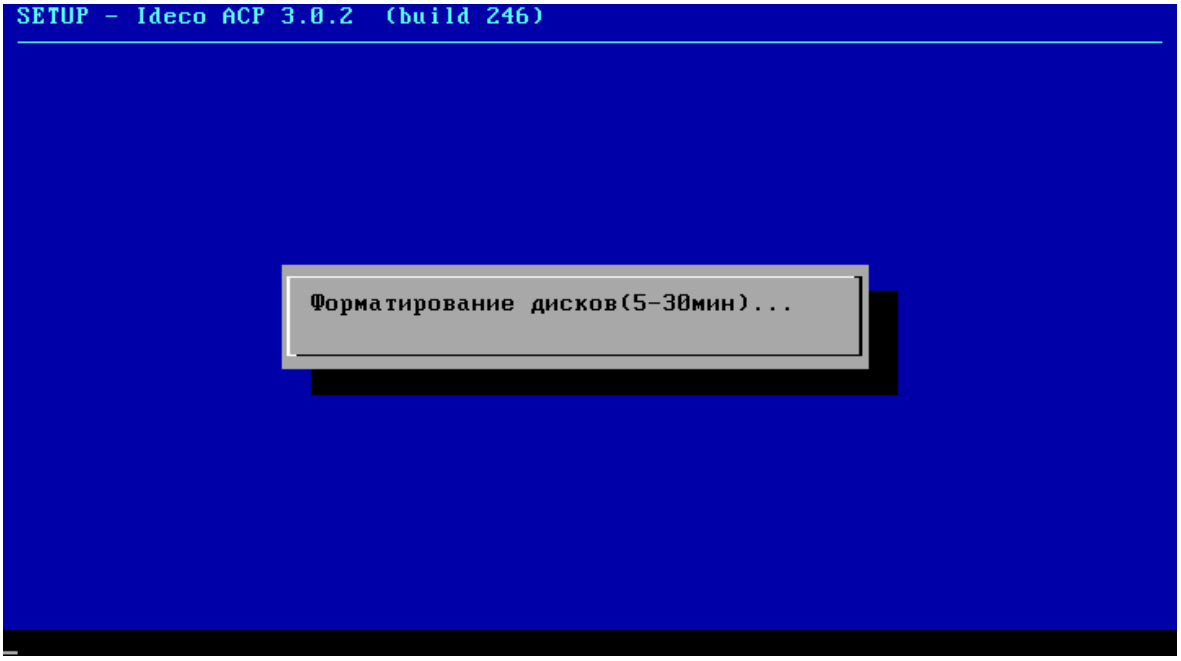
Будут произведены необходимые тесты дисковых накопителей:



Логические разделы при установке системы создаются автоматически. Все свободное место, незанятое файлами системы будет выделено в отдельный раздел

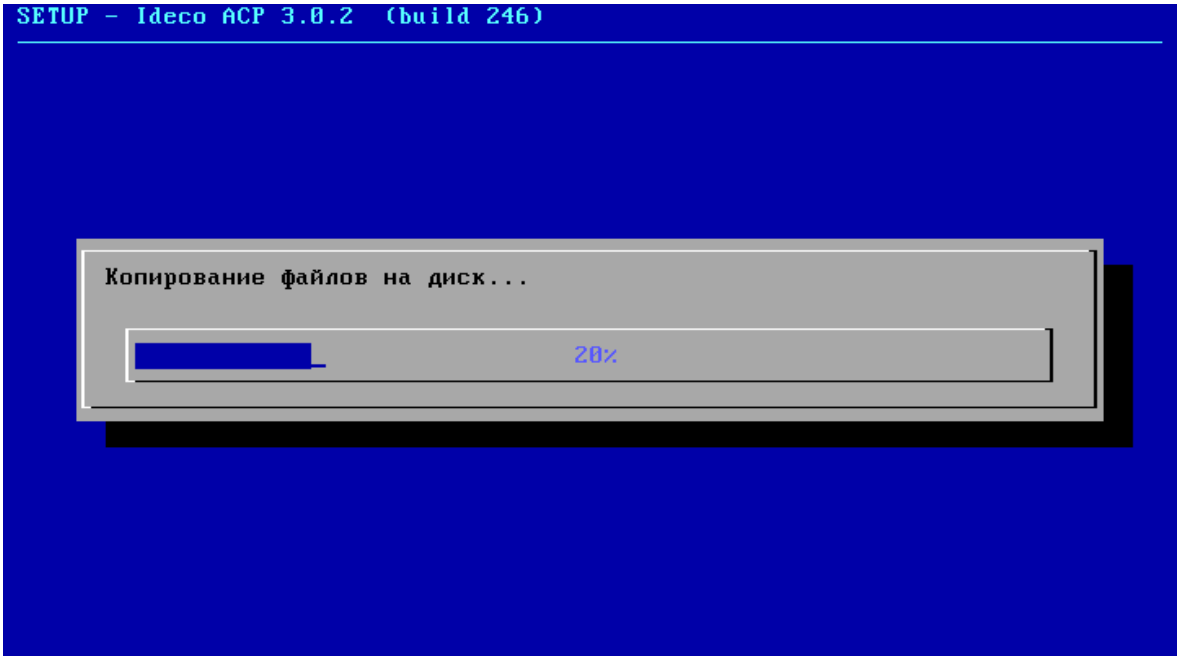
и может понадобится в будущем для подключения дополнительных компонентов системы.

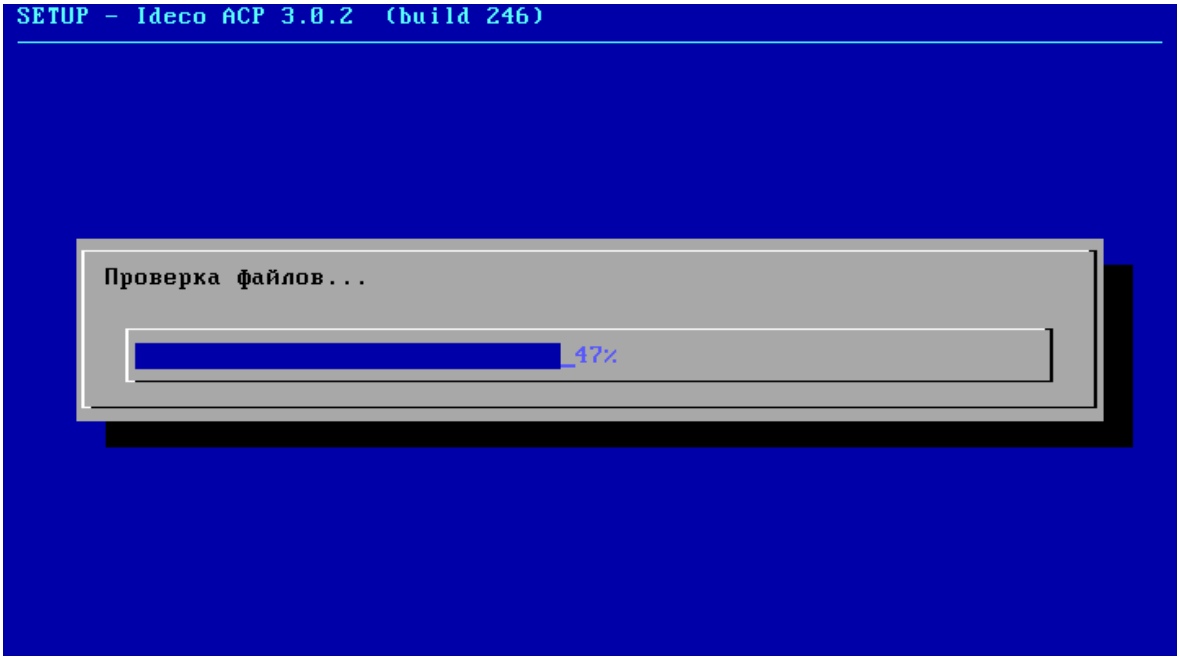




После создания файловой системы начнется копирование системных файлов на диск. Процесс обычно занимает менее 15 минут. Все происходит автоматически, ваше участие в процессе установки системы не требуется. После копирования файлов мастер установки применит конфигурацию вашего компьютера к

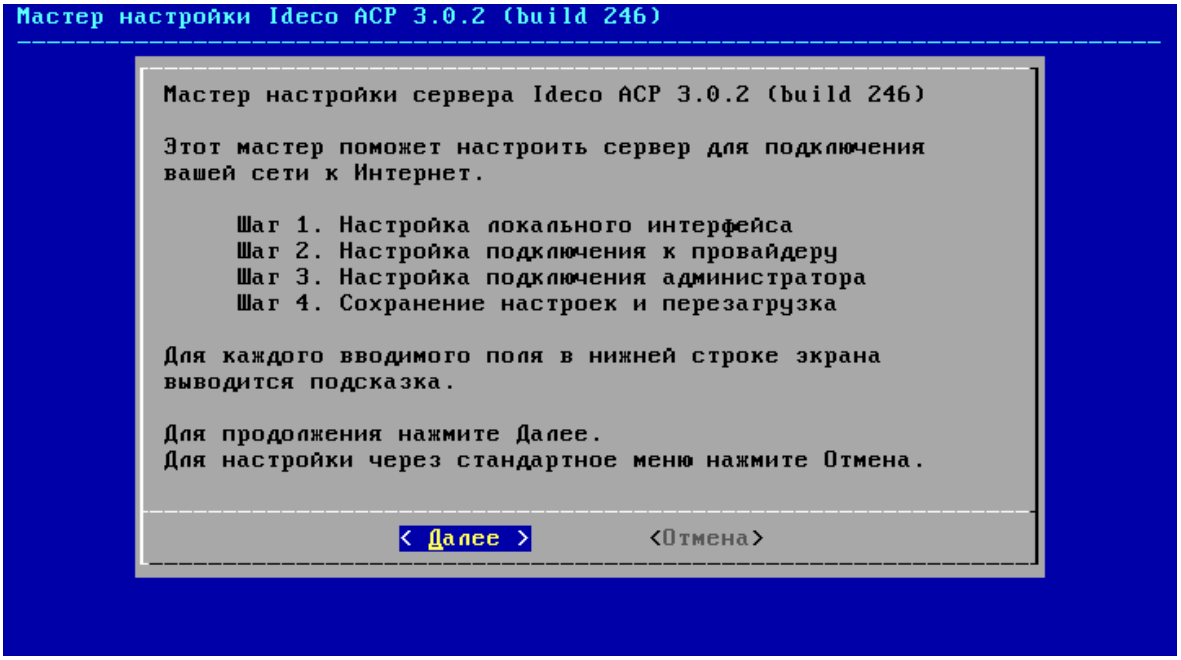
установленной системе.



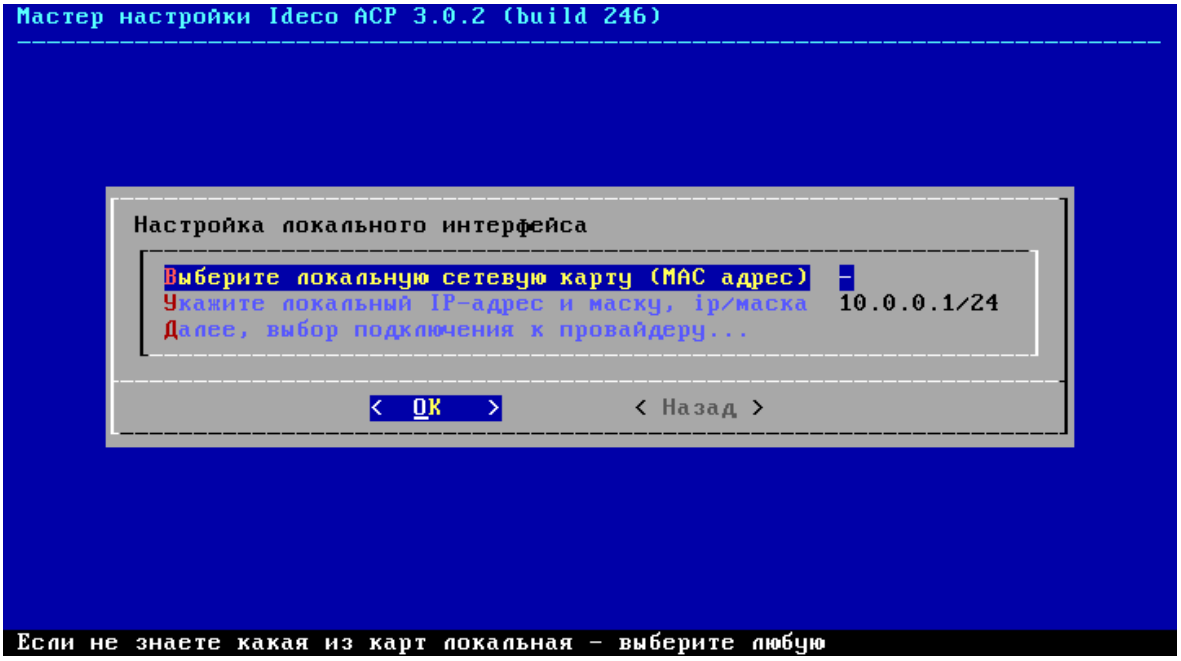


Если все прошло успешно, то будет запущен "мастер настройки сервера", который поможет вам провести первоначальную настройку сервера, а именно: Настроить сетевые интерфейсы на шлюзе, выбрать способ подключения главного администратора к серверу и первичное наполнение вашей будущей базы пользователей из тех устройств в сети, которые будут найдены в сегменте

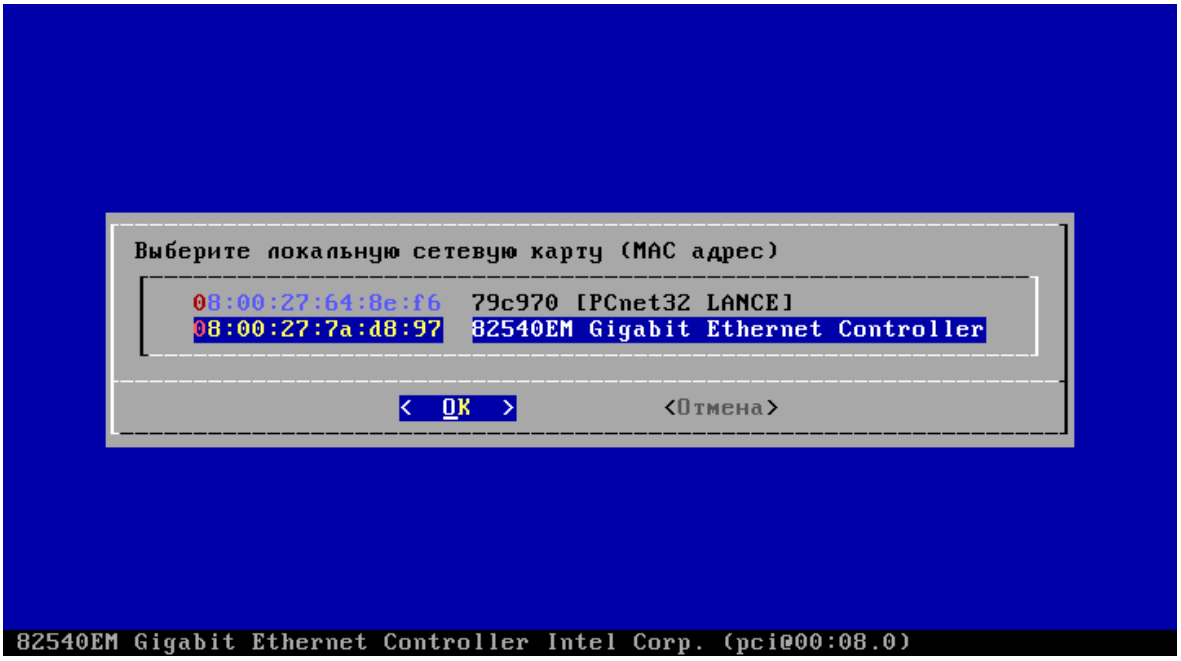
локального интерфейса сервера на момент работы "мастера". Процесс первоначальной настройки можно пропустить и настроить сервер позже, нажав "Отмена".



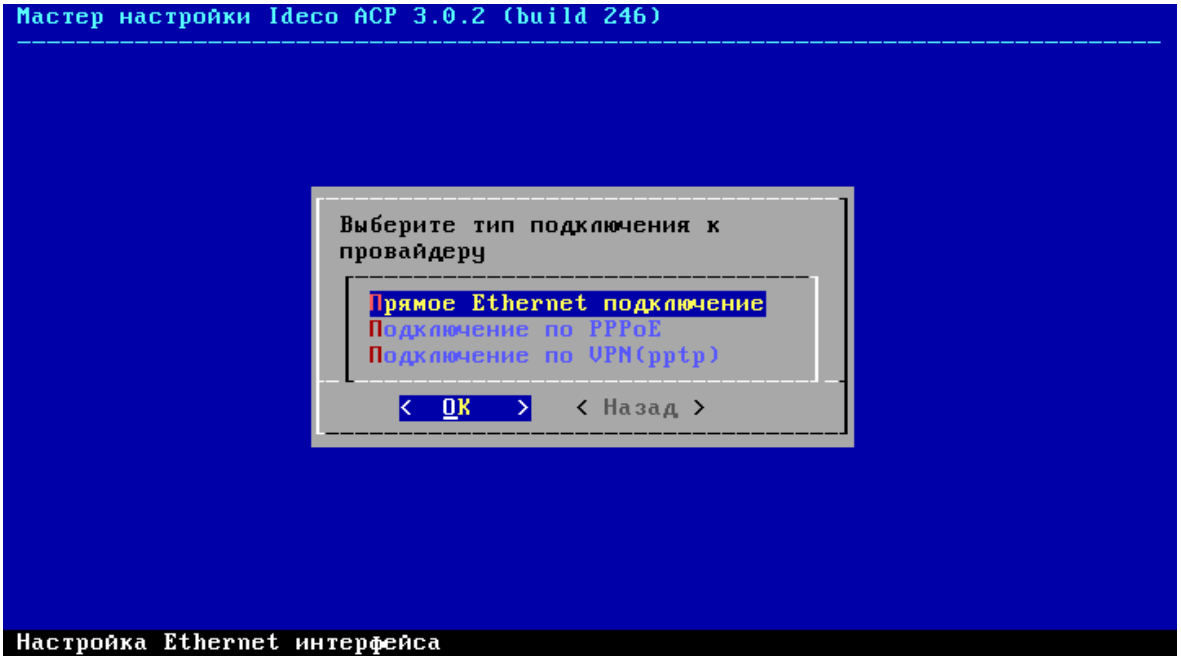
Первичная настройка интерфейсов сервера включает в себя определение к какому физическому интерфейсу (сетевой карте) на сервере будет привязан интерфейс и назначение сети сегмента с указание маски сети и начального адреса сети. На основе этого шага в дальнейшем будет произведен поиск устройств в сети локального интерфейса, поэтому заранее определитесь с адрессацией сети в локальном сегменте ethernet на вашем предприятии и к моменту работы мастера укажите нужную сеть. В дальнейшем настройки на интерфейсах можно будет изменить.



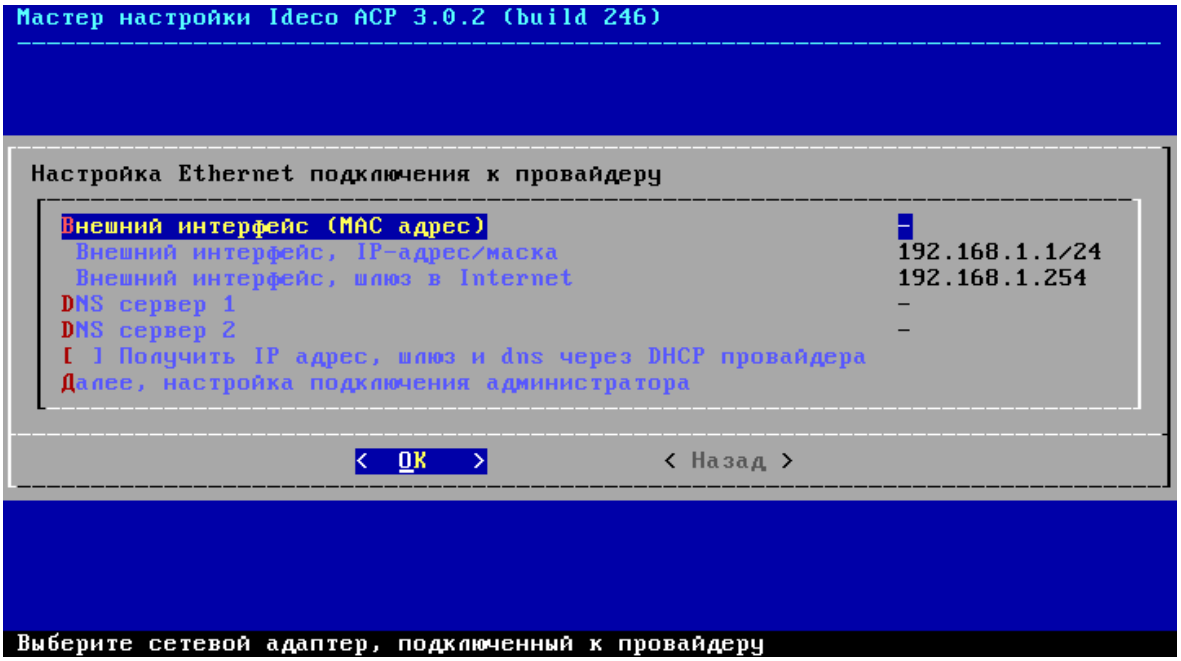
Напротив mac-адресов написаны чипсеты сетевых карт для удобства выбора устройства.



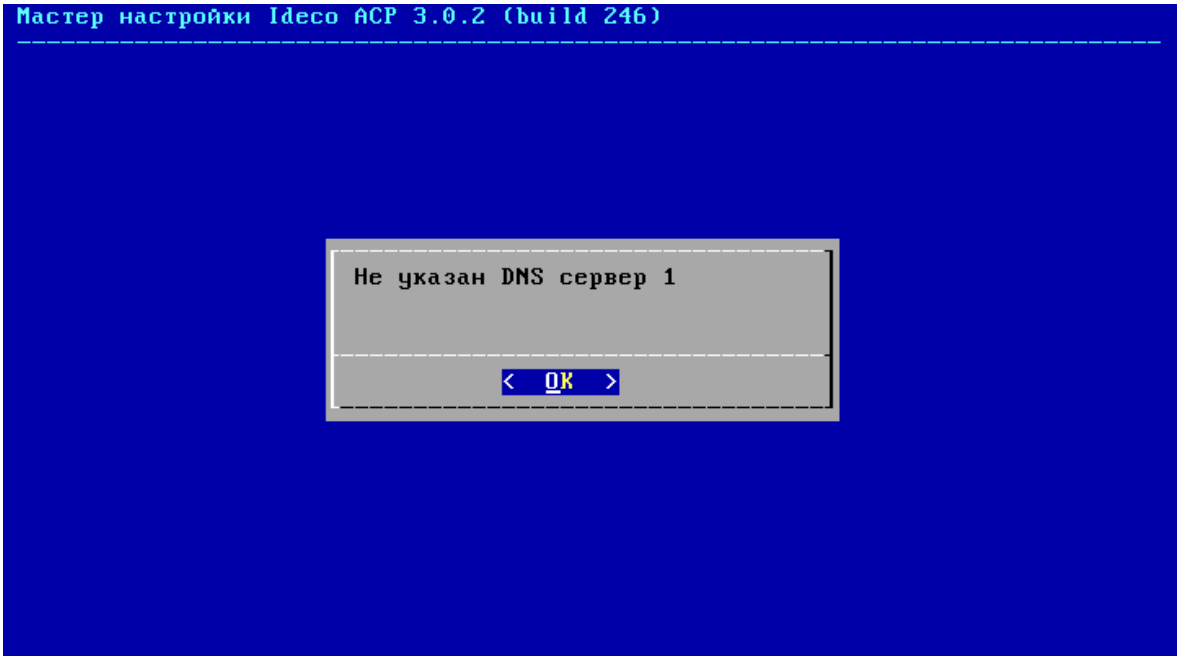
После настройки локального интерфейса будет произведена настройка подключения к провайдеру. Для начала надо выбрать тип подключения (протокол или тип передающей среды можно уточнить у провайдера).



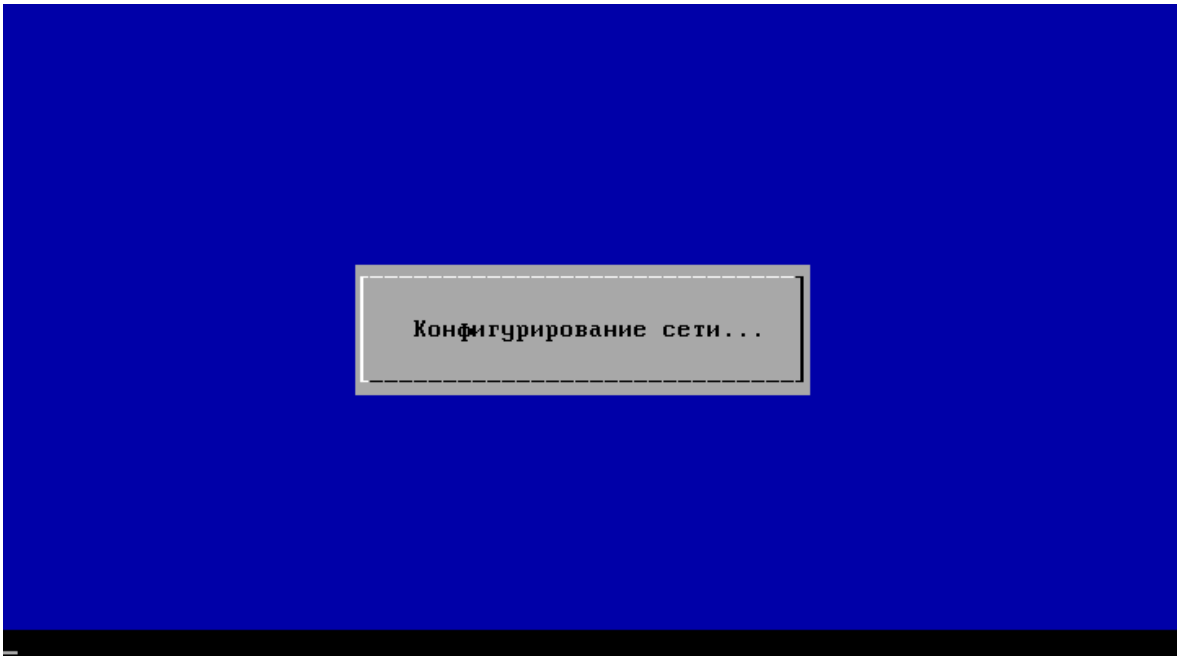
Далее необходимо настроить подключение к интернет по учетным данным, полученным от провайдера. В данном примере рассматривается тип интерфейса ethernet.



Нужно заполнить все поля формы, иначе настройка сети не будет завершена и вы увидите подобное сообщение от "мастера":



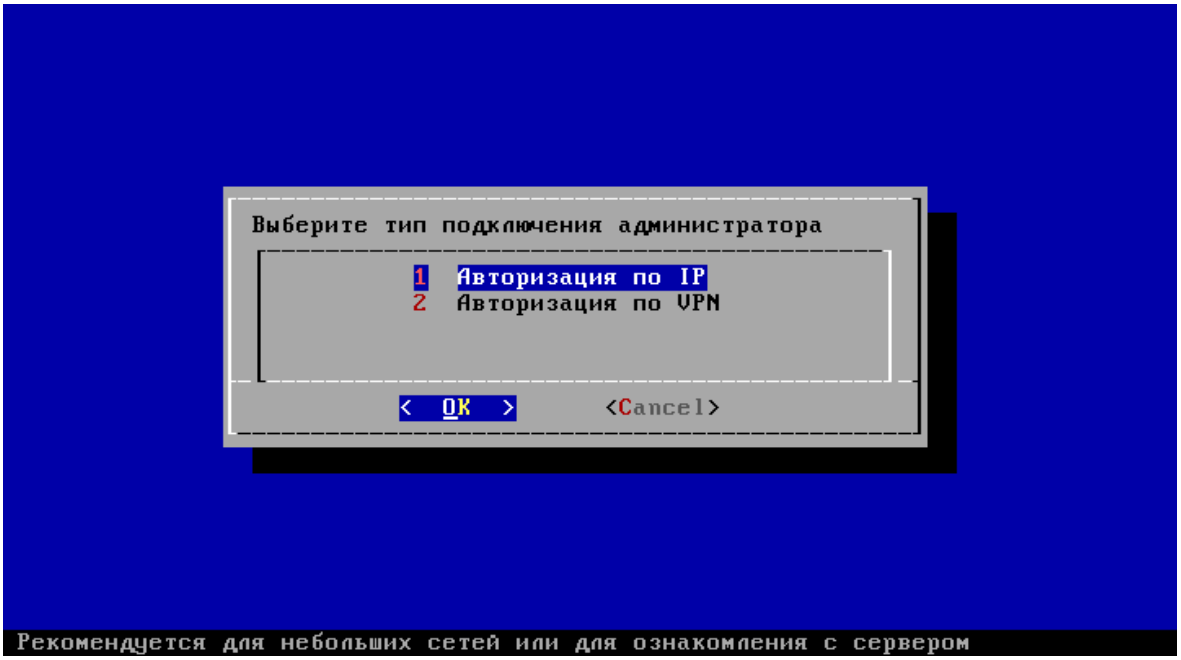
После принятия настроек будут сконфигурированы интерфейсы и сервер станет доступен в сети под указанным выше ip-адресом.

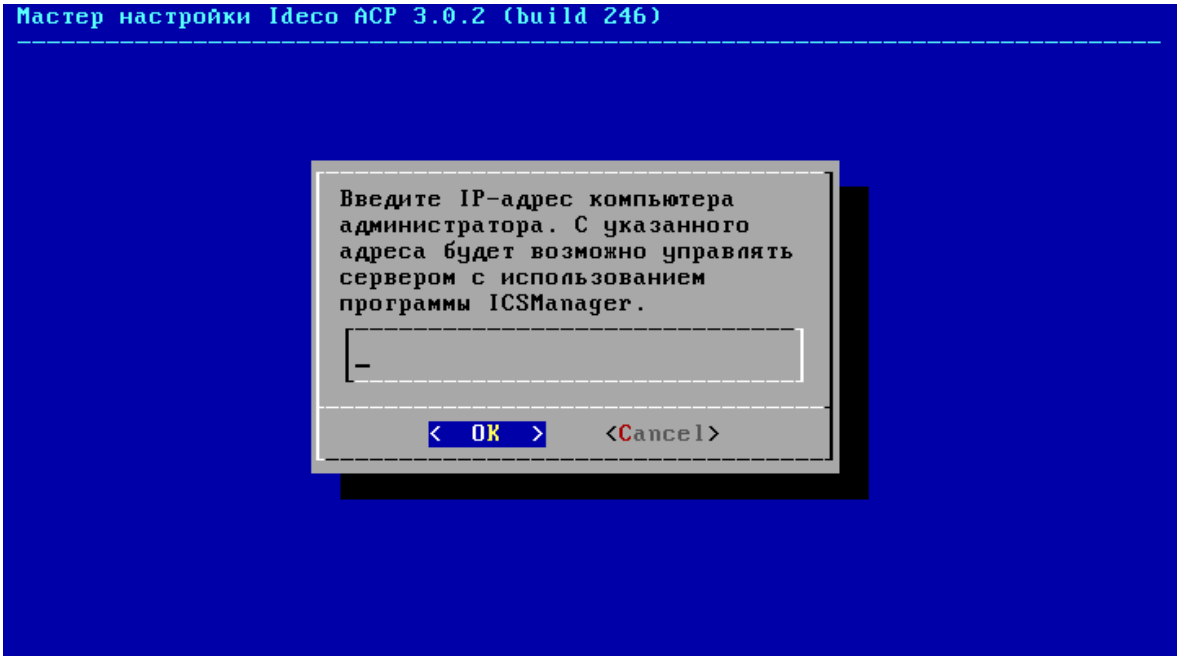


После настройки сети сервер уже готов к работе, но для управления сервером вам нужно подключиться к административному интерфейсу Ideco ACP из-под учетной записи Главного Администратора. Настроим ее сразу. Настраивается только необходимое: тип авторизации и ip-адрес машины в локальной сети с которой

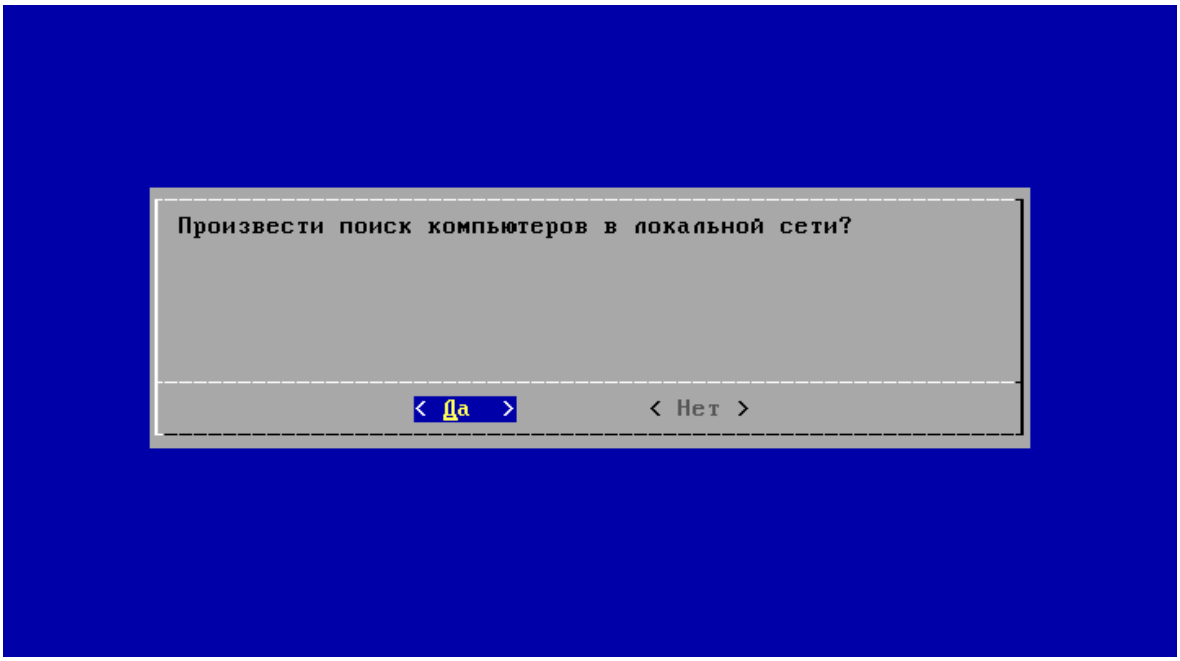
будет осуществляться вход в административный интерфейс с помощью ACP Manager'a. Более тонкую настройку можно будет провести потом.

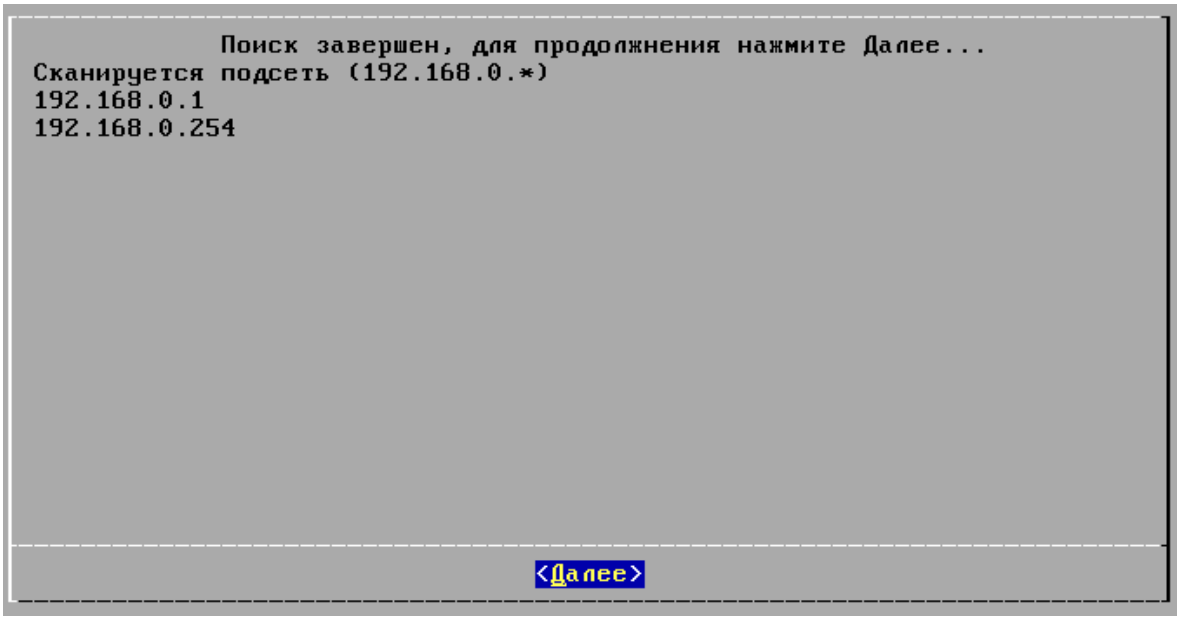
- Если вы выберите тип авторизации по VPN (PPTP или PPPOE), то на машине администртора нужно будет настроить VPN подключение по желаемому вам протоколу с логином Administrator и паролем servicemode на адрес сервера Ideco ACP в локальной сети.
- Если вы не укажите ip-адрес компьютера администратора, то подключение будет возможно с любого компьютера в локальной сети.



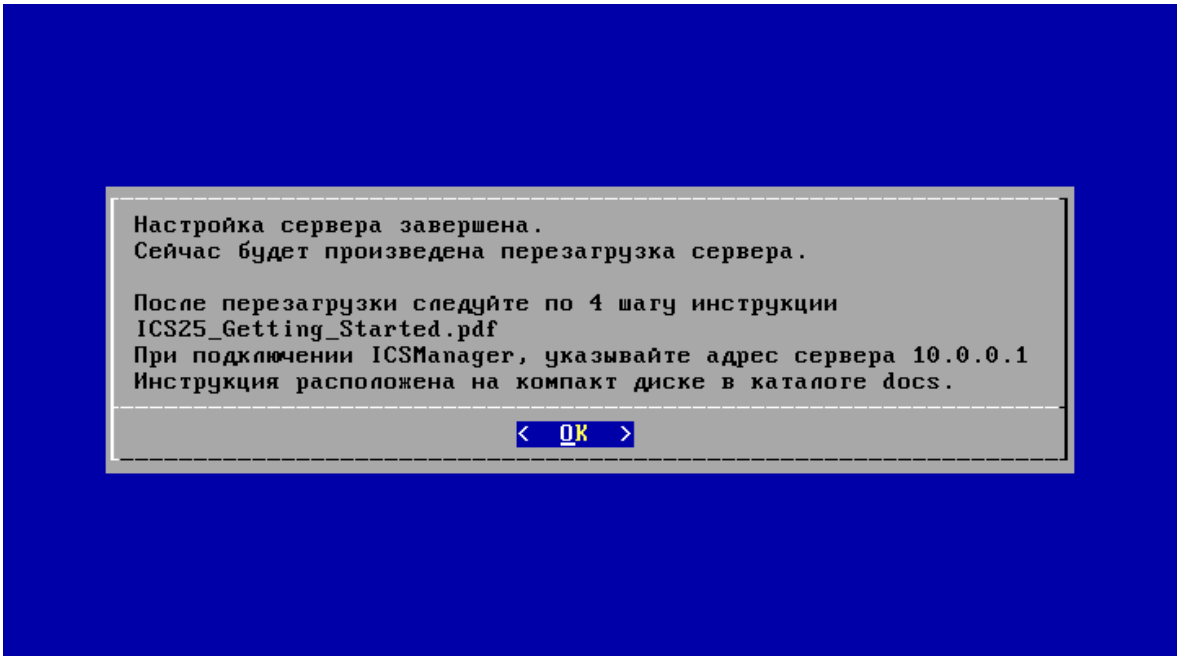


В завершение работы мастера будет произведен поиск устройств в ethernet сегменте локальной сети. Найденные устройства будут добавлены как клиенты в базу данных пользователей, что может облегчить начальный этап заведения пользователей в базу данных при большом количестве пользователей в локальной сети. Этот шаг можно пропустить.





По окончании работы мастера и первоначальной настройки сервера Ideco ACP вам будет предложено перезагрузить сервер.



2.4 Настройка сервера под нужды провайдера

После первичной настройки нужно в первую очередь подключиться к серверу при помощи ACP Manager для наполнения базы данных. Для этого необходимо:

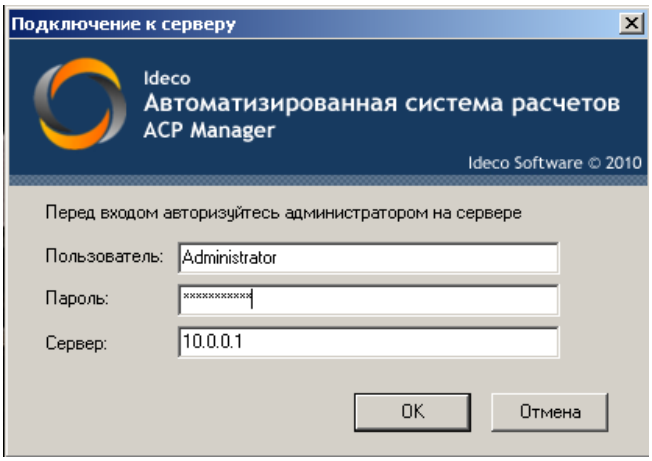
1. Установить ACP Ideco Manager на компьютер администратора. Скачать его можно с установочного диска по ссылке ACP Ideco Manager. Для установки запускаете файл setup.exe и следуете указаниям мастера установки.

2. Авторизоваться на Ideco под логином главного администратора (если была выбрана авторизация по IP, то достаточно прописать на своём компьютере IP адрес администратора, который был указан при установке).

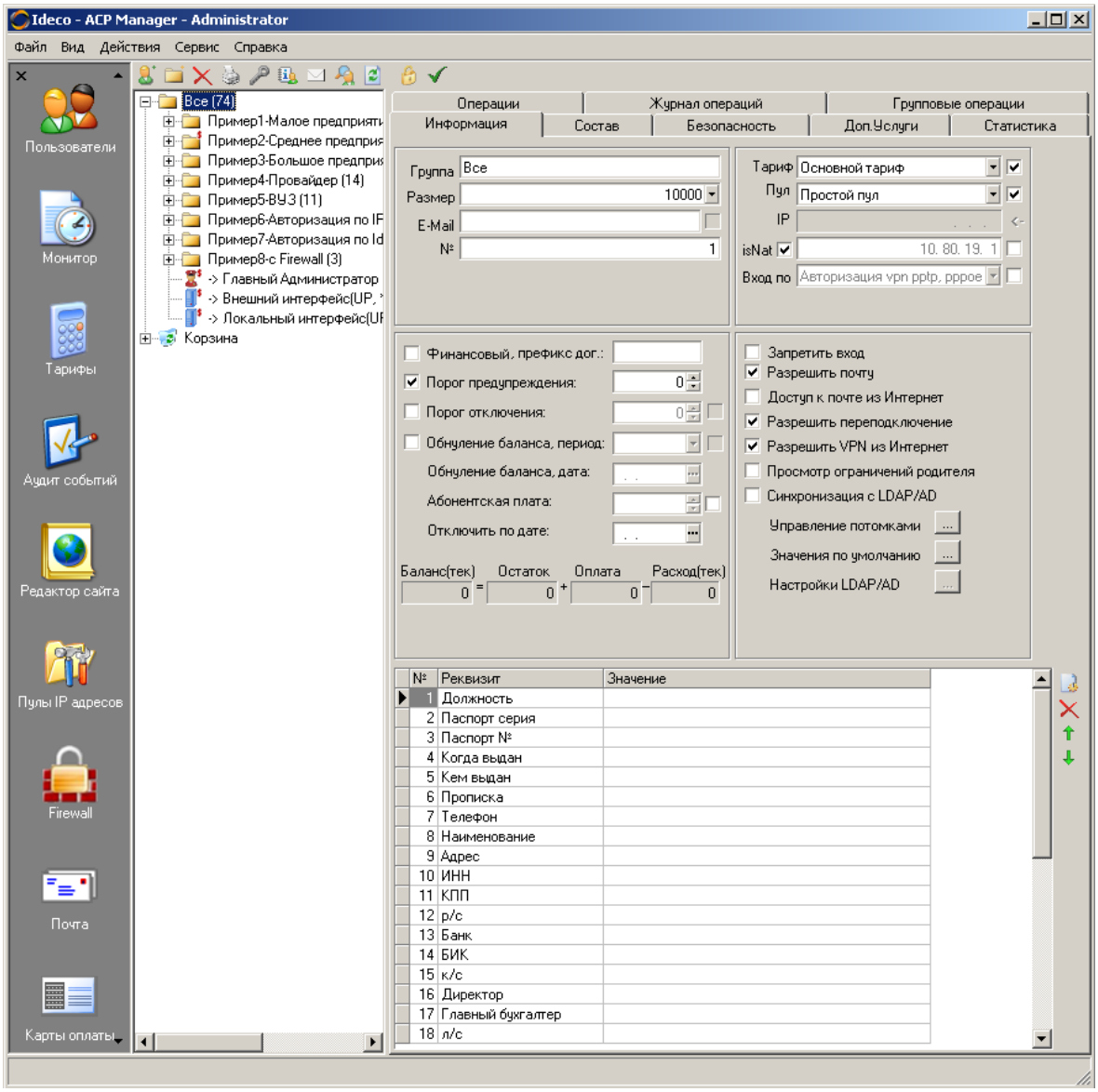
3. Запустить ACP Manager, в качестве сервера указать локальный адрес Ideco (по умолчанию 10.0.0.1) и ввести логин и пароль главного администратора:

Логин: **Administrator**

Пароль: **servicemode**



После того как вы выполните вход вам будет доступен полный контроль над сервером и базой данных пользователей.



Подробнее об управлении можно почитать в главе под названием ACP Manager[178].

Примечание: В целях повышения безопасности обязательно смените пароль главного администратора.

Изначально для корректной настройки сервера необходимо:

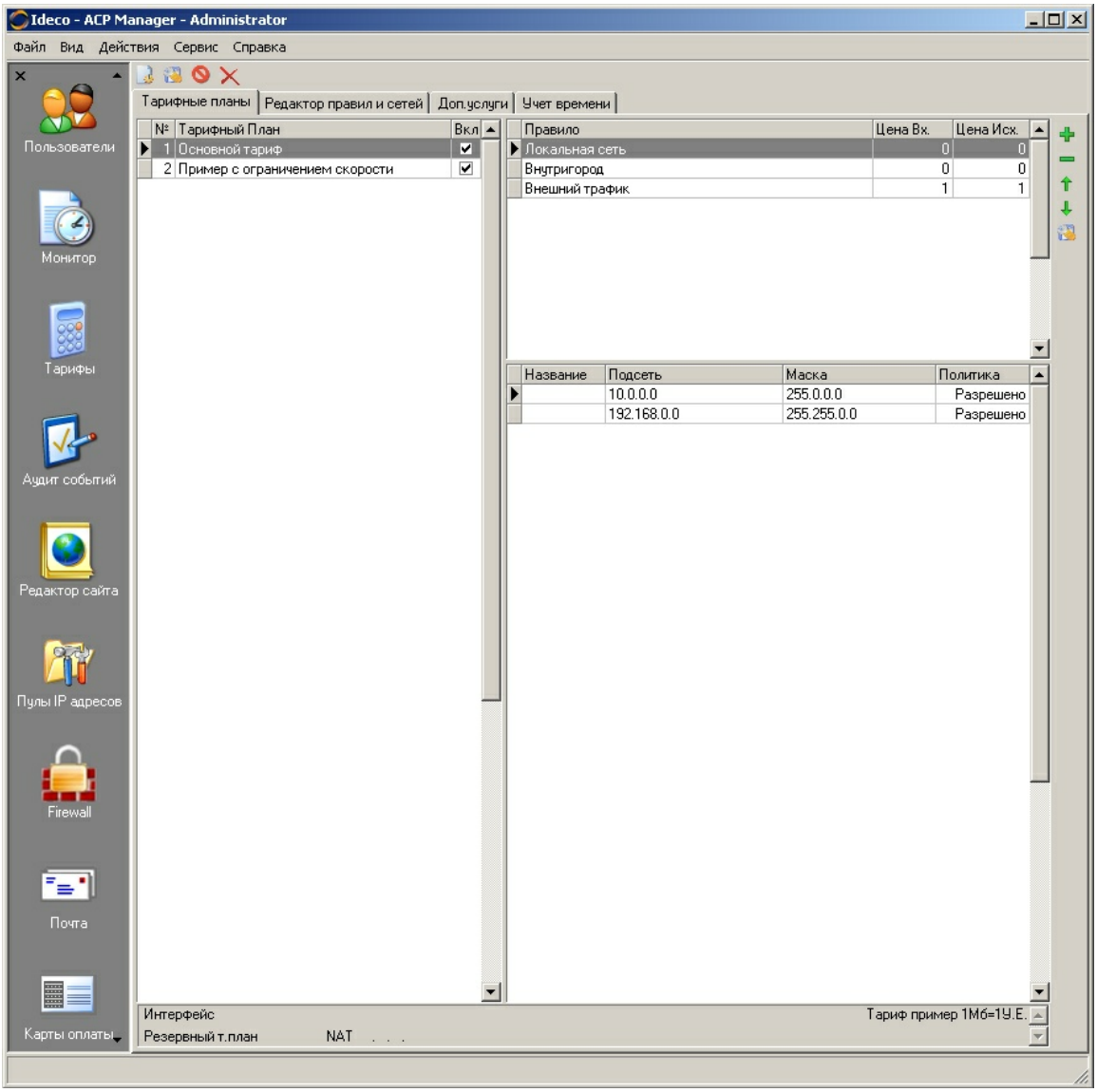
- Настроить тарифные планы[30]
- Наполнить абонентскую базу[36]

2.4.1 Настройка тарифных планов

В соответствии с тарифными планами происходит учет трафика пользователей в денежном эквиваленте.

Тарифный план определяет стоимость трафика в зависимости от подсети, а также от направления трафика (входящий или исходящий). В Ideco ACP тарифный план состоит из списка правил с указанием стоимости входящего и исходящего трафика для этого правила. Понятие **Правило** введено для удобства управления, **Правило** – это список сетей с указанием политики (разрешено или запрещено). Одно и тоже правило может входить в несколько тарифных планов. В одно правило, обычно, объединяются сети, стоимость трафика по которым одинакова. Например, правило "Внутригород" должно содержать список сетей с одной стоимостью, а правило "Локальная сеть" – список сетей предприятия, по которым не должна вестись тарификация (нулевая стоимость).

Для доступа к тарифным планам перейдите в раздел **Тарифные планы**: кнопка **Тарифы** на панели разделов.

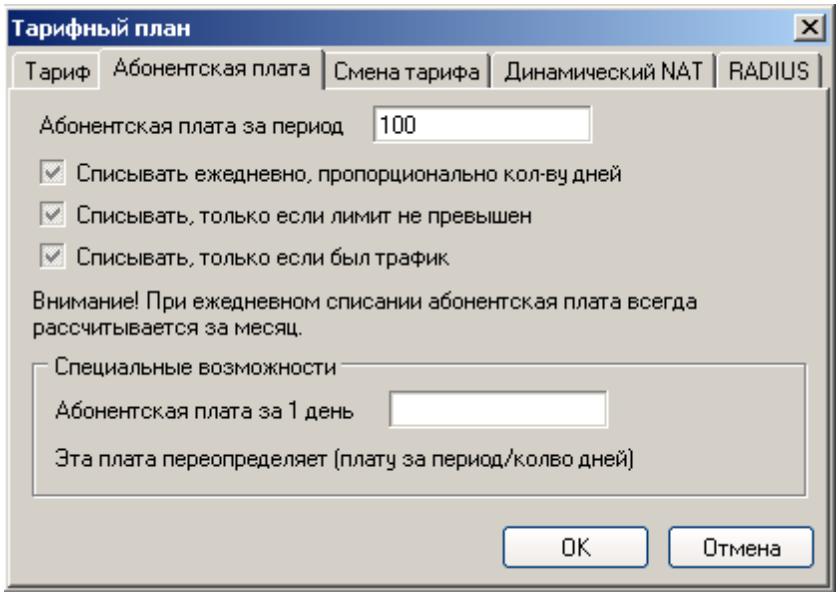


Подробно создание и редактирование тарифных планов описано главе "Тарифные планы 220"

В данной главе рассмотрим несколько тарифных планов, часто используемых современными провайдерами:

Задача: Создать тариф, в котором абонентская плата в месяц 100 рублей - в неё включено 30 мегабайт. Свыше 30 мегабайт днём 2,90 руб/мб, а ночью (с 2:00 до 7:59) цена 2,50 руб/Мб. До сайта www.sibnet.ru трафик льготный и стоит 30 копеек/Мб.

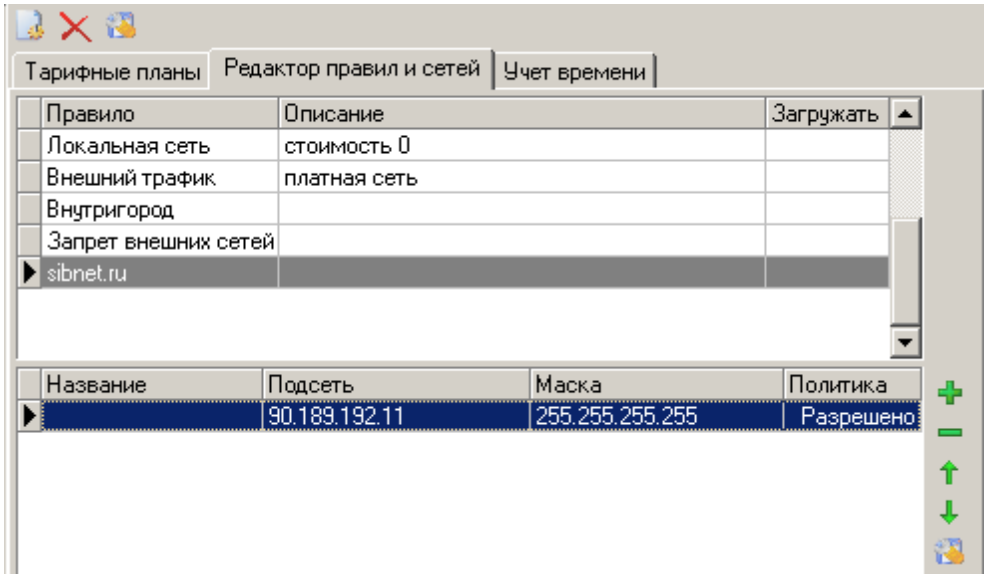
1. Создайте тариф, укажите величину абонентской платы.



2. В тарифе сделайте правила для бесплатных сетей, например локальной.

3. Выясните какой IP адрес у сайта www.sibnet.ru.

4. В редакторе правил и сетей создайте правило с именем sibnet.ru и укажите IP адрес этого сайта с маской 255.255.255.255



5. В тарифе создайте правило для только что созданного sibnet.ru и укажите цену 0,30

6. Создайте правило для платных (внешних) сетей с условиями:

"Скачано, более чем, Мб" = 0, "Но менее чем, МБ" = 30

"Стоимость" = 0.

7. Создайте правило для платных (внешних) сетей с условиями:

"Скачано, более чем, Мб" = 30

"Время действия от " = 02:00:00

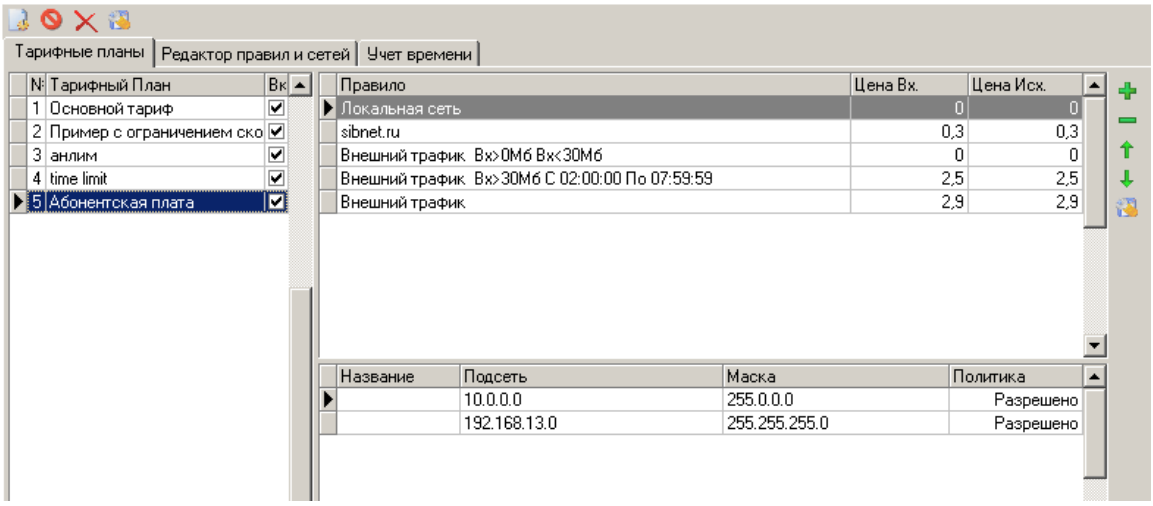
"Время действия до" = 07:59:59.

"Стоимость" = 2,50.

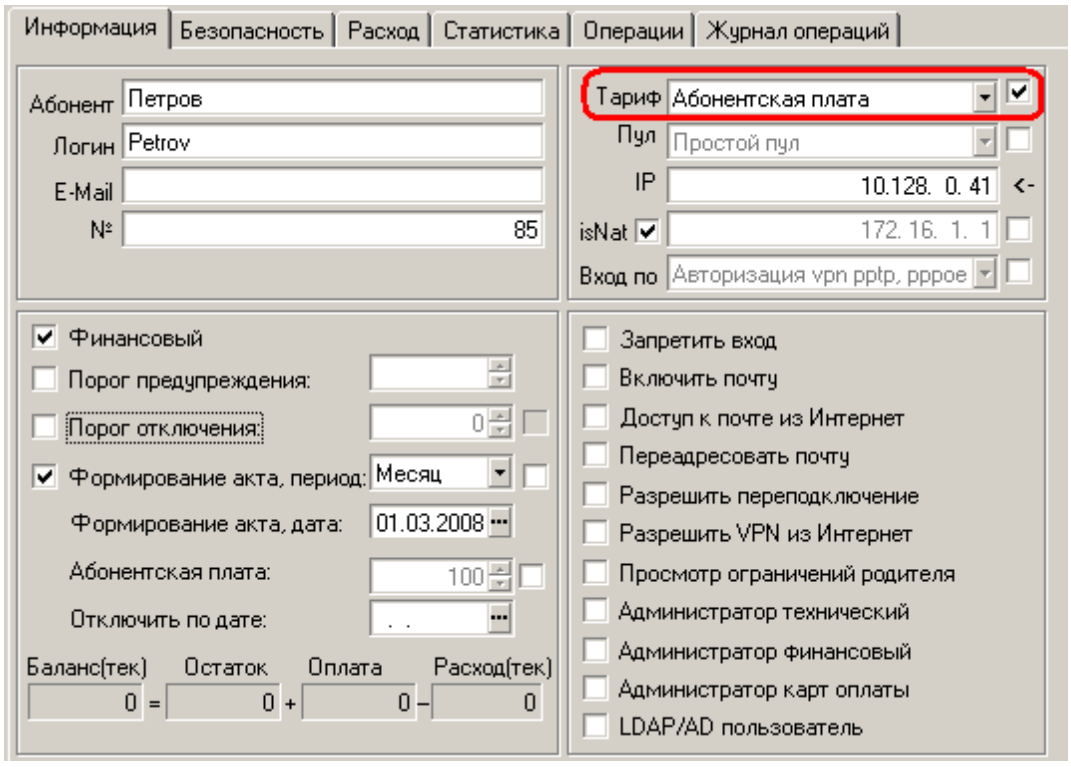
8. Создайте правило для платных (внешних) сетей с условием:

"Стоимость" = 2,90.

Это правило должно быть последним.



9. В настройках пользователя присвойте только что созданный тариф.



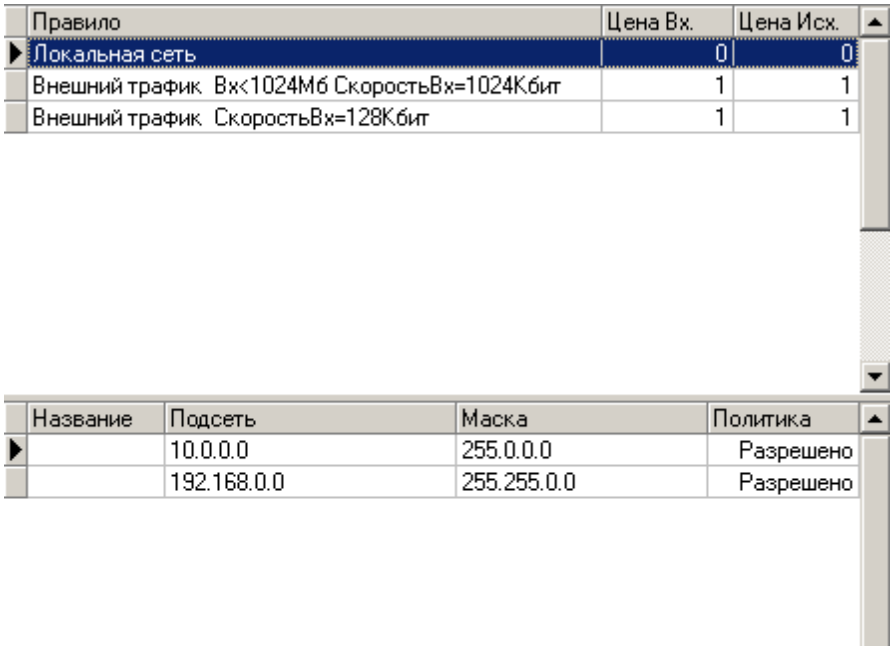
Задача: Создать тариф, в котором пользователям предоставляется 1Гб трафика на скорости 1Мбит/с, а при скачивании больше 1Гб скорость 128кбит/с.

1. Создайте тариф.

2. Добавьте правило(а) для локальной сети.

3. Добавьте правило с условиями "скачано не менее чем, Мб = 1024" и "Скорость Вх, Кбит = 1000", и стоимость указать нужную (см. рисунок)

4. Добавьте правило с условием "Скорость Вх, Кбит = 128" и стоимость указать нужную (см. рисунок)



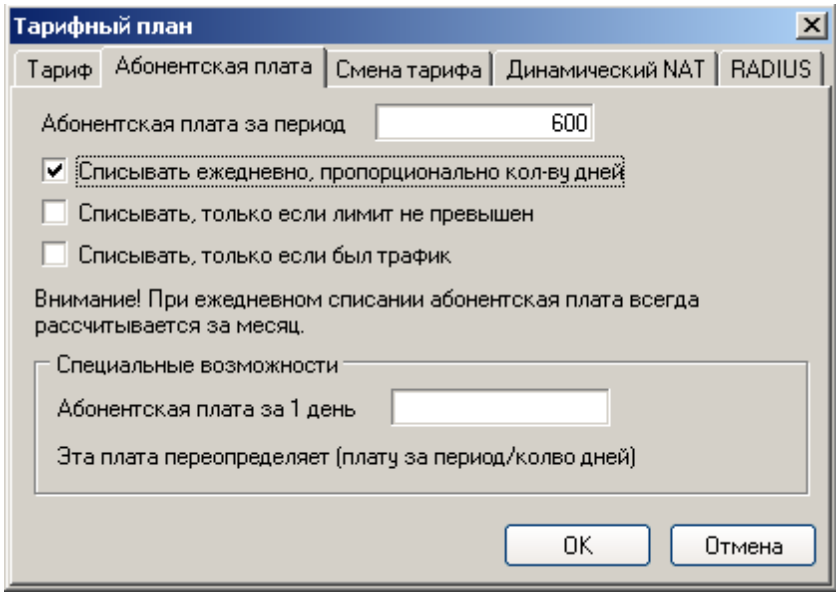
Правило	Цена Вх.	Цена Исх.
Локальная сеть	0	0
Внешний трафик Вх<1024Мб СкоростьВх=1024Кбит	1	1
Внешний трафик СкоростьВх=128Кбит	1	1

Название	Подсеть	Маска	Политика
	10.0.0.0	255.0.0.0	Разрешено
	192.168.0.0	255.255.0.0	Разрешено

5. В настройках пользователя присвойте только что созданный тариф.

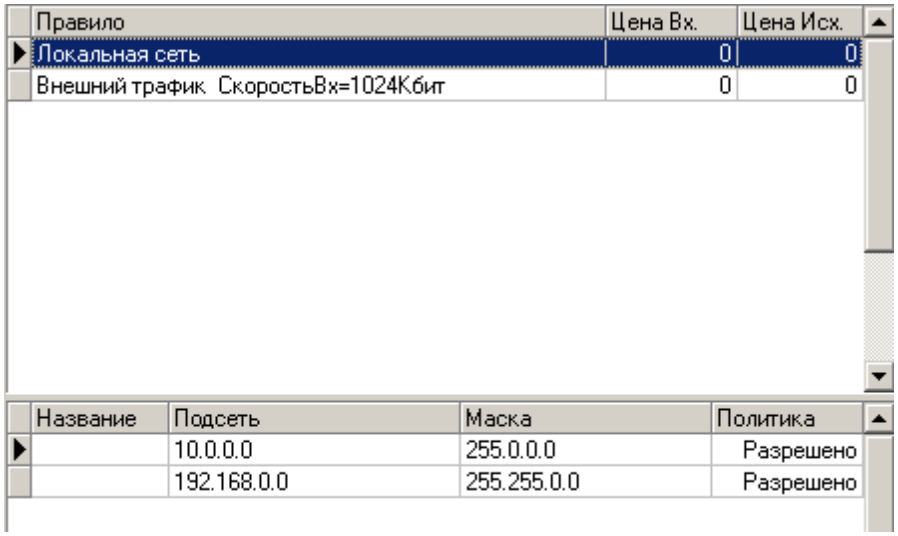
Задача: Создать безлимитный тариф с ограничением скорости в 1024 Кбит/с, на локальные ресурсы скорость не ограничивается, абонентская плата 600 рублей в месяц с ежедневным списанием.

1. Создайте тариф, укажите величину абонентской платы и поставьте галочку "Списывать ежедневно, пропорционально количеству дней".



2. Добавьте правило(а) для локальной сети.

3. Добавьте правило с условием "Скорость Вх, Кбит = 1024"



Правило	Цена Вх.	Цена Исх.
Локальная сеть	0	0
Внешний трафик СкоростьВх=1024Кбит	0	0

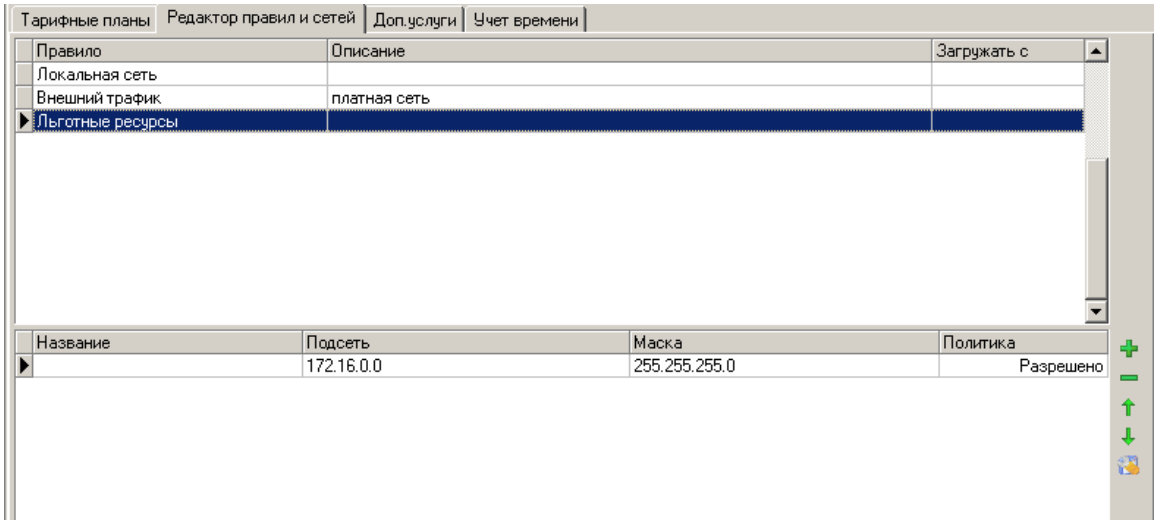
Название	Подсеть	Маска	Политика
	10.0.0.0	255.0.0.0	Разрешено
	192.168.0.0	255.255.0.0	Разрешено

4. В настройках пользователя присвойте только что созданный тариф.

Задача: Создать тариф, в котором внешний трафик тарифицируется по 1 рублю за Мб, локальные сети провайдера тарифицируется по 30 копеек, льготные ресурсы по 50 копеек. Исходящий трафик не тарифицируется.

1. Создайте тариф.

2. В редакторе правил и сетей создайте правила с именами "Локальная сеть" и "Льготные ресурсы" и укажите IP адреса этих сетей.



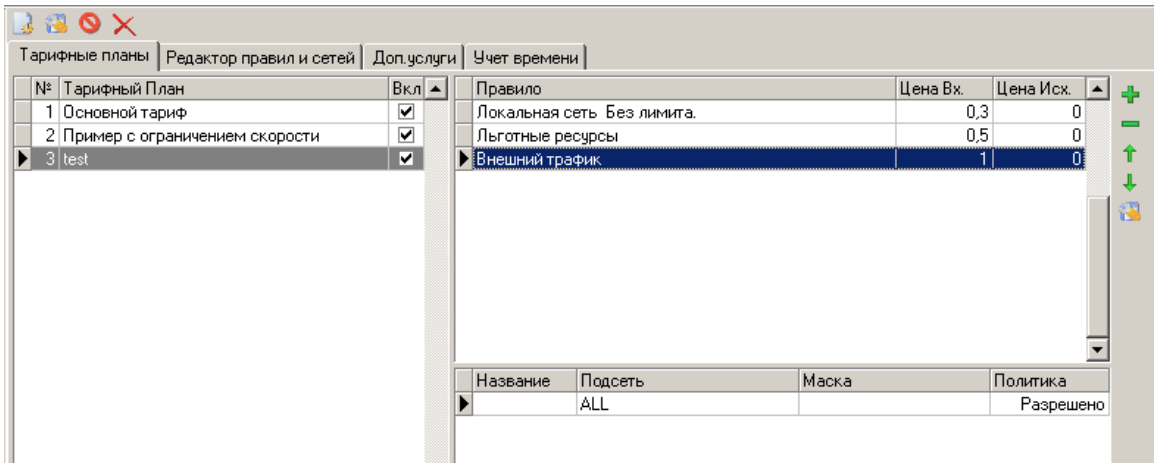
3. В тарифе сделайте правило для локальных сетей провайдера укажите цену 0,30

4. В тарифе создайте правило для льготных ресурсов и укажите цену 0,50

5. Создайте правило для внешних сетей с условием:

"Стоимость" = 1.

Это правило должно быть последним.



6. В настройках пользователя присвойте только что созданный тариф.

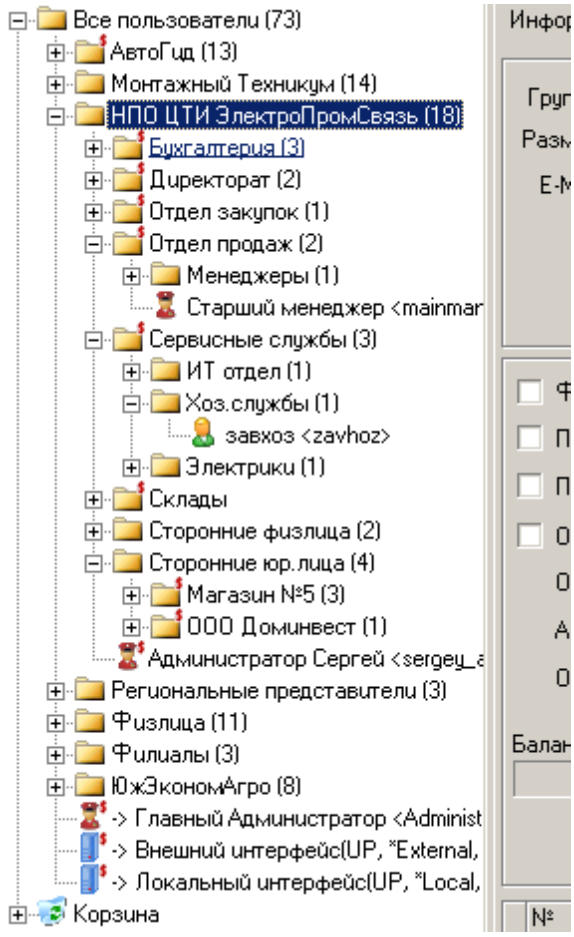
2.4.2 Наполнение абонентской базы

Абоненты в Ideco ACP Manager отображаются в виде дерева состоящего из групп пользователей и самих пользователей. Уровень вложенности групп неограничен.

Древовидная структура позволяет легко отразить реальную структуру сети провайдера. Древовидная структура и принцип наследования позволяет легко задавать и изменять общие параметры для пользователей, определяя их для родительской группы: тарифный план, пул IP-адресов, параметры ограничений и

разрешений, отключать, выполнять групповые операции для всех пользователей группы. При необходимости для отдельных пользователей можно переопределить отличные от общих параметров признаки.

Дерево пользователей выглядит следующим образом:



В дереве отображаются названия групп и пользователей, а у пользователей в скобках также указывается логин.

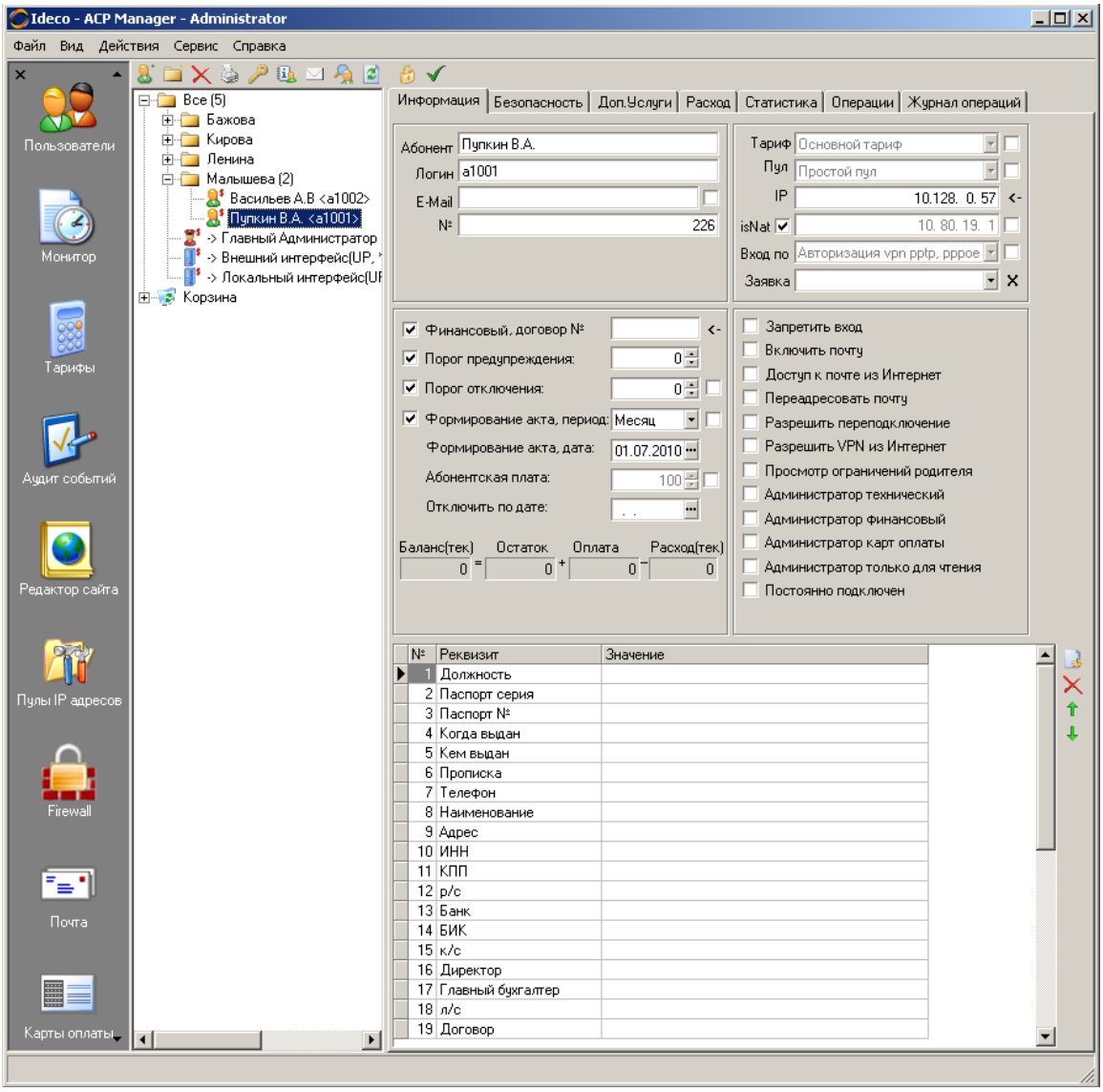
Важно. При наполнении клиентской базы: если вы заводите физических лиц, которые будут самостоятельно оплачивать доступ в интернет им обязательно нужно ставить признак **Финансовый**[205]. При добавлении юридического лица вы можете создать либо конечного пользователя либо группу и установить признак **Финансовый**[205].

Подробно процесс создания групп и пользователей описан в главе "Управление пользователями[184]".

В данной главе рассмотрим способы сортировки пользователей по группам. Ниже приведены 2 основных способа:

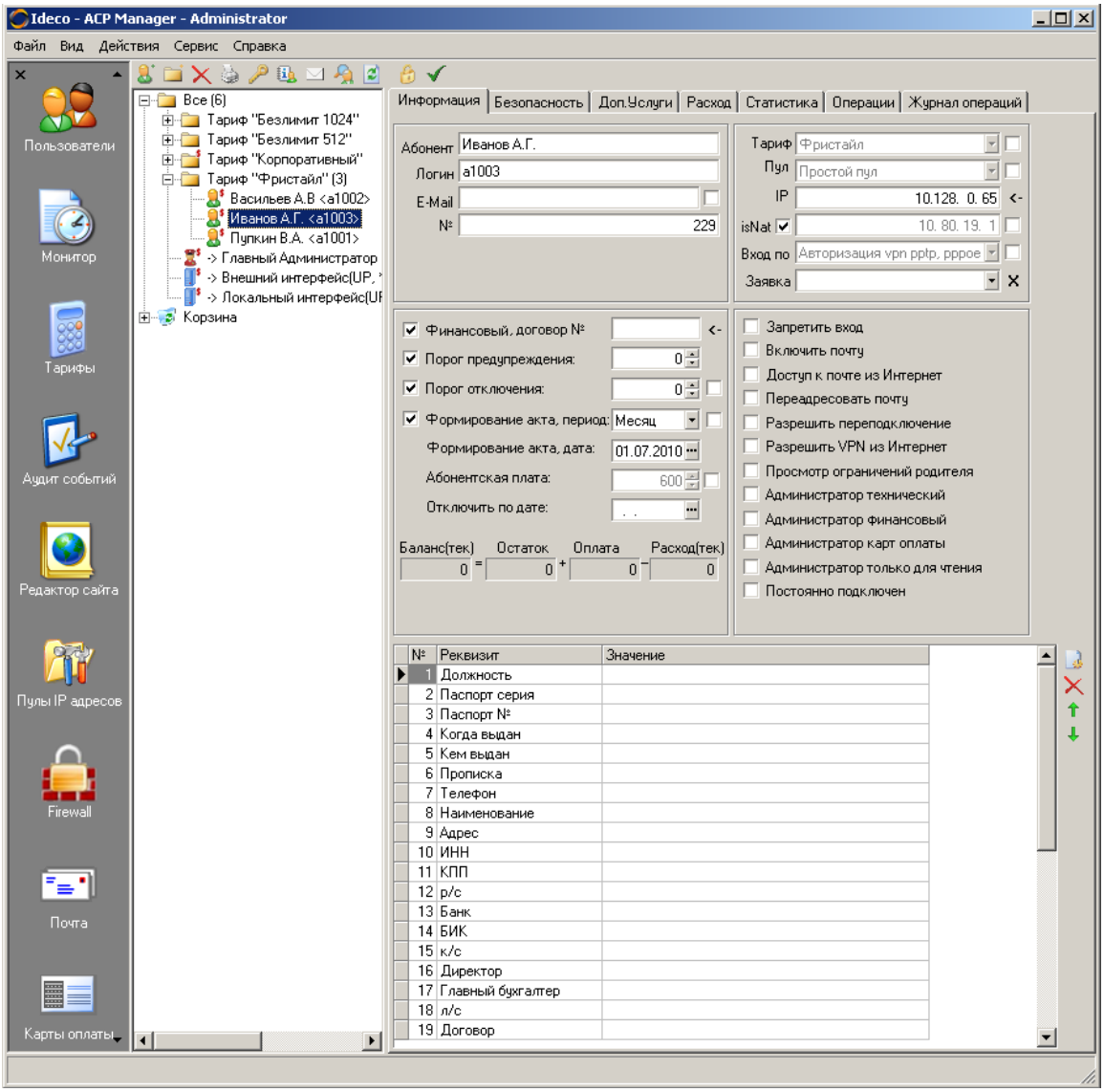
Сортировка в зависимости от адреса проживания абонента.

Суть данного принципа сортировки состоит в том, что в базе создается несколько групп, соответствующих улице, на которой подключены абоненты (в больших городах можно группы с названием улиц поместить в группу с названием района города).



Сортировка в зависимости от тарифного плана.

Суть данного принципа сортировки состоит в том, что в базе создается несколько групп, соответствующих тарифному плану (ТП). Главный плюс этого способа - не надо назначать тариф каждому пользователю вручную, при смене ТП пользователя достаточно переместить в другую группу, соответствующую новому ТП.



Примечание: Часто Юридические лица сортируются отдельно от физических, для них так же можно создать свою группу.

Чтобы у абонентов появился доступ в Интернет им необходимо авторизоваться, подробнее об этом написано в главе "Авторизация пользователей на Ideco ACP 60**"**

2.5 Работа в режим ACP

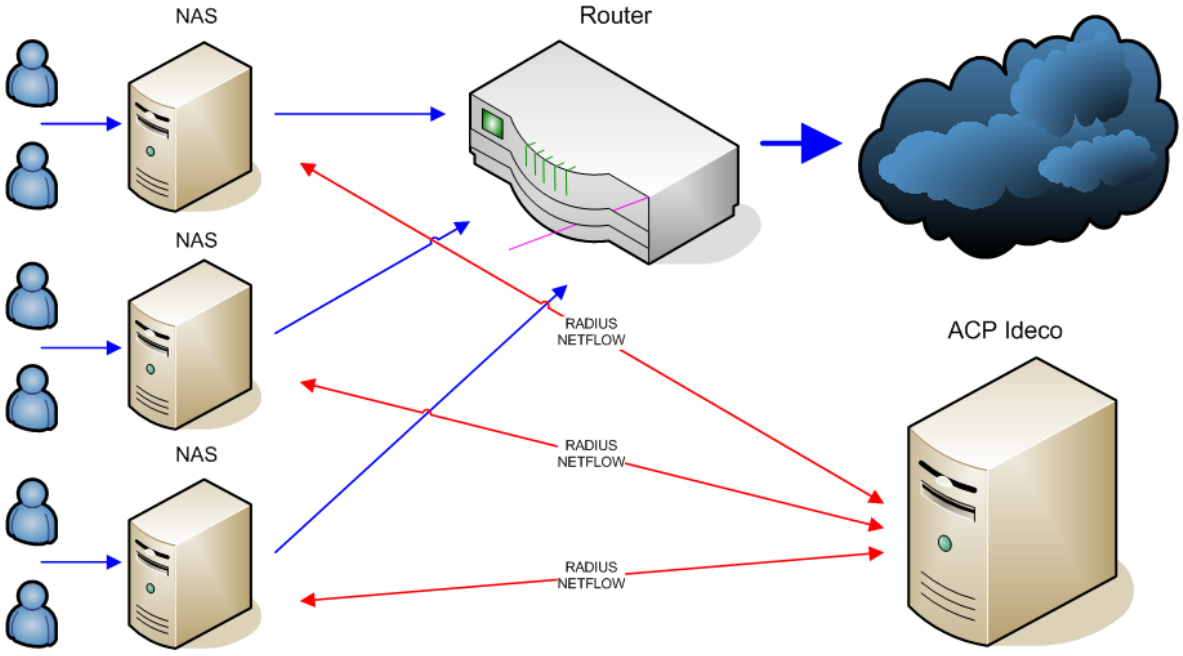
Теперь рассмотрим вариант, когда сеть провайдера разделена на IP-сегменты или VLAN, каждый из которых обслуживается Ideco AS 3000 или другим NAS-сервером или маршрутизатором или коммутатором. Интернет-трафик раздается при помощи маршрутизатора, установленного на границе с Интернетом. NAS-серверы или

коммутаторы подключены к этому маршрутизатору. Авторизация и контроль трафика пользователей осуществляются при помощи протоколов Radius и Netflow, соответствующие сервисы запущенны на сервере Ideco ACP. Ideco ACP имеет возможность как принимать так и отсылать команды NAS серверам и коммутаторам по SNMP/Telnet/SSH/CoA. Таким образом, авторизация, отключение абонентов, и учет трафика возлагается на ACP Ideco. С такой схемой построения сети возможно до 50000-100000 зарегистрированных пользователей и более при дополнительных условиях; Ширина канала ограничена лишь пропускной способностью сети и возможностями маршрутизатора.

2.5.1 Схема работы с NAS

NAS (Network Access Cerver) - это сервер или маршрутизатор, обеспечивающий доступ в Интернет абонентам, а также авторизацию и терминирование сессий по протоколам PPPoE, L2TP, PPTP, IPoE. Как правило, NAS поддерживает Radius AAA и NetFlow.

NAS (BRAS) обычно производят такие компании как Cisco и Hyawei. Так же в качестве NAS можно использовать Ideco AS 3000. Подробнее ..



- Подразумевается, что Ideco ACP будет взаимодействовать непосредственно с NAS серверами.
- Авторизация пользователей должна быть по **VPN/PPPoE/L2TP**.
- В идеале управление роутером в такой схеме не требуется.

Как происходит подключение клиентов

- Пользователь инициирует процесс подключения к NAS по протоколу pptp, pppoe, l2tp.

- NAS-сервер передает RADIUS-запрос на авторизацию клиента на сервер Ideco ACP.
- Ideco ACP отвечает NAS-серверу разрешая (или запрещая) выход пользователя в Интернет и (если указано) передает параметры RADIUS из тарифного плана.
- NAS-сервер авторизует пользователя, открывая ему выход в Интернет и создает шейпер для этого пользователя.

Учет трафика пользователей

- Информация о трафике абонентов, проходящего через NAS, отсылается по NetFlow на ACP Ideco для контроля и тарификации.

Отключение клиентов

- ACP Ideco перестает отвечать на периодические запросы аккаунтинга и NAS-сервер на основании этого отключает клиента(необходима поддержка возможности на NAS), либо можно передать команду разрыва соединения через SNMP/Telnet/SSH/CoA.
- Так же возможно отключение клиента по превышению лимита (если включена галочка "порог отключения" у клиента), то при попытке авторизации доступ будет запрещен, а при достижении лимита запросы аккаунтинга не будут обслуживаться.

Практическая реализация данной схемы на сервере Ideco ACP:

В качестве NAS сервера выступает стороннее оборудование:

Порядок настройки Ideco ACP:

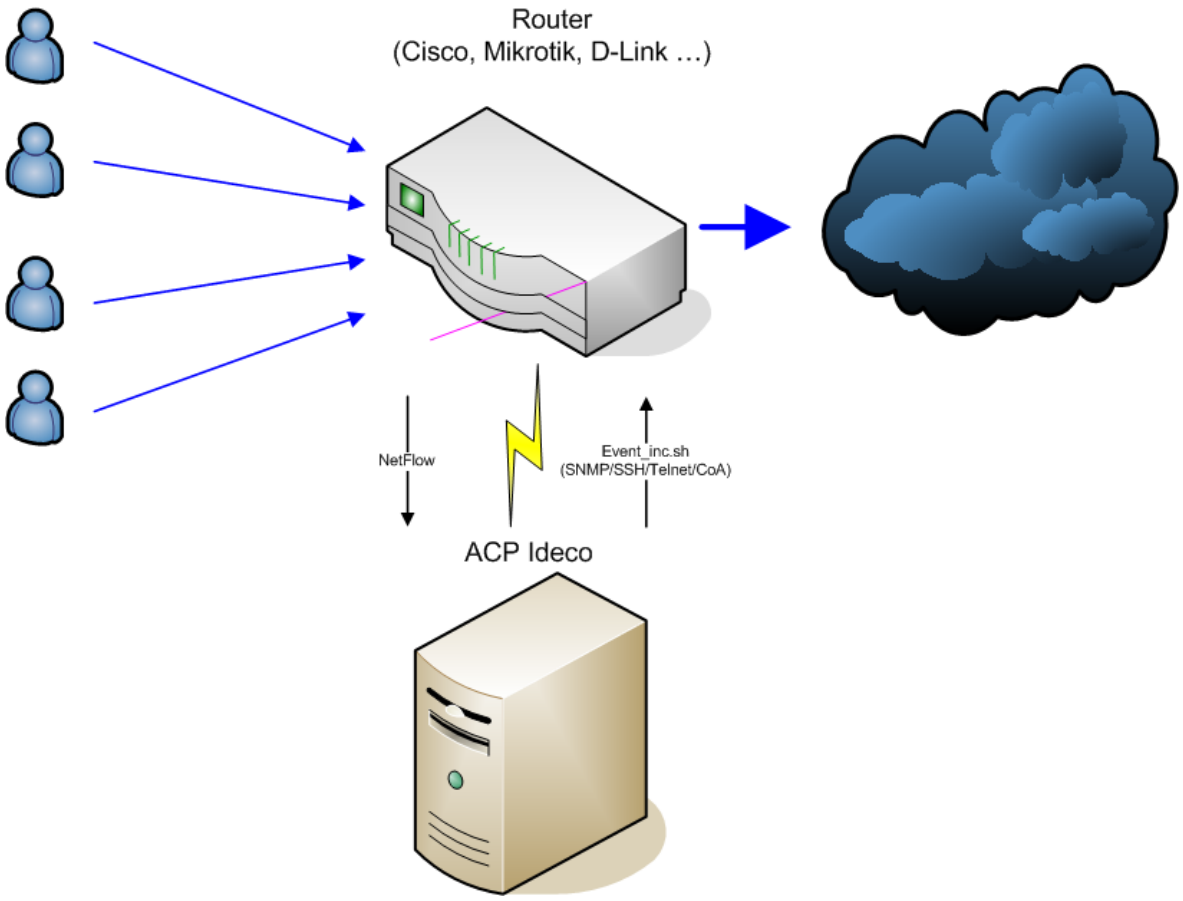
1. Указать порт для Netflow. Подробнее 153 ...
2. Включить Radius сервер. Подробнее 150 ...
3. Внести NAS-клиентов (подробнее 148) в список оборудования Ideco ACP. Настроить Ideco AS 3000 (подробнее 41), если он используется в качестве NAS.
   1) IP
   2) Имя (произвольное)
   3) Секрет
   4) Тип NAS-клиентов
4. В тарифе задать Radius атрибуты (документировано в Cisco и других производителях, не требуется для Ideco AS 3000). Подробнее 224 ..
5. Завести пользователей с помощью Ideco ACP Manager. Выставить авторизацию пользователей по Radius.
6. Поставить галочку в ACP Manager "Сервис - Настройки - Не авторизовывать по Radius при отрицательном балансе"
7. Поставить галочку в ACP Manager "Сервис - Настройки - Авторизация по Radius только для Radius-пользователей"
8. Выполнить мягкую или полную перезагрузку сервера Ideco ACP.

В качестве NAS сервера выступает Ideco AS:

После выполнения необходимых действий по подключению NAS-клиента необходимо произвести соответствующие настройки на самом NAS-сервере:

1. На Ideco ACP включить авторизацию клиентов с использованием RADIUS-сервера и указать на Ideco-NAS локальный IP-адрес ACP Ideco в качестве RADIUS-сервера.
2. Указать секретный пароль для связи с RADIUS-сервером (задается на этапе настройки NAS-клиента в локальном меню)
3. Настроить передачу потоков NetFlow с NAS-сервера на локальный IP-адрес биллинга ACP Ideco на порт 9996 (в случае необходимости порт может быть изменен в локальном меню)

2.5.2 Схема работы с маршрутизатором



- Подразумевается, что Ideco ACP будет взаимодействовать с маршрутизатором или коммутатором.
- К данной схеме более применима авторизация по **IP**.

Как происходит подключение клиентов

- Все клиенты должны иметь тип авторизации по IP. Таким образом они считаются постоянно подключенными и авторизованными на сервере Ideco ACP. По умолчанию доступ в сеть Интернет на маршрутизаторе им открыт.

Учет трафика пользователей

- Трафик пользователя, проходящий через коммутатор, передается на ACP для контроля и тарификации.

Отключение клиентов

- Происходит по событиям системы и вызову управляющих скриптов в event_inc.sh, скрипт посылает команды отключения на коммутатор.
- Явный запрет пользователю на авторизацию и выход в Интернет. Например: установлена галочка "Запретить вход" и IP-аккаунт пользователя перестает считаться авторизованным на сервере.

Практическая реализация данной схемы на сервере Ideco ACP:

Порядок настройки Ideco ACP:

1. Выбрать у пользователей авторизацию по IP.
2. Добавить ваш коммутатор или маршрутизатор в Ideco ACP. Подробнее 148 ...
3. Включить NetFlow. Подробнее 153 ...
4. В /var/lib/event/event_inc.sh создать скрипты для управления оборудованием по протоколам:
   4.1.SNMP
   4.2.Radius (CoA)
   4.3.SSH
   4.4 Telnet

Управление оборудованием с помощью файла инструкций event_inc.sh

Есть несколько сетевых протоколов управления оборудованием. Среди них нельзя выделить какой-то один более приоритетный способ, так как сегодня разные устройства используют разные протоколы управления. Иногда устройство предоставляет выбор: по какому из протоколов им можно управлять, но чаще на практике конкретное устройство лучше поддерживает один способ управления. Выбор протокола управления необходимо проводить на основе опыта специалистов и документации производителей.

На сервере Ideco ACP управление оборудованием (запуск клиента соответствующего протокола управления) работает по заранее определенным событиям в системе. Например: достижение пользователем нулевого баланса, достижение пользователем положительного баланса, подключение пользователя к системе, отключение пользователя от системы, изменение данных клиента и закрытие финансового периода.

Для включения обработки событий (только в Ideco ACP 3) необходимо:
1. Зайти в локальное меню системы "Конфигурирование сервера" -> "Дополнительные настройки..."
2. Поставить галочку "Запускать скрипт обработки событий"
3. Сохранить конфигурацию и произвести мягкую перезагрузку.

После этого для выполнения нужных вам действий с оборудованием по событию необходимо внести требуемые команды в скрипт `event_inc.sh`, расположенный на сервере Ideco ACP в директории `/var/lib/event/`.

Как было сказано выше, способов управления оборудованием много и каждое

устройство работает по своему. Поэтому в Ideco ACP пока не реализованы готовые схемы работы с тем или иным оборудованием в виде команд для скрипта `event_inc.sh`. В связи с этим вам предстоит самостоятельно изучить команды вашего оборудования и составить скрипты, вызывающие их по тому или иному событию и добавить эти скрипты в `event_inc.sh`.

Каждый раз при вызове скрипта event_inc.sh, вместе с названием события ему передаются следующие параметры пользователя в виде переменных (в скобках указаны названия переменных в скрипте):
1. идентификатор (id)
2. IP-адрес (ip)
3. MAC-адрес (mac)
4. электронный почтовый адрес (email)
5. NAT IP-адрес (snat)
6. флаг финансового пользователя (finance)
7. флаг состояния пользователя включен/выключен (enabled)
8. флаг удаленного пользователя (deleted)
9. флаг залогиненого пользователя (logged)
10. тип авторизации пользователя (auth_type)
11. идентификатор тарифа (tariff_id)
12. номер договора (contract_number)

Скрипт event_inc.sh должен быть написан в синтаксисе BASH, командного интерпретатора linux. Инструкции оборудованию по определенному событию нужно передавать с помощью команд-клиентов соответствующего протокола (например snmpset, клиент протокола SNMP) управления вашим оборудованием с передачей нужных параметров (например IP-адрес, MAC-адрес). Для универсальности описываемых вами действий в скрипте и используются переменные BASH перечисленные выше в скобках. Писать инструкцию оборудованию по тому или иному событию нужно в соответствующей части файла event_inc.sh, где начинается обработка этого события. Обработка событий в event_inc.sh начинается после строк:

```
case $EVENT in
```

В настоящее время из-за отсутствия готовых схем управления по каждому событию в скрипте не происходит ничего кроме записи в системный лог того что событие произошло. Сами действия предстоит вписать вам.

Рассмотрим пример, в котором по протоколу управления SNMP мы будем отключать порт на коммутаторе пользователю у кого сработало событие превышения баланса.

Для работы с SNMP в системе существует три программы:
1. snmpwalk - получить список параметров доступных по SNMP
2. snmpset - для установки значений параметров по SNMP
3. snmpget - для получения значений параметров по SNMP

В event_inc.sh ищем после строки `case $EVENT in` начало обработки этого события. Оно начинается строкой "`balance_negative`"). При срабатывании события и вызове файла event_inc.sh ему будет передана переменная названия события $EVENT со значением balance_negative и другие параметры пользователя, у которого был превышен баланс, в виде переменных. Для отключения порта пользователя на коммутаторе впишем команду `snmpset -v 2c -c public 1.3.6.1.2.1.2.2.1.7.5 integer 2`. В итоге блок команд вызываемых по наступлению события превышения баланса будет выглядеть так:

```
"balance_negative")
snmpset -v 2c -c public 172.16.0.253 1.3.6.1.2.1.2.2.1.7.5 integer 2
LOG INFO "event type: $EVENT $DATA"
;;
```

В Ideco ACP реализована возможность создавать и передавать скрипту event_inc.sh свои параметры пользователей из числа реквизитов, начинающиеся с префикса "EVENT_". В нашем случае мы каждому пользователю должны прописать реквизит определяющий номер порта пользователя на коммутаторе. Назовем реквизит "EVENT_PORT". В примере выше SNMP OID `1.3.6.1.2.1.2.2.1.7.5` определяет статус порта (включен, выключен) и номер самого порта, над которым производится операция. Номер порта в этом OID'е указывается последней цифрой ("5"). Чтобы скрипт был универсальным, заменим последний параметр OID'а на переменную BASH $EVENT_PORT, которая берется из одноименного реквизита пользователя. В итоге окончательный вариант инструкции коммутатору будет выглядеть так:

```
"balance_negative")
snmpset -v 2c -c public 172.16.0.253 1.3.6.1.2.1.2.2.1.7.$EVENT_PORT
LOG INFO "event type: $EVENT $DATA"
;;
```

Примечания:

- Чтобы реквизит пользователя в виде переменной передавался скрипту event_inc.sh, этот реквизит должен иметь имя EVENT_*.
- Из скрипта к переменным пользователя можно обращаться через запись $name, где name это название одной из перечисленных выше переменных. Например, "echo $ip" (без кавычек) выведет на экран IP-адрес пользователя
- В будущем станут доступны готовые схемы управления определенными моделями маршрутизаторов. В данный момент эта возможность находится в стадии разработки и если у вас возникли затруднения по реализации конкретной схемы управления вашим оборудованием, то обратитесь напрямую в отдел разработки:

E-Mail: asr@ideco-software.ru

ICQ: 598904096

2.5.3 Схема работы с Cisco ISG

Раздел находится в разработке.

За консультацией по настройке оборудования обратитесь напрямую к разработчикам:

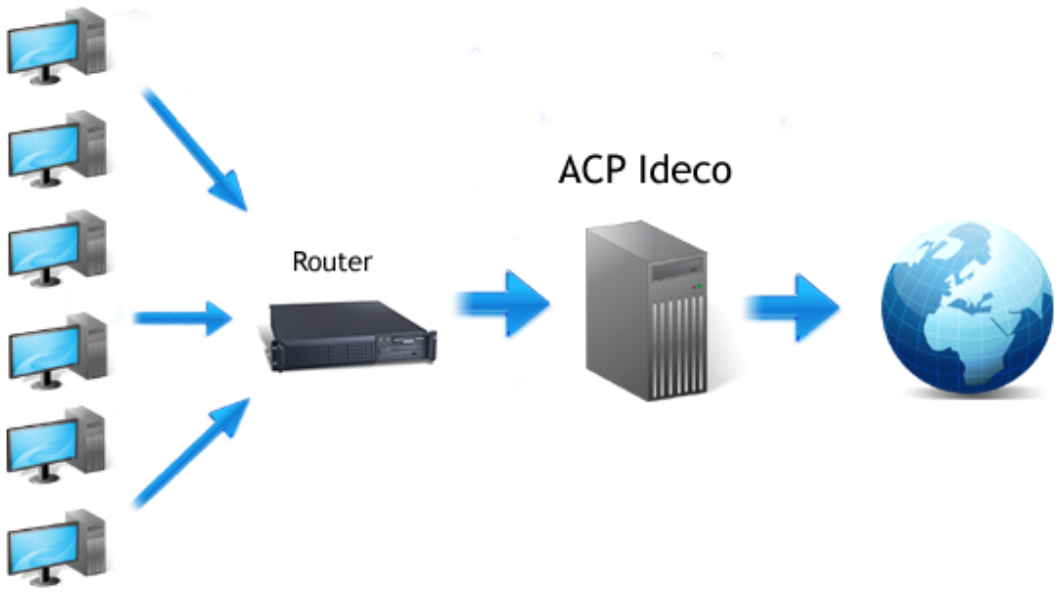
asr@ideco-software.ru

ICQ 598904096

2.6 Работа в режиме SoftRouter

Ideco ACP может работать и без дополнительного оборудования, это удобно для начинающих провайдеров, ВУЗ-ов, гостиниц и т.п. Такой режим называется **SoftRouter**.

Рассмотрим схему работы Ideco ACP в режиме SoftRouter - в этом режиме Ideco ACP устанавливается на границе между Интернет и локальной сетью. Весь Интернет-трафик проходит через Ideco ACP что обеспечивает подсчет, блокирование и лимитирование скорости.

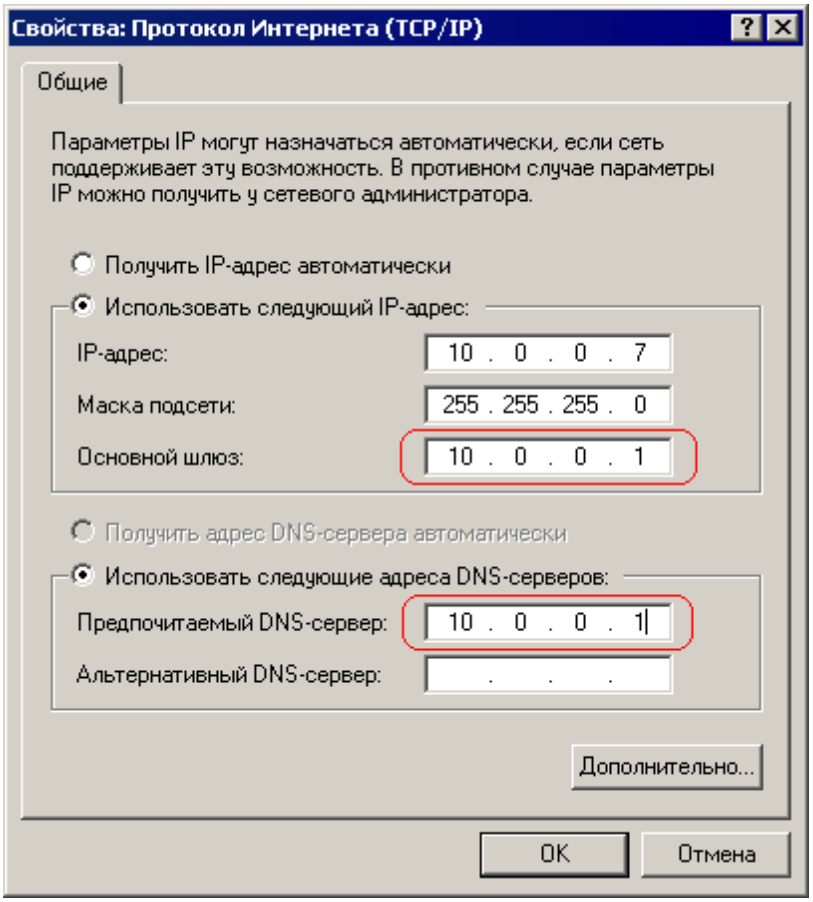


После того как вы закончите настройку сервера и наполните базу данных пора переходить к настройке соединения пользователей с Ideco ACP.

Способы авторизации пользователей на Ideco ACP в режиме SoftRouter:

- Авторизация по IP. Подробнее ...63
- Авторизация по VPN (PPTP). Подробнее ...64
- Авторизация по PPPoE. Подробнее ...69
- Авторизация через Ideco Agent. Подробнее ...69
- Авторизация через веб-интерфейс. Подробнее ...72

Простейший вариант - авторизация по IP. Необходимо на компьютерах пользователей в качестве **шлюза** и **DNS** прописать локальный адрес Ideco ACP:



Таким образом при включении компьютера эти пользователи будут автоматически выходить в Интернет через Ideco ACP.

На компьютере клиента откройте браузер и в адресной строке наберите название любого сайта в Интернете, к примеру:


Яндекс - Windows Internet Explorer
http://www.yandex.ru/
Файл Правка Вид Избранное Сервис Справка
Яндекс
Страница Сервис
Internet Explorer 8 – установите бесплатно новую версию вашего браузера
Установить
Закрыть
Сделать Яндекс стартовой страницей
Настроить
Войти в почту
Сегодня в новостях 09:49 все Екатеринбург
1. ЦСКА выиграл у «Вольфсбурга» в матче 5-го тура группового турнира ЛЧ
2. Магнитский причастен к налоговым преступлениям на 3,5 млрд руб — МВД
3. Федерация бобслея готова взять на себя расходы по лечению Скворцовой
4. Полиция Женевы передала досье россиянина Бабаева в прокуратуру
5. Подозреваемый в убийстве уроженца Абхазии частично признал свою вину
Рекламные возможности Яндекса
10-11 декабря практический семинар в Екатеринбурге
Яндекс
Найдётся всё
Поиск Карты Маркет Новости Словари Блоги Видео Картинки еще
Найти
Например, стоит, стыдясь, зима у входа и не решается войти
расширенный поиск
Почта
логин
пароль
запомнить меня
Войти
вспомнить пароль
Завести почтовый ящик
Фотки
Фото дня
Каталог сайтов
Игры и развлечения
Спорт и отдых
Работа и учеба
Компьютеры
Бизнес
Дом и авто
Сайты Екатеринбурга
Сегодня в блогах
1. Глобальное потепление
2. Россиянка победила в конкурсе "Миссис мира-2009"
3. Два участника съезда "Единой России" упали с трибуны
Маркет
смартфоны до 9 тыс. руб.
Авто
купить в Екатеринбурге
Расписания
поездов и электричек
Мой Круг
новые вакансии
Народ
конструктор сайтов
Деньги
Директ
запустить генератор продаж
Метрика
измерение конверсии сайта
Екатеринбург, 26 ноября, четверг, 09:49
Погода +1
днем +3
Котировки
сегодня
USD ЦБ 28,7909
EUR ЦБ 43,1921
Нефть −0,43% 78,07 26/11
Телепрограмма
09:00 Следствие вели... НТВ
09:05 Малахов+ Первый
09:05 Дальневосточный исход Россия
Пробки 5 баллов
Движение плотное
Скачать на мобильный
Карта Екатеринбурга
Адреса и телефоны
Панорамы Москвы
Афиша
Сумерки 2: Новолуние фантастика
2012 драма
Рождественская история драма
Добавить: Отдам даром · Урал.ру: работа в Екатеринбурге · Форумы на E1.RU и еще 46 виджетов для Екатеринбурга

Часть

3 Конфигурирование

Раздел содержит основные этапы настройки Ideco ACP для обеспечения работы пользователей в сети Интернет, учета и контроля траффика, подключения к провайдеру.

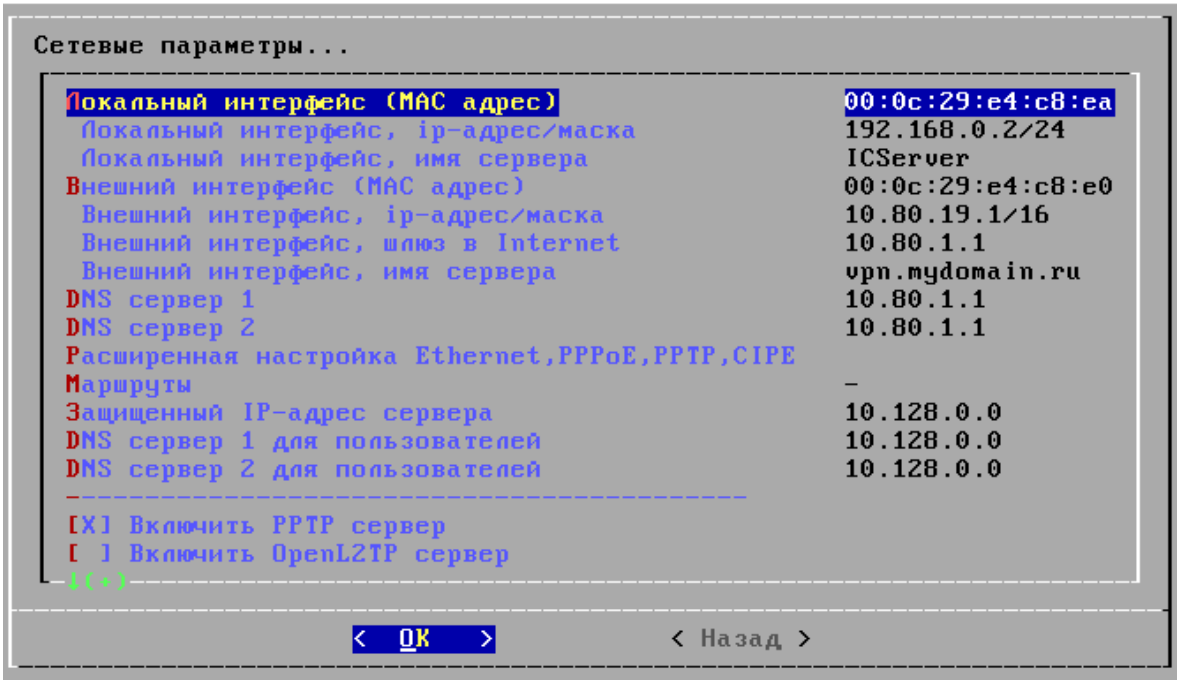
3.1 Настройка подключения к провайдеру

В этом разделе подробно описаны способы подключения сервера к сетям провайдера. В основном данная настройка необходима для версии **SoftRouter**, если сервер используется только в качестве биллинга в распределённых сетях - настраивать подключение к провайдеру не обязательно.

3.1.1 Прямое подключение по Ethernet

Прямое подключение по Ethernet

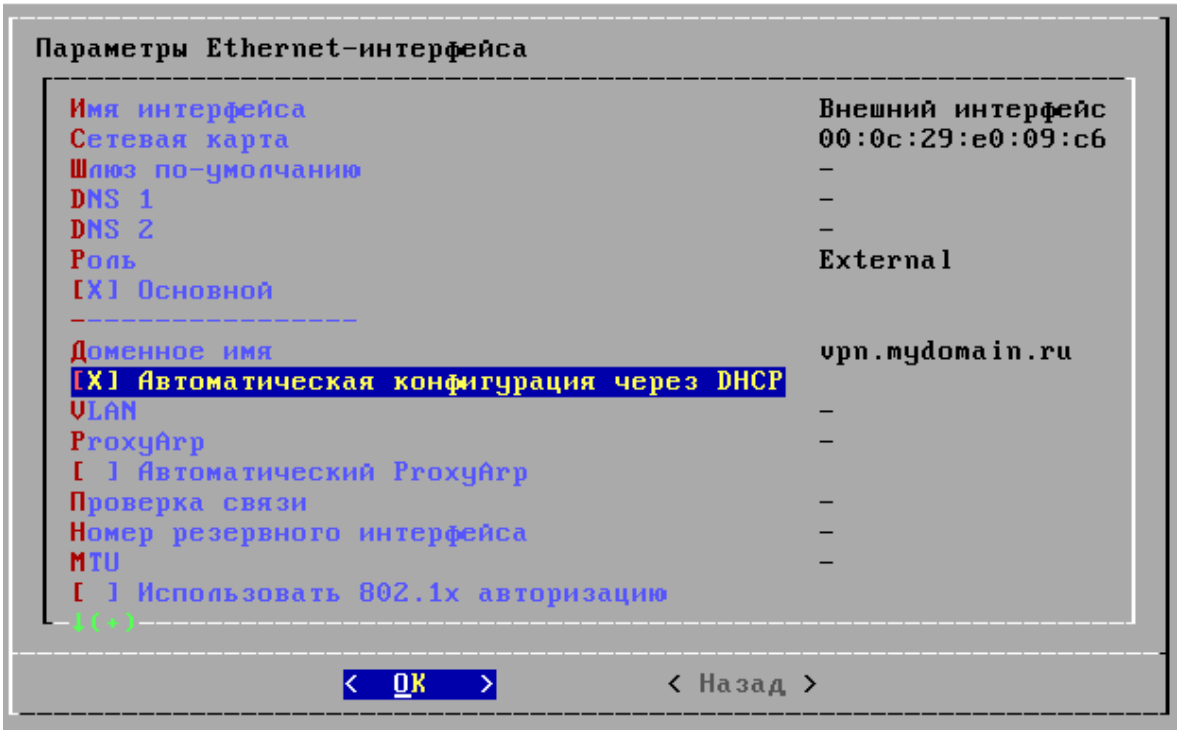
Меню -> Конфигурирование сервера -> Конфигурирование сети



Необходимо выбрать сетевую карту, подключенную к провайдеру в пункте "Внешний интерфейс (MAC адрес)", указать IP-адрес, маску подсети, шлюз и два DNS-сервера провайдера.

Если провайдер предоставляет динамический адрес по DHCP нужно в Меню -> Конфигурирование сервера -> Конфигурирование сети -> Расширенная настройка Ethernet, PPPoE, PPTP, CIPE ->

Выбрать "Внешний интерфейс", нажать "Параметры" и в параметрах интерфейса поставить галочку "Автоматическая конфигурация через DHCP"



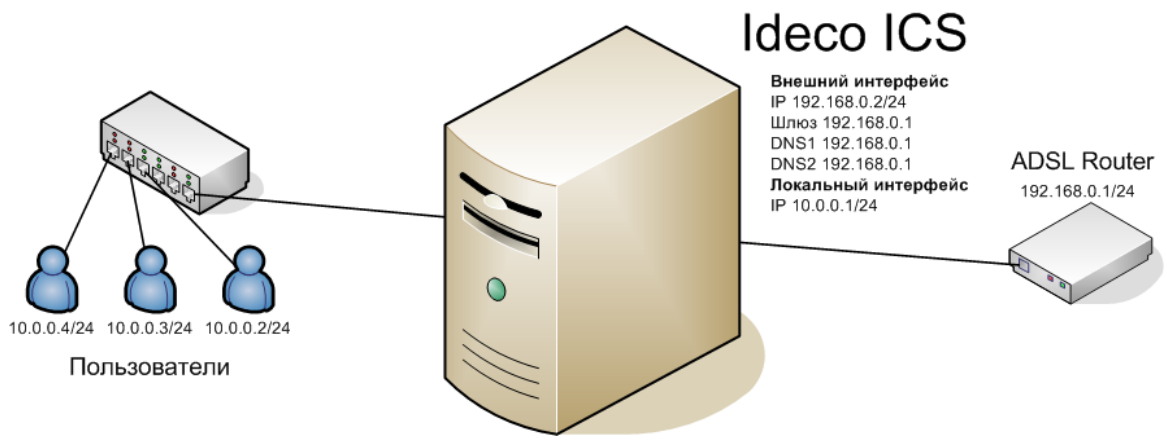
Следует отметить, что в случае перехода с другого оборудования возможно отсутствие интернета ввиду использования провайдером привязки по MAC адресу.

3.1.2 Прямое подключение по Ethernet через ADSL-модем в режиме роутера

Прямое подключение по Ethernet через ADSL в режиме роутера

Если модем находится в режиме роутера, то нужно сменить MTU на внешнем сетевом интерфейсе Ideco, указать их равными 1000. В этом случае необходимо настраивать Ideco ACP как в разделе Прямое подключение по Ethernet 50 и указывать локальный адрес модема в качестве шлюза для Ideco ACP. Необходимо обратить внимание на то чтобы адреса локальной сети не пересекались с адресами модема.

Пример: на модеме настроен адрес 192.168.0.1/24, в этом случае на ideco нужно прописать адрес из сети 192.168.0.0/24 (к примеру 192.168.0.2) а в качестве шлюза и DNS нужно указать 192.168.0.1. Соответственно адресация в локальной сети ни в коем случае не должна пересекаться с сетью 192.168.0.0/24 (как вариант можно использовать локальные адреса по умолчанию - 10.0.0.0/24). Этот вариант настройки изображен на рисунке:



3.1.3 Подключение по PPPoE через ADSL-модем, настроенный в режиме моста

1. Настроить на любом компьютере с Windows такой-же IP-адрес и маску как на внешнем интерфейсе Ideco. Пусть это будет 192.168.1.50 / 255.255.255.0
2. Подключить модем непосредственно к сетевой карте компьютера с Windows
3. Набрать в браузере http://IP-адрес_модема (тот который был указан в качестве шлюза по-умолчанию в Ideco). В большинстве случаев это http://192.168.1.1
4. Убедиться, что модем работает в режиме маршрутизатора (Router). Если это не так, то скорее всего он уже в режиме моста и ничего менять не нужно.
5. В веб-интерфейсе модема выяснить, используется ли PPPoE для подключения к провайдеру.
   Если используется, то переписать из модема логин и пароль для подключения по PPPoE. Если не используется, то переписать IP-адрес, маску подсети, шлюз по-умолчанию и, если есть, IP-адреса двух DNS-серверов.
6. Прежде чем менять какие-либо параметры в модеме - сделайте скриншоты всех настроек **на всех** подразделах ACPa модема - это пригодится если нужно будет откатить изменения обратно.
7. Переключите модем в режим моста. (Bridge). **Никакие другие параметры менять не нужно (включая VPI,VCI,тип инкапсуляции и другие)**. После этого связь с модемом (через браузер) может потеряться. Это нормально.
8. Подключить модем обратно к сетевой карте сервера (ко внешнему интерфейсу Ideco)
9. Если на модеме использовалось подключение PPPoE то настроить PPPoE на внешнем интерфейсе Ideco, указав записанный логин и пароль (Подключение по PPPoE 53). Если нет, то настроить на внешнем интерфейсе Ideco переписанные IP-адрес, маску, шлюз и DNS-сервера которые выдал провайдер.
10. Произвести мягкую перезагрузку сервера

Если использовался PPPoE то в ACP Manager посмотреть, подключился ли к

провайдеру настроенный там интерфейс. (В названии интерфейса в списке пользователей должны присутствовать слова "PING, OK")

Теперь нужно проверить доступность сети интернет непосредственно с сервера. Локальная консоль сервера - Меню - сервис - MC-commander. Далее нажать Ctrl+o, затем набрать команду:

```
ping yandex.ru
```

Если связь есть - значит всё настроено верно. Если связи нет - свяжитесь с технической поддержкой по телефону или ICQ 463710578 (с другого канала Интернет или с другого IP-адреса, если у вас несколько). Прервать проверку связи - Ctrl+C. Далее нажать Ctrl+O и F10.

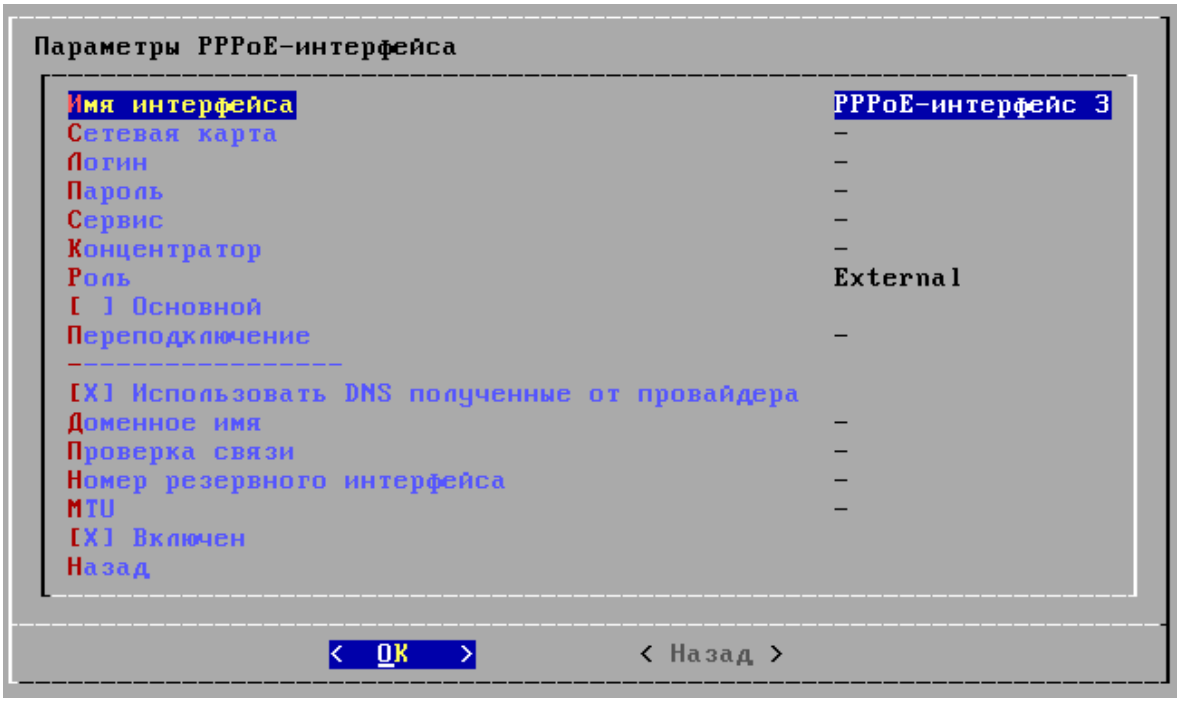
В случае если связи с тех.поддержкой нет и настроить Интернет не удается - нужно откатиться на старые настройки - подключив модем обратно к Windows и набрав http://192.168.1.1. Если это не поможет - то делайте аппаратный сброс модема и восстанавливайте конфигурацию по скриншотам. Если после аппаратного сброса добраться до настроек модема невозможно - обращайтесь к провайдеру.

3.1.4 Подключение по PPPoE

Подключение по PPPoE

Для того чтобы подключить Интернет-шлюз Ideco ACP по протоколу PPPoE к провайдеру необходимо произвести следующее:

1. Открыть "Меню -> Конфигурирование сервера -> Конфигурирование сети -> Расширенная настройка Ethernet, PPPoE, PPTP, CIPE ->"
2. В этом диалоге создать интерфейс и указать тип "PPPoE".



3. В поле "Сетевая карта" выбрать MAC-адрес сетевой карты, подключенной к

провайдеру

4. Указать логин и пароль.

5. Выбрать "[X] Основной".

6. Поставить "[X] Использовать DNS полученные от провайдера"

7. Если провайдер требует указания имени сервиса и концентратора, указать их в соответствующих полях.

8. Сделать мягкую перезагрузку, а затем подключиться к АСРу сервера.

9. В корневой папке должен появиться пользователь, соответствующий созданному интерфейсу. В имени этого пользователя можно смотреть состояние интерфейса: "DOWN" - не подключен, "GOING UP" - производится подключение, "UP" - подключен.

10. В параметрах тарифного плана выбрать этот интерфейс в поле «Интернет интерфейс».

11. Убедиться, что у пользователя в поле isNat 

появился IP адрес выданный провайдером по PPPoE.

Важно! При подключении через ADSL, xDSL модем необходимо выяснить, в каком режиме настроен модем. Если модем настроен в режиме моста, то необходимо настроить PPPoE подключение к провайдеру на Ideco ACP по данной инструкции.

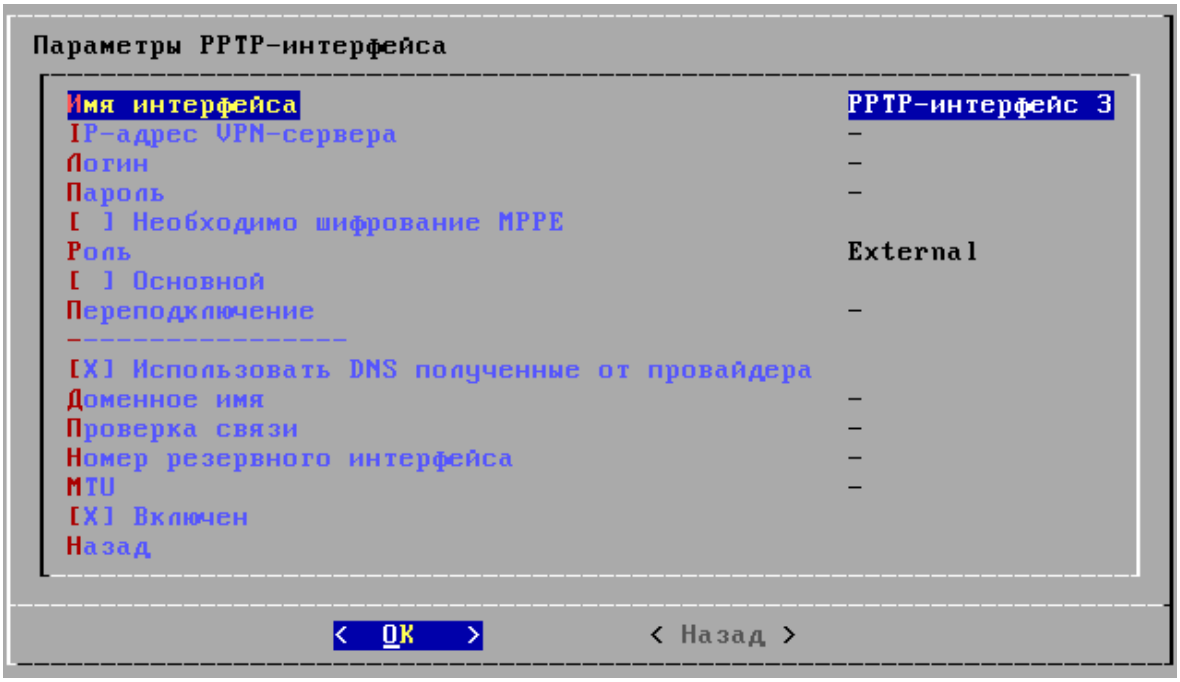
3.1.5 Подключение по VPN (PPTP)

Подключение по PPTP (VPN)

Для этого способа подключения необходимо в первую очередь настроить Ethernet-подключение к провайдеру аналогично разделу Прямое подключение по Ethernet 50 . После чего произвести следующее:

1. Открыть "Меню -> Конфигурирование сервера -> Конфигурирование сети -> Расширенная настройка Ethernet, PPPoE, PPTP, CIPE ->"

2. В этом диалоге создать интерфейс и выбрать тип "PPTP".

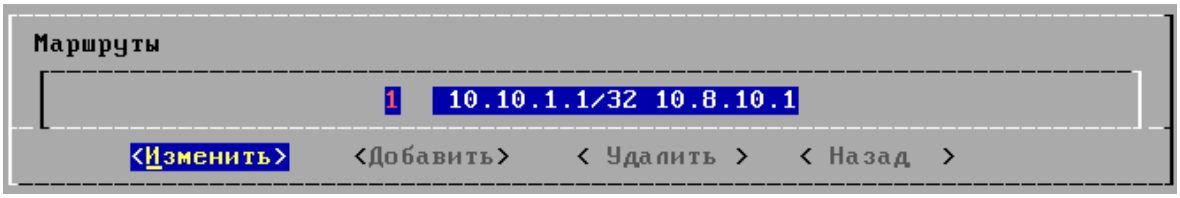


3. В поле "IP-адрес VPN-сервера" ввести IP-адрес VPN-сервера провайдера
4. Ввести логин и пароль.
5. Если провайдер требует шифрования MPPE, установить соответствующий флажок
6. Выбрать "[X] Основной".
7. В локальной консоли открыть раздел "Конфигурирование сервера" – "Конфигурирование сети" – "Маршруты". Добавить маршрут вида: <IP-адрес VPN-сервера провайдера> <"шлюз по-умолчанию" провайдера>

К примеру: IP-адрес VPN-сервера провайдера - 10.10.1.1

На внешнем интерфейсе прописан адрес: 10.8.10.123/24 шлюз 10.8.10.1

Соответственно добавляем маршрут как показано на рисунке:



8. Сделать мягкую перезагрузку, а затем подключиться к АСРу.

В корневой папке должен появиться пользователь, соответствующий созданному интерфейсу. В имени этого пользователя можно смотреть состояние интерфейса: "DOWN" - не подключен, "GOING UP" - производится подключение, "UP" - подключен.

В параметрах тарифного плана выбрать этот интерфейс в поле «Интернет интерфейс».

Убедиться, что у пользователя в поле NAT появился IP адрес выданный

провайдером по PPTP.

3.1.6 Подключение к нескольким провайдерам

Подключение к нескольким провайдерам

Подключение дополнительного провайдера можно использовать для:

Первый случай: Разгрузки основного провайдера, то есть часть пользователей будет постоянно работать через дополнительного. Настраивается следующим образом:

1. Для дополнительного провайдера сконфигурировать сетевой интерфейс (Меню -> Конфигурирование сервера -> Конфигурирование сети -> Расширенная настройка Ethernet, PPPoE, PPTP, CIPE ->). При настройке укажите параметры, указанные в договоре с провайдером. Внешний интерфейс, помеченный как «[X] Основной», будет использоваться по умолчанию и все текущие пользователи будут выходить в Интернет через него.

2. Создать новый пул IP-адресов в ACP Manager. Эти адреса будут выдаваться пользователям, выходящим в Интернет через дополнительного провайдера. Например, 10.230.1.0 / 255.255.255.0.

3. Создать маршрут (подробнее 139) вида:

<выбранная подсеть/маска> <0.0.0.0/0> <шлюз второго провайдера>.

Например,

10.230.1.0/255.255.255.0 0.0.0.0/0 10.15.20.1

Если подключение ко второму провайдеру через интерфейс PPTP или PPPoE, то укажите в качестве шлюза номер этого интерфейса.

Например,

10.230.1.0/255.255.255.0 0.0.0.0/0 4

4. Сделать мягкую перезагрузку, а затем подключиться к АСРу.

5. В разделе "Тарифы 220" создать тарифный план, который будет использоваться для подключения через дополнительного провайдера. Из списка «Интернет интерфейс» выбрать сетевой интерфейс соответствующий нужному провайдеру.

6. В разделе "Пользователи 184" создать новую папку. В параметрах «Тариф» и «Пул» указать созданные в пунктах 4 и 5 тарифный план и пул IP-адресов. Пользователи, созданные в этой папке, будут выходить в Интернет через альтернативного провайдера.

Примечание: Создавать пул IP адресов необязательно, у пользователей, работающих через дополнительный канал, адрес можно изменить вручную.

Второй случай: Маршрутизации части трафика, к примеру когда определённые сети через дополнительного провайдера тарифицируются дешевле. Допустим сеть 83.168.0.0/16 нужно маршрутизировать через дополнительный интерфейс, на котором прописаны IP 10.15.20.10/24 Шлюз 10.15.20.1

1. Для дополнительного провайдера сконфигурировать сетевой интерфейс (Меню

-> Конфигурирование сервера -> Конфигурирование сети -> Расширенная настройка Ethernet, PPPoE, PPTP, CIPE ->). При настройке укажите параметры, указанные в договоре с провайдером. Внешний интерфейс, помеченный как «[X] Основной», будет использоваться по умолчанию и все текущие пользователи будут выходить в Интернет через него.

2. Создать маршрут вида:

<Сеть назначения/маска> <шлюз второго провайдера>.

То есть,

83.168.0.0/16 10.15.20.1

3. Сделать мягкую перезагрузку, а затем подключиться к АСРу.

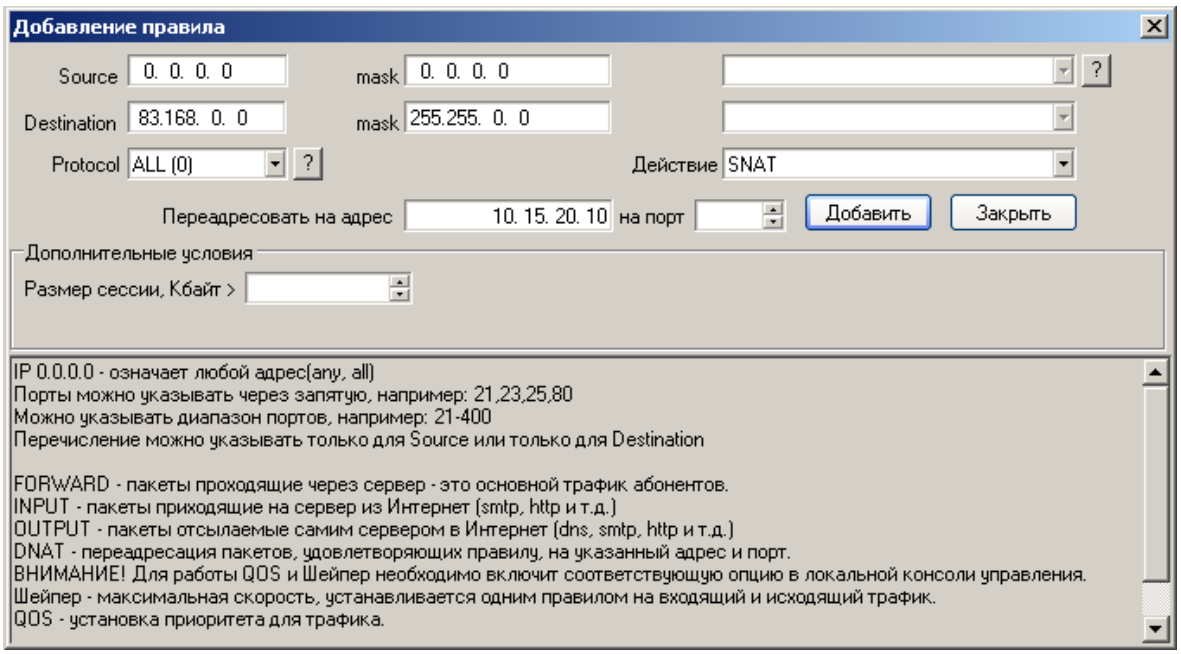
4. В разделе «Безопасность -> Системный Firewall» создать привило SNAT:

src 0.0.0.0 mask 0.0.0.0

dst <Сеть назначения> <Маска сети назначения>

SNAT <IP-адрес на дополнительном внешнем интерфейсе>

Ниже приведен пример такого правила:



5. Перезагрузить Firewall.

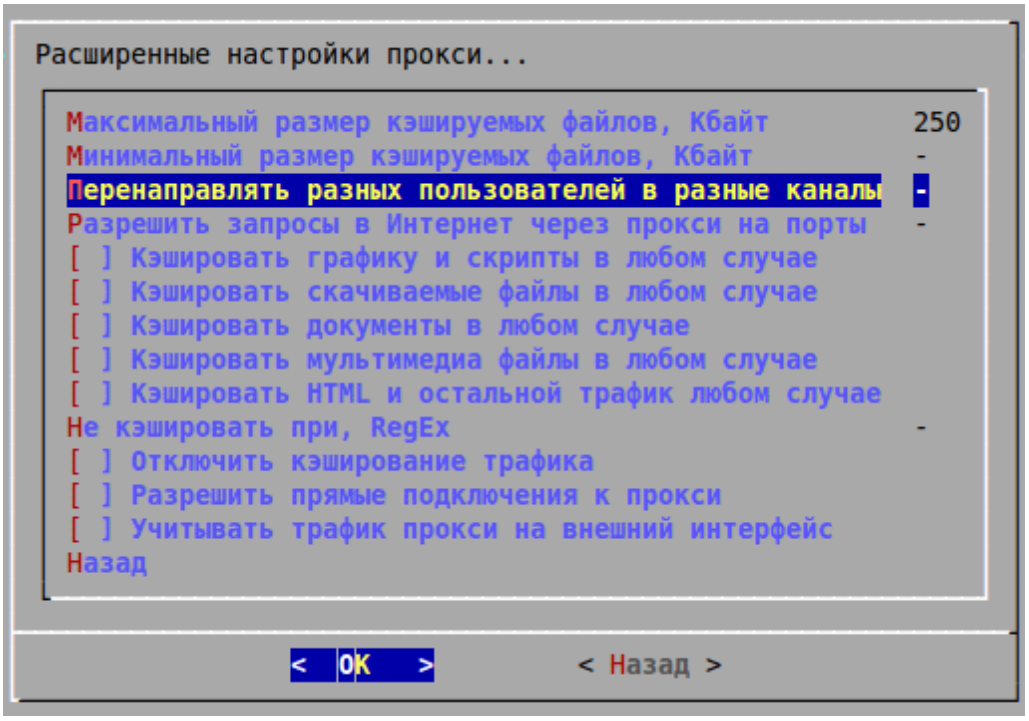
После этого трафик в сеть 83.168.0.0/16 будет ходить через дополнительного провайдера.

Внимание!

Если вы используете прокси-сервер (squid) в нашем продукте и настраиваете подключение к нескольким провайдерам через разные каналы, то для корректной маршрутизации и учета траффика необходимо так же настроить перенаправление траффика прокси-сервера (весь веб-траффик клиентов, 80 порт) через нужный вам канал. По умолчанию весь траффик прокси сервера идет через основной внешний интерфейс, вне зависимости от того какие дополнительные каналы от провайдеров у вас настроены. Учитывая два случая, описанные выше, настроим прокси-сервер так, чтобы весь веб-траффик из сети клиентов 192.168.0.0/24 шел

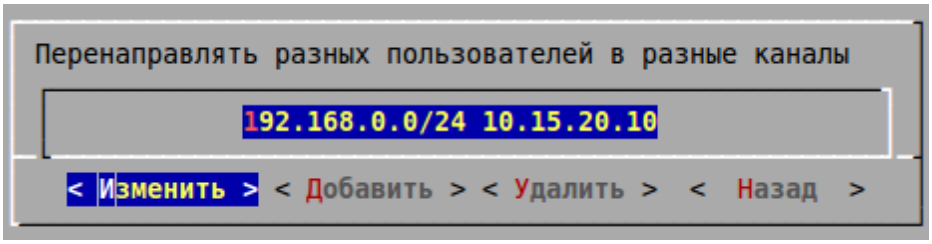
через неосновного провайдера.

В расширенных настройках прокси-сервера найдем пункт "Перенаправлять разных пользователей в разные каналы":



В этом пункте пропишем маршрут вида: <локальная сеть/маска> <ip-адрес интерфейса второго провайдера>

Для сети, описанной в обоих случаях, маршрут перенаправления веб-траффика через второго провайдера будет выглядеть так:



3.1.7 Автоматическое переключение каналов

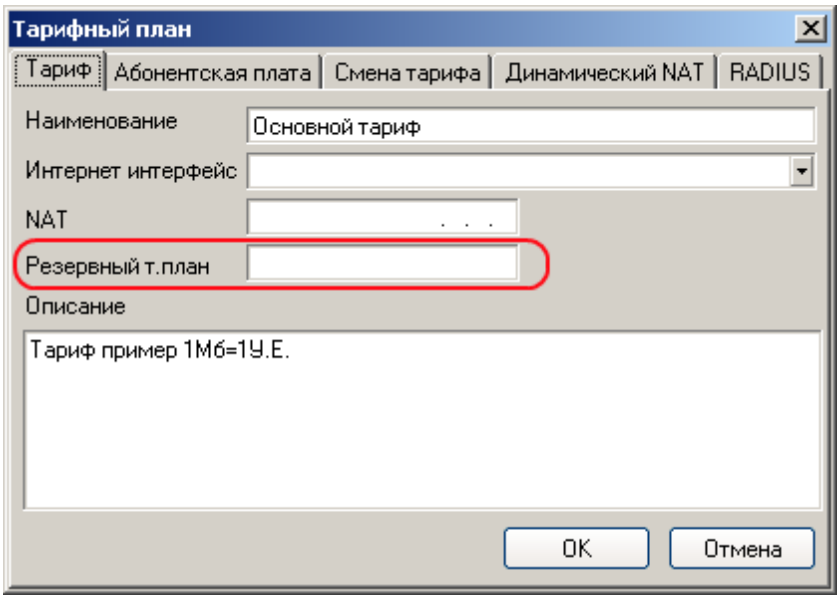
Автоматическое переключение каналов

Для того чтобы настроить резервный канал Интернет, который будет использоваться в случае потери связи через основной канал, необходимо сделать следующее:

1. Подключиться к АСРу.
2. Создать тарифный план для резервного Интернет-канала и в параметрах выбрать из списка «Интернет интерфейс» сетевой интерфейс, соответствующий

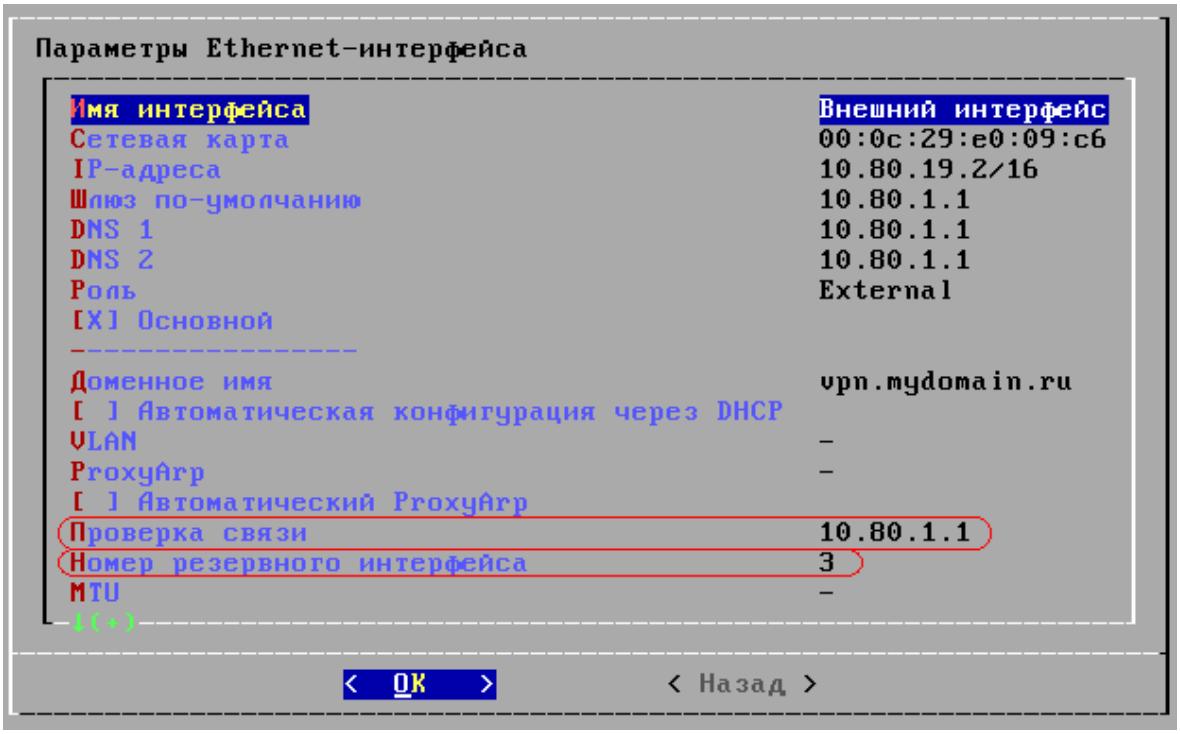
резервному каналу.

3. В параметрах основного тарифного плана выбрать в поле «Интернет интерфейс» сетевой интерфейс основного провайдера. В поле «Резервный т. план» основного тарифного плана указать номер резервного тарифного плана. На этот тарифный план будут переключены все пользователи основного тарифного плана в случае потери связи.



4. В локальной консоли открыть параметры интерфейса, соответствующего основному тарифному плану. Установить в поле «резервный интерфейс» номер интерфейса, связанного с резервным тарифным планом.

5. В параметрах интерфейса можно указать один или несколько IP-адресов, связь с которыми будет проверяться. Для Ethernet-подключений необходимо обязательно указать проверочные IP-адреса, иначе система не сможет определять наличие связи и будет считать, что связь всегда есть. В качестве проверочного IP-адреса, как правило, можно использовать шлюз провайдера, но лучше использовать адрес надежного Интернет-сервера.



6. **Аналогично настроить резервный интерфейс и тарифный план, чтобы при восстановлении связи произошло обратное переключение на основной интернет-канал**.
7. Произвести мягкую перезагрузку.

3.2 Авторизация пользователей на Ideco ACP

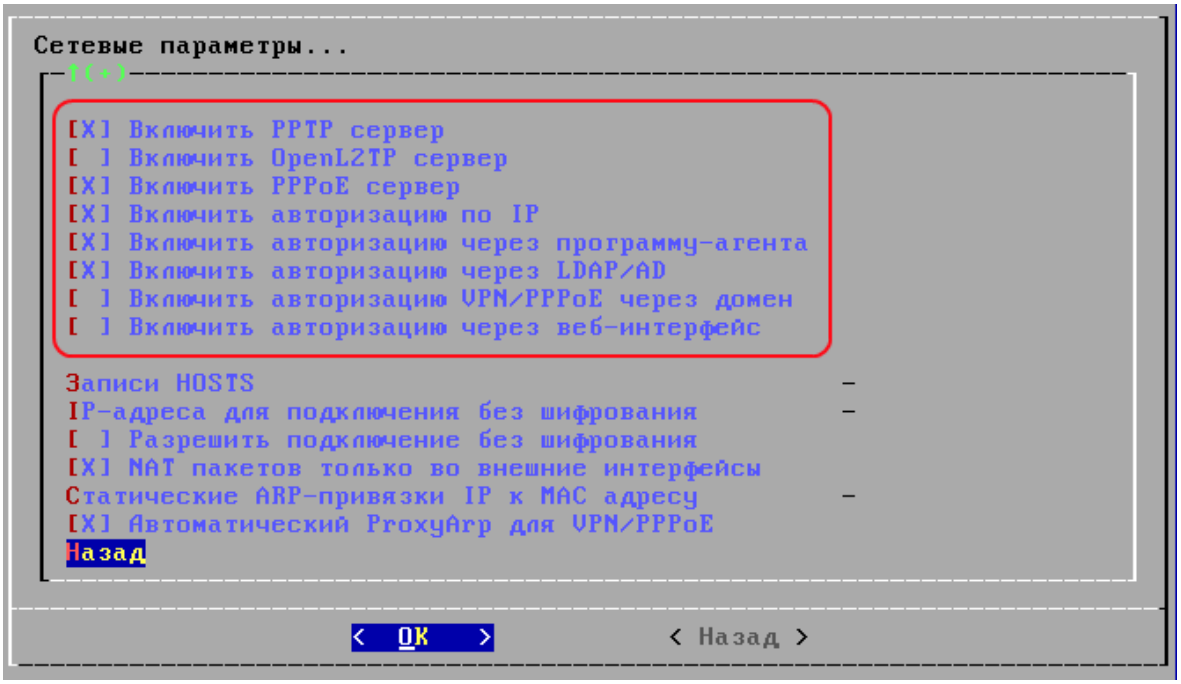
Во всех продуктах компании Ideco доступ в Интернет возможен только авторизованным пользователям.

Авторизация пользователей на Интернет-шлюзе возможна по IP-адресу, через VPN, PPPoE, веб-авторизация и авторизация через программу IdecoAgent.

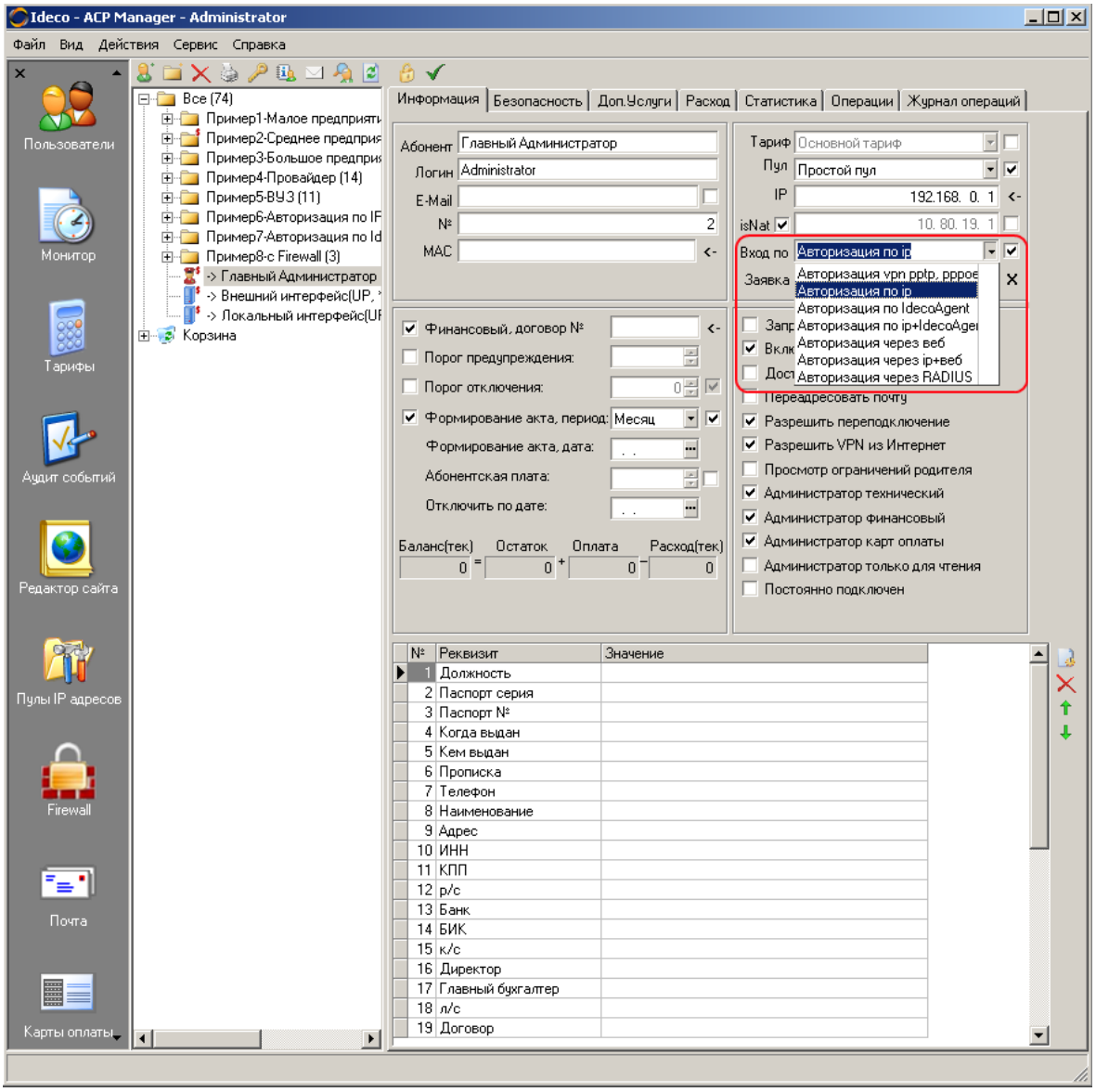
Один пользователь соответствует одному логину. Под одним логином выход в интернет нескольких пользователей (компьютеров) невозможен.

Для того чтобы включить тот или иной тип авторизации на сервере необходимо поставить соответствующий крестик в локальном меню:

Меню -> Конфигурирование сервера -> Конфигурирование сети ->



Для того чтобы применить тип авторизации пользователю необходимо выбрать его в ACP Manager:



Рекомендуется создать группу и устанавливать тип авторизации для всей группы, пользователи автоматически унаследуют выбранный тип.

В этой группе нужно создать пользователя, установить лимит, например "-100", или снять ограничение.

Проверить пользователя: правой кнопкой мыши щелкнуть по пользователю выбрать «Проверить».

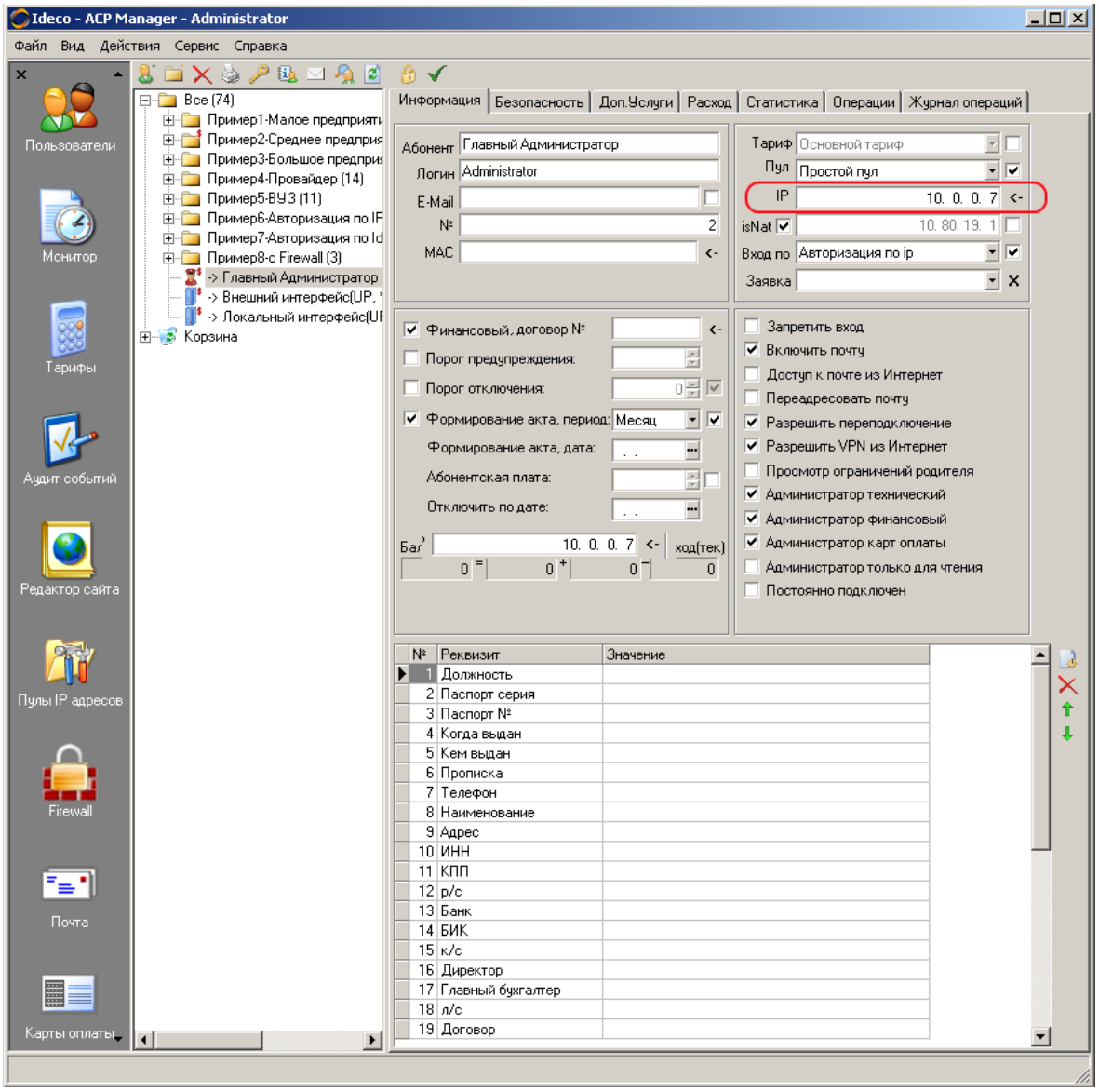
После авторизации пользователь должен появиться в разделе "Монитор 231".

На ПК пользователя рекомендуется убрать все настройки прокси в браузере.

При типах авторизации использующих наличие трафика как основание для авторизации (IP, IP+MAC) при автоматическом обновлении ОС (Windows) или прикладных программ будет производится автоматическая авторизация и использование интернета даже тогда, когда пользователя нет за компьютером. Типичные примеры: обновления Windows, антивирусов.

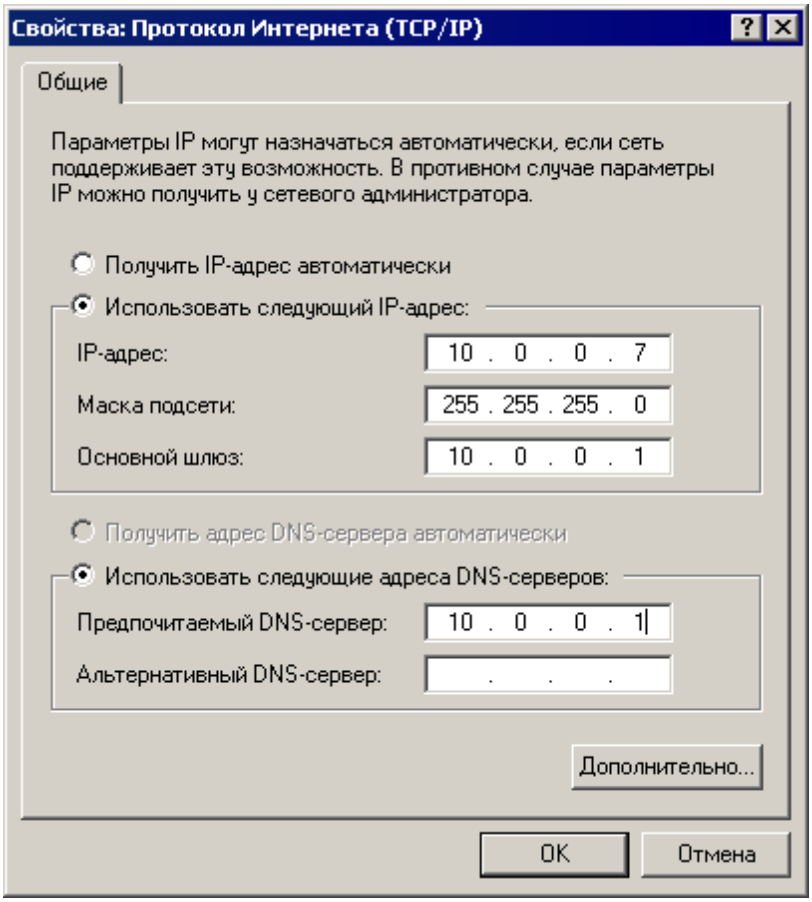
3.2.1 Авторизация по IP

Укажите в свойствах абонента в ACP Manager IP-адрес его компьютера.



Стрелочка справа от поля IP выделяет свободный IP из пула адресов, назначенных клиенту.

На ПК пользователя пропишите IP-адрес из локальной сети и соответствующую маску. В качестве шлюза по-умолчанию и обоих DNS нужно прописать IP-адрес, который прописан на локальной сетевой карте Ideco ACP, например:



Если необходима MAC привязка – укажите MAC-адрес в свойствах пользователя там же в ACP Manager или нажмите кнопку "получить". Если нужно закрепить IP-адрес пользователя в DHCP – тоже сделайте привязку MAC-адреса.

Примечание: Если используется тип лицензии "Concurrent", то при использовании другого типа авторизации совместно с IP (разные машины в сети авторизуются разными из этих методов) необходимо выставить в локальной консоли определение ping доступности для авторизации по IP.

3.2.2 Авторизация по VPN (PPTP)

Настройку VPN-соединения можно выполнить "вручную" или "автоматически":

1. Для автоматической настройки нужно скачать файл с первой страницы ACPа пользователя, адрес по умолчанию "http://10.0.0.1" и запустить этот файл на компьютере пользователя.

При этом будет автоматически настроено VPN-соединение, где в качестве VPN-сервера будет указан **локальный адрес** Ideco ACP. Подробнее об автоматической настойке см. раздел Автоматическая настройка VPN-соединения в Windows 66.

2. Для ручной настройки нужно выполнить обычную настройку VPN-соединения в MS Windows. При этом в Windows 2000 и старше достаточно оставить все параметры по умолчанию. Подробнее о настройке VPN-соединения в различных версиях Windows см. разделы:

- Автоматическая настройка VPN-соединения в Windows 66
- Настройка VPN-соединения в Windows 2000/XP/2003 66
- Настройка VPN-соединения в Windows 95/98/ME 67
- Настройка VPN-соединения в Mac OS X 68
- Настройка VPN-соединения в Linux 68

3. Для серверов под управлением Windows 2000 и 2003 рекомендуется настроить VPN-подключение через службу "Маршрутизация и удаленный доступ".

Замечания:

Следует отметить, что автоматического отключения пользователей по достижении лимита при выбранном типе авторизации "VPN (PPTP)" производиться не будет.

Одновременная авторизация под одним логином с разных адресов невозможна.

3.2.2.1 Автоматическая настройка VPN-соединения в Windows

В Личном кабинете пользователи могут скачать файл, с помощью которого выполняется автоматическая настройка VPN-соединения для работы с сервером Ideco ACP. Этот файл представляет собой профиль Microsoft Connection Manager.

При изменении с локальной консоли Ideco ACP внутреннего адреса сервера, этот адрес (IP-адрес или доменное имя) будет автоматически изменен и установочный файл будет сгенерирован снова. Таким образом, установочный файл при изменении адреса сервера автоматически изменяется, и соединение всегда настраивается на внутренний адрес сервера.

Использование автоматической настройки позволяет быстро настраивать соединения у пользователей администраторам. А также удобно для настройки соединения самими пользователям: им не нужно запоминать IP-адреса или доменные имена, а также выполнять настройку VPN-соединения с помощью стандартного мастера.

Также, если соединение уже установлено, то при щелчке правой кнопкой мышки по иконке соединения в области задач в выпадающем списке появится ссылка на ACP.

Как уже отмечалось установочный файл представляет собой профиль Microsoft Connection Manager (диспетчер подключений). Диспетчер подключений предоставляет настраиваемый клиент удаленного доступа, который позволяет создавать настраиваемые профили подключения, облегчающие работу пользователей и администраторов. Для создания профилей используется мастер пакета CMAK (Connection Manager Administration Kit — пакет администрирования диспетчера подключений), который входит в поставку серверных ОС Microsoft (Windows 2000/2003). Используя CMAK вы можете создавать собственные файлы настройки соединений. При этом можно задавать свои настройки (адреса для подключения, графические элементы, иконки и другие параметры).

3.2.2.2 Настройка VPN-соединения в Windows 2000/XP/2003

1. Запустите Мастер новых подключений. Для этого в меню Пуск выберите команду Настройка > Сетевые подключения > Мастер новых подключений.
2. В окне Мастер новых подключений нажмите кнопку Далее.
3. Выберите вариант Подключить к сети на рабочем месте и нажмите Далее.
4. Выберите вариант Подключение к виртуальной частной сети и нажмите Далее.
5. Введите название создаваемого соединения, например, "Мой доступ в Интернет", и нажмите Далее.
6. Если появилось окно Публичная сеть, то по желанию можно указать подключение, которое будет автоматически устанавливаться перед создаваемым VPN соединением. Если предварительного подключения не требуется, то выберите Не набирать номер для предварительного подключения и нажмите Далее.
7. Введите IP-адрес или имя VPN-сервера. В нашем случае это адрес на

локальном сетевом интерфейсе сервера Ideco ACP. Адрес можно узнать у вашего системного администратора. Нажмите кнопку Далее.

8. Для удобства можно установить флажок  Добавить ярлык на рабочий стол. Нажмите кнопку Готово. Настройка соединения закончена.

9. Для установки соединения запустите созданное соединение, введите свой логин и пароль и нажмите кнопку Подключение.

* Примечание.

- Для серверов, постоянно подключенных к Internet рекомендуется настроить соединение через службу "маршрутизация и удаленный доступ". Такое соединение наиболее надежно.
- Для подключения по VPN в свойствах соединения не указывайте защищенный адрес сервера (по умолчанию 10.128.0.0). Указывать нужно адрес локального Ethernet интерфейса на сервере Ideco ACP.

3.2.2.3 Настройка VPN-соединения в Windows 95/98/ME

Обновление системы "удаленного доступа"

Пользователи компьютеров, работающих под управлением Windows 98 или Windows 95, для использования подключений VPN должны установить последнюю версию программы Удаленный доступ к сети. Программу Удаленный доступ к сети можно загрузить в качестве обновления Windows с этой страницы или с веб-узла корпорации Майкрософт (http://www.microsoft.com). Для Windows 98 Second Edition нет необходимости устанавливать пакет обновлений, кроме случая, когда не удается установить VPN-соединение.

Важно! Перед загрузкой или установкой обновления проверьте версию операционной системы Windows, установленную на компьютере. Для этого щелкните правой кнопкой мыши значок Мой компьютер и выберите Свойства. После установки обновления выполните требуемую перезагрузку.

Установка VPN-адаптера

Зайдите в Панель управления, запустите Установка и удаление программ, выберите вкладку Установка Windows, выберите пункт Связь, нажмите кнопку Состав. Пометьте галочкой следующие компоненты: Виртуальная частная сеть и Удаленный доступ к сети. Нажмите кнопку ОК. Может потребоваться диск с дистрибутивом Windows. После установки выбранных компонентов, выполните требуемую перезагрузку компьютера.

Настройка соединения

1. Откройте окно Мой компьютер. Откройте Удаленный доступ к сети. Выберите Новое соединение.

2. Если мастер запросит ввести код города или телефонный номер, введите любую цифру в каждое поле и нажмите кнопку Далее. Введите название создаваемого соединения, например, "Мой доступ в Интернет". В качестве модема выберите Microsoft VPN Adapter и нажмите на кнопку Далее.

3. Введите IP-адрес или имя VPN-сервера. В нашем случае это адрес на

локальном сетевом интерфейсе сервера Ideco ACP. Адрес можно узнать у вашего системного администратора. Нажмите кнопку Далее.

4. Нажмите кнопку Готово.

5. Войдите в папку Удаленный доступ. Щелкните правой кнопкой мыши по созданному соединению. Выберите в меню пункт Свойства. В появившемся окне выберите вкладку Тип сервера. На вкладке Тип сервера нужно убрать галочки напротив пунктов Войти в сеть, NetBEUI, IPX/SPX-совместимый; установить галочки напротив пунктов: Требуется зашифрованный пароль, Требуется шифрование данных.

6. Установка соединения. Для установки соединения запустите созданное соединение, введите свой логин и пароль и нажмите кнопку Подключиться.

3.2.2.4 Настройка VPN-соединения в Mac OS X

1. Откройте папку Applications на загрузочном диске с Mac OS X.
2. Запустите файл Internet Connect.
3. В меню File выбрать пункт New VPN Connection.
4. В появившемся диалоговом окне выберите пункт PPTP. Нажмите кнопку Continue.
5. Задайте параметры VPN-соединения:

Server address – введите IP-адрес сервера (по умолчанию "10.0.0.1")

Account Name – введите логин

Password – введите пароль.

6. В поле Configuration выберите пункт Edit Configurations…
7. В появившемся окне введите имя создаваемой конфигурации и нажмите кнопку Save.
8. В появившемся окне будут показаны введенные ранее настройки VPN-соединения. Нажмите кнопку OK. Это окно закроется. Нажмите кнопку Connect на главном окне.

3.2.2.5 Настройка VPN-соединения в Linux

Ubuntu (Debian)

Установите из репозиториев пакет pptp-linux и далее из консоли, **используя sudo**, наберите следующую команду:

sudo pptpsetup --create IDECO --server 10.0.0.1 --username Administrator --password servicemode --start --encrypt

Примечание:

По умолчанию во всех версиях ubuntu соединение должно установиться, если возникают ошибки, проверьте что конфигурационный файл `/etc/ppp/options.pptp` содержит следующие строки:

```
refuse-pap
refuse-eap
refuse-chap
refuse-mschap

nobsdcomp
nodeflate
```

Не забывайте, что инициализация драйвера виртуального устройства для установки туннеля и редактирование конфигурационных файлов в системе производится только с наличием прав администратора системы, то есть с помощью команды **sudo**.

Mandriva 2007, 2007.1, 2008, 2008.1, 2009

Файл: /etc/ppp/options

lock
refuse-eap
refuse-chap
refuse-mschap
nobsdcomp
nodeflate
mppe required,stateless,no40,no56
nodetach
debug

Вызывать так:
pppd pty "pptp 192.168.2.245 --nolaunchpppd" user "test" password "test" defaultroute

3.2.3 Авторизация по PPPoE

Откройте "Мастер новых подключений" в свойствах "Сетевого окружения". Выберите пункт "Подключить к Интернету", затем "Установить подключение вручную". Далее выберите вариант "Через высокоскоростное подключение, запрашивающее имя пользователя и пароль". Введите произвольное имя поставщика услуг. Введите логин и пароль, выданные администратором.

3.2.4 Авторизация через Ideco Agent

Для пользователей, у которых установлен способ авторизации "IdecoAgent" либо "IdecoAgent+IP" авторизация через программу агент позволит получить доступ в Интернет. Доступ будет обеспечен только в то время, когда пользователь авторизован с помощью этой программы.

Для пользователей с другими видами авторизации, эта программа на процесс авторизации не влияет. В этом случае ее можно использовать для просмотра

состояния баланса, для приема сообщений и др.

Для авторизации с помощью программы-агента необходимо с локального веб-сайта загрузить программу авторизации и сохранить ее в произвольный каталог.

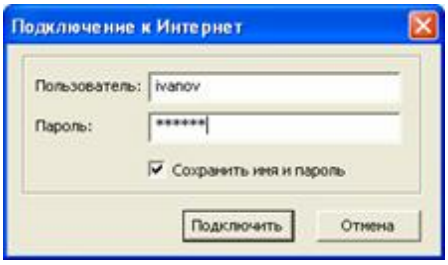
На компьютере пользователя в настройках сетевой карты укажите в качестве шлюза и в качестве DNS локальный адрес Ideco ACP. При необходимости нужно разрешить в межсетевом экране порт 800/TCP.

После запуска программы необходимо ввести логин и пароль пользователя. Состояние авторизации отображается иконкой в системном лотке. Возможные состояния:

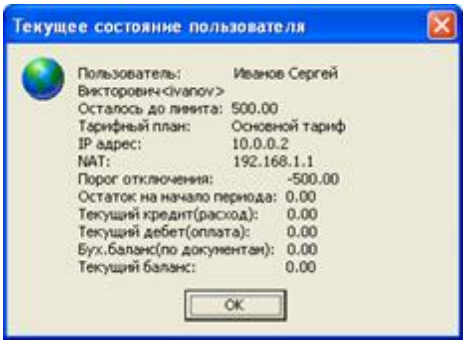
- – Программа не активна
- – Идет подключение к серверу.
- – Доступ в Интернет разрешен.
- – Сработал лимит предупреждения.
- – Сработал лимит отключения.
- – Произошла ошибка. Доступ в Интернет запрещен.

В контекстном меню иконки доступны следующие пункты:

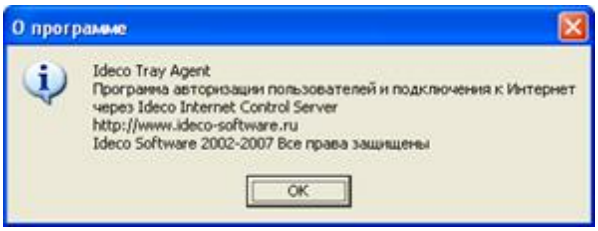
Пункт меню	Значение
Подключить	Отображение диалога подключения



Отключить	Отключиться от сервера
Информация	Отобразить информацию о подключении к Интернет – баланс, порог отключении и т.д.



Запускаться при входе в систему	Установить автоматический запуск программы при входе в Windows.
О программе	Вывод информации о программе авторизации.

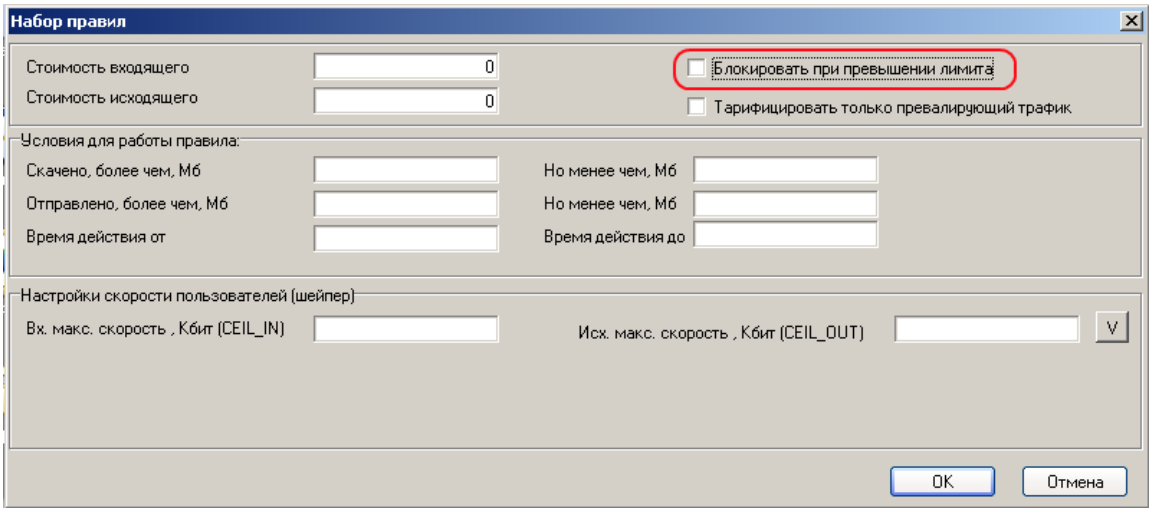


* Примечание. 1) При использовании Ideco Agent в домене AD рекомендуется расположить IdecoAgent.exe на общем сетевом ресурсе и установить в политике входа в домен запуск приложения IdecoAgent.exe с ключом --domain. Таким образом, запуск агента будет централизован и не потребуется его установка на каждый компьютер.

2) При смене локального адреса Ideco ACP обязательно нужно заново скачивать Ideco Agent с сайта, поскольку локальный адрес сервера встраивается в Агент при скачивании.

3) Для использования Ideco Agent при других типах авторизации для просмотра баланса убедитесь что в тарифе, который назначен пользователю, не стоит галочка "запрещать при превышении баланса" на локальной сети:

Тарифы - Тарифные планы - Нужный вам тариф - Локальная Сеть - Блокировать при превышении лимита.



Важно: При использовании VPN соединения Ideco Agent работает, но его функционал ограничен только просмотром статистики и отображением сообщений. Сам Ideco Agent VPN соединение не поднимает.

3.2.5 Авторизация через веб-интерфейс

Если данный тип авторизации включен в локальном меню, то любой запрос неавторизованного пользователя через браузер будет перенаправляться на страницу авторизации. Авторизоваться сможет только тот пользователь у которого данный тип авторизации выбран в ACP Manager.

Для данного типа авторизации **обязательно**, чтобы в качестве шлюза и DNS был прописан локальный адрес Ideco ACP.

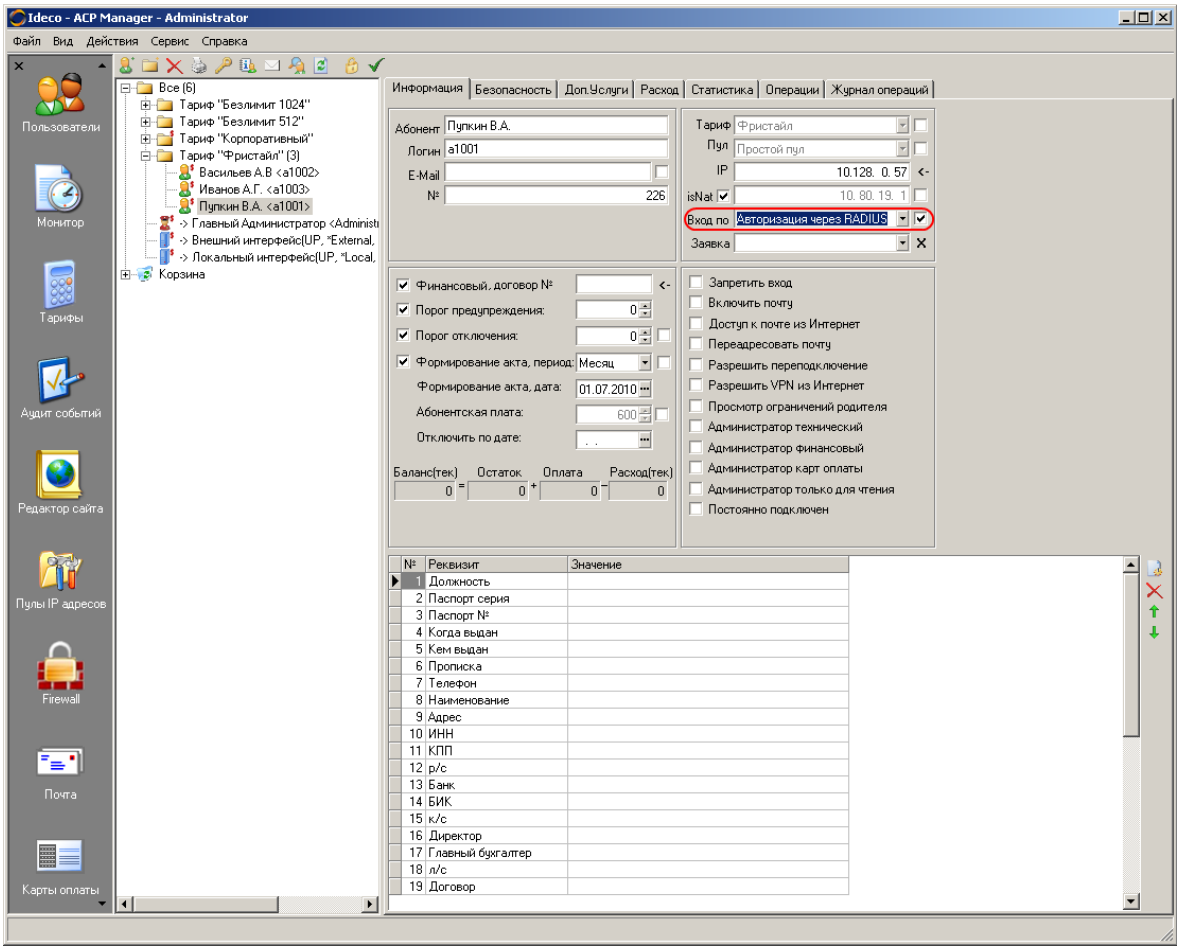
3.2.6 Авторизация через RADIUS

Данный тип авторизации характерен в основном для распределённых сетей (подробнее39), когда пользователи авторизуются на Ideco через NAS сервера или маршрутизаторы.

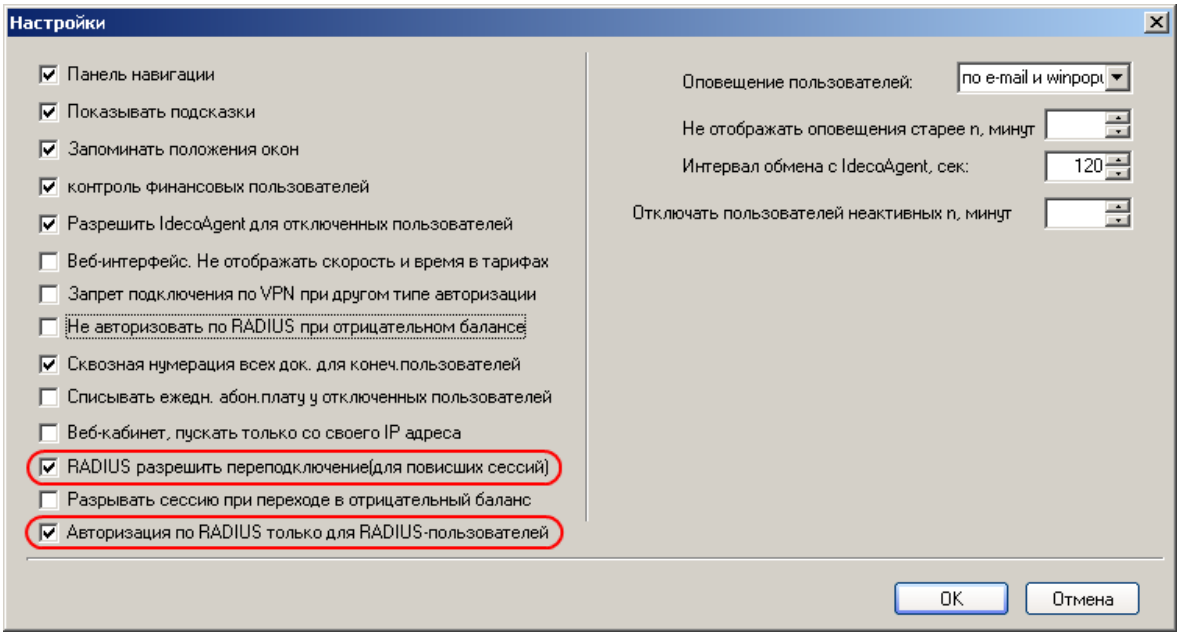
Для его активации необходимо:

1. Включить Radius сервер. Подробнее150 ...
2. Внести NAS-клиентов в список оборудования Ideco ACP. Подробнее148 ...

Как другие типы авторизации RADIUS выбирается в ACP Manager раздел "Пользователи - Информация - Вход по":



Для корректной работы авторизации через RADIUS рекомендуется проставить следующие опции:



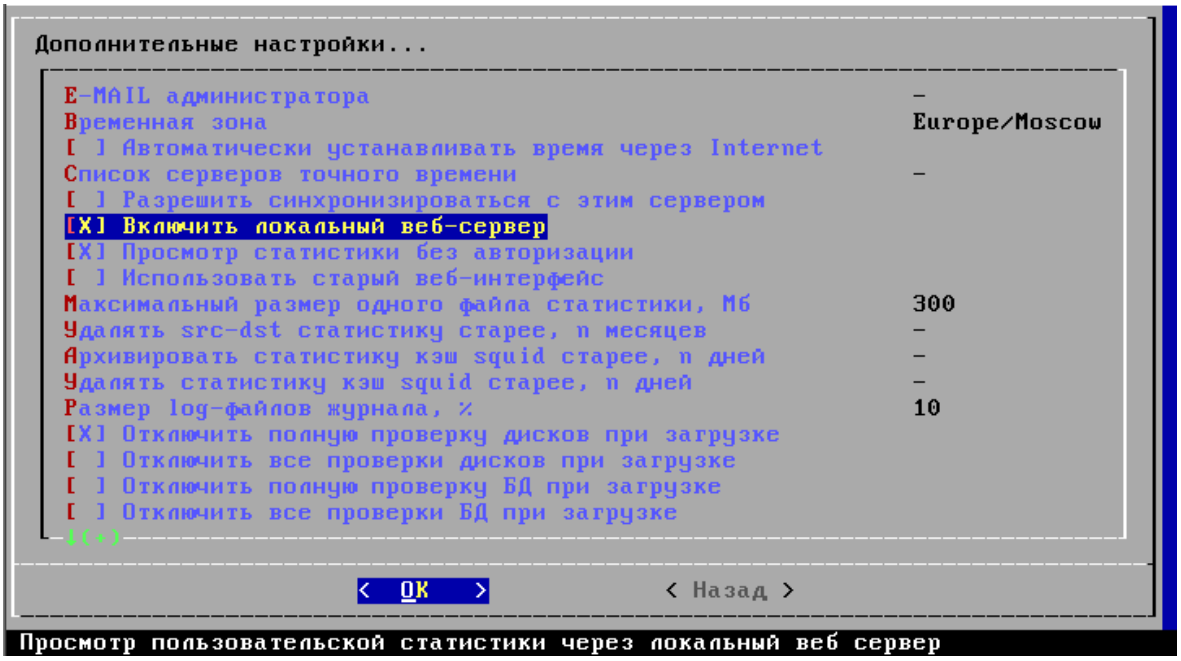
3.3 Службы

В данном разделе описана настройка основных служб, которые необходимы большинству современных провайдеров.

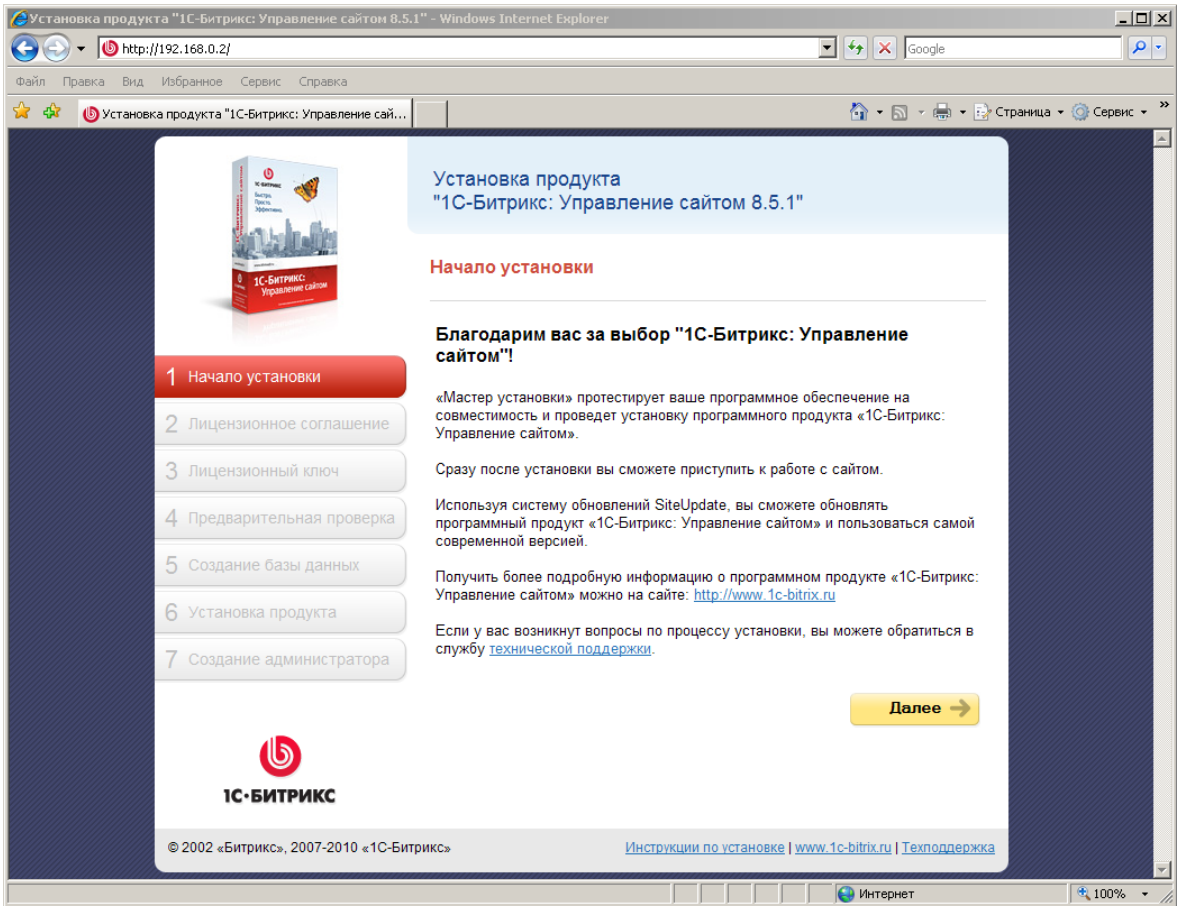
3.3.1 Локальный веб-сервер

В Ideco ACP 3.0 появился новый удобный веб-сайт для провайдера на основе CMS Bitrix, теперь сайт можно редактировать по своему желанию максимально гибко.

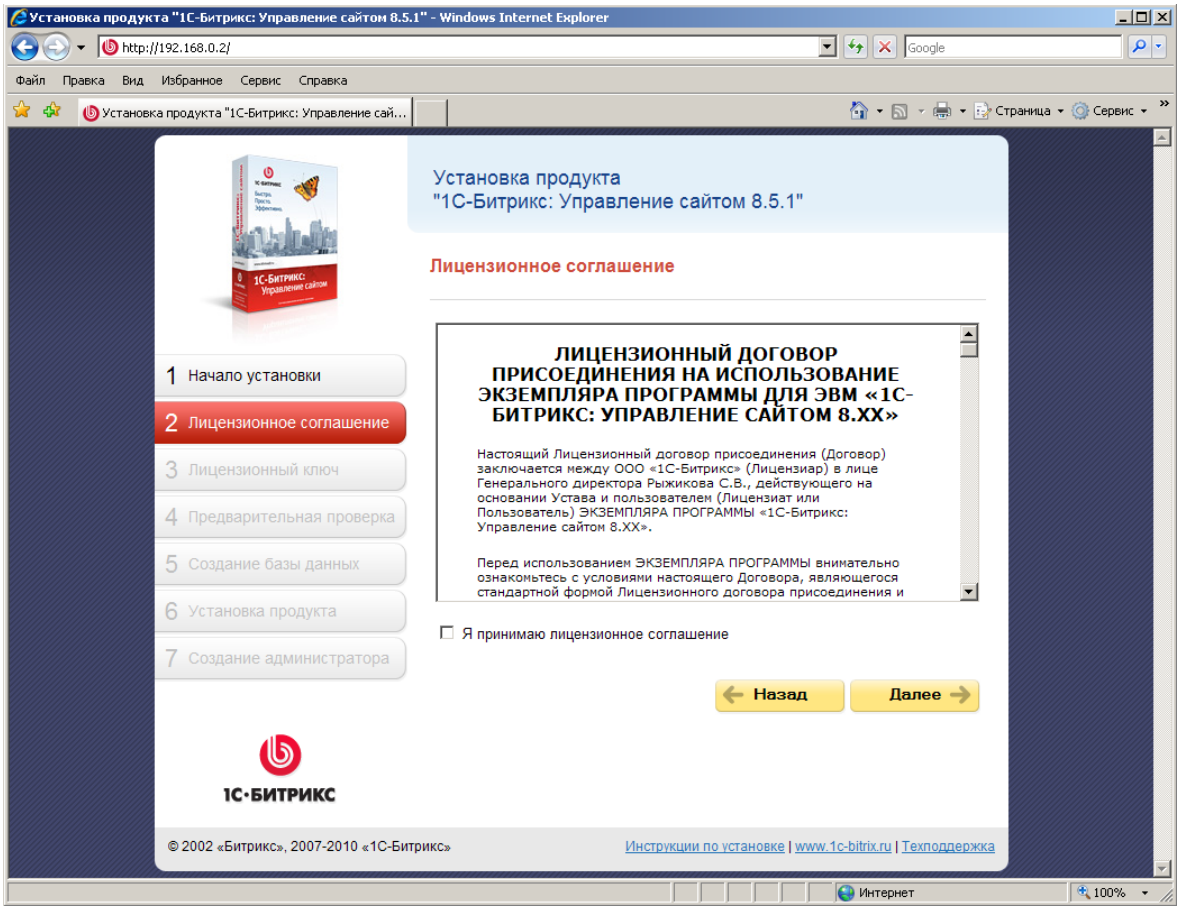
Для того, чтобы его включить необходимо зайти в локальное меню: "Конфигурирование сервера - Дополнительные настройки - Включить локальный веб-сервер" и там же нужно убрать крестик с поля "Использовать старый веб-интерфейс":



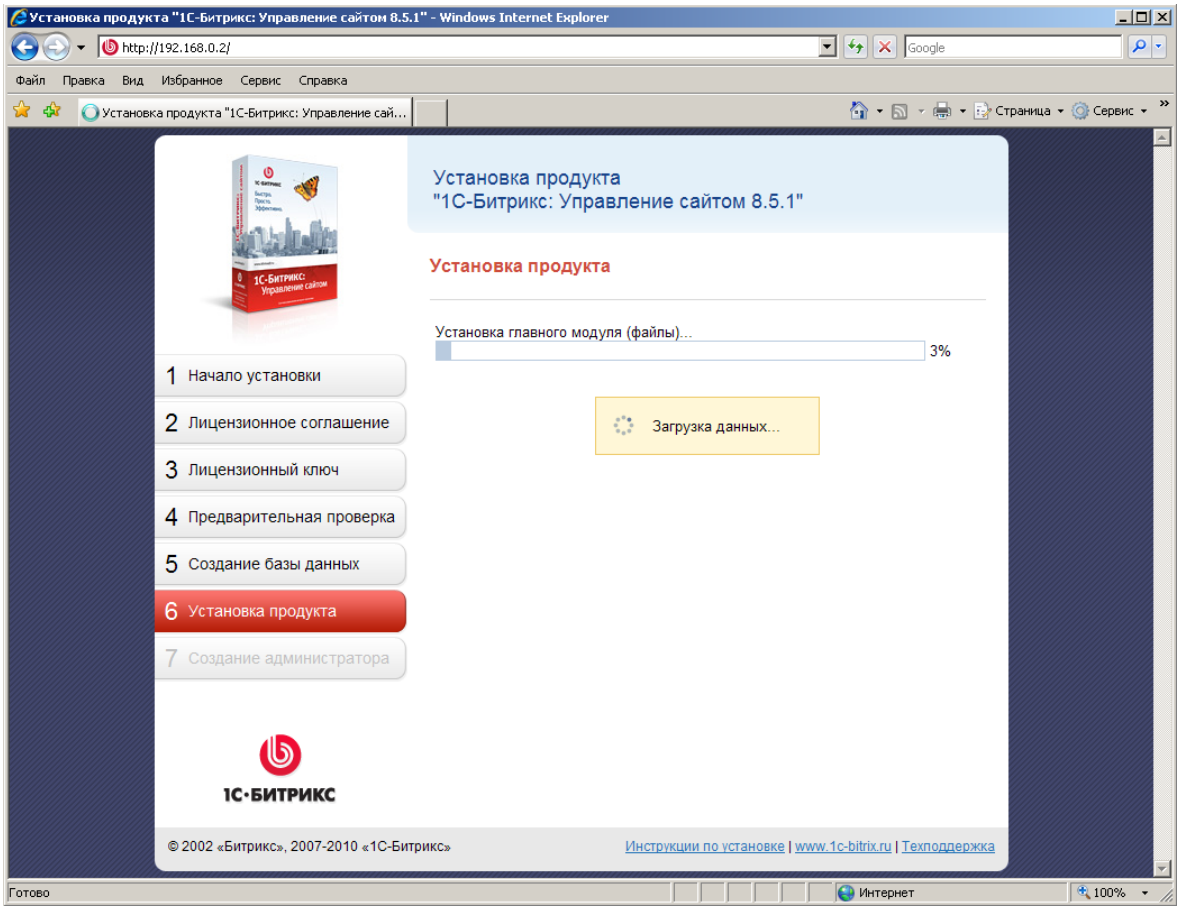
Сервер нужно перезагрузить. После этого открываете на локальном компьютере браузер и в адресной строке набираете локальный адрес Ideco:



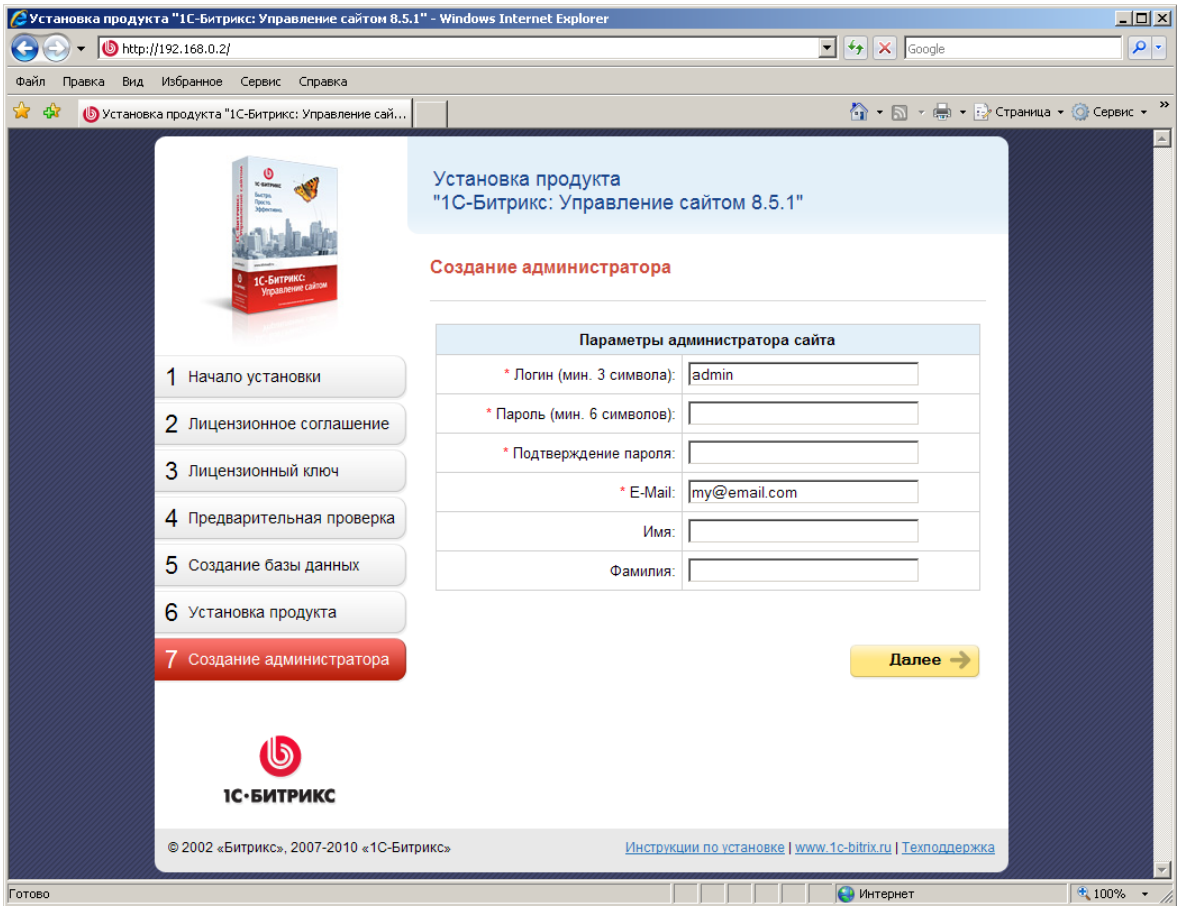
Нажимаете "Далее":



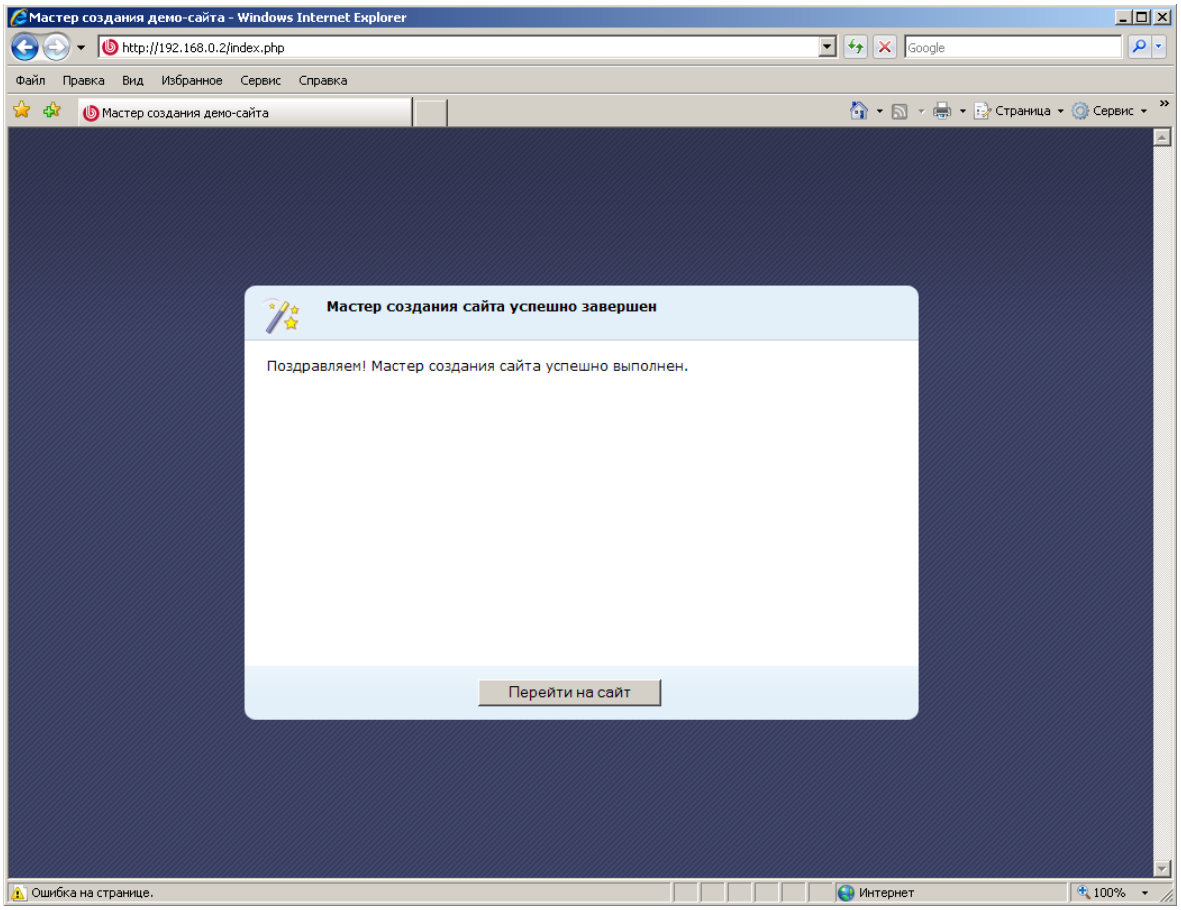
Ставите галочку на пунте "Я принимаю лицензионное соглашение" и нажимаете "Далее":



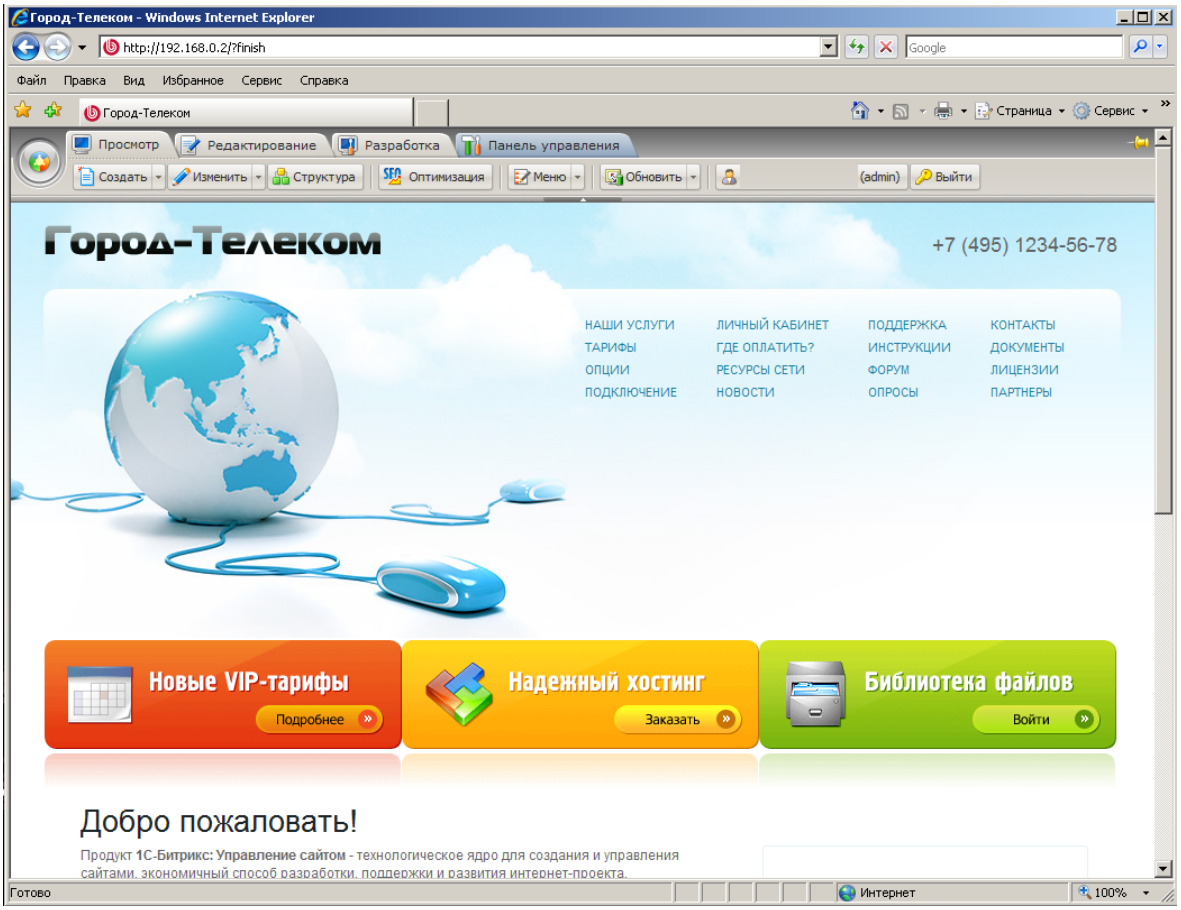
Ждёте пока не закончиться процесс установки:



Заносите данные для аккаунта главного администратора и нажимаете "Далее":

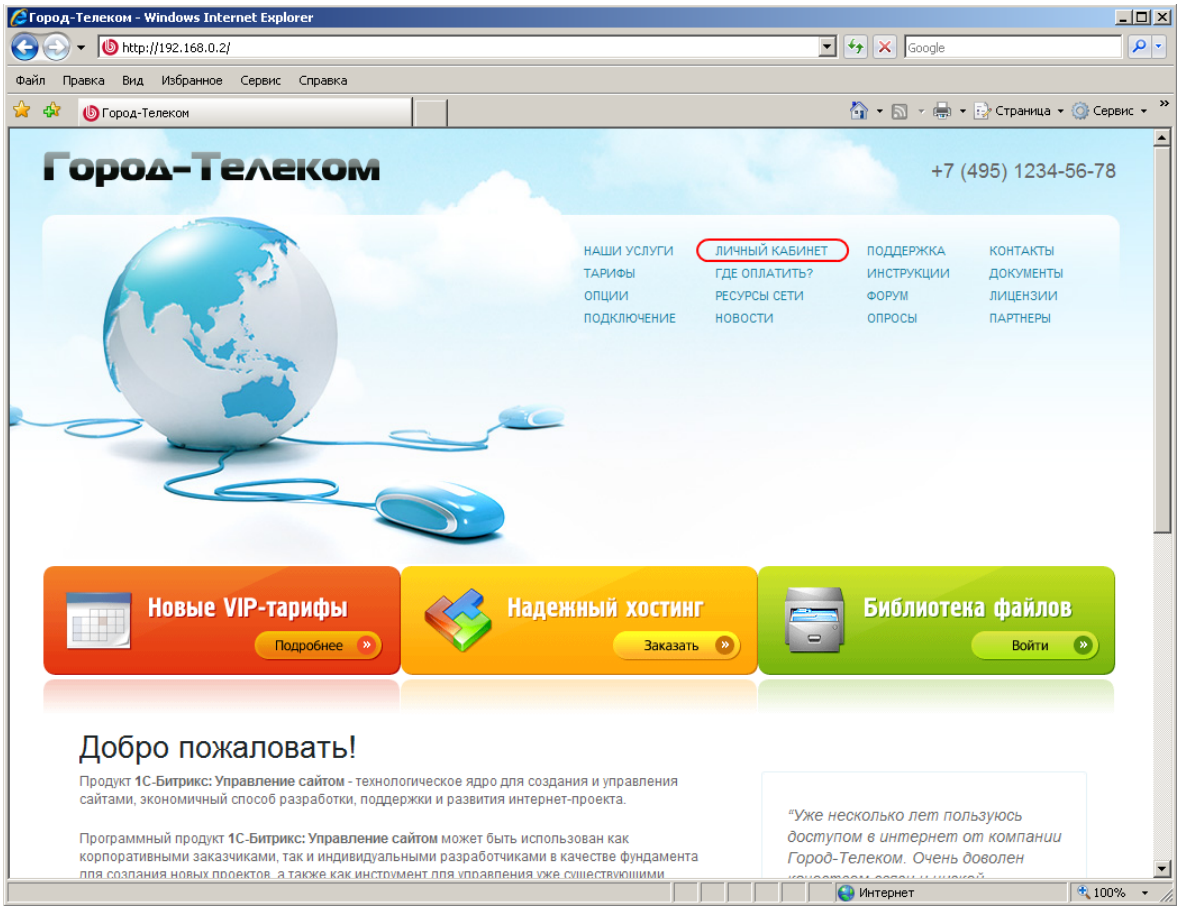


CMS Bitrix установлена, для завершения нажмите "Перейти на сайт":

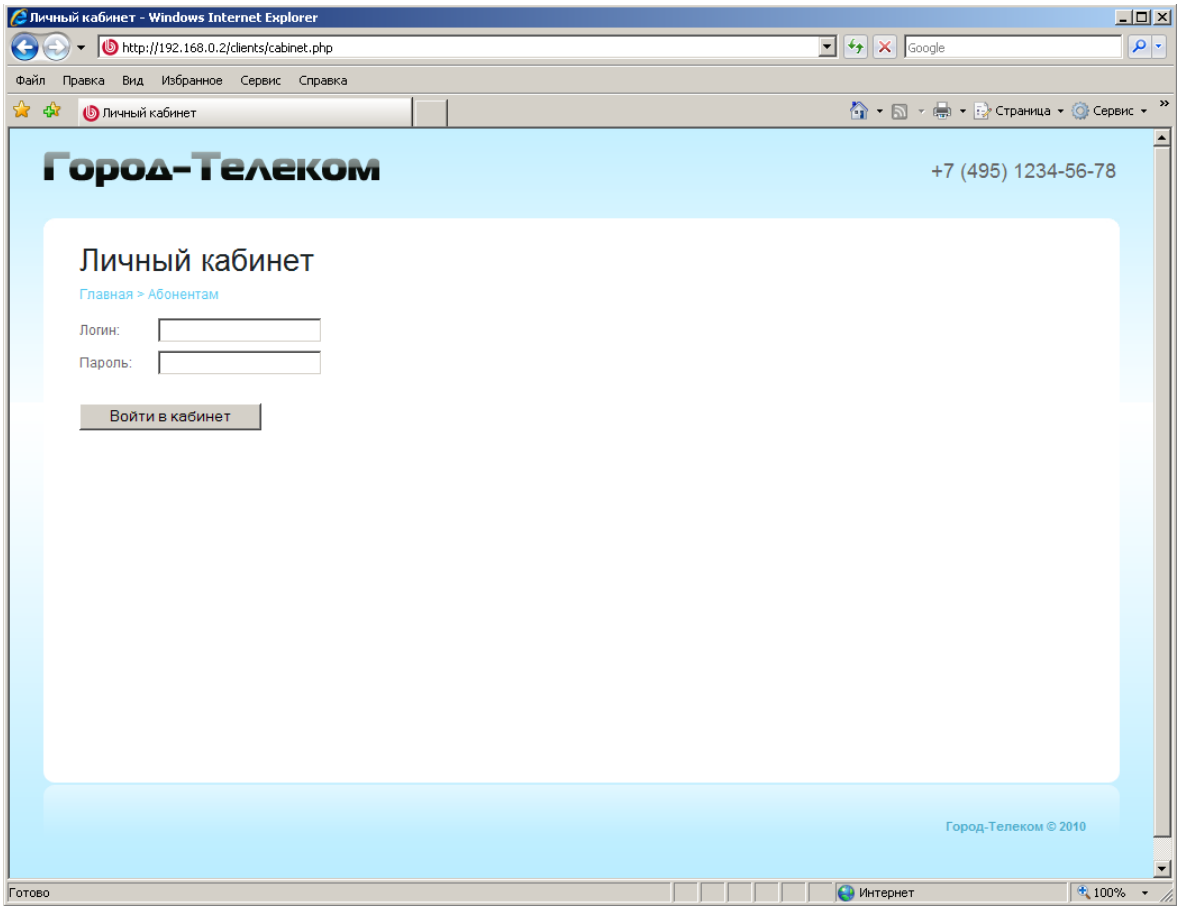


3.3.2 Личный кабинет пользователя

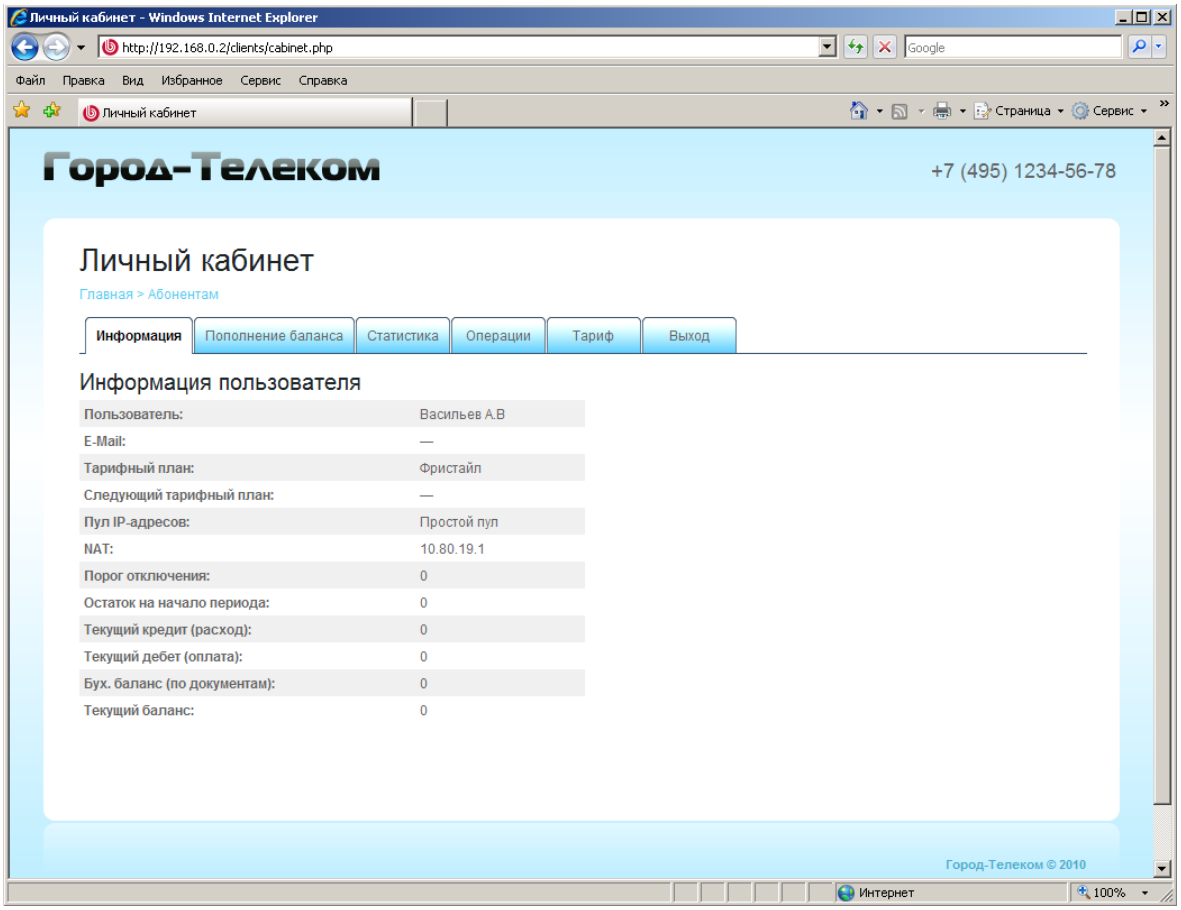
Для доступа в личный кабинет нужно открыть браузер и набрать в адресной строке локальный адрес Ideco, после этого перейти по ссылке "Личный кабинет":



Появиться окно, где будет предложено ввести логин и пароль:



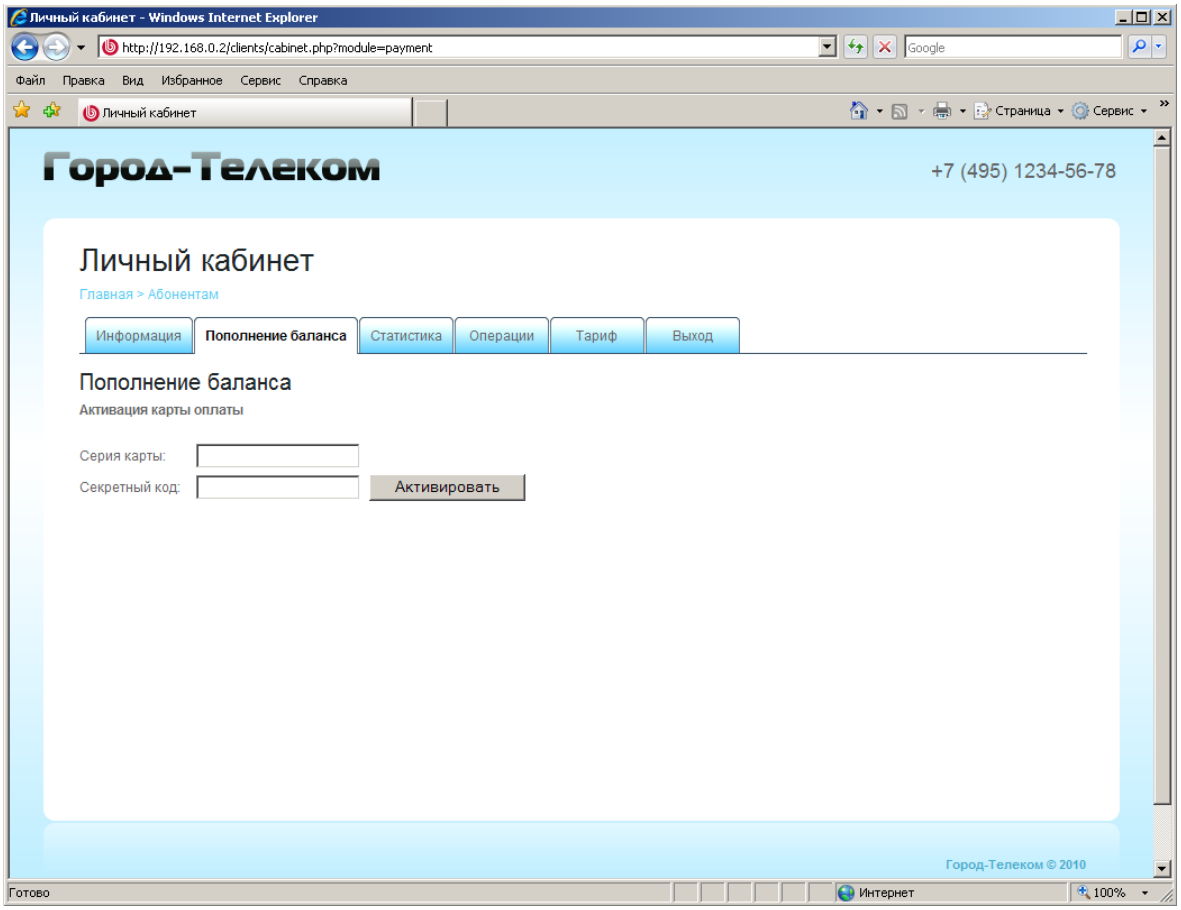
Вводим логин и пароль и попадаем в личный кабинет (у администратор личный кабинет выглядит иначе, его мы рассмотрим позже):



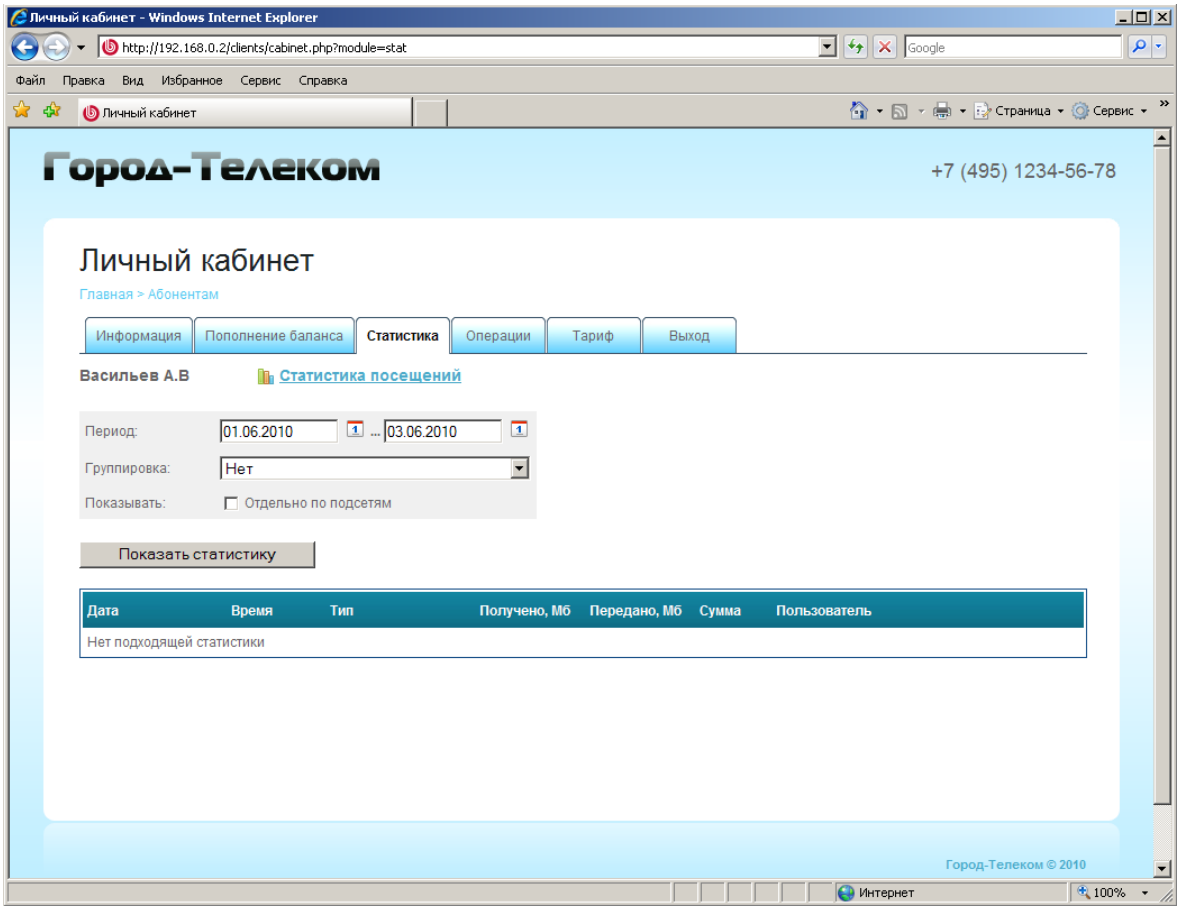
Автоматически попадаем в раздел **Информация**, где можно посмотреть сводные данные по учётной записи пользователя.

Так же в личном кабинете имеются такие разделы как:

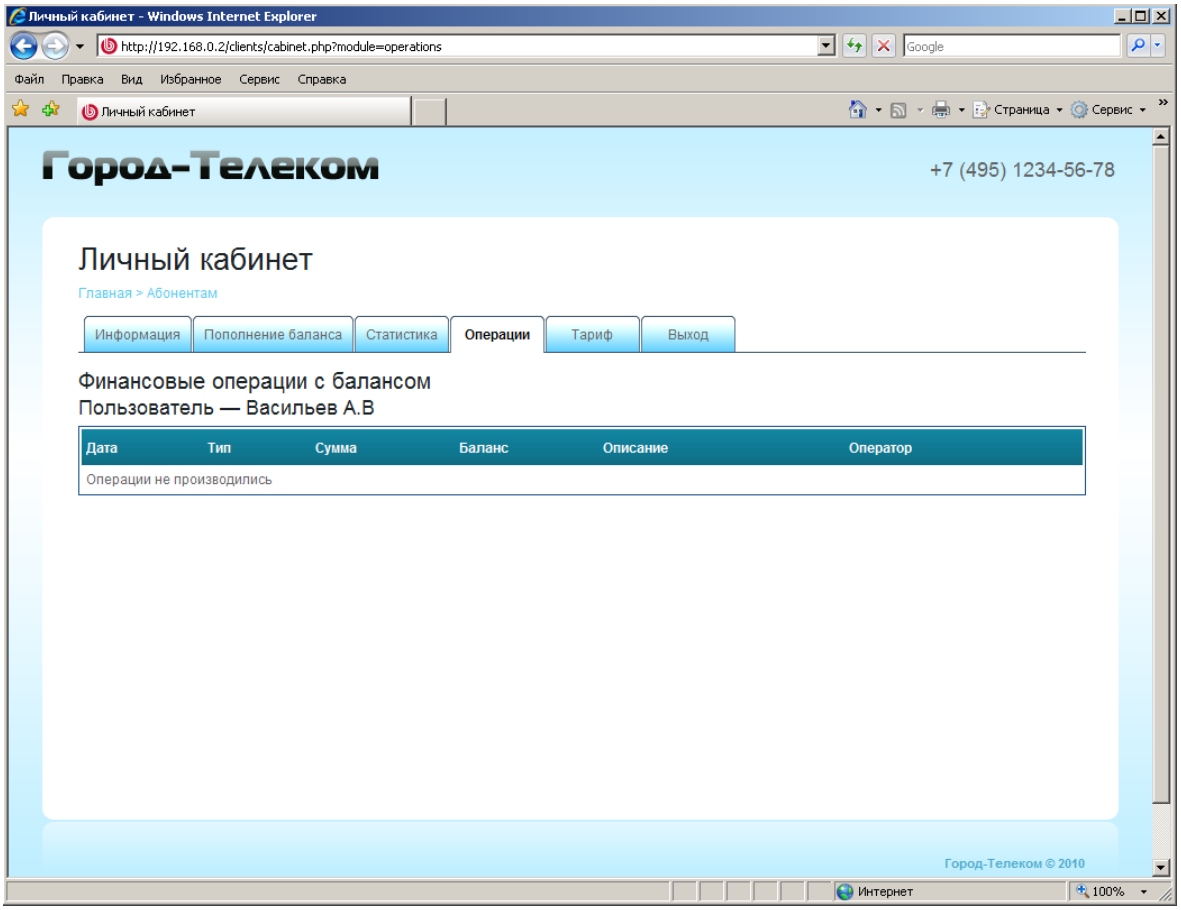
Пополнение баланса, где можно активировать карту оплаты:



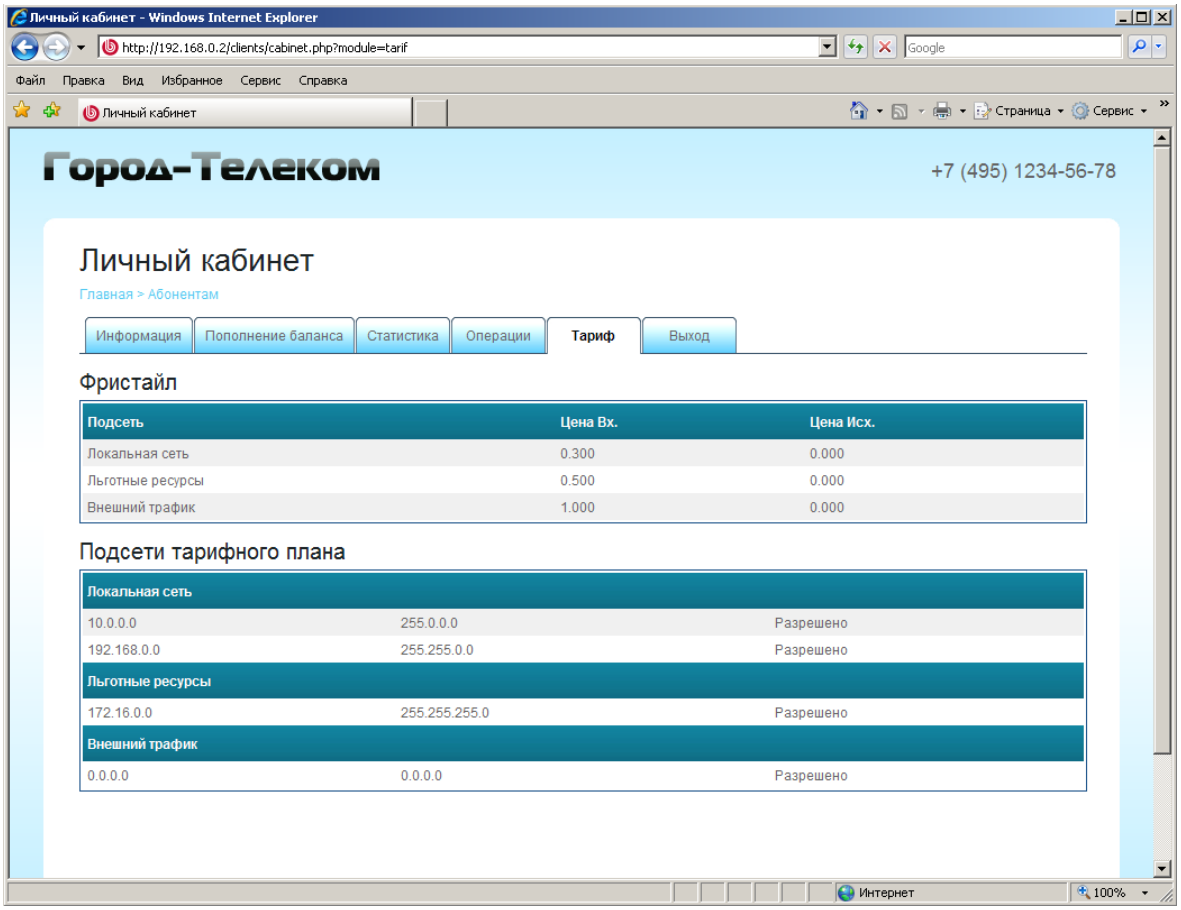
Статистика, где можно посмотреть статистику за произвольный период:



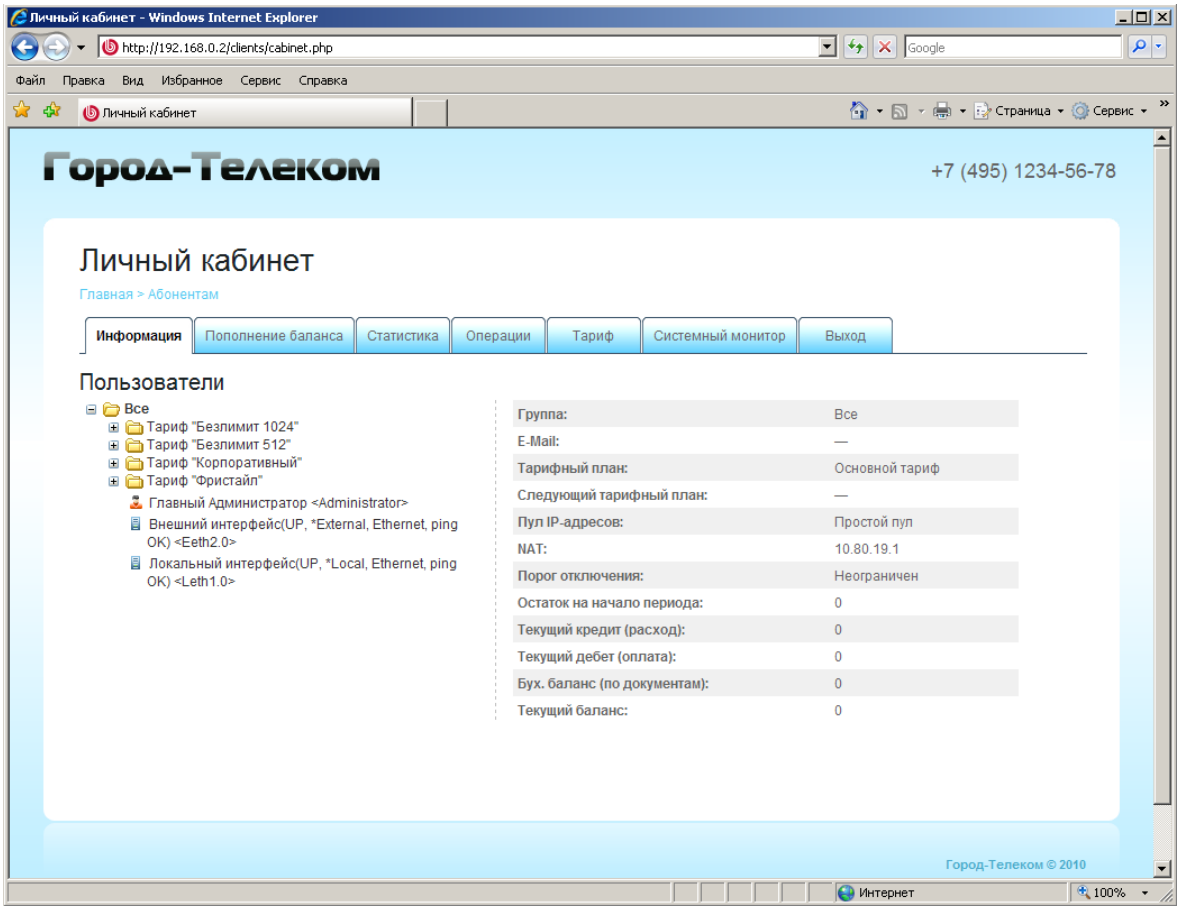
Операции, где отображаются все финасовые операции с балансом пользователя:



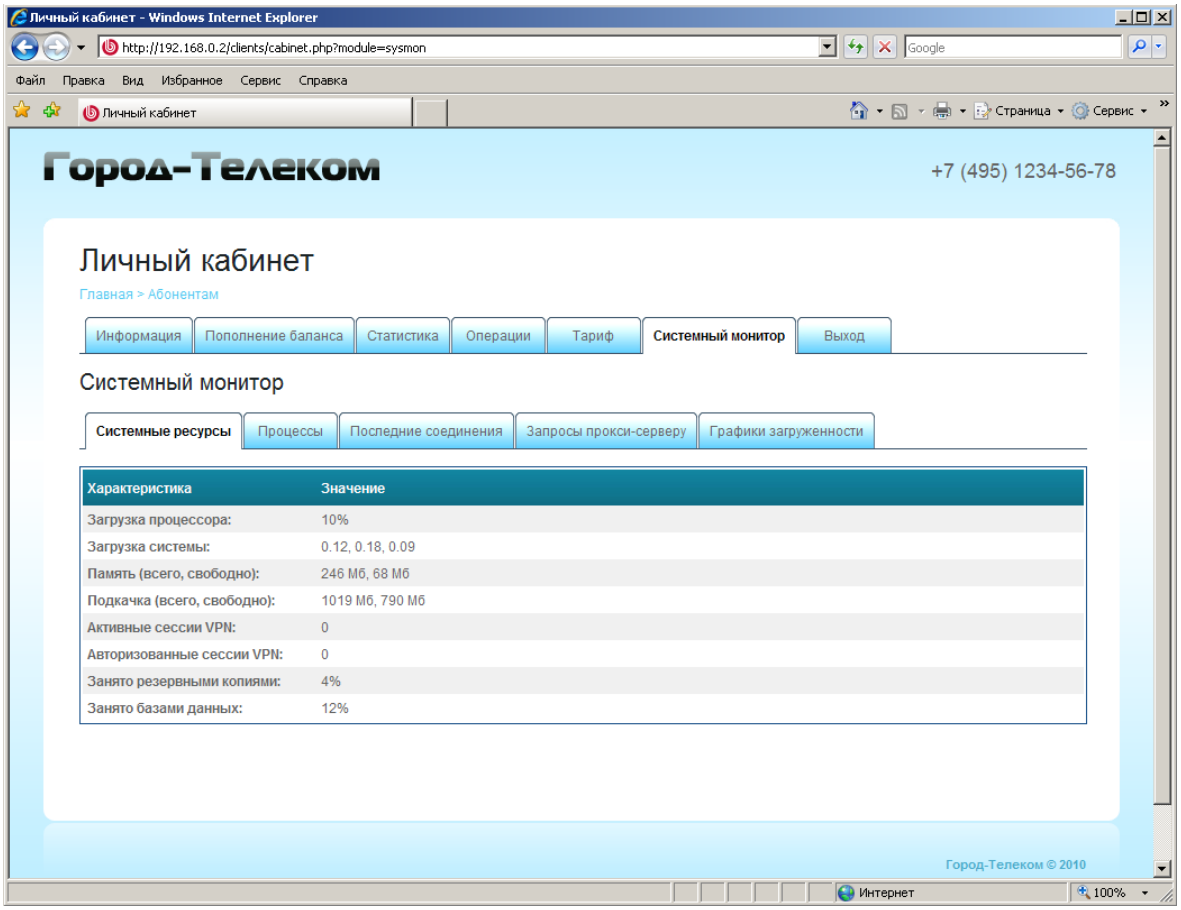
Тариф, где отображаются правила тарифного плана:



У учётной записи главного администратора иначе отображается вкладка **Информация**, так как он может просматривать данные любого пользователя в системе:



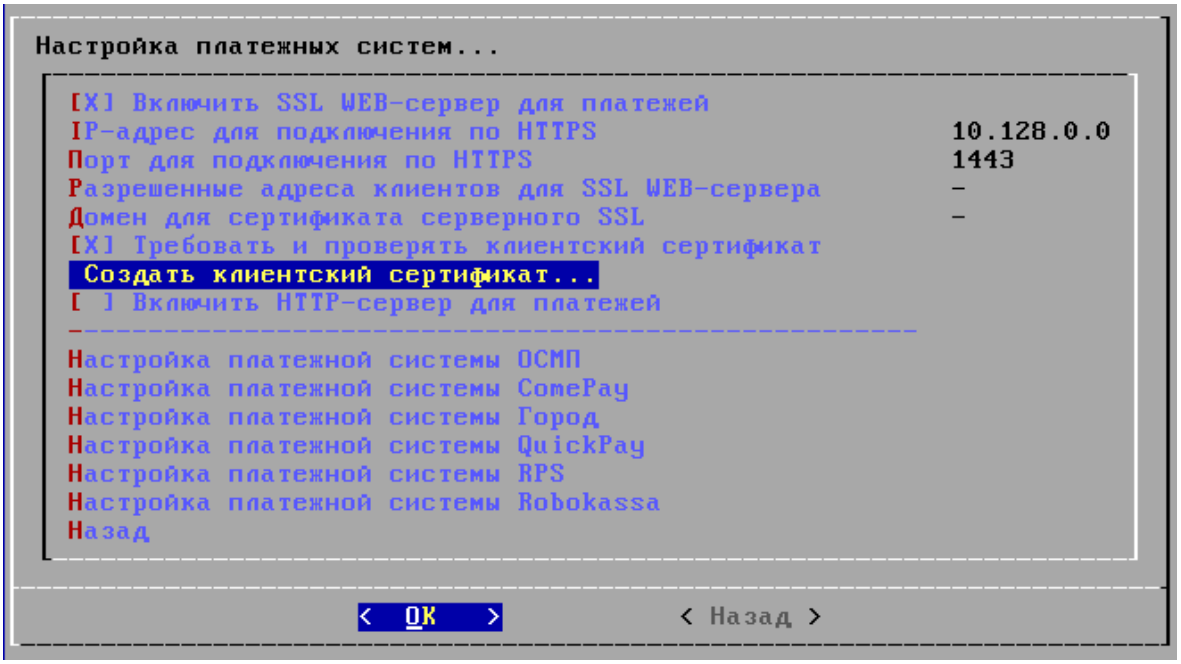
А так же добавлена вкладка **Системный монитор**:



Для выхода из личного кабинета нужно нажать на вкладку **Выход**.

3.3.3 Веб-интерфейс кассира

Веб-интерфейс кассира позволяет удаленно зачислять денежные средства на счета клиентов, занесенных в базе абонентов Ideco ACP. Этот сервис не предполагает связи с кассовым аппаратом. которой не предусмотрено в нашем продукте. Только финансовым абонентам можно зачислять деньги на счет с помощью ACPa кассира. Зачисление денег на счета финансовых абонентов можно производить зайдя в интерфейс от имени финансового администратора группы или вышестоящей группы. Для начала задействуем SSL веб-сервер платежей на Ideco ACP, оснастка которого находится в локальном меню "Конфигурирование сервера" -> "Настройка платежных систем".

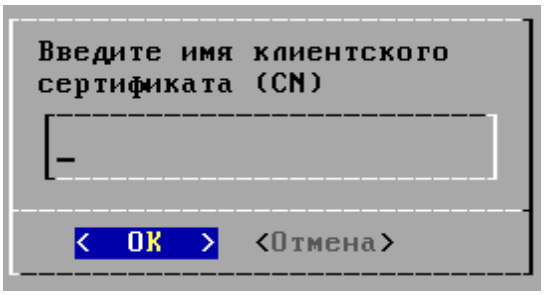


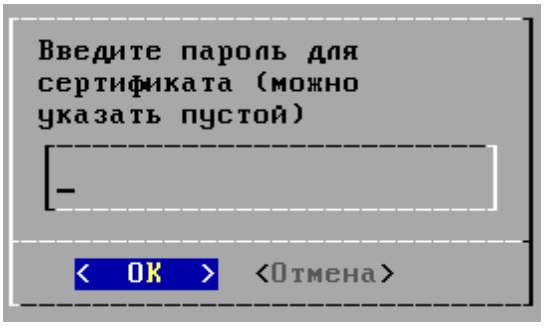
- Включить отдельный SSL веб-сервер для платежей на сервере Ideco ACP.
- IP-адрес по которому будет доступен интерфейс кассира. Лучше указать локальный или защищенный адрес Ideco ACP, но можно и внешний (для доступа к веб кассе извне).
- Обязательно должен быть выбран порт для подключения к вебкассе через браузер, по умолчанию уже выбран нестандартный порт 1443. При смене порта следите чтобы он не был занят другой службой на Ideco ACP.
- Обязательно нужно создать как минимум один клиентсткий сертификат для безопасной работы кассира по сети.
- Нужно обязательно отмечать пункт "Требовать и проверять клиентский сертификат", для того чтобы только компьютеры с сертификатом могли иметь доступ к серверу.

Как видно из скриншота не указаны разрешенные ip-адреса для подключений кассиров в Веб-интерфейсу кассы. Эта опция не обязательна и если она не указана, то можно будет подключиться с любого адреса в лок. сети(не рекомендуется)

Так же не обязательно указывать домен (поддомен) для того чтобы обращаться через браузер по FQDN имени. В таком случае можно попасть в интерфейс веб-кассы набрав в браузере: https://10.128.0.0:1443. Или тот IP который вы укажите в настройках ACP Ideco для интерфейса кассира. Домен может быть реальным (локальным или публичным внешним), вымышленным (будет доступен только из лок. сети).

Создание клиентского сертификата на сервере Ideco ACP уже включает в себя заданные уникальные параметры исходя их установки сервера, необходимо лишь указать уникальное имя для сертификата. Для каждого кассира необходимо создать свой клиентский сертификат и в дальнейшем импортировать его в браузер на клиентском ПК кассира.





CN имя - должно содержать только латинские буквы или цифры.(это произвольное имя для сертификата)

Пароль - можно пустой или только латинскими буквами или цифрами.

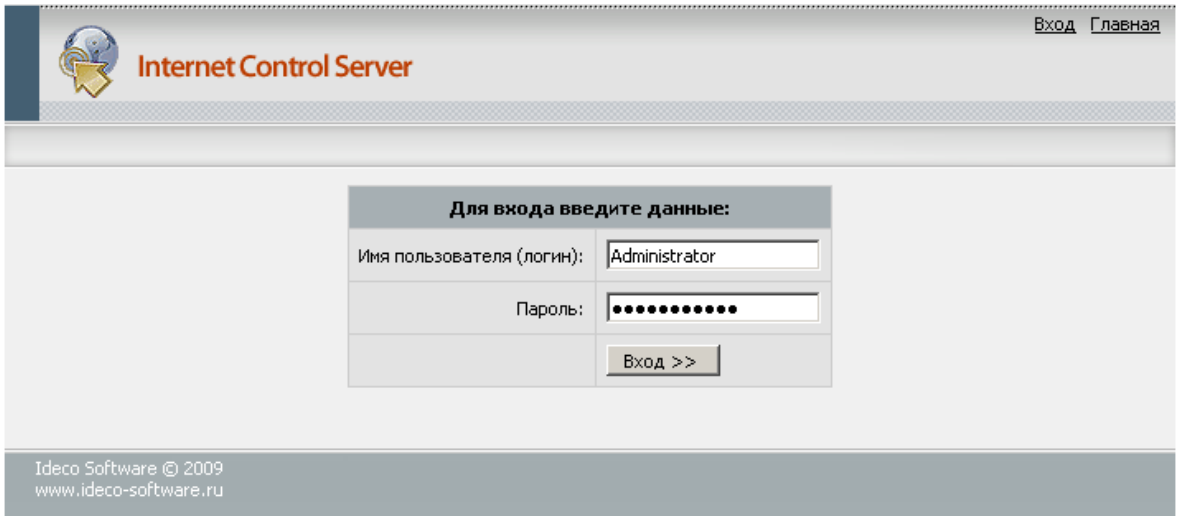
Настройка со стороны сервера завершена, теперь нужно импортировать клиентские сертификаты с сервера с помощью winscp.

- Убедитесь что у вас включен пункт локального меню "Конфигурирование сервера" -> "Безопасность" -> "Разрешить управление файлами по SSH"
- После этого программой winSCP, которую можно взять с установочного диска или бесплатно с сайта производителя, нужно подключиться на локальный или защищенный адрес сервера по порту 22, используя логин sysadm и пароль как в локальной консоли (по умолчанию servicemode).
- В корневом каталоге на сервере вы увидите каталог USRCERT. Из него на машину клиента (кассира) скопируйте его сертификат. Клиентский сертификат имеет имя *.pxf. На каждую клиентскую машину кассира, который будет работать с веб-кассой скопируйте свой сертификат .pxf, отличаться они должны именами файлов, которые совпадают с CN именами, заданными каждому сертификату при его создании.

После этого нужно импортировать сертификат в браузер на машине клиента, подключающегося к АСР кассира. Проверены на работоспособность браузеры IE и Firefox.

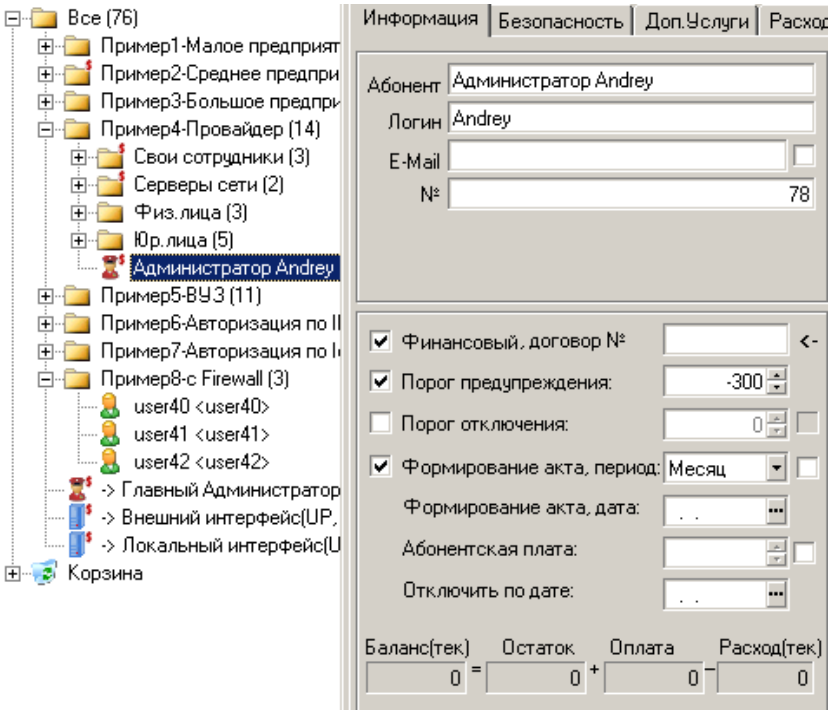
- В среде windows кликните по файлу сертификата правой кнопкой мыши и выберите пункт контекстного меню "установить". Выбор хранилища выберите "Автоматический".
- Если сертификат создавался с паролем то будет спрошен пароль данного сертификата. Укажите его и после этого сертификат импортируется в Internet Explorer. В Firefox сертификаты импортируется из "Инструменты" (или "Правка") -> "Настройки" -> "Шифрование" (или "Дополнительные") -> "Просмотр сертификатов" -> "Ваши сертификаты" -> "Импортировать".

После этого кассир со своей машины может обратиться к серверу Ideco АСР по адресу `https://10.128.0.0:1443`. Зайти и работать в Веб-интерфейсе кассира может **только финансовый администратор**.



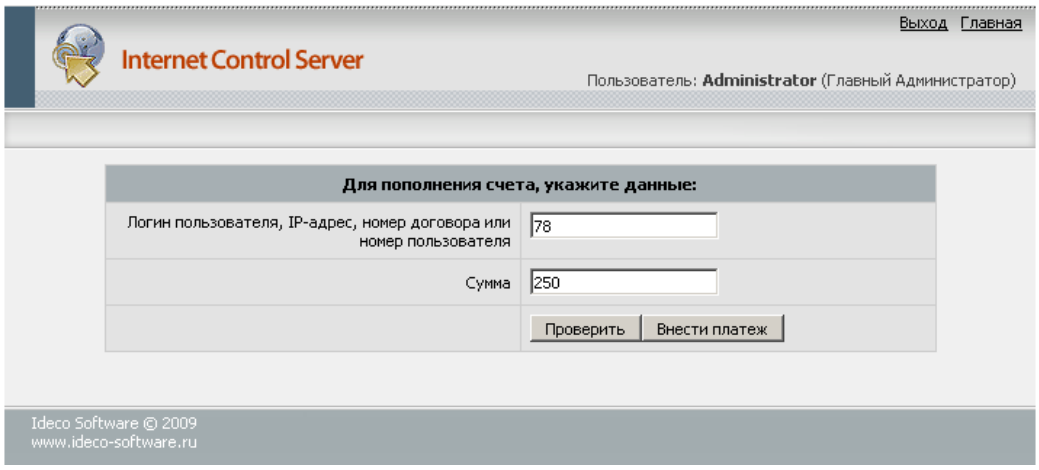
После входа в интерфейс у вас будут только 2 поля, доступные для правки:

Идентификатор абонента и сумма, которую вы хотите положить на счет абоненту. Но перед каждым платежом **необходимо обязательно** проверить возможность проведения операции, поэтому вам так же будут доступны 2 кнопки для проверки и проведения платежа. Итак: абонент, на счет которого вносится платеж должен быть финансовым как на примере ниже абонент с номером 78, (не нужно обращать внимание на, то что он является администратором в группе) :

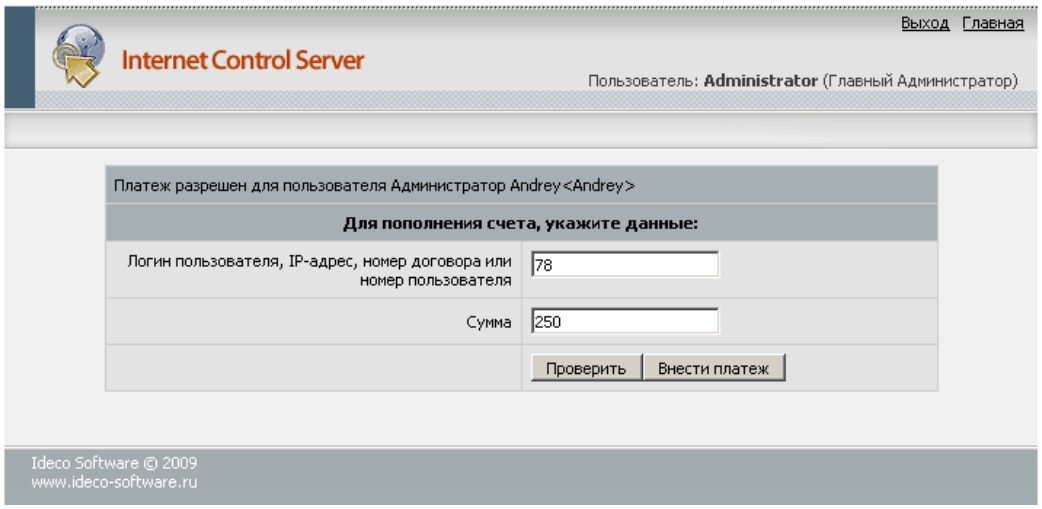


Проведем платеж в размере 250 единиц на имя пользователя "Andrey" заполнив два поля:

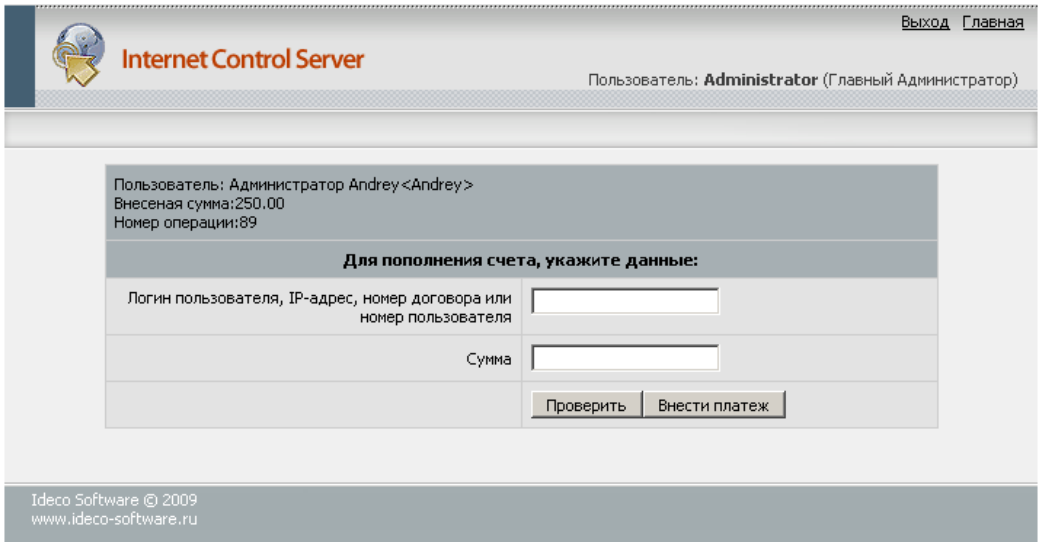
Идентификатором пользователя может выступать его Логин, ip-адрес, номер договора или ID пользователя. Последний мы и используем в нашем примере. Сумма указывается в единицах и после проведения платежа моментально зачисляется на баланс указанного пользователя.



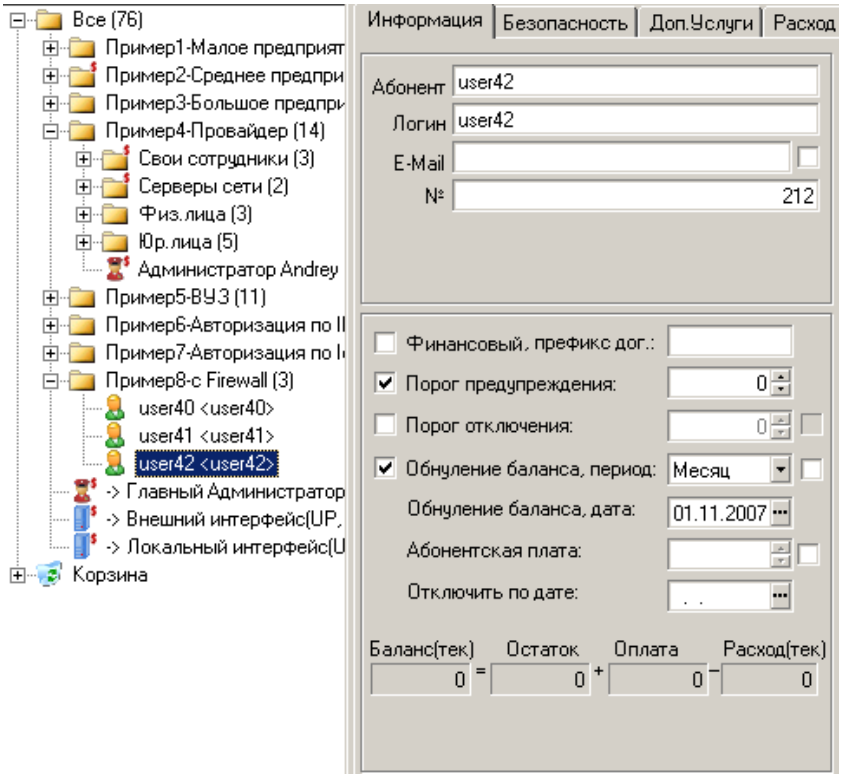
Не забываем что вначале нужно проверить возможность проведения платежа. Платеж разрешен.



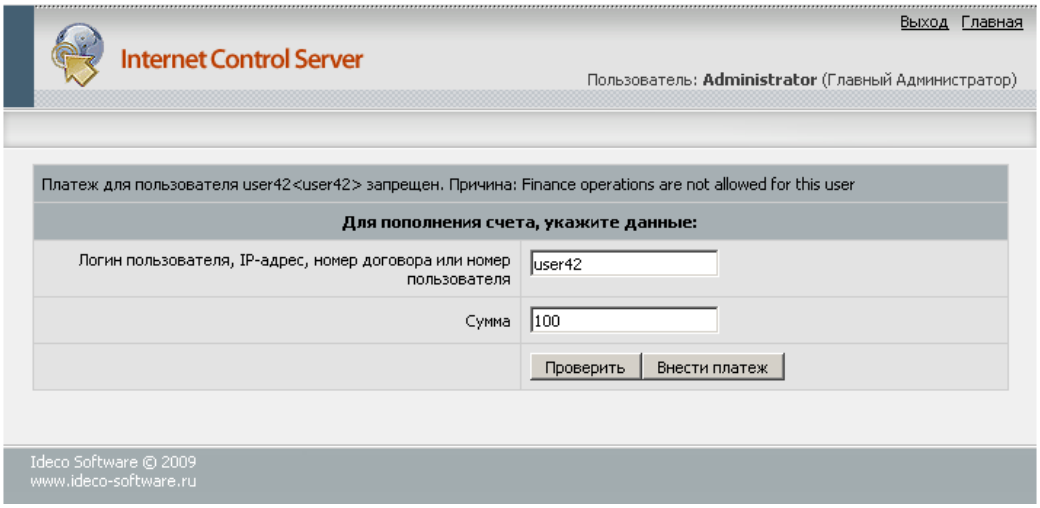
Нажимаем кнопку "Внести платеж" и смотрим состояние пользователя. На баланс были зачислены деньги о чем вам сообщается номером операции и зачисленной суммой.



Имейте ввиду, что если абонент не финансовый, то платеж на его счет не пройдет, что вы можете увидеть ниже на примерах.



Ошибка которую вы увидите при попытке внести средства на счет нефинансового пользователя.



3.3.4 Синхронизация с платёжными системами

Ideco ACP поддерживает синхронизацию с такими платёжными системами как:

- ОСМП
- Город
- RoboKassa
- ComePay
- QuickPay
- RPS
- SFOUR и другие

Практически все они настраиваются однотипно как и ОСМП.

О системе

ОСМП - Это платежная система, позволяющая пользователям самостоятельно пополнять свой счет. Более подробно на сайте osmp.ru

Требования

Для подключения этой системы необходимо:

- Ideco ACP версии 3.0.3 или выше
- Реальный внешний IP-адрес

Для того чтобы пользователь мог внести платеж:

- Пользователь должен быть с признаком Финансовый
- Пользователь не должен быть удален или отключен. То же самое для вышестоящих групп
- При идентификации не должно быть неоднозначностей

Идентификация пользователей при внесении платежа может осуществляться по логину, IP-адресу, номеру пользователя или номеру договора.

Подключение

- На странице www.osmp.ru - Как стать партнером скачать и заполнить анкету
- Отправить заполненную анкету менеджеру, ответственному за ваш регион
- В ответ вы получите пакет документов, которые необходимо заполнить для согласования коммерческих условий использования сервиса
- После согласования коммерческих условий можно приступить к техническому тестированию
- Для тестирования технической части, отправьте письмо на адрес rfp@osmp.ru, указав в копии почтовый адрес курирующего менеджера. В письме укажите:

  - Ваше Юридическое наименование

  - Ваше Коммерческое наименование

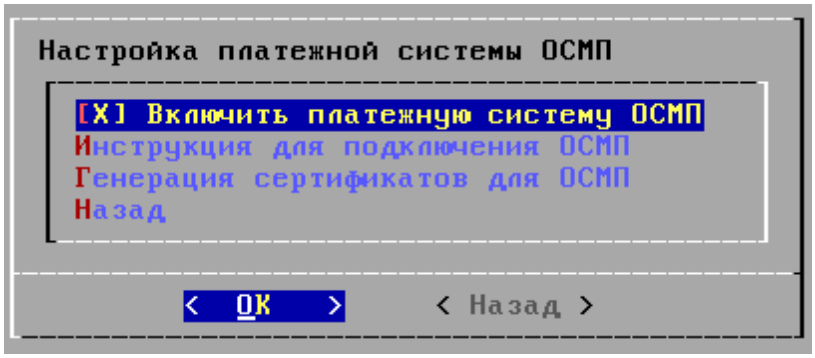
  - Адрес технического специалиста с вашей стороны

  - Адрес технического специалиста с нашей стороны - for-osmp@ideco-software.ru

  - ФИО курирующего менеджера

В ответ будут отправлены инструкции по автоматическому тестированию технической части

- В соответствие с присланной от ОСМП инструкцией, зайдите в интерфейс автоматического тестирования на сайте ОСМП
- Перед тем как указать технические данные, выполните в локальной консоли сервера Ideco ACP действия:



- Включаем пункт в локальном меню: **Конфигурирование сервера -> Настройка платежных систем -> Настройка платежной системы ОСМП -> Включить платежную систему ОСМП.**

- Генерируем сертификаты для ОСМП: **Конфигурирование сервера -> Настройка платежных систем -> Настройка платежной системы ОСМП -> Генерация сертификатов для ОСМП**

- В диалоге нужно указать адрес Вашей электронной почты на которую сервер должен прислать SSL-сертификаты, необходимые для работы с ОСМП. Эти сертификаты потребуются во время проведения тестирования.

- Производим мягкую перезагрузку.

- В интерфейсе автоматического тестирования на сайте ОСМП, В разделе **Справочники -> Провайдеры -> Технические данные** укажите:
  - **URL платежного приложения**:

    https://Ваш внешний IP или доменное имя:1443/osmp.php
  - **Список адресов электронной почты для отправки реестров**:

    Укажите почтовый адрес для отчетов
  - **Регулярное выражение для проверки правильности идентификатора**:

    ^[a-zA-Z0-9._-]+$
  - **Серверный сертификат провайдера в формате X509**:

    Файл приложен в письме. Имя - osmp*_CA.crt
  - **Клиентский сертификат для ОСМП в формате PKCS12**:

    Файл приложен в письме. Имя - osmp*.pfx
  - **Пароль для клиентского сертификата**:

    Указан в письме
  - **Использовать бэйсик-авторизацию**:

    Снимите галочку
  - **Логин и пароль, если требуется авторизация (Basic)**:

    Не указывайте
- Проведите тестирование
- После успешного тестирования свяжитесь с курирующим менеджером, сообщите, что тестирование проведено успешно, и вы готовы к эксплуатации системы
- Возможно, потребуется генерация новых ключей. Для этого, повторно выберите пункт меню **Конфигурирование сервера -> Дополнительные настройки -> Дополнительные службы -> SSL WEB-сервер для платежей -> Генерация сертификатов для ОСМП** в локальной консоли.

3.3.5 Шейпер

Новая модель тарифов и шейперов основана на технологии HTB - **Hierarchy Token Bucket**. Данная технология позволяет строить иерархические структуры из шейперов, что позволяет создавать группы тарифов. Базовый вид правил HTB выглядит следующим образом:

```
[root@vpn-mydomain-ru root]# tc class show dev imq0
class htb 1:1 root rate 90000Kbit ceil 90000Kbit burst 116778b cburst 116778b
class htb 1:10 parent 1:900 rate 10000Kbit ceil 80000Kbit burst 14398b cburst 103987b
```

```
class htb 1:20 parent 1:900 rate 80000Kbit ceil 80000Kbit burst 103987b cburst 103987b
class htb 1:110 parent 1:10 leaf 111: prio 0 rate 1666Kbit ceil 80000Kbit burst 3731b cburst 103987b
class htb 1:120 parent 1:10 leaf 121: prio 1 rate 1666Kbit ceil 80000Kbit burst 3731b cburst 103987b
class htb 1:130 parent 1:10 leaf 131: prio 2 rate 1666Kbit ceil 80000Kbit burst 3731b cburst 103987b
class htb 1:140 parent 1:10 leaf 141: prio 3 rate 1666Kbit ceil 80000Kbit burst 3731b cburst 103987b
class htb 1:150 parent 1:10 leaf 151: prio 4 rate 1666Kbit ceil 80000Kbit burst 3731b cburst 103987b
class htb 1:160 parent 1:10 leaf 161: prio 5 rate 1666Kbit ceil 80000Kbit burst 3731b cburst 103987b
class htb 1:210 parent 1:20 leaf 211: prio 6 rate 26666Kbit ceil 80000Kbit burst 35726b cburst 10398
class htb 1:220 parent 1:20 leaf 221: prio 7 rate 20000Kbit ceil 80000Kbit burst 27197b cburst 10398
class htb 1:900 parent 1:1 rate 90000Kbit ceil 90000Kbit burst 116778b cburst 116778b
class htb 1:1000 parent 1:1 prio 0 rate 80000Kbit ceil 80000Kbit burst 103987b cburst 103987b
```

Первым номером в строке обозначается номер класса шейпера, номер 1:1 является корневым и соответственно обозначен как root, все остальные классы будут для него дочерними. Далее указывается номер родительского класса (для всех кроме корневого). Все классы связанные с 1:900 предназначены для пользователей без активного шейпера, в том числе класс 1:10 предназначен для обычного сетевого трафика и 1:20 для файлообменных сетей, класс 1:30 отвечает за пользовательские шейперы. Все классы связанные с 1:1000 относятся к пользователям с активными шейперами, например безлимитные пользователи с ограничением в 64, 128, 256 Кбит/сек и т.п.

В приведенном выше листинге у шейперов можно увидеть параметры rate и ceil. Параметр rate отвечает за гарантированную скорость, а ceil за максимальную скорость этого шейпера. Таким образом, в зависимости от требований, можно выделить пользователю с небольшой гарантированной скоростью большую скорость, если канал свободен, или жестко ограничить скорость в независимости от доступности канала.

Также изменения коснулись интерфейса настройки тарифов в программе Ideco ACP Manager, появились новые настройки в правилах тарифов, которые доступны при нажатии на кнопку дополнительных

настроек (на рис.1 выделена синей рамкой).

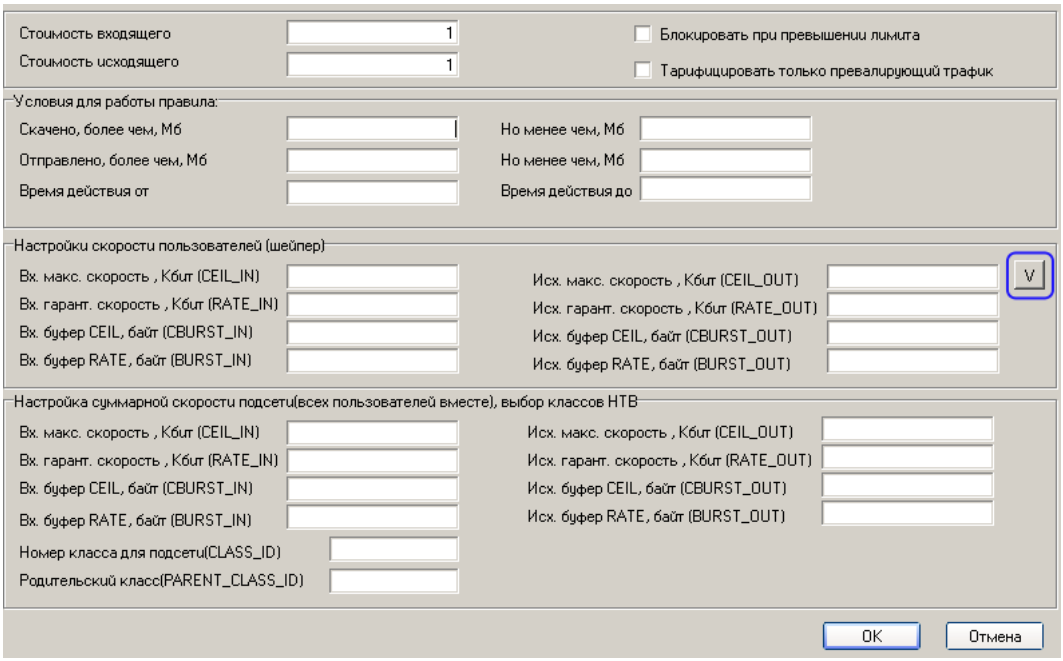


Рис.1 Редактирование тарифного правила.

За каждого пользователя подпадающего под правило настройки задаются в блоке «Настройки скорости пользователей (шейпер)» (см. рис.2), здесь можно указать максимальную и гарантированную скорость входящего и исходящего трафика.

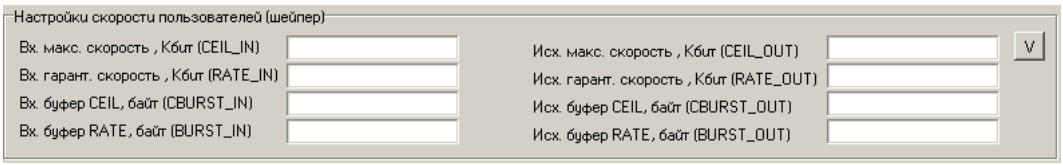


Рис.2 Настройки скорости входящего и исходящего трафика пользователя

Для ограничения общей скорости всех пользователей необходимо задать параметры в блоке «Настройка суммарной скорости подсети (всех пользователей вместе), выбор классов HTB» (см. рис.3).

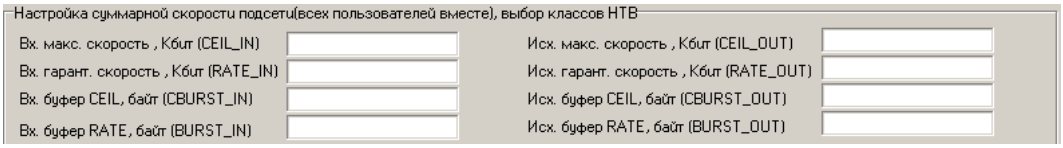


Рис.3 Настройки суммарной скорости входящего и исходящего трафика

Также возможно задать (см. рис.4) номер класса шейпера (CLASS_ID) и его родительский класс(PARENT_CLASS_ID), что позволяет создавать иерархию из тарифов, с более тонкой настройкой разделения скорости входящего и исходящего трафика.

Рис.4 Номер класса шейпера и его родителя

Пример использования новой модели тарифов и шейперов

Далее рассмотрим пример организации тарифов с новыми правилами разграничения скорости канала.

Общее описание проблемы:

Имеется 90 Мбит Интернет канал, который необходимо разделить между тремя группами пользователей с заданными параметрами гарантированной скорости:

1.Юридические лица с безлимитными тарифами (2Мбит/с и 4Мбит/с), гарантировано должны получить

50 Мбит канала.

2.Физические лица с низкоскоростными безлимитными тарифами (128 Кбит/с), гарантированно должны

получить 20 Мбит канала.

3.Физические лица со скоростными безлимитными тарифами (512 Кбит/с и 1Мбит/с), гарантированно

должны получить 20 Мбит общего канала.

Решение:

Создаем пять тарифов (рис.5) с различными параметрами скорости трафика:

1.Группа с классом 1001 для юр.лиц со скоростью 2 Мбит/с (рис.6) и 4 Мбит/с (рис.7).

2.Группа с классом 1002 для физ.лиц со скоростью 128 Кбит/с (рис.8).

3.Группа с классом 1003 для физ.лиц со скоростью 512 Кбит/с (рис.9) и 1 Мбит/с (рис.10).

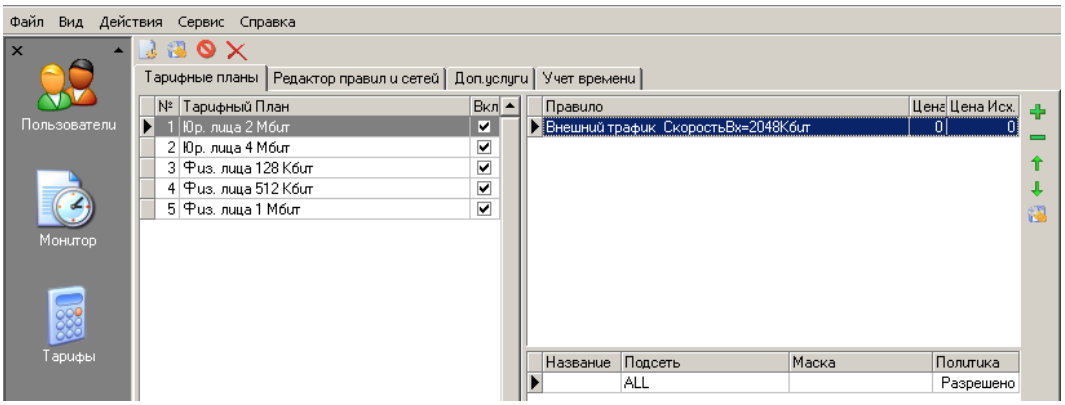


Рис.5 Тарифы

Ниже представлены настройки сети "Внешний трафик" для каждого тарифа с указанием нужных параметров ограничения скоростей и родительских шейперов:

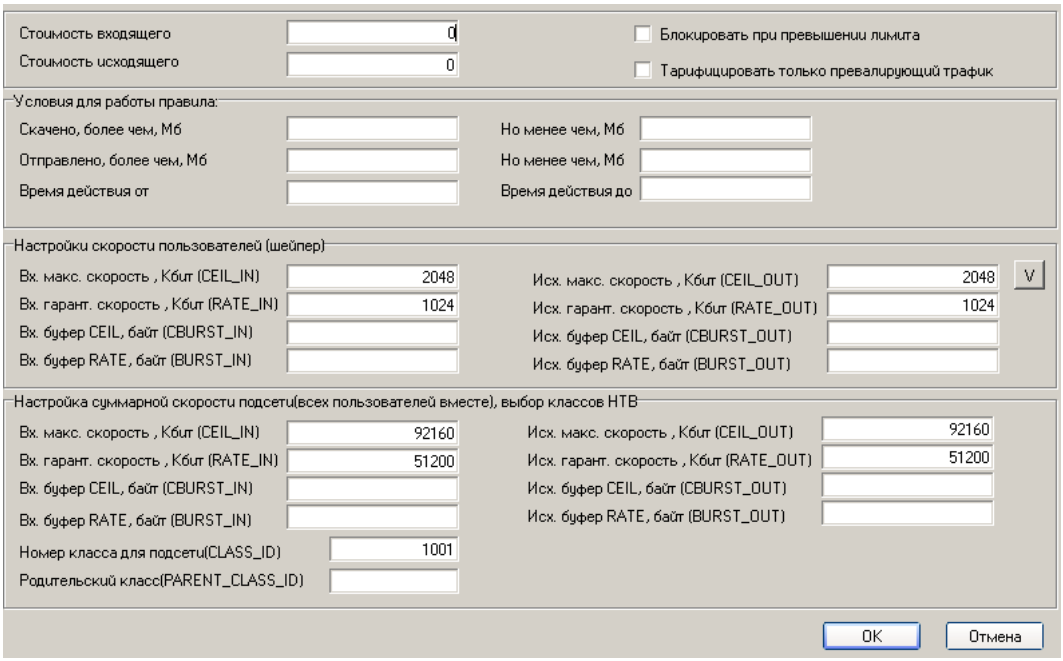


Рис.6 Тариф 2Мбит/с для юр.лиц

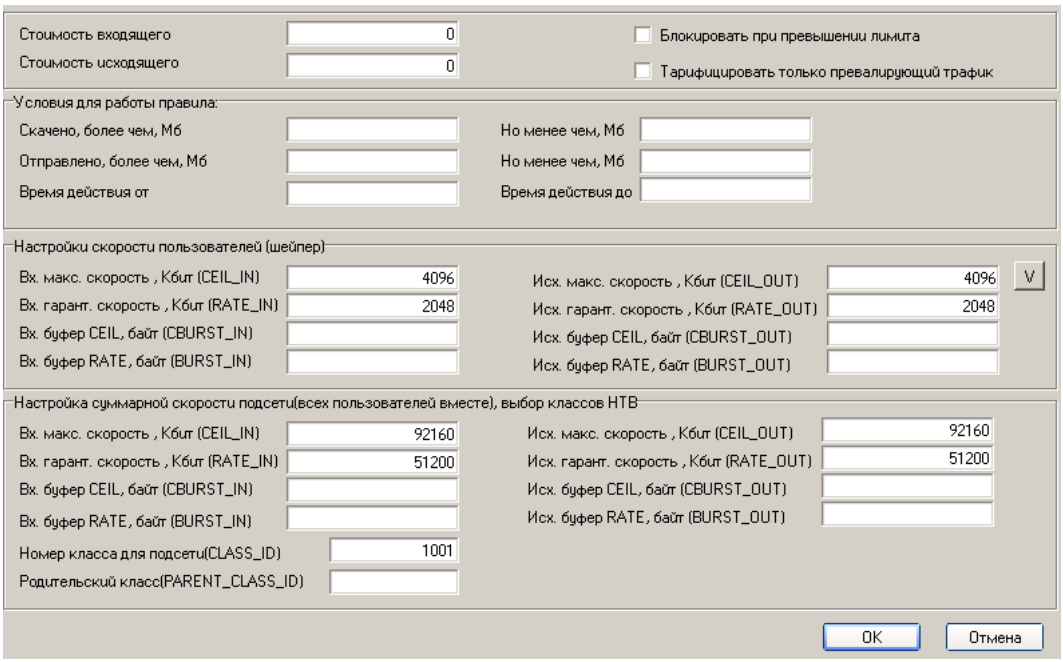


Рис.7 Тариф 4Мбит/с для юр.лиц

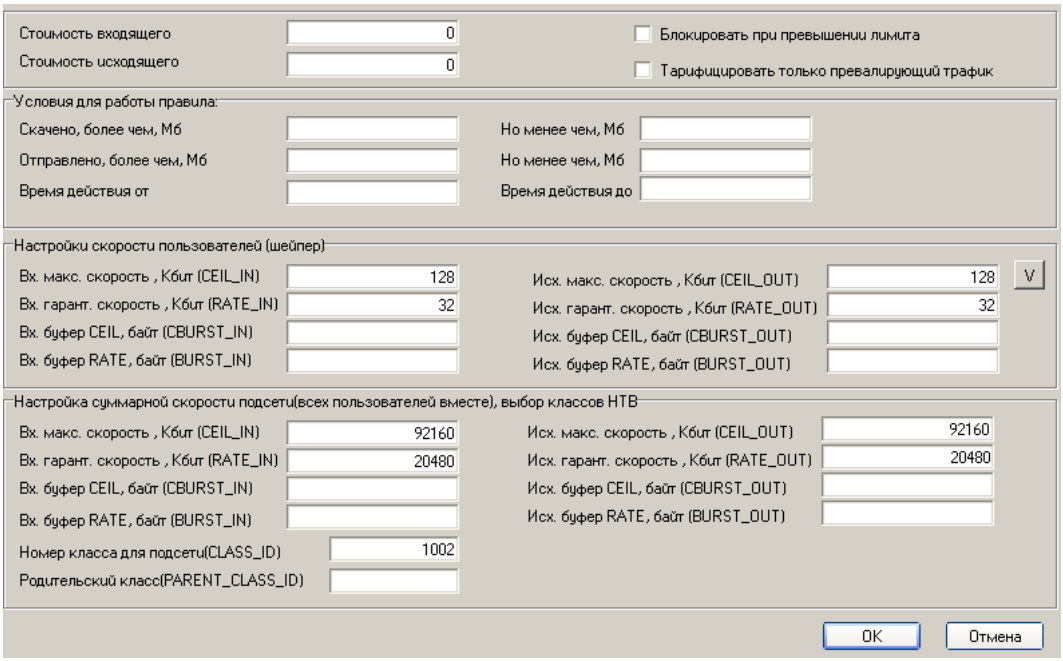


Рис.8 Тариф 128Кбит/с для физ.лиц

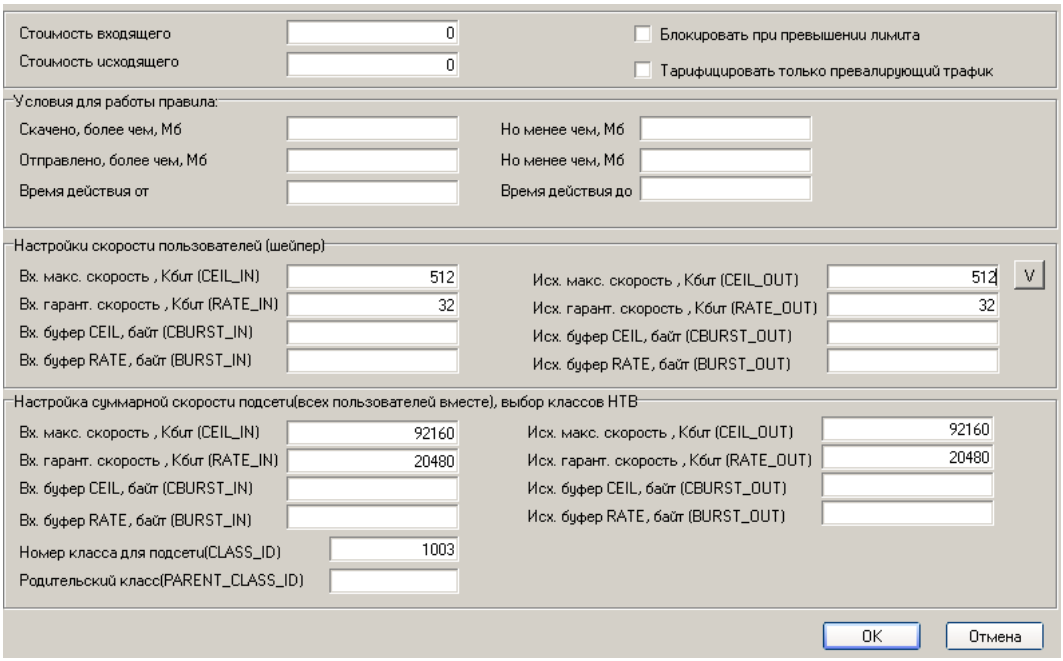


Рис.9 Тариф 512Кбит/с для физ.лиц

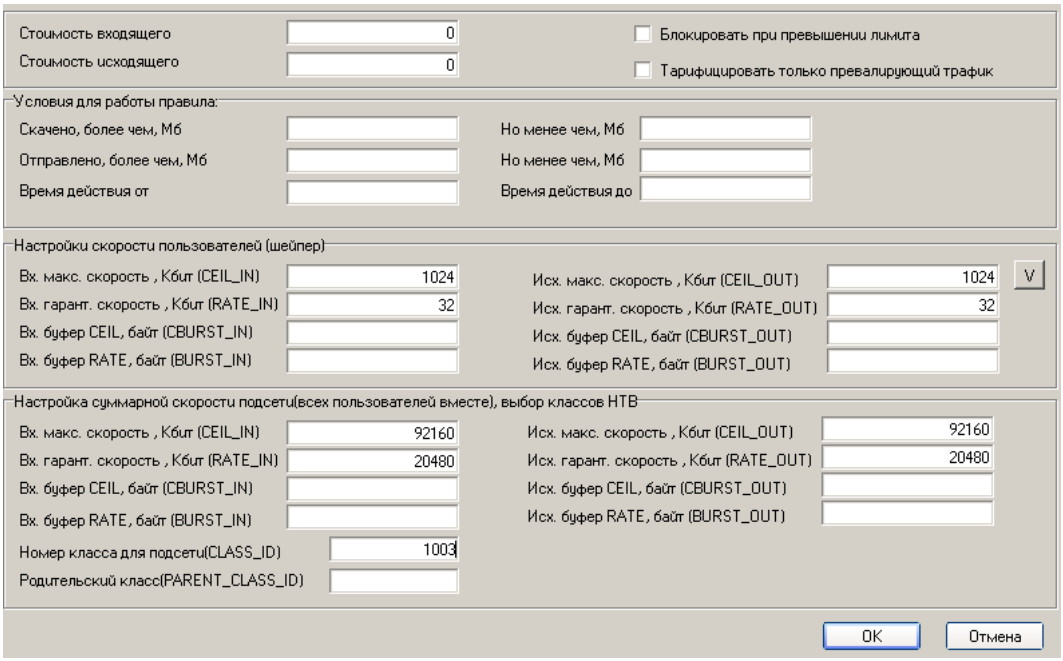


Рис.10 Тариф 1Мбит/с для физ.лиц

Часть

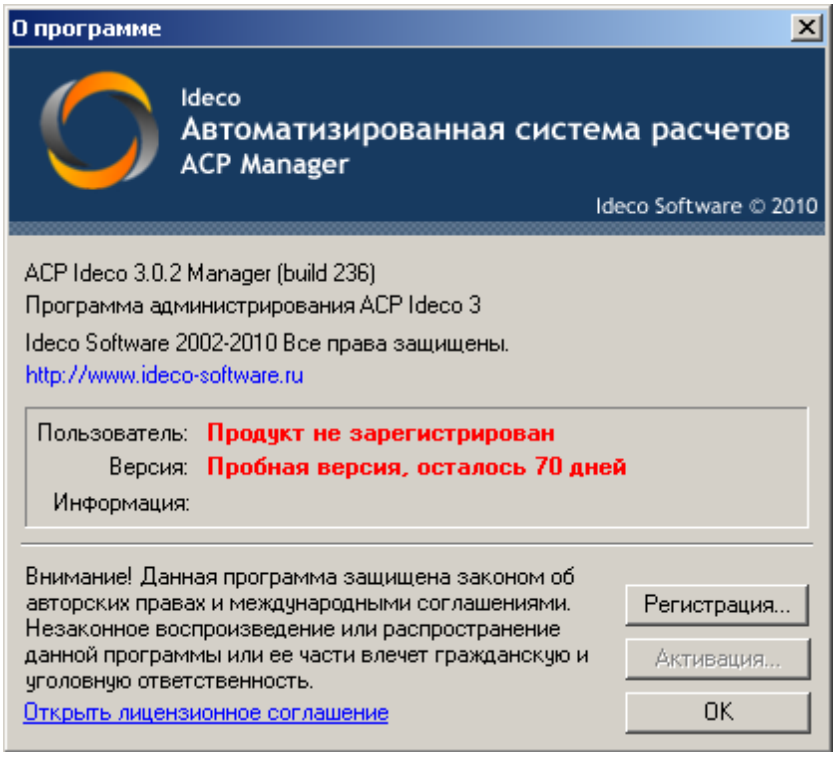
4 Обслуживание сервера Ideco ACP

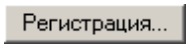
Ideco ICS устроен таким образом, что не требует постоянного обслуживания. Однако некоторые сервисные процедуры проводить рекомендуется, так как возможны аппаратные сбои или может закончиться свободное место на жестком диске.

4.1 Активация сервера Ideco ACP

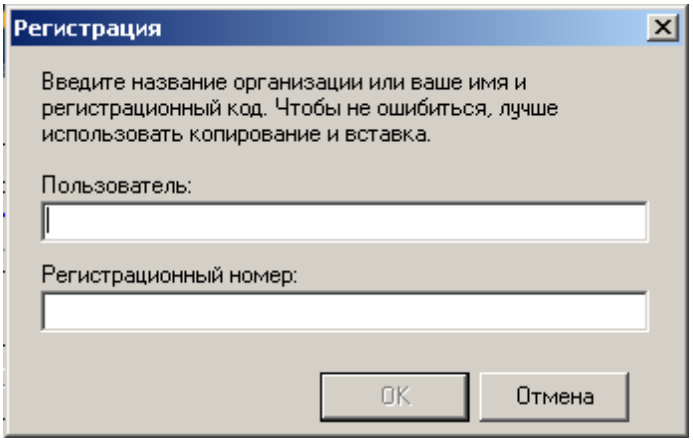
Активация продукта является необходимым шагом в процессе настройки Ideco ACP. При активации все созданные и наработанные вами изменения на сервере как в БД пользователей так и в конфигурации остаются неизменными. Так же повторная активация требуется в том случае если вы переустановили Ideco ACP на новый винчестер и перенесли резервные копии БД на новую установку. В этом случае после активации вам снова в полном объеме станет доступна вся информация о пользователях и настройках сервера на момент создания резервной копии.

Чтобы активировать сервер необходимо зайти в ACP Manager "Справка - О программе ...":

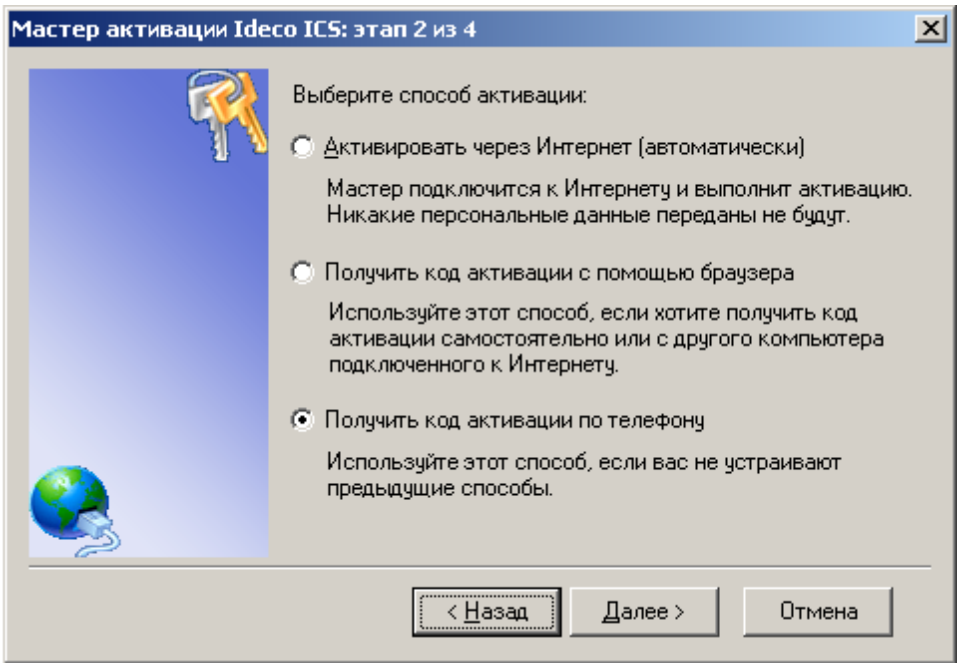


Нажимаем кнопку 

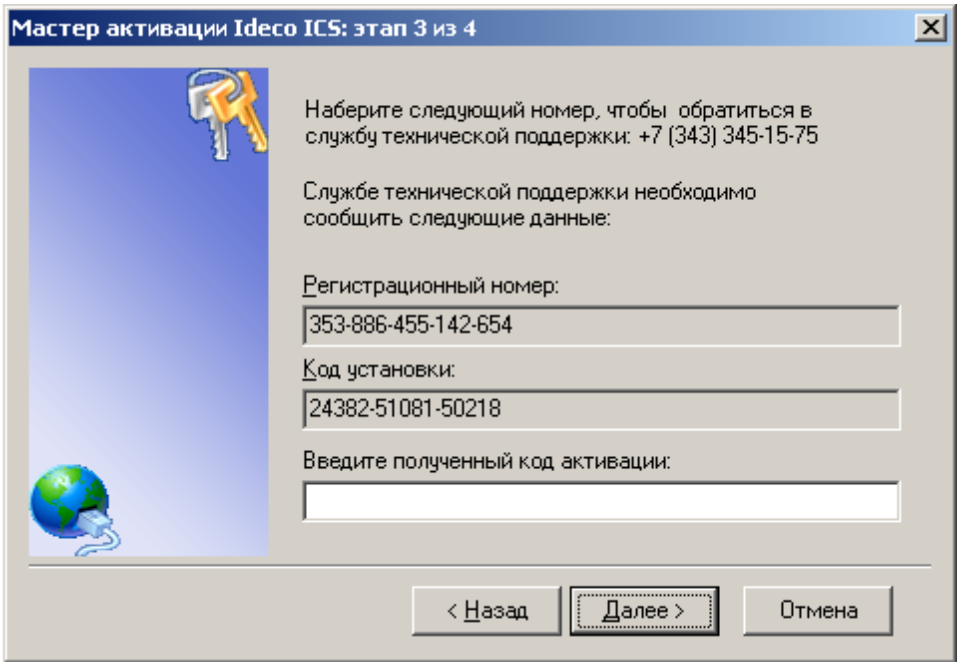
и попадаем на страницу регистрации:



Вводим название организации и регистрационный номер, который необходимо получить в отделе продаж, нажимаем "ОК" и попадаем на мастер активации. Жмём "Далее" и выбираем "Получить код активации по телефону":



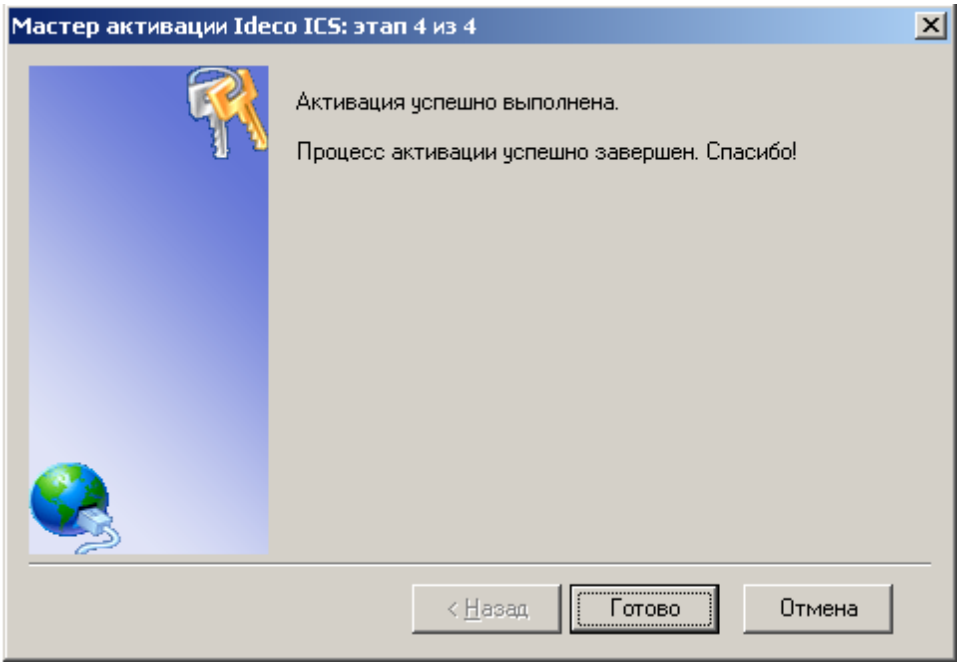
В следующем окне будет предложено ввести код активации:



Для его получения необходимо позвонить по телефону +7 (495) 662-87-34.

Получив код активации вводим его в графе "Введите полученный код активации" и нажимаем "Далее".

Активация завершена, нажимаем "Готово":

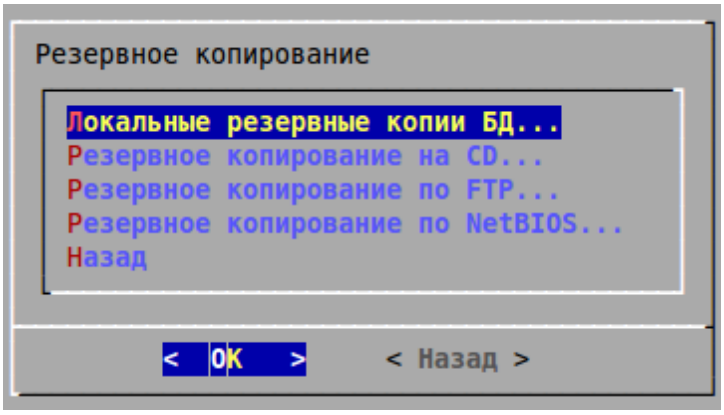


4.2 Резервное копирование средствами Ideco ACP

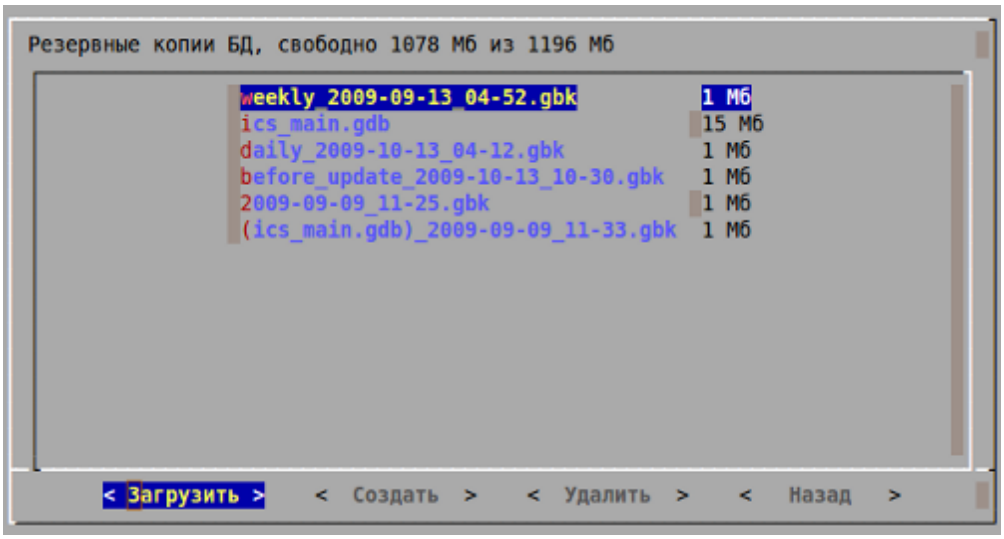
Резервное копирование

Ideco ACP автоматически делает ежедневную копию “daily” , еженедельную “weekly” и ежемесячную “monthly”.

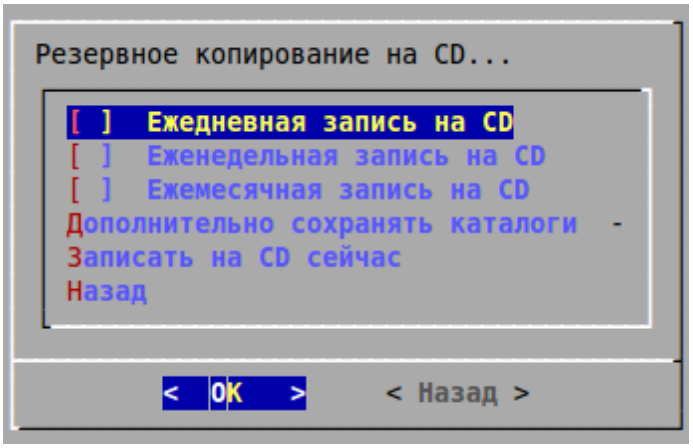
В этом меню можно создать резервную копию текущей БД или восстановить сделанную ранее. В этом пункте меню настраивается метод резервного копирования БД и периодичность создания копий.



Локальные копии БД - список доступных резервных копий БД пользователей, хранящихся на сервере Ideco. Из этого списка вы можете выбрать нужную копию и откатить состояние БД пользователей на предыдущее состояние, выбрав БД и нажав кнопку <Загрузить>. При нажатии кнопки <Создать> будет создан бекап БД пользователей со всеми изменениями на текущий момент (копии БД создаются автоматически ежедневно). Кнопка <Удалить> удаляет выбранную БД пользователей.



Резервное копирование на CD

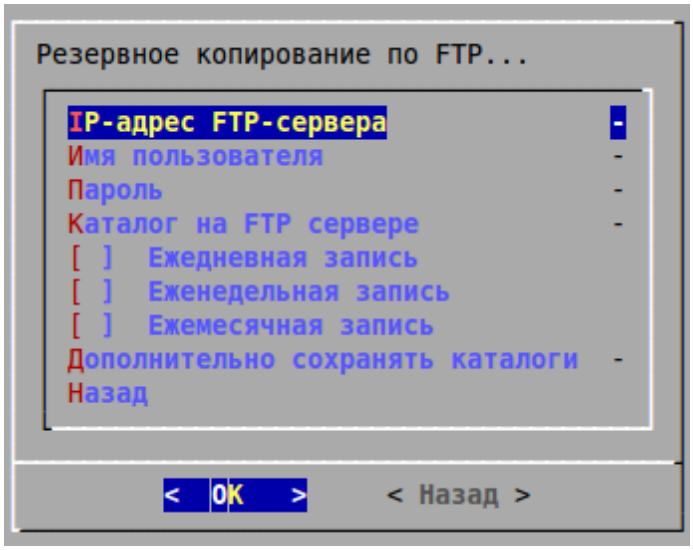


Ежедневная/Еженедельная/Ежемесячная запись - временные интервалы за которые будет производится резервное копирование БД пользователей. Можно выбрать все 3 пункта одновременно.

Дополнительно сохранять каталоги - содержимое указанных каталогов на сервере будет так же записано на диск. (например /var/log/squid)

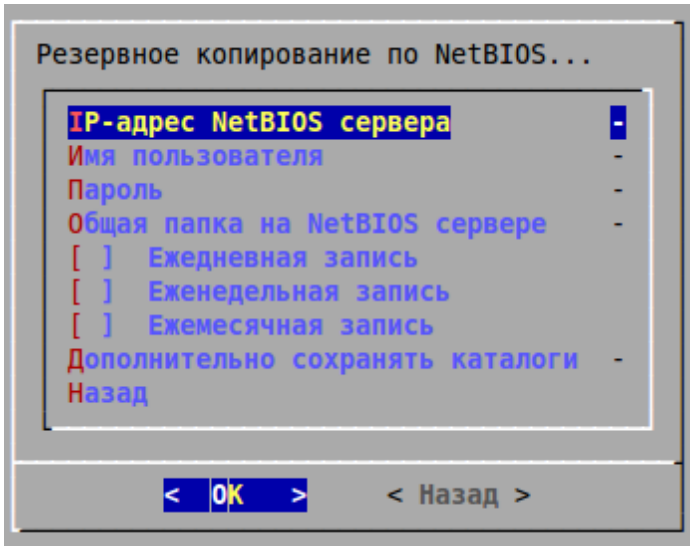
Записать на CD сейчас - разово осуществить запись на CD.

Резервное копирование на FTP



IP-адрес FTP-сервера - адрес удаленнго FTP-сервера. На него будут копироваться копии БД.
Имя пользователя - логин для авторизации на FTP-сервере.
Пароль - пароль для авторизации на FTP-сервере.
Каталог на FTP-сервере - непосредственно в этот каталог будут записываться копии БД.
Ежедневная/Еженедельная/Ежемесячная запись - временные интервалы за которые будет производится резервное копирование БД пользователей. Можно выбрать все 3 пункта одновременно.
Дополнительно сохранять каталоги - содержимое указанных каталогов на сервере будет так же копироваться на FTP-сервер. (например /var/log/squid)

Резервное копирование по NetBIOS



IP-адрес NetBIOS сервера - на компьютер с этим адресом будут передаваться копии БД.
Имя пользователя - логин для авторизации на сетевом ресурсе Windows.
Пароль - пароль для авторизации на сетевом ресурсе Windows.
Общая папка на NetBIOS-сервере - каталог, куда будут записываться копии БД.
Ежедневная/Еженедельная/Ежемесячная запись - временные интервалы за которые будет производится резервное копирование БД пользователей. Можно выбрать все 3 пункта одновременно.
Дополнительно сохранять каталоги - содержимое указанных каталогов на сервере будет так же копироваться на FTP-сервер. (например /var/log/squid)

4.3 Резервное копирование и восстановление из бекапов при помощи WinSCP

В случае переноса данных системы на другой компьютер или переустановки системы с последующим восстановлением конфигурации и базы пользователей, необходимо сначала сделать полный бекап данных с работающей системы. Для того чтобы сделать полный бекап системы необходимо скопировать резервные копии самой базы пользователей и бекап конфигурационного файла системы. Это делается с помощью программы winscp, дистрибутив которой вы всегда можете найти на локальном сайте ideco, или в Интернете по адресу: http://winscp.net/. Программа бесплатна.

Процесс восстановления данных из бекапов можно разбить на два шага: Копирование данных с сервера, и последующая запись резервных копий на новый сервер.

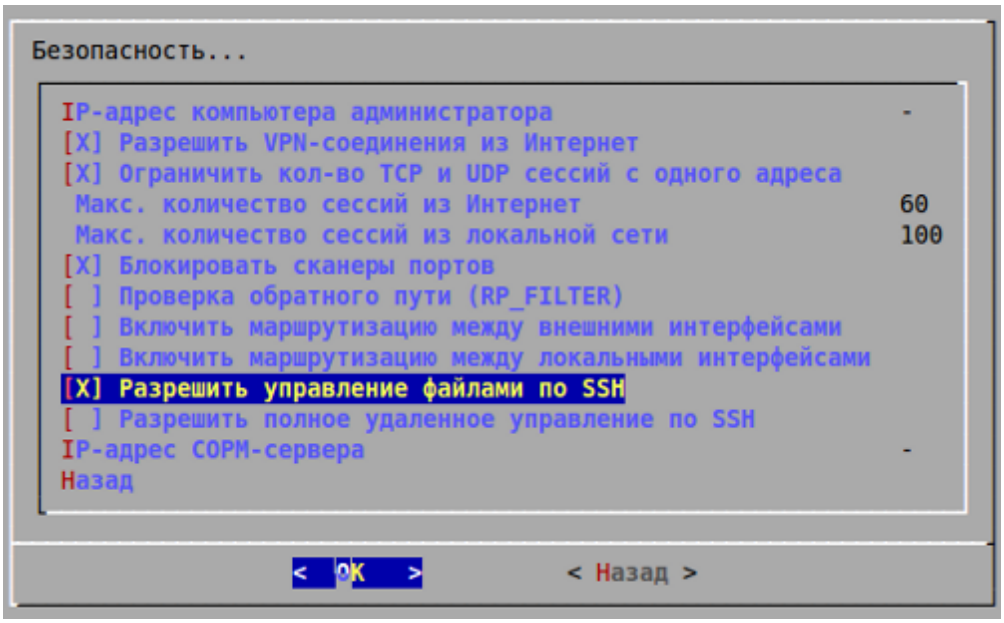
ШАГ 1: Копирование данных с сервера

Для того чтобы подключиться к Ideco с помощью winscp нужно включить пункт

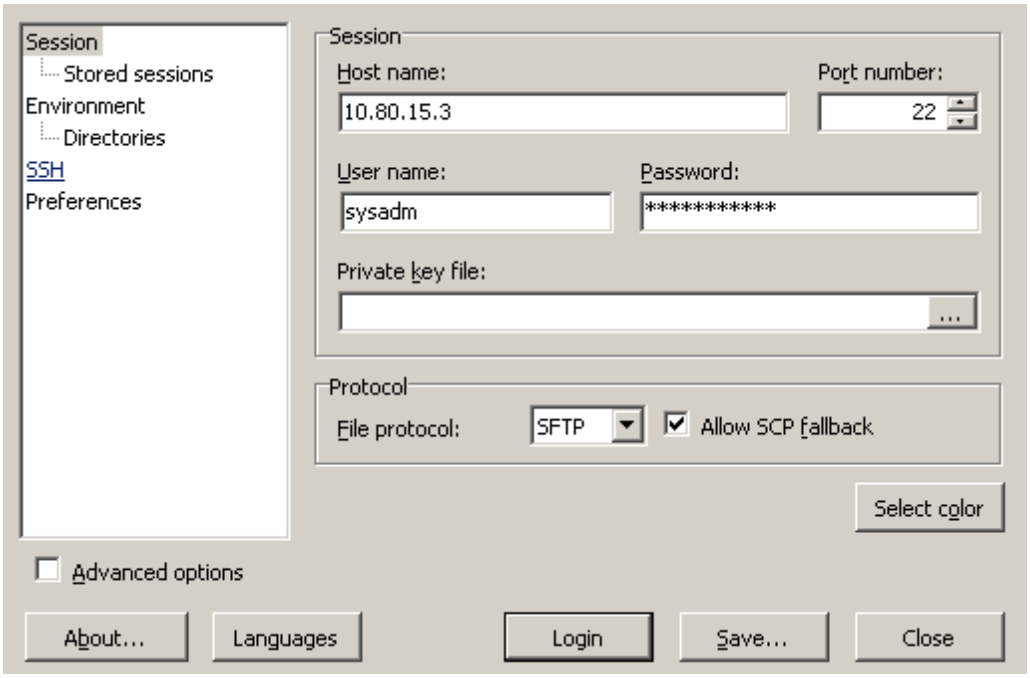
"Разрешить удаленное подключение по SSH" в меню Безопасность:

"Конфигурирование сервера - Безопасность - [X] Разрешить управление файлами по SSH"

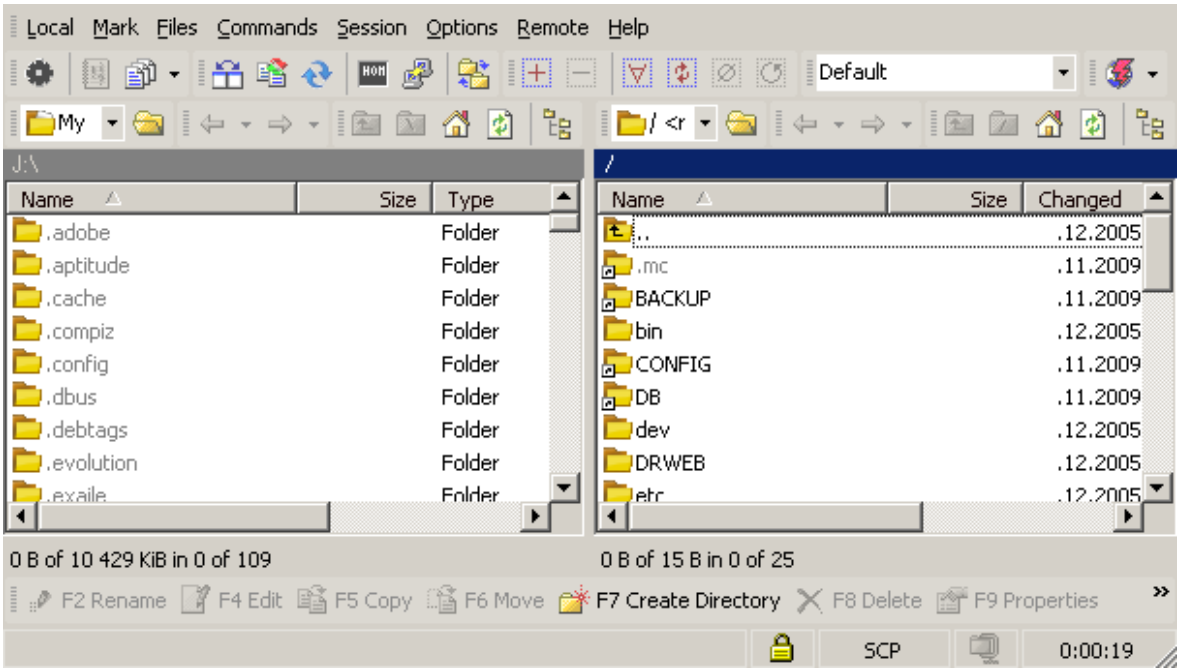
Обязательно необходимо выполнить **полную перезагрузку** сервера.



После этого можно подключаться к серверу на 22 порт из локальной сети (из интернета работать не будет), в качестве логина и пароля использовать sysadm и servicemode (пароль по умолчанию от локальной консоли). В примере ниже 10.80.15.3 это адрес шлюза ideco в локальной сети, у вас он может быть другим.

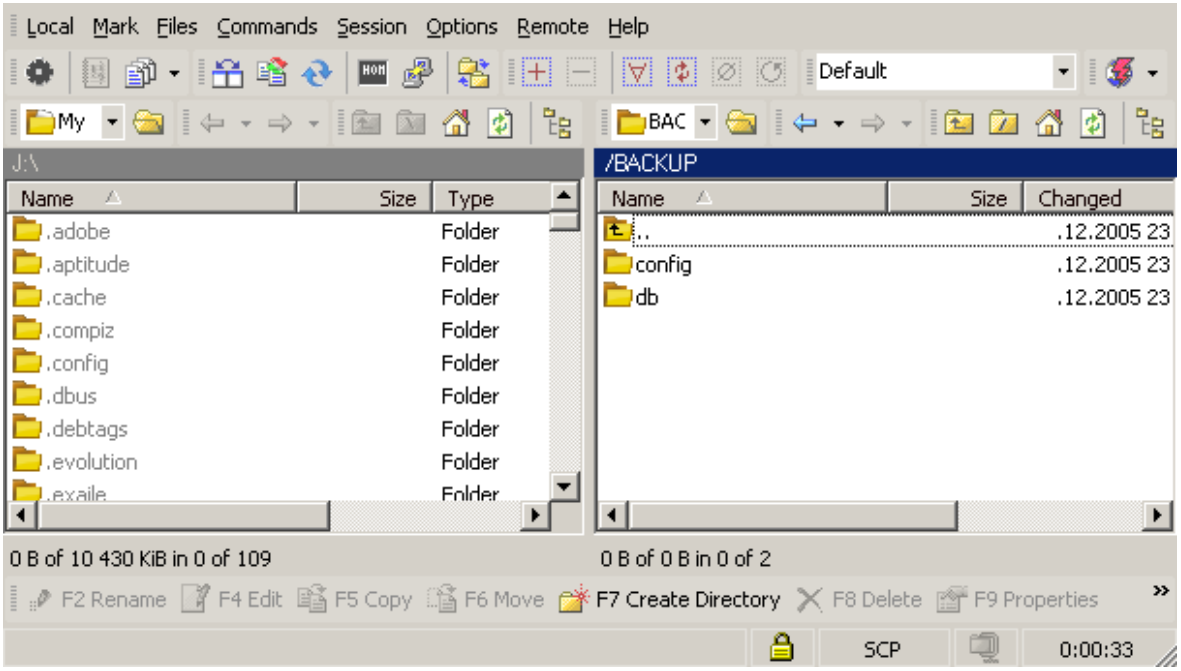


Убедитесь что данные введены верно и нажимайте "Login", после подключения вы увидите окно, похожее на обычный файловый менеджер с двумя панелями, слева будет ваш локальный компьютер, справа - файловая система ideco, вас интересует каталог BACKUP на ней.



В каталоге BACKUP находятся резервные копии базы данных и конфигураций

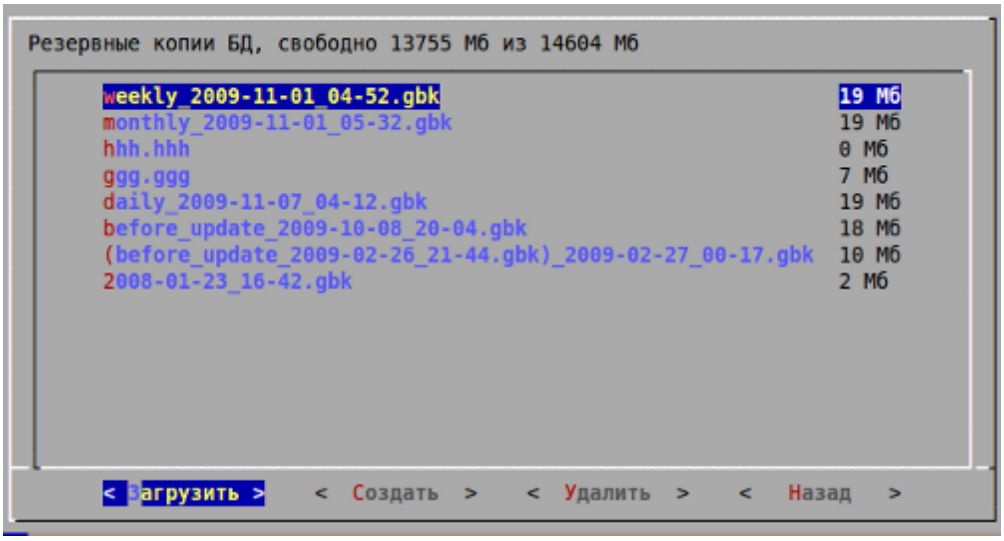
системы. Архивированные базы данных хранятся в подкаталоге /BACKUP/db (это файлы с расширением .gbk), а копии конфигураций, соответственно, в /BACKUP/config (это файлы с расширением .conf). Это видно на скриншоте ниже. Вы можете выборочно скопировать нужные вам файлы из этих каталогов, или полностью весь каталог BACKUP на свой компьютер.



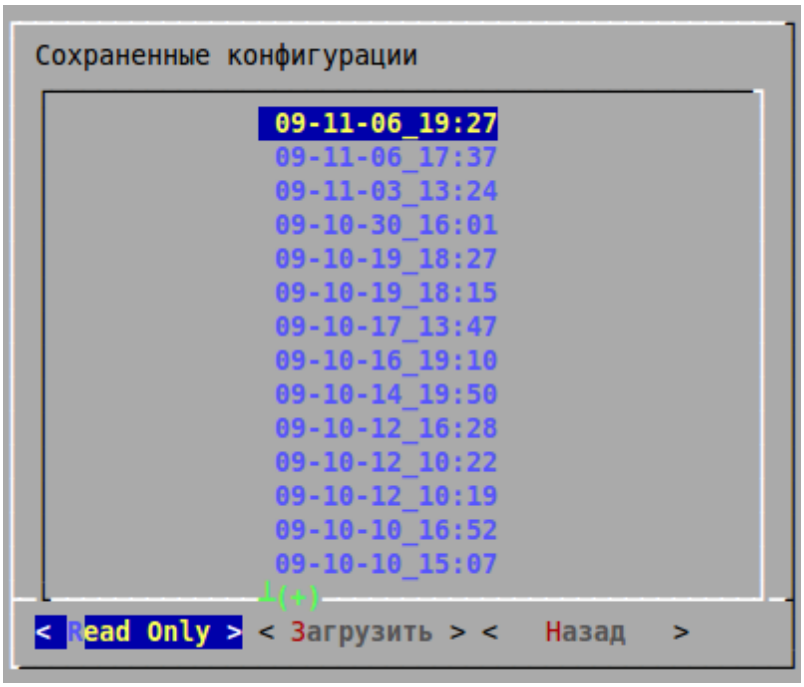
*** Примечание**: Статистика копируется отдельно из папки **STAT**.

ШАГ 2: Запись данных на сервер

Все резервные копии всегда храняться в каталоге BACKUP, содержимое этого каталога, как было сказано выше, состоит из двух подкаталогов, в которых хранятся бекапы баз данных и конфигураций. В меню "Резервное копирование" - "Резервные копии БД" вы можете увидеть присутствующие на сервере бекапы баз данных пользователей и восстановить текущую базу до нужной стадии там же. Бекапы могут быть созданы вручную или автоматически по расписанию.



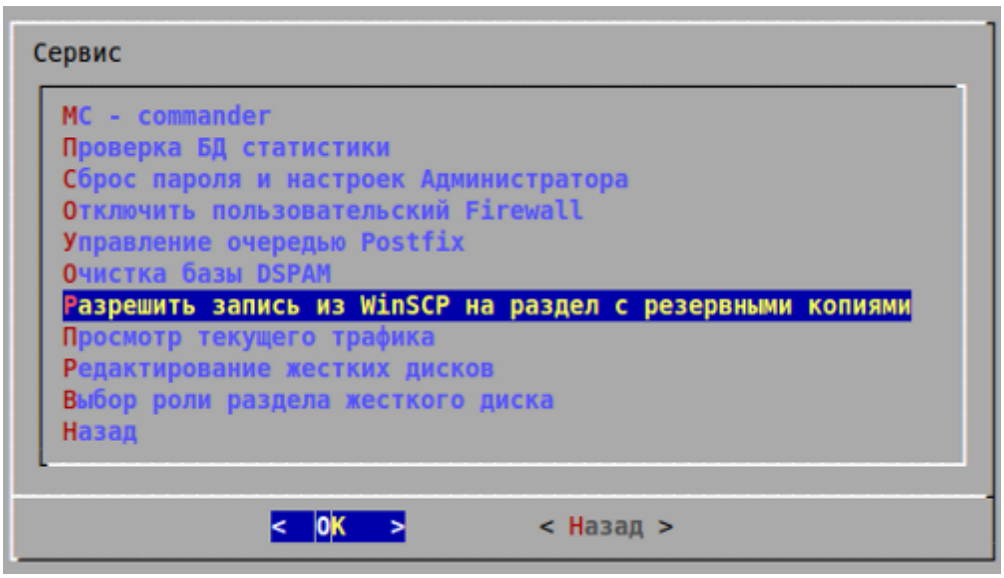
Присутствующие бекапы конфигураций на сервере можно увидеть в меню "Сохраненные конфигурации" в меню "Конфигурирование сервера". Оттуда же можно восстановить конфигурацию сервера из нужного вам бекапа.



Соответственно чтобы восстановиться из бекапов, которые вы предварительно скопировали со старого сервера, нужно их записать в каталог BACKUP на новом сервере, после чего они появятся в обоих списках резервных копий, и из них можно будет восстановить систему.

По умолчанию запись на раздел с резевными копиями в каталог BACKUP запрещена.

Для того чтобы иметь возможность записи на диск с резервными копиями, необходимо на сервере в меню "Сервис" вкючить пункт "Разрешить запись из WinSCP на раздел с резервными копиями". Пункт не имеет флажка, при нажатии запись просто включается до следующей перезагрузки сервера. Не нажимайте дважды. На сервере должен предварительно быть настроен локальный интерфейс и включен пункт "Разрешить удаленное подключение по SSH" в меню Безопасность, чтобы можно было подключиться к серверу.



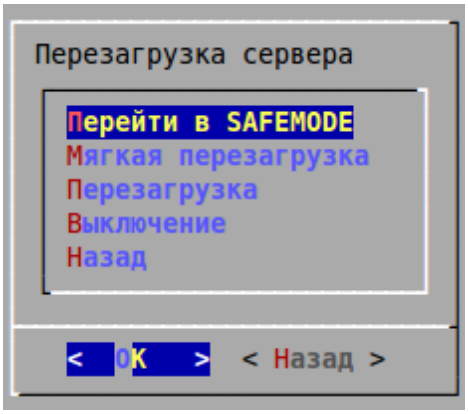
- После этого подключаемся по winscp к серверу от sysadm на 22 порт. Адрес сервера и пароль должны соответствовать настройке вашего нового сервера.

- Подключившись к серверу копируем с локального компьютера на сервер в каталог BACKUP резервные копии базы данных и конфигурационных файлов, **соблюдая иерархию подкаталогов!**

- Скопировав нужную копию базы данных и конфигурационного файла вы должны обнаружить их в локальном меню вашего сервера в соответствующих им разделах ("Локальные копии БД" и "Сохраненные конфигурации"). Оттуда же вы можете восстановить БД или конфигурацию сервера.

ШАГ 3: Восстановление БД из резервной копии

- Восстановление базы данных пользователей возможно только если сервер загружен в режиме SAFEMODE. Поэтому в локальном меню сервера в разделе "Перезагрузка" выберите пункт "Перйти в SAFEMODE".



- После загрузки сервера в режиме SAFEMODE, перейдите в раздел копий БД на сервере: "Резервное копирование" => "Локальные резервные копии БД...". Выберите нужную вам копию базы данных и нажмите кнопку "Загрузить".

- После того как бекап базы данных будет успешно применен к системе, перезагрузите сервер в обычном режиме.

- После восстановления базы данных вам потребуется заново пройти процесс активации продукта. Для этого обратитесь в отдел продаж нашей компании по телефону: (495) 987-32-70 или в ICQ 563191479

Примечание: Если вы копируете резервные копии на новый винчестер (переустановка Ideco ACP на другой винчестер), то после восстановления БД и Конфигурации из бекапа вам необходимо заново пройти процесс активации. Подробнее105 ..

Если что то пошло не так, обращайтесь в отдел технической поддержки: ICQ 463710578, 416479735 или по телефону (495) 987-32-70.

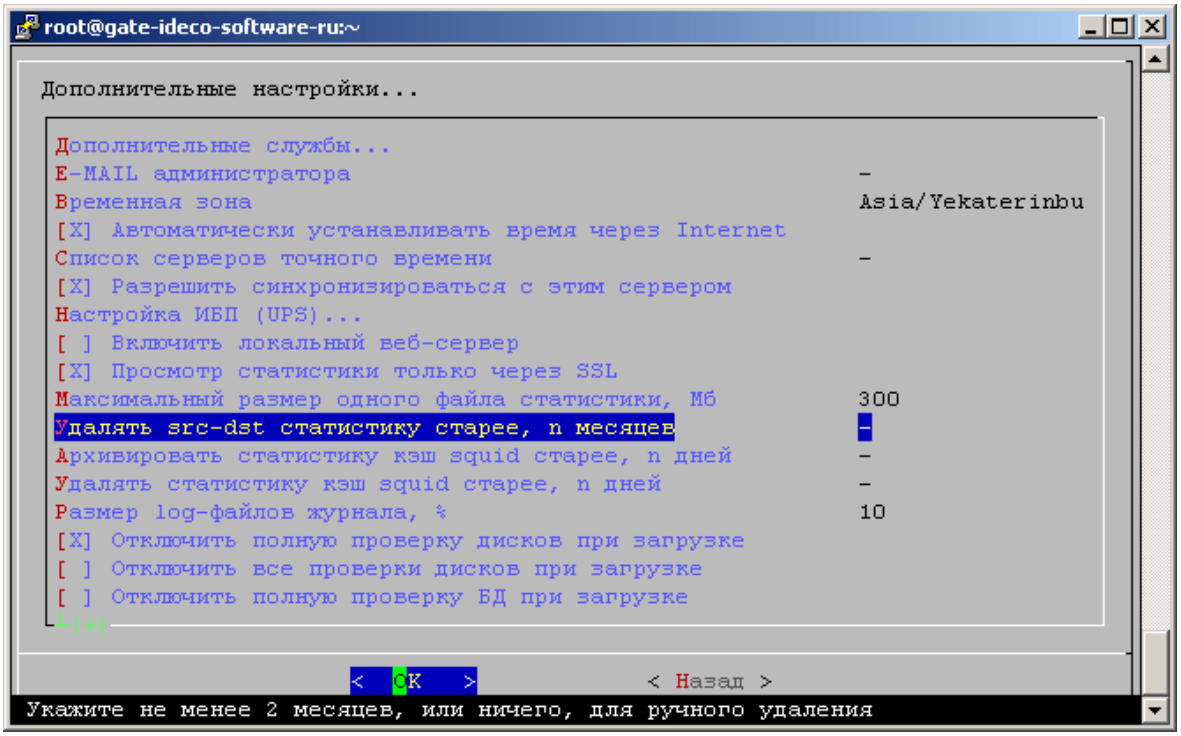
4.4 Архивирование, копирование и очистка статистики на сервере Ideco

Очистка и архивирование статистики с заданным интервалом через локальное меню

Удаление src-dst статистики на сервере ideco с заданным интервалом

В локальном меню выберите: "Конфигурирование сервера - Дополнительные настройки"

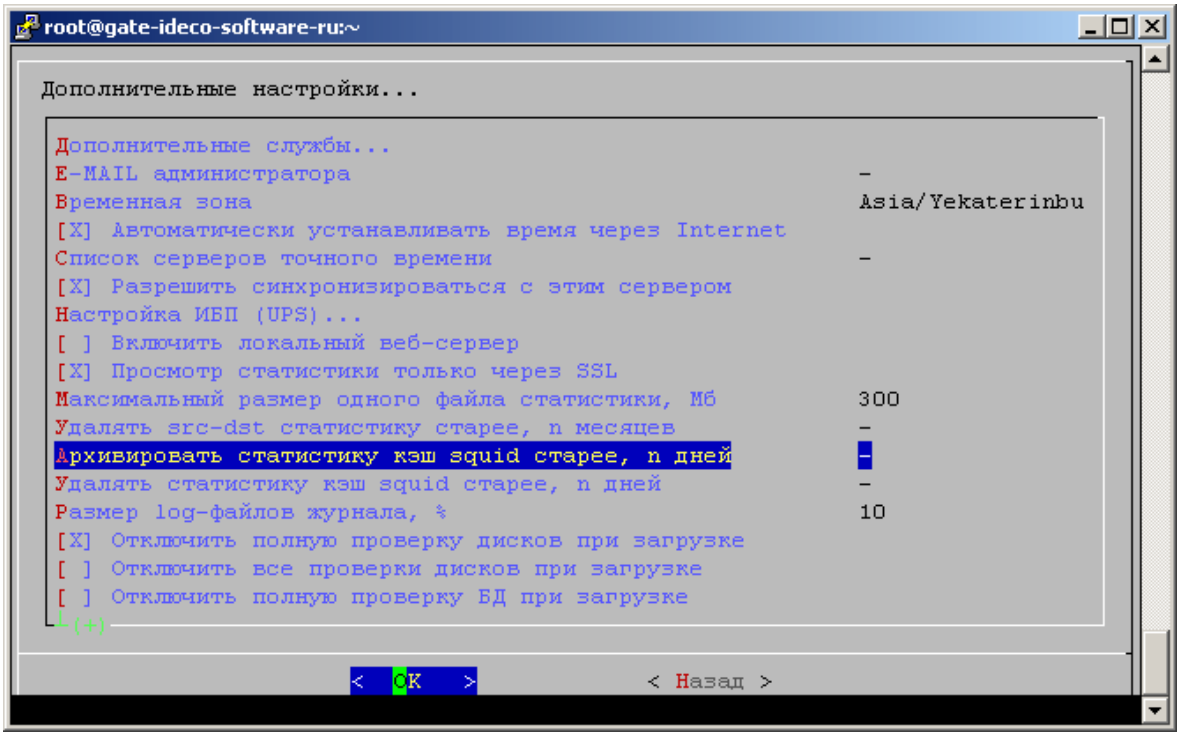
Далее в пункте "Удалять src-dst статистику старее, n месяцев" укажите количестве месяцев, за которое статистика считается актульной, данные старее этого срока будут удаляться:



Периодическое архивирование статистики прокси-сервера squid

Если у вас включен прокси-сервер и статистика по посещениям сайтов занимает слишком много места, то может оказаться полезной периодическая архивация статистики squid. Настроить период архивации можно там же в локальном меню: "Конфигурирование сервера - Дополнительные настройки".

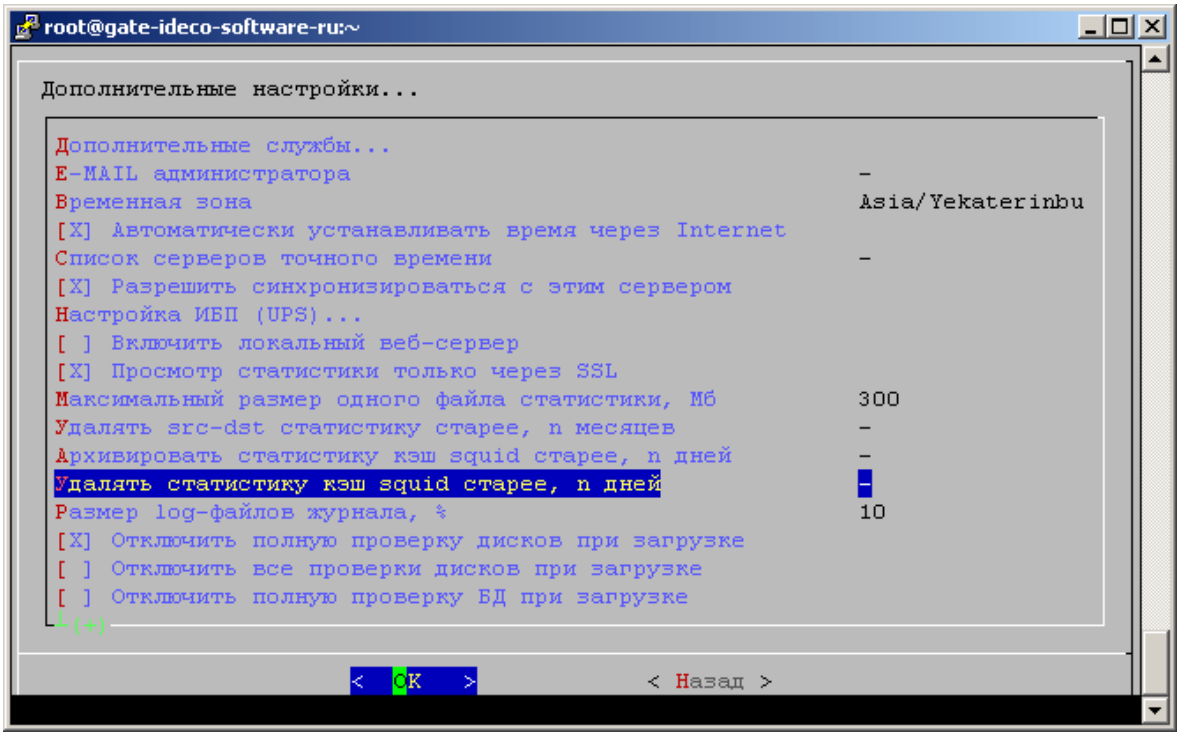
В пункте "Архивировать статистику кэш squid старее, n дней" укажите количестве дней, за которое статистика кэша считается актульной, данные старее этого срока будут архивироваться:



Периодическое удаление статистики прокси-сервера squid

Можно так же удалять статистику squid старше определенного срока, настраивается это так же в локальном меню: "Конфигурирование сервера - Дополнительные настройки"

В пункте "Удалять статистику кэш squid старее, n дней" укажите количестве дней, за которое статистика кэша считается актульной, данные старее этого срока будут удаляться:



*** Примечание**: Как правило этих действий оказывается достаточно для предотвращения заполнения дискового пространства файлами статистики пользователей. Если вам необходима более радикальная чистка директорий статистики Ideco или вы, например, хотите скопировать файлы статистики с сервера, то обратите внимание на методы доступа к статистике, описанные ниже.

Удаление только статистики src–dst

- Если вы управляете сервером локально или подключены по SSH на порт 22: Зайдите при помощи локальной консоли в меню **Сервис > MC-commander** или WinSCP в каталог **STAT** и удалите каталог с устаревшими БД. Удалять старые каталоги необходимо, чтобы не закончилось место на диске. Администратор будет предупрежден о нехватке свободного места на жестком диске.
- Если вы подключены удалённо по SSH на порт 33 под логином root: Запустите Midnight Commander командой **mc** и удалите устаревшую статистику из каталога **/var/dbstat**.

Обнулить статистику src-dst, "сырую" неагригированную статистику и статистику прокси-сервера (lightsquid)

1. Нужно подключиться к Ideco по SSH 120 (Загрузиться в режиме удаленного помощника или создать пользователя root и подключиться под root на порт 33)
2. Статистика по подсетям (src-dst), доступная в веб-интерфейсе хранится в /var/dbstat. В этой директории вас интересуют каталоги с названиями типа: 200901 - их и надо удалить. Другие каталоги в /var/dbstat трогать не нужно.
3. "Сырая" неагригированная статистика находится в директории /var/stat/all но

удалять ее самостоятельно крайне не рекомендуется, может привести к перезагрузкам сервера и другим нежелательным эффектам.

4. Статистика proxy-сервера (Статистика LightSquid) хранится /mnt/rw_disc/chroot_thttpd_L/var/www/local/lightsquid/report. В этой директории вы дожны удалить все каталоги типа: 20090518. Файлы group.cfg и realname.cfg, если они есть в каталоге report, удалять не нужно.
5. После этих действий вам потребуется Мягкая Перезагрузка.

Очистить все каталоги из консоли можно этими командами (обладая правами root):

```
find /var/dbstat/* -name [0-9]* -type d -maxdepth 0 -exec rm -r {} \;
find /mnt/rw_disc/chroot_thttpd_L/var/www/local/lightsquid/report/ -name [0-9]* -type d -exec rm -r {} \;
```

Так же проверьте объем занимаемый файлами "сырой" статистики на сервере:

```
du -sh /var/stat/all
```

Если их значение покажется вам большим, то не работайте с этим каталогом самостоятельно, а **обязательно обратитесь по этому вопросу в техподдержку с выводом этой команды в icq 463710578 или 416479735.**

Если вам нужно скопировать эти файлы статистики с Ideco ACP, то в WinSCP место нахождения файлов будет то же.

4.5 Удаленный доступ к меню сервера

- **Подключение из локальной сети**

1. В локальной консоли в меню безопасность разрешите управление файлами по SSH:

"Конфигурирование сервера - Безопасность - [X] Разрешить управление файлами по SSH"

2. Подключиться к серверу через программу putty, протокол SSH, порт 22. Указать логин sysadm, пароль как в локальной консоли. (По умолчанию servicemode)

Для вывода меню – команда menu, для запуска файлового менеджера - команда mc .

- **Подключение из Интернета**

Подключиться по SSH к Ideco ACP из Интернета под пользователем sysadm нельзя и порт 22 открыт только для локальной сети, это сделано в целях повышения безопасности.

Чтобы подключиться из Интернета по SSH, нужно:

1. В локальной консоли в меню безопасность разрешите управление файлами по SSH:

"Конфигурирование сервера - Безопасность - [X] Разрешить полное управление файлами по SSH"

2. Создать пользователя root. Подробнее263 ...

После завершения этих манипуляций можно будет подключаться из Интернета любым SSH-клиентом (например putty, есть на установочном диске ideco) на 33-ий порт, с логином root и паролем который назначили при создании root'a. Для вывода меню – команда menu, для запуска файлового менеджера - команда mc.

Под пользователем root можно подключаться также и из локальной сети на локальный адрес сервера, но всё равно нужно будет подключаться на 33-ий порт.

*** Примечание:**

- Если root для постоянного пользования не нужен, то можно загрузить сервер в режиме удалённого помощника 121 (root будет создан до следующей перезагрузки сервера).
- Описанные здесь методы доступа к локальному меню не касаются режима "Удаленный Помощник". Доступ к локальному меню сервера и к консоли linux используя "Удаленный Помощник" описаны здесь 121.

4.6 Режим удаленного помощника

Для решения многих вопросов часто требуется вводить сервер Ideco в режим удаленного помощника, чтобы служба технической поддержки могла подключиться к вашему серверу удаленно. В режиме удаленного помощника все сервисы и весь функционал Ideco работает неизменно, так что на работе пользователей это не отразится. Так же с некоторыми задачами системные администраторы могут справиться сами, но для их решения часто бывает необходимы права пользователя root. В режиме удалённого помощника пользователь root создаётся до следующей перезагрузки сервера.

- **Загрузка сервера в режиме удаленного помощника**

Что бы загрузиться в режиме удаленного помощника вам необходимо сделать следующее:

1. При загрузке сервера, сразу после таблицы BIOS нажимайте раз в секунду Ctrl-x, до появления приглашения «boot:».

2. Придумайте временный пароль для удаленного помощника максимум из 8 букв.

3. В приглашении введите ICServer p=пароль nc=1.

Например, ICServer p=serv nc=1

4. После этого нажмите Enter и введите пароль: servicemode. При вводе пароля на экран ничего не отображается. После нажатия Enter должна продолжиться обычная загрузка системы. В этом режиме сервер функционирует как обычно.

5. Внешний IP адрес и временный пароль, который вы указали после p= отправьте специалисту технической поддержки с которым вы общаетесь по icq, почте или продиктуйте по телефону.

- **Работа с консоли сервера от пользователя root в режиме удалённого помощника**

1. Нажмите Alt+F7, тем самым вы выходите на свободную консоль
2. Напишете login, затем root, потом временный пароль, который вы указали после "p="
3. Теперь вы вошли в систему с правами пользователя root, в строке приглашения должен быть символ "#"

- **Работа с сервером удаленно поп ротоколу ssh в режиме удаленного помощника**

1. На вин-системах для подключения к серверу по протоколу ssh используйте клиент putty. Программа бесплатна и скачать ее всегда можно с сайта разработчика:

   http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

или с нашего диска из каталога utils.

2. При подключении из локальной сети подключаться нужно на локальный адрес сервера (тот адрес, который настроен на локальной сетевой карте Ideco ACP)
3. Параметры для подключения: Порт 33, Логин: root, Пароль: временный пароль, указанный вами при загрузке сервера в режиме удаленного помощника (после "p=").
4. В полученной консоли в putty знак "#" говорит о том что вы работает от имени пользователя root.

Примечания:

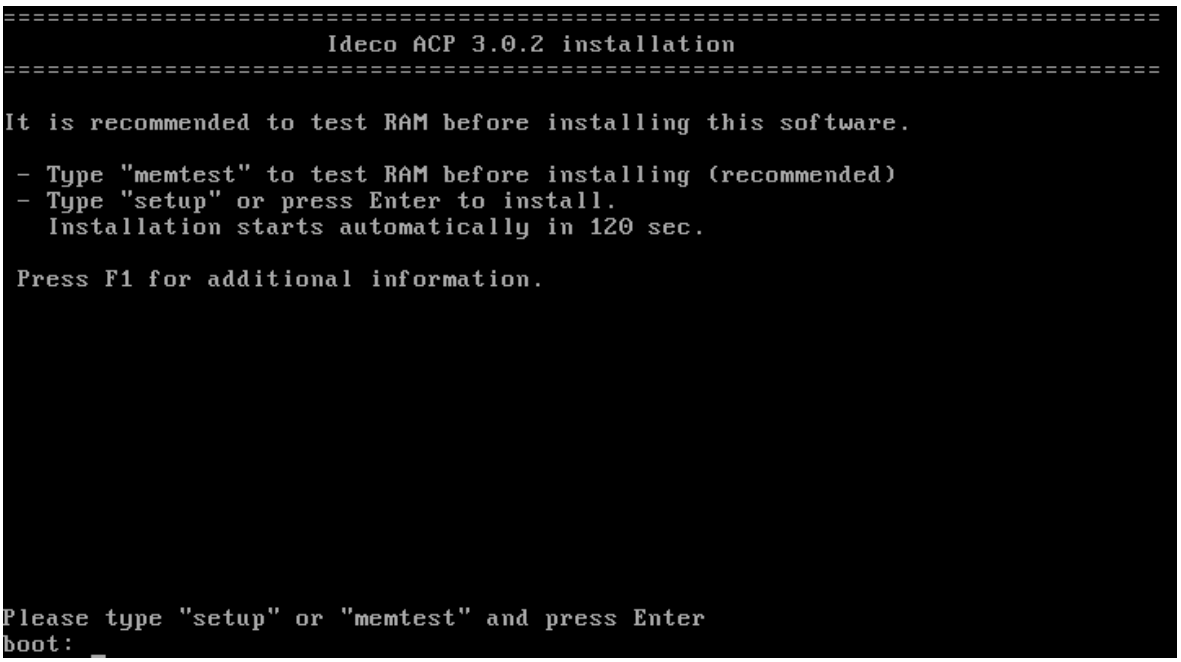
- Загружая сервер в режиме "удаленного помощника" с ядром, отличным от стандартного,нужно вместо icserver писать название нужного вам ядра. Например так: **pptp p=serv nc=1**. Указав такие параметры при загрузке в строке boot: вы загрузите сервер с ядром **pptp** в режиме "удаленного помощника".

4.7 Обновление сервера

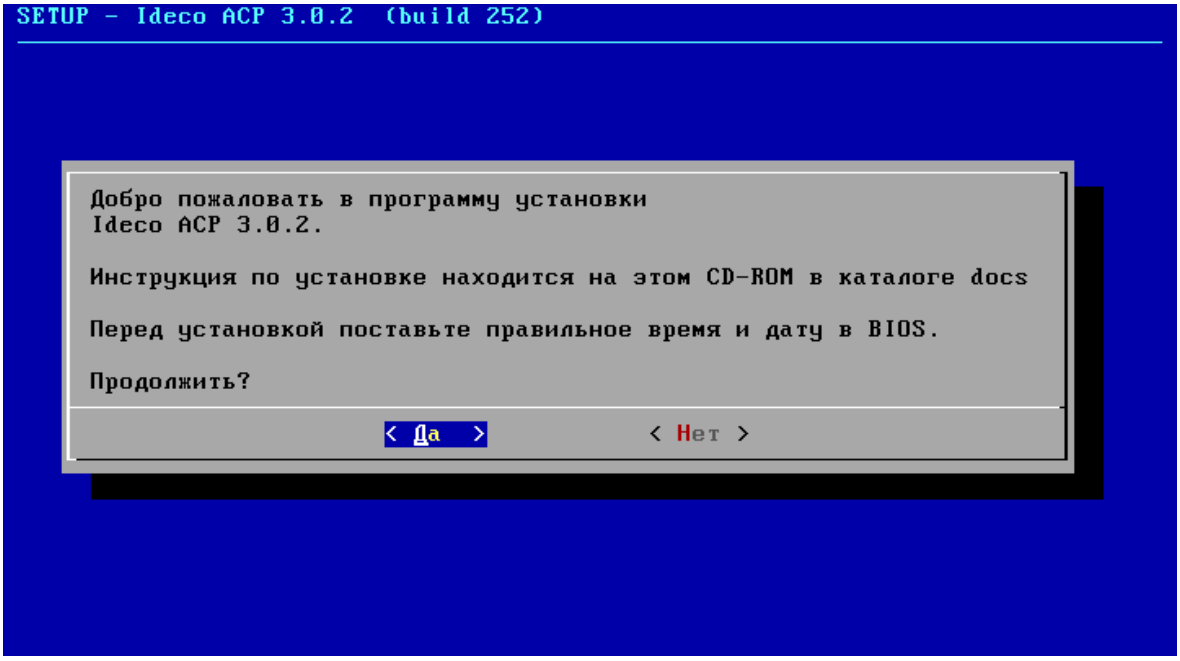
Прежде всего вам нужно скачать актуальный CD-образ (.iso) с нашего сайта. Актуальная версия всегда доступна на официальном сайте компании Ideco (http://ideco-software.ru/products/billing/download.html). После того как вы скачали образ диска на ваш PC, запишите его на CD как дисковый образ, а не как файл.

Для того чтобы быть уверенным, что ваша копия образа была получена с сайта без ошибок и корректно записана на CD, нужно сравнить сначала полученный образ на соответствие хеш-суммы MD5, а затем проверить записанный диск. MD5-хеш опубликованного файла образа всегда указан на странице загрузки iso-образа. Поэтому при скачке образа со страницы загрузки настоятельно рекомендуется скопировать на свой PC так же значение хеш-суммы образа диска для последующего сравнения образа и диска с ней. Скачивать образ желательно менеджером закачек, поддерживающим докачку после обрывов сессии.

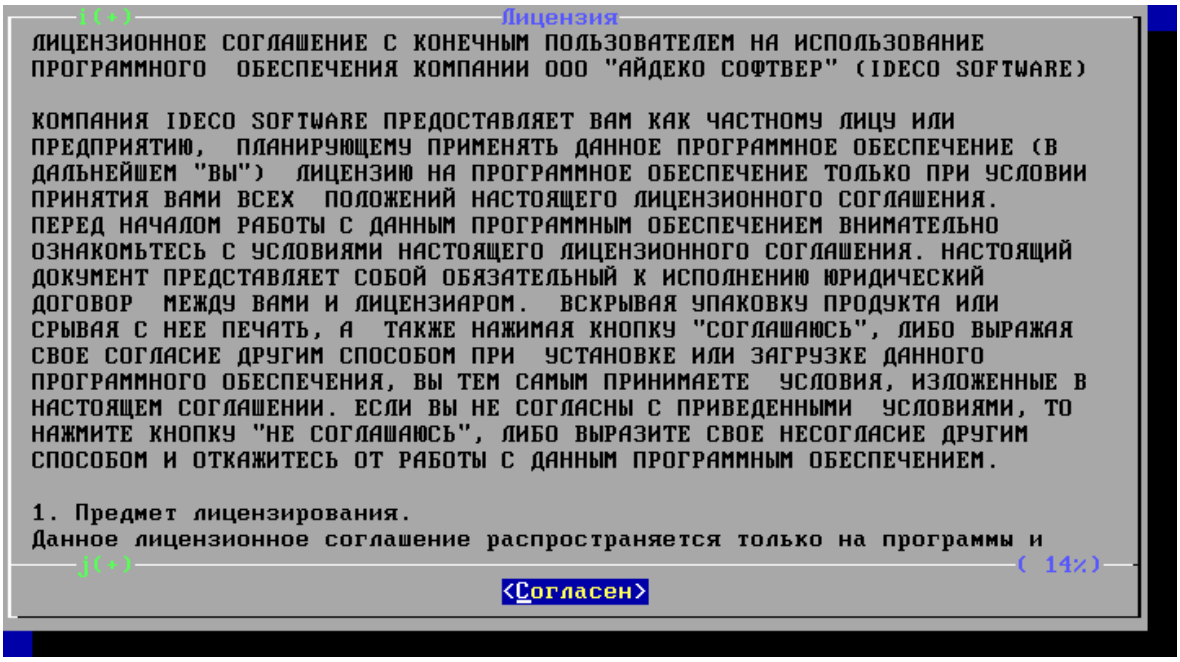
Записанный установочный диск вставьте в CD-ROM вашего сервера. Убедитесь что в BIOS выбрана загрузка с CD-ROM (если вы записали образ на DVD-диск, то в сервере должен быть установлен DVD-ROM, иначе загрузка с DVD-диска будет невозможна). При загрузке с диска будет выведено приглашение загрузчика lilo. Не нужно выбирать никаких особых опций, просто нажмите Enter на клавиатуре (кроме тех случаев если памяти более 4Гб необходимо вводить setupbigmem, либо если ставите на виртуальную машину необходимо вводить setup100hz).



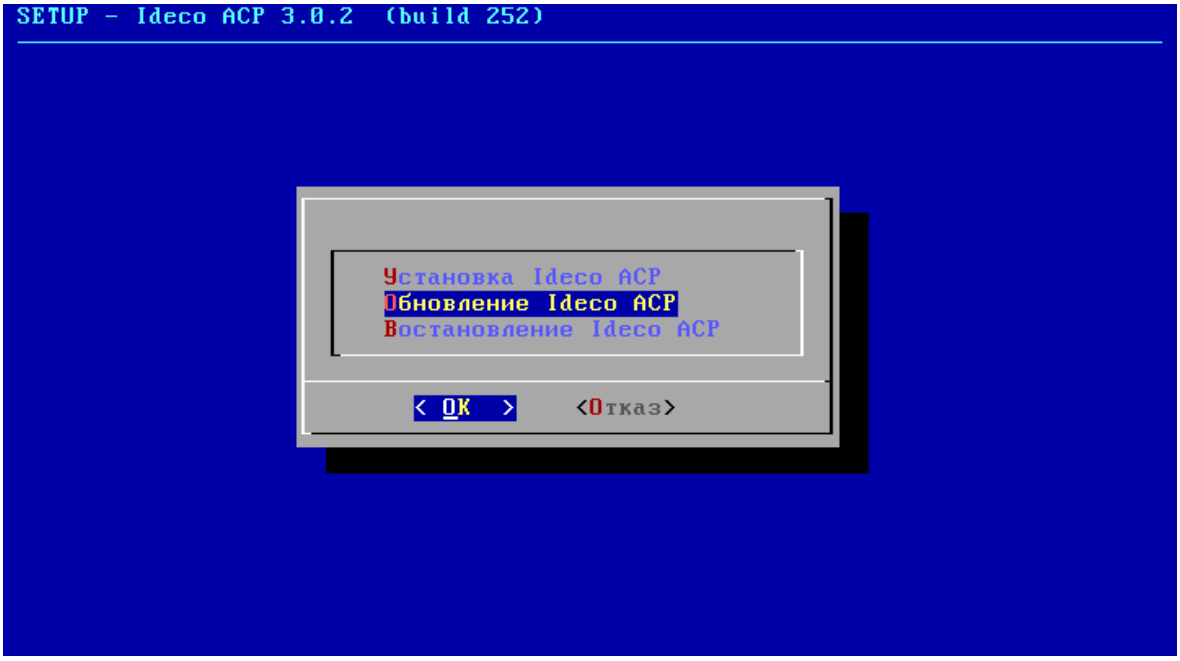
Будет загружена базовая система установки Ideco ACP. Дата на сервере как при установке так и при обновлении не должна сильно отличаться от реальной. Нажимаете Да.



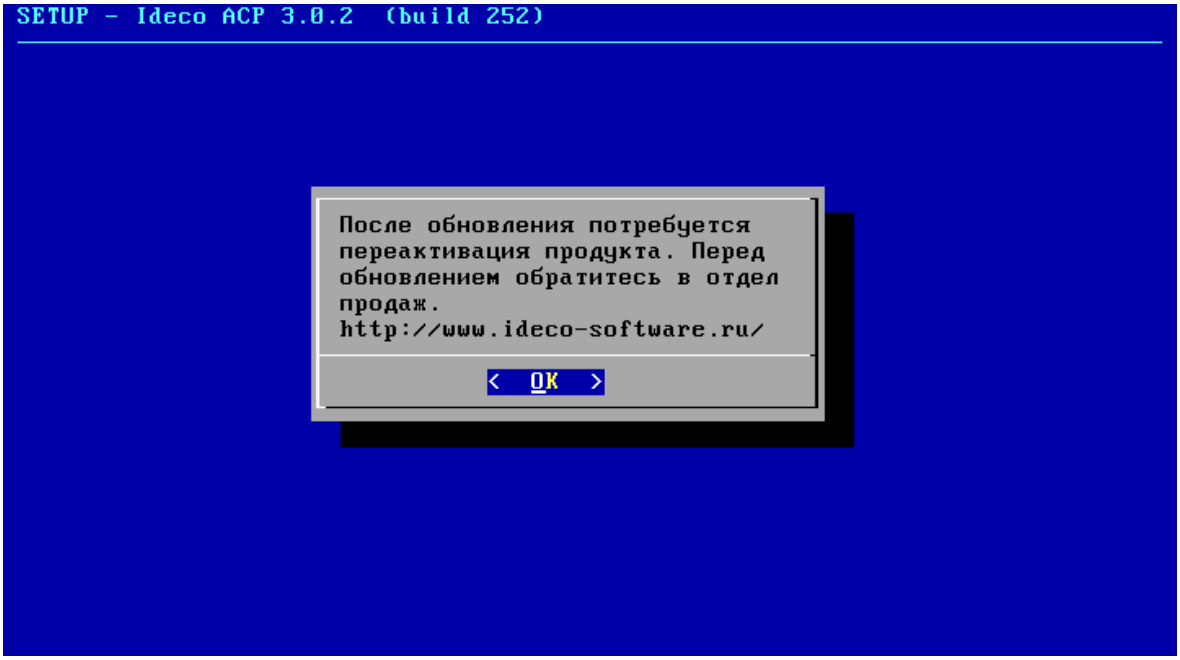
Будет показано лицензионное соглашение. Вы должны были ознакомиться с ним при первоначальной установке.



В следующем меню будет предложен выбор: Обновить Ideco ACP или установить заново, нужно выбрать пункт "Обновление Ideco ACP" а не установку заново. Будьте внимательны.

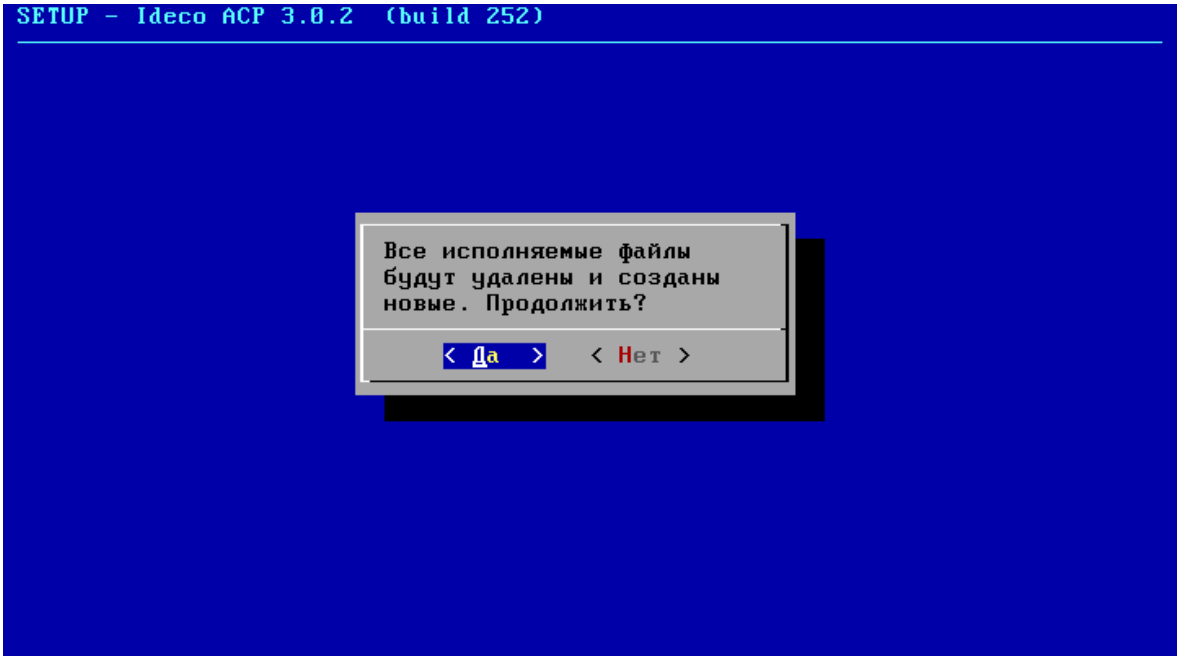


При обновлении с более ранних версий продукта, например таких как Ideco ACP 2.5.11, потребуется заново активировать продукт. Обязательно свяжитесь с отделом продаж перед обновлением, так как в этом случае вы переходите с использования одной лицензии на другую. Если же вы обновляете более старый билд Ideco ACP 30, например билд 242 на 252, то повторной активации не потребуется.

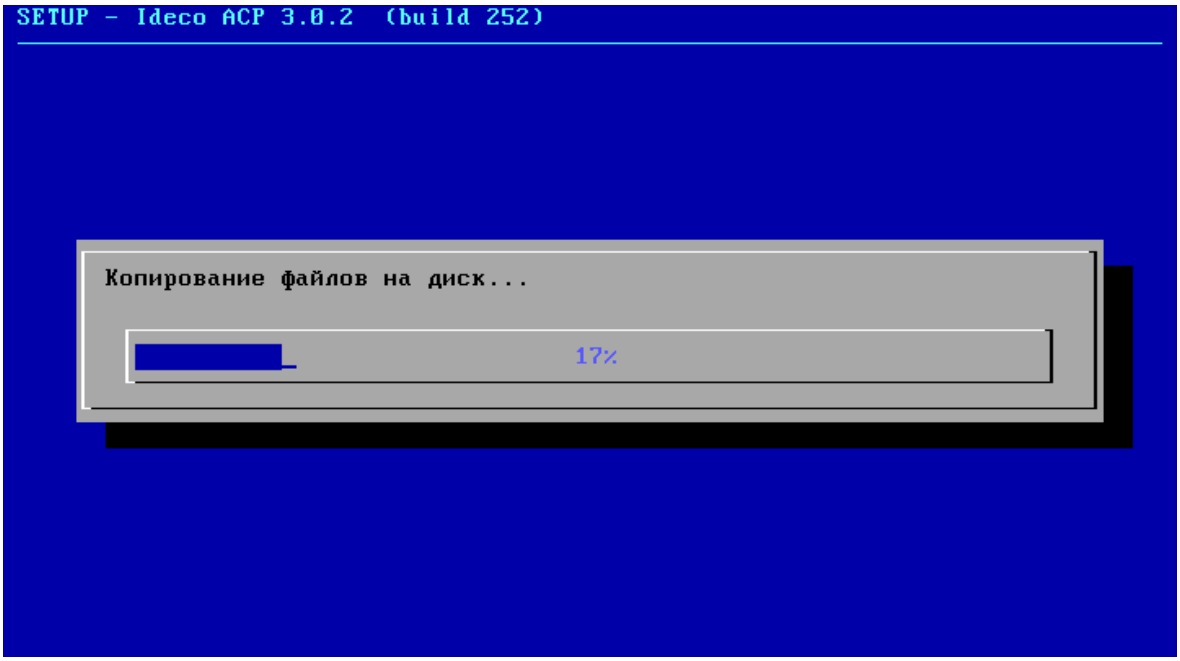


В процессе обновления заменяются старые версии всех системных файлов на новые с диска. Наработанные вами данные на сервере (контент-сайтов, содержимое FTP-сервера, статистика и т.д.) задеты не будут. Конфигурационные файлы будут обновлены при первой загрузке обновленного сервера. Об этом вас предупреждает система, нажимаете Да, после чего процесс становится

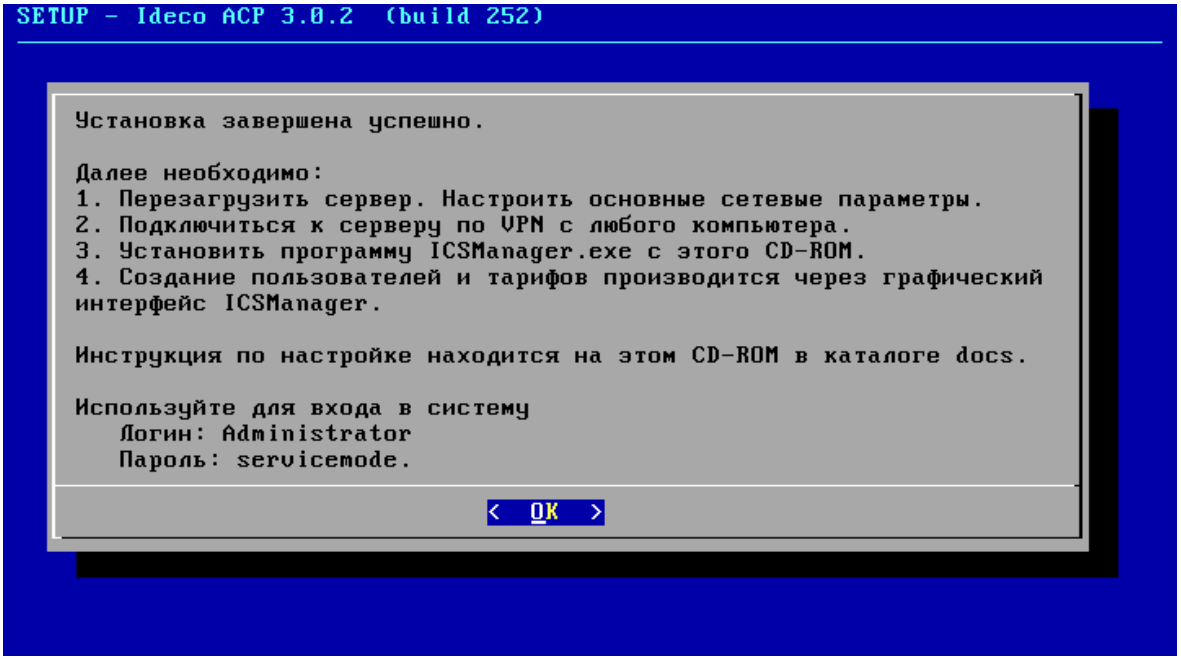
необратимым и полностью автоматическим.



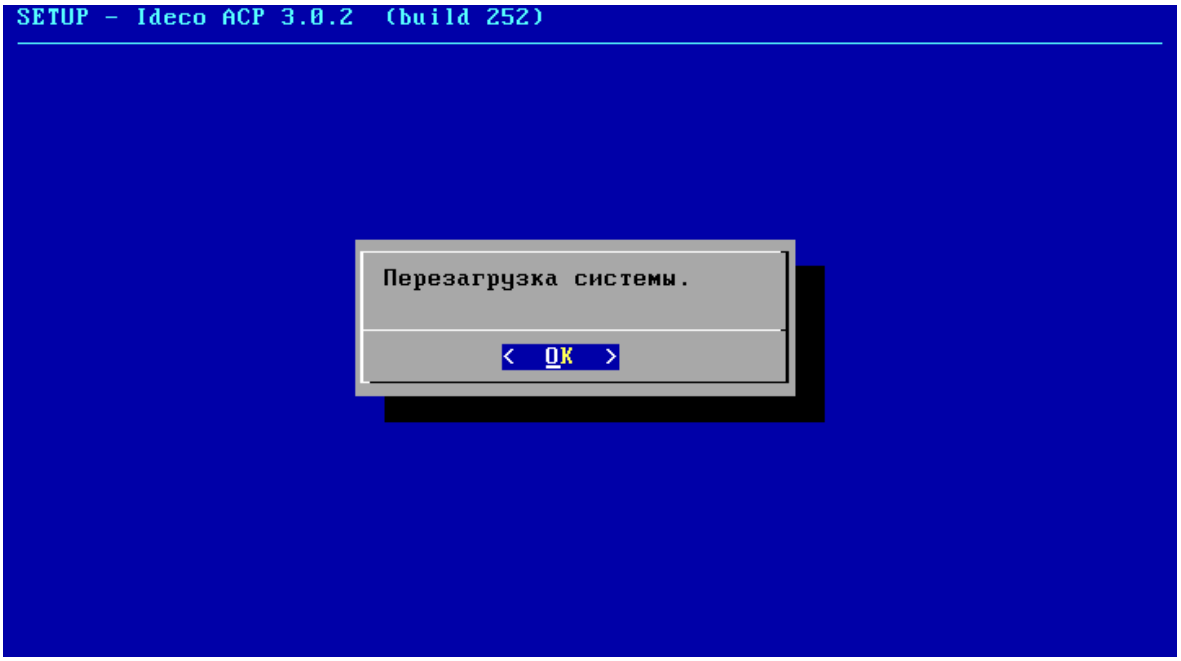
Процесс обновления файлов может занять от нескольких минут до получаса. Вашего вмешательства не требуется.



Будет выведено сообщение о завершении процесса обновления. Если вы меняли пароль на вход в локальное меню, то он останется прежним.



Перезагрузка сервера начнется сразу после того как вы нажмете ОК.



При загрузке системы следите чтобы все запускаемые и реально используемые вами сервисы на Ideco были запущены со статусом **[OK]**. Если при загрузке возникли какие либо ошибки - обратитесь в службу технической поддержки.

Часть V

5 Администрирование

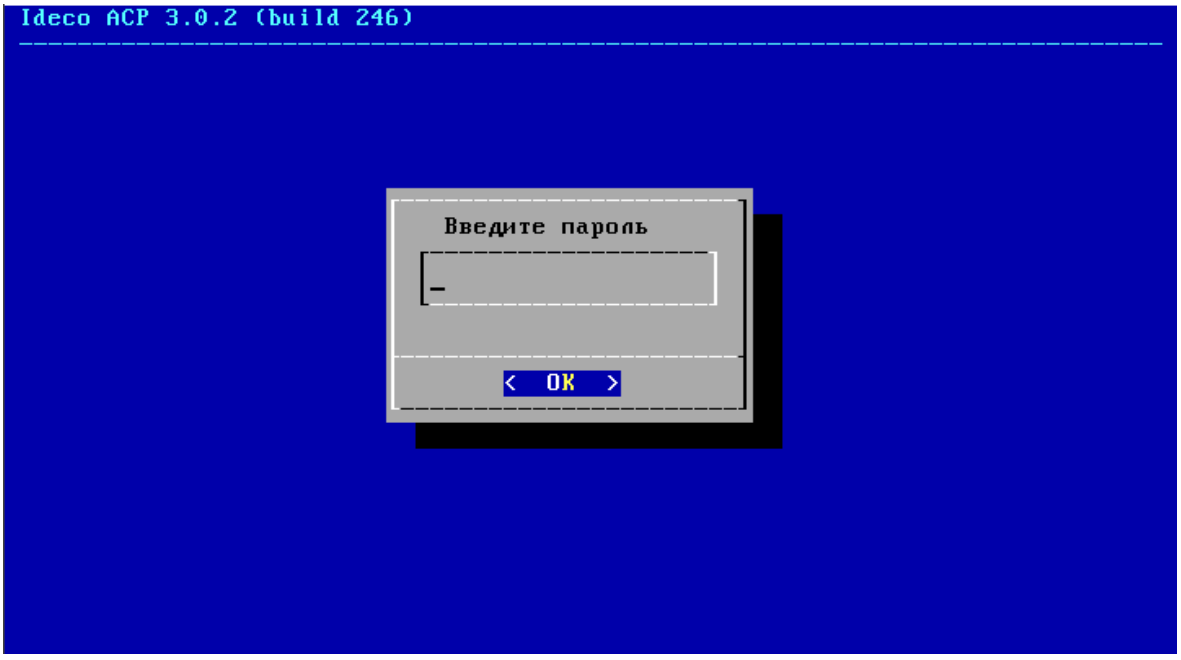
Администрирование сервера состоит из двух частей:

- **Локальная консоль сервера** предназначена для задания глобальных параметров сервера Ideco ACP и для проведения его сервисного обслуживания. Подробнее 129 ..
- **ACP Manager** предназначен для управления пользователями, редактирования тарифных планов, редактирования встроенного Firewall, просмотра статистики, построение отчетов и другого. Подробнее 178 ..

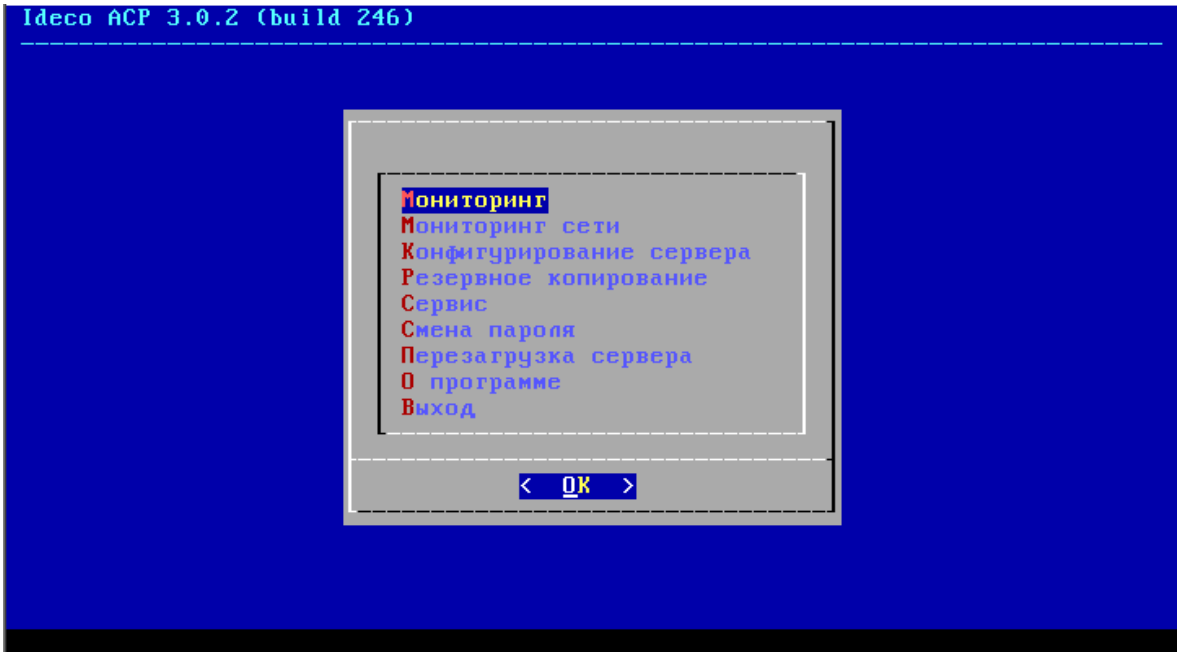
5.1 Локальная консоль сервера

Локальная консоль сервера предназначена для задания глобальных параметров сервера Ideco ACP и для проведения его сервисного обслуживания. Использование локальной консоли необходимо, например, для удаления старой статистики посещений src-dst, очистки почтовых ящиков в случае необходимости, резервного копирования БД и конфигурационного файла сервера. Кроме того, в локальной консоли можно просмотреть текущее состояние сервера, перезагрузить систему и другое.

После первоначальной установки сервера, а также при смене провайдера необходимо сконфигурировать сервер. Для этого, введите пароль.



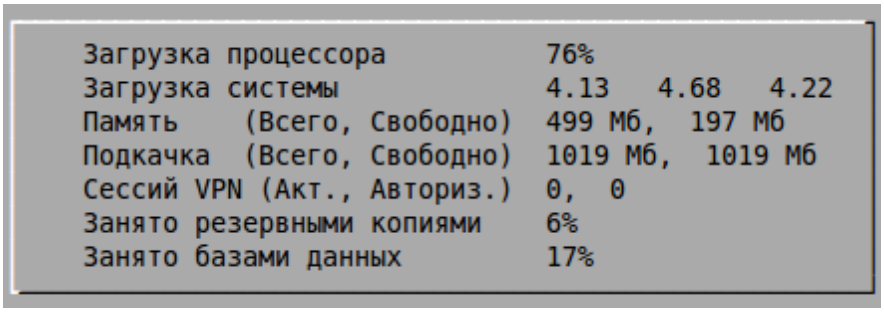
Пароль по умолчанию – servicemode. После ввода пароля доступно главное меню конфигурирования сервера.



Примечание: Доступ к локальной консоли можно получить удаленно, если заранее в ней включить параметр "Разрешить управление файлами по SSH". Подробнее см. Безопасность 145.

5.1.1 Мониторинг

Выбрав этот пункт меню можно отобразить текущее состояние сервера:



- Загрузка процессора
- Загруженность самой системы (за последнюю минуту, 5 минут и 15 минут соответственно)
- Загруженность памяти
- Загруженность раздела подкачки
- Количество подключенных пользователей (активных и подключающихся)
- Занятость диска для БД и диска для резервных копий

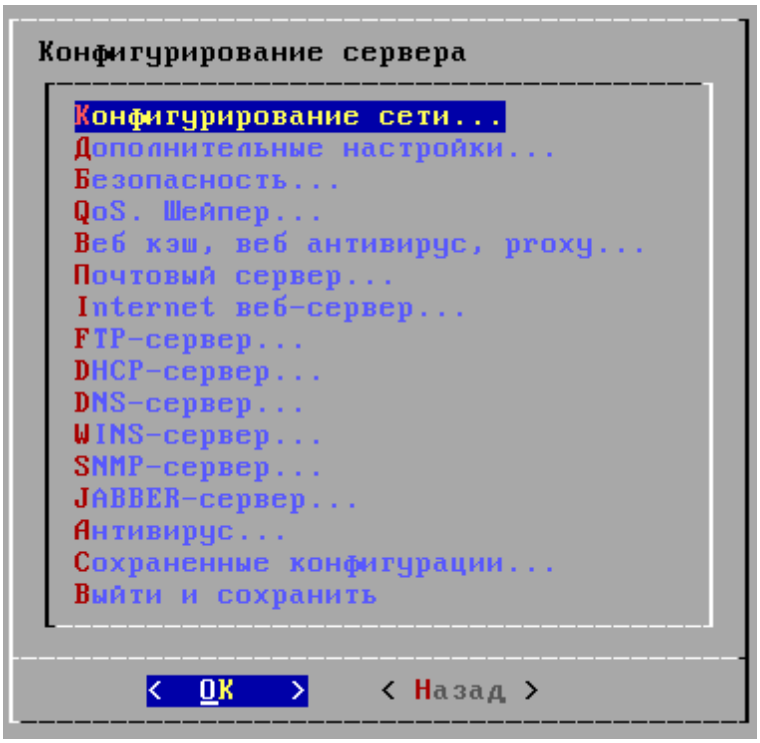
5.1.2 Мониторинг сети

Выбрав этот пункт меню можно отобразить текущее состояние сети:

Интерфейс	Получено Кбит/с	Отправлено Кбит/с	Получено Пакетов/с	Отправлено Пакетов/с	Потери Пакетов/с
Leth1	4279	1331	573	439	0
Eeth4_	0	0	0	0	0
Eeth8	489	4214	281	476	0
Eppp7	0	0	0	0	0

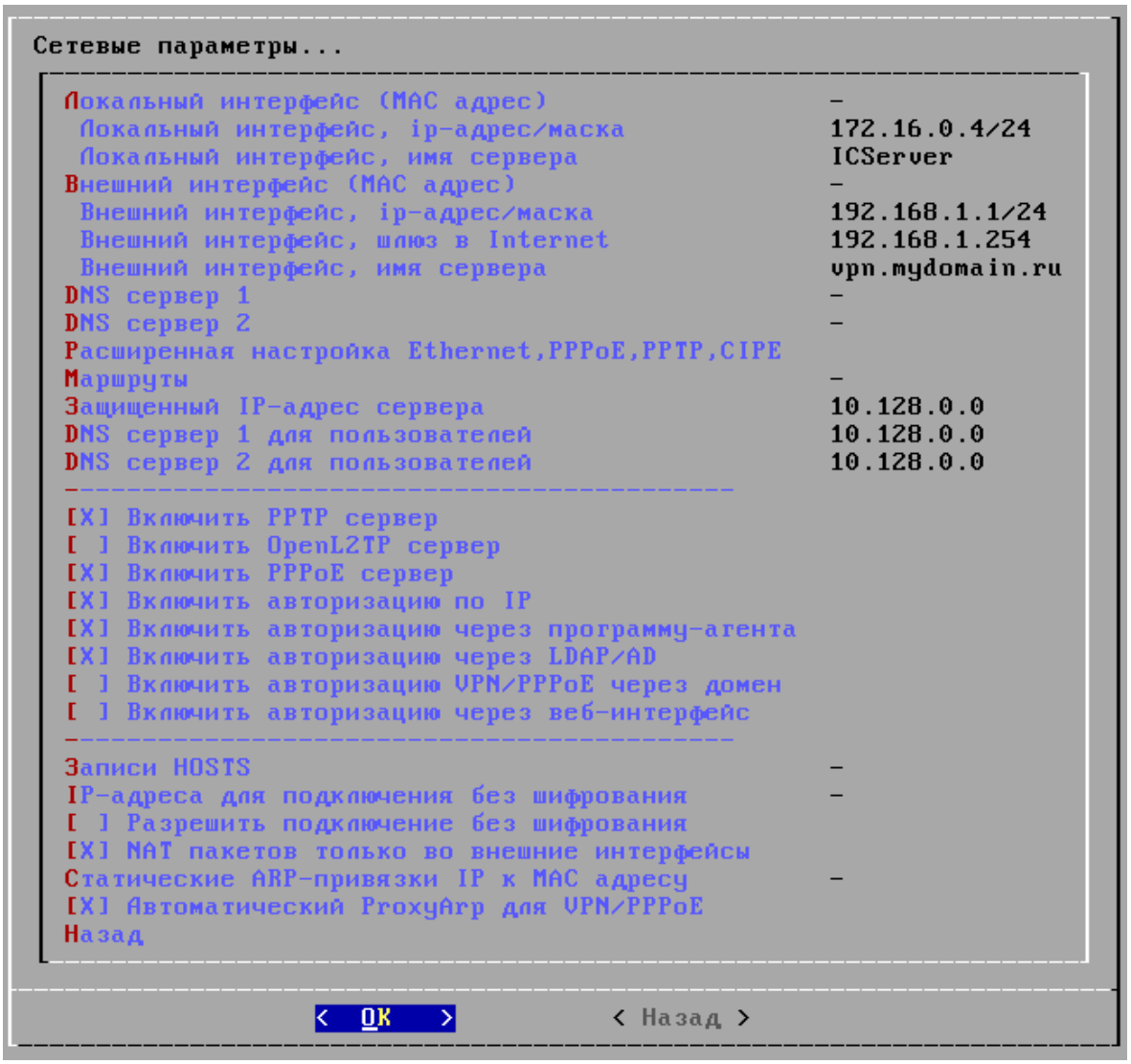
Статистика ведётся по всем интерфейсам как по количеству пакетов так и в килобитах.

5.1.3 Конфигурирование сервера



С помощью этого меню можно настроить сетевые параметры, включить или выключить дополнительные сервисы (DCHP, DNS, шейпер и другие), установить параметры, связанные с безопасностью, загрузить или сохранить конфигурацию.

5.1.3.1 Конфигурирование сети



Локальный интерфейс (MAC адрес) – нажмите Enter и выберите сетевой адаптер, подключенный к локальной сети. На экране отобразится список MAC-адресов обнаруженных сетевых карт. Если вы не знаете, какая сетевая карта к какой сети подключена, то выберите любую. После неудачной проверки связи командой ping из локальной сети, выберите другую сетевую карту для локального интерфейса или поменяйте местами кабеля, подключенные к сетевым картам.

Локальный интерфейс, IP-адрес/маска – укажите IP-адрес настраиваемого сервера в локальной сети. К этому адресу будут подключаться пользователи. Например, если у вас сеть "192.168.1.x", то укажите адрес "192.168.1.254/255.255.255.0". По умолчанию, значение "10.0.0.1/255.255.255.0".

Локальный интерфейс, имя сервера – обязательно укажите имя сервера в вашей локальной сети, например, "vpn.myorg". Если прописать это имя на локальном DNS или разрешить доступ ко внутреннему DNS из локальной сети, то можно заходить на внутренний сайт по этому имени сервера, а не по IP-адресу.

Внешний интерфейс (MAC адрес) – нажмите Enter и выберите сетевой адаптер,

подключенный к вашему провайдеру. На экране отобразится список MAC-адресов обнаруженных сетевых адаптеров.

Внешний интерфейс, IP-адрес/маска – укажите реальный IP-адрес, который вам выдал Интернет провайдер. От этого адреса пользователи будут выходить в Интернет, и к этому адресу будут подключаться удаленные пользователи по VPN.

Внешний интерфейс, шлюз в Internet – укажите шлюз вашего провайдера.

Внешний интерфейс, имя сервера – укажите реальное доменное имя вашего сервера в Интернет. Если у вас нет зарегистрированного имени, то попросите провайдера зарегистрировать имя третьего уровня. Если зарегистрировать имя нет возможности, то укажите любое несуществующее имя, например "vpn.mydomain". Подробнее о регистрации имен в зоне .ru см. на сайте http://www.nic.ru.

DNS сервер 1 – укажите первый DNS вашего провайдера.

DNS сервер 2 – укажите второй DNS вашего провайдера или адрес открытого внешнего DNS.

Расширенная настройка интерфейсов ETHERNET,PPPoE,PPTP, CIPE...

Подробное конфигурирование и создание дополнительных интерфейсов, задание дополнительных параметров.

Маршруты – если у вас многосегментная сеть с маршрутизаторами, то укажите сетевые маршруты. Например, если сервер в сегменте "10.33.2.x" с маршрутизатором "10.33.2.1", то укажите "10.0.0.0/255.128.0.0 10.33.2.1". Здесь также можно указать маршруты по адресу источника.

Защищенный IP-адрес сервера – адрес сервера внутри защищенных соединений, по умолчанию – "10.128.0.0". Адрес доступен только для авторизованных пользователей.

DNS сервер 1 для пользователей – укажите первый DNS, который будет выдан пользователям. По умолчанию – "10.128.0.0" для использования встроенного кэширующего DNS.

DNS сервер 2 для пользователей – укажите второй DNS, который будет выдан пользователям. Это может быть, например, DNS локальной сети. По умолчанию – "10.128.0.0", для использования встроенного кэширующего DNS.

Включить PPTP-сервер – Позволяет пользователям подключаться к серверу (авторизоваться) по протоколу PPTP (VPN). Включен по умолчанию. Этот способ авторизации является наиболее предпочтительным. VPN-сервер будет "слушать" подключения на локальном сетевом интерфейсе Ideco ACP.

Включить PPPoE-сервер – Позволяет пользователям подключаться по протоколу PPPoE. Это возможно только в пределах одного Ethernet-домена. Для сети с маршрутизаторами такой способ подключения использовать нельзя.

Включить авторизацию по IP – Включить возможность прямого выхода в Интернет без установки виртуального соединения. Этот способ обеспечивает меньшую безопасность чем PPTP или PPPoE . Многие устройства могут подключаться по протоколу PPPoE, и если это возможно, то лучше использовать именно его.

Включить авторизацию через программу-агента – Включить возможность авторизации через программу-агент под Windows.

Включить авторизацию через LDAP/AD – Включить возможность авторизации пользователей через отдельный LDAP-сервер или через контроллер домена Windows посредством сервиса Active Directory.

Включить авторизацию VPN/PPPoE через домен - Включить возможность авторизации VPN/PPPoE для пользователей импортированных из Active Directory (необходимо чтобы Ideco вошёл в домен).

Включить авторизацию через веб-интерфейс - Включить возможность авторизации через веб-интерфейс (любой запрос неавторизованного пользователя через браузер будет перенаправляться на страницу авторизации).

HOSTS – Нажмите Enter для добавления записей типа "A" для встроенного DNS сервера.

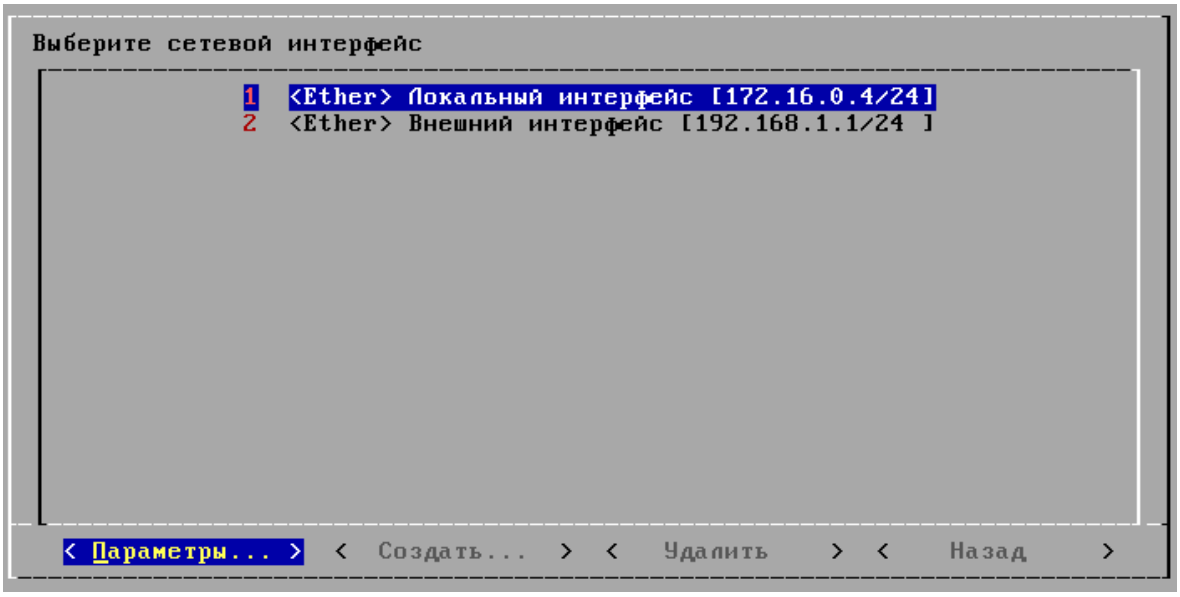
IP-адреса для подключения без шифрования – укажите IP-адреса для подключения без использования алгоритма шифрования MPPE. Это необходимо для подключения Pocket PC и стандартных BSD клиентов без расширения MPPE. Передача данных по VPN-каналу будет производиться без шифрования, поэтому пользователи, подключающиеся по VPN к этому адресу, должны быть предупреждены, что при просмотре статистики их пароль пройдет по сети в открытом виде, поэтому статистику лучше просматривать, подключившись на стандартный IP-адрес сервера с любого другого компьютера.

NAT пакетов только во внешние интерфейсы – Производить подмену адреса (NAT) только для соединений через внешние интерфейсы. При этом, для соединений через локальные интерфейсы будет работать обычная маршрутизация (если включена).

Статические ARP-привязки IP к MAC-адресу – Здесь можно указать список статических ARP-привязок. При обращении к этим IP-адресам сервер не будет использовать ARP-запросы. Это позволяет исключить ряд атак с подстановкой адреса.

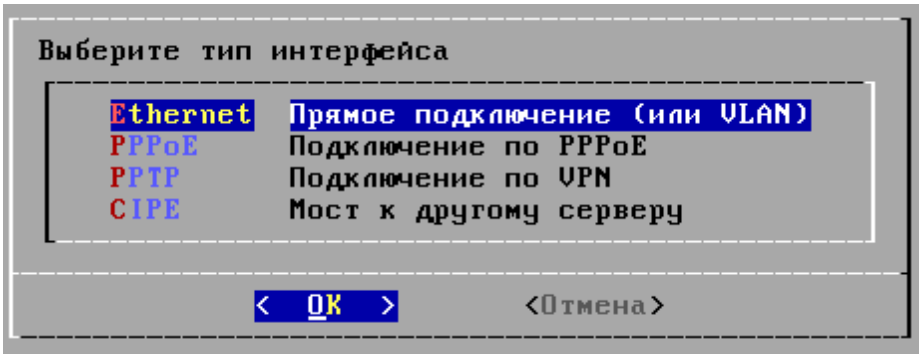
Автоматический ProxyArp для VPN/PPPoE – эффект присутствия в Ethernet-сети при подключении по VPN/PPPoE. Если у пользователя стоит галочка "Разрешить VPN из Интернет" и в качестве ip-адреса указан адрес из локальной сети сервера, то после подключения при arp-запросе из локальной сети гейт будет отвечать (будет работать, например, команда ping).

5.1.3.1.1 Расширенная настройка Ethernet,PPPoE,PPTP,CIPE



Данный раздел предназначен, для создания дополнительных сетевых интерфейсов. Также позволяет получить доступ к более полным настройкам сетевых интерфейсов.

При выборе кнопки **<Создать>**, появится следующий диалог:



Выберите тип интерфейса, которые хотите создать. Если необходимо использовать на сервере более двух сетевых карт, создайте в этом диалоге новый Ethernet-интерфейс, и выберите MAC-адрес нужной карты из списка. Кроме того, имеется возможность создавать виртуальный Ethernet-интерфейс, назначив ему номер 802.1q VLAN ID в параметрах. Если Ваш провайдер требует подключения по VPN (PPTP) или PPPoE, создайте соответствующие интерфейсы здесь. Для организации шифрованного виртуального туннеля между серверами настоятельно рекомендуется использовать CIPE-интерфейс.

Общие параметры интерфейсов

Роль – для локальных интерфейсов, укажите "Local", для внешних – "External".

Основной – Укажите, какой из внешних интерфейсов должен быть основным. На первом IP-адресе основного внешнего интерфейса будет работать внешний WEB-сервер.

Доменное имя – Укажите доменное имя, соответствующее первому IP-адресу

интерфейса. Если нет зарегистрированного доменного имени – укажите вымышленное, например, "iface-domain.myorg".

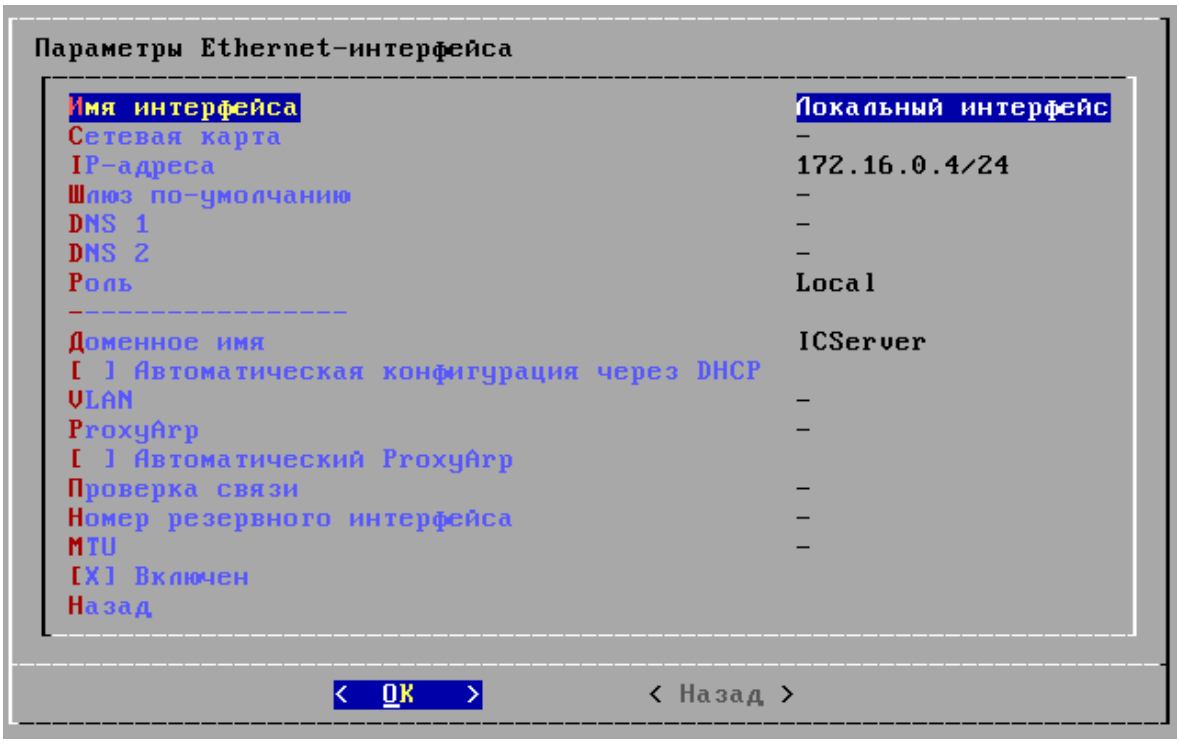
Проверка связи – Укажите список адресов для проверки связи через этот интерфейс. Эта возможность необходима для работы автоматического выбора провайдера. Укажите IP-адрес или "IP-адрес:порт". В первом случае связь будет проверяться с помощью ICMP-Echo пактов, во втором случае – проверкой возможности соединиться на указанный TCP-порт. Также есть возможность указать конкретный IP-адрес источника для проверок – для этого укажите его перед адресом назначения, например, "10.0.0.1 10.0.0.2:80".

Номер резервного интерфейса – Укажите номер интерфейса, который должен быть использован вместо конфигурируемого интерфейса в случае, если отсутствует связь со всеми, указанными в параметре "Проверка связи". В этом случае, все маршруты через конфигурируемый интерфейс будут заменены маршрутами через резервный интерфейс.

MTU – Укажите максимальное значение MTU для интерфейса.

Включен – Для того чтобы задействовать интерфейс в системе – установите этот флажок.

Параметры Ethernet-интерфейса



Имя интерфейса – Задайте имя интерфейса. Это имя будет использоваться веб-интерфейсе и локальной консоли.

Сетевая карта – Нажмите Enter и выберите сетевой адаптер, подключенный к нужной сети. На экране отобразится список MAC-адресов обнаруженных сетевых карт. Если вы не знаете, какая сетевая карта к какой сети подключена, то выберите любую. После неудачной проверки связи командой ping, выберите другую сетевую карту для этого интерфейса.

IP-адреса – В этом пункте можно назначить адаптеру один или несколько IP-адресов. Маска подсети указывается после каждого IP-адреса через символ "/".

Шлюз по-умолчанию – укажите шлюз по умолчанию для интерфейсов к провайдеру.

DNS 1 и DNS 2 – Укажите первый и второй DNS, доступные через этот интерфейс.

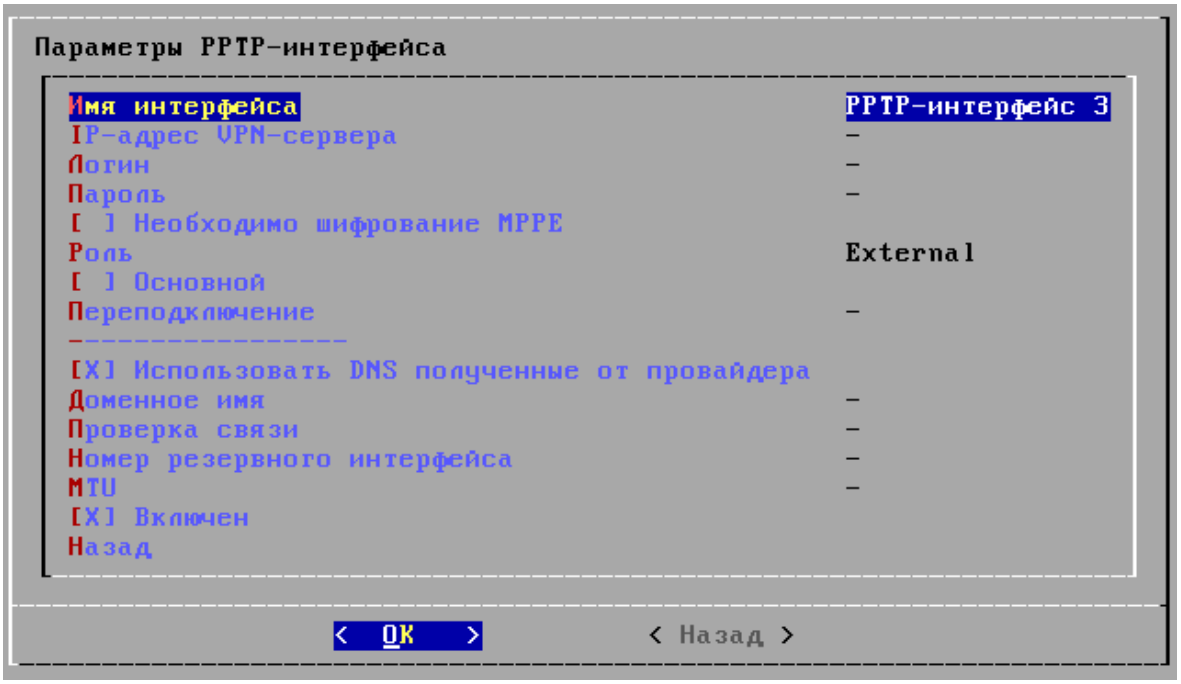
VLAN – Для того чтобы создать виртуальный 802.1q интерфейс, укажите VLAN ID в этом поле. В этом случае, интерфейс будут работать только с тегированными пакетами через выбранную сетевую карту. На одном физическом Ethernet-интерфейсе может быть сконфигурировано несколько VLAN-интерфейсов.

ProxyArp – Если провайдер выдал несколько реальных IP-адресов, не обеспечив, при этом, их маршрутизацию, то можно указать список дополнительных внешних IP-адресов, на которые сервер должен отвечать ARP-ответами. В качестве элемента списка можно указать диапазон IP-адресов через тире. Например, 192.168.1.3-192.168.1.10. С точки зрения провайдера, будет казаться, что компьютеры с этими IP-адресами находятся в одном Ethernet-сегменте с сервером.

Примечание: Эти IP-адреса не будут назначены самому серверу, но их можно будет использовать для пользователей без NAT, указав им эти IP-адреса. Для большего удобства, можно создать отдельный пул из этих IP-адресов и назначать серверным логинам адреса из этого пула.

Автоматический ProxyArp – Сервер будет отвечать на ARP-запросы, если IP-адрес доступен на другом интерфейсе.

Параметры PPTP-интерфейса



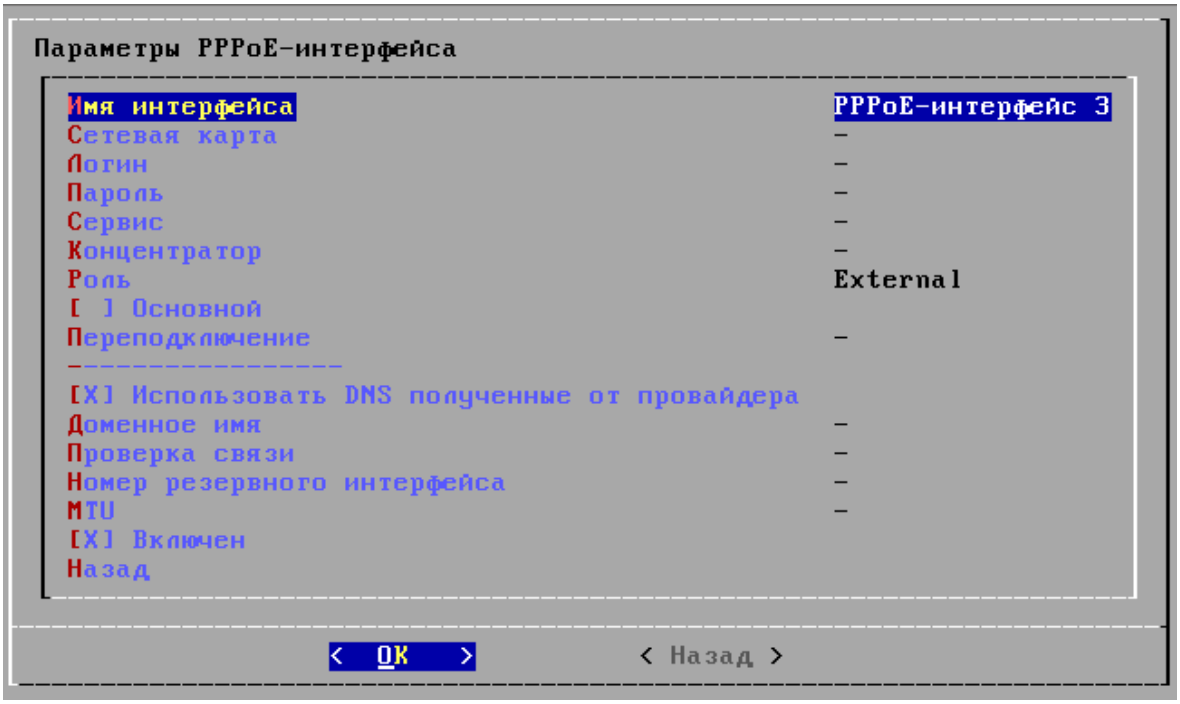
IP-адрес – Укажите IP-адрес сервера для подключения к провайдеру.

Логин и Пароль – Укажите логин и пароль. Указаны в договоре с провайдером.

Необходимо шифрование MPPE – Установите этот флажок, если для подключения к провайдеру требуется шифрование.

Переподключение – Укажите часы, когда необходимо принудительно произвести подключение интерфейса. Это может потребоваться в тех случаях, когда провайдер считает трафик по дневному/ночному режиму в зависимости от времени, в которое было произведено подключения по VPN.

Параметры PPPoE-интерфейса



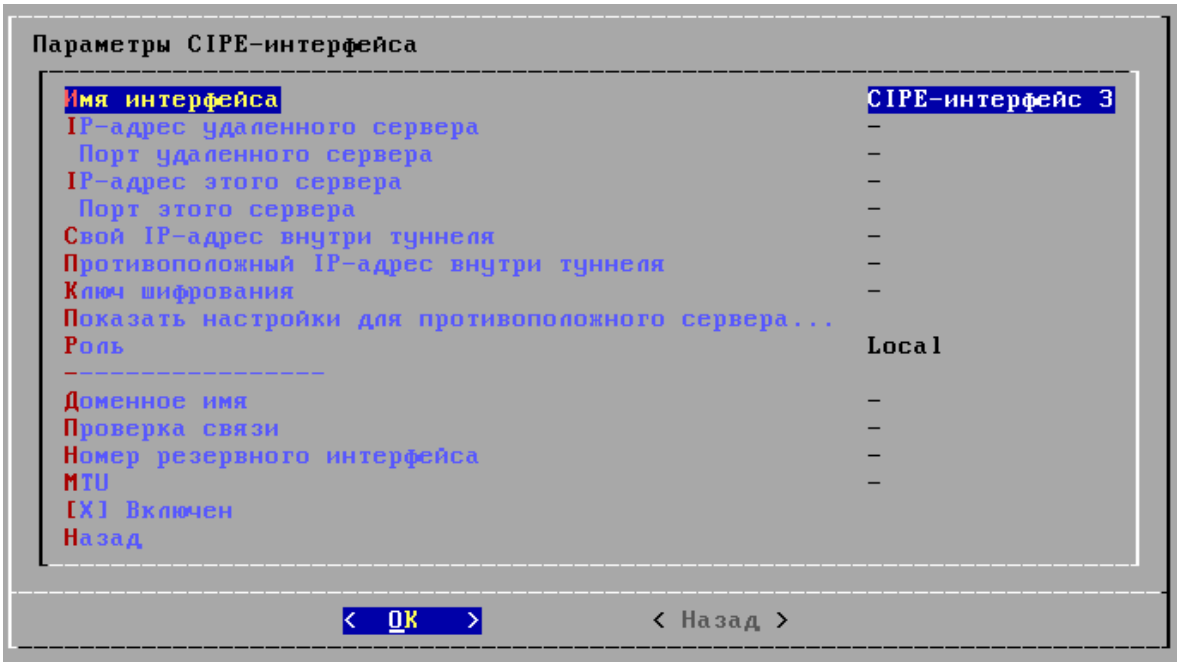
Сетевая карта – Укажите сетевую карту, через которую необходимо подключаться по PPPoE.

Логин и Пароль – Укажите логин и пароль. Указаны в договоре с провайдером.

Сервис и Концентратор – Укажите эти параметры, только если они присутствуют в договоре на подключение к провайдеру. Иногда в договоре эти параметры указываются через косую черту.

Переподключение – Укажите часы, когда необходимо принудительно произвести подключение интерфейса. Это может потребоваться в тех случаях, когда провайдер считает трафик по дневному/ночному режиму в зависимости от времени, в которое было произведено подключения по PPPoE

Параметры CIPE-интерфейса



IP-адрес удаленного сервера и порт – Укажите IP-адрес и порт удаленного сервера к которому производится подключение.

IP-адрес этого сервера и порт – Укажите IP-адрес и порт этого сервера с которых будет производиться подключение.

Свой IP-адрес внутри туннеля – Укажите IP-адрес этого сервера внутри туннеля.

Противоположный IP-адрес внутри туннеля – Укажите IP-адрес противоположного сервера внутри туннеля.

Ключ шифрования – в этом меню можно создать, просмотреть или ввести ключ шифрования, созданный на другом сервере. Для того чтобы серверы соединились, необходимо чтобы ключ совпадал не обеих сторонах. На одном сервере необходимо создать ключ, а на другом ввести такой же.

Показать настройки для противоположного сервера – Выбрав этот пункт меню, можно просмотреть настройки, которые необходимо сделать на противоположном сервере, рекомендуется их переписать на бумагу.

5.1.3.1.2 Маршрутизация по протоколу и маршруту

Для перенаправления сетевых пакетов с учетом протокола, маршрута, а так же базовых функций балансировки канала применяется система маршрутизации.

Введите маршрут в формате:

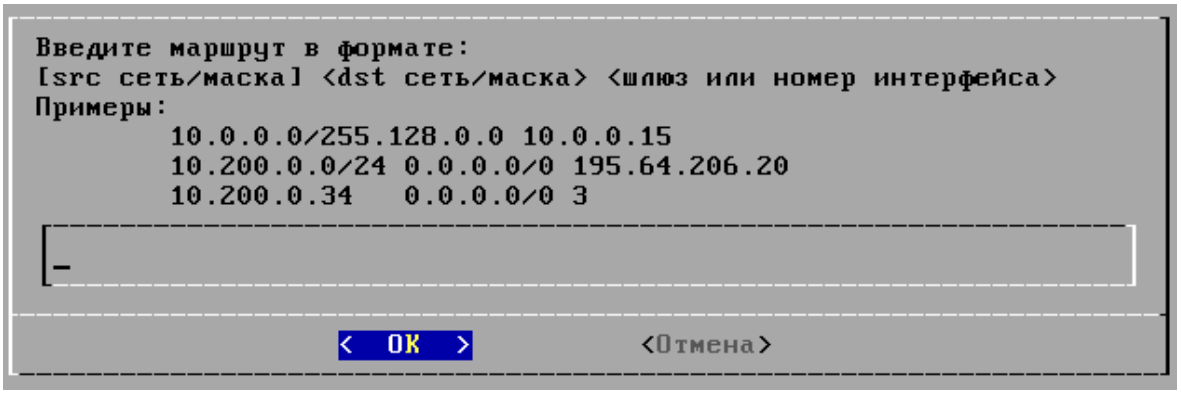
[src сеть/маска[:порт]] <dst сеть/маска[:порт]> <шлюз или номер интерфейса> [опции]

Параметры в квадратных скобках являются обязательными, параметры в угловых скобках можно опустить.

В качестве опций можно указать через пробел:

- Протокол: TCP, UDP, GRE или ICMP
- Флаги SNAT и FORCE
- SNAT - подставлять IP адрес интерфейса от которого пользователи будут выходить в Интернет
- FORCE - маршрутизировать независимо от маски интерфейсов (использовать не рекомендуется)
- Вероятность срабатывания, например, 50% (для балансировки каналов).

Примеры:



10.0.0.0/255.128.0.0 10.0.0.15 - любой трафик идущий в подсеть 10.0.0.0/255.128.0.0 направлять на шлюз 10.0.0.15.

10.200.0.0/24 0.0.0.0/0 195.64.206.20 - любой трафик приходящий из подсети 10.200.0.0/24, идущий на любой адрес, направлять на шлюз 195.64.206.20 .

10.200.0.34 0.0.0.0/0 3 - любой трафик приходящий от компьютера 10.200.0.34 и идущий на любой адрес направлять на интерфейс №3.

10.200.0.0/24 0.0.0.0/0:80 3 TCP SNAT - весь TCP трафик подсети 10.200.0.0/24 идущий на 80 порт для любого адреса, направлять на интерфейс №3.

10.200.0.0/24 0.0.0.0/0:80 10.2.2.2 TCP SNAT - весь TCP трафик подсети 10.200.0.0/24 идущий на 80 порт для любого адреса, направлять на шлюз 10.2.2.2.

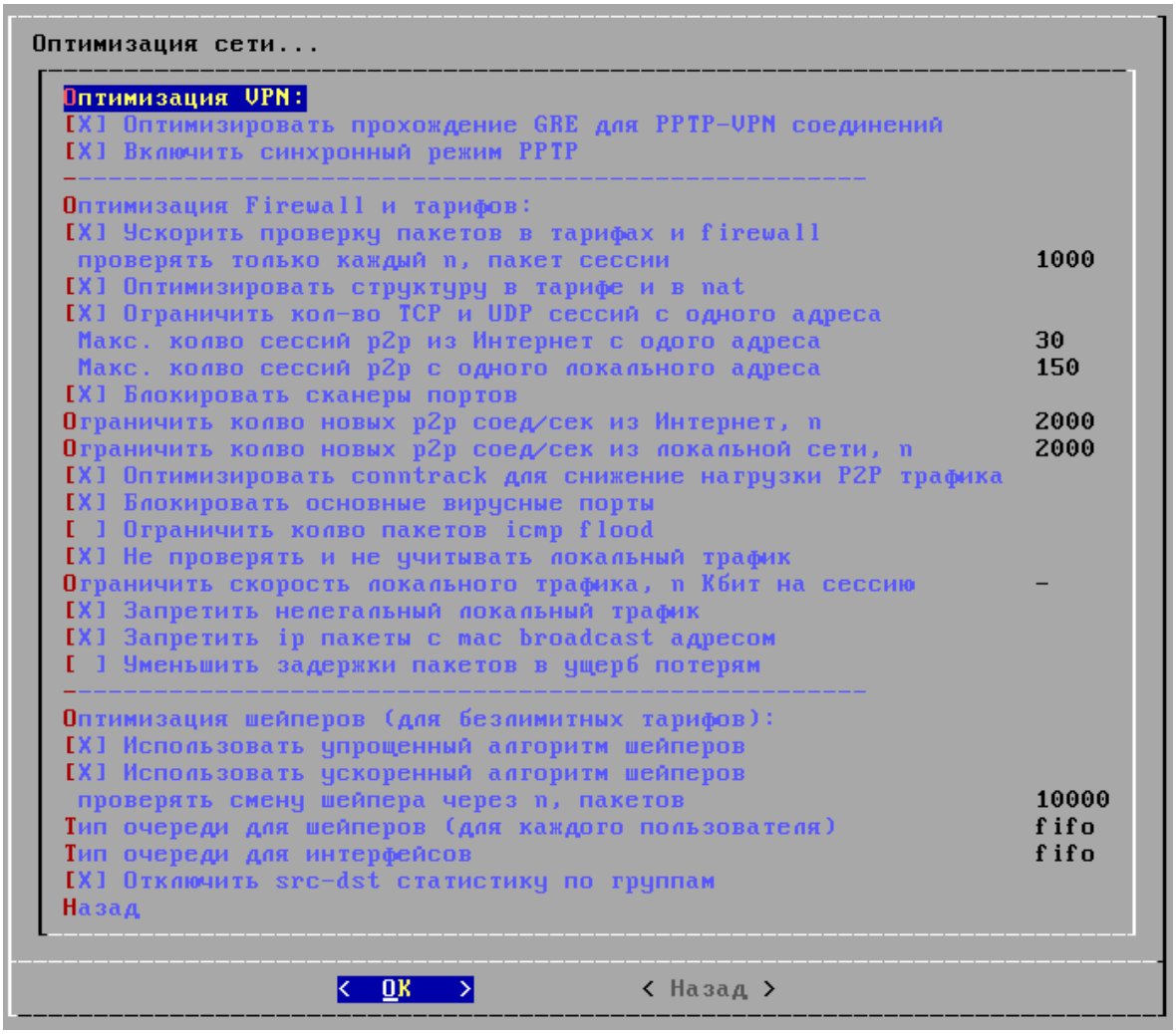
10.0.0.0/8 0.0.0.0/0 50% 3 TCP SNAT - балансировка канала. 50% TCP трафика пользователей подсети 10.0.0.0/8 будет направлено на интерфейс №3.

192.168.1.0/24 0.0.0.0/0 50% 10.0.0.4 SNAT - балансировка канала. 50% трафика пользователей подсети 192.168.1.0/24 будет направлено на шлюз 10.0.0.4.

Примечание: **!Важно**: Если маршрутизировать нужно на Ethernet интерфейс, то маршрут прописывается относительно **адреса шлюза**. Если же маршрутизируется на виртуальный (PPTP, PPPoE, CIPE, OpenVPN, IPSec), то маршрут прописывает

относительно **номера интерфейса**.

5.1.3.2 Оптимизация сети



Ограничить количество сессий с одного адреса – Обычный пользователь и сервер не устанавливают более 150 соединений одновременно. Большое количество соединений означает, что компьютер заражен вирусами или adware программами. Включение этой опции остановит большой трафик, вызванный вирусной эпидемией. Данная опция также ограничивает использование сетей peer-to-peer, так как поведение клиентов этих сетей не отличается от вирусных эпидемий. Кроме того, эта опция позволяет защитить компьютеры пользователей и сервер от отказа в обслуживании (DOS-атаки).

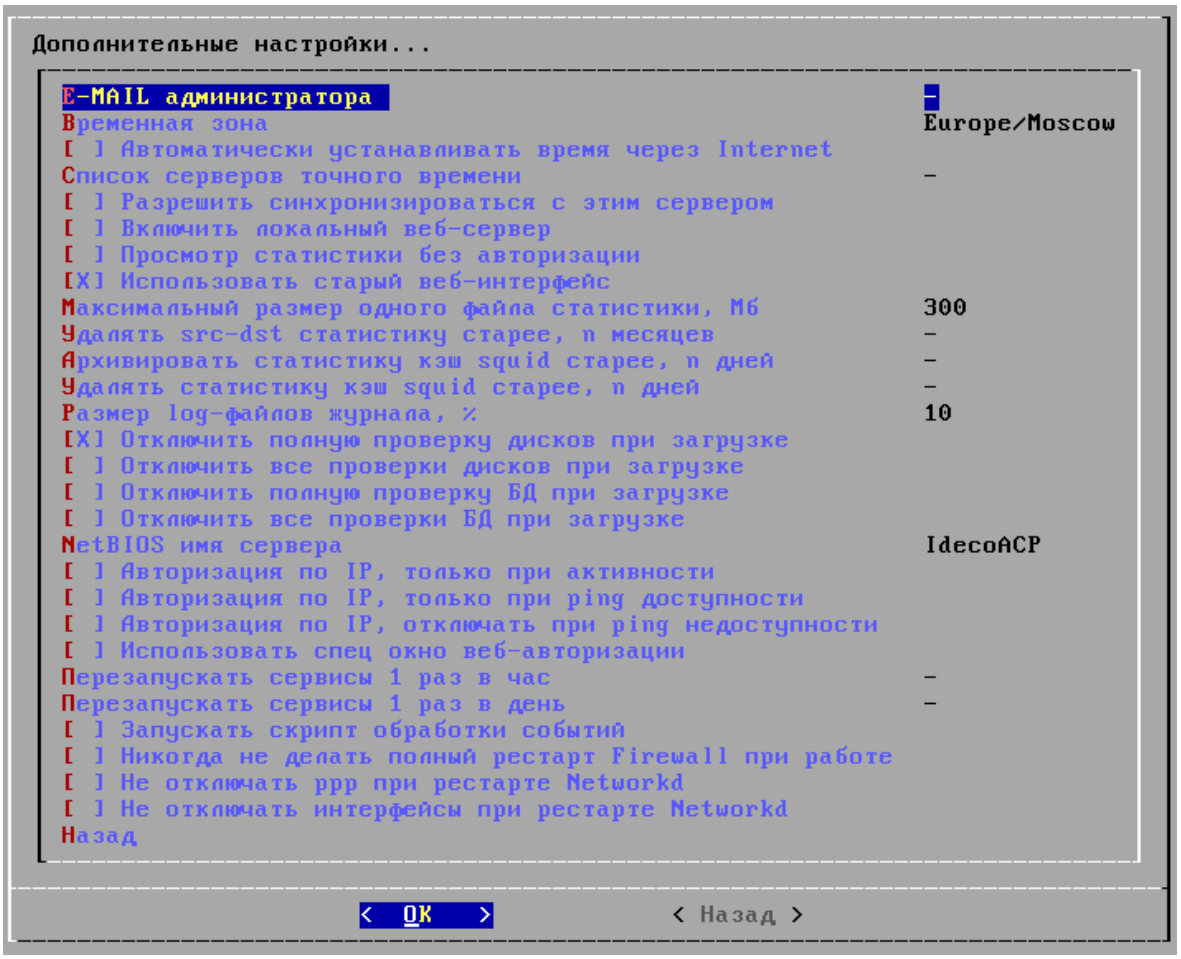
Макс. количество сессий из Интернет – Укажите максимальное количество соединений, которое можно будет произвести с одного адреса в Интернет.

Макс. количество сессий из локальной сети – Укажите максимальное количество соединений, которое можно будет произвести с одного адреса локальной сети (от одного пользователя).

Блокировать сканеры портов – Если будет проводиться сканирование портов локальной сети или сервера, то IP-адрес сканирующего компьютера будет отключен на несколько минут. Это позволяет блокировать поиск уязвимостей в локальной сети. Если пользователи вашей локальной сети активно используют p2p-программы (torrents), то опцию "Блокировать сканеры портов" рекомендуется выключить.

Использовать упрощенный шейпер - этот параметр задействует особый алгоритм работы шейпера в системе который сможет значительно снизить нагрузку на сервер. Включать этот параметр имеет смысл только если клиентов на которых действуют правила шейпинга (в тарифах или в firewall) больше 1000 и если в тарифах используется не более одного правила шейпинга, при том это правило должно действовать на сеть ALL (внешний траффик 0.0.0.0) Рекомендуется для использовать в крайнем случае и только крупным провайдерам. Обратитесь за консультацией в техническую поддержку.

5.1.3.3 Дополнительные настройки



E-mail администратора – укажите почтовый адрес для оповещения о системных событиях, таких как перезагрузка сервера, недостаток свободного места на диске и других. Также можно указать e-mail для отправки SMS, так как все сообщения

очень короткие и их удобно просматривать на сотовом телефоне. Можно указывать несколько e-mail адресов, разделяя их точкой с запятой. Не рекомендуется указывать адрес на внутреннем почтовом сервере, так как в случае перехода в защищенный режим (SAFE MODE), прием и отправка писем внутренней почты не работает.

Временная зона – укажите ваш временной пояс. Система автоматически произведет переход на летнее время при необходимости.

Автоматически устанавливать время через Internet – автоматическая установка точного времени на сервере с использованием серверов точного времени. Имейте в виду, что время на сервере устанавливается в соответствие с выбранной временной зоной.

Список серверов точного времени – Здесь можно указать один или несколько серверов для синхронизации времени. Можно указывать IP-адреса либо доменные имена. В таком случае будут использованы все IP-адреса для доменного имени. По умолчанию используется "pool.ntp.org".

Разрешить синхронизироваться с этим сервером – Разрешить синхронизацию с сервером времени на Ideco для пользователей локальной сети.

Включить локальный веб-сервер – включить веб-сервер на локальном интерфейсе для того чтобы пользователи могли просматривать свою статистику, менять пароль, активировать карты и т.д. Подробнее см. Личный кабинет пользователя 80.

Просмотр статистики без авторизации - позволяет пользователям заходить в личный кабинет через браузер даже если у клиент не авторизован (отключен). При такой схеме работы сайта статистики не будет использоваться защищенный адрес Ideco ACP (10.128.0.0 по умолчанию).

Использовать старый веб-интерфейс - включает использование старого веб-интерфейса локального сайта статистики, каким он был в версии 2.5.11. При включенном пункте невозможно использовать систему управления сайтом Bitrix. Подробнее 80 .. В текущей версии использовать старый веб-интерфейс не рекомендуется, если по какой то причине это потребовалось обратитесь в службу технической поддержки.

Максимальный размер одного файла статистики – обычно файл статистики src-dst по одному пользователю не превышает 100 мб. в месяц. Если файл будет больше 500 Мб, то просмотр статистики будет сильно загружать систему. Рекомендуется установить ограничение 300 Мб, так как больший объем говорит о чрезмерной активности и возможном заражении компьютера пользователя вирусами. Если объем будет превышен, то появится файл <name>.1 потом <name>.2 и так далее. Просмотреть такую статистику можно только вручную. Администратор будет предупрежден о превышении размера файла статистики.

Удалять src-dst статистику старее, n месяцев – Здесь можно указать количество последних месяцев, за которые будет храниться детализированная статистика. Если не установить этот параметр, то детализированная статистика не будет удаляться. Кок только свободного места на диске станет мало, системный администратор будет предупрежден

Архивировать статистику кэш squid старее, n дней – Здесь можно указать количество последних дней, за которые будет архивироваться детализированная статистика прокси-сервера.

Удалять статистику кэш squid старее, n дней – Здесь можно указать

количество последних дней, за которые будет храниться детализированная статистика прокси-сервера.

Размер log-файлов журнала, % – Здесь можно указать максимальный объем log-файлов на сервере в процентах от емкости диска.

Отключить полную проверку дисков при загрузке – Здесь можно указать отключение проверки дисков. Отключение не рекомендуется.

Отключить все проверки дисков при загрузке – Проверка дисков не будет выполнена при любых обстоятельствах. Отключение не рекомендуется.

Отключить полную проверку БД при загрузке – Здесь можно указать отключение проверки БД. Отключение не рекомендуется.

Отключить все проверки БД при загрузке – Проверка БД не будет выполнена при любых обстоятельствах. Отключение не рекомендуется.

NetBIOS-имя сервера - Здесь можно указать имя сервера в сети Windows.

Авторизация по IP, только при активности – При включенной опции авторизация пользователей будет проходить только при наличии трафика от компьютера пользователя. Следует отметить, что трафиком от пользователя будет считаться любой тип трафика с заданного IP в сторону Internet. К этому относятся различные программы антивирусы, обновляющие свои базы, обновления Windows и т.п. трафик не инициированный пользователем или запущенными им программами напрямую.

Авторизация по IP, только при ping доступности – При включенной опции авторизация пользователей будет проходить только при наличии ping до компьютера пользователя.

Авторизация по IP, отключать при ping недоступности – Пользователь будет отключен от сервера, как только до его компьютера пропадет ping.

Перезапускать сервисы 1 раз в час - указанные сервисы будут перезапускаться раз в час, название сервиса можно посмотреть в директории /etc/init.d

Перезапускать сервисы 1 раз в день - указанные сервисы будут перезапускаться раз в день, название сервиса можно посмотреть в директории /etc/init.d

Запускать скрипт обработки событий - скрипт используется для управления сетевым оборудованием по определенным событиям в биллинге. За более подробной информацией обратитесь в отдел технической поддержки.

Никогда не делать полный рестарт firewall при работе - если у вас много пользователей или в сети действуют сложные правила шейпинга, то возможно вам следует включить эту опцию для удобной работы пользователей.

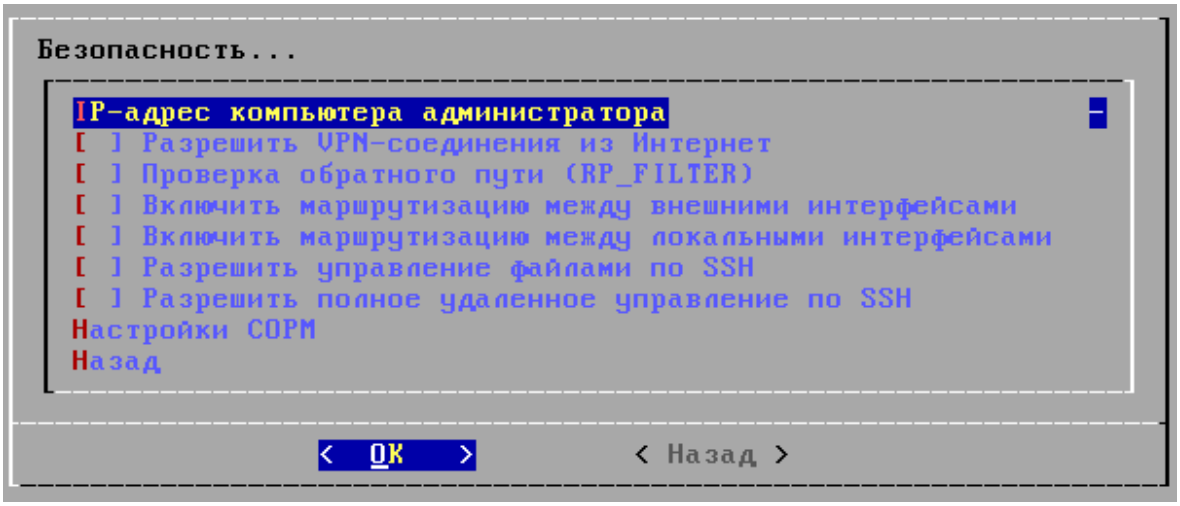
Не отключать ppp при рестарте Networkd - если в ходе работы сервера или в процессе его настройки сетевая подсистема будет перезапущена, то ppp сессии клиентов не будут разорваны. Делает работу пользователей с авторизацией по PPtP или PPPoE более прозрачной и устойчивой к изменениям на сервере. Может быть полезно если у вас много таких пользователей в сети.

Не отключать интерфейсы при рестарте Networkd - при перезапуске сетевой подсистемы сервера не будут заново инициализированы сетевые интерфейсы. Может быть полезно если инициализация интерфейсов происходит медленно, у вас много пользователей в сети или переподключение к провайдеру длится очень долго.

Список серверов для IdecoAgent – Если в локальной сети есть несколько

серверов Ideco, необходимо перечислить IP адреса локальных интерфейсов всех серверов (где используется авторизация по IdecoAgent)

5.1.3.4 Безопасность



IP-адрес компьютера администратора – Адрес компьютера, с которого можно управлять сервером без авторизации. По умолчанию административный интерфейс доступен с любого IP адреса. Если требуется, чтобы административная часть была доступна только с компьютера администратора - введите IP адрес компьютера главного администратора.

Разрешить VPN соединения из Интернет – Разрешить подключение удаленных пользователей и подразделений по VPN. Если это глобальное разрешение не установлено, то пользователи с установленным признаком "разрешить удаленное подключение", удаленно подключиться не смогут.

Проверка обратного пути (RP_FILTER) – Проверять обратный путь проходящих пакетов. Ответные пакеты должны направляться в тот же интерфейс, из которого поступил запрос.

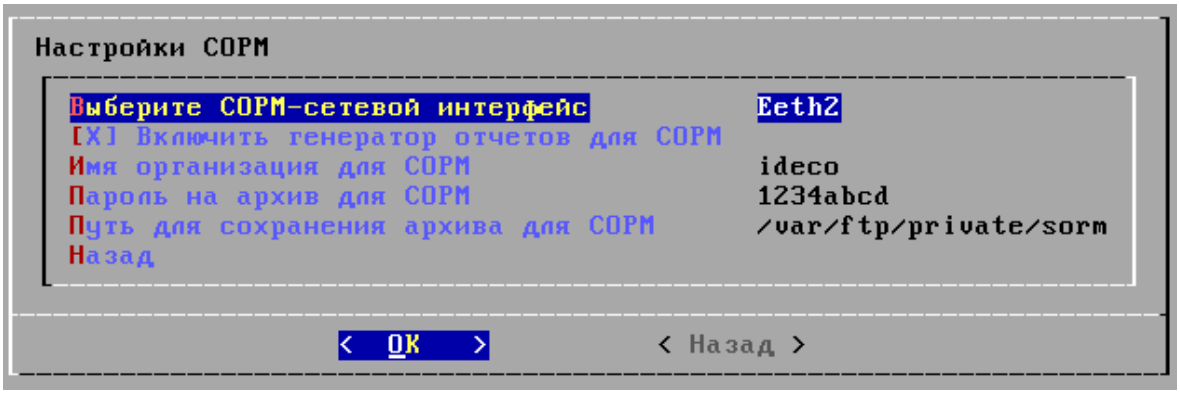
Включить маршрутизацию между внешними интерфейсами – Разрешить маршрутизацию между внешними интерфейсами. Ограничения по IP-адресам и другим параметрам можно установить в разделе Firewall в веб-интерфейсе.

Включить маршрутизацию между локальными интерфейсами – Разрешить маршрутизацию между локальными интерфейсами. Ограничения по IP-адресам и другим параметрам можно установить в разделе Firewall в веб-интерфейсе.

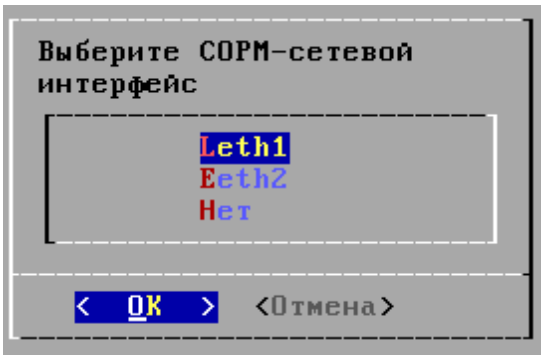
Разрешить управление файлами по SSH – Разрешить подключения к серверу по SSH. Эта опция необходима для удаленного обслуживания сервера и удаленного доступа к меню. (Глава 7. Обслуживание 105)

Разрешить полное удаленное управление по SSH – Если на вашем сервере включена учетная запись пользователя root и есть постоянный системный администратор, который следит за сервером, то данная опция разрешит ему доступ по протоколу SSH на нестандартный порт 33 для удаленного администрирования. Не включайте эту опцию без необходимости.

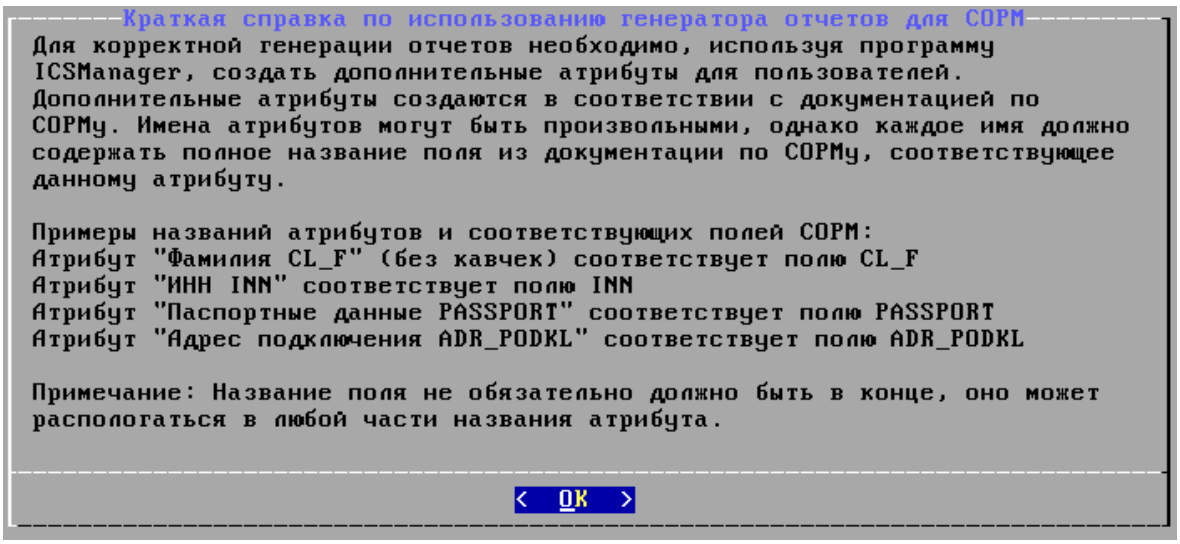
Настройки COPM:



Выберите COPM-сетевой интерфейс - укажите здесь тот интерфейс, с которого вы хотите снимать весь проходящий трафик в файл.



Включить генератор отчетов для COPM - поможет упорядочить данные о трафике интерфейса. Отчеты будут создаваться раз в месяц. Краткая инструкция по настройке отчетов в ICS Manager будет выведена на экран при включении этой опции.



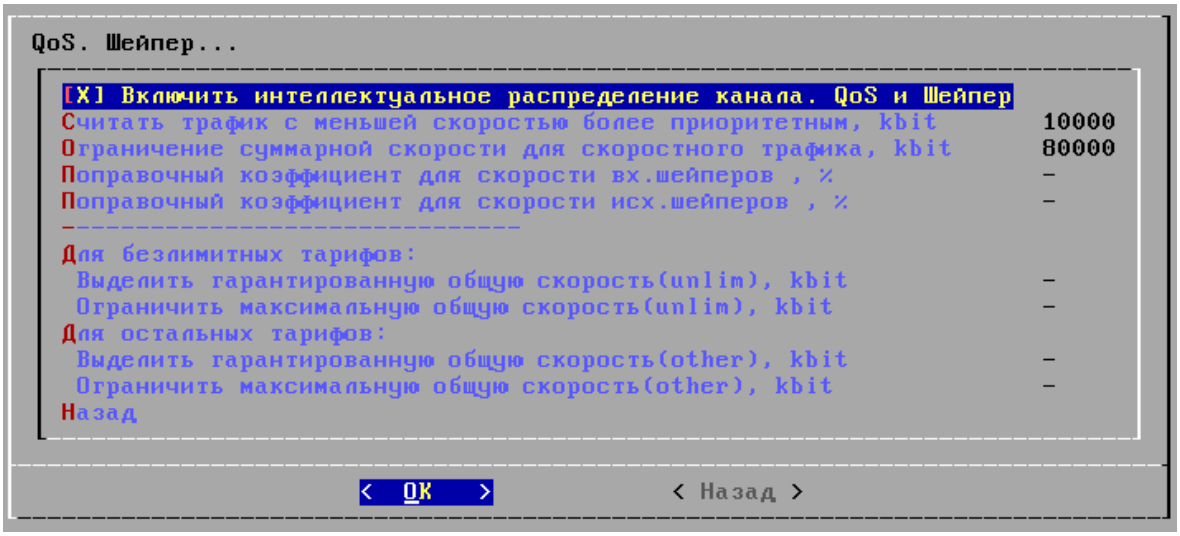
Имя организации для COPM - в названии допускается использовать только латинские буквы и цифры.

Пароль на архив для COPM - по желанию можно защитить создаваемый архив с

данными паролем.

Путь для сохранения архива для СОРМ - файл с дампом трафика будет создан в виде архива и размещен на сервере в том каталоге, который вы укажите. Потом по желанию архив можно выгрузить с сервера по FTP, с помощью WINscp или другим способом.

5.1.3.5 Qos и Шейпер



Включить интеллектуальное распределение канала. QoS и Шейпер - Эта возможность позволяет интеллектуально распределять ширину канала в случае его полной загрузки и равномерно распределить канал между пользователями. При включении этой опции интерактивный трафик становится более приоритетным, чем, например, скачивание файлов.

Важно. Включение этой опции позволяет использовать Правила QoS и Шейпера во встроенном Firewall. В противном случае, при загрузке сервера, правила не будут задействованы, а администратору придет предупреждение.

Считать трафик с меньшей скоростью более приоритетным, kbit – Это управляющий параметр для интеллектуального распределения пропускной способности канала. Если скорость трафика будет меньшей указанной скорости, то приоритет такого трафика повышается. Приоритет трафика со скоростью больше этого значения понижается. Таком образом, загрузки файлов будут обрабатываться с меньшим приоритетом, а трафик реального времени – с высоким. Скорость указывается в килобитах в секунду. Например, скорости 10 килобайт в секунду соответствует скорость примерно 90 килобит в секунду (с учетом служебных данных).

Ограничение полосы пропускания для высокоскоростного трафика, kbit – С помощью этого параметра можно ограничить максимальную скорость для высокоскоростного трафика. Оставшаяся часть полосы пропускания будет использована для интерактивного трафика. Скорость указывается в килобитах в секунду.

Поправочный коэффициэнт для скорости входящих шейперов - это

множитель, выраженный в %, на который умножаются все скоростные параметры входящих шейперов (и гарантированные и максимальные ограничения). Этот коэффициент рекомендуется использовать только в случае большого количества одновременных VPN сессий (больше 500). Перед использованием обратитесь в службу технической поддержки.

Поправочный коэффициэнт для скорости исходящих шейперов - это множитель, выраженный в %, на который умножаются все скоростные параметры исходящих шейперов (и гарантированные и максимальные ограничения). Этот коэффициент рекомендуется использовать только в случае большого количества одновременных VPN сессий (больше 500). Перед использованием обратитесь в службу технической поддержки.

Расширенные настройки шейпера

Условно работу шейпера в Ideco ACP можно представить как набор правил с указанием скорости, разделенный на две основные группы: группа правил, действующих на основании тарифов и другая группа правил в которую входят правила с указаниями скорости, настроенные в системном или пользовательском Firewalle, в разделе шейпер (в локальном меню или в веб-инетрфейсе). Правила Qos тоже относятся сюда (правила для приоритетного и неприоритетного траффика). Для каждой из этих 2х групп можно настроить глобальные указания по гарантированной скорости всех правил в группе и максимально возможной скорости.

Для безлимитных тарифов

Выделить гарантированную общую скорость, kbit - гарантированная полоса пропускания для группы правил шейпинга траффика заданных в тарифах. Действует суммарно на все правила сразу.

Ограничить максимальную общую скорость, kbit - Верхний лимит по скорости для группы правил шейпинга, определенных в тарифах. Действует суммарно на все правила сразу.

Для остальных тарифов

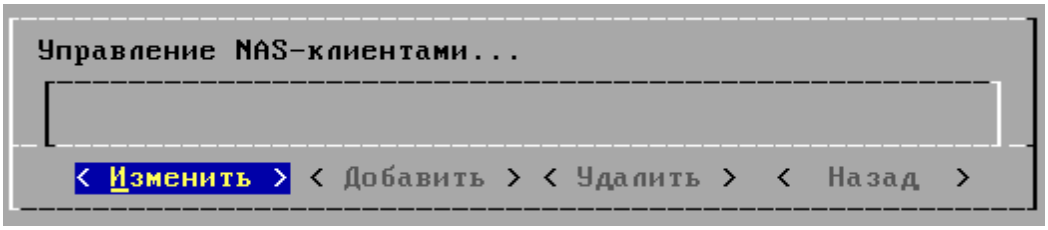
Выделить гарантированную общую скорость, kbit - гарантированная полоса пропускания для правил шейпинга траффика заданных в firewall'e и шейпере (в локальном меню или в веб-интерфейсе). Действует суммарно на все правила сразу.

Ограничить максимальную общую скорость, kbit - Верхний лимит по скорости для группы правил шейпинга, определенных в firewall'e и шейпере (в локальном меню или в веб-интерфейсе). Действует суммарно на все правила сразу.

5.1.3.6 Управление NAS и маршрутизаторами

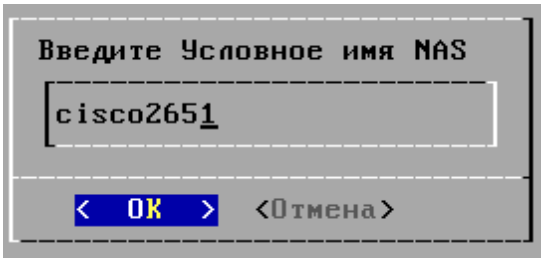
С помощью сервера Ideco ACP вы можете принимать информацию от NAS-устройств о трафике клиентов по Netflow и управлять этими устройствами. Если у вас несколько NAS-устройств, то для возможности работы сервера с ними, вам обязательно нужно перечислить здесь все NAS-устройства. Далее приводится случай описания NAS-устройства на сервере Ideco ACP на примере NAS Cisco.

В начале список устройств пуст, нажимаем кнопку **<Добавить>**.

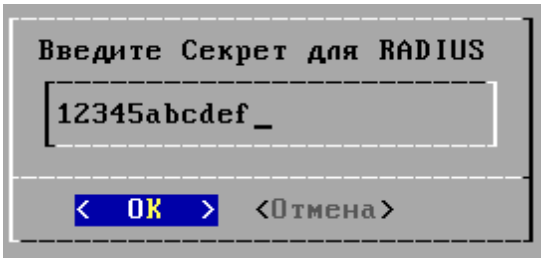


NAS должен находиться в локальной сети предприятия, т.е. быть подключен к одному сегменту сети с локальным сетевым интерфейсом на Ideco ACP. Если такая схема подключения NAS-устройств и сервера Ideco ACP не возможна, то обратитесь в отдел технической поддержки.

В имени устройства нельзя использовать спецсимволы и желательно избегать пробелов. Параметр является условным и нужен для удобства работы с устройством.

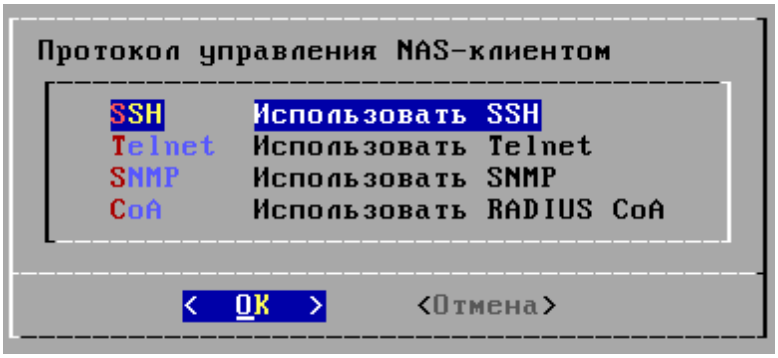


Секрет должен совпадать с аналогичным параметром на NAS-устройстве. Если NAS не поддерживает передачу данных с секретом, то введите здесь любую строку. Не оставляйте поле пустым.

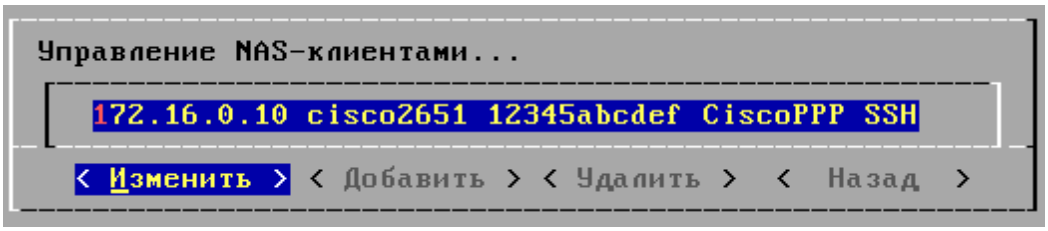


В будущем в нашем продукте у типу оборудования будут привязаны готовые схемы управления.Если вы знаете тип вашего NAS-устройства, то выберите его из предложенных вариантов или укажите любой тип. Тип устройства можно будет изменить позже.

Укажите протокол управления NAS-устройством. Если устройство поддерживает несколько протоколов, то выберите наиболее удобный для вас, так как от протокола управления зависит содержимое управляющих скриптов, которые вам надо будет настроить.

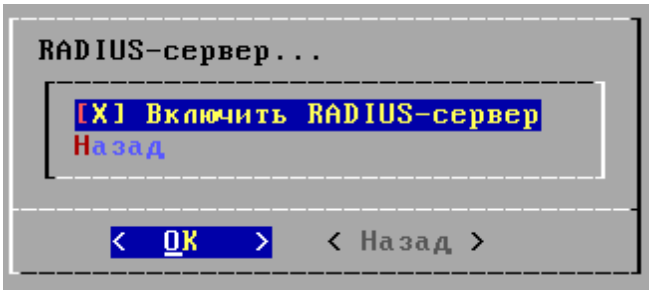


В итоге все доступные для работы с Ideco ACP устройства будут перечислены в виде списка с параметрами. Параметры каждого устройства всегда можно изменить.



5.1.3.7 RADIUS-сервер

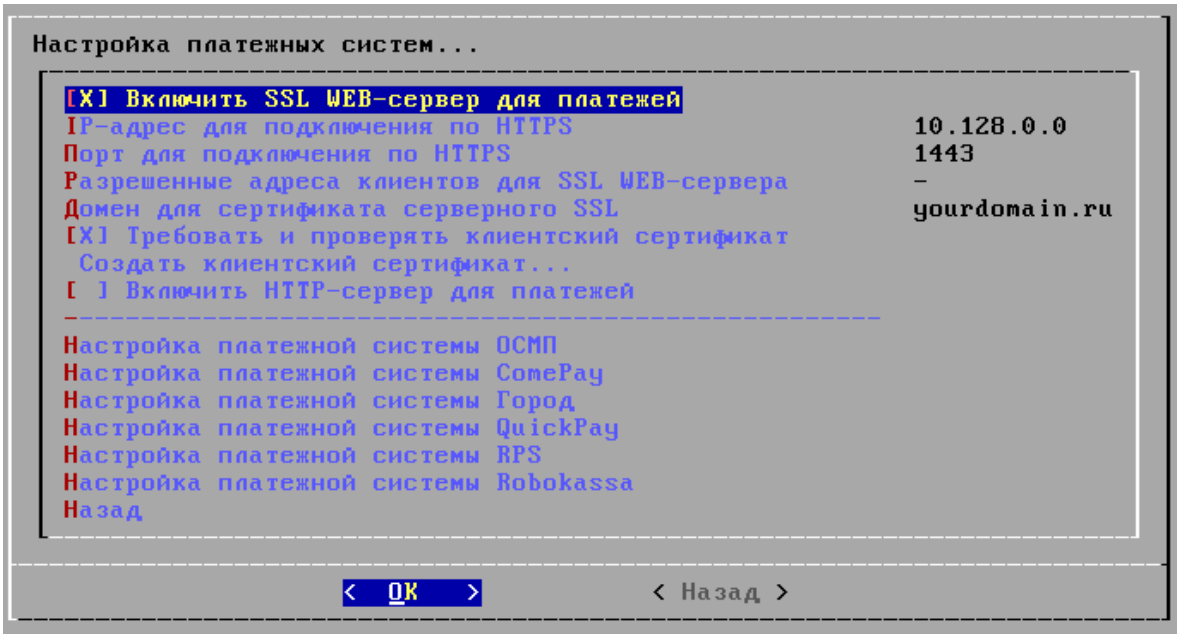
Все параметры для передачи управляющих сообщений NAS-устройствам по протоколу RADIUS указываются в текстовом виде в свойствах тарифа в отдельной вкладке. Управляющие параметры, указанные в тарифе, начинают поступать авторизующему клиента NAS-устройству когда включена эта опция. В остальном RADIUS-сервер на Ideco ACP не имеет настроек.



5.1.3.8 Настройка платежных систем

Настройка платежных систем во многом зависит от того как предоставляет связь со своими терминалами сам оператор платежной системы. Как правило если используются терминалы городских платежей, то используется защищенное SSL-соединение и вам нужно включить и настроить для связи с терминалами SSL WEB-сервер как показано ниже. Если для проведения платежей используются веб-сайты в интернете, то как часто в таких случаях нужно настраивать именно http сервер на Ideco ACP. Предварительно обязательно уточните у вашего оператора платежных систем по какому именно протоколу связи он предоставляет подключение к своим терминалам оплаты перед настройкой Ideco ACP.

SSL WEB-сервер для платежей имеет несколько параметров, значения которых описаны ниже.



Включить SSL WEB-сервер для платежей - Если оператор платежной системы осуществляет работу с терминалами оплаты по SSL, то нужно включить именно SSL WEB-сервер.

IP-адрес для подключения по HTTPS - адрес для подключения терминалов или сайтов платежных систем для проведения платежа клиенту в БД Ideco.

Порт для подключения по HTTPS - по умолчанию используется порт 1443. Если есть необходимость изменить этот порт, то по возможности указывайте порты выше 1024.

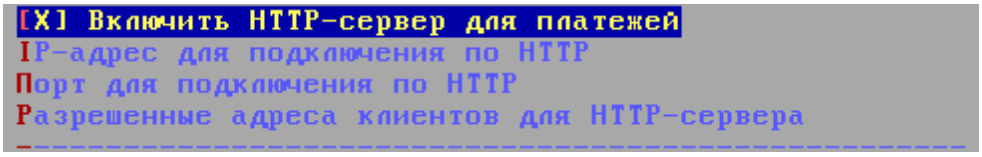
Разрешенные адреса клиентов для SSL WEB-сервера - если не указано, то доступ будет открыт всем.

Домен для сертификата серверного SSL - укажите здесь ваш публичный домен или отдельно зарегистрированный для сервера платежей на Ideco ACP домен. Опция не обязательна и позволяет обратится к SSL- WEB-серверу по доменному имени вместо IP-адреса.

Требовать и проверять клиентский сертификат - Обязательно отметить если настраиваете веб-интерфейс кассира. Если настраиваете работу с платежной системой, то уточните необходимость проверки клиентского сертификата у оператора платежной системы.

Создать клиентский сертификат - Будет создан клиентский сертификат, который нужно будет предоставить оператору платежной системы. Сертификат с суффиксом .pfx будет доступен на сервере в каталоге /var/lib/usrcert и будет иметь имя файла равное CN-имени, указанном вами при создании сертификата. Скачать файл сертификата с сервера можно программой winscp.

В случае настройки HTTP WEB-сервера для платежей.



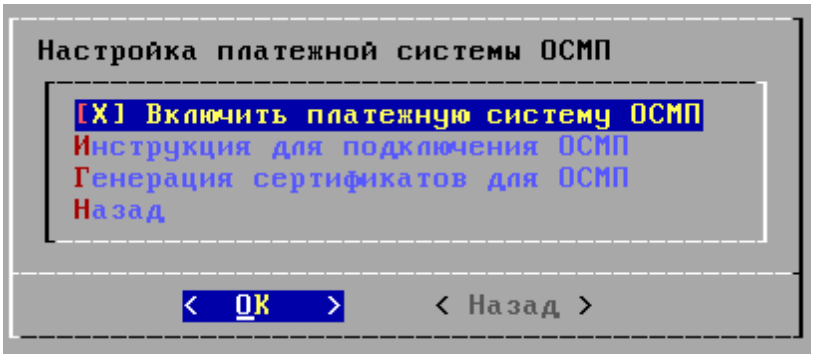
Включить HTTP-сервер для платежей - Если оператор платежной системы осуществляет работу с терминалами оплаты по открытому http-соединению, то включите именно HTTP-сервер.

IP-адрес для подключения по HTTP - Адрес веб-сервера для подключения к нему терминалов или серверов платежей.

Порт для подключения по HTTP - по умолчанию используется порт 1444. Если есть необходимость изменить этот порт, то по возможности указывайте порты выше 1024.

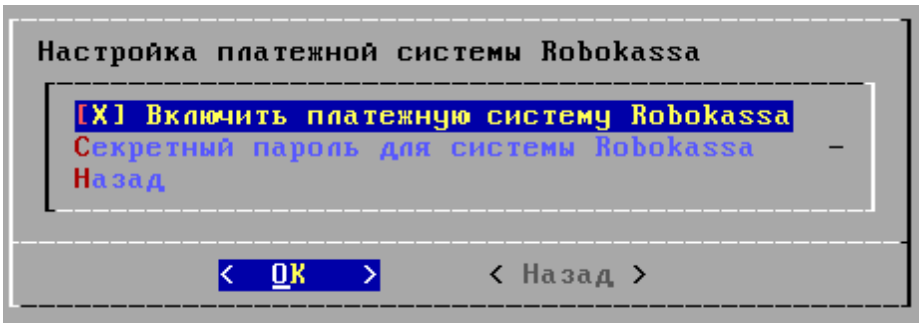
Разрешенные адреса клиентов для HTTP-сервера - если не указано, то доступ будет открыт всем.

Настройка синхронизации с платежными системами ОСМП подробно описана в статье "Синхронизация с платёжными системами 95".



Если вы пользуетесь услугами операторов платежных систем, указанных ниже на этой вкладке, то включите соответствующие им пункты меню. В будущем эти флажки будут устанавливать специфичные настройки системы, необходимые для каждого из используемых вами операторов. Если ваш оператор не входит в число перечисленных ниже, то не включайте ни один из них.

При настройке системы платежей Robokassa не забудьте указать секретный пароль, необходимый для организации соединения между терминалом и сервером.

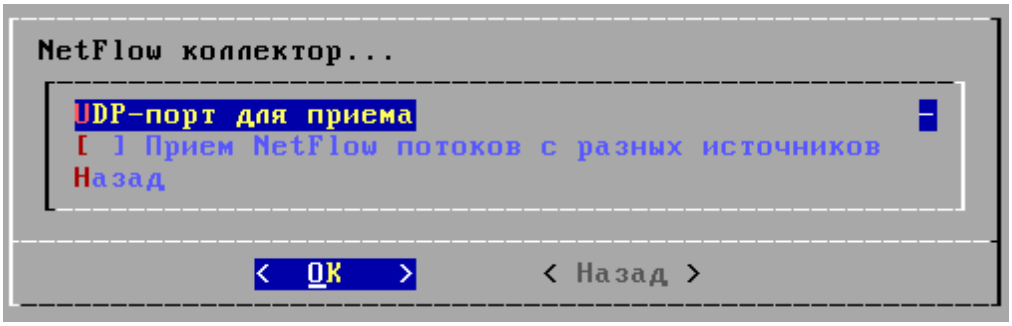


5.1.3.9 NetFlow коллектор

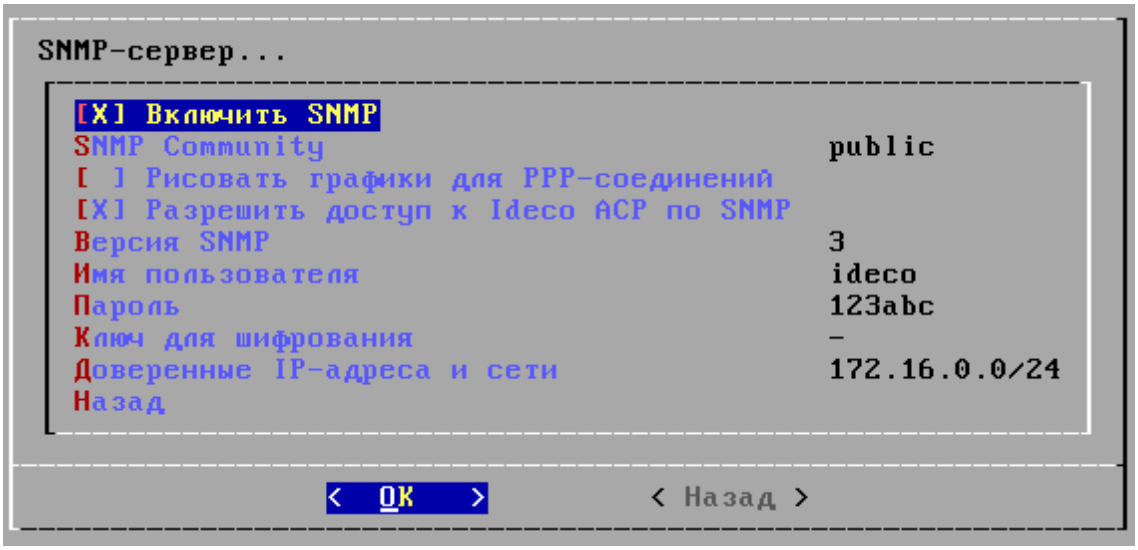
На сервере по умолчанию включена возможность приема netflow трафика от NAS-устройств в локальной сети, поэтому включать отдельно этот сервис не нужно.

UDP-порт для приема - По умолчанию сервис работает на порту 9996. Порт должен быть одинаковым на всех NAS-устройствах сети и на сервере Ideco ACP, поэтому если ваши устройства используют порт отличный от 9996, то укажите его ниже.

Прием NetFlow потоков с разных источников - обязательно включите эту опцию если вам нужно принимать NetFlow с нескольких источников в локальной сети. Так же, чтобы прием был возможен, эти устройства должны быть перечислены в управлении NAS-устройствами. Подробнее 148 ..



5.1.3.10 SNMP-сервер



Включить SNMP - Включить отдачу системной информации сервером по протоколу SNMP. При включении только одной этой опции во всем разделе SNMP, включается отдача информации только в пределах самого сервера (системная информация о сервере предоставляется самому серверу). При этом программа MRTG будет генерировать графики загрузки центрального процессора сервера (CPU), использования ОЗУ и сетевых Ethernet адаптеров, находящихся на самом сервере. Графики доступны в веб-интерфейсе администратора, в разделе Монитор.

SNMP Community - обязательный параметр, необходимый для аутентификации клиентов по SNMP протоколу. Значение по умолчанию - public. Используется для аутентификации сервера при отдаче SNMP статистики на SNMP-коллектор или приеме SNMP статистики от клиентов.

Рисовать графики для PPP-соединений - Включает отрисовку графиков загруженности ppp соединений пользователей, авторизующихся на Ideco ACP по pptp или pppoe, отрисовку загруженности pptp интерфейсов на сервере (например к провайдеру).

Разрешить доступ к Ideco ACP по SNMP - Ideco сможет предоставлять информацию по SNMP другим устройствам в сети. Отдача может вестись со всех сетевых интерфейсов.

Версия SNMP - версия протокола (3 и 1/2c). По умолчанию используется версия 2c. Версия 3 более безопасная и использует шифрование при передаче данных. При ее выборе становятся доступными для заполнения поля "Имя Пользователя", "Пароль", "Ключ для шифрования".

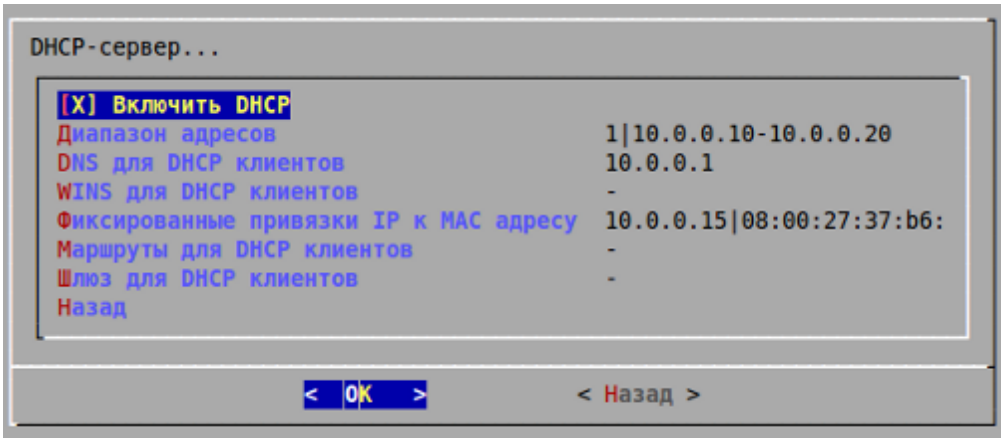
Имя пользователя - логин для аутентификации на удаленном SNMP-коллекторе.

Пароль - пароль для аутентификации на удаленном SNMP-коллекторе.

Ключ для шифрования - текстовое значение, используемое как ключ при шифровании передаваемых данных. Слово должно состоять из 8 символов или более для обеспечения должного уровня защиты от расшифровки данных.

Доверенные IP-адреса и сети - разрешить указанным адресам и подсетям получать данные от сервера по SNMP.

5.1.3.11 DHCP-сервер



Включить DHCP – Включение этой опции позволяет автоматически раздавать IP-адреса компьютерам, находящимся в одном Ethernet-сегменте с сервером. Если у Вас несколько локальных интерфейсов, то DHCP-сервер будет отвечать на запросы только на интерфейсе с номером 1.

Диапазон адресов – диапазон адресов выдаваемых компьютерам сети. Эти адреса не должны пересекаться с адресами пользователей. Диапазон должен обязательно умещаться в сеть, указанную на локальном интерфейсе. Диапазон адресов должен соответствовать подсети, сконфигурированной на интерфейсе. Например, если локальный интерфейс "10.0.0.1/255.255.255.0", то диапазон может быть "10.0.0.2 - 10.0.0.254".

DNS для DHCP клиентов – Укажите DNS-сервера, которые должны быть выданы при автоматической настройке компьютеров по DHCP-протоколу (если в качестве DNS будет использоваться Ideco, то поле заполнять не обязательно).

WINS для DHCP клиентов – Если в Вашей сети используется WINS-сервер или контроллер домена, то укажите его IP-адрес в этом поле.

Фиксированные привязки IP к MAC адресу – Укажите привязки IP и MAC адресов. Таком способом можно обеспечить гарантию того что выбранному компьютеру будет назначен постоянный адрес.

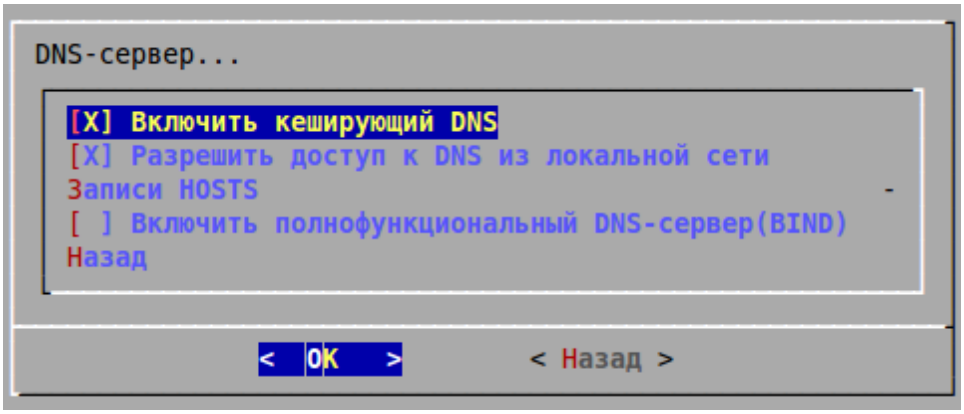
Маршруты для DHCP клиентов – Укажите список маршрутов которые должны

быть установлены на компьютерах пользователей. Из-за ограничений протокола маршруты могут быть только с маской 32 (указывать маску в конфигурации не нужно).

Шлюз для DHCP клиентов - Укажите шлюз по умолчанию для DHCP клиентов. По умолчанию в качестве шлюза используется сам сервер Ideco. Если шлюзом для Интернета в вашей сети является не Ideco. то укажите сдесь адрес этого устройства.

Внимание! Не все операционные системы могут принимать маршруты по протоколу DHCP.

5.1.3.12 DNS-сервер

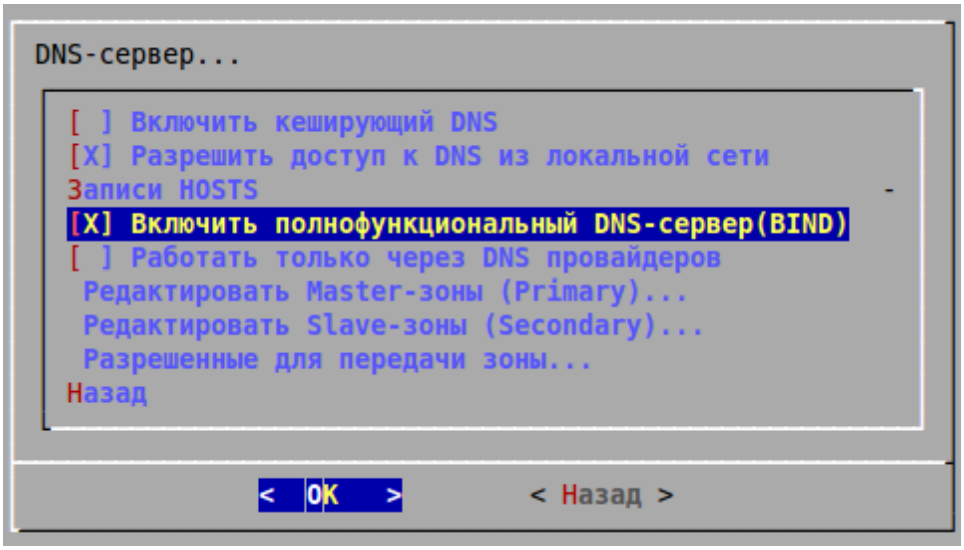


Включить кеширующий DNS – Включен по умолчанию. Используется для кеширования DNS-запросов из локальной сетп.

Разрешить доступ к DNS из локальной сети – Опция имеет смысл, если используется сервер DHCP или авторизация по IP.

Записи HOSTS - Здесь можно указать соответствие доменных имен и IP-адресов.

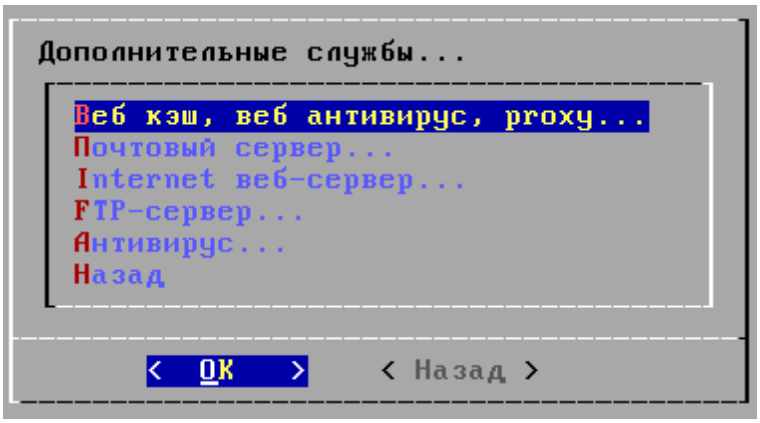
Включить полнофункциональный DNS-сервер (BIND) – Здесь можно указать настройки DNS, если сервер является держателем зоны. При включении этого пункта вам станут доступны Master и Slave зоны для настройки, а так же вы сможете настроить Разрешение для передачи зоны (Делегирование)



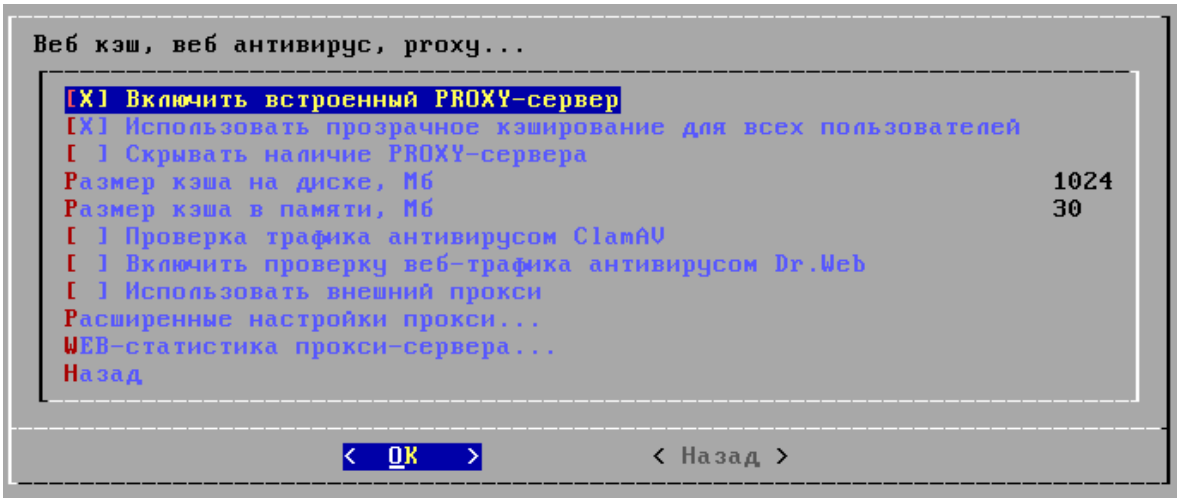
Важно! Ideco ACP только предоставляет инетрфейс для настройки и редактирования собственных DNS зон. Системный администратор сам занимается настройкой DNS зон для своей организации, специалисты техподдержки Ideco не оказывают консультаций по настройке DNS-сервера BIND.

5.1.3.13 Дополнительные службы

Важно. Использование дополнительных служб не рекомендуется для средних и больших провайдеров. В основном этот функционал применим для ВУЗ-ов и офисных зданий.



Прокси-сервер



Включить встроенный PROXY-сервер – задействует встроенный прокси сервер. После активации этой опции необходима полная перезагрузка.

Использовать прозрачное кэширование для всех пользователей – Автоматически перенаправляет веб-трафик всех пользователей на встроенный прокси. Если эта опция не активирована, то пользователей нужно будет перенаправлять вручную. Перенаправление производится с помощью Firewall, действие DNAT на адрес 169.254.254.254, порт 80.

Скрывать наличие PROXY-сервера – Позволяет не показывать страницы ошибок прокси сервера и убирать HTTP-заголовки, формируемые прокси сервером.

Размер кэша на диске, Мб – укажите объем диска который будет отводиться под кэш прокси сервера. В подсказке снизу отображается рекомендуемое значение.

Внимание! Не устанавливайте значение этого параметра свыше 2048 Мб без предварительного согласования с отделом технической поддержки.

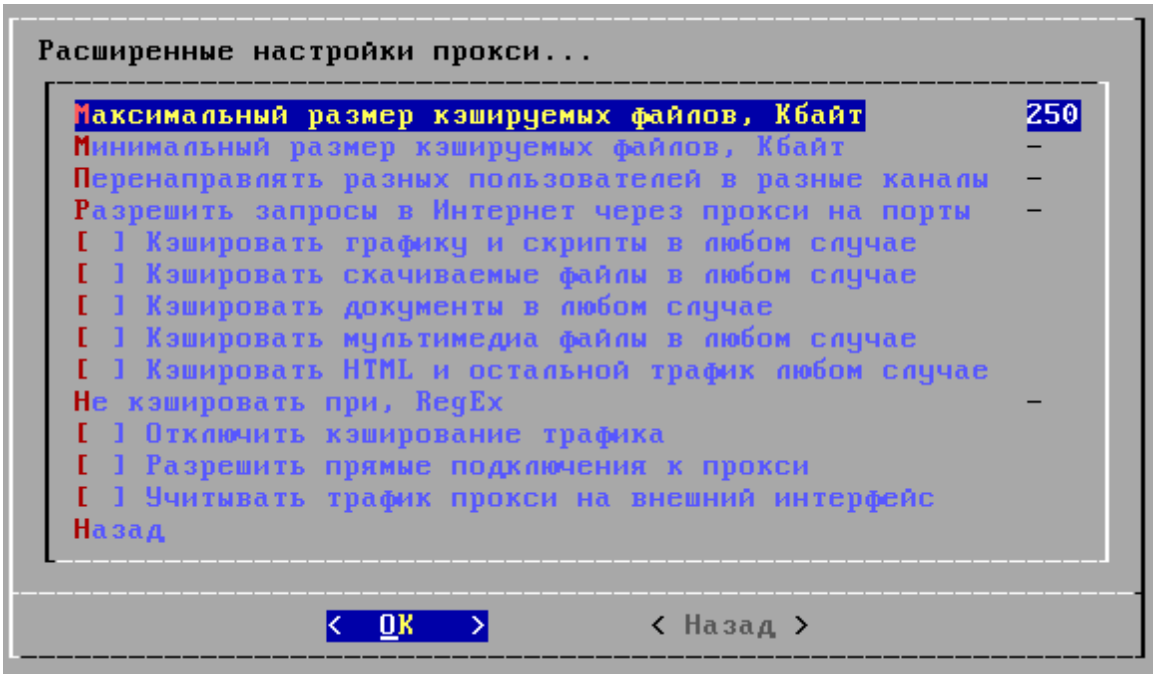
Размер кэша в памяти, Мб – укажите объем оперативной памяти, которая будет использоваться под кэш прокси сервера. В подсказке снизу отображается рекомендуемое значение.

Внимание! Не устанавливайте значение этого параметра свыше 128 Мб без предварительного согласования с отделом технической поддержки.

Проверка трафика на вирусы антивирусом ClamAV – Проверка веб трафика встроенным антивирусом ClamAV. При включенной опции некоторые страницы могут отображаться неправильно. Если система обнаружит вирус, то в браузер выведется соответствующее сообщение и файл загружен не будет.

Включить проверку веб-трафика антивирусом Dr. Web – Проверка веб-трафика антивирусом Dr. Web.

Использовать внешний прокси - Здесь можно задать параметры прокси-сервера, через который вы получаете доступ в Интернет от провайдера.



Максимальный и минимальный размер кэшируемых файлов, Кбайт – Укажите диапазон размеров файлов, которые должны кэшироваться.

Перенаправлять разных пользователей в разные каналы – Возможность указать, какие пользователи, через какого провайдера должны выходить в Интернет.

Разрешить запросы в Интернет через прокси на порты – Укажите список портов, на которые разрешено подключаться с помощью директивы CONNECT. (пишите только порты используемые для передачи веб-траффика, например 80, 8080, 443, 8010, 8008...)

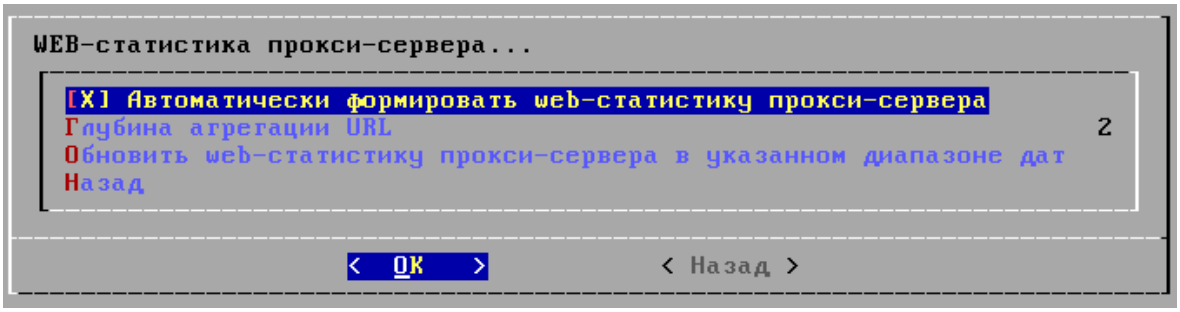
Кэшировать в любом случае – Укажите, какие файлы необходимо кэшировать вне зависимости от настроек запрашиваемого веб-сервера.

Не кэшировать при, RegEx – Укажите регулярное выражение для URL, которые не должны кэшироваться.

Отключить кэширование трафика – Установите этот параметр, если кэширование не требуется.

Разрешить прямые подключения к прокси – разрешить пользователям подключаться к прокси серверу на указанный IP-адрес и порт. Для использования этой возможности, необходимо указывать выбранный IP-адрес и порт в настройках программ. В большинстве случае это не требуется, так как программы должны работать напрямую, без прокси.

Учитывать трафик прокси на внешний интерфейс - необходимо включить если вы разрешили прамые подключения к серверу Ideco в firewall. Заставляет сервер считать трафик от самого сервиса прокси в инетернет (веб трафик прокси самого сервера Ideco)

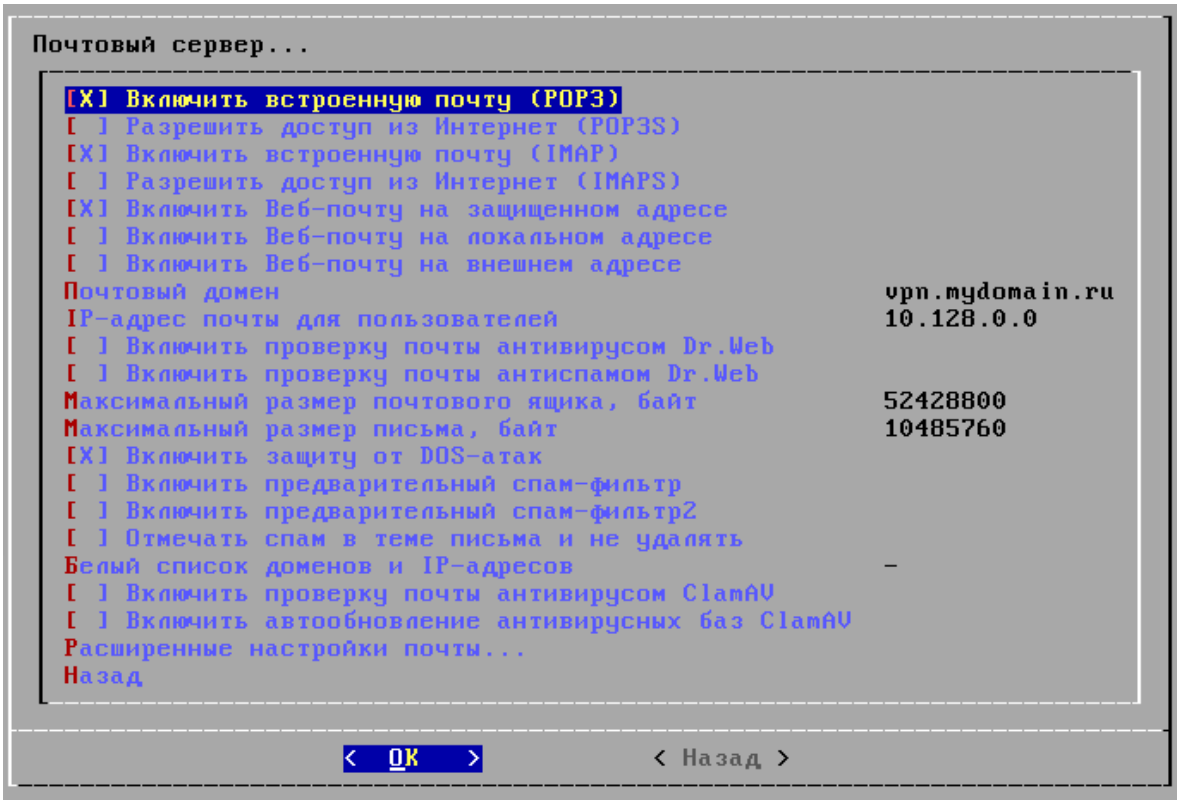


Автоматически формировать web-статистику прокси-сервера - При включении этой опции в разделе "Личный кабинет пользователя[80]" в Личном кабинете администратора становится доступна для просмотра статистика по посещаемым страницам

Глубина агрегации URL - насколько глубоко будет различаться статистика по сайтам относительно вложенных каталогов на веб-сервере (при чочтавлении статистики по посещениям будет формироваться общая статистика по somedomain.ru или отдельно по somedomain.ru и somedomain.ru/mail и somedomain.ru/forum и т.д.) "0" - будут считаться только домены. domain.ru, anotherdomain.ru и т.д.

Обновить web-статистику прокси-сервера в указанном диапазоне дат - заставит перечитать лог-файлы прокси сервера и сформировать статистику заново за указанный диапазон дат. Полезно в случае если прокси-сервер был включен давно, формировать статистику по посещениям вы начали недавно. Т.о. воспользовавшись этим меню вы сможете получить сгенерировать статистику за все время работы прокси-сервера, указав соответствующий временной диапазон.

Почтовый Сервер



Включить встроенную почту (POP3,IMAP) – задействует встроенный почтовый сервер. Для пользователей, у которых установлен атрибут "разрешить почту" будет создан почтовый ящик. Каждая опция включает соответствующий протокол работы с почтой.

Разрешить доступ из Интернет(POP3S, IMAPS) – Разрешить подключение к почтовым сервисам через протоколы с шифрованием. Таким образом, для защищенной работы с почтой при подключении из Интернет, не требуется устанавливать VPN-соединение.

Включить Веб-почту на локальном, внешнем и защищенном интерфейсах – Включить Веб-почту на соответствующих адресах. Доступ к Веб-почте можно получить только по протоколу с шифрованием - SSL. Для доступа к Веб-почте необходимо набрать в адресной строке браузера:

"https://<доменное имя или IP-адрес>/mail", "https://<доменное имя или IP-адрес почты для пользователей>/"

Почтовый домен – укажите ваш почтовый домен. Это правая часть от символа @ в e-mail адресе, например, "mydomain.ru". Почтовый домен должен быть зарегистрирован. Если у вас нет зарегистрированного домена второго уровня, то зарегистрируйте его или попросите вашего провайдера зарегистрировать домен третьего уровня. Для того чтобы работала электронная почта, необходимо в качестве MX записи для выбранного почтового домена указать внешний IP-адрес сервера Ideco ICS.

IP-адрес почты для пользователей – укажите отдельный IP-адрес, на котором будет работать электронная почта, например "10.222.222.222". Это может потребоваться для отдельной тарификации почты в тарифном плане. При отдельной тарификации электронной почты нет возможности отдельно тарифицировать

локальную и внешнюю почту. Есть возможность тарифицировать только всю почту, в том числе и внутрисетевую (внутреннюю). Этот адрес будет использоваться только для отправки и приема писем внутренних пользователей и не влияет на возможность приема почты от внешних почтовых серверов в Internet.

Включить проверку почты антивирусом Dr. Web – Проверять почту антивирусом Dr. Web (требуется ключ регистрации Dr. Web).

Включить проверку почты антиспамом Dr. Web – Проверять почту на спам антивирусом Dr. Web (требуется ключ регистрации Dr. Web).

Расширенные настройки Dr.Web антивирус... (Доступно только при включенном пункте "Включить проверку почты антивирусом Dr. Web") - См. на этой странице ниже.

Расширенные настройки Dr.Web антиспам... (Доступно только при включенном пункте "Включить проверку почты антиспамом Dr. Web") - См. на этой странице ниже.

Максимальный размер почтового ящика, байт – ограничить максимальный размер почтовых ящиков указанным количеством байт. По умолчанию – 30 Мб.

Максимальный размер письма, байт – ограничить максимальный размер одного письма указанным количеством байт. По умолчанию – 2 Мб.

Включить защиту от DOS-атак – Рекомендуется включить. Защита от внешних сетевых атак на отказ в обслуживании.

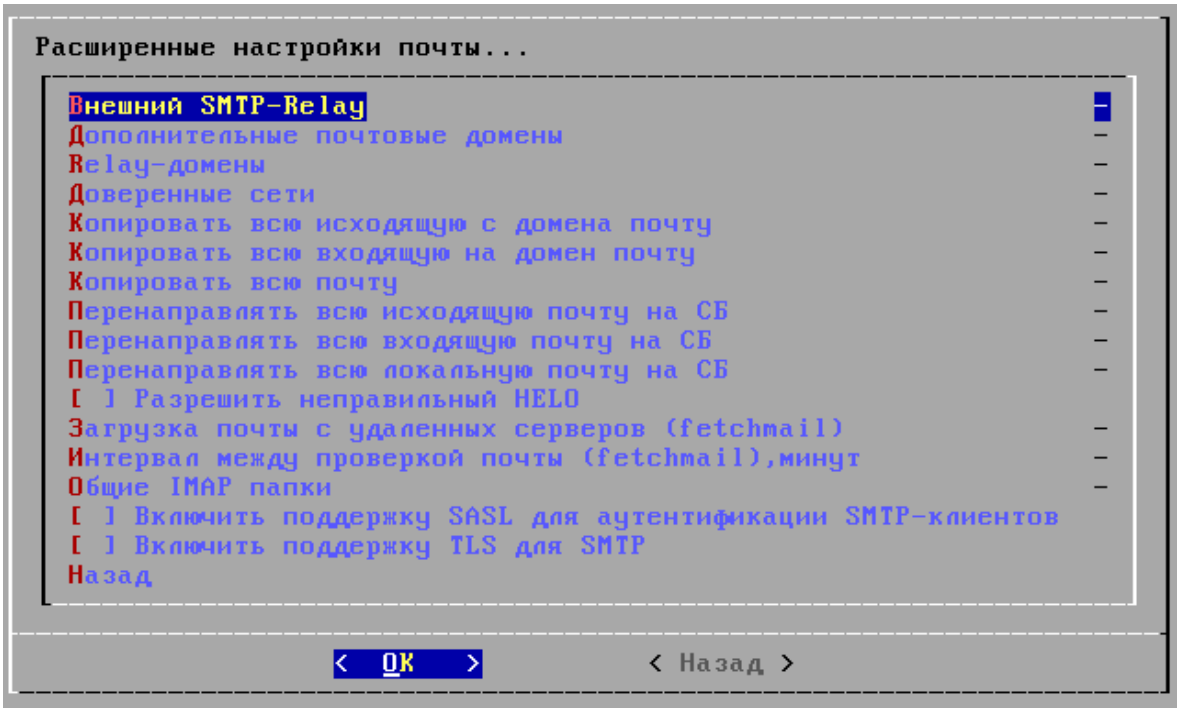
Включить предварительный спам-фильтр 1 и 2 – Не принимать письма, идентифицированные как спам. Определение таких писем производится на основе анализа заголовков писем с помощью регулярных выражений. При включении только первого предварительного спам-фильтра это позволяет блокировать тривиальный спам, который составляет около 70% всего спама. В случае включения только первого предварительного спам-фильтра возможность ошибочной блокировки письма как спама сведена к нулю. При включении обоих предварительных спам-фильтров блокируется около 85-90 % спама. Начинают действовать более строгие проверки по регулярным выражениям. Некоторые письма не являющиеся спамом могут быть блокированы.

Отмечать спам в теме письма и не удалять – При включенной опции спам-почта будет помечаться, а не удаляться.

Белый список доменов и IP-адресов - доверенные ресурсы в сети Интернет проверка почты с которых не ведется.

Включить проверку почты антивирусом Clamav – Проверять всю внутреннюю почту на вирусы бесплатным open-source антивирусом ClamAV. На вирусы будет проверяться только почта, проходящая через встроенный SMTP-сервер.

Включить автообновление антивирусных баз Clamav – Автоматически обновлять антивирусные базы. Включение этой опции позволит иметь всегда самые свежие антивирусные базы. Загрузка обновления баз данных составляет примерно 2 Мб в месяц.



Внешний SMTP-Relay – Необязательный параметр. Если ваш провайдер бесплатно предоставляет SMTP-сервер (mail relay), то можно указать его адрес для отправки всей электронной почты через него.

Дополнительные почтовые домены – Укажите список дополнительных почтовых доменов, для которых сервер будет принимать почту и сохранять письма в почтовые ящики.

Relay-домены – Укажите список почтовых доменов, для которых сервер будет принимать почту с целью отправки на почтовый сервер в локальной сети.

Доверенные сети – Укажите список локальных подсетей, для которых будет разрешена отправка писем без автоизации на сервере.

Копировать всю исходящую с домена почту – Укажите почтовый адрес, на который должна копироваться вся исходящая с этого почтового домена почта

Копировать всю входящую в домен почту – Укажите почтовый адрес, на который должна копироваться вся почта, приходящая пользователям вашего домена.

Копировать всю почту – Укажите почтовый адрес для копирования всех писем, которые принял почтовый сервер.

Перенаправлять всю (исходящую, входящую, локальную) почту на СБ – Здесь можно указать e-mail службы безопасности. Служба безопасности может отправлять проверенную почту перемещением в OUTBOX.

Разрешить неправильный HELO – Установите этот флажок для приема почты с неверно сконфигурированных почтовых серверов в Интернет.

Загрузка почты с удаленных серверов (fetchmail) – Здесь можно указать параметры для получения почты сервером с внешних почтовых служб.

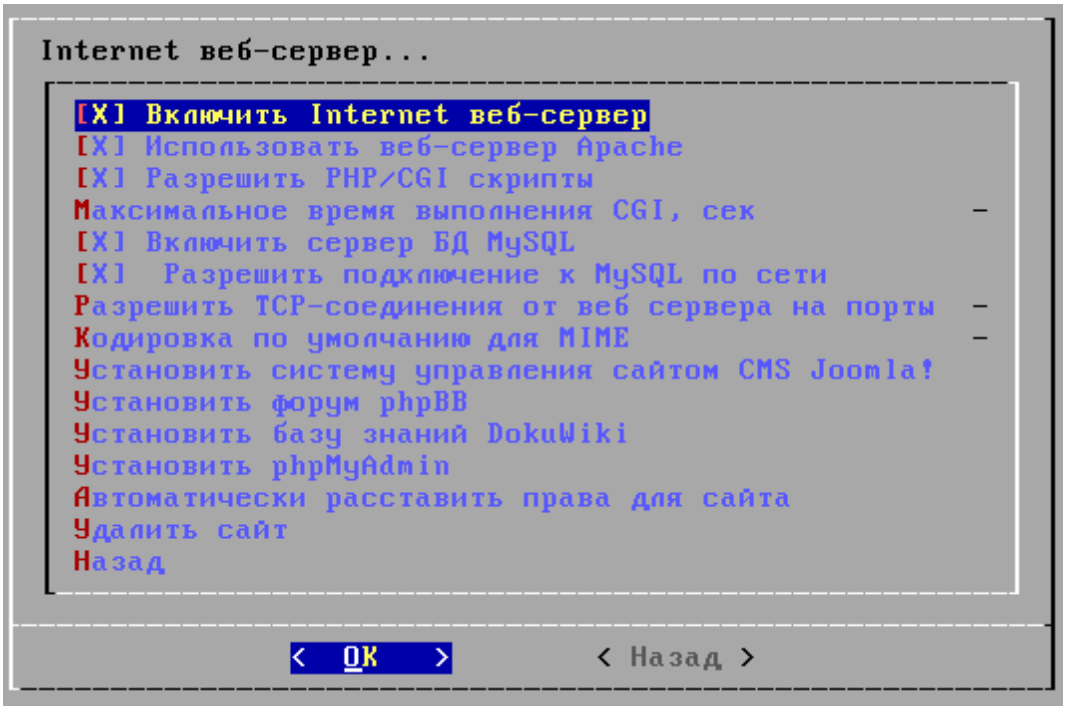
Интервал между проверкой почты (fetchmail), минут – Рекомендуется 5-15 минут.

Общие IMAP папки – укажите список папок, которые будут общими при работе с почтой по протоколу IMAP. Путь к вложенным папкам необходимо указывать через косую черту "/".

Включить поддержку SASL для аутентификации SMTP-клиентов – Опция позволяет подключаться пользователям из Интернет со своей учетной записью.

Включить поддержку TLS для SMTP – Здесь можно включить поддержку шифрования соединений для отправки почты.

Internet веб-сервер



Включить Internet веб-сервер – Включить веб-сервер на внешнем интерфейсе для расположения внешнего сайта компании. Копировать файлы сайта можно с помощью утилиты WinScp, подробнее см. Размещение сайта.

Использовать Internet веб-сервер Apache - использовать сервер Apache вместо THTTPD для внешнего веб-сайта.

Разрешить php/cgi скрипты – Разрешить выполнение сценариев на веб-сервере. Включение этого параметра позволяет создавать динамические сайты на PHP, Perl и любые другие.

Максимальное время выполнения CGI, сек – Ограничить максимальное время выполнения CGI сценариев на сервере.

Включить сервер БД MySql – Включить поддержку базы данных MySql для внешнего веб-сервера. С включением этого параметра появляется возможность использовать базу данных MySql для CGI-скриптов (PHP, Perl, и т.д.).

Разрешить подключение к MySQL по сети – Разрешить подключаться на защищенный адрес (обычно, 10.128.0.0) с помощью сетевых программ управления БД MySQL.

Разрешить TCP соединения от веб-сервера на порты – Здесь можно ввести

список TCP-портов, на которые будут подключаться CGI-скрипты.

Кодировка по умолчанию для MIME – Кодировка по-умолчанию для файлов веб-сайта.

Установить систему управления сайтом CMS Joomla! – Установить систему управления сайтом Joomla!. С помощью этой системы можно легко создать сайт компании. Для установки этой CMS необходимо включить поддержку MySQL, включить Internet веб-сервер и перезагрузиться (можно использовать мягкую перезагрузку).

Установить форум phpBB – установить форум phpBB. По умолчанию, форум доступен по адресу внешнего доменного имени в каталоге forum. Например, http://vpn.mydomain.ru/forum. Для установки форума необходимо включить поддержку MySql, включить Internet веб-сервер и перезагрузиться (можно использовать мягкую перезагрузку).

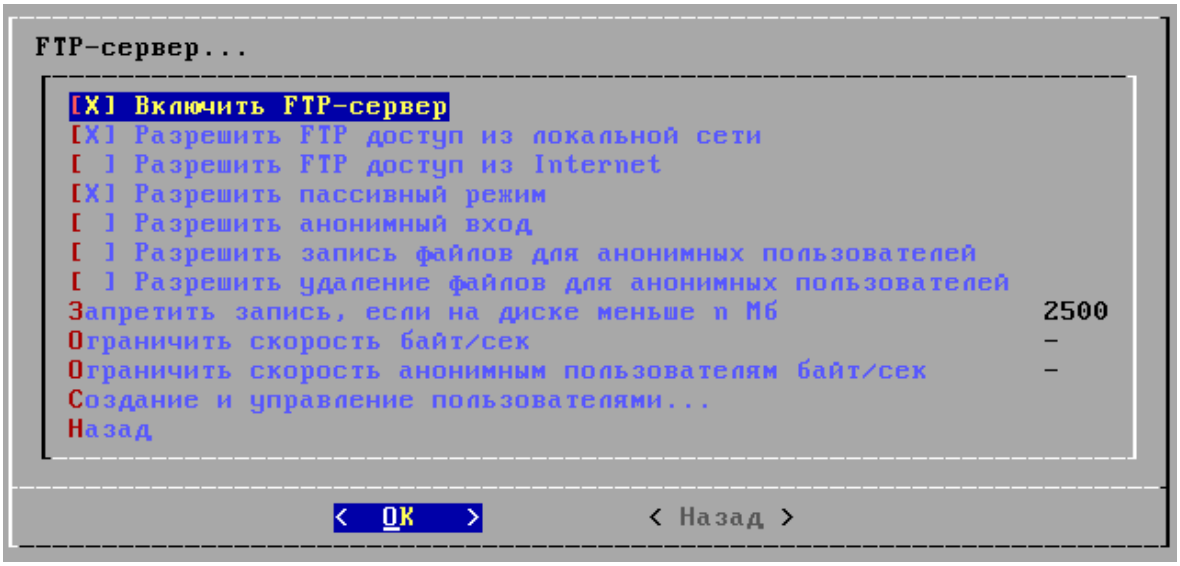
Установить базу знаний DokuWiki – Dokuwiki будет по умолчанию доступна по адресу внешнего доменного имени в каталоге forum. Например, http://vpn.myorg.ru/doku.php . Для установки форума необходимо включить поддержку MySql, включить Internet веб-сервер и перезагрузиться (можно использовать мягкую перезагрузку).

Установить phpMyAdmin - По умолчанию будет доступен по адресу внешнего доменного имени, можно указать подкаталог. Для установки phpMyAdmin необходимо включить поддержку MySql, разрешить выполнение cgi-скриптов и произвести мягкую перезагрузку.

Автоматически расставить права для сайта – После копирования сайта на сервер, выберите этот пункт меню для автоматической расстановки прав доступа к файлам.

Удалить сайт – для удаления определенного каталога или сайта можете воспользоваться этим пунктом меню.

FTP сервер



Включить FTP-сервер – Включить встроенный FTP-сервер. Включив этот параметр можно организовать общее хранилище файлов. Подключаться к FTP

серверу по умолчанию могут пользователи, авторизованные на сервере и только по защищенному адресу, по умолчанию 10.128.0.0. Имейте в виду, что включение FTP сервера создает дополнительную нагрузку на сервер с Ideco ICS.

Разрешить FTP доступ из локальной сети – Позволить пользователям локальной сети (без авторизованного подключения к серверу) получать доступ к FTP-серверу, по адресу локального интерфейса. Имейте в виду, что статистика трафика локальной сети для FTP-сервера ведется только на уровне его LOG-файлов.

Разрешить FTP доступ из Internet – Разрешит подключение к серверу FTP из сети Интернет, при этом крайне не рекомендуются включать запись для анонимных пользователей.

Разрешить пассивный режим – Разрешить пассивный режим подключения к FTP. Используется по умолчанию во многих браузерах.

Разрешить анонимный вход – Разрешить подключение к FTP-серверу без ввода логина и пароля. При входе на FTP без логина и пароля будет использованы соответствующие права доступа к файлам, находящимся на FTP-сервере.

Разрешить запись файлов для анонимных пользователей – Позволить анонимным пользователям выгружать на сервер файлы (при наличии разрешений в правах доступа).

Разрешить удаление файлов для анонимных пользователей – Позволить анонимным пользователям удалять файлы с сервера (при наличии разрешений в правах доступа).

Запретить запись, если на диске меньше n Мб – Запретить создавать и выгружать файлы на сервер, если свободного места на диске меньше, чем указанное число мегабайт.

Ограничить скорость, байт/сек – ограничить максимальную скорость загрузки и выгрузки указанным значением.

Ограничить скорость анонимным пользователям байт/сек – ограничить максимальную скорость загрузки и выгрузки файлов указанным значением для анонимных пользователей.

Создание и управление пользователями – с помощью этого пункта меню можно настраивать FTP пользователей. FTP-пользователи никак не связаны с глобальной базой данных пользователей и настраиваются отдельно.

Антивирусы

При настройке работы антивирусов в этом меню, следует учесть следующие особенности:

- При проверке веб-траффика (траффика проходящего через прокси) антивирусной программой одновременно может работать только один антивирус из тех что имеется в нашем продукте. (Антивирус Касперского,Clamav или Dr.Web).

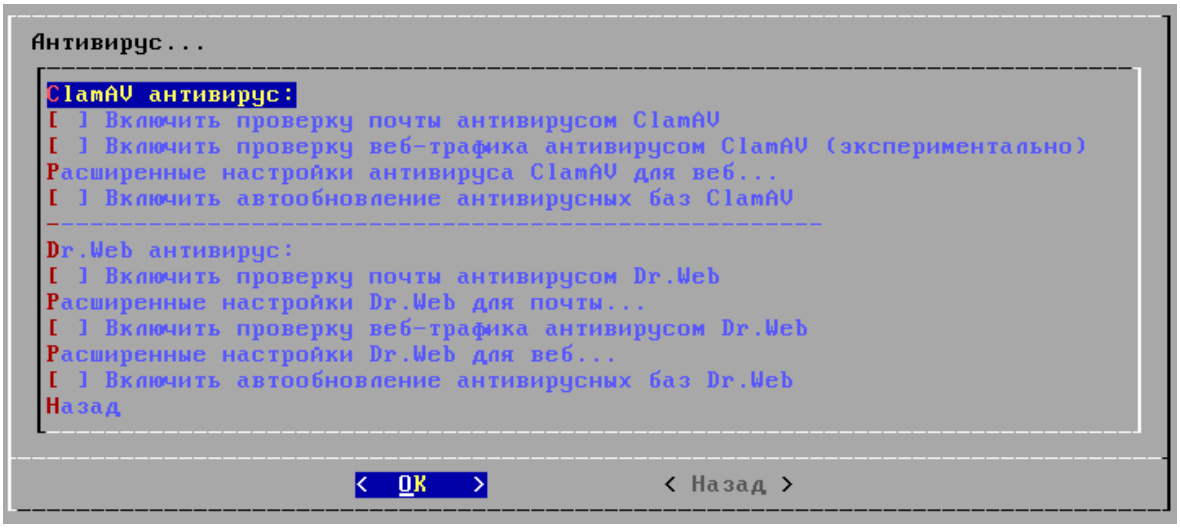
- При использовании Антивируса Касперского вам необходимо приобрести лицензию на IdecoICS с возможностью использования Антивируса Касперского.

- При использовании Dr.Web вы задейсвуете тот функционал, в зависимости от того какие ключи у вас куплены на Dr.Web. Проверка веб-трафика, проверка почтового траффика или антиспам. Ключи покупаются отдельно в представительствах компании Dr.Web, с отделом продаж Ideco это не связано. При

покупке ключей вам необходимо поместить их на сервер, что описано здесь 264.

- Clamav является бесплатным решением и доступен к использованию при покупке любой лицензии нашего продукта, никаких дополнительных ключей покупать не нужно.

- Dr.Web антиспам настраивается в параметрах почтового сервера.



Clamav

Включить проверку почты антивирусом Clamav - Задействовать проверку проходящей через Айдеко почты со всеми вложениями в письмах. Почтовый сервер должен быть при этом настроен на Ideco в качестве самостоятельного сервера или почтового релея.

Включить проверку веб-трафика антивирусом Clamav (экспериментально) - Включение проверки проходящего через прокси веб-трафика на вирусы, вредоносные программы и нежелательный код. Прокси-сервер при этом должен быть включен.

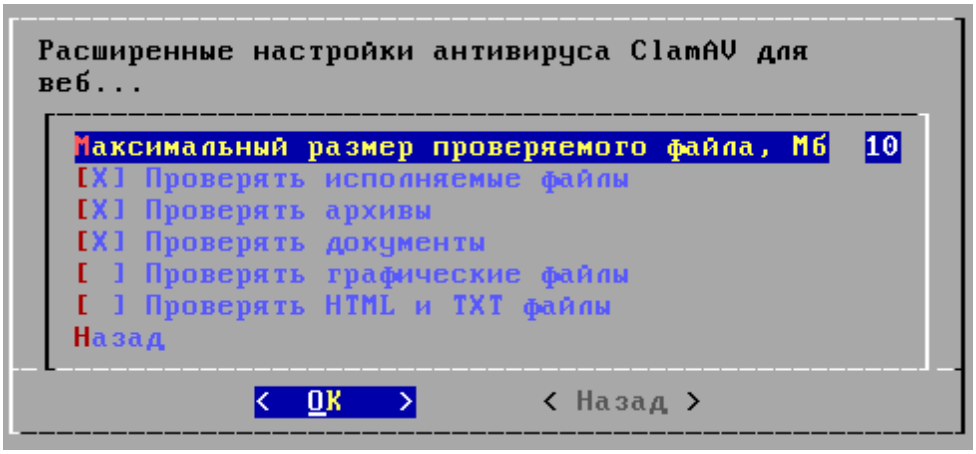
Включить автообновление антивирусных баз Clamav - Автообновление антивирусных баз будет происходить ежедневно.

Dr. Web

Включить проверку почты антивирусом Dr. Web - Задействовать проверку проходящей через Айдеко почты со всеми вложениями в письмах. Почтовый сервер должен быть при этом настроен на Ideco в качестве самостоятельного сервера или почтового релея.

Включить проверку веб-трафика антивирусом Dr. Web - Включение проверки проходящего через прокси веб-трафика на вирусы, вредоносные программы и нежелательный код. Прокси-сервер при этом должен быть включен.

Включить автообновление антивирусных баз Dr. Web - Автообновление антивирусных баз будет происходить несколько раз в сутки.



Максимальный размер проверяемого файла - Размер файла в мегабайтах, выше которого файлы не будут проверяться программой. Не рекомендуется ставить значения больше 50.

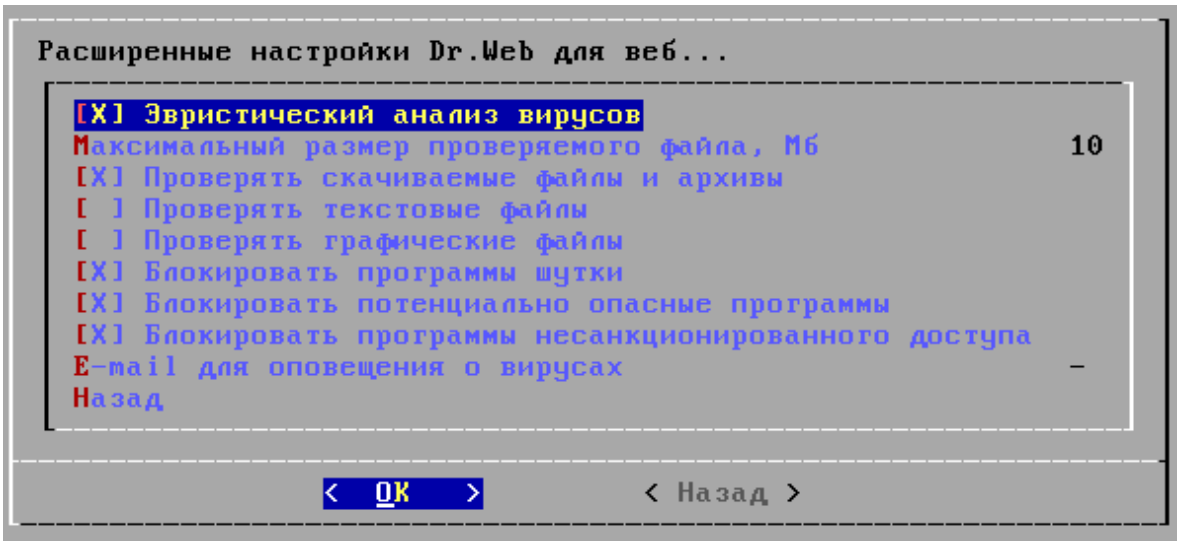
Проверять исполняемые файлы - включает проверку исполняемых файлов, active-x приложений, исполняемых скриптов, библиотек.

Проверять архивы - включает проверку архивных файлов.

Проверять документы - включает проверку офисных документов.

Проверять графические файлы - включает проверку графических объектов.

Проверять html и txt - включает проверку файлов соответствующих форматов.



Эвристический анализ вирусов - включает более интеллектуальный метод проверки траффика на вредоносный код. Теоритически может выявить вирусы, которых еще нет в базе. Требует повышенного расхода вычислительных ресурсов сервера.

Максимальный размер проверяемого файла - Размер файла в мегабайтах, выше которого файлы не будут проверяться программой. Не рекомендуется ставить значения больше 50.

Проверять скачиваемые файлы и архивы - включает проверку всех файлов получаемых из Интернета и сохраняемых непосредственно на PC клиента.

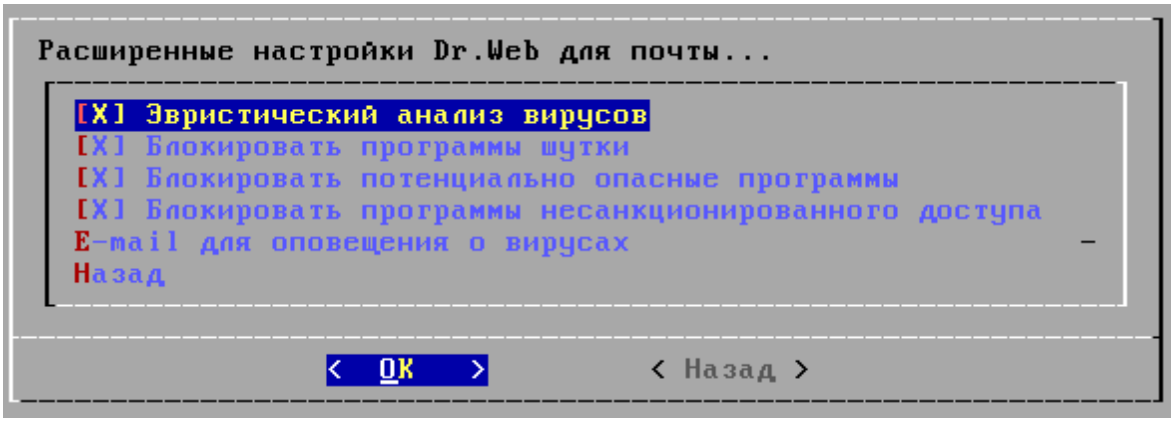
Проверять текстовые файлы - включает проверку текстовых файлов отображаемых в браузере.

Проверять графические файлы - включает проверку графических объектов.

Блокировать программы шутки - запрещает выполнение получаемых из Интернета программ, имитирующих неправильную работу PC клиента. (Например имитирующие "синий экран смерти")

Блокировать потенциально опасные программы - включает запрет на скачку и выполнение потенциально опасных программ.

Блокировать программы несанкционированного доступа - включает запрет на скачку и выполнение программ, незаконно пытающихся получить доступ к конфиденциальным данным пользователей.



Эвристический анализ вирусов - включает более интеллектуальный метод проверки траффика на вредоносный код. Теоритически может выявить вирусы, которых еще нет в базе. Требует повышенного расхода вычислительных ресурсов сервера.

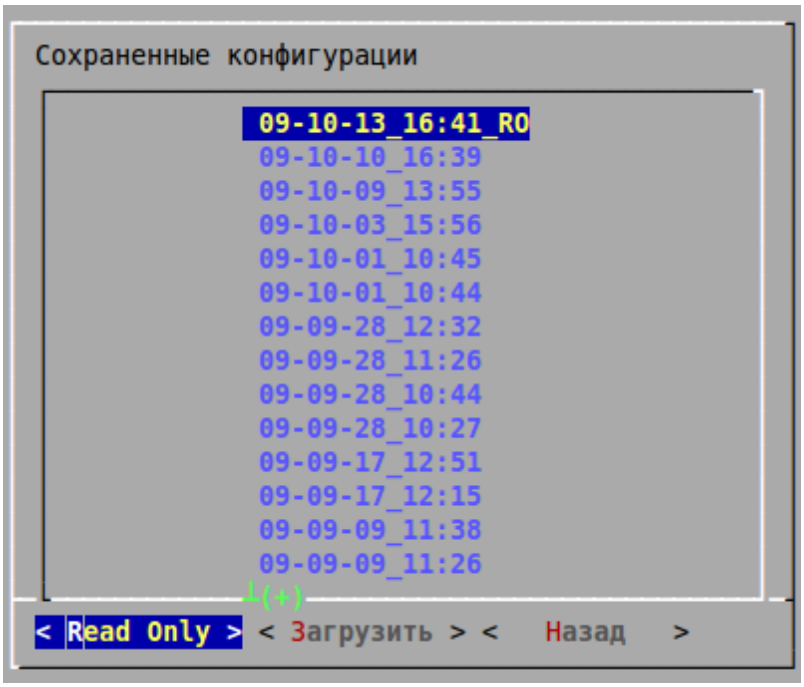
Блокировать программы шутки - запрещает выполнение получаемых по почте программ, имитирующих неправильную работу PC клиента. (Например имитирующие "синий экран смерти")

Блокировать потенциально опасные программы - включает запрет на выполнение потенциально опасных программ, получаемых по почте.

Блокировать программы несанкционированного доступа - включает запрет на выполнение программ, незаконно пытающихся получить доступ к конфиденциальным данным пользователей, полученных по почте.

E-mail для оповещения о вирусах - здесь можно указать электронный адрес для отсылки сообщения в случае обнаружения вирусов в почтовом траффике.

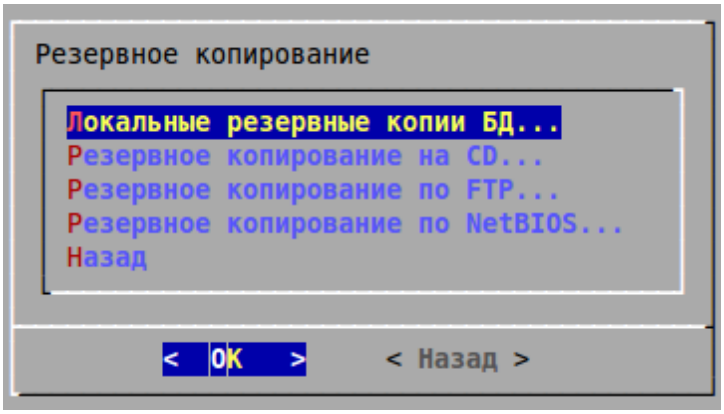
5.1.3.14 Сохраненные конфигурации



Здесь указан список последних 20 сохраненных конфигураций. При записи большего числа конфигураций самая первая из списка будет удалена. Если вы хотите, чтоб какая-либо конфигурации никогда не удалялась, установите для нее режим "Read-Only".

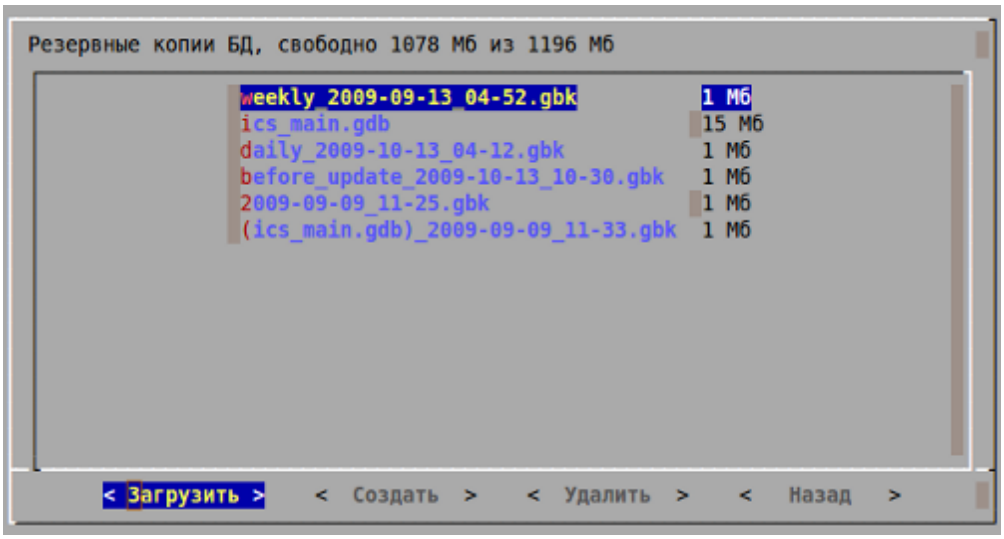
5.1.4 Резервное копирование

В этом разделе можно создать резервную копию текущей БД или восстановить сделанную ранее. Ideco ACP автоматически делает ежедневную копию “daily” , еженедельную “weekly” и ежемесячную “monthly”. В этом лиалоге настраивается метод резервного копирования БД и периодичность создания копий.

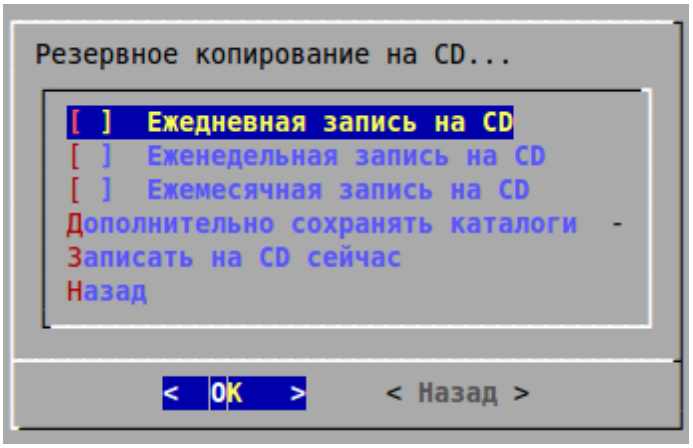


Локальные копии БД - список доступных резервных копий БД пользователей, хранящихся на сервере Ideco. Из этого списка вы можете выбрать нужную копию

и откатить состояние БД пользователей на предыдущее состояние, выбрав БД и нажав кнопку <Загрузить>. При нажатии кнопки <Создать> будет создан бекап БД пользователей со всеми изменениями на текущий момент (копии БД создаются автоматически ежедневно). Кнопка <Удалить> удаляет выбранную БД пользователей.



Резервное копирование на CD

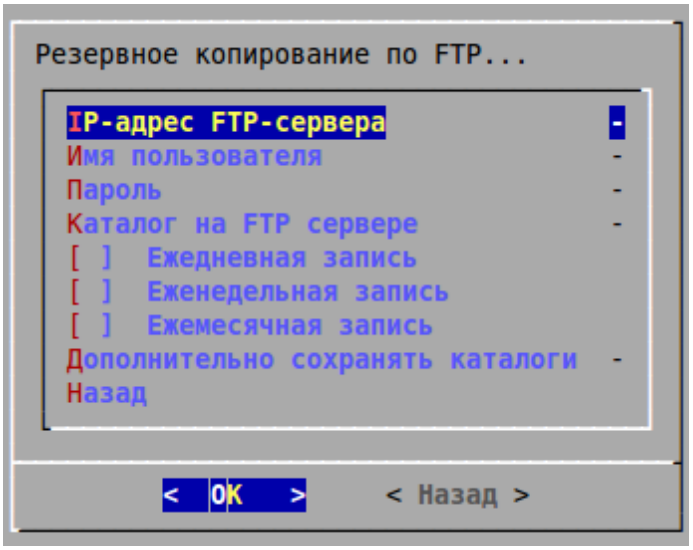


Ежедневная/Еженедельная/Ежемесячная запись - временные интервалы за которые будет производится резервное копирование БД пользователей. Можно выбрать все 3 пункта одновременно.

Дополнительно сохранять каталоги - содержимое указанных каталогов на сервере будет так же записано на диск. (например /var/log/squid)

Записать на CD сейчас - разово осуществить запись на CD.

Резервное копирование на FTP



IP-адрес FTP-сервера - адрес для подключения на удаленный FTP-сервер. На него будут копироваться копии БД.

Имя пользователя - логин для авторизации на FTP-сервере.

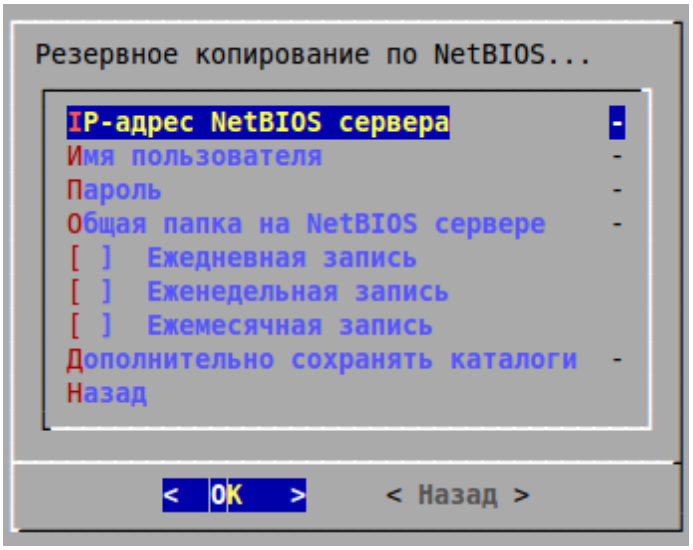
Пароль - пароль для авторизации на FTP-сервере.

Каталог на FTP-сервере - непосредственно в этот каталог будут записываться копии БД.

Ежедневная/Еженедельная/Ежемесячная запись - временные интервалы за которые будет производится резервное копирование БД пользователей. Можно выбрать все 3 пункта одновременно.

Дополнительно сохранять каталоги - содержимое указанных каталогов на сервере будет так же копироваться на FTP-сервер. (например /var/log/squid)

Резервное копирование по NetBIOS



IP-адрес NetBIOS сервера - на компьютер с этим адресом будут передаваться копии БД.

Имя пользователя - логин для авторизации на сетевом ресурсе Windows.

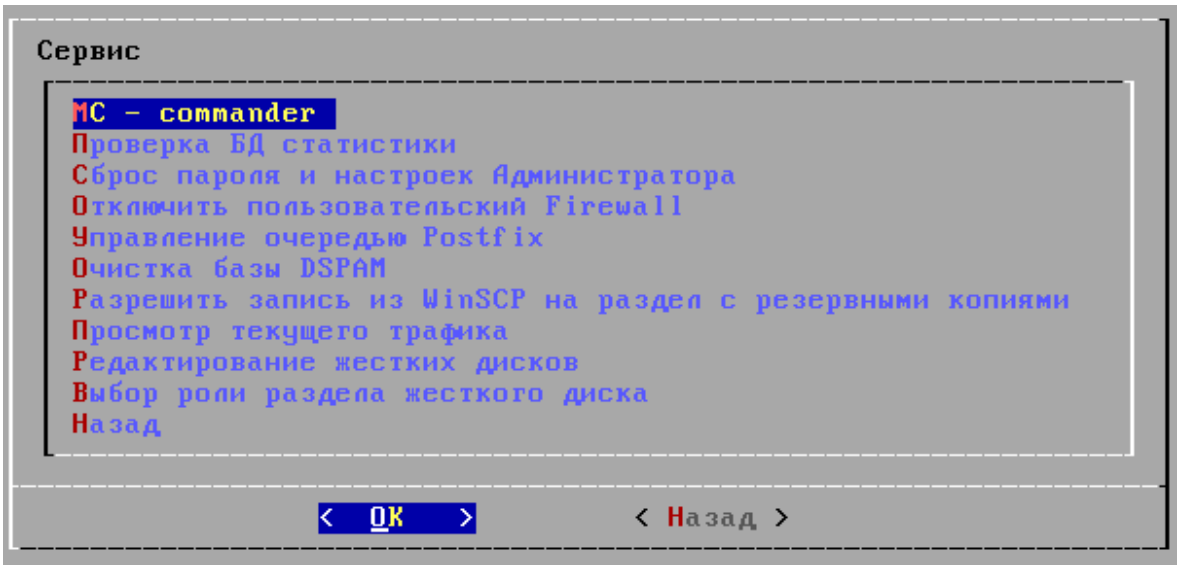
Пароль - пароль для авторизации на сетевом ресурсе Windows.

Общая папка на NetBIOS-сервере - каталог, куда будут записываться копии БД.

Ежедневная/Еженедельная/Ежемесячная запись - временные интервалы за которые будет производится резервное копирование БД пользователей. Можно выбрать все 3 пункта одновременно.

Дополнительно сохранять каталоги - содержимое указанных каталогов на сервере будет так же копироваться на FTP-сервер. (например /var/log/squid)

5.1.5 Сервис



MC-commander – файловый менеджер. Позволяет просматривать файлы журнала, удалять старую статистику src–dst, удалять почтовые сообщения.

Проверка БД статистики – в случае повреждений жесткого диска эта возможность позволит восстановить файлы статистики src–dst.

Сброс пароля и настроек Администратора – если вы забыли пароль Администратора в веб-интерфейсе, или настроили сервер так, что не можете подключиться под Администратором, то этот пункт меню позволит установить его настройки в начальное значение, установить логин Administrator и пароль servicemode, а так же сбросить все настройки запрета доступа под Администратором.

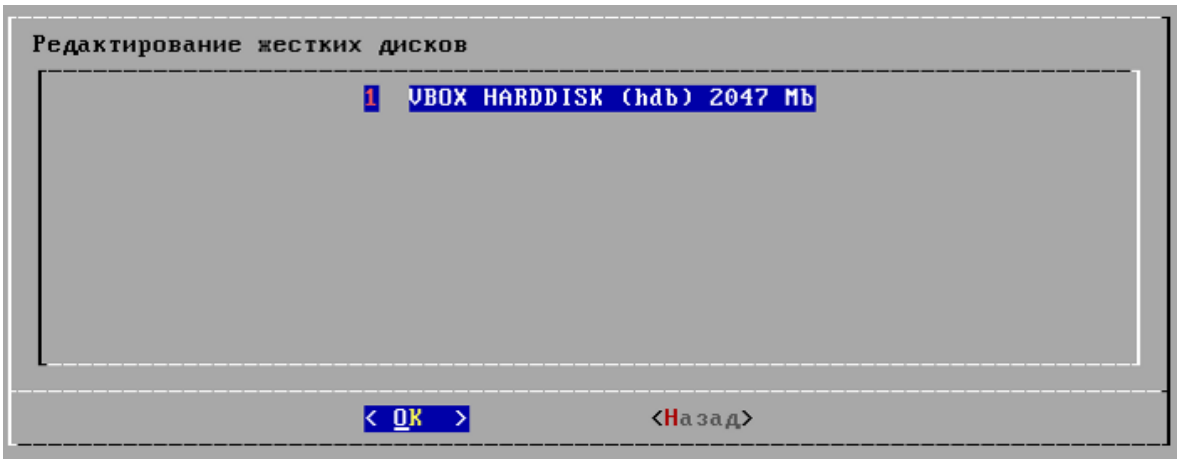
Отключить пользовательский Firewall – Эта команда меню позволяет отключить все правила пользовательского Firewall. При этой операции выключаются все правила Firewall, а сами правила не удаляются. При необходимости можно включать правила по одному, используя веб-интерфейс.

Управление очередью Postfix – Здесь вы можете посмотреть почтовую очередь, очистить и удалить сообщения.

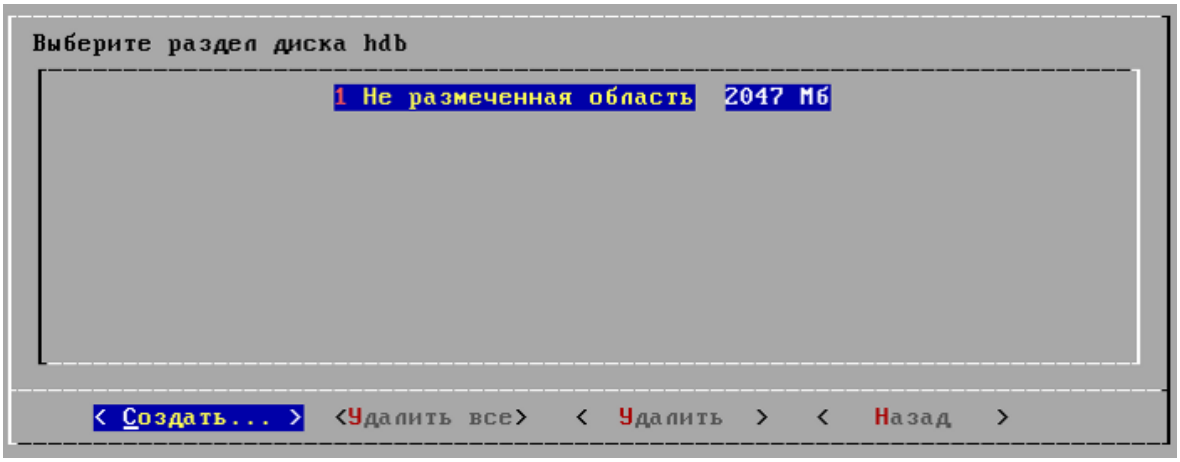
Разрешить запись из WinSCP на раздел с резервными копиями – Эта возможность позволит производить операции записи и удаления на разделе резервных копий через программу WinSCP.

Просмотр текущего трафика – Возможность просмотра трафика бесплатной open-source программой IPTraf . Подробная документация есть на официальном сайте программы - http://iptraf.seul.org/

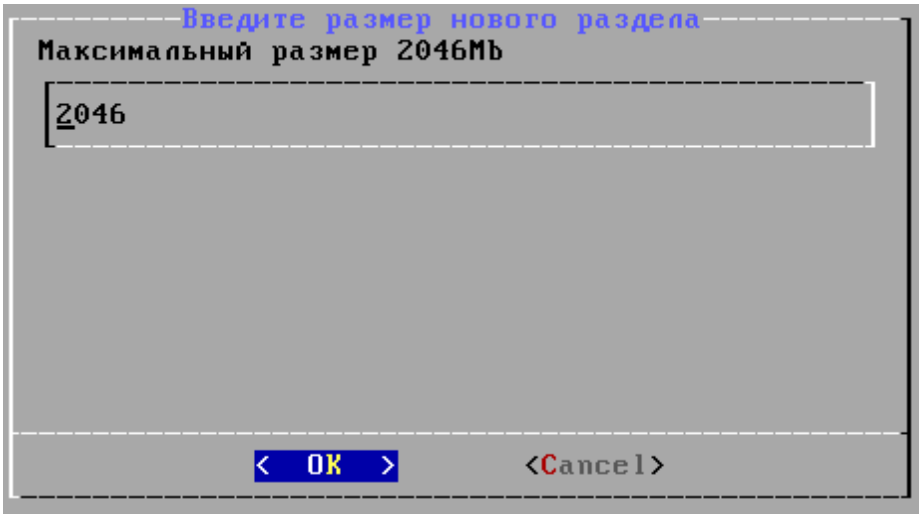
Редактирование жёстких дисков - если к вашему серверу физически подключен дополнительно один или более жестких дисков и они корректно определились ядром системы, то в этом меню вы можете их увидеть. На этом этапе файловая система подключенного диска не имеет значения. Далее мы создадим ее.



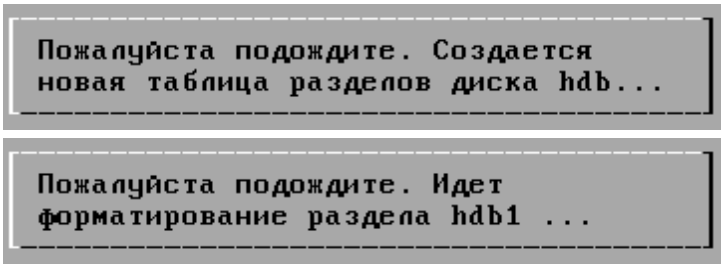
Выберите ваш винчестер. Если на нем не было файловой системы, или файловая система не определилась ядром системы, то вы увидите надпись как на скриншоте. Если же у вас определились разделы, то они будут отражены в меню. Настоятельно рекомендуем удалить все разделы (кнопка <Удалить все>) и в последствии создать раздел(ы) средствами Ideco ACP.



Нажав на кнопку **<Создать>** система спросит у вас какого размера надо будет создать новый логический раздел на винчестере. По умолчанию отводится все доступное на винчестере место для создания одного-единственного логического раздела, что подходит большинству задач в нашем продукте.



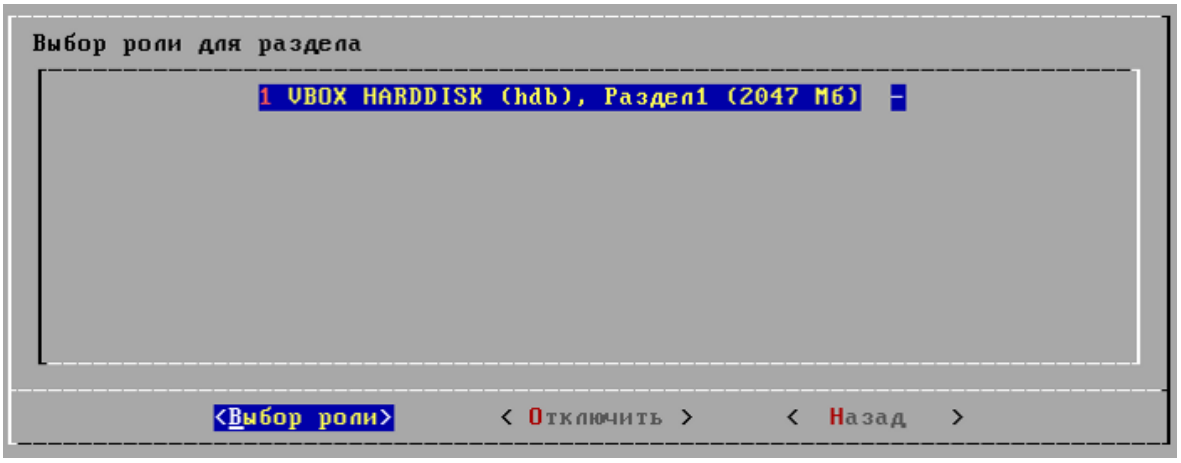
Указав размер система создаст логический диск с файловой системой в формате, наиболее удобном Ideco ACP для работы с данными .



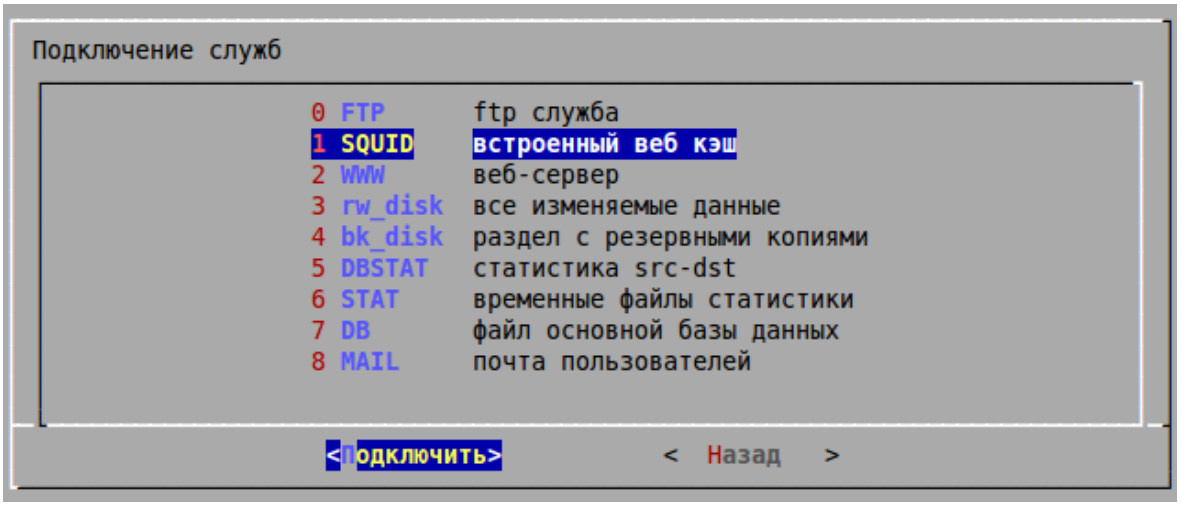
После создания логического раздела (или нескольких) - они будут отражены в локальном меню. Далее можно переходить в раздел "Сервис - Выбор роли раздела жесткого диска"

Выбор роли раздела жесткого диска

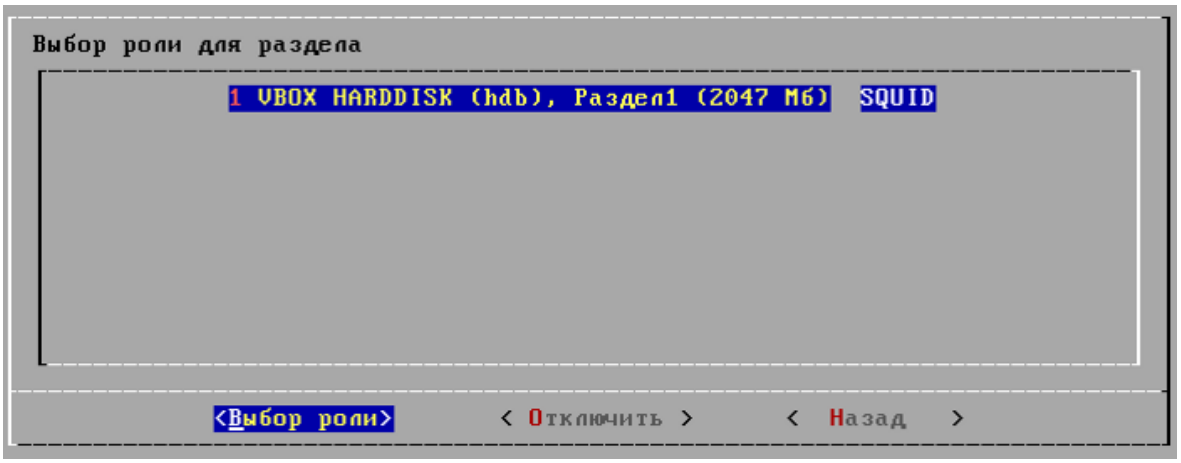
Здесь вам предстоит указать системе для каких целей ей нужно использовать ваш новый размеченный жесткий диск. Для начала выберите логический раздел жесткого диска (в нашем случае один-единственный раздел, который занимает все пространство жесткого диска в 2Гб)



Нажав кнопку **<Выбор роли>** вам будет предоставлен на выбор список служб с кратким описанием того, для чего в каждой из слкжб может быть использован жесткий диск. Вам просто нужно выбрать соответствующий сервис.



После чего в списке логических разделов ваших дополнительных жестких дисков справа напротив раздела будет указано для какой службы используется дисковое пространство вашего винчестера. После всех изменений обязательно сделайте полную перезагрузку сервера.



После полной перезагрузки ваш жесткий диск будет использоваться выбранным вами сервисом по назначению. Настройка завершена.

Примечание: Если вы затрудняетесь в определении роли нового жесткого диска и не можете сказать какая именно служба на сервере потребляет много дискового пространства, то следующий способ может вам в этом помочь:

1. Получите доступ к linux-консоли в Ideco ACP (лучше через SSH, подробнее 120)

2. Проверьте занятость раздела с изменяемыми данными от его общего объема: `df -sh /mnt/rw_disc/`

4. Если вы видите что на разделе осталось совсем немного места (20% или менее), то дальше нужно определить чем занят раздел.

3. Теперь вам нужно с помощью команды "`du -sh /путь/до/каталога/`" просмотреть основные каталоги используемые службами на файловой системе linux сервера Ideco ACP:

`du -sh /var/ftp/` - покажет занятость диска данными ФТП-сервера. Роль №0.

`du -sh /mnt/rw_disc/chroot_squid/var/log/squid/` - покажет сколько занимают на диске логи прокси сервера. **Роль №1**.

`du -sh /var/www/internet/` - объем внешнего сайта (сайтов). **Роль №2**.

Роль №3 позволит перенести весь раздел с изменяемыми данными на новый винчестер. Это стоит делать например тогда когда место на rw_disc активно используеся несколькими службами или изначально вы установили сервер на винчестер маленького объема или неостаточной скорости и хотите улучшить работу дисковой системы сервера. Как было сказано выше, объем всего раздела можно посмотреть так: df -sh /mnt/rw_disc/

`df -h /mnt/bk_disc/` - Аналогично роли №3 вы можете вынести на отдельный винчестер весь раздел предназначенный для хранения резервных копий БД и Конфигурации. **Роль №4**.

`du -sh /var/dbstat/` - покажет сколько места занимает агрегированная статистика пользователей. Как правило счет идет на Гигабайты. Важна скорость заполнения этими данными всего раздела и процент от общего объема раздела с изменяемыми данными. **Роль №5**.

`du -sh /var/stat/` - Временная (сырая) статистика, обычно очищается вовремя при своевременной агрегации. **Роль №6**.

`du -sh /var/db/` - объем занимаемый самой базой данных пользователей Ideco ACP. Как правило имеет небольшой объем. **Роль №7**.

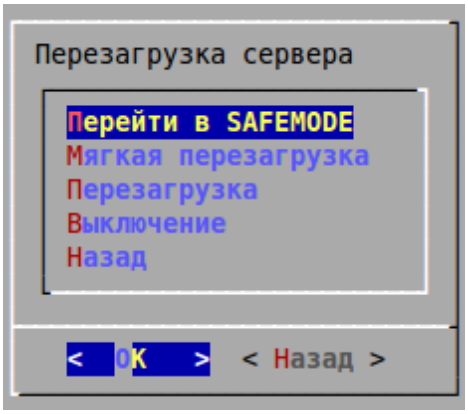
`du -sh /var/spool/mail/` - покажет объем занимаемый всеми почтовыми ящиками и хранимыми в них письмами. Может достигать больших объемов при длительном или интенсивном использовании почтового сервера. **Роль №8**.

5.1.6 Смена пароля

Этот пункт меню позволяет сменить пароль локальной консоли. Будьте внимательны, если вы забудете пароль, то восстановить его можно только полной переустановкой Ideco ACP. Этот пароль также используется для удаленного

администрирования по SSH.

5.1.7 Перезагрузка сервера



Перейти в SAFEMODE – перейти в режим минимальной загрузки компонентов Ideco ACP. В этом режиме работает удаленное администрирование по SSH.

Мягкая перезагрузка – произвести перезагрузку всех программных компонентов. Удобно для проверки настроек сервера. После того как настройки проверены, необходимо полностью перезагрузить сервер, выбрав пункт "Перезагрузка".

Перезагрузка – произвести полную перезагрузку сервера. Это необходимо для гарантированной проверки правильности настроенных параметров. Если все настроено верно, сервер должен загрузиться и нормально функционировать.

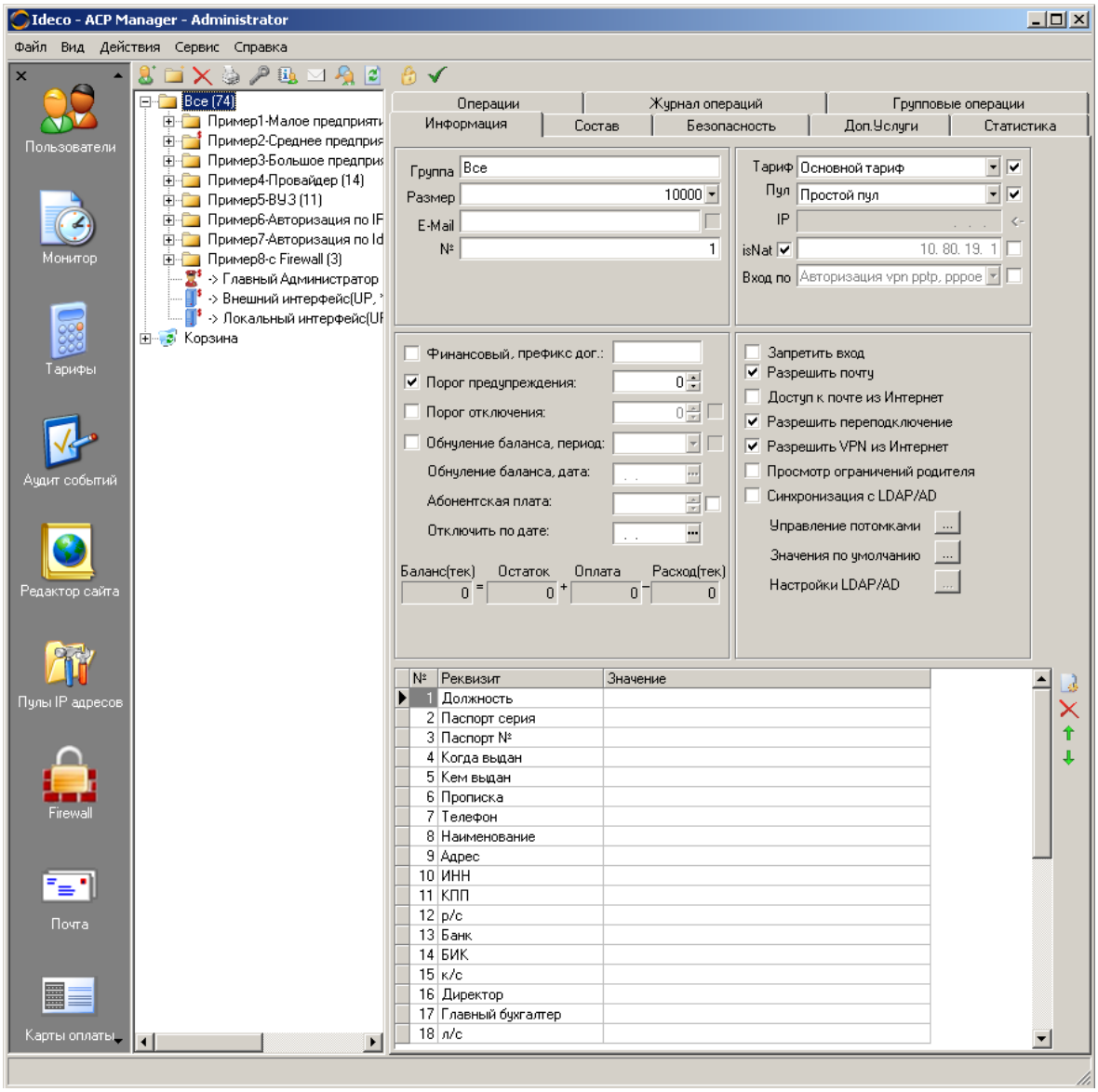
Выключение – Произвести выключение сервера. Необходимо выключить питание компьютера при появлении надписи System halted. Не выключайте питание, пока не появилась это сообщение.

5.2 ACP Ideco Manager

Ideco ACP Manager – приложение под Windows для администрирования Ideco ACP, устанавливаемое на компьютеры администраторов. Предназначено для управления пользователями, редактирования тарифных планов, редактирования встроенного Firewall, просмотра статистики, построение отчетов и другого.

Удобный и понятный интерфейс Ideco ACP Manager позволяет управлять Ideco ACP не только опытным системным администраторам, но и обычным пользователям.

По умолчанию в системе создан **Главный администратор**. Главный администратор имеет полные права, может создавать других администраторов для отдельных групп (Администраторов групп). Администратор может управлять только пользователями группы, в которой находится сам, а также всеми подгруппами этой группы, может создавать других администраторов в пределах своей группы. Это распространяется на все элементы интерфейса ACP Manager. В дереве пользователей, в мониторе и в аудите событий отображаются только "свои" пользователи. Подробнее 183 ..



5.2.1 Установка Ideco ACP Manager

Системные требования

- Компьютер с операционной системой MS Windows 98 или более новой.
- Для построения и печати отчетов MS Excel 97 или более новый.

Установка

Ideco ACP Manager можно установить с компакт диска с дистрибутивом Ideco ACP или с локального сайта:

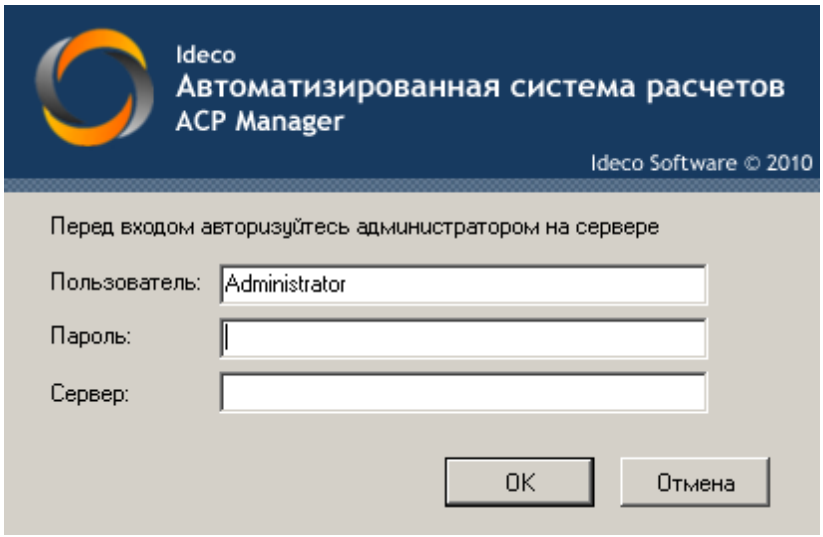
1. Вставьте CD с дистрибутивом Ideco ACP, выберите пункт **ACP Ideco**

Manager, или вручную запустите файл **setup.exe** в каталоге **ICSManager** на установочном компакт-диске. Либо скачайте **setup.exe** с локального сайта http://10.128.0.0/setup.exe и http://10.0.0.1/setup.exe

2. Следуйте инструкциям мастера.

5.2.2 Подключение к Ideco ACP

1. Компьютер администратора, с установленным ACP Manager, должен быть **авторизован** на Ideco ACP (по IP, VPN или другим способом) под учетной записью администратора (подробнее см. Авторизация пользователей на Ideco ACP 60). С компьютеров простых пользователей доступ к ACP запрещен.
2. Запустите Ideco ACP Manager. Появится следующее окно подключения:



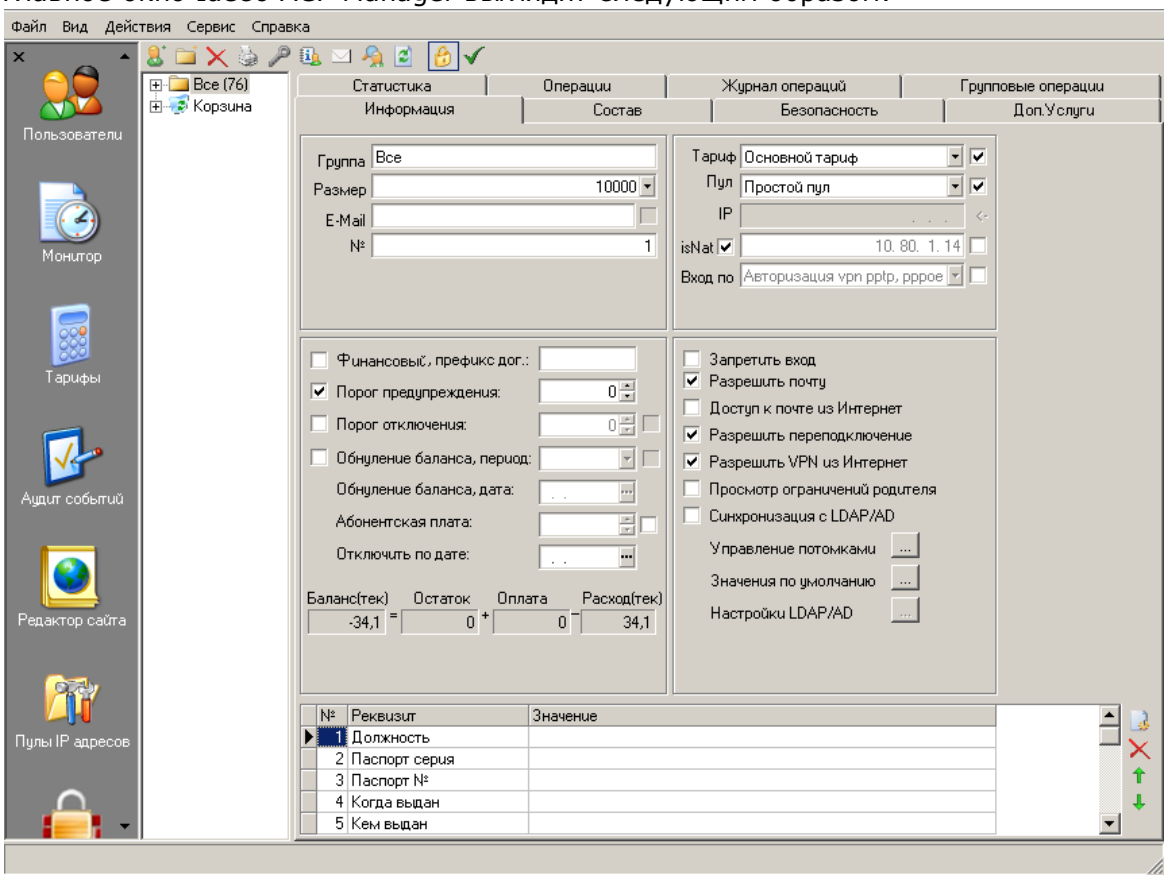
Введите логин и пароль. Укажите закрытый IP-адрес сервера (по умолчанию – "10.128.0.0"). Нажмите кнопку **OK**.

Замечания:

1. Для подключения Ideco ACP Manager необходимо указать защищенный IP-адрес сервера (по умолчанию "10.128.0.0"). Обратите внимание, что это не локальный адрес Ideco ACP.
2. Если Ideco ACP Manager запущен впервые после установки Ideco ACP, то в системе зарегистрирован только один администратор. Поэтому подключайтесь к серверу под пользователем "**Administrator**" с паролем " **servicemode**". Адреса по умолчанию: внутренний адрес сервера для установки VPN-соединения вручную – "10.0.0.1"; защищенный адрес сервера для подключения Ideco ACP Manager – "10.128.0.0".
3. Для работы Ideco ACP Manager используется TCP-порт **3050**. Поэтому, если на компьютере, с которого выполняется подключение, используется персональный Firewall, то в нем необходимо установить соответствующие разрешения.

5.2.3 Главное окно Ideco ACP Manager

Главное окно Ideco ACP Manager выглядит следующим образом:



Главное окно Ideco ACP Manager состоит из следующих элементов:

- **Панель разделов** расположена в левой части главного окна. Позволяет быстро переключаться между разделами с помощью соответствующих кнопок.
- **Главное меню**. Пункт меню "Действия" изменяется в зависимости от раздела, и содержит команды доступные в текущем разделе.
- **Панель инструментов раздела** расположена в верхней части окна. Панель инструментов привязана к текущему разделу, и содержит основные команды доступные в текущем разделе. Вы можете посмотреть функцию каждой кнопки, удерживая над ней курсор около секунды
- **Рабочая область раздела**. Изменяется в зависимости от раздела.

Замечание: В зависимости от прав администратора часть разделов может быть недоступна.

Переключаться между разделами можно с помощью кнопок на **Панели разделов** или из пункта **Вид** главного меню.

Ниже представлено описание разделов:

Раздел	Описание	Примечание
	**Пользователи**. Основной раздел программы. Предназначен для управления пользователями: создание новых, редактирование параметров, управление разрешениями и ограничениями пользователей, выполнение финансовых операций, просмотр статистики и т.д.	**Администраторам групп** доступны пользователи только своей группы.
	**Монитор**. Просмотр пользователей, которые подключены в настоящий момент.	**Администратору группы** показываются пользователи своей группы.
	**Тарифные планы**. Просмотр и редактирование тарифных планов	Создавать и редактировать тарифные планы может только **Главный администратор**. Другим администраторам показываются только те тарифные планы, которые используются у пользователей их группы. Но редактировать эти тарифные планы они не могут.
	**Аудит событий**. Просмотр действий и операций, которые были выполнены администраторами.	**Администратор группы** может видеть события только в своей группе.
	**Редактор сайта**. Позволяет редактировать информацию отображаемую в Личном кабинете пользователя: название организации, раздел "поддержка" и раздел "новости".	Раздел доступен только администраторам, находящимся в корневой группе.
	**Пулы IP-адресов**. Просмотр и редактирование пулов IP-адресов.	Раздел доступен только **Главному администратору**
	**Firewall**. Управление встроенным Firewall.	Раздел доступен только **Главному администратору**
	**Почта**. Позволяет настроить произвольную переадресацию почты и настроить ее фильтрацию.	Раздел доступен только **Главному администратору**
	**Карты оплаты***. Управление картами оплаты.	Раздел доступен **Главному администратору**, а также другим администраторам с установленным признаком " **администратор карт**

оплаты".

5.2.4 Администраторы

Администратор – пользователь, имеющий право управлять Ideco ACP через Ideco ACP Manager.

Всегда есть пользователь **Главный администратор**. Главный администратор имеет полные права, может создавать других администраторов для отдельных групп (Администраторов групп). **Главный администратор** может быть только один и не может быть удален. По умолчанию, логин – **Administrator**, пароль – **servicemode**.

Администратор может управлять только пользователями группы, в которой находится сам, а также всеми подгруппами этой группы, может создавать других администраторов в пределах своей группы. Это распространяется на все элементы интерфейса ACP Manager. В дереве пользователей, в мониторе и в аудите событий отображаются только "свои" пользователи.

Различают администраторов **технических** и **финансовых**, управляющих соответственно техническими или финансовыми параметрами пользователей в пределах своей группы. Один администратор одновременно может являться техническим и финансовым.

Такая структура позволяет сделать управление системой гибкой и в тоже время удобной: передавать управление нижележащим группам, делить администраторов на технических и финансовых. Особенно это относится к крупным предприятиям, в небольших предприятиях обычно достаточно одного администратора.

Для того чтобы создать администратора:

1. Создайте обычного пользователя.
2. Установите у этого пользователя признаки: **Администратор технический** и/или **Администратор финансовый** (подробнее см. Создание пользователя 187 и Закладка "Информация" (у пользователя) 189).

Замечания:

1. Некоторыми параметрами системы может управлять только **Главный администратор**:
   - Редактировать пулы IP-адресов.
   - Редактировать тарифные планы.
   - Переопределять вручную пользователю IP-адрес, пул, адрес NAT.
2. Администраторы, находящиеся в корневой группе, в отличие от администраторов других групп, имеют дополнительные права:
   - Возможность смены тарифного плана пользователя.
   - Имеют доступ к разделу **Редактор сайта**.
   - В случае необходимости могут вручную исправлять баланс пользователей и групп с использование кнопки **Исправить баланс** на

закладке **Операции**.

3. Все администраторы, кроме **Главного администратора**:
   - Не могут изменять параметры группы, в которой находятся сами.
   - Не могут изменять администраторов одного уровня с собой, то есть находящихся непосредственно в этой же группе.
   - Не могут создавать администраторов одного с собой уровня, если этот уровень в дереве расположен до группы с признаком **финансовая**. Это дополнительное разграничение полномочий, так как такие администраторы могут создавать финансовые группы.
4. В редакции Enterprise Edition может быть определен **Администратор карт оплаты**, имеющий права по управлению картами оплаты.
5. Действия администраторов журналируются. Просмотреть их можно в разделе **Аудит событий**.

5.2.5 Управление пользователями

В этом разделе подробно описан процесс создания и управление пользователями в Ideco ICS.

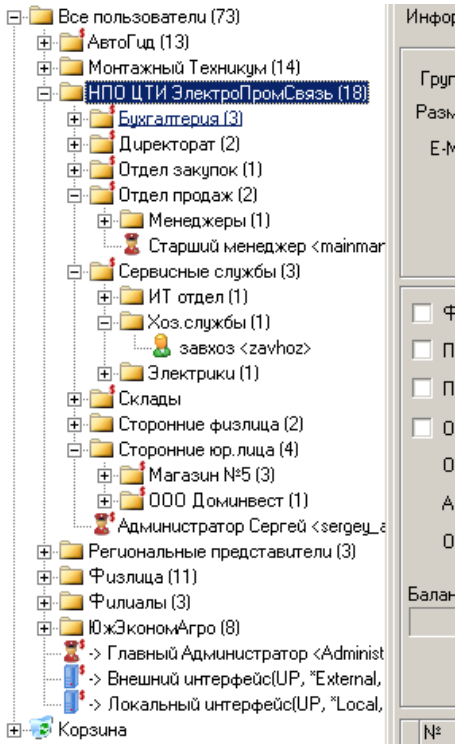
5.2.5.1 Дерево пользователей

Пользователи в Ideco ACP Manager отображаются в виде дерева состоящего из групп пользователей и самих пользователей. Уровень вложенности групп не ограничен.

Древовидная структура позволяет легко отразить реальную структуру предприятия с подразделениями, отделами, офисами и т.п. Позволяет облегчить управление большим количеством пользователей, назначая администраторов для отдельных групп. Такие администраторы групп могут создавать внутри своих групп других пользователей, группы, администраторов для нижележащих групп.

Древовидная структура и принцип наследования позволяет легко задавать и изменять общие параметры для пользователей, определяя их для родительской группы: тарифный план, пул IP-адресов, параметры ограничений и разрешений, отключать, выполнять групповые операции для всех пользователей группы. При этом при необходимости для отдельных пользователей можно переопределить отличные от общих параметров признаки.

Дерево пользователей выглядит следующим образом:



В дереве отображаются названия групп и пользователей, а у пользователей в скобках также указывается логин.

В дереве используются следующие обозначения:

Группа пользователей

Пользователь с NAT. Пользователь с установленным признаком isNat и защищенным посредством NAT. Подробнее см. Использование NAT 206.

Пользователь без NAT (сервер). Пользователь со снятым признаком isNat. Как правило, это серверные учетные записи

Администратор. Пользователь с установленным признаком "администратор технический" или "администратор финансовый".

Финансовый. Символ **$** означает, что у пользователя или группы установлен признак финансовый. Подробнее см. Признак "Финансовый" 205.

Подключен. Стрелка означает, что пользователь в настоящее время подключен.

Ниже представлено описание кнопок Панели инструментов:

Создание нового пользователя. Подробнее см. Создание пользователя 187.

Создание новой группы. Подробнее см. Создание группы 186


Удаление пользователя или группы. Подробнее см. Удаление пользователей 209.


Восстановление пользователя или группы.


Смена пароля пользователя. Подробнее см. Смена пароля 213.


Проверка параметров пользователя и возможности пользователя выйти в Интернет. Подробнее см. Проверка пользователя 213


Отправить сообщение по e-mail и winpopup. Подробнее см. Оповещение пользователей 214


Поиск пользователей. Подробнее см. Поиск пользователей 210.


Обновить данные


Режим только для чтения. Для предотвращения случайного изменения данных на закладке **Информация**.


Сохранение изменений после редактирования свойств на закладке "Информация"

Информация по группе или по пользователю отображается на закладках справа от дерева. При перемещении по дереву информация на закладках обновляется.

Основные операции по управлению пользователями, такие как создание группы, создание пользователя, смена пароля и т.п. доступны с помощью кнопок панели инструментов, а также из контекстного меню – вызываемого щелчком правой кнопки мышки по дереву.

У пользователя доступны следующие закладки: **Информация**, **Статистика**, **Операции**, **Журнал операций**. У группы есть две дополнительные закладки: **Состав** и **Групповые операции**.

Назначение и описание закладок см. в разделах:

- Закладка "Информация" (у пользователя) 189
- Закладка "Информация" (у группы) 194
- Закладка "Статистика" 200
- Закладка "Операции" 202
- Закладка "Состав" (у группы) 203
- Закладка "Журнал операций" 254
- Закладка "Групповые операции" 254

5.2.5.2 Создание группы

Чтобы создать новую группу пользователей:

- В дереве выберите ту группу, в которой вы хотите создать новую. На

панели инструментов нажмите кнопку  **Создать группу**, или

- Щелкните правой кнопкой мышки на группе, в которой хотите создать новую группу, и выберите пункт **Создать группу...**

Появится следующее окно:

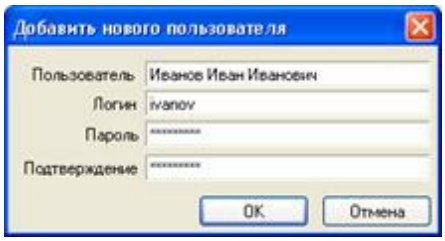
Заполните название новой группы пользователей. После создания группы, задайте остальные свойства группы на закладке "Информация" (подробнее см. Закладка "Информация" (у группы) 194).

5.2.5.3 Создание пользователя

Чтобы создать пользователя:

- В дереве пользователей выберите ту группу, в которой вы хотите создать пользователя, и на панели инструментов нажмите кнопку  **Создать пользователя**, или
- Щелкните правой кнопкой мышки на группе, в которой хотите создать пользователя, и выберите пункт **Создать пользователя...**

Появится следующее окно:



Заполните поля

Пользователь – имя пользователя

Логин – логин пользователя

Пароль – пароль пользователя

Подтверждение пароля.

Замечания:

Логин и пароль используются для авторизации, а также для подключения с помощью ACP Manager, если пользователь является администратором. Пользователи, импортированные из AD, проходят проверку пароля средствами AD.

Логин и пароль необходимо вводить латинскими символами, соблюдая регистр.

Посмотреть или восстановить пароль пользователя нельзя. Поэтому пароль необходимо либо сразу сообщить пользователю, либо записать. Также рекомендуется напоминать пользователям, о том, чтобы они обязательно сменили пароль в Личном кабинете. В случае необходимости, администратор может сменить пароль.

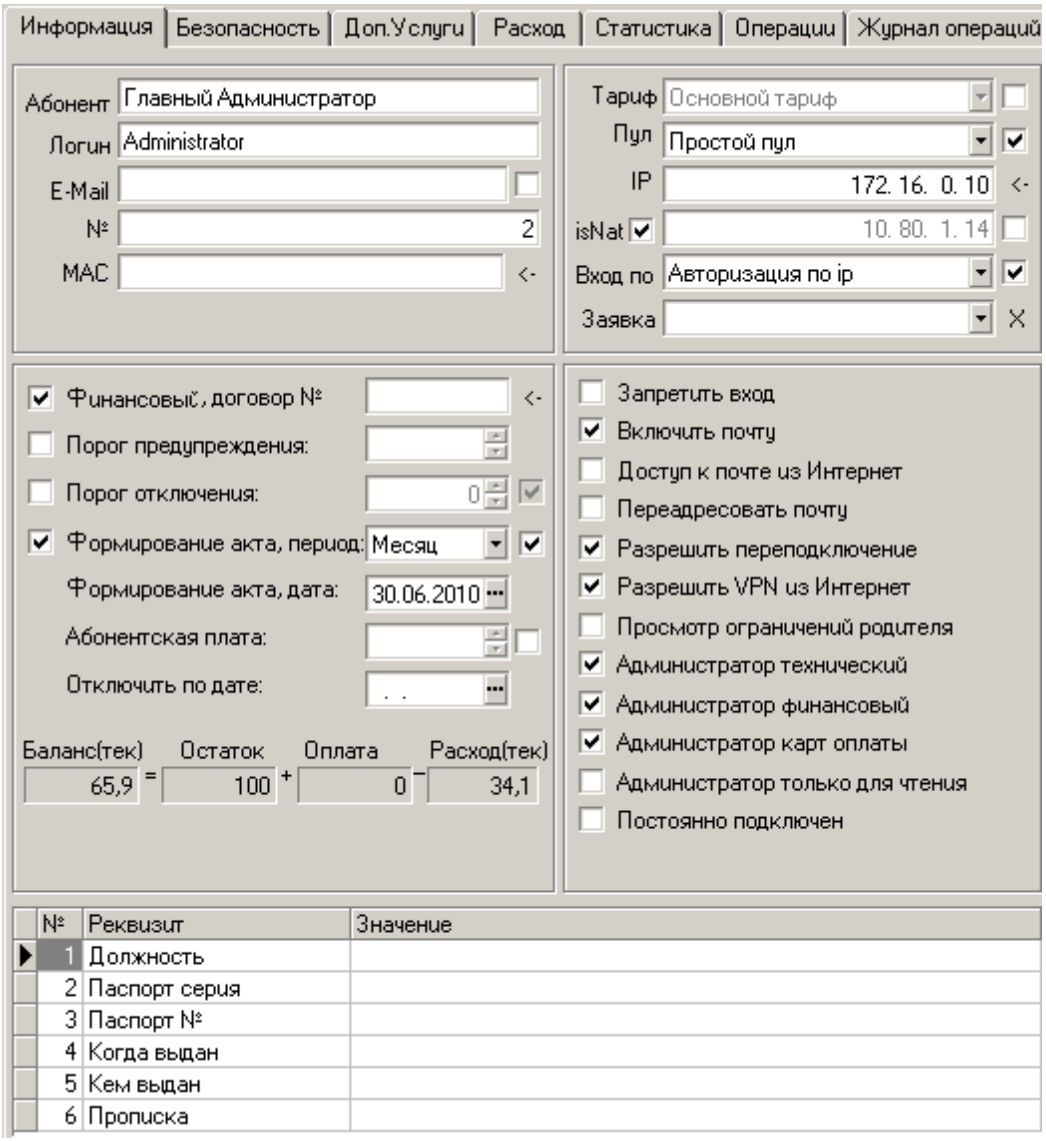
Нажмите кнопку **ОК**. В текущей группе будет создан пользователь. При этом автоматически установлены следующие свойства:

6. **Тарифный план**, **адрес NAT**, **пул IP-адресов** унаследованы от родительской группы.
7. **IP-адрес** автоматически установлен из пула – выбирается первый не занятый IP-адрес в пуле.
8. Признак **Финансовый** установится, если выше по иерархии нет финансовой группы, и снимется, если такая группа есть.

Параметры созданного пользователя редактируются на закладке "Информация" (подробнее см. Закладка "Информация" (у пользователя) 189).

5.2.5.4 Закладка "Информация" (у пользователя)

На закладке **Информация** отображаются параметры выбранного пользователя.



Замечания:

В зависимости от прав администратора можно изменять все или только часть параметров.

Для редактирования свойств пользователя нужно с помощью кнопки  на панели инструментов отключить режим **Только для чтения**. При запуске программы он устанавливается по умолчанию.

Параметры пользователя условно сгруппированы по смыслу и описываются в разделах:

- Общие параметры 190
- Параметры ограничений 191

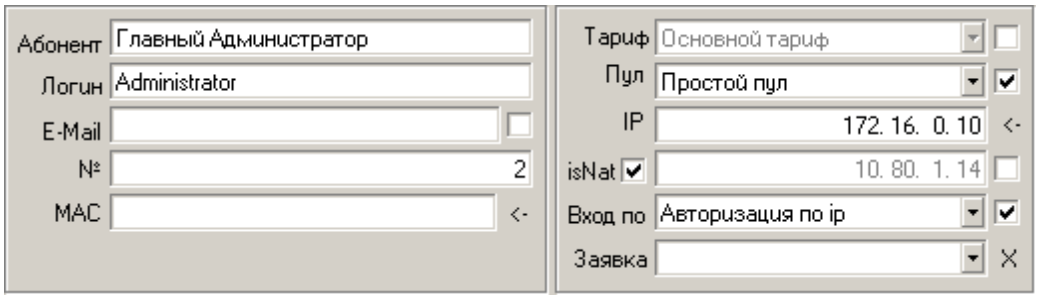
- Параметры разрешений[193]

Внизу закладки **Информация** отображается таблица с **реквизитами**. Вы можете создавать свои реквизиты. Список реквизитов общий для всех пользователей и групп. Реквизиты носят информационный характер и могут выводиться в шаблоны документов. Подробнее см. Закладка "Групповые операции"[254].

После изменения свойств пользователя нажмите кнопку **Сохранить** на панели инструментов. В случае перехода к другому пользователю при несохраненных изменениях – будет выдано предупреждение.

Замечание: При сохранении некоторых свойств пользователя, соединение, установленное этим пользователем может отключиться. Это не распространяется на соединение**Главного Администратора.**

5.2.5.4.1 Общие параметры



Абонент – Имя пользователя (например, Фамилия Имя Отчество сотрудника или название сервера).

Логин – логин пользователя.

E-mail – на этот адрес будут отправляться служебные сообщения. Если установлена галочка справа, то это будет почтовый ящик пользователя на сервере.

№ – уникальный идентификатор пользователя, никогда не повторяется и не изменяется.

Тариф – тарифный план, в соответствии с которым происходит тарификация для этого пользователя.

Пул – пул IP-адрес, из которого был назначен IP-адрес пользователю.

IP – IP-адрес пользователя. Кнопка <- позволяет получить свободный IP-адрес из пула.

MAC – MAC-адрес компьютера, используется для привязки и/или для раздачи закрепленных IP по DHCP.

isNat – признак того, что для текущего пользователя используется маскировка NAT. Здесь же отображается IP-адрес NAT, которым прикрывается пользователь выходящий в Интернет.

Замечания:

9. Значения полей **Тариф**, **Пул**, **Адрес Nat** по умолчанию не заданы и наследуются от родительской группы. То есть при смене этих атрибутов у группы, они автоматически начинают действовать на вложенных пользователей.

   Для того чтобы переопределить значения этих параметров вручную:

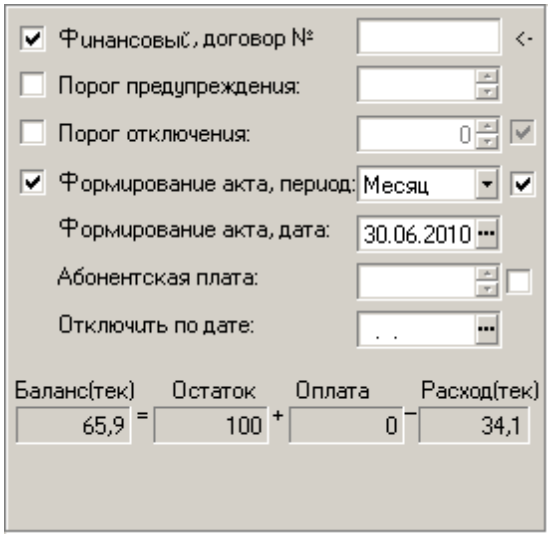
   - Установите флажок ☑ (переопределить вручную) справа от нужного поля.
   - Задайте значение параметра вручную.

10. Если у пользователя вручную установлен **Тарифный план**, то **Адрес NAT** по умолчанию ставится равным IP-адресу интерфейса указанного в тарифном плане.
11. При изменении свойства **Пул** у пользователя или у группы, IP-адрес пользователя автоматически не меняется и остается прежним. **Пул** используется при создании пользователя, а также при нажатии кнопки <-. При этом ему назначается IP-адрес из пула.
12. У большинства пользователей рекомендуется использовать флажок ☑ **isNAT**. Такие пользователи защищены технологией NAT.

    Для того, чтобы создать **пользователя без NAT**:

    - В поле **IP** введите один из реальных IP-адресов, выданных провайдером. Или выберите из заранее созданного пула реальных IP-адресов.
    - Снимите флажок ☑ isNAT.

5.2.5.4.2 Параметры ограничений



Финансовый

Признак того, что пользователь несет финансовую ответственность за использование Интернет и сам оплачивает расходы за Интернет. Такой пользователь называется **финансовым**. Как правило, в обычных организациях все пользователи нефинансовые. Подробнее см. Признак "Финансовый" 205.

Порог предупреждения

Если этот признак установлен, то пользователю будет выслано e-mail и winpopup сообщение, когда баланс пользователя достигнет указанного значения. Подробнее см. Оповещение пользователей 214

Порог отключения

В случае если этот признак установлен, то когда баланс пользователя достигнет указанного значения, ему автоматически будет закрыт доступ в платные сети и выслано оповещение. Можно указать отрицательное значение для работы в кредит. Подробнее см. Баланс пользователя и группы, порог отключения 204.

Автоматическое обнуление баланса

Эта функция доступна только у нефинансовых пользователей. Позволяет с заданной периодичностью обнулять баланс пользователя. При этом поля остаток, расход и оплата обнуляются. Подробнее об использовании этой возможности см. Автоматическое обнуление баланса 207.

У финансовых пользователей взамен "Обнуление баланса" есть функция "Формирование акта". Подробнее см. Автоматическое формирование акта 247.

Абонентская плата

Автоматическое списание суммы со счета пользователя за каждый период, совпадающий с периодом автоматического обнуления баланса (формирования акта).

Отключить по дате

После указанной даты система отключит пользователя, и он не сможет авторизоваться.

Баланс

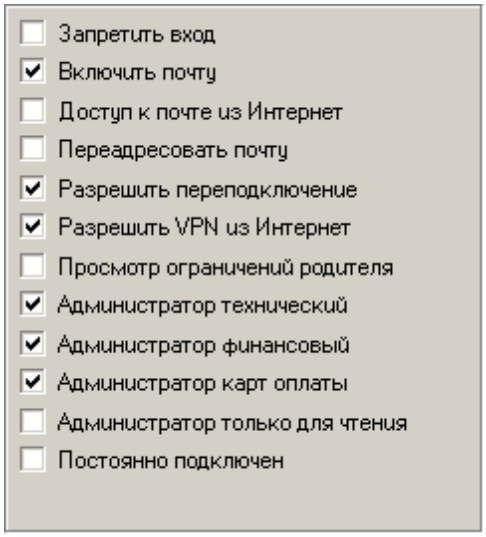
Отображается текущий баланс пользователя в условных единицах, а также остаток, расход и оплата. Подробнее см. Баланс пользователя и группы, порог отключения 204.

Замечания:

13. Как правило, признак **Финансовый** устанавливается у конечных пользователей только в случае, если предприятие оказывает услуги по доступу в Интернет физическим лицам.
14. Если признак **Порог отключения** не установлен, то это означает, что баланс пользователя неограничен, и пользователь использует Интернет без ограничений. Это может привести к неограниченным расходам, если у вышестоящих групп ограничение также отсутствует.
15. Значение параметра **Порог отключения**, а также параметры **обнуления баланса**, можно переопределять для всех пользователей группы. Для этого у группы на закладке **Информация** есть кнопка **Управление потомками...** (подробнее). В случае, если нужно чтобы у пользователя, всегда оставались свои (отличные от других пользователей) настройки, необходимо запретить автоматическое переопределение параметров с

помощью флажка **Изменять только вручную** справа от полей **Порог отключения** или **Обнуление баланса, период**.

5.2.5.4.3 Параметры разрешений



Запретить вход
Означает блокирование пользователя. В этом случае он не сможет установить VPN-соединение с сервером. Если пользователь является администратором, то он также не сможет работать с Ideco ACP Manager.

Включить почту
В случае если признак установлен, то пользователю автоматически создается почтовый ящик на сервере.

В редакции Standard Edition в качестве примера каждый пятый пользователь может иметь почтовый ящик, но не более 15-ти почтовых ящиков во всей системе. Разрешить доступ к корпоративной почте из Интернет по защищенным протоколам IMAPS, POP3S, HTTPS.

Переадресовать почту
Автоматически переадресовывать письма, приходящие на встроенный почтовый ящик на адрес, указанный в общих параметрах пользователя.

Разрешить переподключение

Если признак установлен, то пользователь сможет установить соединение с сервером, даже если оно уже установлено с другого компьютера. Например, если он забыл его отключить. Прошлое соединение будет разорвано. Подробнее см. Переподключение 210.

Разрешить удаленное подключение

Означает возможность VPN подключения к внешнему адресу Ideco ACP. Например, в случае нахождения пользователя дома или в командировке. Подробнее см. Удаленное подключение 211.

Просмотр ограничения родителя

Разрешить пользователю просматривать ближайшее ограничение вышестоящих групп. Страница "Информация" 74

Администратор технический, **Администратор финансовый**

В случае если признак установлен, то пользователь является администратором и может управлять техническими или финансовыми параметрами пользователей группы, в которой находится сам. Подробнее см. Администраторы 183.

Администратор карт оплаты

Пользователь сможет управлять картами оплаты. Доступно только в редакции Enterprise Edition.

LDAP/AD-пользователь

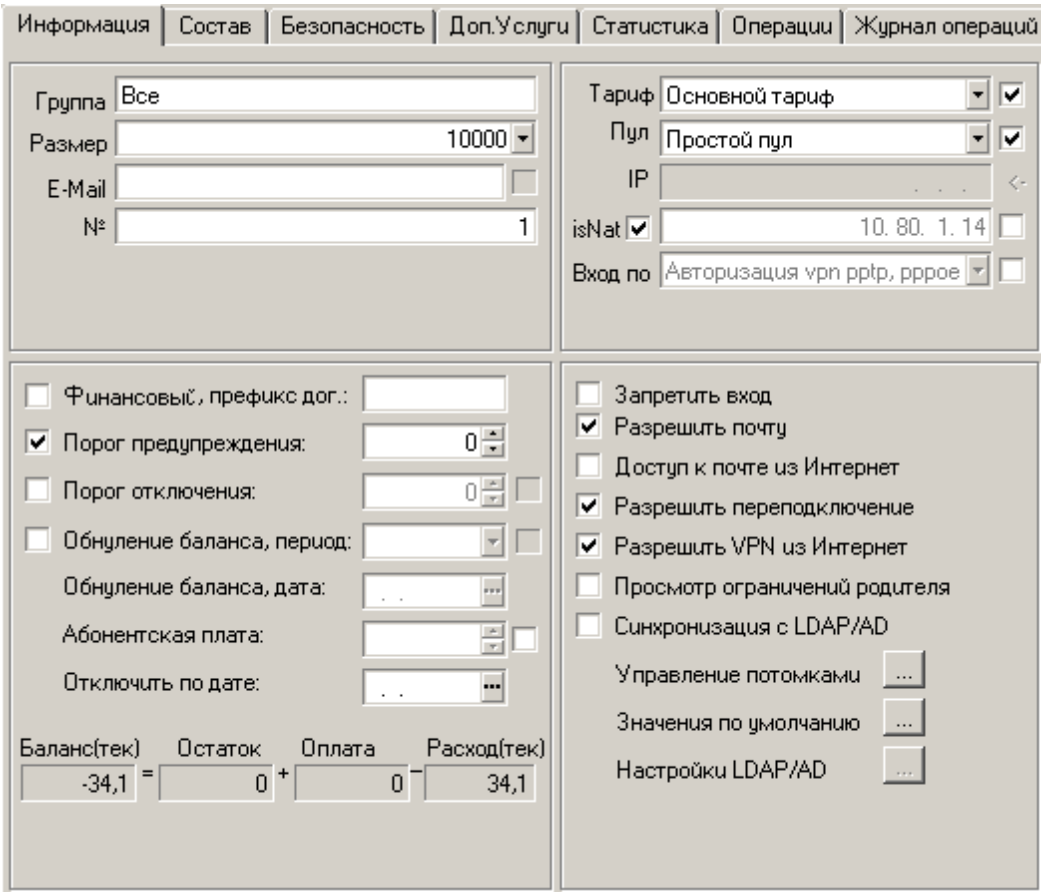
Этот пользователь синхронизируется с доменом Windows. Тоесть проверка пароля и установка некоторых параметров пользователя производится с помощью домена Windows.

Постоянно подключен

Пользователь будет считаться подключенным к серверу, даже если выключен его компьютер.

5.2.5.5 Закладка "Информация" (у группы)

На закладке информация отображаются свойства группы выбранной в дереве пользователей.



Замечания:

В зависимости от прав администратора можно изменять все или только часть параметров. Для редактирования свойств группы нужно с помощью кнопки на панели инструментов отключить режим **Только для чтения**. При запуске программы он устанавливается по умолчанию.

Большинство параметров группы совпадают с параметрами, имеющимися у пользователя. Все параметры условно сгруппированы по смыслу и описываются в разделах:

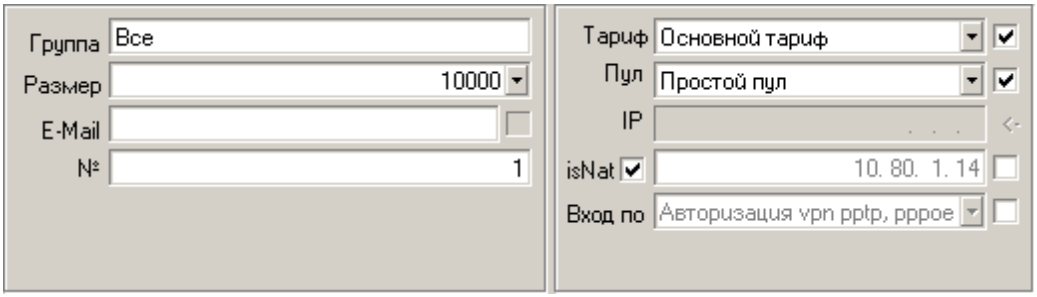
- Общие параметры 196
- Параметры ограничений 197
- Параметры разрешений 198

Внизу закладки Информация отображается таблица с **реквизитами**. Подробнее см. Реквизиты пользователя и группы 248.

После изменения свойств группы нажмите кнопку **Сохранить** на панели инструментов.

Замечание: При сохранении некоторых свойств группы, соединения, установленные пользователями этой группы могут отключиться.

5.2.5.5.1 Общие параметры



Группа – Название группы (например, это может быть название отдела или название сторонней организации).

Размер – максимальное количество пользователей в группе, включая все вложенные группы. Если размер равен нулю, это означает, что размер группы неограничен.

E-mail – на этот адрес могут отправляться служебные сообщения

№ – уникальный идентификатор группы, никогда не повторяется и не изменяется.

Тариф – тарифный план, в соответствии с которым происходит тарификация пользователей группы.

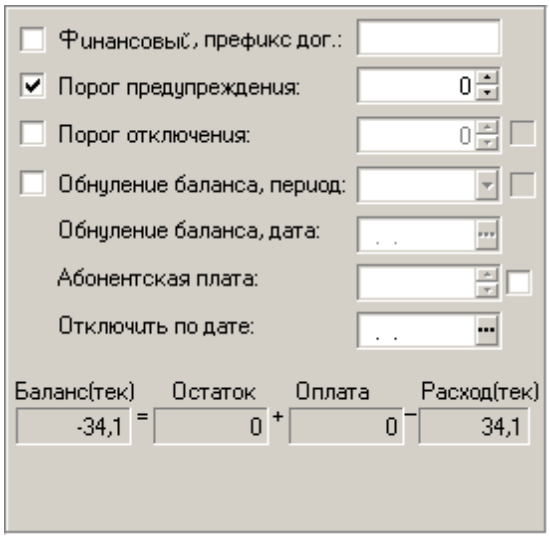
Пул – пул IP-адресов, из которого назначаются IP-адреса пользователей группы.

isNat – признак того, что для пользователей группы используется NAT.

Замечание: Значения полей Тариф, Пул, и адрес NAT по умолчанию не заданы и наследуются от родительской группы. При необходимости использовать значения отличные от родительской группы, необходимо установить галочку рядом с полем и ввести требуемое значение. После этого значение от родительской группы наследоваться не будет.

Вход по: - Тип авторизации клиента на сервере Ideco ACP. От типа авторизации зависит тип подключения клиентского ПК к серверу. Подробное описание каждого типа авторизации см. здесь 60.

5.2.5.5.2 Параметры ограничений



Финансовый
Признак того, что группа является **финансовой**, т.е. несет финансовую ответственность за использование Интернет и сама планирует и оплачивает расходы за Интернет. Подробнее см. Признак "Финансовый" 205.

Порог предупреждения

Если это признак установлен, то когда баланс группы достигнет указанного значения, на e-mail указанный в свойствах группы будет выслано сообщение.

Порог отключения

В случае если этот признак установлен, то когда баланс группы достигнет указанного значения, всем пользователям группы автоматически будет закрыт доступ в платные сети и на e-mail указанный в свойствах группы будет выслано сообщение. Можно указать отрицательное значение. Подробнее см. Баланс пользователя и группы, порог отключения 204.

Автоматическое обнуление баланса

Эта функция доступна только у нефинансовых групп. Позволяет с заданной периодичность обнулять баланс группы. При этом поля остаток, расход и оплата обнуляются. Подробнее об использовании этой возможности см. Автоматическое обнуление баланса 207.

У финансовых групп вместо "Обнуления баланса" есть функция "Формирование акта". Подробнее см. Автоматическое формирование акта 247.

Абонентская плата
Автоматическое однократное списание со счета группы за каждый период автоматического обнуления баланса.

Отключить по дате
Эта функция позволяет запретить подключение пользователя или группы после указанной даты

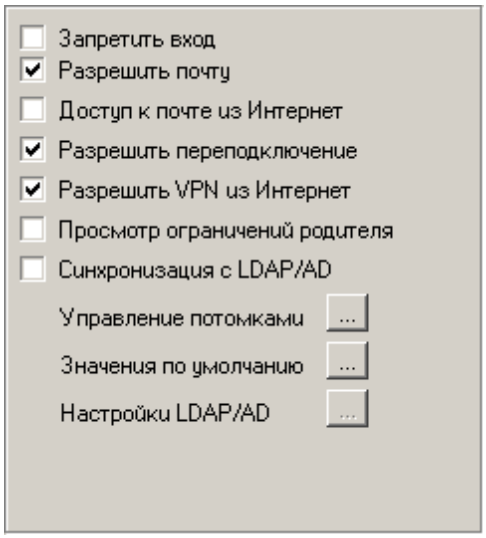
Баланс
Отображается текущий баланс группы в условных единицах, а также остаток, расход и оплата. Подробнее см. Баланс пользователя и группы, порог отключения

204.

Замечания:

1. Как правило, признак **Финансовый** используется у групп пользователей, в случае, когда они сами определяют свои расходы на Интернет. Например, такими группами могут быть или крупные подразделения предприятия, или сторонние организации.
2. Если признак **Порог отключения** не установлен, то это означает, что баланс группы неограничен, и может сколь угодно "уходить в минус".

5.2.5.5.3 Параметры разрешений



Важно! Обратите внимание, что параметры **Запретить вход**, **Разрешить почту**, **Разрешить переподключение**, **Разрешить удаленное подключение**, в отличие от таких же параметров пользователя, имеют несколько другой смысл. А параметр **Запретить вход** отличается по способу действия от остальных параметров.

Запретить вход

Означает блокирование всех пользователей группы, включая все вложенные группы. Если признак установить, то в этом случае пользователи этой и всех вложенных групп не смогут установить соединение с сервером и выйти в Интернет. При этом значение признака **Запретить вход** у вложенных пользователей и групп значения не имеет.

Разрешить почту, **Разрешить переподключение**, **Разрешить удаленное подключение**, **Просмотр ограничения родителей**

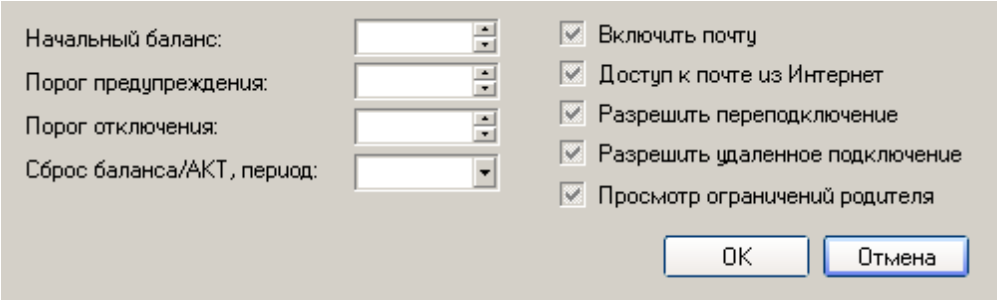
Означает возможность администраторов этой группы управлять соответствующими параметрами пользователей этой группы. При этом, на соответствующую возможность пользователя установки этих параметров не влияют. То есть, если у групп установить признак "Разрешить почту", то администратор этой группы, сможет устанавливать и убирать признак "Разрешить почту" у своих пользователей. И наоборот, если признак "Разрешить почту" не

установлен, то администратор группы не сможет ни установить признак "Разрешить почту" у своих пользователей, ни убрать его.

Подробнее о работе самих параметров у пользователей см.:

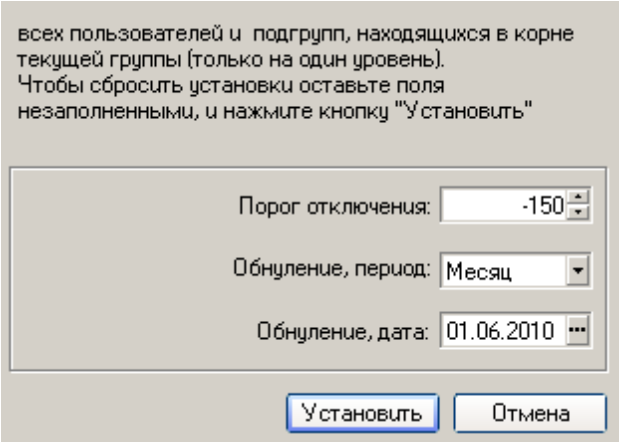
- Переподключение 210
- Удаленное подключение 211

Значения по умолчанию для новых пользователей



Все новые созданные пользователи этой группы будут иметь указанные значения. На пользователей вложенных групп установка не распространяется.

Управление потомками



Позволяет установить для всех пользователей и групп, находящихся непосредственно в текущей группе, значение параметров **Порог отключения**, **Период** и **Дата автоматического обнуления баланса**.

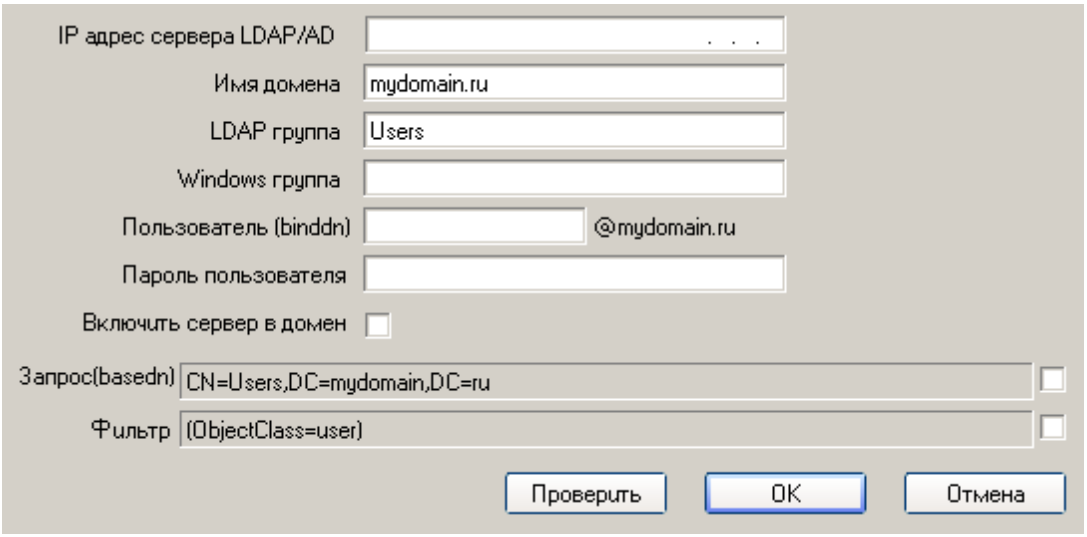
Для этого установите нужные значения и нажмите кнопку **Установить**.

Замечания:

1. Значения устанавливаются только для пользователей и групп находящихся в корне текущей, то есть на пользователей вложенных групп установка не производится.
2. Для того что бы убрать признаки **Порог отключения** и **Обнуления баланса** у дочерних пользователей нужно оставить поля не заполненными и нажать кнопку **Установить**.
3. Если в настройках пользователя на закладке **Информация**, рядом с признаками "Порог отключения" и "Обнуление баланса, период", установлен

флажок  (изменять только вручную), то для них изменение соответствующих признаков при нажатии кнопки **Установить** происходить не будет.

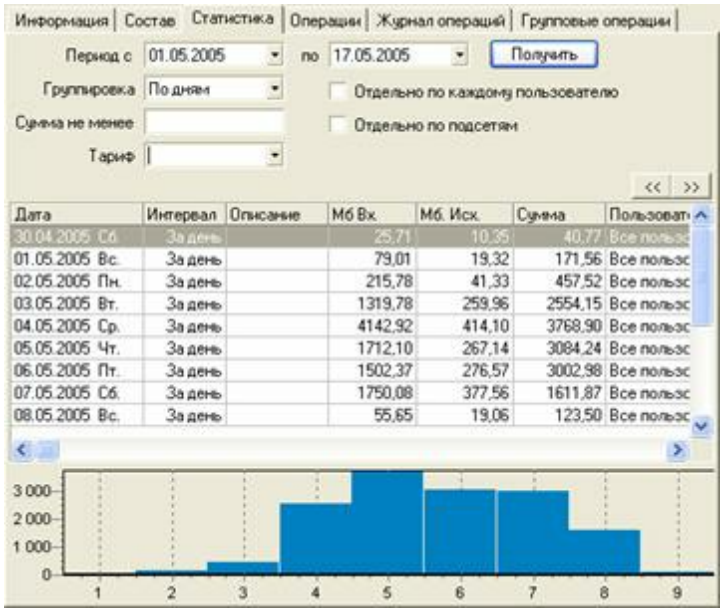
Настройка синхронизации с LDAP/AD сервером



Необходимо указать IP-адрес контроллера домена, имя домена, пароль пользователя с правами просмотра пользователей. При авторизации VPN через AD необходимо включить сервер в домен, потребуется пароль администратора домена. LDAP группа в AD по умолчанию Users.

5.2.5.6 Закладка "Статистика"

Для просмотра статистики выберите в дереве пользователей нужную группу или пользователя. Перейдите на закладку **Статистика**. На этой закладке отображается статистика расхода трафика в МБ и денежном эквиваленте.



Для выбора статистики:

4. Задайте параметры выбора, группировки и отображения статистики:

   Период – укажите период, за который нужно получить статистику.

   Группировка – выберите как группировать статистику: "По сессиям", "По дням", "По месяцам", "По годам", "Нет" (суммарная).

   Сумма не менее – позволяет выводить только те записи, у которых значение поля "Сумма" более указанной.

   Отдельно по каждому пользователю – в случае, если запрашивается статистика по группе, то статистика будет выводиться отдельно по каждому пользователю этой группы.

   Отдельно по подсетям – статистика будет выводиться отдельно по подсетям тарифных планов.

5. После задания параметров выборки нажмите кнопку **Получить**.

   В таблице показываются следующие поля: **Дата**, **Интервал**, **Описание**, **Мб. Вх**, **Мб. Исх.**, **Сумма**, **Пользователь**.

   В случае группировки **По сессиям**:

   · поле **Дата** выводится дата и время начала сессии.

   · в поле **Интервал** продолжительность сессии.

Замечания:

6. В Ideco ACP одновременно ведется две разные по смыслу статистики: **Основная статистика**, рассматриваемая в этом разделе, и **Детализированная статистика** (Статистика посещений или статистика "source–destination"). В основной статистике учет ведется по сессиям пользователей. Одна сессия пользователя равняется одному установленному им авторизованному соединению. При этом для каждой сессии фиксируется:

- Пользователь
- IP-адрес компьютера, с которого было установлено соединение
- Время начала сессии
- Продолжительность сессии
- Объем входящего и исходящего трафика для каждой подсети тарифного плана за время сессии.
- Расход в денежном эквиваленте

В большинстве случаев такой статистики является достаточно как для администраторов так и для пользователей. Поэтому эта статистика является основной. При необходимости получения более подробной информации (IP-адрес источника и получателя, время и т.п.), нужно обратиться к детализированной статистики.

7. При выводе статистики учитывается незакрытые сессии пользователей, тоесть сессии установленные в текущий момент.
8. В некоторых случаях соединение может быть установлено продолжительное время. Но в статистике вы никогда не увидите сессий с продолжительностью больше 24 часов. Это связано с тем, что с периодичностью в 24 часа происходит "виртуальный сброс" сессий. При этом само соединение не сбрасывается. Поэтому, например, соединение было установлено 30 дней, при этом ни разу не сбросившись, а в статистике будет отображаться 30 сессий.
9. **Основная статистика**, а также **Детализированная статистика** доступны в Личном кабинете пользователям. При этом пользователи могут посмотреть только свою статистику, а администраторы могут посмотреть статистику по всем пользователям своей группы.

5.2.5.7 Закладка "Операции"

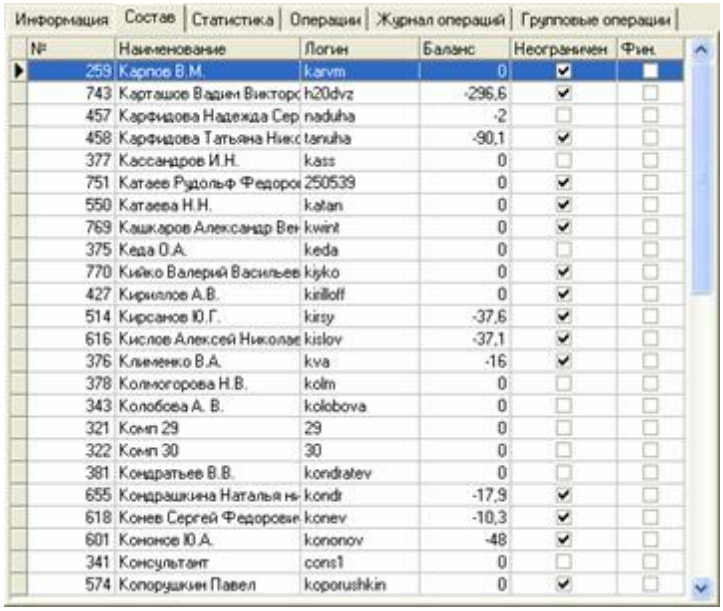
Ideco ACP поддерживает работу с финансовыми и нефинансовыми операциями. Эти возможности включают: формирование самих операций (приход, расход и т. п.), печать документов, формирование шаблонов для печати, автоматическое формирование актов.

Эти возможности, как правило, используются в крупных организациях, или в случае оказания услуг по доступу в Интернет другим организациям.

Подробнее смотрите разделы:

- Операции 250
- Закладка "Операции" 250
- Закладка "Журнал операций" 254
- Закладка "Групповые операции" 254
- Реквизиты пользователя и группы 248
- Автоматическое формирование акта 247
- Шаблоны документов 245

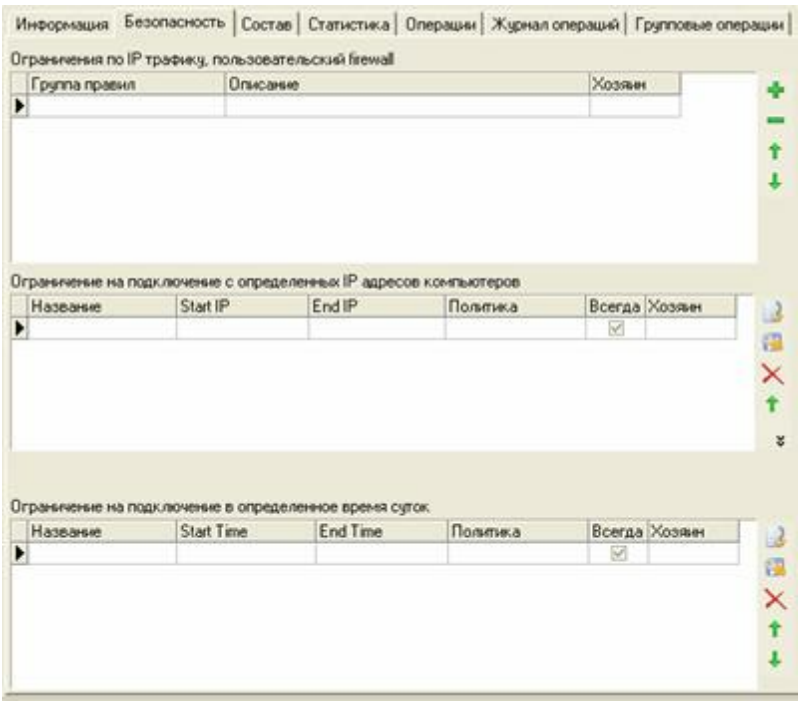
5.2.5.8 Закладка "Состав" (у группы)



№	Наименование	Логин	Баланс	Неограничен	Фин.
259	Карпов В.М.	karvm	0	☑	☐
743	Карташов Вадим Виктор	h20dvz	-296,6	☑	☐
457	Карфидова Надежда Сер	naduha	-2	☐	☐
458	Карфидова Татьяна Нико	tanuha	-90,1	☑	☐
377	Кассандров И.Н.	kass	0	☐	☐
751	Катаев Рудольф Федоро	250539	0	☑	☐
550	Катаева Н.Н.	katan	0	☑	☐
769	Кашкаров Александр Ве	kwint	0	☑	☐
375	Кеда О.А.	keda	0	☐	☐
770	Кийко Валерий Васильев	kiyko	0	☑	☐
427	Кириллов А.В.	kirilloff	0	☑	☐
514	Кирсанов Ю.Г.	kirsy	-37,6	☑	☐
616	Кислов Алексей Николае	kislov	-37,1	☑	☐
376	Клименко В.А.	kva	-16	☑	☐
378	Колмогорова Н.В.	kolm	0	☐	☐
343	Колобова А. В.	kolobova	0	☐	☐
321	Комп 29	29	0	☐	☐
322	Комп 30	30	0	☐	☐
381	Кондратьев В.В.	kondratev	0	☐	☐
655	Кондрашкина Наталья Н	kondr	-17,9	☑	☐
618	Конев Сергей Федорови	konev	-10,3	☑	☐
601	Кононов Ю.А.	kononov	-48	☑	☐
341	Консультант	cons1	0	☐	☐
574	Копорушкин Павел	koporushkin	0	☑	☐

На закладке **Состав** показываются все пользователи и группы находящиеся в корне группы выбранной группы. По каждому пользователю и группе выводится **Логин**, **Наименование**, **текущий Баланс**, значение признаков **Неограничен** (установлено ли свойство **Порог отключения**) и **Финансовый**.

5.2.5.9 Закладка Безопасность



На закладке **Безопасность** можно задать список правил доступа, ограничивающих подключение выбранного пользователя или пользователей выбранной группы по времени или по IP-адресу компьютера с которого производится подключение. Правила являются наследуемыми и проверяются последовательно.

5.2.5.10 Баланс пользователя и группы, порог отключения

Каждый пользователь и группа имеет лицевой счет, содержащий его баланс.

Баланс = **Остаток** + **Оплата** – **Расход**, где

Остаток – остаток на начало текущего периода

Оплата – поступление в течении текущего периода

Расход – расход трафика в денежном эквиваленте за текущий период.

В соответствии с назначенным тарифным планом происходит тарификация и **Расход** увеличивается, соответственно происходит изменение текущего баланса (текущий баланс уменьшается). Изменение баланса происходит почти в реальном времени.

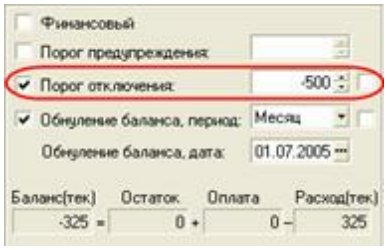
При тарификации пользователя и увеличении его **Расхода**, увеличивается **Расход** и всех вышестоящих групп.

Расход группы за период равен расходу всех вложенных пользователей за этот

период.

Расход корневой группы равен сумме расходов всех финансовых групп и финансовых пользователей и составляет полный расход за прошедший через сервер трафик за период.

Такой принцип распространения **Расхода** вверх по дереву позволяет устанавливать ограничения не только на отдельных пользователей, но и на группы.



Если у пользователя установлен **Порог отключения**, то при достижении балансом указанной величины происходит автоматическое отключение от платных сетей.

Если же баланс группы превышает порог отключения, то отключаются от платных сетей все пользователи этой группы.

Списание и начисление средств может происходить как автоматически с использованием механизмов тарификации, так и вручную администратором.

Баланс нефинансовых пользователей на начало периода (например, месяца) равен нулю. В течение периода расход увеличивается, а баланс уменьшается. Когда баланс будет меньше порога отключения (например, -500), система отключит пользователя от платных сетей.

В конце отчетного периода автоматически или вручную производится обнуление баланса для нефинансовых групп и пользователей. И новый период опять начинается с нулевого баланса.

Для финансовых пользователей в конце периода производится формирование акта (списание кредита в "остаток на начало периода"), при этой операции **Расход** обнуляется, а **Остаток** увеличивается, при этом **общий баланс не изменяется**. С начала нового периода расход вновь начинает увеличиваться с нуля.

В конце месяца для финансовых пользователей рекомендуется проводить подведение баланса (списание дебета в "остаток на начало периода").

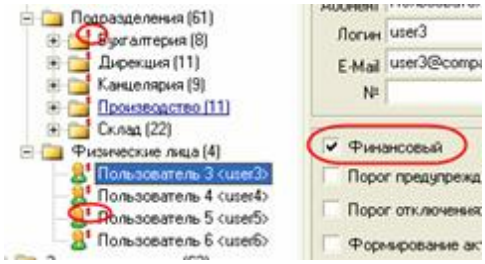
Для удобства администрирования есть признак "Обнуление баланса" который позволяет автоматически проводить списание баланса в ноль при наступлении нового периода.

У финансовой группы вместо "**Обнуление баланса**" есть признак " **Автоматическое создание акта**".

5.2.5.11 Признак "Финансовый"

Пользователь и группа имеют признак финансовый, означающий финансовую ответственность за использование Интернет. Такие группы и пользователи сами

планируют и оплачивают расходы за Интернет. Если признак установлен, то такие пользователи и группы называются **финансовыми**.



По таким группам и пользователям ведется строгий учет по лицевому счету. Суммарный объем показателей по финансовым группам и пользователям равняется показателям корневой группы.

За нефинансовых пользователей и групп несет ответственность родительская финансовая группа

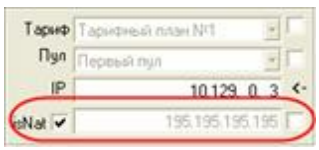
В одной ветке дерева от пользователя до корневой группы обязательно должна быть одна финансовая группа или он сам должен быть финансовым. Если пользователь нефинансовый и выше него нет финансовой группы, то он не сможет получить доступ в Интернет.

Рекомендации:

1. В небольших предприятиях рекомендуется использовать одну финансовую группу – корневую "**Все пользователи**". Или создать в корневой группе группу с именем вашей организации и установить признак у этой группы признак **Финансовый.**
2. В больших предприятиях можно создавать финансовые группы для крупных подразделений.
3. В случае, если предприятие оказывает услуги по доступу в Интернет сторонним организациям или физическим лицам, то для таких организаций нужно создавать финансовые группы, а для физических лиц финансовых пользователей.

5.2.5.12 Использование NAT

Технология NAT (Network Address Translation) защищает компьютеры пользователей от атак из сети Интернет. NAT скрывает компьютеры пользователей от доступа из внешней Интернет сети.



Рекомендуется для всех пользователей использовать признак isNat, так как практически всем пользователям реальный IP-адрес не нужен.

Использование NAT обладает следующими преимуществами:

1. Основной плюс -- это защита компьютеров пользователей, так как в

Интернет они выходят под другим IP-адресом. И злоумышленник не имеет возможности установить соединение к пользователю из Интернет.

2. Все пользователи могут выходить в Интернет под одним внешним IP-адресом, то есть снимается проблема нехватки реальных IP-адресов.
3. Использование NAT позволяет открывать доступ сразу большому количеству пользователей (например, всем сотрудникам предприятия) к внешним ресурсам, если на этих ресурсах заложена проверка по IP-адресу.
4. Для разных групп пользователей можно использовать разные адреса NAT. Так, например, если оказывается услуга доступа в Интернет сторонней организации и у нее есть реальный IP-адрес, то рекомендуется для всех пользователей этой организации установить в качестве адреса NAT этот IP-адрес. Для этого достаточно указать его в свойствах группы.

Замечание: Если IP-адрес NAT нигде не указан: ни в тарифном плане, ни в свойствах корневой группы, то в качестве NAT будет использоваться IP-адрес основного внешнего интерфейса Ideco ACP.

5.2.5.13 Автоматическое обнуление баланса

Функция "**Автоматическое обнуление баланса**" позволяет простым способом вводить ограничения на расход пользователя или группы за определенный период. При этом с определенной периодичностью происходит автоматическое обнуление баланса пользователя и группы. Эта функция доступна только для нефинансовых пользователей.

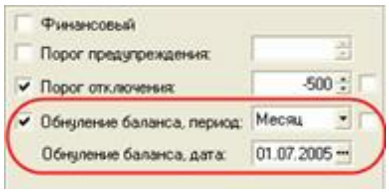
5.2.5.13.1 Принцип работы

У пользователя или группы устанавливается **Порог ограничения** с минусовым значением. В начале периода баланс пользователя равен нулю. Таким образом, за период пользователь может израсходовать не более того, что указано в пороге ограничения. А в конце периода автоматически происходит обнуление баланса: баланс пользователя становится равным нулю. И пользователь снова сможет расходовать "деньги" до достижения порога отключения.

5.2.5.13.2 Установка автоматического обнуления

Для работы автоматического обнуления баланса нужно в свойствах пользователя или группы установить порог отключения, а также период и дату обнуления баланса. Для этого:

1. Выберите нужного пользователя или группу в дереве пользователей.
2. Перейдите на закладку Информация.
3. Задайте необходимые параметры. Например, как показано ниже:



Порог отключения – установите значение, которым хотите ограничить расход пользователя. Нужно указывать со знаком минус.

Обнуление баланса, период – установите период обнуления баланса. Возможны следующие значения: день, неделя, 10 дней, 15 дней, месяц или квартал.

Обнуление баланса, дата – укажите дату начала действия обнуления, то есть дату следующего обнуления. Когда обнуление сработает, дата автоматически изменится на следующую дату обнуления.

4. Сохраните изменения  .

5.2.5.13.3 Варианты использования автоматического обнуления

1. **Ограничение расходов пользователя**

   Пользователю необходимо ввести ограничение в размере 100 условных единиц в месяц. Тогда нужно установить **Порог ограничения** в размере "-100", и установить период обнуления **Месяц**. Тогда каждый месяц баланс пользователя будет автоматически обнулятся: обнулятся поля **Оплата**, **Остаток** и **Расход**. Таким образом, если пользователь израсходует с начала месяца 100 условных единиц, то ему автоматически заблокируется доступ в платные сети. То есть пользователь не сможет израсходовать больше 100 условных единиц в месяц.

2. **Ограничение расходов группы**

   Одно из подразделений предприятия не должно расходовать более 1000 условных единиц в месяц. Тогда нужно установить **Порог ограничения** в размере -1000, и установить период обнуления **Месяц**. Тогда каждый месяц баланс группы будет автоматически подводиться до нуля. И в течении месяца пользователи этого подразделения суммарно не смогут израсходовать больше 1000 условных единиц.

3. **Предотвращение несанкционированного расхода трафика**

   При поражении вирусами, взломе компьютеров пользователей или внутренних серверов предприятия, трафик может скачкообразно вырасти. При этом факт значительного расхода трафика, а, следовательно, и факт появления ненормальной ситуации, может быть не замечен или замечен значительно позже. Использование автоматического обнуления позволяет избежать этой ситуации.

- Например, один из серверов предприятия с выходов в Интернет, в среднем расходует не более 100 условных единиц в день. Для гарантированного предотвращения ситуации, при которой этот сервер сможет сгенерировать очень большое количество трафика, установите порог ограничения в размере 200, а период обнуления один день.
- Также можно установить обнуление баланса на всю организацию с заведомо большим порогом отключения, и периодом обнуления в один день. Таким образом, в нормальном режиме работы это никак не повлияет на пользователей. А в случае нештатной ситуации позволит избежать большого расхода трафика и вовремя обнаружить проблему.

4. **Для получения статистических данных. Группы "Счетчики"**

   Увеличение расхода автоматически распространяется вверх по дереву до корневой группы. То есть если при увеличении поля расход у пользователя, оно на эту же величину увеличивается для всех вышележащих групп. Это позволяет создавать группы "Счетчики" используемые для подсчета расхода за различные периоды: например за день, неделю месяц и т.п. В этом случае можно не устанавливать **порог отключения**.

5.2.5.14 Удаление пользователей

Для того, что бы удалить пользователя:

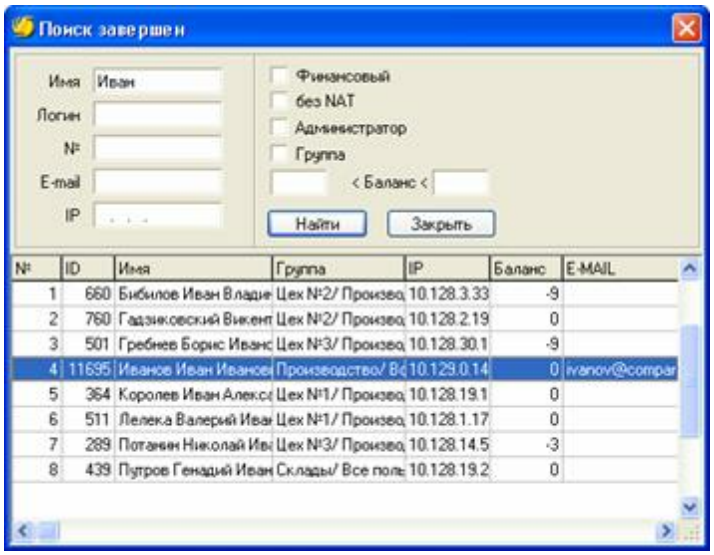
1. Выберите нужного пользователя в дереве и нажмите кнопку  **Удалить** пользователя, или щелкните правой кнопкой мышке на пользователе, которого хотите удалить, и выберите пункт **Удалить**.
2. Появится окно с предупреждением. Нажмите кнопку **ОК**.
3. Пользователь будет перемещен в папку **Корзина** и не сможет подключиться к серверу.

Замечания:

4. Удаление группы пользователей аналогично удалению пользователей. При этом вся группа перемещается в **Корзину**.
5. При проведении операции "Закрытие периода" производится окончательное удаление пользователей и их статистики из БД.
6. Параметры удаленного пользователя сменить нельзя.
7. Для восстановления пользователя или группы, выберите нужного пользователя или группу в **Корзине** и нажмите кнопку  **Восстановить**.
8. В Ideco ACP нельзя создать пользователей с повторяющимися логинами и IP-адресами. При необходимости использовать логин или IP-адрес, которые заняты удаленным пользователем, нужно сменить эти параметры у удаленного пользователя. Для этого его потребуется сначала восстановить, сменить логин или IP-адрес и снова удалить.
9. Удаление пользователя не влияет на значение баланса вышележащих групп.

5.2.5.15 Поиск пользователей

Для поиска пользователей перейдите в раздел **Пользователи**. Для этого нажмите кнопку **Пользователи** на панели быстрого запуска. Затем нажмите кнопку **Поиск** на панели инструментов или выберите пункт главного меню: **Действия** > **Поиск пользователей**.



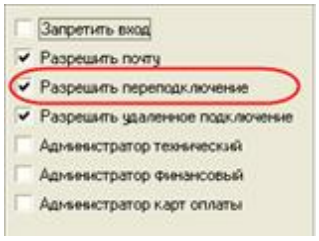
Задайте нужные параметры поиска и нажмите кнопку **Найти**.

Будет выведен список пользователей удовлетворяющих условиям поиска.

Для перехода к нужному пользователю в дереве пользователей выполните двойной щелчок мышкой на нужном пользователи. При этом окно поиска закроется.

Можно не закрывая окно поиска просматривать информацию по пользователям. Для этого можно перемещаться по результатом поиска и информация на закладках **Информация**, **Операции**, **Статистика** будут отображаться для текущего пользователя.

5.2.5.16 Переподключение



Свойство пользователя **Разрешить переподключение** означает возможность пользователя установить соединения с сервером Ideco ACP, если его соединение

уже установлено с другого компьютера. При этом старое соединение разрывается.

И наоборот, если **Разрешить переподключение** не установлено, то если соединение уже установлено, то пользователь не сможет его установить с другого компьютера.

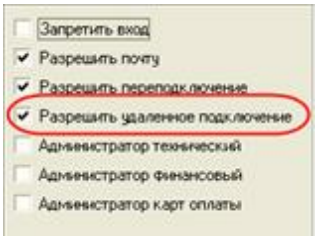
Рекомендуется использовать для пользователей, которые могут подключаться к Ideco ACP с разных компьютеров.

Замечания:

Свойство **Разрешить переподключение** устанавливается отдельно для каждого пользователя. Подробнее см. пункт Параметры разрешений[193] в разделе Закладка "Информация" (у пользователя)[189].

На возможность администратора группы устанавливать своим пользователям это разрешение влияют соответствующие установки в свойствах группы. Подробнее см. пункт Параметры разрешений[198] в разделе Закладка "Информация" (у группы)[194].

5.2.5.17 Удаленное подключение



Свойство пользователя **Разрешить VPN из Интернет** означает возможность пользователя подключиться к внешнему адресу Ideco ACP, например из дома или командировки. По умолчанию все пользователи подключаются ко внутреннему адресу.

Возможность пользователя подключиться к внешнему адресу позволяет подключаться к внутренней сети предприятия через защищенное соединение. Для дополнительной защиты сети предприятия разрешать удаленное подключение нужно только пользователям, которым это действительно необходимо.

Замечания:

Свойство **Разрешить удаленное подключение** устанавливается отдельно для каждого пользователя. Подробнее см. пункт Параметры разрешений[193] в разделе Закладка "Информация" (у пользователя)[189].

На возможность администратора группы устанавливать своим пользователям это разрешение влияют соответствующие установки в свойствах группы. Подробнее см. пункт Параметры разрешений[198] в разделе Закладка "Информация" (у группы)[194].

В Ideco ACP есть глобальный параметр "**Разрешить удаленные подключения**", устанавливаемый в локальной консоли сервера. В случае, если он не установлен, то ко внешнему адресу нельзя подключиться по VPN. По умолчанию этот параметр не установлен. Поэтому при использовании этой возможности, нужно включить эту настройку.
Подробнее см. пункт Безопасность[145] в разделе Конфигурирование сервера[131].

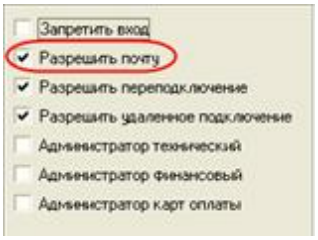
5.2.5.17.1 Особенности работы

Для использования удаленного подключения, нужно обратить внимание на следующие особенности, и по возможности информировать о них пользователей.

1. При удаленном подключении используется внешний (реальный) IP-адрес Ideco ACP. В то время как для обычного подключения из сети предприятия, как правило, используется внутренний IP-адрес Ideco ACP. Поэтому пользователям нужно сообщить внешний IP-адрес, а также уточнить, что уже настроенное соединение для работы из сети предприятия, например, на ноутбуке, не будет работать извне. Файл автоматической настройки соединения, находящийся в Личном Кабинете, также настраивает соединение для работы только с внутренним IP-адресом.
2. ACP пользователя содержит инструкции по настройке VPN-соединения. При этом ACP пользователя по умолчанию закрыт от доступа извне. Поэтому если пользователю придется настраивать VPN-соединение вручную, то у него могут возникнуть затруднения. В этом случае, ему следует помочь настроить соединение или заранее скачать инструкцию по настройке VPN-соединения в виде файла с ACPа.
3. При удаленном подключении, трафик, который пользователь генерирует на сервер, считается не для этого пользователя, а для системного пользователя "Внешний интерфейс сервера". Для таких внешних пользователей, можно создать специальный тарифный план и установить стоимость исходящего трафика равную стоимости входящего трафика для пользователя "Внешний интерфейс сервера".

5.2.5.18 Использование почты

При установке флажка **Разрешить почту**, для пользователя создается почтовый ящик.



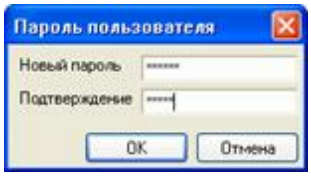
Важно: Для использования почты необходимо в локальном интерфейсе установить параметр **Разрешить почту** и указать ваш почтовый домен.

5.2.5.19 Смена пароля

Пользователи могут самостоятельно изменять свои пароли в Личном кабинете. Если он забыл свой пароль то восстановить его нельзя, в этом случае сменить его может только администратор.

Для того что бы сменить пароль пользователя:

4. Выберите пользователя.
5. Нажмите кнопку  **Пароль** на панели инструментов, или Щелкните правой кнопкой мышки на пользователи и выберите пункт **Пароль**.
6. Появится следующее окно:



7. Введите пароль и подтверждение.

5.2.5.20 Проверка пользователя

Возможность пользователя авторизоваться и подключиться к серверу, а также его возможность работы в Интернет (доступ к платным сетям) зависит от большого количества параметров: как его собственных свойств, так и настроек вышележащих групп.

Для того чтобы проверить правильность установки всех свойств или определить, почему пользователь не может подключиться или выйти в Интернет, есть функция "**Проверка возможности подключения и работы в Интернет"**, которая позволяет быстро определить причину, и избавляет от проверки всех свойств вручную.

Для того чтобы проверить пользователя:

8. Выберите пользователя и нажмите кнопку  **Проверить возможность**

подключения и работы в Интернет на панели инструментов, или

Щелкните правой кнопкой мышки на пользователи и выберите пункт **Проверить**.

9. После чего появится сообщение, с указанием причины.

Возможные сообщения:

- "Пользователь отключен"
- "Отключен один из родителей"
- "В ветке нет финансово-ответственного"
- "Параметры указаны верно, превышен лимит"
- "Все параметры пользователя указаны верно"
- "Пользователь не существует"
- "Пользователь удален"
- "Структура пользователей нарушена"
- "Нет тарифного плана"
- "Тарифный план отключен"
- "Пул IP-адресов отключен"

5.2.5.21 Оповещение пользователей

Ideco ACP содержит возможность отправки сообщений пользователям. Отправка сообщений может быть автоматической при наступлении определенного события, а также выполняться администраторами.

В случае если баланс достигает порога предупреждения, пользователю или группе автоматически высылается сообщение.

В случае возникновения неполадок в работе Ideco ACP, например, в случае переполнения жесткого диска, высылается сообщение **Главному администратору**.

5.2.5.21.1 Способ доставки

Сообщения пользователям могут доставляться по e-mail, по winpopup, по Ideco Agent, а также пользователь может их посмотреть в личном кабинете.

Для того чтобы задать способ доставки сообщений или отключить доставку сообщений:

1. Выберите пункт меню **Сервис** > **Настройки**.
2. В появившемся окне выберите значение параметра **Оповещение пользователей**. Возможны три варианта:

- Отключено
- По e-mail
- По e-mail и winpopup

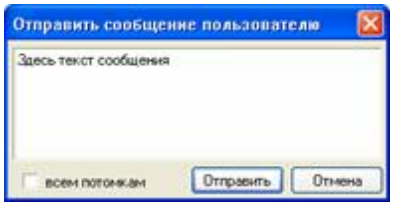
3. Нажмите кнопку **OK**.

Замечание: Сообщения в личный кабинет пользователя доставляются всегда, вне зависимости от вышеуказанных установок.

5.2.5.21.2 Отправка сообщений

Для того, что бы отправить сообщение:

1. Выберите в дереве пользователя или группу.
2. На панели инструментов или в контекстом меню нажмите кнопку  **Отправить сообщение**.
3. Появится следующее окно:



Введите текст сообщения.

Если вы отправляете сообщение группе, то если установить флажок  **всем потомкам**, то сообщение будет отправлено также и всем вложенным пользователям и подгруппам текущей группы.

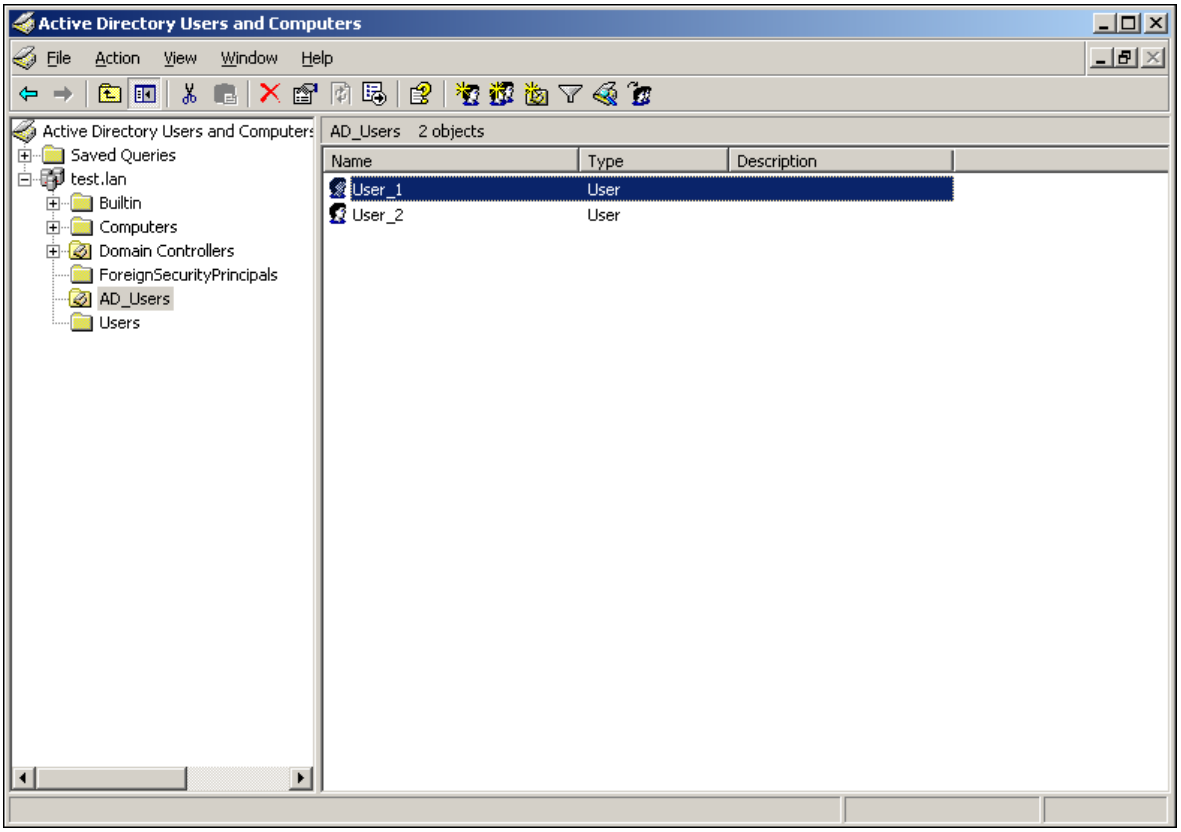
4. Нажмите кнопку "**Отправить**".

5.2.6 Настройка синхронизации Ideco ICS с Active Directory или LDAP сервером

Настройка синхронизации Ideco ICS с Active Directory или LDAP сервером

Важно. Данный функционал рекомендуется только для ВУЗ-ов, гостиниц и тому подобное, но не для провайдеров.

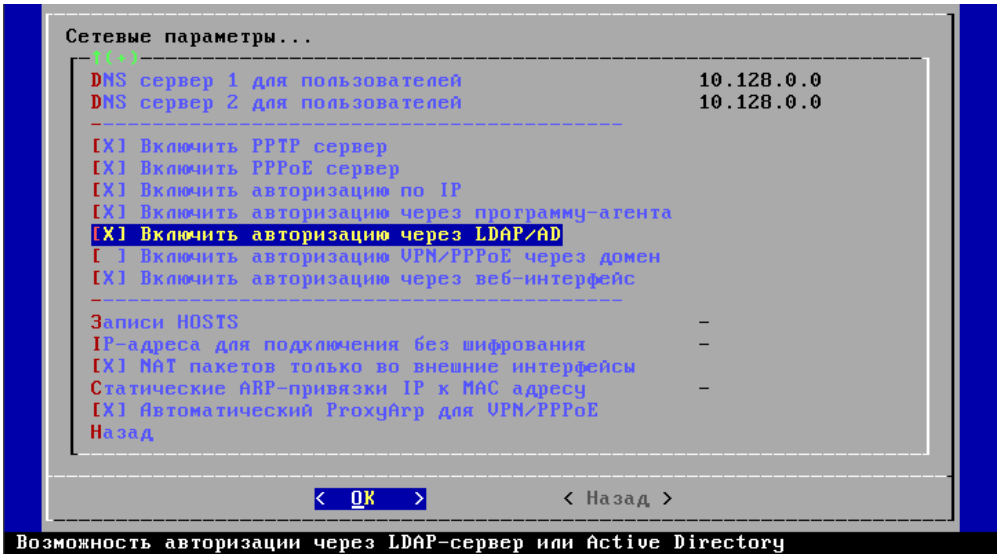
Эта операция выполняется для того, чтобы импортировать сущестующую базу пользователей с контроллера домена, пароли при этом будут храниться на сервере AD, а при авторизации Ideco будет их оттуда запрашивать. В качестве примера рассмотрим контроллер домена, имеющий следующую структуру дерева пользователей:



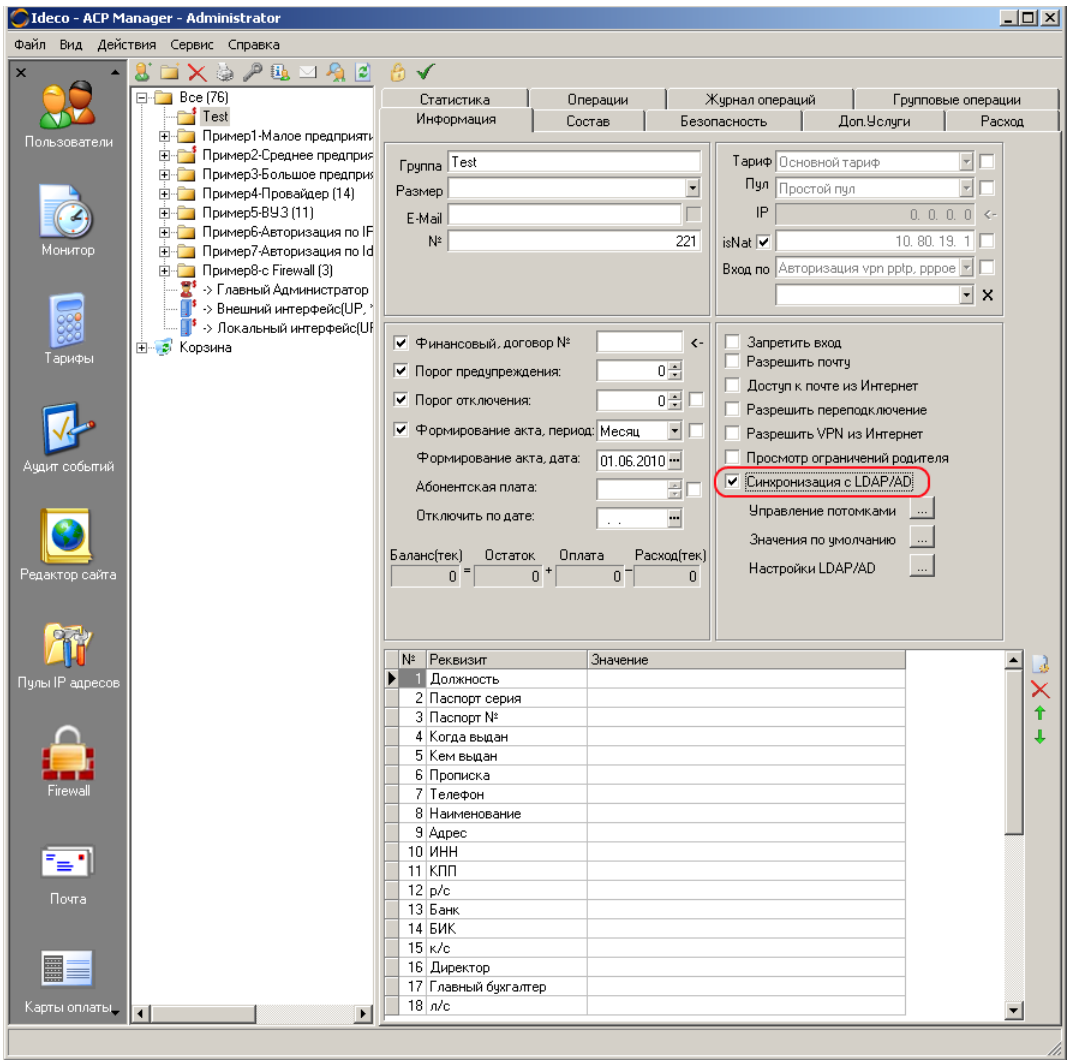
Для того чтобы осуществить авторизацию пользователей через LDAP сервер либо службу Active Directory необходимо произвести следующие операции:

1. В локальной консоли в разделе "Конфигурирование сервера" - "Конфигурирование сети" установить флажок "[X] Включить авторизацию через LDAP/AD".

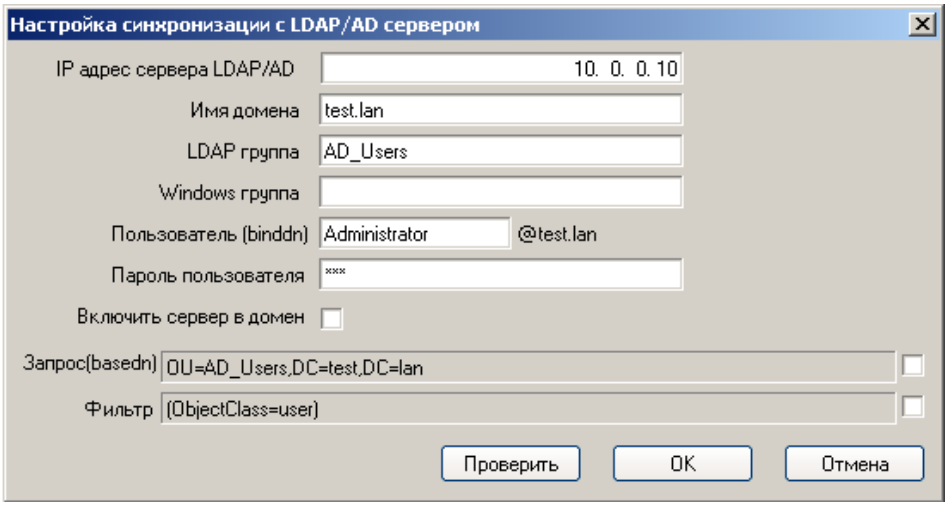
"[X] Включить авторизацию VPN/PPPoE через домен" ставиться только в том случае, когда для пользователей, импортированных из AD, планируется авторизация по VPN.



2. Произвести мягкую перезагрузку.
3. Подключиться к веб-интерфейсу.
4. Создать новую группу пользователей. В параметрах группы установить флажок "Синхронизация с LDAP/AD".



5. Нажать на кнопку "Настройки LDAP/AD ..."



Установить параметры:

- "IP адрес сервера LDAP/AD" – указать IP адрес контроллера домена
- "Доменное имя" – указать DNS имя домена. Контроллер домена обычно имеет имя "имя.имя домена". Необходимо указать имя домена без имени контроллера.
- "LDAP группа" – указать название папки в LDAP дереве. Для Windows, обычно "Users"
- "Windows группа" – указать название Группы пользователей Windows, пользователи которой должны выходить в Интернет с помощью Ideco ICS. Если такая группа не создана, то оставить это поле пустым. В этом случае будут синхронизироваться все пользователи из папки "LDAP группа"(в нашем примере Windows группа не используется).
- "Пользователь" и "пароль пользователя" – указать логин и пароль для подключения к LDAP серверу. От имени этого пользователя должна быть доступна на чтение "LDAP группа"
- "Включить сервер в домен" - галочка нужна только в том случае если будет использоваться авторизация по VPN.
- Нажать на кнопку "Проверить". Будет произведено тестовое подключение к серверу и проверка пароля.
- Нажать OK.

6. Выбрать в дереве пользователей созданную папку и выбрать меню "Действия" - "Обновить". В папке должны появиться пользователи, загруженные из LDAP. Если число пользователей очень большое, то обновление может занять некоторое время. Если пользователей больше 1000, то необходимо разделить их на отдельные группы.

7. Настроить параметры пользователей, если это требуется.

Более подробно процесс синхронизации с AD показан на одном из наших семинаров:

Специальный проигрыватель - http://www.ideco-software.ru/download/seminars/NV_NetPlayer.exe

Файл записи – http://www.ideco-software.ru/download/seminars/2009_06_23.zip

*** Примечание**: "Windows группа" при синхронизации используется только тогда, когда необходимо из LDAP группы (на языке AD - Контейнер или Organizational Units) импортировать только часть пользователей, обьединённых в группу.

5.2.7 Рекомендации и замечания по работе с Ideco ICS Manager

В этом разделе содержатся рекомендации и замечания по работе Ideco ACP Manager, которые не вошли в другие разделы.

5.2.7.1 Интерфейс Ideco ICS Manager

1. **Для ввода IP-адресов можно использовать копирование-вставку**.

   Поля для ввода IP-адресов используются в интерфейсе Ideco ACP Manager в большом количестве, и, в отличие от стандартных полей ввода IP-адресов в Windows, поддерживают копирование и вставку.

2. **Для обновления информации используйте клавишу F5 или кнопку "Обновить"**.

   Информация, отображаемая в Ideco ACP Manager, берется из БД. При этом информация может изменяться другими администраторами, а некоторые параметры (такие как баланс пользователя, статистика, состояние пользователей) изменяются непрерывно. При переходе между разделами, пользователями или группами информация обновляется автоматически. Для принудительного обновления дерева пользователей или информации в других разделах используйте клавишу **F5** или кнопку  Обновить.

3. **Все таблицы Ideco ACP Manager поддерживают сортировку**.

   Для сортировки нажмите по заголовку колонки, по которой нужно отсортировать. Для сортировки в обратном порядке нажмите еще раз.

4. **Все таблицы поддерживают поиск по полям**.

   Для этого установите курсов в таблицу на нужное поле и нажмите **Ctrl + F**.

5. **Все таблицы поддерживают копирование**

   Для этого нажмите <**Ctrl + A> и <Ctrl + C>**.

6. **Дерево пользователей поддерживает операции перемещения и множественного выделения**.

   Работает аналогично проводнику Windows.

5.2.7.2 Безопасность логинов и паролей

Логин и пароль пользователя используется для авторизации и установки соединения, поэтому его нужно оберегать и аккуратно использовать. К администраторам это относится в большей степени, так как их пароли используются для работы с Ideco ACP. Например, при установке соединения с чужих компьютеров, особенно с установленной опцией сохранения паролей в Windows 98, пароль может быть получен злоумышленником имеющему доступ к этому компьютеру.

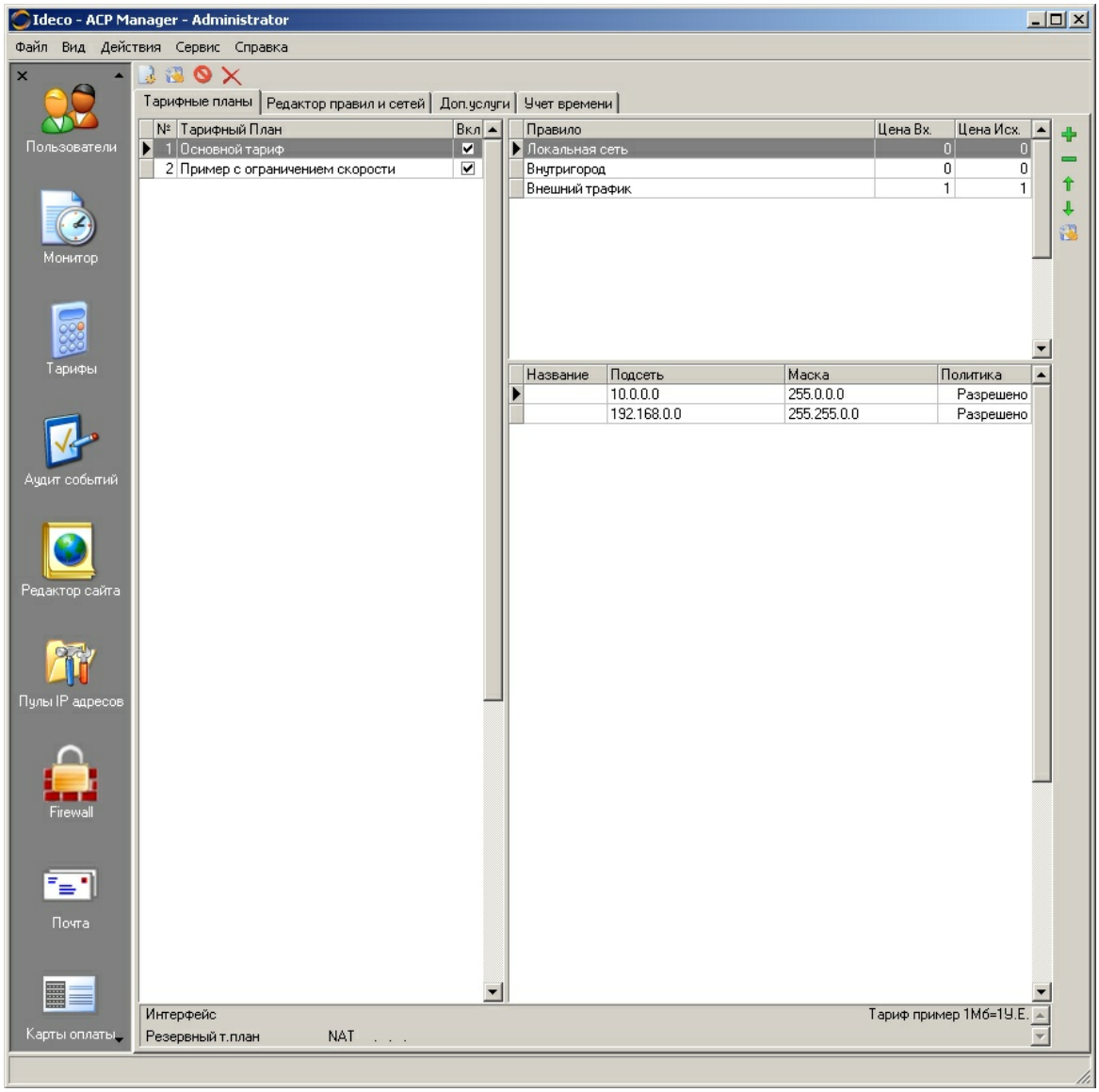
При подключении с чужих компьютеров следует иметь в виду, что на них может быть установлен клавиатурный шпион (Keylogger) и набранные пароли могут быть перехвачены злоумышленником.

В таких ситуациях использовать логин администраторов настоятельно не рекомендуется. Если администраторам необходимо работать в Интернет с различных компьютеров, или проверять установку соединения у многих пользователей, то рекомендуется создать для этих целей дополнительный логин простого пользователя.

5.2.8 Тарифные планы

В соответствии с тарифными планами происходит учет трафика пользователей в денежном эквиваленте.

Тарифный план определяет стоимость трафика в зависимости от подсети, а также от направления трафика (входящий или исходящий). В Ideco ACP тарифный план состоит из списка правил с указанием стоимости входящего и исходящего трафика для этого правила. Понятие **Правило** введено для удобства управления, **Правило** – это список сетей с указанием политики (разрешено или запрещено). Одно и тоже правило может входить в несколько тарифных планов. В одно правило, обычно, объединяются сети, стоимость трафика по которым одинакова. Например, правило "Внутригород" должно содержать список сетей с одной стоимостью, а правило "Локальная сеть" – список сетей предприятия, по которым не должна вестись тарификация (нулевая стоимость).



Таким образом, при создании тарифных планов нужно сначала создать правила, а потом создавать тарифные планы, включая в них правила, и указывая стоимость трафика для этих правил.

Замечания:

1. Каждый пользователь обязательно работает в соответствии с одним тарифным планом. Если тарифный план у пользователя не определен или тарифный план, определенный у пользователя отключен, то пользователь не сможет подключиться.
2. Редактировать тарифные планы может только **Главный администратор**. Администраторы групп могут только просматривать тарифные планы используемые для пользователей их групп.
3. Сменить тарифный план у пользователя может **Главный администратор**, а также администраторы корневой группы.
4. При редактировании тарифного плана, все соединения от пользователей

подключенных на этот тарифный план разрываются.

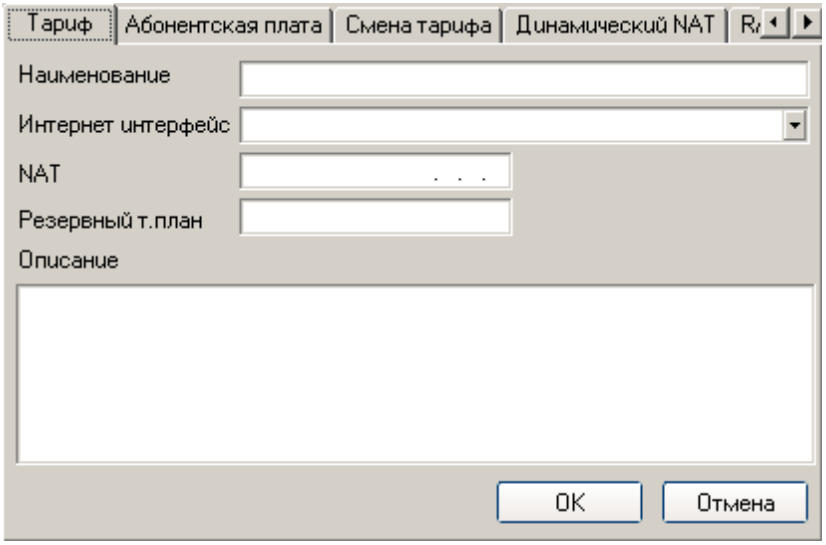
5. В небольших организациях, как правило, используется один тарифный план. Использовать несколько тарифных планов целесообразно только в том случае, если для разных пользователей необходимо тарифицировать трафик по разным ценам. А также если используется возможность закрытия части ресурсов предприятия с использованием тарифных планов (подробнее см. Создание закрытых ресурсов 228).

Для доступа к тарифным планам перейдите в раздел **Тарифные планы**: кнопка **Тарифы** на панели разделов.

5.2.8.1 Создание тарифного плана

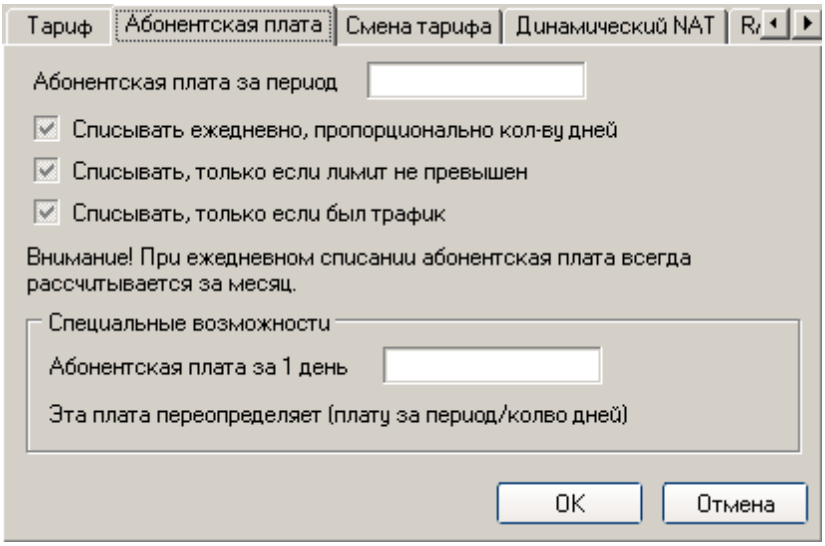
Для того чтобы создать новый тарифный план:

1. Перейдите в раздел **Тарифные планы**.
2. На панели инструментов нажмите кнопку  **Создать тарифный план**.

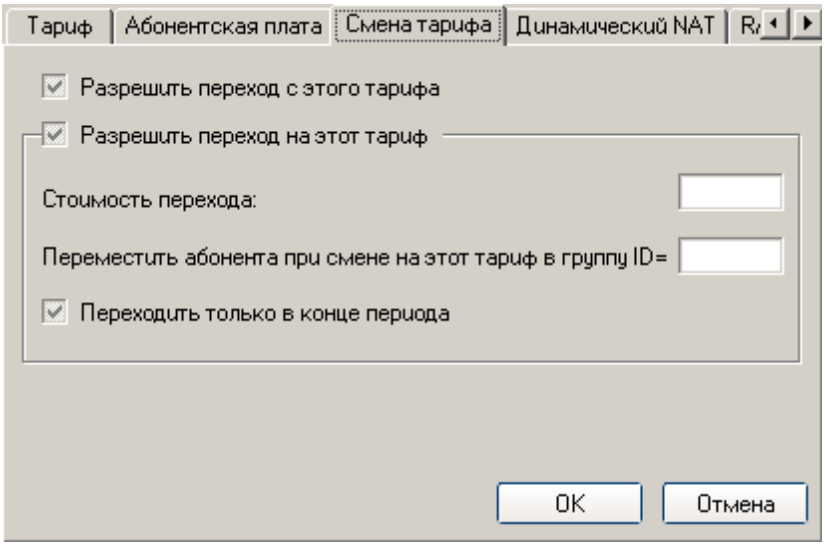


В появившемся диалоговом окне укажите Название тарифного плана и вспомогательное описание, выберите сетевой интерфейс, который будет использоваться по умолчанию у пользователей подключенных на этот тарифный план. В небольших организациях, с одним тарифным планом можно не указывать интерфейс по умолчанию, так как в качестве него будет подставлен основной внешний интерфейс.

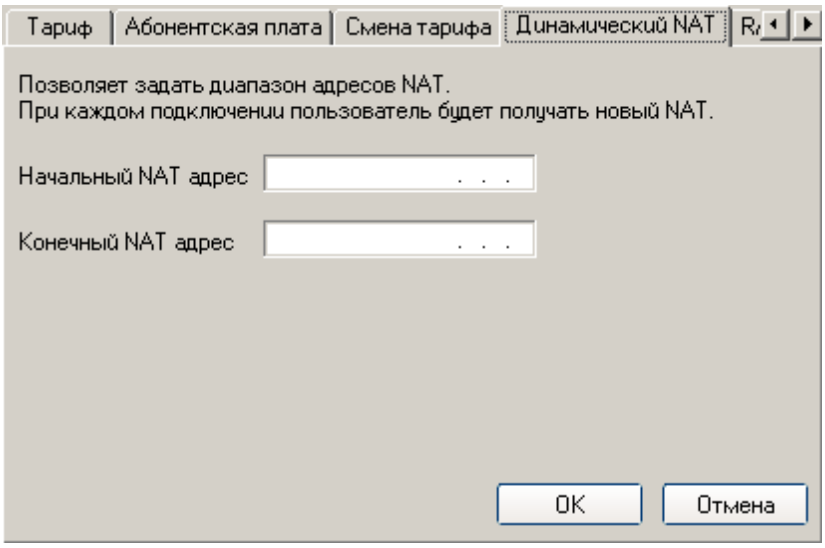
3. При необходимости установите абонентскую плату и метод ее списания со счета



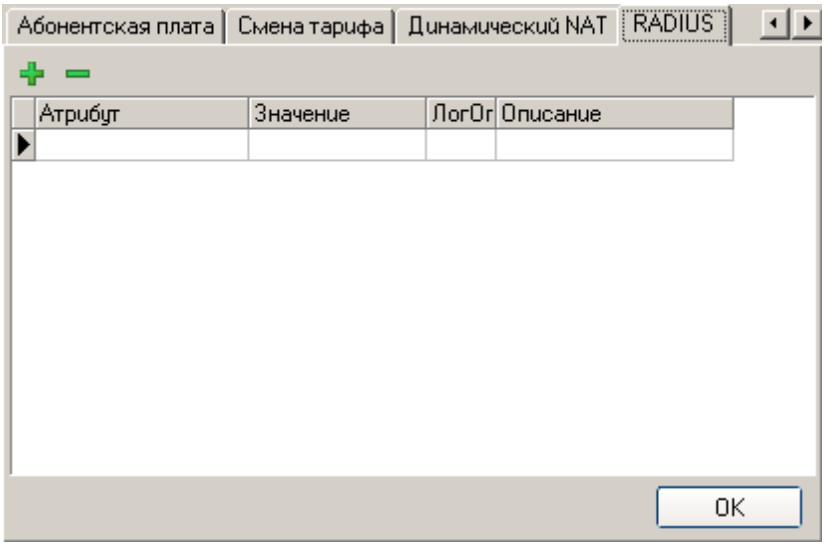
4. Смена тарифа



5. При необходимости установите диапазон адресов NAT, которые будут выдаваться пользователям.



6. Нажмите кнопку **ОК**.
7. При использовании схем подключения абонентов через NAS или роутеры, принимающие параметры по RADIUS, можно настроить передачу этих параметров в тарифе во вкладке RADIUS. Параметры будут передаваться каждый раз при авторизации пользователя по этому тарифу. Синтаксис написания правил зависит от используемого вами оборудования и должен быть описан в инструкции к нему.



8. Теперь нужно добавить в тарифный план правила и указать стоимость.

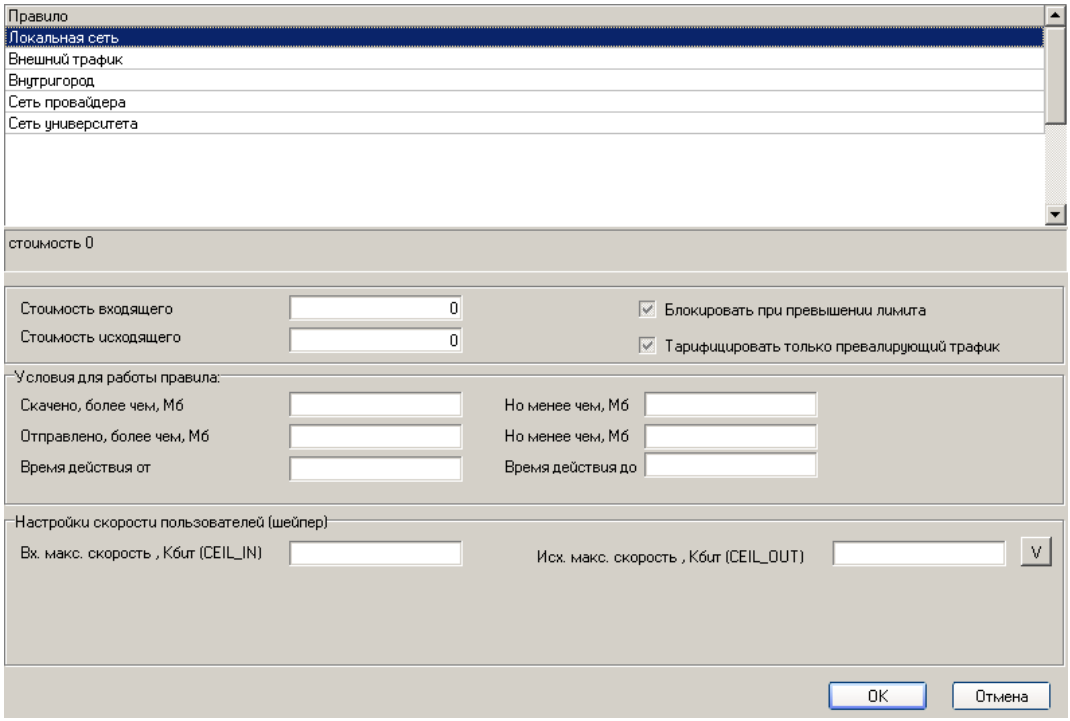
Добавление правил в тарифный план

В списке тарифных планов выберите созданный тарифный план. В таблице справа появится пустой список правил этого тарифного плана.

Справа от таблицы нажмите кнопку  **Добавить правило** в тарифный план.

Появится диалоговое окно выбора правила. Показываются все имеющиеся Правила, за исключением уже имеющихся в этом тарифном плане.

Выберите нужное правило, укажите стоимость входящего и исходящего трафика в условных единицах для этого правила и нажмите кнопку **OK**.



Далее также добавьте все нужные правила.

Замечание: Если нужного вам правила нет в списке правил, то его нужно сначала добавить. Подробнее см. Редактор правил и сетей.

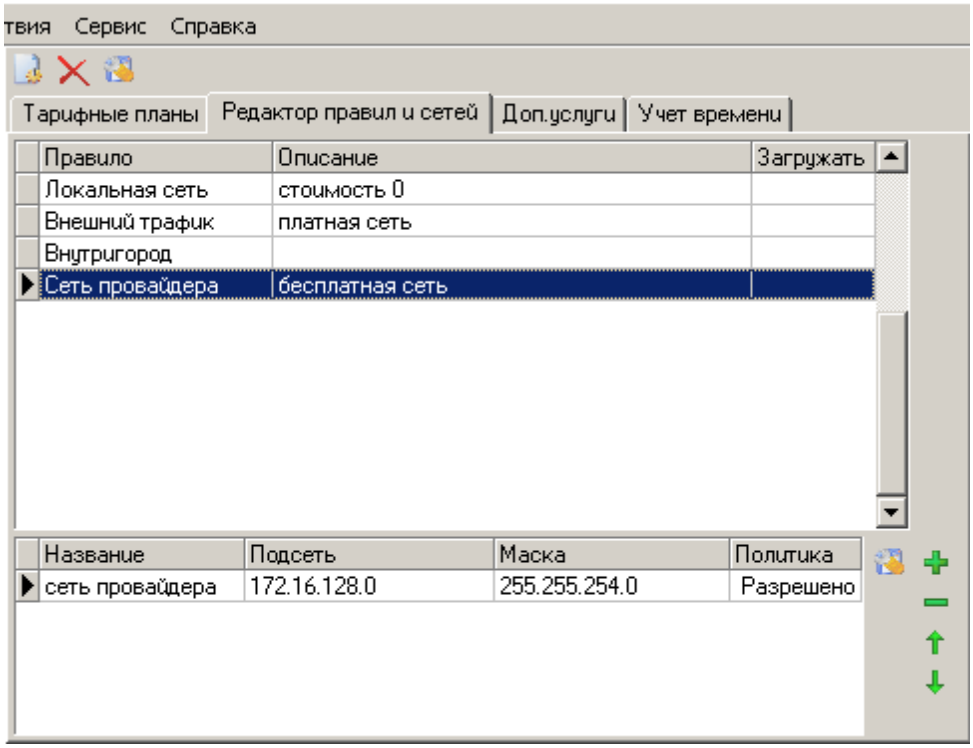
Обратите внимание, что:

- При тарификации, правила проверяются сверху вниз, то есть если трафик не попадает в первое правило, то проверятся следующее и так до последнего правила.
- Если трафик не попадает ни в одно правило, то он блокируется. Поэтому последним правилом, как правило, следует указывать правило Внешний (Весь Интернет).
- После добавления правил, проверьте их порядок. При необходимости измените их последовательность с помощью кнопок вверх и вниз. Как правило, первым стоит правило локальной сети со стоимостью равной нулю.

5.2.8.2 Редактор правил и сетей

Правила используются в тарифных планах. Правило в свою очередь состоит из списка сетей с указанием политики.

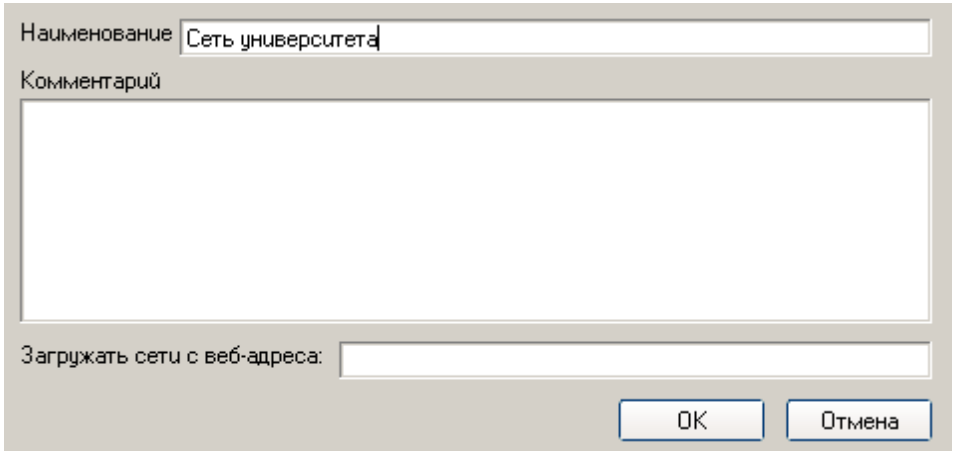
Для редактирования правил нажмите в разделе **Тарифные планы** нажмите закладку **Редактор правил и сетей**.



В таблице показаны все имеющиеся правила, а в нижней таблице все сети этого правила.

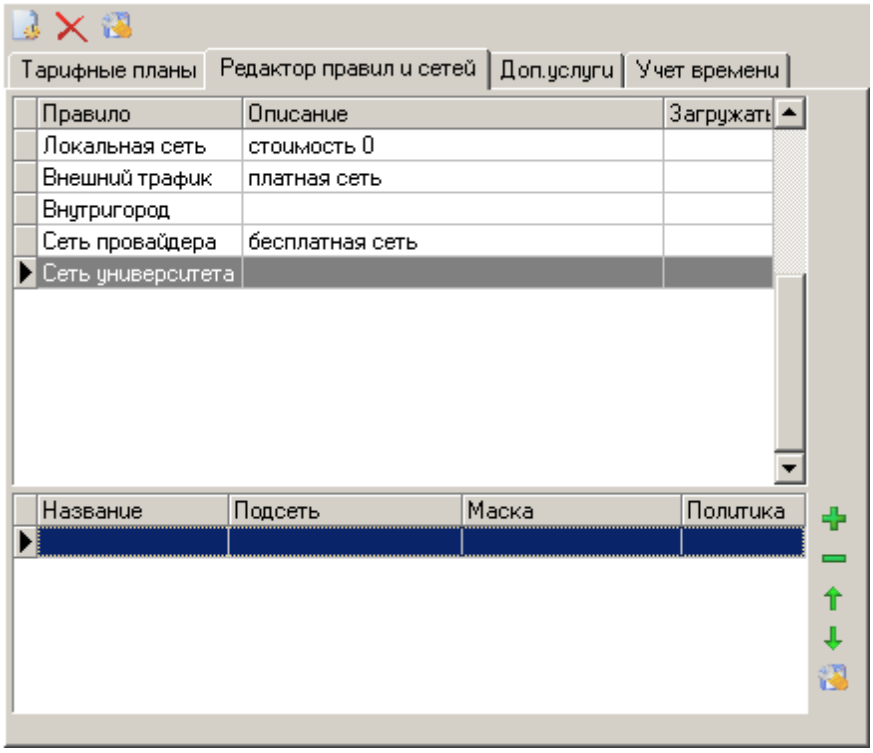
Для создания нового правила:

1. Нажмите кнопку  **Создать новое правило** на панели инструментов.



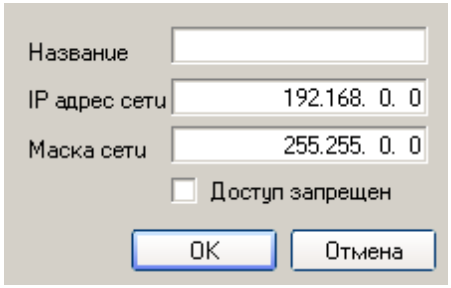
2. В появившемся окне введите название правила и описание. Нажмите кнопку **OK**.
3. Выберите вновь созданное правило.

   Снизу отображается пустой список сетей:



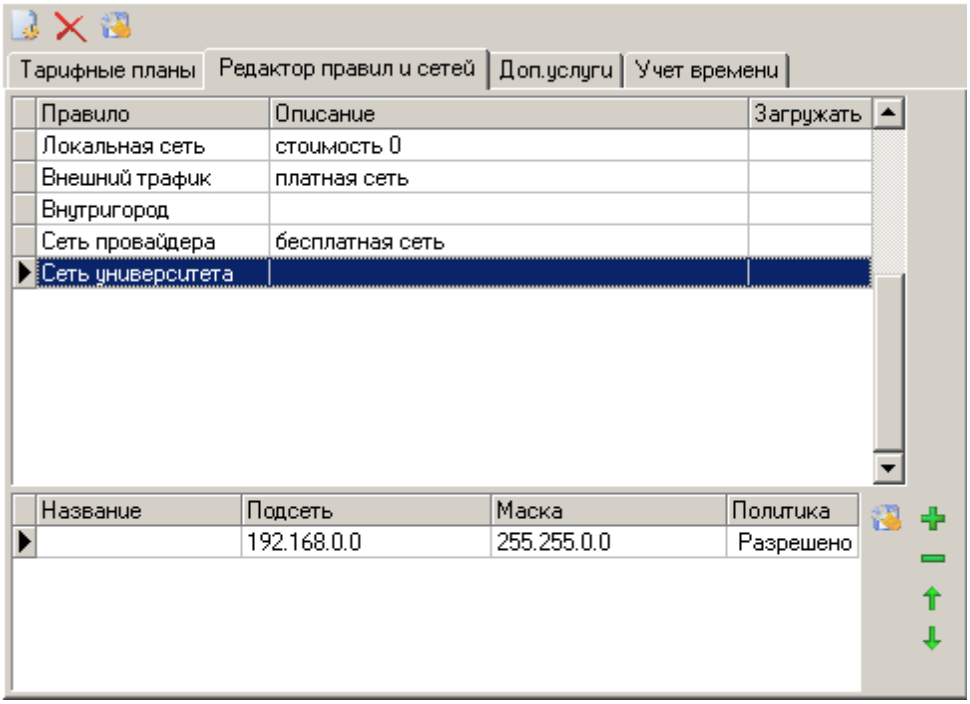
4. Для добавления новой сети нажмите кнопку **Добавить подсеть в правило** .

5. Появится окно задания подсети.



- **Название** – описательное название, можно пропустить.
- **IP-адрес** сети – указать адрес сети
- **Маска сети** – указать маску сети
- **Доступ запрещен** – означает, что к этой сети доступ будет полностью закрыт.

6. Нажмите кнопку **ОК.** Создано правило для сети университета с описанным в нем диапазоном адресов, готовое к добавлению в тариф.



Замечание: Сети внутри правила, также как и правила внутри тарифных планов, проверяются сверху вниз. Если у всех подсетей в правиле стоит **Разрешено**, то это не имеет значения. В противном случае это нужно учитывать.

Варианты использования политики **Запрещено**:

- **Исключение IP-адресов из правила**
  Например, есть большая подсеть тарифицируемая одинаково. Но в ней есть маленькие подсети или просто одни IP-адрес который нужно тарифицировать по-другому. В этом случае можно создать правило, состоящее из этой большой подсети и для нужных IP-адресов закрыть доступ, и добавить их в другое правило.
- **Закрытие ресурсов**. Подробнее см. Создание закрытых ресурсов 228.

5.2.8.3 Создание закрытых ресурсов

Тарифные планы позволяют создавать закрытые ресурсы, то есть ресурсы, доступ к которым могут иметь только определенные пользователи. Такими ресурсами, например, могут быть внутренние сервера предприятия, или внешние ресурсы Интернет, доступ к которым должен обеспечиваться только закрытой группе пользователей или из определенных подсетей.

Создавать такие ресурсы с использованием тарифных планов можно двумя способами:

1. В тарифном плане назначаемом пользователя определить подсети доступ к которым должен быть закрыт и установить у них политику **Запрещено**. Этот тарифный план использовать для пользователей, которым должен быть закрыт доступ к указанным ресурсам. А в другом тарифном плане для этих

подсетей установить политику **Разрешено**, и назначать его пользователям, которым нужно разрешить доступ.

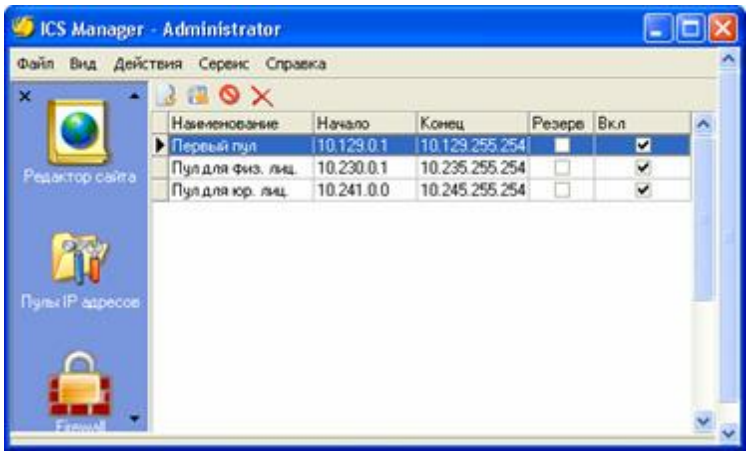
2. Другой вариант (применим только для внутренних серверов предприятия). Для того чтобы создать такой "закрытый" сервер, нужно что бы он сам был подключен к серверу Ideco ACP. И использовать для него отдельный тарифный план. В этом тарифном плане определить подсети, с которых можно подключаться к этому серверу и с которых нельзя: например, запретить все и открыть только нужным пользователям (по их IP-адресам или подсетям-пулам). При этом, не только для самого сервера будут закрыты некоторые подсети, но и пользователи из этих подсетей не смогут подключиться к нему.

Замечания:

При создании таким способом закрытых серверов предприятия, нужно обеспечить, что бы доступ к ним был только через сервер Ideco ACP. Более развитые возможности по созданию закрытых ресурсов предоставляет встроенный Firewall (доступен только в редакции Enterprise Edition). Подробнее см. Встроенный Firewall 255.

5.2.9 Пулы IP-адресов

Для удобства управления IP-адресами назначаемыми пользователям и компьютерам используется понятие **Пул IP-адресов**. Пул IP-адресов – это диапазон IP-адресов, из которого назначаются IP-адреса пользователям при создании пользователей.



Замечания:

1. Рекомендуется разделить IP-адреса используемые для компьютеров в локальной сети предприятия и IP-адреса пользователей выдаваемые Ideco ACP.

   По умолчанию, используется следующая схема:

   - Диапазон "10.0.0.2 – 10.127.255.255" используется для IP-адресов компьютеров
   - Диапазон "10.128.0.1 – 10.255.255.254" используется для IP-адресов

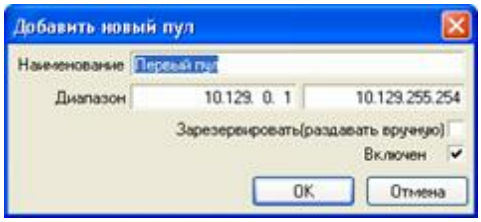
пользователей.

2. Раздел **Пулы IP-адресов** доступен только **Главному администратору**.

5.2.9.1 Создание пула IP-адресов

Чтобы создать новый пул:

1. В разделе **Пулы IP-адресов** на панели инструментов нажмите кнопку  **Добавить новый пул IP-адресов**. Появится следующее окно:



2. Заполните поля:

   Наименование – название создаваемого пула. Например, "Пул для всех пользователей".

   Диапазон – диапазон IP-адресов (IP-адрес первого и IP-адрес последнего). Например, "10.230.0.1 – 10.235.255.254".

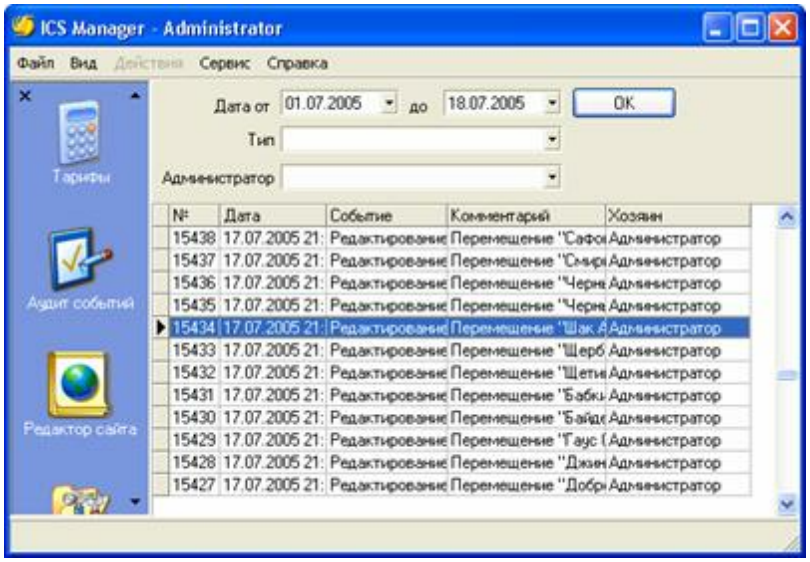
   Зарезервировать – Если признак установлен – это означает что этот пул будет "зарезервирован", тоесть IP-адреса из этого IP-диапазона не будут раздаваться автоматически, даже если они входят в какой-нибудь другой пул. Рекомендуется для пулов реальных IP-адресов.

   Включен – если признак не установлен, то пользователи, у которых установлен данный пул, не смогут выйти в Интернет.

Совет: Если правильно распределить для различных групп пользователей разные пулы и придерживаться этого при назначении IP-адресов пользователям, то это позволит простым образом использовать различные настройки Firewall для разных пользователей, или создавать закрытые ресурсы с помощью тарифных планов. В этом случае в качестве подсетей нужно будет указывать не разрозненные IP-адреса, а те же подсети что указаны в качестве пулов.

5.2.10 Аудит событий

Операции администраторов в Ideco ACP Manager фиксируются. Это позволяет определить администратора и время выполнения того или иного действия.



Для просмотра событий нажмите на панели быстрого запуска кнопку **Аудит событий**.

Для вывода конкретных типов событий можно использовать фильтр: по дате, по типу, по администратору.

По каждому событию фиксируются следующие параметры:

Дата – дата и время изменения БД

Событие – тип события: редактирование пользователя, редактирование тарифных планов и т.д.

Комментарий – пояснение что было изменено/создано.

Хозяин – пользователь, который произвел действие.

5.2.11 Монитор

Показывает список подключенных в настоящий момент пользователей.

IP-абонента – адрес пользователя, выдаваемый при VPN-соединении.

IP-компьютера – физический адрес компьютера

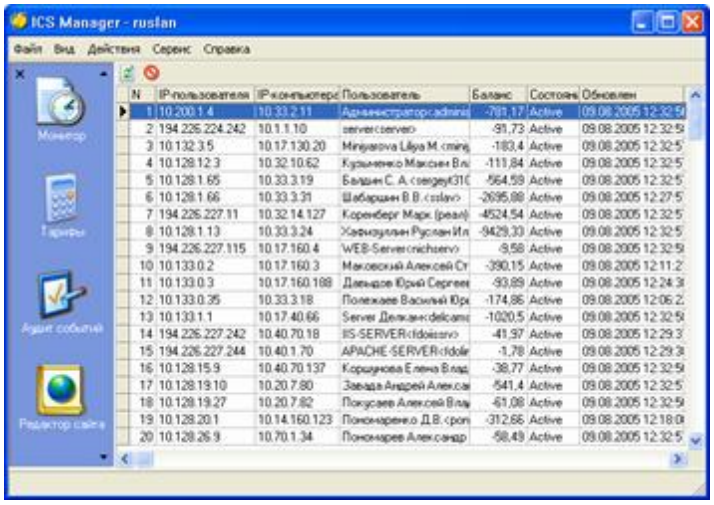
Пользователь – название пользователя

Баланс – баланс пользователя

Группа – родительская группа

Состояние – Текущее состояние пользователя. **Active** – была активность (создавался трафик) за последние 10 минут. **Not Active** – не было активности за последние 10 минут

Обновлен – время последнего обновления статистики



5.2.12 Редактор сайта

В разделе **Редактор сайта** редактируется информация, отображаемая в Личном кабинете пользователя.

При редактировании контактной информации и содержания новостей можно использовать форматирование HTML. При этом все тэги HTML должны быть обязательно закрыты. Например, "…" или так
.

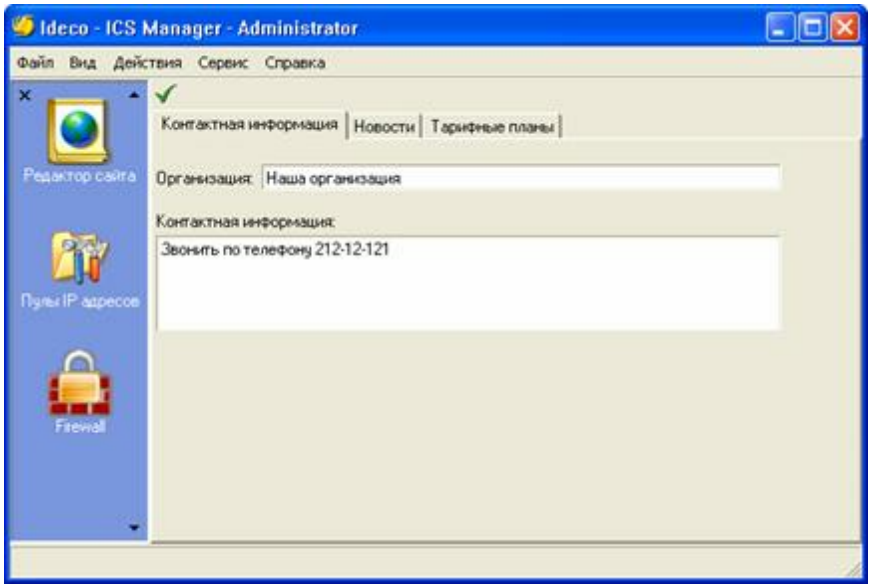
После редактирования информации в этом разделе обязательно проверьте правильность ее отображения в Личном кабинете пользователя.

Редактировать данные могут только администраторы, находящиеся в корневой группе.

Контактная информация

Организация – отображается в заголовке всех страниц АСРа. Напишите название вашей организации.

Контактная информация – отображается на странице "Поддержка". Напишите координаты администраторов сети (телефоны, e-mail и т.д.) куда будут обращаться пользователи в случае необходимости.



Новости

Редактируется раздел "Новости" АСРа пользователя, с помощью которого можно информировать пользователей об изменениях в сети, тарифных планах и т.д.

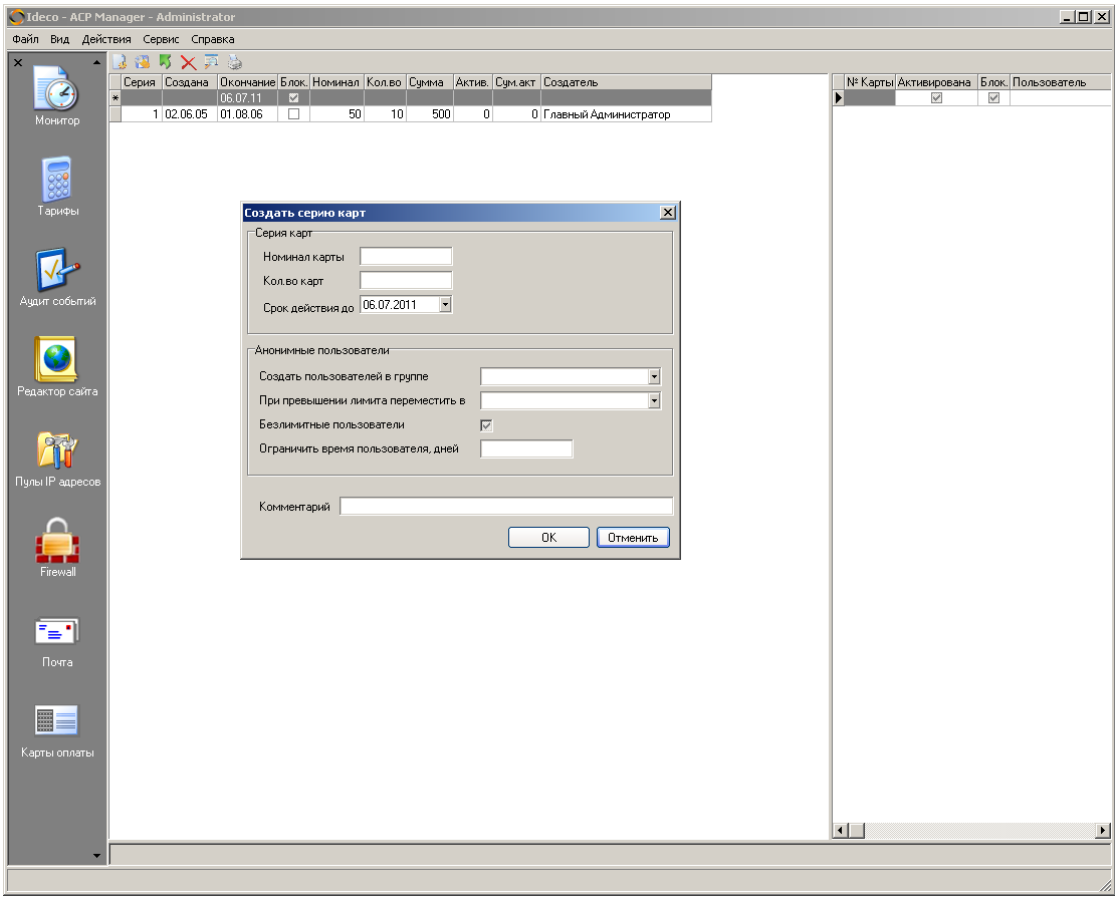
Тарифные планы

Редактируется раздел "Тарифные планы" главной страницы. Указывается, какие тарифные планы будут отображать в разделе "Тарифные планы".

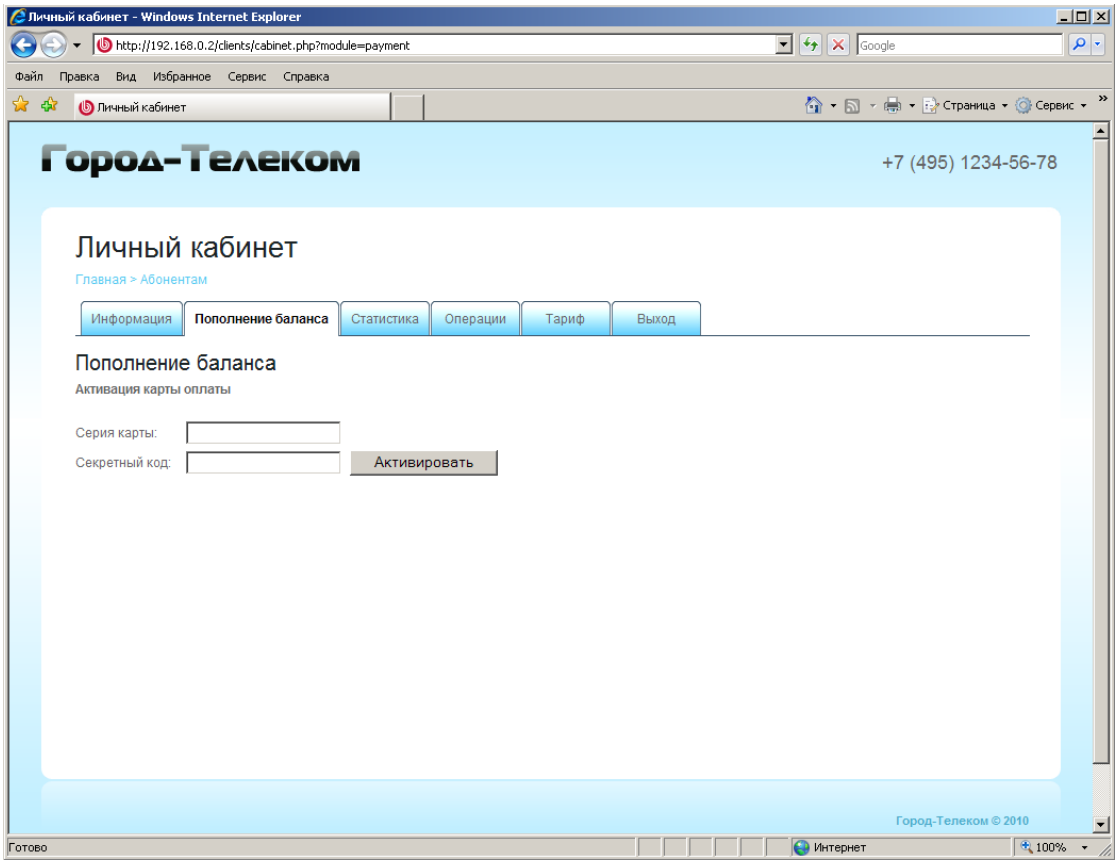
5.2.13 Карты оплаты

Ideco ACP содержит ряд средств позволяющих предлагать пользователям для оплаты услуг карты оплаты с закрытым секретным полем (также известные как "scratch cards"). Эти средства включают:

1. Раздел "Карты оплаты" в Ideco ACP Manager. Позволяет генерировать заданное количество уникальных карт оплаты различного номинала с возможностью разбития на серии. Позволяет выполнять операции: добавление и удаление серий и отдельных карт в/из списка разрешенных к платежу, печать карт оплаты, блокирование карт оплаты (в том числе сериями), управление сроком действия карт и др.



2. Занесение средств с Карты оплаты на счет клиента. Выполняется пользователем из веб-интерфейса. При активации карты оплаты определяется ее номинал и проверяется платежеспособность. В случае успеха проверки сумма, равная номиналу, зачисляется на счет пользователя, а сама карта помечается как активированная.



5.2.13.1 Параметры карт оплаты

Создаваемые в системе Ideco ACP карты оплаты описываются следующими параметрами:

Серия – идентификатор серии, которой принадлежит карта. Номера серий создаются последовательно. Также используется для проведения платежа по карте;

Создание – дата создания карты;

Окончание – дата окончания срока действия карты;

Блокирована – признак блокирования карты, означает, что карта недоступна к платежу. Может устанавливаться как у всей серии, так и у отдельной карты;

Номинал – номинал карты. Измеряется в условных единицах;

Код – секретный код карты, использующийся при проведении платежа по карте. Поддерживается уникальность кодов на всем времени жизни системы. Состоит из 9 десятичных цифр;

Активирована – признак того, что карта использована.

Уничтожена – Признак полного уничтожения серии карт без возможности

восстановления.

5.2.13.2 Управление картами оплаты

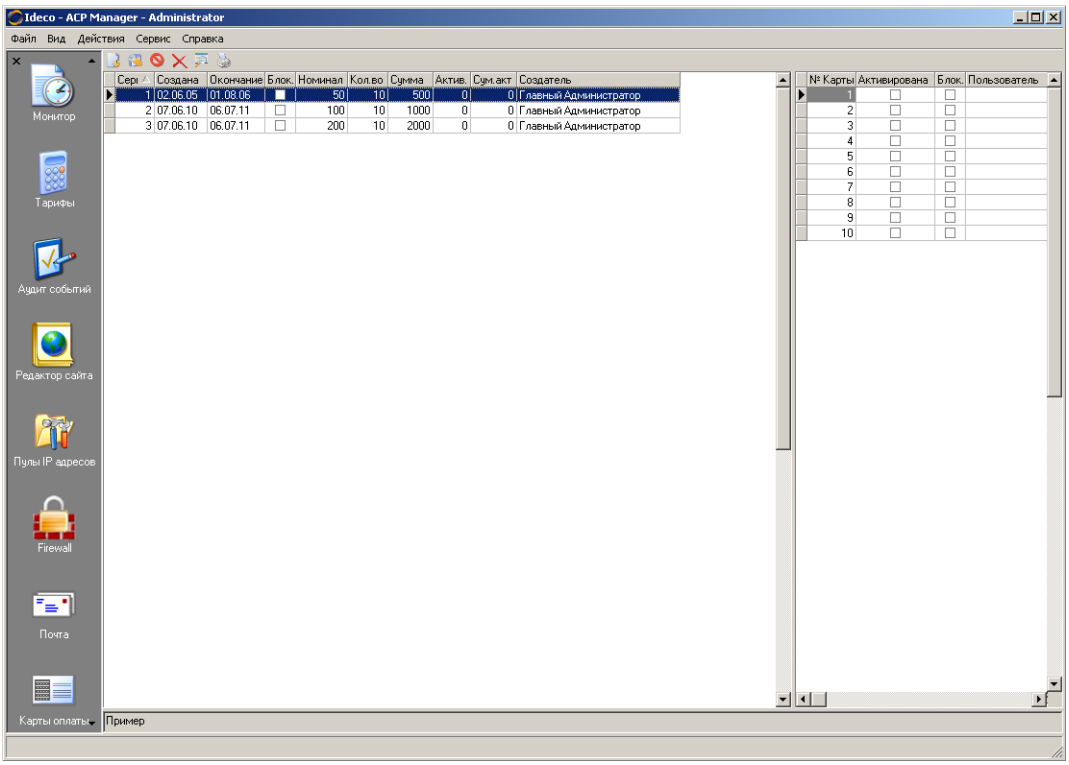
Генерирование карт оплаты, операции над картами оплаты выполняются в Ideco ACP Manager в разделе **Карты оплаты**.

Замечание: Функции для работы с картами оплаты доступны только **Главному администратору** и администраторам с установленным признаком "Администратор карт оплаты".

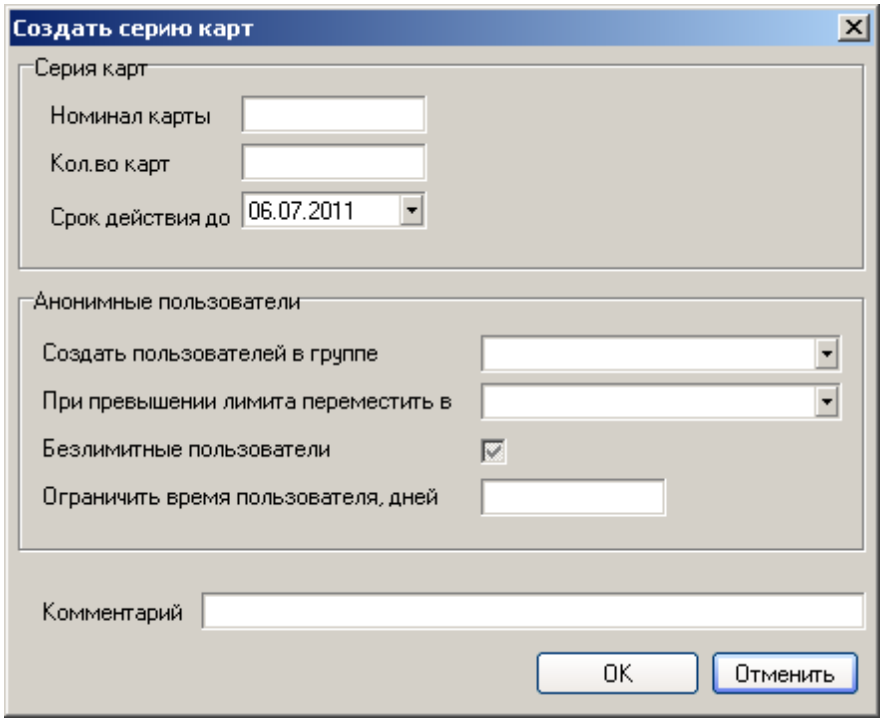
5.2.13.2.1 Создание карт оплаты

Карты генерируются сериями с идентификаторами серии. Параметры карт задаются администратором. Секретный код генерируется случайно.

1. На панели разделов выберите **Карты оплаты**.



2. На панели инструментов нажмите кнопку **Создать серию**.



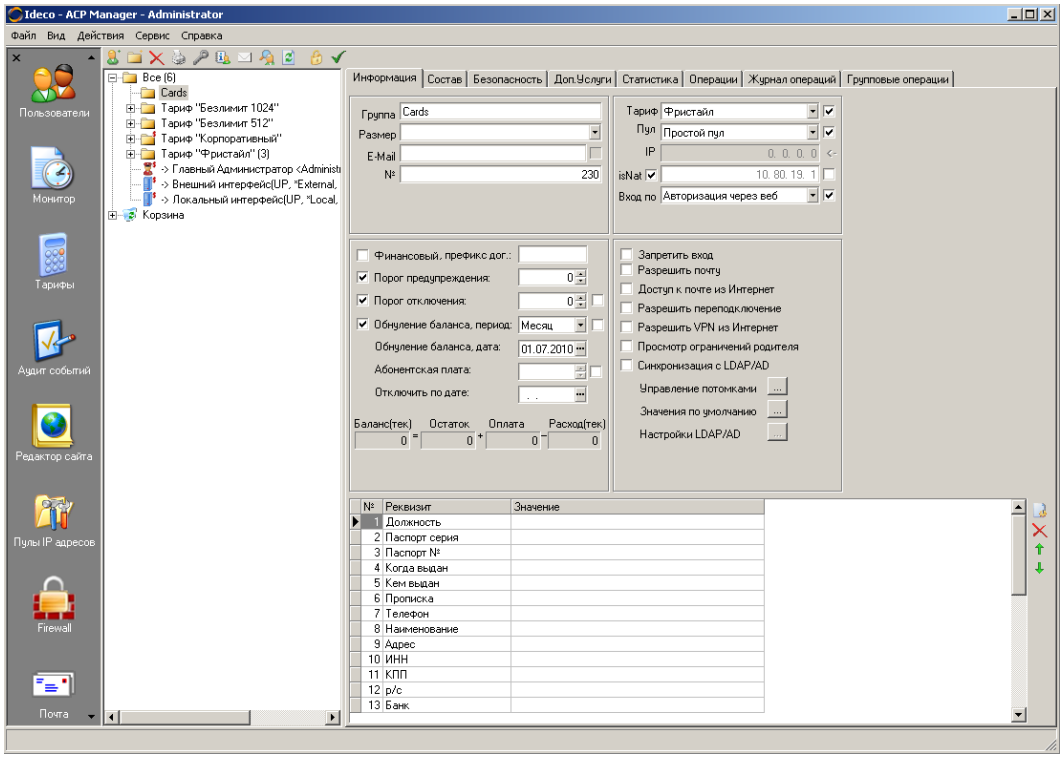
3. Задайте параметры:
   - **Номинал** – номинал создаваемых карт.
   - **Кол-во карт** – общее количество карт в серии.
   - **Срок действия** – срок действия карт в серии
   - **Комментарий** – при желании можете ввести комментарий
4. Нажмите кнопку **ОК**. После чего будет создана серия карт.

5.2.13.2.2 Создание карт оплаты для анонимных пользователей

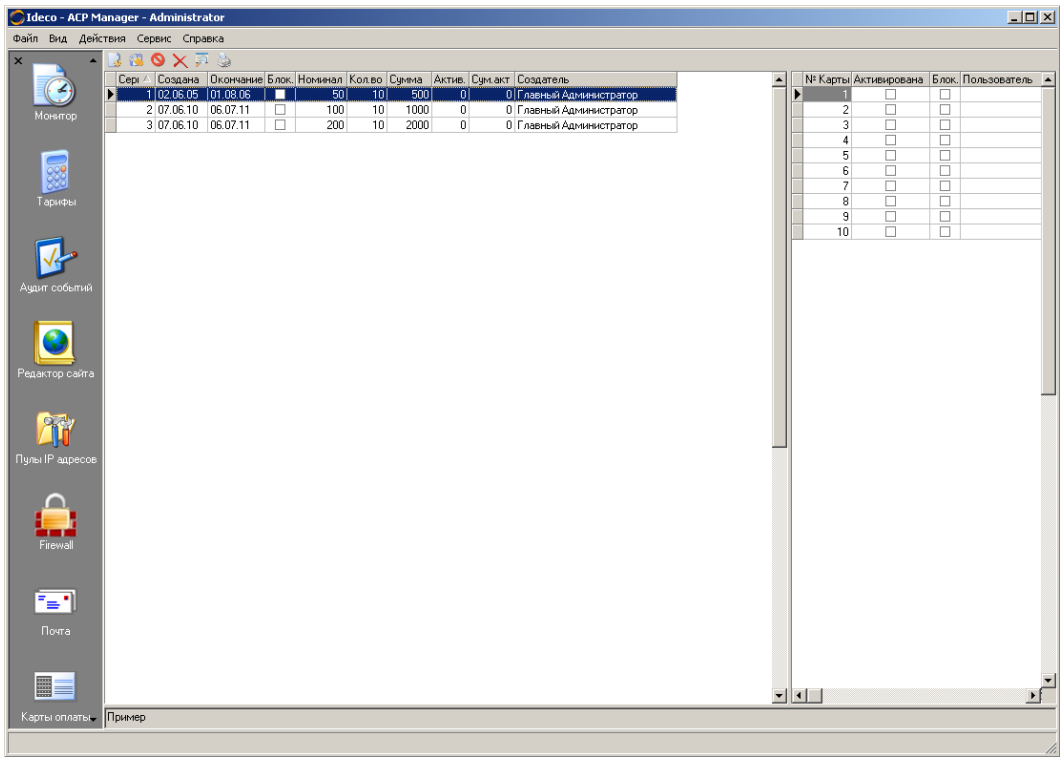
В Ideco ACP есть возможность создавать серии карт для анонимных пользователей ещё не зарегестрированных в базе.

1. На панели разделов выберите **Пользователи**, создайте в дереве пользователей новую группу задайте на этой группе требуемые параметры:
   - Тарифный план
   - Пул адресов
   - Тип авторизации
   - Порог отключения
   - Порог предупреждения

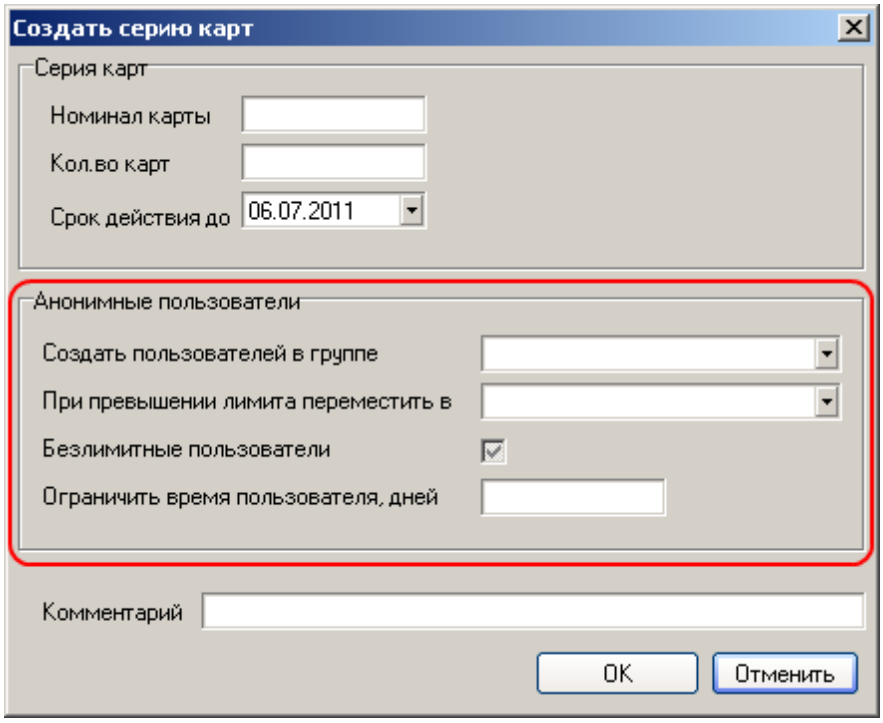
   В этой группе в дальнейшем будут созданы карточные пользователи:



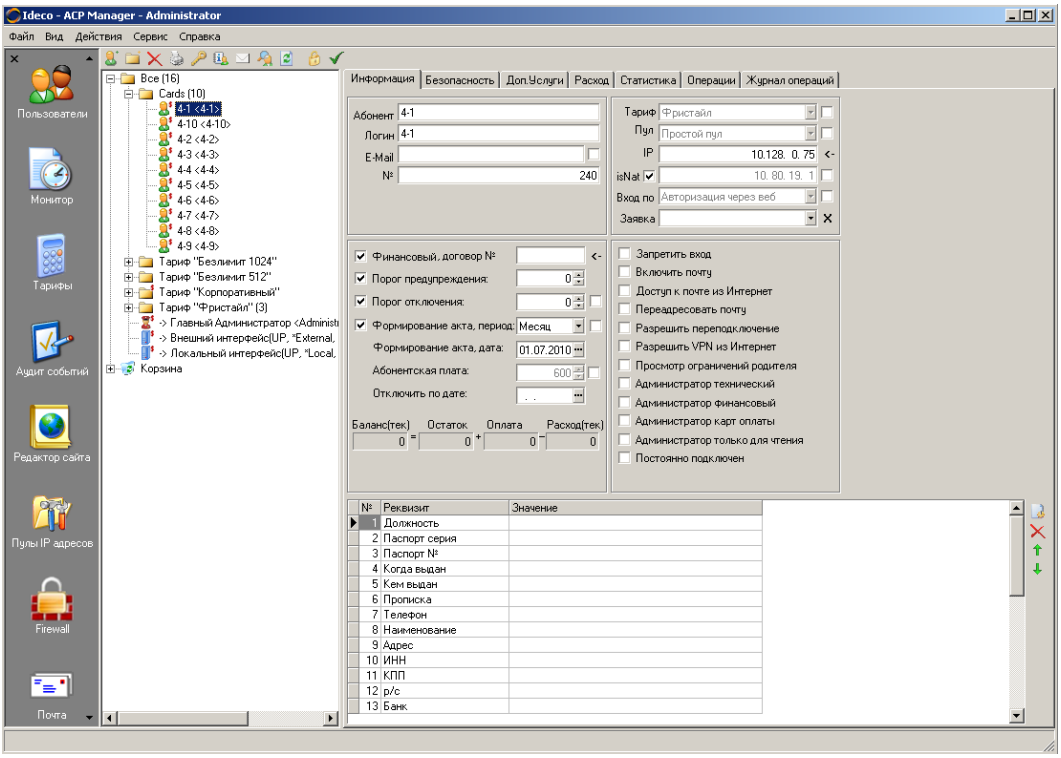
2. На панели разделов выберите **Карты оплаты**.



3. На панели инструментов нажмите кнопку **Создать серию**.



4. Задайте обязательные параметры:
   - **Номинал** – номинал создаваемых карт
   - **Кол-во карт** – общее количество карт в серии
   - **Срок действия** – срок действия карт в серии
   - **Создать пользователей в группе** - укажите ранее созданную группу
5. При необходимости задайте дополнительные параметры:
   - **При превышении лимита переместить в** - укажите группу куда будут перемещены анонимные пользователи, превысившие лимит.
   - **Безлимитные пользователи** - данная опция используется если пользователь будет ограничен только в количестве дней на использовании карты оплаты и, соответственно, эту галочку можно поставить только указав параметр **Ограничить время пользователя, дней**.
   - **Ограничить время пользователя, дней** - количество дней, в течение которого будет работать карточка после её активации.
   - **Комментарий** – можно ввести комментарий.
6. Нажмите кнопку **OK**. После чего будет создана серия карт.
7. Зайдите обратно в раздел **Пользователи**, нажмите кнопку **Обновить** на панели задач и убедитесь, что в группе для карт оплаты появились анонимные пользователи:



5.2.13.2.3 Операции над картами оплаты

Над уже сгенерированными картами оплаты можно проводить следующие операции:

Изменение срока действия карт в серии

Для изменения нажмите кнопку **Редактировать** на панели инструментов, укажите необходимое значение.

Блокирование или **разблокирование** серии

Для блокирования/разблокирование серии выберите нужную серию в списке, на панели инструментов нажмите кнопку **Блокировать** или **Разблокировать** серию.

Блокирование или разблокирование отдельной карты

Выполняется прямо в таблице со списком карт. Для этого выберите нужную серию, затем выберите нужную карту в серии, установите или снимите флажок в колонке **Блок**.

Уничтожение серии карт

Для того что бы уничтожить серию карт выберите нужную серию в списке и нажмите кнопку **Уничтожить**. При этом серия карт физически из БД не уничтожается. Физическое уничтожение проводится только после закрытия периода.

Важно! После уничтожения эту серию восстановить уже невозможно. Для просмотра уничтоженных серий нажмите кнопку **Показать уничтоженные серии**.

5.2.13.2.4 Печать карт оплаты

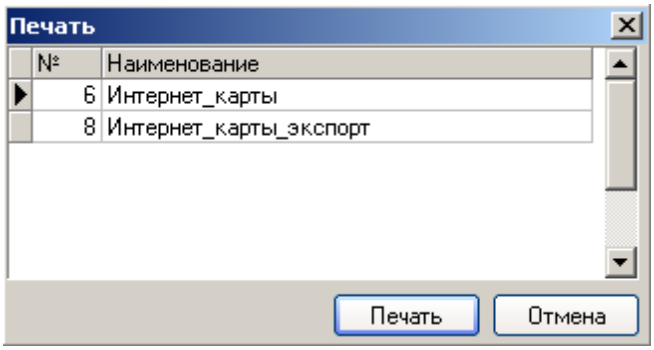
В системе имеется возможность вывода на печать сгенерированных карт оплаты.

Замечание: В случае необходимости выпуска карт со стираемым полем эту возможность можно использовать для экспорта данных по картам и последующего их использования при выпуске в другом месте.

Как и для всех документов в системе для печати используется MS Excel, при этом шаблон вывода можно настраивать под свои потребности. Подробнее см. Шаблоны документов 245.

Карты печатаются сериями.

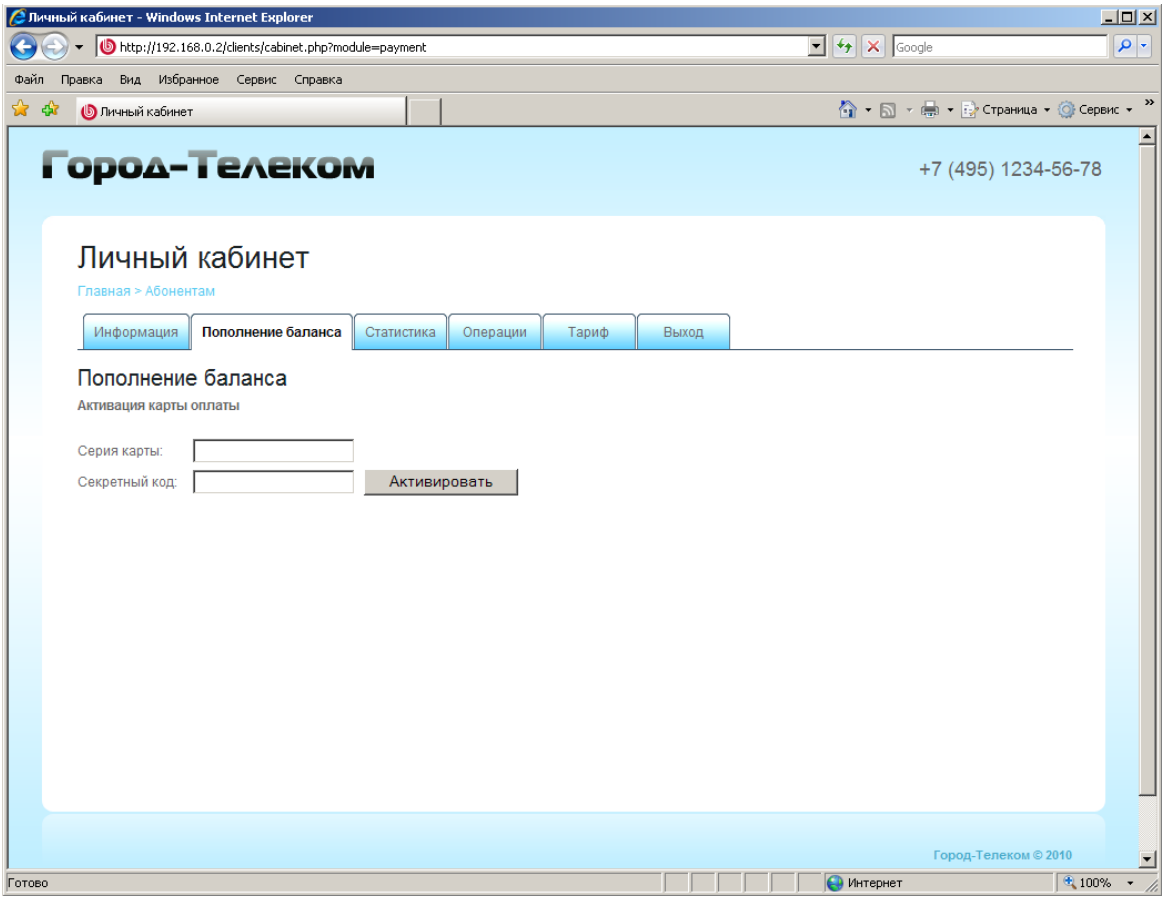
1. Для печати выберите нужную серию, нажмите кнопку **Печать серии карт**.



2. Нажмите кнопку **Печать**.

5.2.13.3 Платежи по картам оплаты

Осуществляется пользователем из веб-интерфейса пользователя. При проведении платежа он вводит номер серии и секретный код карты.



Платеж производится при наступлении следующих условий:

- номер серии и секретной код совпадают с имеющимися в БД;
- срока действия карты больше текущей даты;
- серия не уничтожена, серия не заблокирована, карта не заблокирована, карта не активирована

После проведения платежа карта помечается как активирована.

5.2.13.4 Активация карт оплаты анонимными пользователями

Для активации анонимной карты оплаты необходимо авторизоваться на Ideco ACP. Подробнее 60 ..

Независимо от типа авторизации (кроме авторизации по IP) в качестве логина используется связка: Серия карт - Номер карты, например, если серия карт 4, а номер карты 1, то логин будет **4-1**. В качестве пароля используется поле **Код**:

Интернет карта Карта авансового платежа Номинал: 100 рублей Рег. №: 1		Серия: 4 Код: 239977164
Интернет карта Карта авансового платежа Номинал: 100 рублей Рег. №: 2		Серия: 4 Код: 570770777
Интернет карта Карта авансового платежа Номинал: 100 рублей Рег. №: 3		Серия: 4 Код: 931527467

5.2.14 Учет времени

Учет времени позволяет учитывать и тарифицировать время соединения пользователя с сервером.

5.2.14.1 Варианты использования

1. В местах платного предоставления рабочего времени за компьютером. Например, в Интернет кафе, Игровые клубы и т.п. В этом случае можно учитывать и тарифицировать время работы пользователя за компьютером.
2. При использовании ограниченных ресурсов для подключения. Например, в WiFi сетях количество одновременно работающих пользователей, а также их качество работы, ограничивается количеством радиоканалов. В этом случае, в дополнение к трафику можно также тарифицировать и время соединения пользователя, т.к. при этом он занимает один из радиоканалов.
3. Ограничить часы разрешенной работы с Интернет например с 10:00 до 18:00. Для этого нужно определить диапазон от 10:00 до 18:00 и указать стоимость 0/час. В остальное время установить соединение не получится.

5.2.14.2 Принцип работы

Учет времени работает аналогично тарифным планам по учету трафика, но при этом как самостоятельный тарифный план, т.е. не включается в тарифные планы по учету трафика. Таким образом, у пользователя будут работать одновременно и обычный тарифный план и учет времени.

Учет времени работает следующим образом: указывается диапазон IP-адресов, при подключении с которых, нужно учитывать время работы и указывается стоимость одного часа в зависимости от времени. Таким образом, если IP-адрес пользователя или компьютера попадает в указанный диапазон, то для

пользователя ведется учет времени.

В отличие от тарифных планов, которые явно назначаются пользователям, учет времени для пользователей явно не задается и работает для всех пользователей, в зависимости от того какой у них IP-адрес или с какого IP-адреса они подключаются.

5.2.14.3 Создание тарифного плана по учету времени

1. Перейдите в раздел **тарифные планы**. Выберите закладку **Учет времени**.
2. На панели инструментов нажмите кнопку  **Создать тарифный план**.
3. Введите название тарифного плана и нажмите кнопку **ОК**.
4. Справа покажется два пустых списка: интервалы времени с указанием стоимости одного часа и список IP-диапазонов.
5. Заполните эти списки, используя кнопки редактирования справа от таблиц.

   Например. Если, время работы на стоимость работы не влияет, то создайте один интервал:

   Начало интервала – 0:00:00; Конец интервала – 23:59:59; Цена за 1 час – 10.

   И, например, следующие диапазоны IP-адресов: 10.33.3.0 – 10.33.3.255; 10.33.5.0 – 10.33.5.256.

   Тогда для всех пользователей с такими IP-адресами, а также для всех подключающихся с компьютеров, IP-адреса которых входят в указанные диапазоны, будут тарифицироваться в соответствии 10 условных единиц за 1 час.

5.2.15 Расположение администраторов в дереве пользователей

В системе Ideco ACP заложен принцип, что администратор может управлять всеми пользователями и подгруппами группы, в которой находится сам. При этом он одновременно как пользователь является и пользователем этой же группы. Т.е. на его трафик считается на эту группу и на него действуют ограничения этой группы.

Такой принцип размещения администраторов является удобным, понятным и удовлетворяет большинству реальных ситуаций. В редких случаях, как правило, в крупных предприятиях и, как правило, для корневых администраторов, может потребоваться другие схемы размещения администраторов:

1. Необходимо, чтобы администратор как пользователь находился в какой-то конкретной группе пользователей своего отдела. И при этом мог управлять, например, всеми пользователями или всей вышележащей группой.

   Такую ситуацию можно решить так:

Для таких администраторов создать два логина:

- Один, как для пользователя в той группе где он должен находиться как пользователь. Под этим логином он будет устанавливать VPN-соединение и работать в Интернет.
- И второй как для администратора, в корне той группы, которой он должен управлять. Установить для него ограничение доступа. Т.е. с этим логином он не сможет выходить в Интернет, и будет использовать его только для работы с БД.

Для удобства работы, у первого логина установить один из административных признаков. Т.к. для работы с Ideco ACP Manager нужно обязательно установить соединение под пользователем являющимся администратором. Тогда для установки VPN-соединения он будет использовать первый логин, а для подключения к БД второй.

2. Администратор должен управлять группами пользователей находящихся в разных местах дерева. Для этого:
   - Как и в предыдущем случае, создать по отдельному логину в каждой группе пользователей с ограничением доступа, или
   - Что более удобно, поместить такие группы в одну группу верхнего уровня.

5.2.16 Шаблоны документов

Для вывода всех документов и отчетов для печати используются шаблоны Microsoft Excel. Поэтому для просмотра и печати необходим установленный Microsoft Excel.

Все шаблоны хранятся в БД. По умолчанию в системе задан типовой набор шаблонов. Все шаблоны сгруппированы по типу документа.

Есть следующие типы:

- Расход
- Приход
- Баланс подвести
- Счет
- Документы
- Отчет за период
- Карты оплаты

Каждый шаблон относится к какому-то одному типу, т.е. в может быть определено несколько шаблонов для каждого типа документа. Тогда, в случае печати, нужно будет указать, какой из имеющихся для данной операции шаблонов использовать.

Принцип работы следующий. Ideco ACP Manager загружает из БД файл с шаблоном и заполняет его данными.

Замечание: Все генерируемые файлы MS Excel (*.xls) сохраняются во

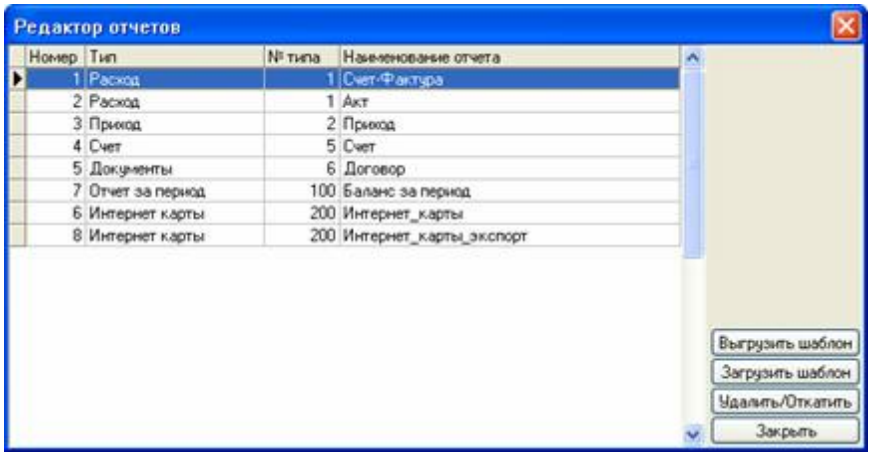
временной папке Windows. После закрытия Ideco ACP Manager они удаляются. Если требуется сохранить файл, то сохраните его в другой папке, для этого – выберите в MS Excel меню "**Файл** > **Сохранить как...**".

5.2.16.1 Редактирование шаблонов

Если имеющихся по умолчанию шаблонов не достаточно, то можно создать новый, или отредактировать существующий.

Замечание: Редактировать шаблоны (сохранять или удалять из БД) может только Главный администратор. Редактирование шаблонов возможно или из отдельного окна – Редактор отчетов или прямо из окна формирования операций.

В главном меню выберите пункт меню **Настройки** > **Редактор отчетов**. Появится окно со списком всех имеющихся в БД отчетов:



Выгрузить шаблон – выгрузить шаблон в виде файла.

Загрузить шаблон – загрузить файл шаблона в БД.

Замечание: Тип документа отдельно не указывается, а выбирается тип шаблона, который выбран в списке. Поэтому если вы хотите загрузить шаблон типа расход, то сначала нужно в списке шаблонов выбрать какой-нибудь шаблон с типом расход. После выбора файла появится диалоговое окно для ввода имени шаблона в БД.

Если будет введено имя уже существующего шаблона в БД, то шаблон будет записан сверху – как новая версия, при этом старый шаблон будет сохранен в БД, и при необходимости к нему будет можно вернуться.

Удалить/Откатить – удаляет выбранный шаблон. При этом если он был записан по верх другого, то происходит "откат" и возвращается предыдущая версия. Таким образом, если шаблон имел много "версий", то при последовательном нажатии этой кнопки будет происходить откат к более ранней версии, пока не будет удалена последняя версия. Заданные по умолчанию системные шаблоны удалить нельзя.

Сами шаблоны редактируются в Excel. Для редактирования шаблона надо понимать принцип вывода данных в шаблон. Самый простой способ сделать свой шаблон следующий:

1. Выгрузить имеющийся шаблон того типа документа, который вы хотите создать.
2. Открыть этой файл в Excel.
3. Понять смысл шаблона, т.е. определить из каких ячеек берутся данные. При этом вы увидите, что часть ячеек используются как служебные, в них выводятся данные. И из "печатных" ячеек есть ссылки на эти ячейки. Служебные поля, как правило, скрыты.
4. Отредактировать шаблон. Сохранить файл. Закрыть файл. Загрузить его в БД.
5. Проверить работоспособность. В случае если выводятся не те данные (другие атрибуты) или отчет не работает повторить пункты 1-4 сначала, стараясь вносить изменения постепенно.

5.2.17 Автоматическое формирование акта

Функция "**Автоматическое формирование акта**" позволяет автоматизировать процесс выставления актов, в случае предоставления услуг доступа в Интернет другим организациям или частным лицам. Эта функция доступна только для финансовых пользователей и групп.

При предоставлении услуг доступа в Интернет юридическим лицам в кредит процесс расчетов, как правило, выглядит следующим образом:

В конце расчетного периода (обычно месяц) определяется сумма оказания услуг, в нашем случае эта сумма равняется "**Расходу за текущий период**" пользователя или группы. На эту сумму одновременно выставляется акт об оказании услуг, счет фактура и выполняется подведение баланса. После подтверждения факта оплаты, оплаченная сумма с помощью операции **Приход** заносится в поле **Оплата**.

При предоставлении услуг доступа в Интернет юридическим лицам по предоплате процесс расчетов, как правило, выглядит следующим образом. Порог отключения устанавливается равным нулю. С помощь операции **Приход** заносится предоплата. В конце расчетного периода (обычно месяц) определяется сумма оказания услуг, в нашем случае эта сумма равняется "**Расходу за текущий период**" пользователя или группы. На эту сумму одновременно выставляется акт об оказании услуг, счет фактура и выполняется подведение баланса.

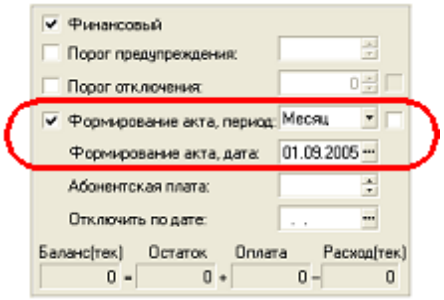
Функция автоматического формирования акта позволяет автоматически выполнять операции:

- Операцию **Расход/Акт** на сумму равную **Расход за текущий период**.
- Операцию **Подвести баланс**.

5.2.17.1 Установка автоматического формирования акта

Для работы автоматического формирования актов нужно в свойствах пользователя или группы установить период и дату формирования акта. Для этого:

1. Выберите нужного пользователя или группу в дереве пользователей.
2. Перейдите на закладку **Информация**.
3. Задайте необходимые параметры. Например, как показано ниже:



Формирование акта, период – установите период формирование акта, обычно месяц.

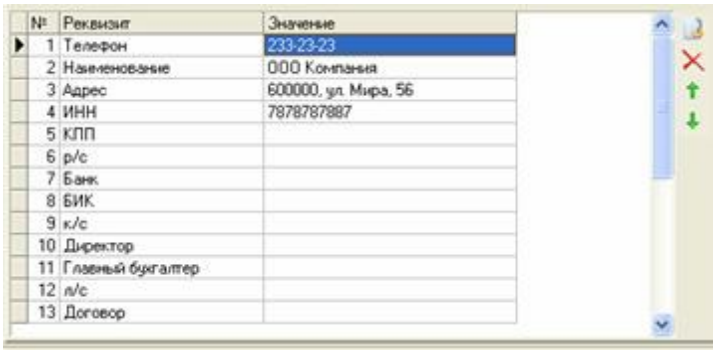
Формирование акта, дата – укажите дату первого формирования акта, т. е. дата следующего формирования акта. Когда формирование акта сработает, дата автоматически изменится на следующую дату.

Совет: Для того чтобы вывести на печать документы сразу по всем сгенерированным операциям можно воспользоваться закладкой "Групповые операции". Подробнее см. Закладка "Групповые операции"

5.2.18 Реквизиты пользователя и группы

Для пользователя и группы в дополнение к основным свойствам можно задавать реквизиты. **Реквизиты** – это информационные поля, не влияющие на работу системы. По реквизитам можно делать поиск пользователей, выводить в документах. Список реквизитов можно изменять.

Список реквизитов находится внизу закладки **Информация** пользователя и группы:



№	Реквизит	Значение
1	Телефон	233-23-23
2	Наименование	ООО Компания
3	Адрес	600000, ул. Мира, 56
4	ИНН	7878787887
5	КПП	
6	р/с	
7	Банк	
8	БИК	
9	к/с	
10	Директор	
11	Главный бухгалтер	
12	л/с	
13	Договор	

5.2.18.1 Ввод значений

Значения реквизитов редактируются прямо в таблице. Для изменения нужного реквизита встаньте на запись с нужным реквизитом в ячейку колонки Значение и введите нужно значение.

Замечание: При редактировании реквизитов они сразу сохраняются в БД. Т.е. не нужно нажимать кнопку "**Сохранить**" на панели инструментов, как при редактировании остальных свойств на закладки "Информация".

5.2.18.2 Редактирование списка реквизитов

Если среди имеющихся по умолчанию реквизитов нет нужного реквизита, или для удобства работы нужно изменить порядок реквизитов в списке, то можно отредактировать сам список реквизитов.

Замечания:

Редактировать список реквизитов может только **Главный администратор**.

Список реквизитов общий для всех пользователей и групп. Поэтому при удалении реквизита, создании нового, изменения порядка следования реквизитов – эти изменения отобразятся у всех пользователей. А при удалении реквизита будет удален сам реквизит, а также его значения у всех пользователей.

Для редактирования списка реквизитов, рядом с таблицей расположена панель с кнопками редактирования:

Кнопка	Назначение
	Создать новый реквизит
	Удалить реквизит


Переместить реквизит по списку вверх


Переместить реквизит вниз по списку вниз

5.2.19 Операции

В этой главе описываются возможности Ideco ICS по работе с лицевым счётом абонента.

5.2.19.1 Закладка "Операции"

Для учёта финансовых операций пользователей предусмотрена система расчётов, которая автоматизирует такие операции как: списание денежных средств, начисление денежных средств, формирование отчётов, вывод на печать документов и т.д. Доступ к системе расчётов осуществляется через раздел **Операции** в ACP Manager.

Для перехода на закладку Операции выберите в дереве пользователей нужную группу или пользователя и перейдите на закладку **Операции**. На этой закладке выполняются операции с лицевыми счетами пользователей и групп, формируются и выводятся на печать документы.

Информация о состоянии лицевого счета

Параметр	Описание
Баланс (бух.)	"Бухгалтерский" баланс. Баланс (бух.) = Остаток + Оплата
Остаток	Остаток на начало отчетного периода, т.е. с последнего подведения баланса и выставления акта.
Оплата	Сумма поступлений с начала отчетного периода.
Расход за текущий период	Сумма расхода трафика с начала отчетного периода.
Итого текущий	= Баланс (бух.) - Расход за текущий период

баланс

Кнопки формирования операций

Кнопка	Описание
Приход	Начисление денег на лицевой счет. При формировании этой операции увеличивается поле **Оплата**.
Расход/Акт	Списание с лицевого счета за трафик. При этом указанная сумма вычитается из поля **Расход за текущий период** и вычитается из поля **Остаток**
Подвести баланс	Закрытие бухгалтерского периода. При этом поле **Оплата** обнуляется, а поле значение поля **Баланс (бух.)** переносится в поле **Остаток**.
Обнуление баланса	Обнуление баланса, при этом все поля обнуляются. Доступно только для нефинансовых абонентов.
Документы	Формирование нефинансовых документов, т.е. не влияющих на состояние баланса. Например, договор на оказание услуг.
Счет на предоплату	Счет не предоплату. Не влияет на состояние баланса. Доступно только для финансовых абонентов.
Исправить баланс	Кнопка ручного исправления баланса. Позволяет напрямую редактировать состояние баланса пользователя (поля **Остаток**, **Оплата**, **Расход за текущий период**). Пользоваться ей следует только в исключительных ситуациях. Например, при внедрении системы Ideco ACP может потребоваться перенести баланс пользователя из другой системы.

Замечания:

1. Выполнять операции могут только администраторы с установленным признаком **Администратор финансовый**. При попытке выполнить операцию администратором, у которого этот признак не установлен, появится сообщение: "Недостаточно прав. Вы не являетесь финансовым администратором!".
2. Кнопка **Исправить Баланс** доступна, только администратором находящимся в корне дерева пользователей.
3. Финансовые операции отменить нельзя. В случае выполнения ошибочной операции нужно выполнить дополнительную операцию устраняющую ошибку – "сторнирование", то есть запись аналогичной операции с отрицательной (противоположной) суммой.
4. Операции **Расход/Акт** для финансовых абонентов и **Обнуление баланса** для нефинансовых, как правило, выполняются с определенной периодичностью, обычно раз в месяц. Этот процесс можно автоматизировать. Подробнее см. Автоматическое обнуление баланса 207 и Автоматическое формирование акта 247.

5.2.19.1.1 Нумерация операций

Каждой операции, в момент ее формирования, автоматически присваивается номер.

Схема нумерации операций для разных абонентов отличается:

1. Для нефинансовых пользователей и групп – сквозная нумерация по всем операциям внутри пользователя или группы.
2. Финансовый пользователь – нумерация по каждому типу операции внутри пользователя.
3. Финансовая группа – сквозная нумерация по всей БД по каждому типу операции.

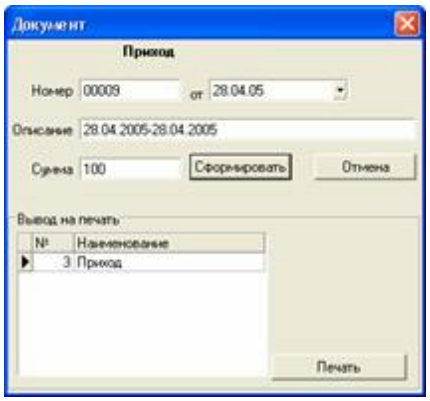
Совет: По умолчанию номера операций имею вид "00001, 00002, 00003...". Для того чтобы установить другой вид номеров, например, принятых в вашей организации, или для того чтобы задать начальные номера, нужно просто задать номер при создании операции. Тогда установленный номер будет использоваться при выполнении следующих операций. Например, если при создании новой операции вместо сгенерированного номера вида "00010" написать номер "AB0127", то номера следующих операций автоматически будут генерироваться так: "AB0128, AB0129, AB0130…".

5.2.19.1.2 Формирование операции

Процесс формирования всех операций однотипен. Покажем на примере выполнения операции **Приход**.

Для зачисления денег на лицевой счет абонента:

1. Выберите нужного пользователя или группы в дереве пользователей.
2. Перейдите на закладку **Операции**.
3. Нажмите кнопку **Приход**.
4. Появится следующее диалоговое окно:



Номер – генерируется автоматически

От – дата операции, выводимая на печать

Описание – описание операции

Сумма – сумма операции. Это поле есть при выполнении операций: Приход, Расход/Акт, Документы, Счет на предоплату.

Заполните эти поля и нажмите кнопку **Сформировать**. После этого операция будет сформирована и записана в БД.

5.2.19.1.3 Вывод на печать

- Если вы только что сформировали операцию, то не закрывая окно формирования операции, выберите в списке один из доступных шаблонов для данной операции и нажмите кнопку **Печать**, или
- Если операция была сформирована ранее, то найдите эту операции в списке и дважды щелкните на ней, появится это же окно Формирования операции. Выберите нужный шаблон и нажмите кнопку **Печать**.

После этого на основе шаблона будет сформирован и открыт файл **MS Excel**. Подробнее о создании, редактировании и работе с шаблонами см. Шаблоны документов 245.

Примечание: О возможности выполнения операций одновременно по нескольких группам или пользователям см. Закладка "Групповые операции" 254.

Совет: Выполнение операций Расход/Акт и Обнуление баланса можно автоматизировать. Подробнее об этом см. Автоматическое обнуление баланса и Автоматическое формирование акта.

5.2.19.1.4 Список операций

Все операции фиксируются в БД и отображаются в виде списка. В нижней части закладки **Операции** отображается список операций по текущему пользователю или группе.

Выводятся следующие поля:

Номер, **Описание**, **Сумма**

Тип (расход, приход или документ)

Дата (от какого числа, может не совпадать с датой создания)

Знак (знак операции: "1" – приход, "-1" - расход, "0" – нефинансовая)

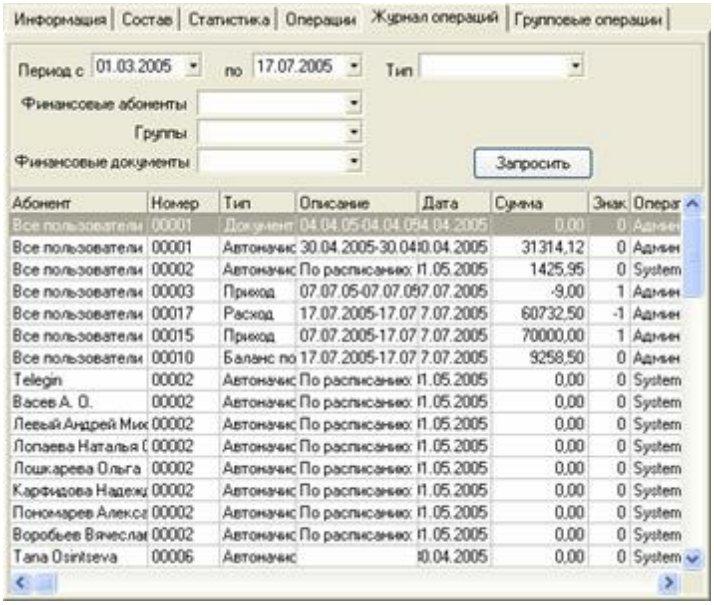
Баланс (бух.) (значение "бухгалтерского" баланса, после проведения операции)

Оператор (человек выполнивший операцию).

Замечание: На закладке **Операции** отображается только информация по текущему пользователю или группе. О возможности просмотра, поиска операций учитывая подгруппы см. Закладка "Журнал операций" 254.

5.2.19.2 Закладка "Журнал операций"

На этой закладке можно просматривать все выполненные операции, задавая различные условия для выбора. Список всех операций оп одному абоненту можно посмотреть также на закладке **Операции**.



Для просмотра операций выберите нужную группу или пользователя в дереве пользователей. Если выбрана группа то будут учитываться все операции по этой группе, а также по всем вложенным группам и пользователям. Для просмотра всех операций выберите группу **Все пользователи**.

Перейдите на закладку **Журнал операций**.

В верхней части окна задайте условия для выбора операций и нажмите кнопку **Запросить**.

В таблице будут выведены все операции, удовлетворяющие заданным условиям выбора.

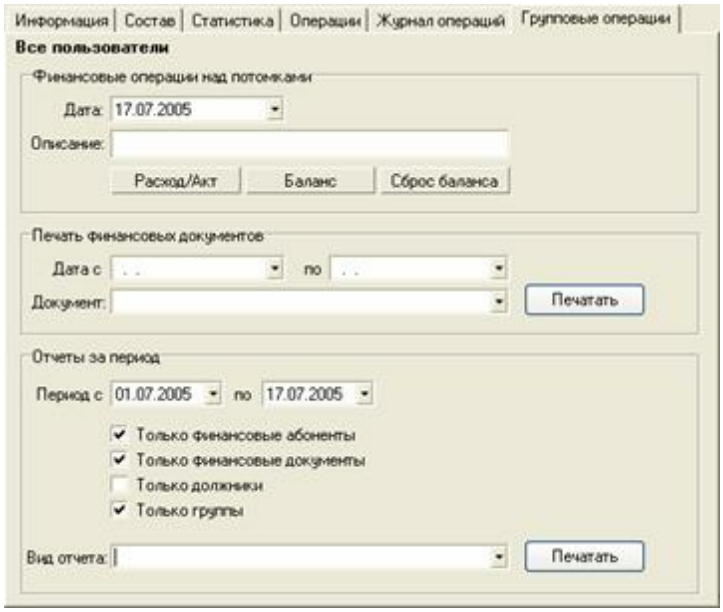
Для печати выполните двойной щелчок на нужной операции. После этого появится окно формирования операции, без возможности редактирования операции. Выберите нужный шаблон и нажмите кнопку **Печать**.

5.2.19.3 Закладка "Групповые операции"

Данная закладка в основном интересна большим предприятиям и провайдерам.

Для выполнения групповых операций над всеми потомками группы выберите закладку групповые операции. Нажмите кнопку Расход, Баланс или Сброс баланса и данная операция будет выполнена для всех вложенных пользователей и групп.

На закладке групповые операции также можно выводить на печать документы за период и распечатывать групповые отчеты по документам.



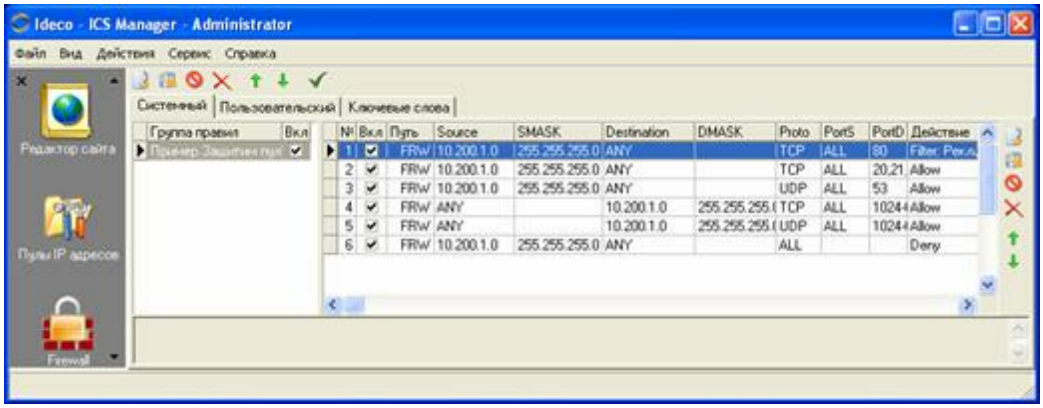
5.2.20 Встроенный Firewall

По умолчанию, все пользователи Ideco ACP защищены технологией NAT, кроме этого возможно наложить различные ограничения для пользователей через Firewall.

Ideco ACP содержит в себе встроенный многофункциональный Firewall. С помощью этого Firewall можно ограничивать трафик пользователей, а также исходящий и входящий на сервер трафик по различным критериям. Firewall настраивается с помощью Ideco ACP Manager.

Важно:

1. Если у вас более 500 пользователей, то не рекомендуется использовать Пользовательский Firewall. Правила в этом случае лучше писать в Системном, разделяя подсетями права доступа к ресурсам.
2. Для того чтобы правильно устанавливать правила Firewall рекомендуется обратиться к соответствующей литературе по безопасности или к специалистам



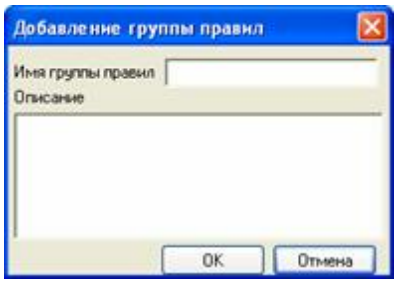
Во встроенном Firewall все правила объединяются в группы. **Правила проверяются строго сверху вниз.**

Firewall в Ideco ACP разделяется на системный и пользовательский:

- Правила написанные в системном Firewall действуют на всех пользователей.
- Правила написанные в пользовательском Firewall действуют только на тех пользователей или групп у пользователей, у которых они добавлены в разделе "Пользователи - Безопасность - Ограничение по IP трафику, Пользовательский Firewall". Подробнее204 ..

5.2.20.1 Создание группы правил

Для добавления группы правил, нажмите на кнопку  в верхней панели.

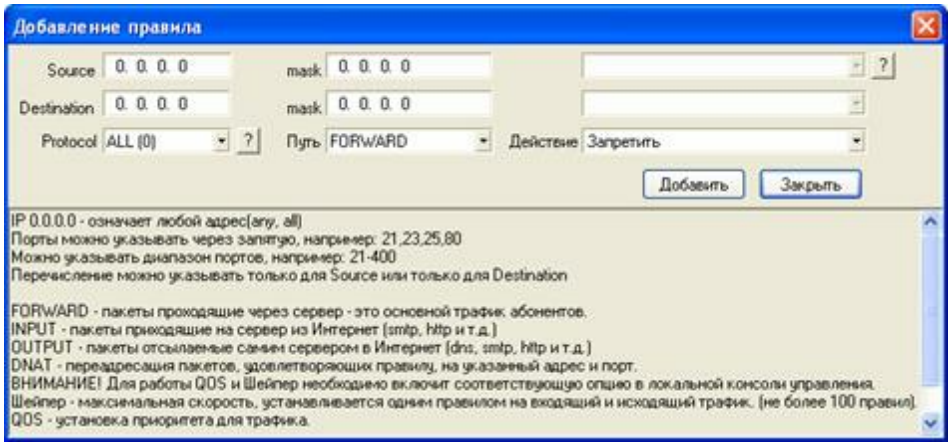


1. Введите **Имя группы правил** и описание (не обязательно).
2. Нажмите **OK**.

После того, как группа создана, в нее можно добавлять правила Firewall.

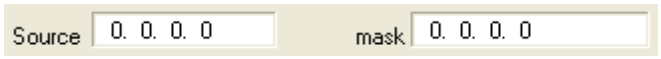
5.2.20.2 Создание правила Firewall

Для создания правила в группе, выделите ее и нажмите на кнопку  в панели инструментов справа.



Далее, необходимо ввести параметры правила Firewall:

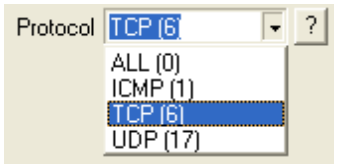
Источник, назначение и протокол



Source, **mask** – IP-адрес и маска подсети источника пакетов.

Destination, **mask**– IP-адрес и маска подсети назначения пакетов.

Примечание: Маска подсети 0.0.0.0 означает любые пакеты, а маска 255.255.255.255 означает только указанный в соответствующем поле IP-адрес.



Protocol – Протокол передаваемых данных. Самый распространенный протокол - TCP.

В качестве протокола, можно выбрать пункт из списка, или указать номер протокола в виде числа. 0 – означает любые протоколы. Список закрепленных за номерами протоколов можно посмотреть, нажав на кнопку ? справа от списка протоколов. Для возврата к справке по общим параметрам, нажмите на эту кнопку еще раз.

Замечание: При выборе протокола, отличного от **ALL** в верхней правой части окна появляются дополнительные опции правила

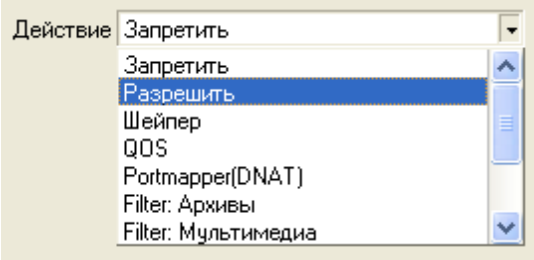
Для протоколов TCP и UDP появляются поля ввода портов для источника и назначения. Можно выбрать порты либо из списка, либо ввести вручную. Допускается ввод нескольких портов через запятую. В этом случае, порты будут проверяться по принципу ИЛИ. 0 – означает любы порты. Список закрепленных за номерами портов можно увидеть, нажав на кнопку ? справа от списка портов. Для возврата к справке по общим параметрам, нажмите на эту кнопку еще раз.

Для протокола ICMP появится поле, позволяющее выбрать конкретный тип ICMP-

сообщений. ВНИМАНИЕ! 0 – означает эхо-запросы (команда ping), а не любые ICMP-сообщения.

Действие

Далее необходимо выбрать **Действие**:



Запретить – Запрет трафик

Разрешить – Разрешить трафик

Шейпер – Ограничить скорость трафика. С помощью этого правила можно ограничить скорость трафика пользователей, серверов или протоколов. При выборе этого действия появится параметр **Макс. Скорость**. Скорость указывается в Килобит/сек. Например, максимальной скорости в 10 Кбайт/сек, соответствует скорость примерно 90 Кбит/сек.

QOS – Назначить приоритет трафика. Всего есть 8 приоритетов трафика, которые можно назначить трафику, отобранному по критериям, указанным в общих правилах Firewall. При выборе этого действия, появится поле для ввода приоритета. В первую очередь будет обрабатываться (передаваться) трафик с приоритетом 1, а в последнюю очередь – трафик с приоритетом 8.

Важно:

Правила QOS и Шейпер будут работать только в случае, если в консоли включен параметр "**Включить интеллектуальное распределение канала**". Подробнее, см. Qos и Шейпер 147

Не рекомендуется создавать более 100 правил с действием **QOS** или **Шейпер**

Portmapper (DNAT) – Перенаправить трафик. При выборе этого правила, появятся поля: 

. Здесь необходимо указать адрес и, опционально, порт назначения. Порт имеет смысл указывать, только если протокол TCP или UDP. С помощью этой возможности можно прозрачно переадресовать трафик на другой адрес или порт. Например, для использования внутреннего прозрачного прокси-сервера или для публикации внутреннего веб-сервера. Можно перенаправить HTTP-запросы ко внешнему IP-адресу на внутренний веб-сервер. Или, например, перенаправить все запросы пользователей на определенный сайт на внутренний прокси-сервер. При учете трафика будет использованы параметры уже после перенаправления. Перенаправление осуществляется на сетевом уровне.

Примечание:

Для перенаправления на встроенный прокси сервер необходимо сделать перенаправление на IP-адрес 169.254.254.254, порт 80. В большинстве случаев, необходимо перенаправлять только **TCP с портом назначения 80**. Для использования такого правила,

встроенный прокси сервер должен быть включен. Подробнее см Веб кэш, веб антивирус, proxy 157.

Следует учесть, что если будет использовано перенаправление WEB-трафика на сторонний прокси сервер, то он должен быть настроен на такой режим работы.

Filter: Название фильтра – С помощью этого действия можно запретить трафик, если передаваемые данные удовлетворяют критерию фильтра. Фильтры настраиваются отдельно – на вкладке "**Контент фильтр**", подробнее см. Ключевые слова 259

Путь

Далее необходимо выбрать какие пакеты будут проверяться. Для этого необходимо выбрать из списка **Путь** одно из следующих значений:

FORWARD – Пакеты, проходящие через сервер. Это основной трафик абонентов.

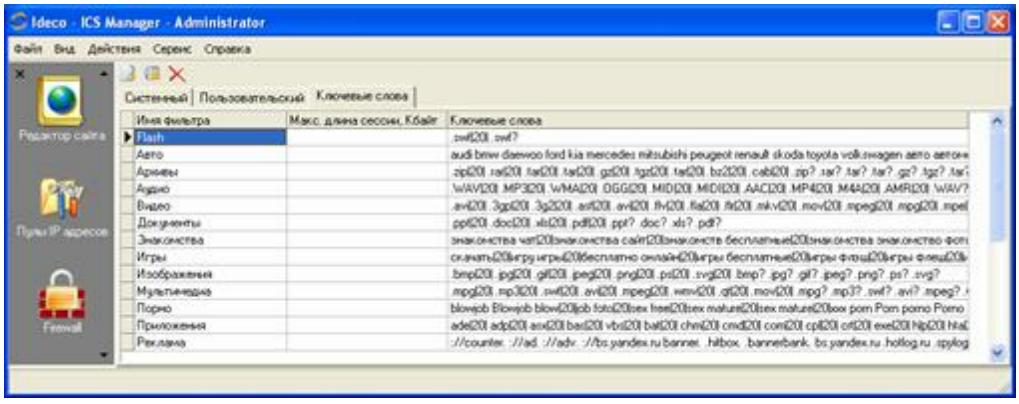
INPUT – Входящие пакеты, предназначенные для самого сервера.

OUTPUT – Пакеты, исходящие от самого сервера.

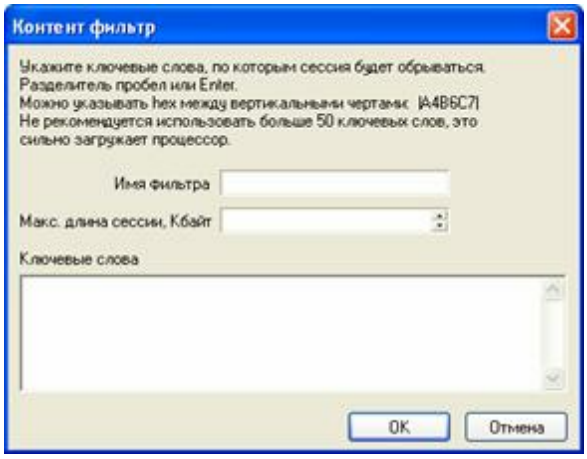
Если вы хотите ограничить доступ к серверу Ideco ACP, например, для блокировки серверов "спамеров", используйте путь **INPUT** и **OUTPUT**. Для ограничения доступа пользователя или нескольких пользователей к сайту, используйте путь **FORWARD**. Для более удобного ограничения нескольких пользователей одним правилом, назначьте этим пользователем IP-адрес из отдельного пула. Тогда в качестве IP-адресов источника или назначения можно будет указать подсеть, соответствующую этому пулу.

5.2.20.3 Ключевые слова

Ключевые слова позволяет задавать правила для запрета трафика, в данных которого находится определенный текст. Ключевые слова настраивается в разделе Firewall на вкладке "**Ключевые слова**".



Во встроенном Firewall Ideco ACP можно создать несколько Ключевых слов. Для создания такого фильтра необходимо нажать на кнопку  в панели инструментов. Появится окно:



Необходимо ввести следующие параметры:

Имя фильтра – Имя правила фильтрации, на которое можно будет сослаться со вкладки "**Правила**".

Макс. Длина сессии – Количество первых килобайт данных соединения, которые необходимо просканировать для поиска ключевых слов.

Ключевые слова – Список ключевых слов, разделенных пробелом или переносом строки. Если при поиске не важен регистр, то необходимо вводить слова со всем возможными вариантами. То же самое касается различных кодировок. Поиск производится напрямую без преобразования кодировок. Используется Win-1251. Если необходимо вставить в текст двоичные данные, то необходимо использовать следующий синтаксис: "|XX|", "|XXXX|" и т.д. То есть, необходимо в текст вставлять символ вертикальной черты, далее четное количество шестнадцатеричных цифр, а затем символ вертикальной черты. Каждая пара шестнадцатеричных цифр будет означать соответствующий байт при поиске ключевого слова. Например, каждый исполнимый файла ОС Windows или DOS начинается с |4D5A5000|. Если синтаксис не будет соблюден, администратор будет предупрежден по почте, а соответствующее правило будет пропущено.

Примечание: Не рекомендуется указывать в правиле более 50 ключевых слов, так как это сильно загружает процессор при активном трафике. Также, следует иметь в виду, что проверяется каждый отдельный IP-пакет независимо от других пакетов этого же соединения. Таким образом, не гарантируется 100% предотвращение пропускания трафика с помощью этих правил. Однако стоит заметить, что вероятность пропуска очень мала.

5.2.20.4 Отключение Firewall

Если оказалось, что Firewall случайно сконфигурирован неверно и стало невозможным подключение к серверу с помощью Ideco ACP Manager, то отключить все правила Firewall можно в локальной консоли, выбрав пункт **Отключить пользовательский Firewall**. При выборе этого пункта отключатся все группы правил Firewall. Никакие правила при этом не удалятся. После этой операции

можно подключиться к серверу с помощью Ideco ACP Manager и разобраться в ситуации.

Часть VI

6 Дополнительно

В данном разделе описана настройка дополнительных служб и приведено несколько примеров по тонкой настройке сервера.

6.1 Создание пользователя root

Инструкция по созданию пользователя root:

1. При загрузке сервера сразу после таблицы BIOS нажимать раз в секунду Ctrl-x, до появления приглашения "**boot:**"

2. Для загрузки в сервисный режим,

в приглашении ввести следующую строку, а вместо слова "ПАРОЛЬ" указать желаемый пароль:

ACPerver p=ПАРОЛЬ nc=1 nm=1

3. набрать пароль servicemode

4. После загрузки сервера нажмите Alt+F7

5. Наберите слово login и нажмите клавишу Enter

6. Введите логин root и нажмите клавишу Enter

7. Введите пароль, который указали при загрузке

8. Наберите команду umount /etc/shadow

9. Наберите команду chattr -i /etc/shadow

10. Наберите команду cat /shadow > /etc/shadow

11. Нажмите Alt+F1

12. Войдите в консоль, набрав соответсвующий пароль

13. Выберите пункт Перезагрузка сервера => Перезагрузка

Для выбора консоли нажмите Alt-F7 и Alt-F8. Для входа в систему нужно набрать "login".

Далее для удаленного доступа, необходимо в локальной консоли сервера, в меню безопасность разрешить

[X] Разрешить полное удаленное управление по SSH

Тогда можно подключаться по SSH на порт 33

Если вы эту опцию поменяли то нужна мягкая перезагрузка.

14. Нажмите **Alt+F1**, чтобы попасть обратно в меню.

Примечание: Внимательней с пробелами.

Если нужно чтоб пользователи могли работать, то сделайте мягкую перезагрузку.

Если будет после первой перегрузке Kernel Panic - это нестрашно -- нажмите reset.

6.2 Как поместить ключ Dr.Web на сервер Ideco ACP

1. Зарегистрировать ваш серийный номер на http://buy.drweb.com/register/ (если нужно активировать и файловый антивирус и почтовый нужен единый ключ, для его получения обратитесь в отдел продаж ICQ 563191479).
2. Скачать ключевой файл, там же.
3. Включить управление файлами по SSH в локальной консоли в меню безопасность. Если было выключено - произвести полную перезагрузку.
4. Скопировать ключевой файл в каталог /DRWEB/key с помощью программы winscp (есть на установочном компакт-диске)
   для winscp логин sysadm пароль как в локальной консоли (servicemode). При копировании обязательно выбрать режим binary (двоичный).
5. Если выбрана лицензия с защитой до 30 почтовых ящиков, то необходимо с помощью putty (есть на установочном компакт-диске) подключиться к серверу, набрать mc и зайти в каталог /DRWEB/etc. Там отредактировать файл email.ini, вписав в него защищаемые адреса вида user@your.domain, по одному адресу на каждой строке. Затем добавить пустую строку в конец файла.

Замечание:

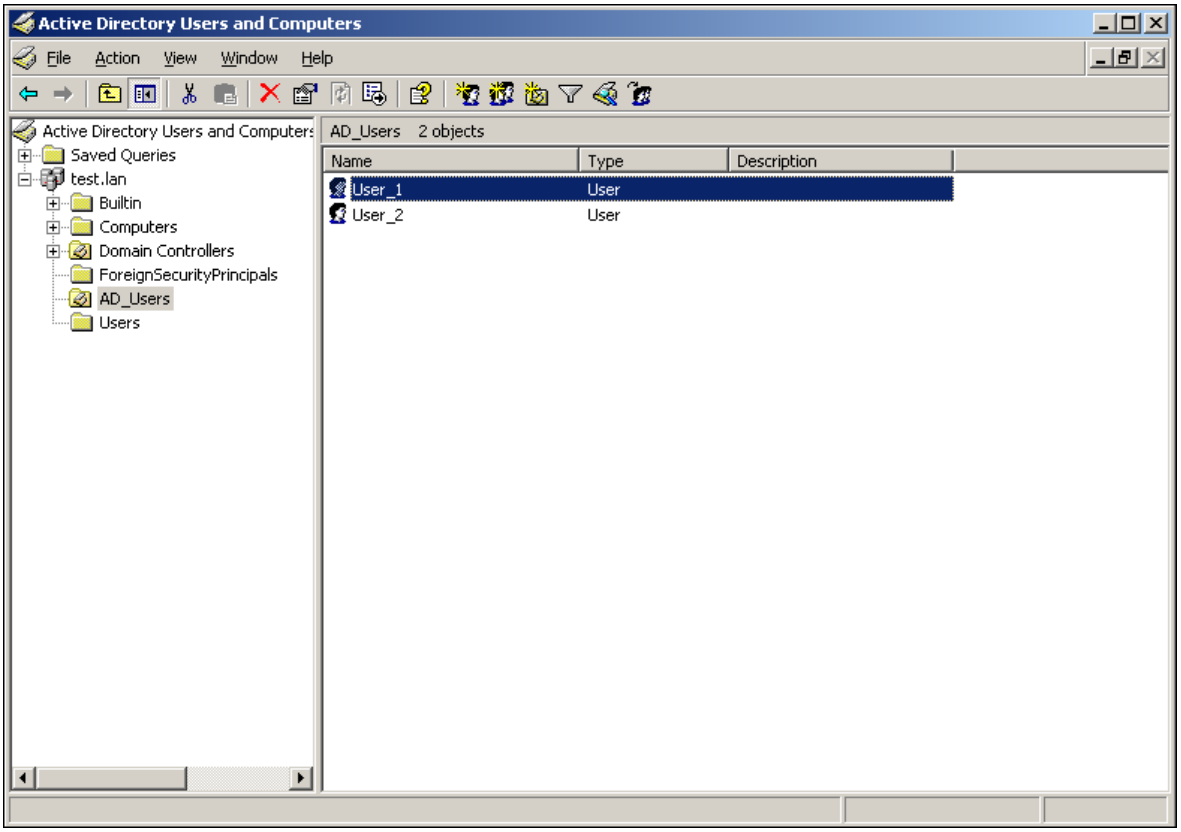
Также адреса необходимо продублировать в файле /var/drweb/emails
Данный файл можно отредактировать из под рута. Или из под рута дать права 666 этому файлу, после этого можно будет редактировать из под sysadm
Иначе в логах будет:

```
drweb-maild: [16384] maild FATAL main: exception: no
addresses found in emails file
drweb-monitor: [16384] ERROR cannot start component "drweb-
maild" from application "MAILD": component stoped himself
drweb-monitor: [16384] ERROR application "MAILD" cannot
start
```

6.3 Настройка синхронизации Ideco ACP с Active Directory или LDAP сервером

Настройка синхронизации Ideco ACP с Active Directory или LDAP сервером

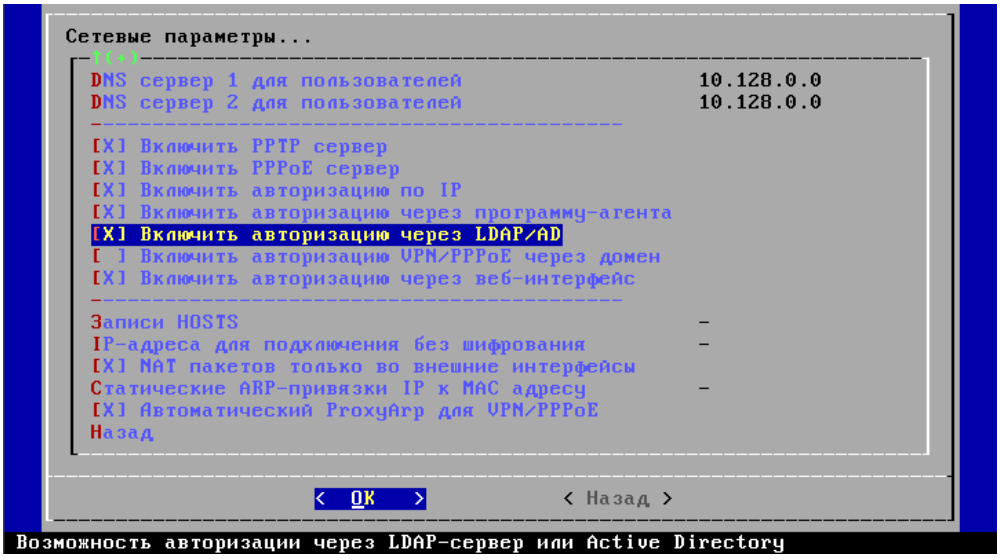
Данная операция выполняется для того, чтобы импортировать сущестующую базу пользователей с контроллера домена, пароли при этом будут храниться на сервере AD, а при авторизации Ideco будет их оттуда запрашивать. В качестве примера рассмотрим контроллер домена, имеющий следующую структуру дерева пользователей:



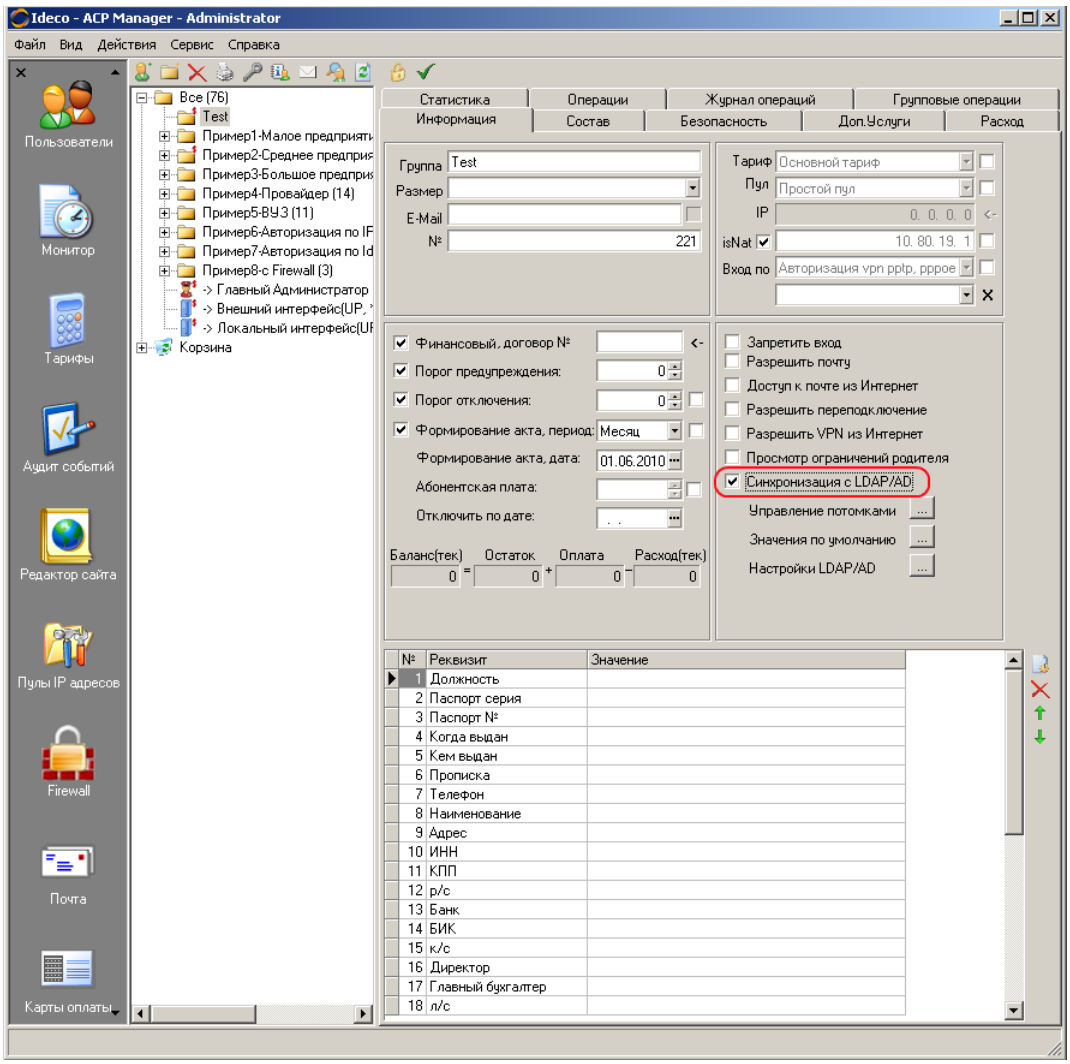
Для того чтобы осуществить авторизацию пользователей через LDAP сервер либо службу Active Directory необходимо произвести следующие операции:

1. В локальной консоли в разделе "Конфигурирование сервера" - "Конфигурирование сети" установить флажок "[X] Включить авторизацию через LDAP/AD".

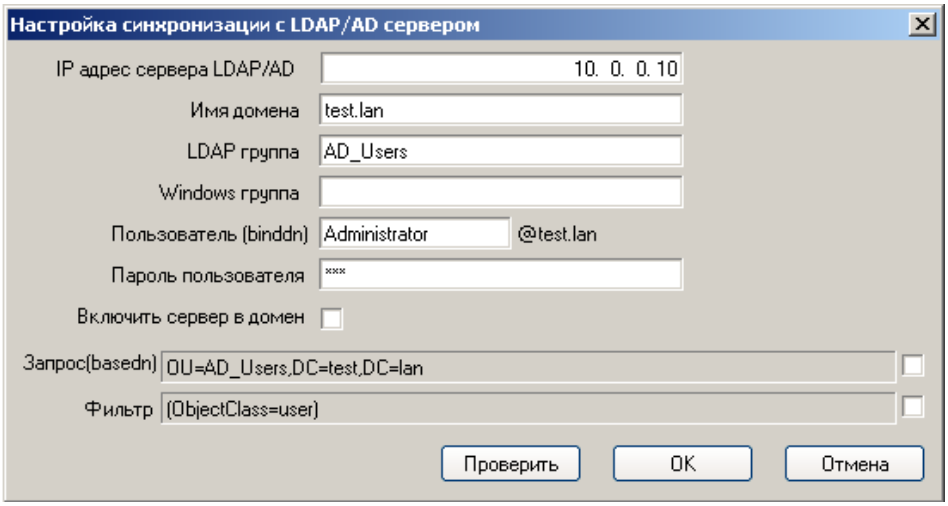
"[X] Включить авторизацию VPN/PPPoE через домен" ставиться только в том случае, когда для пользователей, импортированных из AD, планируется авторизация по VPN.



2. Произвести мягкую перезагрузку.
3. Подключиться к АСРу.
4. Создать новую группу пользователей. В параметрах группы установить флажок "Синхронизация с LDAP/AD".



5. Нажать на кнопку "Настройки LDAP/AD ..."



Установить параметры:

- "IP адрес сервера LDAP/AD" – указать IP адрес контроллера домена
- "Доменное имя" – указать DNS имя домена. Контроллер домена обычно имеет имя "имя.имя домена". Необходимо указать имя домена без имени контроллера.
- "LDAP группа" – указать название папки в LDAP дереве. Для Windows, обычно "Users"
- "Windows группа" – указать название Группы пользователей Windows, пользователи которой должны выходить в Интернет с помощью Ideco ACP. Если такая группа не создана, то оставить это поле пустым. В этом случае будут синхронизироваться все пользователи из папки "LDAP группа"(в нашем примере Windows группа не используется).
- "Пользователь" и "пароль пользователя" – указать логин и пароль для подключения к LDAP серверу. От имени этого пользователя должна быть доступна на чтение "LDAP группа"
- "Включить сервер в домен" - галочка нужна только в том случае если будет использоваться авторизация по VPN.
- Нажать на кнопку "Проверить". Будет произведено тестовое подключение к серверу и проверка пароля.
- Нажать OK.

6. Выбрать в дереве пользователей созданную папку и выбрать меню "Действия" - "Обновить". В папке должны появиться пользователи, загруженные из LDAP. Если число пользователей очень большое, то обновление может занять некоторое время. Если пользователей больше 1000, то необходимо разделить их на отдельные группы.

7. Настроить параметры пользователей, если это требуется.

Более подробно процесс синхронизации с AD показан на одном из наших семинаров:

Специальный проигрыватель - http://www.ideco-software.ru/download/seminars/NV_NetPlayer.exe

Файл записи – http://www.ideco-software.ru/download/seminars/2009_06_23.zip

Примечание: "Windows группа" при синхронизации используется только тогда, когда необходимо из LDAP группы (на языке AD - Контейнер или Organizational Units) импортировать только часть пользователей, обьединённых в группу.

6.4 Словарь терминов

CIPE
CIPE — это реализация VPN, разработанная в основном для Linux. В CIPE шифрованные IP-пакеты инкапсулируются, или «заворачиваются», в датаграммы (UDP). Пакеты CIPE шифруются по стандартному алгоритму CIPE и получают заголовок с информацией о получателе. Затем пакеты передаются поверх IP в виде UDP-пакетов через виртуальное сетевое устройство CIPE (cipcbx) в физическую сеть к удалённому получателю. Официальная страница CIPE - http://sites.inka.de/bigred/devel/cipe.html.

PPPoE
PPPoE (англ. Point-to-point protocol over Ethernet) — сетевой протокол передачи кадров PPP через Ethernet. В основном используется XDSL сервисами.
Более подробную информацию по протоколу PPPoE можно найти тут - http://ru.wikipedia.org/wiki/PPPoE.

PPTP
PPTP (англ. Point-to-point tunneling protocol) — туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой, сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля. Более подробную информацию по протоколу PPTP можно найти тут - http://ru.wikipedia.org/wiki/PPTP. PPTP использует порт 1723 (TCP) и протокол номер 47 (GRE).

Регулярные выражения (regexp) и то как ими пользоваться
Регулярные выражения (regular expression, regexp) — современная система поиска текстовых фрагментов в электронных документах, основанная на специальной системе записи образцов для поиска. Образец (англ. pattern), задающий правило поиска, по-русски также иногда называют «шаблоном», «маской», или на английский манер «паттерном». Информацию об их использовании вы можете найти в Интернет, например здесь - http://regexp.by.ru/, специфические регулярные выражения для почтового сервера postfix можно посмотреть здесь - http://www.postfix.org/regexp_table.5.html.

Сетевая маска или маска подсети
Посмотрите данную статью на википедии - http://ru.wikipedia.org/wiki/Маска_подсети

IP-адрес
Посмотрите данную статью на википедии - http://ru.wikipedia.org/wiki/IP-адрес

VLAN
Посмотрите данную статью на википедии - http://ru.wikipedia.org/wiki/VLAN

SSH
Посмотрите данную статью на википедии - http://ru.wikipedia.org/wiki/Ssh

6.5 Почтовый сервер

В Ideco ACP встроен полноценный почтовый сервер. Отправляемая и получаемая корреспондеция может проверяться на вирусы, спам и вредоносные программы несколькими фильтрами сразу. Поддерживаются все популярные протоколы и схемы работы почтового сервера в сети Интернет и в локальной сети предприятия. Эта инструкция поможет вам настроить полноценный почтовый сервер для отправки и приема почты из сети Интернет в несколько шагов:

1. Регистрация домена 269
2. Проверка работоспособности домена 275
3. Настройка почтового сервера на Ideco ACP 276
4. Настройка клиентских программ для получения и отправки почты 277
5. Рекомендации по защите сервера 281

Дополнительные варианты настройки работы почтового сервера.

- Синхронизация с удаленными серверами 281
- Смена хостинга 282
- Настройка почтового релея 283
- Корпоративная почта 284

ШАГ1: Настройки DNS-зон для работы с почтовыми серверами из Интернета

Для настройки полноценного почтового сервера на ACP Ideco 3 прежде всего вам нужно зарегистрировать доменное имя. Это можно сделать как у провайдера так и у регистратора (например nic.ru). Прежде чем зарегистрировать домен, убедитесь что на сервере Ideco ACP на внешнем интерфейсе настроен публичный (белый) IP-адрес. Если это не так, то обратитесь к провайдеру с просьбой выделить вам публичный IP-адрес.

В общем случае вы должны настроить доменную зону для публичного IP-адреса и почтовую (MX) запись к ней. Она представляет из себя текстовый файл, к которому дает доступ регистратор (провайдеры, как правило настраивают DNS-зоны сами). Если вы используете DNS-сервер BIND на Ideco ACP, и доменное имя (mydomain.ru) у вас зарегистрировано, то сами настройки зоны для вашего домена вы можете производить на вашем сервере, но обычно это не требуется.

Пример настройки прямой зоны на сайте регистратора nic.ru

При регистрации домена на nic.ru как минимум нужно купить его и зарегистрировать на сайте. Нужно различать покупку домена и его регистрацию. Регистрация домена это отдельная ***услуга*** на сервисе nic.ru. **Покупая** домен, вы

просто резервируете доменное имя цифробуквенного значения для себя и только вы сможете его использовать в будущем. При **регистрации** домена вы связываете доменное имя с публичным IP-адресом вашего сервера (в нашем случае это внешний IP-адрес Ideco ACP). После успешной регистрации домен начинает функционировать и DNS-сервера в Интернете ассоциируют имя вашего домена с IP-адресом сервера Ideco ACP.

Итак: Для работы домена необходимо заказать на сервисе nic.ru следующие услуги.

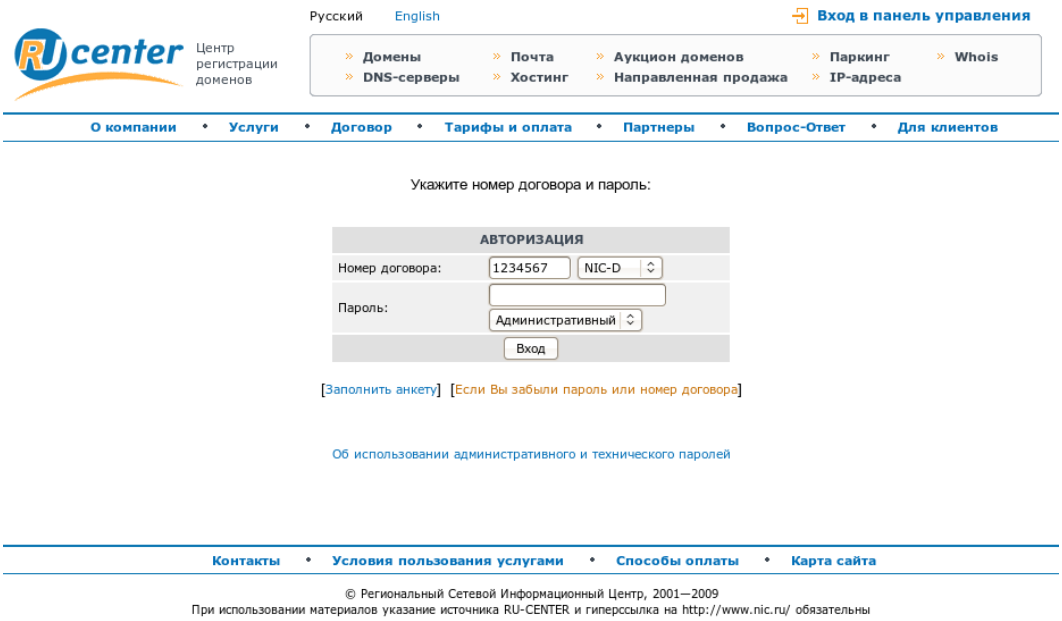
1. Регистрация домена. (Обязательная услуга при регистрации домена на nic.ru)
2. Primary-DNS (На nic.ru эта услуга дословно называется "primary standart"), можно настроить этот сервис на другом DNS-сервере, например на Ideco ACP.
3. Slave-DNS (На nic.ru эта услуга дословно называется "secondary"), можно настроить этот сервис на другом DNS-сервере, например на Ideco ACP.

Примечание: В соответствии с требованиями nic.ru для каждого домена услуги приобретаются отдельно. **Одна** из услуг primary-standart или secondary может быть реализована не на сервисе nic.ru, а например с помощью DNS-сервера BIND на Ideco ACP, другая при этом должна быть приобретена на nic.ru. Если вы реализуете оба сервиса (Primary и Secondary DNS) не на nic.ru, то имейте ввиду, что оба сервера дожны находиться в разных подсетях как минимум с префиксом подсети /24 и не забудьте перечислить их в настройке услуги **Регистрации домена**. Иначе **Регистрация домена** не будет настроена в соответствии с требованиями nic.ru и домен не будет успешно зарегистрирован в сети Интернет.

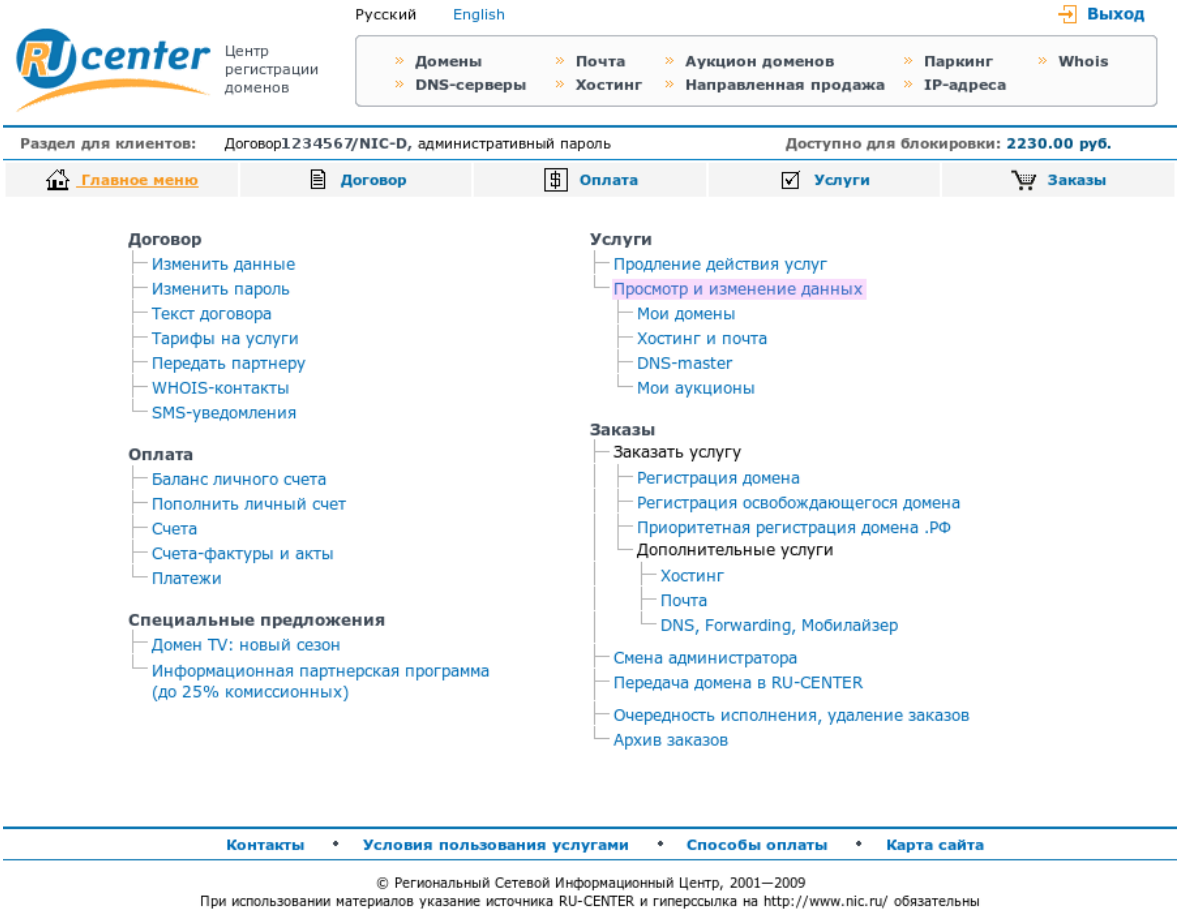
Для успешной **регистрации** домена на nic.ru нужно указать все DNS-сервера домена. В них входят и primary и slave DNS-сервера. Для серверов вида xxx.nic.ru IP-адрес указывать не надо. Для других DNS-серверов нужно указывать доменное имя DNS-сервера и его IP-адрес. Свои DNS-сервера нужно называть ns<номер>. mydomain.ru**.** Например: ns1.mydomain.ru**.**

Важно! IP-адреса всех DNS-серверов должны быть разными (разные подсети с маской как минимум с префиксом /24). Таким образом для одного домена нельзя одновременно размещать на одном сервере и primary и secondary.

Если услугу **Primary-DNS** вы приобретаете на nic.ru, то настройка и этой услуги осуществляется прямо на сайте регистратора через веб-интерфейс. При этом нужно будет перечислить все IP-адреса всех slave-DNS-серверов вашего домена в веб-интерфейсе. Настройка услуги primary standart заключается в редактировании файла первичной зоны для вашего домена непосредственно на сайте nic.ru. Nic.ru в этом случае будет являться первоисточником для вашего домена. В примере ниже показано как войти в личный кабинет на сайте nic.ru и перейти к настройкам услуги primary standart.



Выберите пункт изменение настроек (в примере выделено розовым цветом). Вы попадете на страницу где вы можете приобретать и редактировать услуги для вашего домена. Нас интересует услуга primary standart.

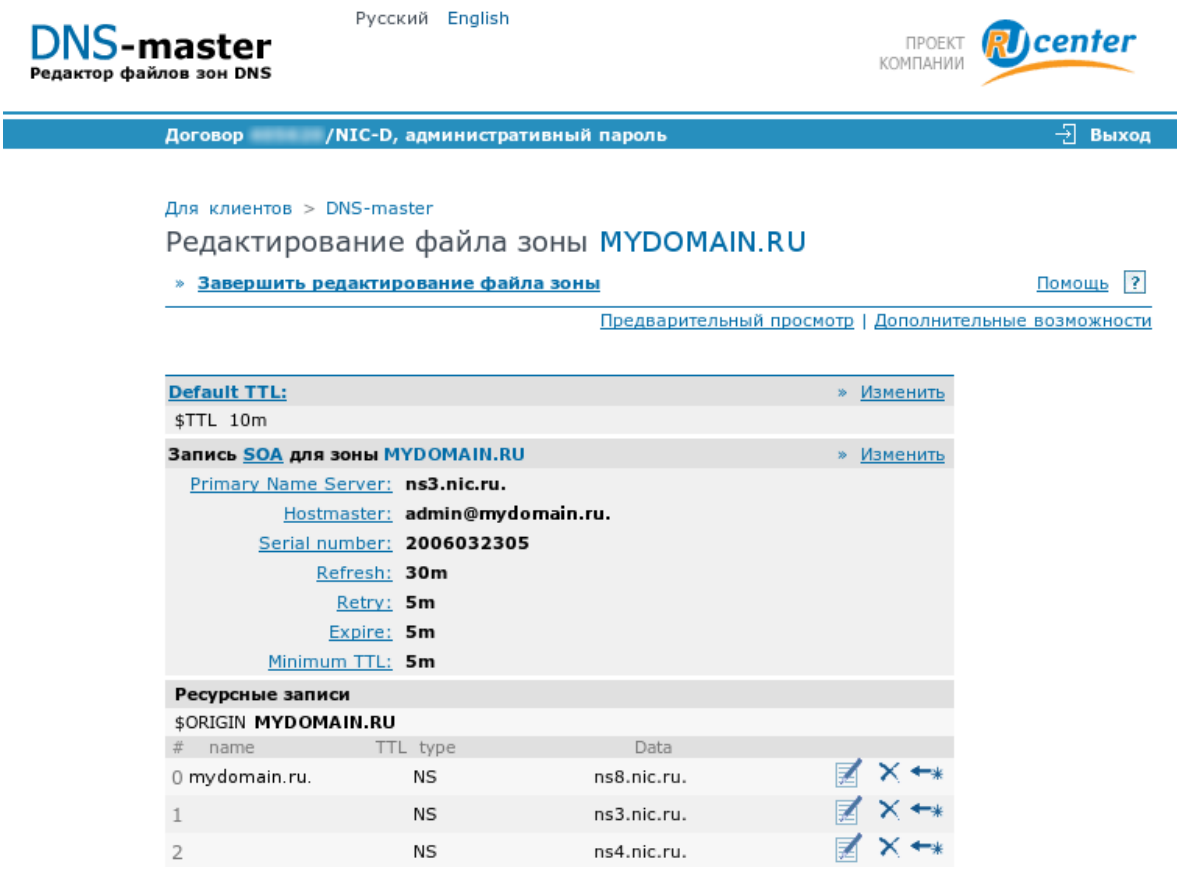


В результате увидите следующее окно:

1.	MYDOMAIN.RU Регистрация домена	Делегирован	DNS-серверы домена: ns1.mydomain.ru 11.11.11.11 ns3.nic.ru ns4.nic.ru ns8.nic.ru Изменить Индивидуальные контакты в Whois: не заданы Изменить	22.08.2010	история
2.	MYDOMAIN.RU Secondary	Зона размещена	IP-адрес primary: 22.22.22.22 Изменить Выключить услугу	23.08.2010	история
3.	MYDOMAIN.RU Primary-Standard	Настройка услуги произведена	Редактировать файл зоны IP-адреса secondary: 33.33.33.33, 44.44.44.44, 11.11.11.11 Изменить Выключить услугу	23.08.2010	история

Редактирование зоны осуществляется на одной странице и сводится к редактированию отдельных строк файла первичной зоны вашего домена. Фрагмент

того как это выглядит на сайте nic.ru представлен ниже:



Типичный файл прямой DNS-зоны для домена вымышленного домена mydomain.ru представлен ниже с пояснениями.

```
1  mydomain.ru 600  IN   SOA  ns3.nic.ru.    admin.mydomain.ru. (
2              2006032305     ; serial
3              1800 ; refresh
4              300  ; retry
5              300  ; expire
6              300  ; minimum ttl
7              )
8          NS   ns8.nic.ru.
9          NS   ns3.nic.ru.
10         NS   ns1.mydomain.ru.
11         TXT   "v=spf1 a mx -all exp=spam.mydomain.ru."
12         A    1.2.3.4
13 ns1     A    5.6.7.8
14 smtp    A    9.10.11.12
```

```
15        MX   10 smtp.mydomain.ru.
16 spam   TXT   "MTA%{c}(%{r}):helo=%{h},sender=%{i},sender=%{s}."
17 www    CNAME     site.mydomain.ru.
18 site   A    1.2.3.4
```

- Имейте ввиду что в соответствии со стандартом RFC-1034 в названии доменного имени можно использовать только цифробуквенные выражения и символ "-" (то есть: **[a-z],[A-Z],[-]**) все остальные символы, включая "_" использовать запрещено. Так же имейте ввиду что система не различает регистр букв.
- Запись типа "**A**" (прямая запись) или запись адреса связывает имя хоста с адресом IP. Например для зоны mydomain.ru: `smtp A 9.10.11.12`
- Запись типа **MX** (запись определения почтового посредника) определяет хост, который занимается непосредственно приемом и отправкой почты и **должна ссылаться на доменное имя почтового сервера (на A запись), а не на IP-адрес.** Так же следует учитывать что MX запись как правило не совпадает с именем обслуживаемого домена. Таким образом для домена вида mydomain.ru MX запись может ссылаться на smtp.mydomain.ru, mail.mydomain.ru или mx10. mydomain.ru. Первый вариант предпочтительней, т.к. некоторые владельцы почтовых серверов настраивают их таким образом, что блокируется прием всех почтовых писем с почтовых серверов, MX запись которых не имеет вида "smtp. somedomain.com".
- В файле зоны, в записи SOA должно содержаться доменное имя primary-DNS. (ns3.nic.ru).
- В NS-записях для вашего домена, а их должно быть несколько, должны быть перечислены все DNS-сервера.
- При указании доменных имен в записях типа MX, CNAME, NS и других необходимо указывать **полное доменное имя и завершать его точкой**. Например: «smtp. mydomain.ru.». В простейшем случае ваш шлюз и будет являться почтовым сервером, то есть A запись для домена будет ссылаться на публичный IP-адрес шлюза (Ideco ACP), еще как минимум одна A-запись с именем хоста почтового сервера (smtp) будет ссылаться на этот же IP-адрес и MX запись будет ссылаться на A запись хоста почтового сервера.
- MX записей может быть несколько, например если у вас настроено несколько smtp серверов. В таком случае приоритет для работы с этими серверами извне будет устанавливаться числом после слова MX. Чем больше число, тем меньше приоритет для сервера. Обычно числа увеличиваются кратно 10, начиная с 10. В нашем примере мы имеем одну MX запись, тем не менее приоритет должен быть, и он уставновлен в стандартное значение 10. В других случаях могла быть еще запись MX или даже несколько записей. Пример нескольких записей показан ниже.Заметьте, у вас два почтовых сервера, для каждого из них есть A запись и MX запись, ссылающаяся на A запись. Для удобства имя серверов отображает их приоритетность.

```
...
14 smtp10 A    9.10.11.12
15 smtp30 A    13.14.15.16
16        MX   10 smtp10.mydomain.ru.
17        MX   30 smtp30.mydomain.ru.
...
```

- Файл прямой зоны, приведенный в примере, учитывает все вышеприведенные требования и рекомендации. В этом файле 1.2.3.4 - это публичный IP-адрес вашего сервера Ideco ACP, 5.6.7.8 - IP-адрес ДНС-сервера, обслуживающего вашу зону, 9.10.11.12 - IP-адрес непосредственно почтового сервера. Все три IP-адреса могут совпадать и быть публичным адресом Ideco ACP. Измените этот файл, учитывая ваши данные. Остальные записи в файле зоны, такие как NS, SOA изменять не нужно. Перед изменением записей CNAME, TXT и др. посоветуйтесь со специалистом.

Для улучшения прохождения ваших писем через сторонние анти-спам системы желательно добавить SPF-записи. Это записи с типом TXT, имеющие специальный формат. Указывать необходимо с точностью до символа.

```
TXT "v=spf1 a mx -all exp=spam.mydomain.ru."
```

Эта запись означает что почту с отправителем `...@mydomain.ru` разрешено отправлять только с серверов, чьи адреса указаны в A либо MX записях для данного домена — т.е. Для нашего примера — это smtp.mydomain.ru и mydomain.ru. Если сторонний сервер попытается отправить спам от вашего имени, то другие сервера не примут такое письмо при наличии такой записи в DNS. Необходимо создать запись с именем spam.mydomain.ru и типом TXT в которой нужно указать причину по которой письмо не будет принято сторонними серверами, как в примере:

```
spam TXT   "MTA%{c}(%{r}):helo=%{h},sender=%{i},sender=%{s}."
```

- **Если Slave-DNS планируется приобретать на nic.ru, то в настройках услуги (на nic.ru она называется "secondary") через веб-интерфейс необходимо указать IP-адрес primary-сервера.**

- Так же необходима обратная запись или запись типа PTR. Эта запись должна быть прописана в файле обратной зоны, который не представлен в нашем примере, т.к. создание обратной зоны это исключительно прерогатива провайдера (а не регистратора). Обратитесь к вашему провайдеру с просьбой прописать обратную запись для вашего IP-адреса, ссылающуюся на вашу MX запись (а не на доменное имя).

Более подробную информацию по настройкам DNS-зон вы можете найти здесь 286.

ШАГ2: Проверка настроек.

Проверить правильность настроек можно командами nslookup (windows) или host (unix/linux). Для nslookup команда проверки MX записи после применения настроек на серверах регистратора и провайдера будет выглядеть так:

```
nslookup -type=mx mydomain.ru
```

в ответ вы должны получить вывод примерно следующего содержания:

```
mydomain.ru MX preference = 10, mail exchanger = smtp10.mydomain.ru
mydomain.ru MX preference = 30, mail exchanger = smtp30.mydomain.ru
smtp10.mydomain.ru internet address = 9.10.11.12
smtp30.mydomain.ru internet address =  13.14.15.16
```

Для команды host команда проверки будет выглядеть так:

```
host -t mx mydomain.ru
```

в ответ вы должны получить ответ вида:

```
mydomain.ru mail is handled by 10 smtp10.mydomain.ru
mydomain.ru mail is handled by 30 smtp30.mydomain.ru
```

Для проверки PTR записи в Windows можно так же использовать nslookup, команда будет следующая:

```
nslookup 9.10.11.12
```

Ответ будет выглядеть следующим образом:

```
Name:    smtp10.mydomain.ru
Address:  9.10.11.12
```

Для проверки PTR записи в Linux/Unix лучше использовать команду dig. Команда для проверки будет выглядеть так:

```
dig PTR 12.11.10.9.in-addr.arpa.
```

в ответ вы можете получить довольно обьемный вывод, вам нужно найти такой блок вывода:

```
;; ANSWER SECTION
12.11.10.9.in-addr.arpa.     81461     IN PTR    smtp10.mydomain.ru
```

как вы видите после "IN PTR"в секции ответа DNS-сервера вы видите доменное имя вашего почтового сервера, полученое из IP-адреса, записанного в системе записи домена in-addr.arpa. Для проверки PTR записи - каждая запись проверяется отдельно.

ШАГ3:Настройка почтового сервера на ACP Ideco для работы в Интернет в соответствии с данными, полученными от регистратора (провайдера)

К моменту настройки почтового сервера все зоны должны быть настроены, DNS-сервера должны применить внесенные изменения касательно ваших зон, записи должны быть вами проверены. При настройке почтового сервера для работы в Интернет важны следующие пункты в локальном меню.

[X] Включить встроенную почту (POP3) - для доставки писем конечным пользователям в сети вашего предприятия по протоколу POP3

[X] Разрешить доступ из Интернет (POP3S) - для возможности доставки почты пользователям, находящимся не в сети предприятия (например для получения почты из дома, из другого офиса) по протоколу POP3 с шифрованием

[X] Включить встроенную почту (IMAP) - для доставки писем конечным пользователям в сети вашего предприятия по протоколу IMAP

[X] Разрешить доступ из Интернет (IMAPS) - для возможности доставки почты пользователям, находящимся не в сети предприятия (например для получения почты из дома, из другого офиса) по протоколу IMAP с шифрованием

Следующие три параметра задействуют Веб-почту на соответствующих адресах. Доступ к Веб-почте можно получить только по протоколу с шифрованием - SSL.

[X] Включить Веб-почту на защищенном адресе

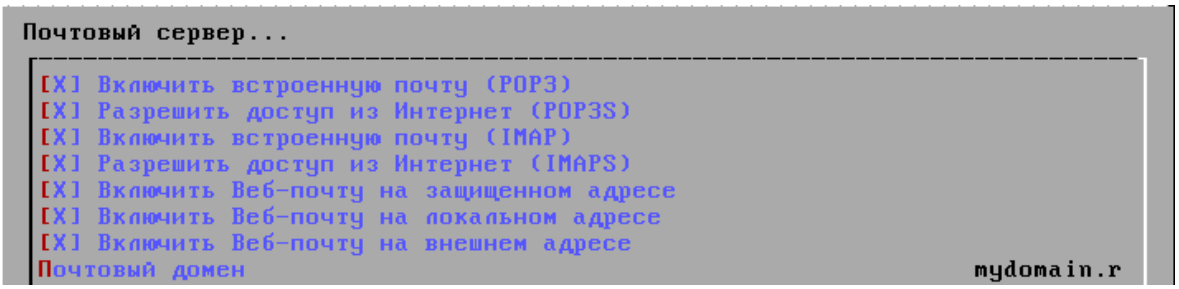
[X] Включить Веб-почту на локальном адресе

[X] Включить Веб-почту на внешнем адресе

В качестве почтового домена вы должны указать доменное имя, которое будет писаться в названии почтовых ящиков после "@". В нашем случае это mydomain.ru.

Из перечисленных выше, обязательными параметрами при настройке почты для работы с Интернет являются:

- Включение отдачи писем пользователям в локальной сети по одному из протоколов (POP3 и/или IMAP)
- Включение отдачи писем пользователям во внешних сетях по одному из протоколов (POP3S и/или IMAPS)
- Почтовый домен



После всех настроек сервер необходимо перезагрузить.

ШАГ4: Настройка клиентских программ для получения почты с сервера Ideco ACP (SASL,POP3S)

При настройке клиентских машин для получения почты возможны следующие варианты:

- **Доставка почты в локальной сети предприятия (по протоколу POP3/IMAP)**

На пользовательских машинах вам нужно установить какой либо почтовый клиент (Thunderbird, Microsoft Outlook, The Bat), либо использовать стандартный почтовый клиент Outlook Express, которым укомплектованы все версии Windows.

В зависимости от того, какой протокол для доставки почты вы выбрали при настройке сервера (POP3/IMAP), настраиваете ваш почтовый клиент на использование того или иного протокола (или обоих сразу).

В случае авторизации по VPN в качестве сервера исходящей и входящей почты нужно указать **защищенный адрес Ideco ACP** (по умолчанию 10.128.0.0). Если клиент использует авторизацию по IP, IP+ Ideco Agent или Web, то необходимо указать **локальный адрес Ideco ACP**.

При использовании нашего продукта в качестве почтового сервера в качестве логина для учетной записи почты необходимо указывать часть имени почтового адреса до символа "@" (левую половину почтового адреса).

- **Доставка почты клиентам в локальной сети и клиентам, подключающимся к локальной сети извне, используя VPN подключение к Ideco ACP (POP3/ IMAP).**

При такой схеме принципиальных отличий нет, так как вы подключаетесь к локальной сети предприятия по защищенному каналу и организовывать защищенное соединение с почтовым сервером по протоколам POP3S и IMAPS не нужно, в качестве серверов исходящей и входящей почты будет использоваться защищённый адрес (по умолчанию 10.128.0.0).

- **Работа с почтовым сервером из сети Интернет через защищенное соединение. (POP3S, SASL SMTP/TLS)**

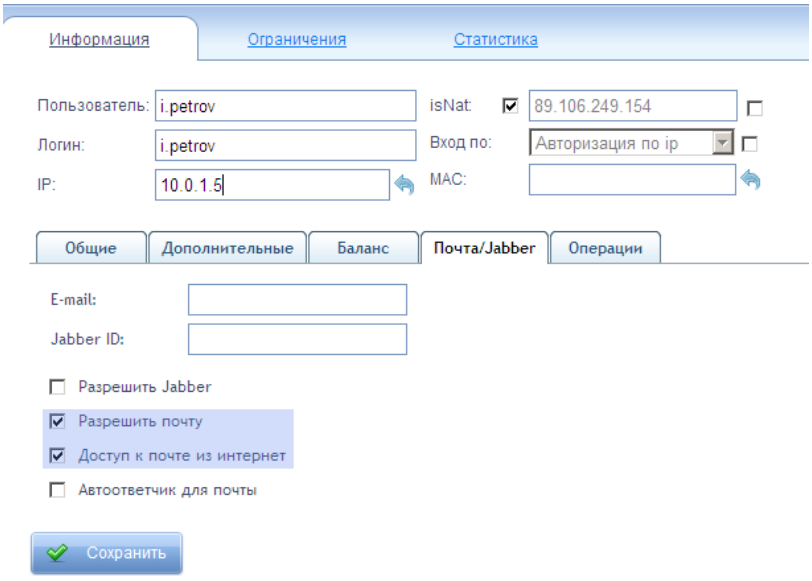
На сервере Ideco ACP в локальном меню включаем два пункта:

"Конфигурирование сервера -> Почтовый сервер -> Расширенные настройки почты":

[X] Включить поддержку SASL для аутентификации по SMTP

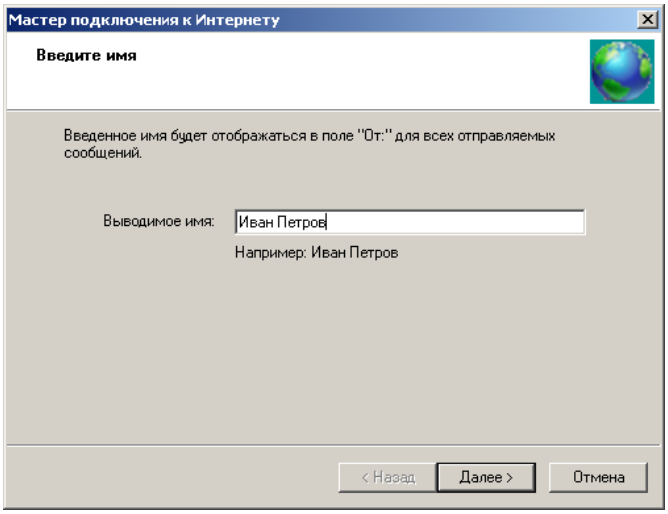
[X] Включить поддержку TLS для SMTP

У пользователя, почтовый ящик которого должен быть доступен из Интернета, включаем использование почты и разрешаем доступ к почте из Интернет. Как видите поле "E-mail" заполнять не нужно. Логин для почтового ящика автоматически будет приравнен к логину пользователя, но при желании можно указать уникальный e-mail для пользователя:

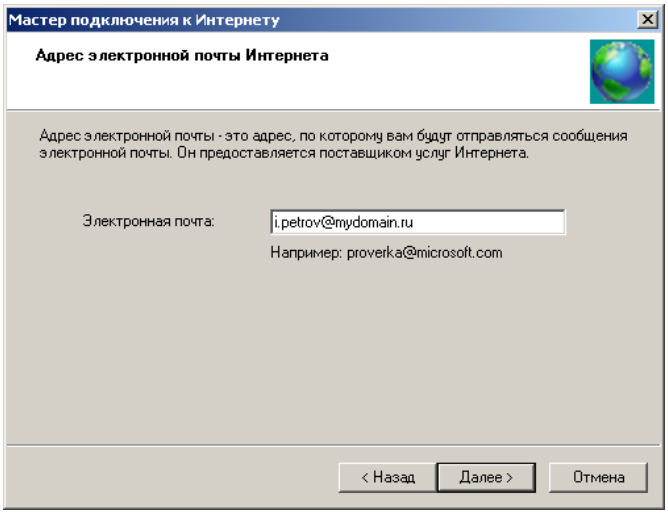


После этого, на компьютере клиента настроим учетную запись Outlook Express для получения и отправки почты по (POP3S, SASL/TLS SMTP):

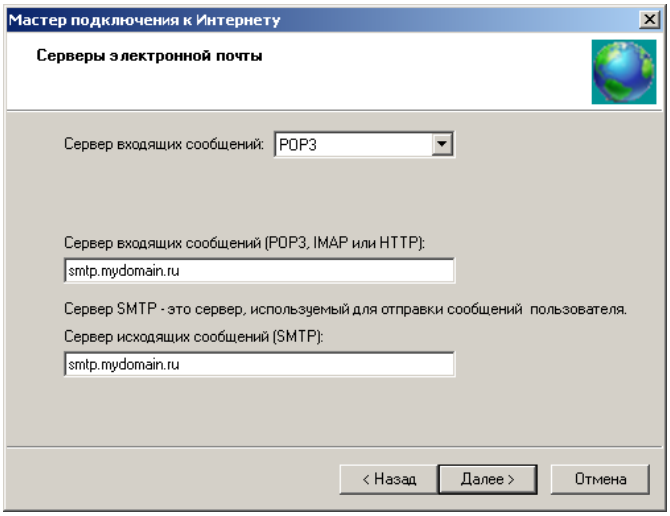
Создаем новую учетную запись:



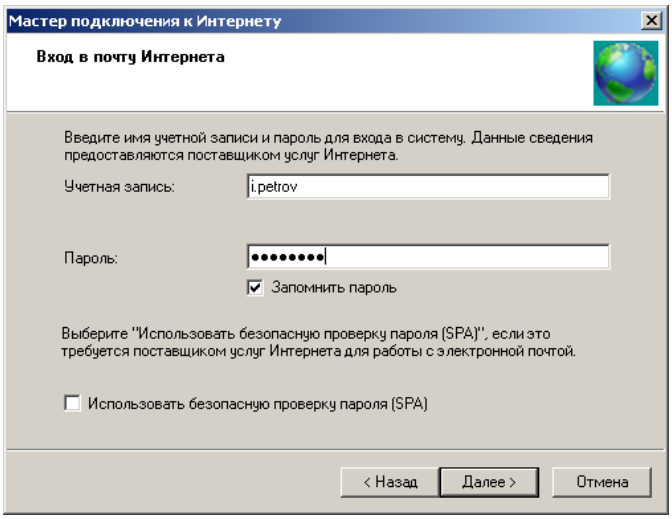
Вписываем почтовый ящик клиента.



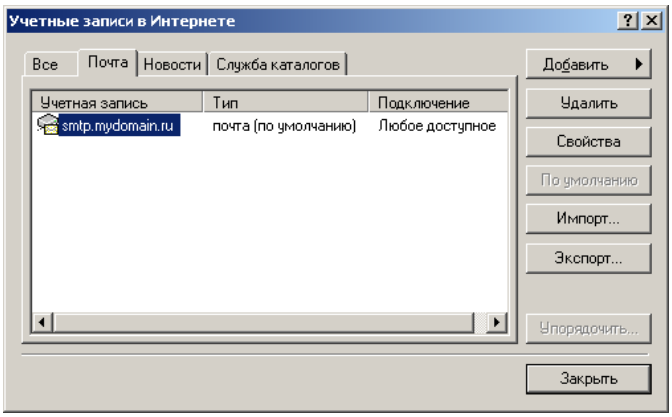
Выбираем протокол, по которому сервер будет нам отдавать почту. Формально это POP3, шифрование включим позже. Сервер для отправки и приема почте в нашем случае - Ideco ACP. Указываем его доменное имя, которое к этому времени настроено и правильно распознается DNS-серверами в Интернете (либо можно указать внешний IP адрес сервера).



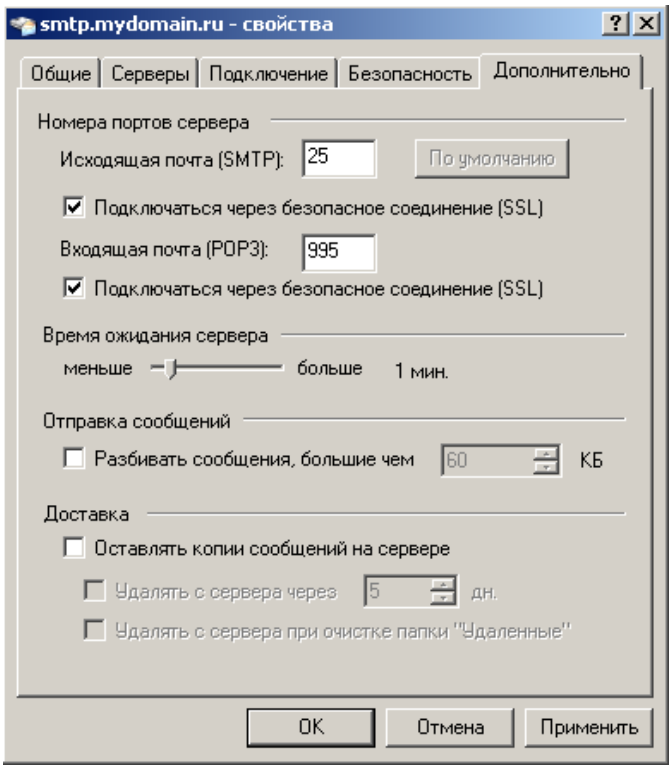
В качестве логина к почтовому ящику указываем **часть имени почтового ящика до символа "@"** . Указываем пароль. Логин и пароль от почтового ящика совпадают с логином и паролем самого пользователя в БД Ideco ACP.



В конце настройки учетной записи у вас должна появиться ваша новая учетная запись в списке учетных записей. Выбираем ее и нажимаем на кнопку "**Свойства**"



В открывшемся окне переходим на вкладку "**Дополнительно**". Включаем оба пункта "Подключаться через безопасное соединение (SSL)" и меняем порт обращения к POP3-серверу на 995.



После этого ваша почтовая учетная запись готова к использованию. Вы можете отправлять и принимать почту в любом месте где есть доступ к сети Интернет по шифрованному соединению с проверкой пользователя и пароля на сервере Ideco ACP.

ШАГ5: Обеспечение безопасной работы сервера в Интернет.

В комплекте идет несколько мощных средств защиты от спама, вирусов и другого вредоносного кода. Прежде всего желательно включить в настройках почтового сервера предварительные спам-фильтры. Так же в комплекте поставки идет бесплатный антивирус ClamAV. Эти компоненты могут использоваться вне зависимости от типа купленной лицензии.

В дополнении к этим мерам вы можете использовать Антивирус и Антиспам Касперского, Dr. Web. По вопросам приобретения этих продуктов обратитесь, пожалуйста, в отдел продаж.

Теперь ваш почтовый сервер можно считать настроенным и готовым к использованию. После применения всех настроек не забудьте перезагрузить сервер.

Далее описаны некоторые специфичные варианты настройки почтового сервера. Ознакомьтесь с ними при необходимости. По всем вопросам настройки обращайтесь, пожалуйста, в отдел технической поддержки.

Синхронизация с удаленным почтовым сервером в Интернете с помощью

Fetchmail.

Для того чтобы поместить почту с удаленного почтового сервера на сервер Ideco ACP используем сборщик почты fetchmal настройка которого доступна в локальном меню. "Конфигурирование сервера -> Почтовый сервер -> Расширенные настройки почты -> Загрузка почты с удалённых серверов (fetchmail)". При выборе этого пункта вам становится доступно редактирование правил для работы fetchmail'a. Для каждого почтового ящика создается отдельное правило.

Предположим:

- Почтовый домен в Интернете на котором у вас зарегистрирован почтовый ящик: maildomain.ru, его IP-адрес: 10.20.30.40
- Почтовый ящик, зарегистрированый на этом сервере имеет логин: petrov.
- Пароль от этого ящика: petrovpasswd
- Почтовый домен Ideco ACP: mydomain.ru
- Почта должна быть направлена в ящик пользователя i.petrov@mydomain.ru

Тогда правило будет выглядеть так:

```
10.20.30.40:pop3 aka maildomain.ru petrov petrovpasswd i.petrov@mydomain.ru
```

Если нужно не удалять загруженные письма с удалённого почтового сервера нужно использовать ключ Keep:

```
10.20.30.40:pop3 aka maildomain.ru petrov petrovpasswd i.petrov@mydomain.ru keep
```

После добавления всех правил и сохранения конфигурации правила начинают действовать незамедлительно и начнется сбор почты с учетных записей удаленного сервера и сортировка писем по почтовым ящикам на сервере IdecoACP.

Отказ от старого хостинга почты и переход на использование нового сервера настроенного на Ideco ACP

Тут может быть несколько вариантов.

Первый вариант. Самый распространенный. Когда ваш настоящий хостер: maildomain.ru, а вы только что настроили полноценный почтовый сервер на IdecoACP.

Рассмотрим случай с использованием fetchmail, описанный выше. Если вы хотите перестать пользоваться почтой у хостера (в примере maildomain.ru), то сразу после сбора почты с вашего старого почтового домена делаете перенаправление каждой учетной записи на новый почтовый домен, настроеннный на сервере Ideco ACP. Обычно эта функция доступна через web-интерфейс в свойствах каждого конкретного почтового ящика. Перенаправляем письма с текущего ящика у хостера на ящик того же пользователя в новом почтовом домене. То есть в веб-интерфейсе хостера в свойствах ящика petrov@maildomain.ru выбираете функцию перенаправления (редирект или forward) на i.petrov@mydomain.ru. Таким образом

вся приходящая на этот ящик почта будет перенаправляться на ящик в вашем почтовом домене на почтовый сервер Ideco ACP. За более подробной информации по настройке перенаправления обратитесь к вашему хостеру. При такой схеме не нужно удалять ящики у старого хостера как можно дольше.

При этом:

- Старые почтовые ящики у хостера продолжают действовать. Клиенты знают о них и отправляют почту на них, но вся почта автоматически перенаправляется на ваш почтовый сервер на IdecoACP. Таким образом вы не теряете старых клиентов.
- Вы можете везде публиковать ваши новые почтовые ящики из домена mydomain.ru и пользоваться ими. Все ваши новые клиенты будут знать только о новых ящиках.
- Все происходит прозрачно для пользователей вашей компании, они просто начинают пользоваться ящиками из домена mydomain.ru, в то же время корреспонденция от старых клиентов тоже приходит им, но пользователя могут не следить и попросту "забыть" о своих старых учетных записях у хостера.
- Вся корреспонденция оставшаяся находившаяся у хостера переписывается на ваш новый почтовый домен и пользователям доступна их старая переписка.

Второй вариант. Вы когда то зарегистрировали домен mydomain.ru у хостера и почтовый сервер тоже при этом находился у хостера. Таким образом MX запись ссылалась на почтовый сервер, находящийся у хостера. Вы хотите сохранить домен, но почтовый сервер настроить на Ideco ACP. В таком случае вам нужно поменять MX запись так, чтобы она ссылалась на публичный адрес непосредственно на Ideco ACP. **MX запись должна ссылаться на A запись, которая в свою очередь будет ссылается на публичный адрес Ideco ACP в Интернете.** У хостера, обслуживающего ваш домен надо завести запись типа A. И настроить MX запись на эту A запись. Например:

```
...
smtp      A    11.22.33.44
          MX 10 smtp.hostingdomain.ru.
...
```

Где 11.22.33.44 это публичный IP-адрес Ideco ACP. hostingdomain.ru - доменное имя, для которой настроена DNS-зона в которой вы и будете вносить изменения.

Так как вариантов настройки в этом случае может быть много, то указать конкретные примеры будет сложно. Общий смысл перехода от использования одного почтового сервера к другому, не меняя регистратора и доменной зоны - это **ассоциирование MX записи у регистратора с вашим новым почтовым сервером на IdecoACP**. Вам лучше согласовать этот вопрос с держателем вашей зоны.

Настройка почтового релея для сервера в локальной сети

Если Ideco ACP имеет внешний IP-адрес и на него зарегистрирован домен и настроены необходимые записи у регистратора и провайдера, но вы хотите чтобы отправкой и доставкой почты занимался другой сервер (к примеру заранее настроенная машина в локальной сети), то Ideco ACP может ретранслировать всю

входящую почту на эту машину.

Для настройки почтового релея обратимся к пункту локального меню "Конфигурирование сервера - Почтовый сервер - Расширенные настройки почты - Relay-домены"
В этом пункте нужно добавить запись вида: mydomain.ru 10.20.30.40 , где mydomain.ru - ваш почтовый домен, зарегистрированный в Интернете на публичный адрес Ideco ACP.
10.20.30.40 - адрес вашего почтового сервера в локальной сети.

Принципиально, чтобы почтовый домен Ideco отличался от Relay-домена. (в поле Почтовый домен в настройках почтового сервера в локальном меню можно прописать вымышленный домен не совпадающий с зарегистрированным)

При такой схеме IdecoACP будет пропускать проходящую через себя почту прямо на почтовый сервер в локальной сети.

Важно! Релей не должен быть открыт всем (внешним сетям Интернет), что позволяет недоброжелателям отправлять письма через ваш сервер, иначе ваш сервер моментально попадет в спам-листы и перестанет работать. Для этого достаточно строго следовать рекомендациям, приведённым ранее. Попутно письма могут проверяться на вирусы и спам, просто включите соответствующие сервисы.

Необходимые настройки для запуска почтового сервера только для работы в локальной сети предприятия (корпоративная переписка).

Настройки на сервере. В локальном меню или в веб-интерфейсе в разделе Почтовый Сервер.

- Включить встроенную почту (POP3 или IMAP)
- Указать вымышленный почтовый домен. Например vpn.mydomain.ru
- По желанию включить вебпочту на защищенном и/или локальном адресе Ideco ACP.
- По желанию для удобства сортировки статистики пользователей изменить поле "IP-адрес почты для пользователей". Адрес будет создан виртуально на шлюзе.

Настройки касающиеся клиента:

- В веб-интерфейсе, в настройках аккаунта пользователя включите галочку "Разрешить почту"
- По желанию укажите имя почтового аккаунта отличное от логина пользователя. Например sequrity@vpn.mydomain.ru. Именно с доменной частью после символа "@".
- Желательно при первом входе в аккаунт пользоваться почтовыми клиентами на конечном ПК. Например Thunderbird, Outlook, The Bat, Evolution, а не веб-почтой.

6.6 DNS сервер

В большинстве случаев для работы сервера DNS на Ideco достаточно включение кэширующего DNS 156, который работает по умолчанию. В случае если вы приобрели доменное имя у регистратора (к примеру на www.nic.ru) и хотите в качестве полноценного сервера DNS использовать Ideco , то воспользуйтесь данной инструкцией.

Для работы системы доменных имен внутри вашего домена необходимо иметь минимум один первичный сервер DNS (может называться как Primary или Master) и один вторичный сервер DNS (Secondary, или Slave). Оба этих сервера можно заказать на nic.ru, либо в качестве одного из них использовать Ideco ICS. Регистрация сервера DNS для доменного имени называется делегированием. Без делегирования доменное имя само по себе работать не будет.

- **Использование IDECO ICS в качестве первичного сервера DNS.**
  Это означает что сервер IDECO будет первоисточником информации о DNS-зоне.
  1. Для этого необходимо иметь постоянный внешний реальный IP-адрес.
  2. Меню -> конфигурирование сервера -> днс-сервер -> включить полнофункциональный DNS-сервер(BIND)
  3. Редактировать Master-зоны (Primary)
  4. Добавить.
  5. Ввести имя зоны
  6. Будет готов шаблон для редактирования.
  7. Добавить или поменять записи. (см. «Правила формирования записей доменных зон 286»)
  8. Меню -> конфигурирование сервера -> днс-сервер -> Разрешенные для передачи зоны...
  9. Указать запись вида <имя зоны> <разрешенный адрес или сеть> <разрешенный адрес или сеть> ...
  Необходимо указать как минимум IP-адреса всех вторичных DNS серверов для этой зоны

- **Использование АСР Ideco в качестве вторичного сервера DNS.**
  Это означает что сервер IDECO будет резервным сервером для определенной зоны.
  И в случае недоступности первичного будет выполнять основные его функции. Даже если первичный сервер доступен, запросы на разрешение имен будут поступать равномерно ко всем вторичным и первичному серверу DNS.
  1. Для этого необходимо иметь постоянный внешний реальный IP-адрес.
  2. Меню -> конфигурирование сервера -> днс-сервер -> включить полнофункциональный сервер DNS (BIND)
  3. Редактировать Slave-зоны (Secondary)
  4. Добавить.
  5. Ввести имя зоны и через пробел IP-адрес первичного сервера DNS для этой зоны. Дополнительно можно указать IP-адреса вторичных серверов кроме своего собственного.
  6. Меню -> конфигурирование сервера -> днс-сервер -> Разрешенные для передачи зоны...

7. Указать запись вида <имя зоны> <разрешенный адрес или сеть> <разрешенный адрес или сеть> ...
Необходимо указать как минимум IP-адреса всех вторичных серверов DNS для этой зоны кроме своего собственного.

6.7 Правила формирования записей доменных зон

Зоны бывают **прямые** и **обратные**.
Прямые зоны предназначены для преобразования доменного имени в IP-адрес. Имя прямой зоны имеет привычный вид, например, "myorg.ru.".
Обратные зоны — для преобразования IP-адреса в доменное имя.
Обратные зоны начинаются тремя цифрами IP-адреса в зеркальном порядке и заканчиваются на "in-addr.arpa.". Например, "100.168.192.in-addr.arpa." — это пример зоны для преобразования адресов вида "192.168.100.*".

При формировании зоны большое значение имеет символ точки в конце любого имени — нужно быть с этим аккуратнее!

Одна строка означает одну запись.Порядок записей в общем случае не важен. Но рекомендуется делать первой запись типа SOA, далее записи типа NS для самой зоны, затем прочие записи для самой зоны, затем всё остальное.
Символ @ автоматически заменяется на имя зоны.

Рассмотрим примеры для зоны "myorg.ru".
Первое поле любой записи означает то к чему она относится.
например, @ - означает запись для самой зоны. "name" означает "name.myorg.ru.".
Если имя не заканчивается точкой, то к нему справа пристыковывается через точку имя зоны.
Использовать имена, не входящие в зону, например, "name2.myorg2.ru." нельзя.
В имени поля можно использовать только латинские буквы (регистр не важен) цифры, дефис, точку и символ @ который преобразуется в имя самой зоны.
Другие символы использовать нельзя!
Если имя записи не указано (строка начинается с пробела), то будет браться имя предыдущей записи - в этом случае порядок записей важен. будьте внимательны.

Второе поле каждой записи — тип.
Существует несколько общеупотребимых типов:
SOA - означает информацию о зоне заданной указанным именем.
NS - указывает какие DNS сервера отвечают за указанное имя
MX - указывает на какой сервер должна идти электронная почта если после символа @ в почтовом адресе будет указанное имя.
A - указывает какой IP-адрес соответствует указанному имени
CNAME - создает псевдоним для другой записи.
PTR - указывает соответствие между IP-адресом и доменным именем.
В прямой зоне можно указывать все вышеперечисленные записи кроме PTR. В обратной — только SOA, NS и PTR

Запись SOA
Формат:

@ SOA <ИМЯ PRIMARY DNS> <ПОЧТА> (служебные поля)
Описывает служебную информацию для конфигурируемой зоны.
Можно делать только одну запись типа SOA. В поле <ИМЯ PRIMARY DNS> нужно указать полное доменное имя первичного DNS.
В поле почта нужно указать адрес электронной почты администратора этой зоны. Символ @ в адресе почты нужно заменить на точку. Нельзя использовать почтовый адрес в котором перед @ есть точки.
Подробности о служебных полях можете прочитать в RFC Обычно их менять не требуется.

Запись NS
формат: **<ИМЯ> NS <ИМЯ СЕРВЕРА>**
Указывает какие DNS сервера отвечают за указанное <ИМЯ>. Здесь необходимо указывать первичные и вторичные DNS сервера.
Если серверов несколько, то необходимо несколько раз вписать запись типа NS. Порядок не важен. В качестве <ИМЯ СЕРВЕРА> нельзя указывать IP-адрес. Нужно указывать полное имя с точкой на конце. Принято использовать имена вида "ns1. myorg.ru.", "ns2.myorg.ru." и так далее.
Необходимо следить чтобы для указанного <ИМЯ СЕРВЕРА> не было записи типа CNAME и чтобы обазательно была запись типа A.
Это имя может не находиться в конфигурируемой зоне. т.е. абсолютно нормально, если записи выглядят так:

```
@ NS ns1.myorg.ru.
@ NS ns2.myorg.ru.
@ NS ns8.nic.ru.
```

Запись A
Формат: **<ИМЯ> A <IP-адрес>**
Указывает, какой IP-адрес соответствует данному имени. IP-адрес может быть совершенно произвольным.
Есть возможность указать несколько записей типа A для одного и того же имени. В этом случае, при преобразовании имени в IP-адрес будет выбрана случайная запись.
IP-адрес можно указывать ТОЛЬКО в записях типа A и ни в каких других. Нарушение этого правила приведет к тому что в некоторых случаях будет работать, а в некоторых нет.
Желательно чтобы в обратной зоне для <IP-адрес> существовала PTR запись, ссылающаяся на <ИМЯ>.
Пример:

```
qwe@ A 1.2.3.3
havemirrors A 1.2.3.4
havemirrors A 1.2.3.5
```

Запись MX
Формат: **<ИМЯ> MX <приоритет> <ИМЯ ПОЧТОВОГО СЕРВЕРА>**
Указывает, на какие почтовые сервер необходимо отправить почту если справа от @ в адресе почты будет указано полное имя **<ИМЯ>**.
В качестве **<ИМЯ ПОЧТОВОГО СЕРВЕРА>** нельзя использовать IP-адрес. Вместо этого, необходимо писать полное имя с точкой в конце.

Необходимо следить чтобы для указанного **<ИМЯ ПОЧТОВОГО СЕРВЕРА>** не было записи типа CNAME и чтобы обязательно была запись типа A.
Если почтовых серверов несколько, то имеет смысл указать необязательное поле **<приоритет>**. В этом поле должно быть число кратное 10, больше нуля и меньше 250.

Если есть несколько почтовых серверов, которые должны принимать почту, то такие сервера нужно указывать с помощью нескольких записей типа MX. При этом сам конечный сервер, который будет хранить почту должен быть указан с минимальным значением поля **<приоритет>**.
Пример:

```
@ MX 10 mx10.myorg.ru.
@ MX 20 mx20.myorg.ru.
@ MX 50 some-relay.ru.
MX10 A 1.2.3.4
MX20 A 1.2.3.5
```

Если необходимо чтобы ваш сервер принимал почту предназначенную для поддомена, а затем передавал ее, скажем, на сервер внутри локальной сети, то создайте запись:

Code:

```
name2 MX 10 mx10.myorg.ru
```

Затем, в настройках этого почтового сервера настройте параметр "relay-домены".

Запись CNAME
Синтаксис:
<ИМЯ> CNAME <ПОЛНОЕ ИМЯ>
Означает, что при просмотре имени <ИМЯ> нужно обратиться к имени <ПОЛНОЕ ИМЯ>.
В поле <ПОЛНОЕ ИМЯ> нельзя указывать IP-адрес и это имя должно заканчиваться точкой.
Нельзя использовать несколько CNAME для одного имени. <ПОЛНОЕ ИМЯ> не должно иметь CNAME записи.
Не рекомендуется использовать другие виды записей для одного имени совместно с CNAME. Особено это касается записи типа A.
Не рекомендуется в качестве <ПОЛНОЕ ИМЯ> указывать доменное имя не лежащее в конфигурируемой зоне.
Пример:

```
website A 1.2.3.6
www CNAME site.myorg.ru.
ftp CNAME site.myorg.ru.
Другой пример:
Code:
```

```
@ A 1.2.3.7
www CNAME @
ftp CNAME @
```

Запись PTR
Формат:
<ЦИФРА> PTR <ДОМЕННОЕ ИМЯ>
Запись этого типа может использовать только в обратной зоне.
Например, для того чтобы сделать обратное преобразование адреса 192.168.100.123, необходима зона "100.168.192.in-addr.arpa."(первые 3 цифры IP-адреса в зеркальном порядке), означает, что IP-адресу с последней цифрой **<ЦИФРА>** соответствует доменное имя **<ДОМЕННОЕ ИМЯ>**.
<ДОМЕННОЕ ИМЯ> обязательно должно быть полным и заканчиваться точкой. Не рекомендуется делать несколько PTR записей для одной цифры.
Крайне желательно чтобы для **<ДОМЕННОЕ ИМЯ>** существовала запись типа A (в другом файле, разумеется), которая ссылается на тот же самый IP-адрес.
Пример:

```
123 PTR myorg.ru.
124.100.168.192.in-addr.arpa. PTR server.myorg.ru.
```

6.8 Права доступа к файлам в UNIX

Система прав доступа к файлам в системах UNIX:

1. У файла или каталога есть владелец и принадлежащая файлу группа, а также права доступа, состоящие из трёх троек бит.
   первая тройка:
   используется если текущий пользователь совпадает с владельцем файла.
   вторая тройка:
   используется если владелец файла не совпадает с текущим пользователем и пользователь находится в группе которая присвоена файлу.
   третья тройка:
   используется в остальных случаях.
2. В каждой тройке каждый бит обозначается своей буквой:
   Для файлов:
   r - возможность чтения (read)
   w - возможность записи (Write)
   x - файл является исполнимым (интерпретируется как программа)
   Для каталогов:
   r - возможность чтения (просмотра) содержимого каталога (read). Дает право прочитать тип и имя вложенных элементов.
   w - возможность создавать/удалять/переименовывать элементы непосредственно внутри каталога или изменять их права доступа.
   x - возможность перейти в каталог или получить возможность какого-либо доступа к вложенным элементам.
3. Дополнительные биты для каталогов:
   SGID - В случае, если этот бит установлен, при создании элемента в этом

каталоге, элементу назначается та же группа что и у каталога.
Sticky - В случае, если используется третья тройка и установлен этот бит, то удалять из такого каталога можно только те файлы, владелец которых совпадает с текущим пользователем.

4. Права доступа может менять только пользователь являющийся владельцем файла.
Группу, принадлежащую файлу можно поменять только на группу, в которой находится текущий пользователь.
Владельца сменить нельзя.

Это описание очень краткое и полностью не описывает все возможности.
подробности -- http://www.opennet.ru/man.shtml?topic=chmod&category=1

- На пользователя root никакие из вышеперечисленных ограничений не распространяются.
- В отличие от Windows систем, права доступа на файловой системе не наследуются.

Пример:

```
ls -l file
-rw-r----- 1 owner1 grp1 1765 Янв 1 2006 file
```

Здесь команда ls выводит в таком виде:
первый '-' -- показывает тип элемента, а именно -- файл. 'rw-' -- показывает, что если к файлу будет обращаться пользователь owner1, то доступ будет на запись и чтение. 'r--' показывает, что если другой пользователь будет обращаться к файлу, и будет находиться в группе grp1, то доступ будет только на чтение. '---' -- показывает что для других никакого доступа нет.

```
ls -l folder
drwxr-x--x 1 owner1 grp1 1024 Янв 1 2006 folder
```

первая 'd' -- показывает тип элемента, а именно -- каталог. 'rwx' -- показывает, что если к файлу будет обращаться пользователь owner1, то для него будет полный доступ. 'r-x' показывает, что если другой пользователь будет обращаться к каталогу, и будет находиться в группе grp1, то он сможет посмотреть содержимое каталога и перейти в подкаталоги или открыть файл. '--x' -- показывает, что получить доступ к подкаталогу или файлу можно только зная его имя (посмотреть список нельзя) (удобно, для доступа к файлам вида abc/def/file1, abc/def/file2 -- при этом на каталоге def можно сделать права rwx--x--x).

Некоторые команды:
Список групп, в которых находится пользователь:

```
id
```

или

```
id "имя пользователя"
```

вывод с просмотром прав доступа:

```
ls -lsdh "файл или каталог"
```
вывод всех файлов каталога с их правами:
```
ls -lsh "каталог"
```

Замечания:

- Удалять каталоги можно только рекурсивно. Удалить непустой каталог нельзя.
- Если есть W на каталоге, то можно удалить или переименовать любой элемент внутри, независимо от прав доступа к этому элементу. Однако, нельзя удалить каталог, если в нем есть файлы которые нельзя удалить (по причине отсутствия прав доступа, или по причине того что где-то есть права --x на подкаталог, и поэтому рекурсивно удалить нельзя).

Часть VII

7 Контакты

Контакты

Всю информацию по приобретению продуктов, обновлениям, технической поддержке можно получить на нашем сайте:

http://www.ideco-software.ru

Также вы можете связаться с нами по e-mail info@ideco-software.ru или телефонам

+7 (495) 987-32-70, +7 (495) 662-87-34 (тех.поддержка);