

Ideco

Internet Control Server 2.5.8

Руководство пользователя



<http://www.ideco-software.ru>

Ideco Internet Control Server

Руководство пользователя

Это полное и подробное руководство по системе Ideco ICS 2.5.8. Если Вам нужна первоначальная информация о начале работы с Ideco ICS, обратитесь к "[Руководству по быстрому запуску](#)".

Информация, содержащаяся в этом документе, может быть изменена без предварительного уведомления, и Компания Ideco Software не берет на себя на этот счет никаких обязательств.

Программное обеспечение, описываемое в этом документе, поставляется в соответствии с Лицензионным договором. Это программное обеспечение может быть использовано или скопировано лишь в строгом соответствии с условиями этого лицензионного договора. Копирование этого программного обеспечения на какой-либо носитель информации, если на это нет специального разрешения в Лицензионном договоре или в ином договоре, заключенном с Компанией Ideco Software, является нарушением Закона Российской Федерации "О правовой охране программ для ЭВМ и баз данных" и норм международного права.

Никакая часть настоящего Руководства ни в каких целях не может быть воспроизведена или передана в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотокопирование и запись на магнитные носители, если на то нет письменного разрешения Компании Ideco Software.

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.

© 2008 Ideco Software

<http://www.ideco-software.ru>

Дата редакции: июль 2008 года

Содержание

Введение	2
Знакомство с Idesco ICS	2
Обзор возможностей.....	2
Интегрированные Интернет службы.....	4
Преимущества Idesco ICS.....	5
Что нового?	7
Новое в версии 2.5.8.....	7
Новое в версии 2.5.5.....	8
Новое в версии 2.5.4.....	9
Новое в версии 2.5.3.....	9
Новое в версии 2.5.2.....	10
Новое в версии 2.5.1.....	12
Новое в версии 2.5.0.....	13
Отличия версий Idesco ICS.....	14
Глава 1. Основы Idesco ICS	17
Назначение и принцип действия.....	17
Состав Idesco ICS.....	19
Пользователи и группы	21
Управление.....	22
Учет, тарификация, ограничение доступа	22
Защита и безопасность	23
Защита пользователей и локальной сети.....	23
Защита сервера	24
Глава 2. Установка и конфигурирование	25
Порядок установки и конфигурирования	25
Системные требования	25
Установка Idesco ICS	26
Начальное конфигурирование сервера	27
Конфигурирование локальной сети.....	28
Плоская сеть (без маршрутизаторов)	28
Сеть с подсетями (с маршрутизаторами)	28
Сеть с контроллером домена	29
Настройка подключения к провайдеру.....	29

Прямое подключение по Ethernet.....	29
Подключение по PPPoE.....	30
Подключение по PPTP.....	32
Подключение к нескольким провайдерам.....	33
Автоматическое переключение каналов.....	34
Авторизация пользователей на сервере IdecO ICS.....	34
Авторизация по IP.....	35
Авторизация по VPN.....	35
Авторизация по PPPoE.....	36
Авторизация через IdecO Agent.....	36

Глава 3. Администрирование (IdecO ICS Manager)

37

IdecO ICS Manager.....	37
Установка IdecO ICS Manager.....	38
Подключение к IdecO ICS.....	38
Главное окно IdecO ICS Manager.....	39
Администраторы.....	42
Управление пользователями.....	43
Дерево пользователей.....	43
Создание группы.....	46
Создание пользователя.....	46
Закладка "Информация" (у пользователя).....	48
Закладка "Информация" (у группы).....	53
Закладка "Статистика".....	59
Закладка "Операции".....	61
Закладка "Состав" (у группы).....	62
Закладка Безопасность.....	63
Баланс пользователя и группы, порог отключения.....	63
Признак "Финансовый".....	65
Использование NAT.....	65
Автоматическое обнуление баланса.....	66
Удаление пользователей.....	68
Поиск пользователей.....	69
Переподключение.....	70
Удаленное подключение.....	70
Использование почты.....	72
Смена пароля.....	72
Проверка пользователя.....	73
Оповещение пользователей.....	74
Настройка синхронизации IdecO ICS с Active Directory или LDAP сервером.....	75
Авторизация через программу агент – IdecOAgent.....	77
Рекомендации и замечания по работе с IdecO ICS Manager.....	78
Интерфейс IdecO ICS Manager.....	78
Безопасность логинов и паролей.....	79
Тарифные планы.....	79

Создание тарифного плана	81
Редактор правил и сетей.....	83
Создание закрытых ресурсов.....	85
Пулы IP-адресов	86
Создание пула IP-адресов.....	87
Аудит событий	88
Монитор.....	88
Редактор сайта	89

Глава 4. Локальная консоль сервера 91

Мониторинг	92
Конфигурирование сервера	94
Сетевые параметры.....	94
Конфигурация сетевых интерфейсов	97
Дополнительные настройки	103
Безопасность	105
Qos и Шейпер.....	106
Веб кэш, веб антивирус, проху	108
Почтовый сервер.....	110
Internet веб-сервер.....	113
FTP-сервер	114
DHCP-сервер	116
DNS-сервер.....	117
Сохраненные конфигурации	118
Резервное копирование	118
Сервис	119
Смена пароля.....	120
Перезагрузка сервера.....	120

Глава 5. Веб-интерфейс пользователя 122

Открытая часть.....	122
Страница "Главная".....	123
Страница "Вход"	124
Страница "Новости"	124
Страница "Тарифы".....	124
Страница "Подключение".....	124
Страница "Поддержка".....	124
Закрытая часть.....	124
Страница "Информация".....	125
Страница "Статистика"	126
Страница "Детализированная статистика"	126
Страница "Операции"	127
Страница "Тариф".....	127
Страница "Пароль"	128

Глава 6. Обслуживание	129
Резервное копирование	129
Удаление БД статистики посещений src-dst	130
Закрытие периода	130
Удаленный доступ к меню сервера	131
Глава 7. Дополнительные возможности Ideco ICS	132
Операции.....	132
Закладка "Операции"	132
Закладка "Журнал операций"	136
Закладка "Групповые операции"	137
Реквизиты пользователя и группы	138
Ввод значений	139
Редактирование списка реквизитов	139
Автоматическое формирование акта	139
Установка автоматического формирования акта.....	140
Шаблоны документов	141
Редактирование шаблонов	142
Расположение администраторов в дереве пользователей.....	143
Учет времени.....	144
Варианты использования	144
Принцип работы.....	144
Создание тарифного плана по учету времени.....	145
Карты оплаты.....	145
Параметры карт оплаты	146
Управление картами оплаты.....	146
Платежи по картам оплаты	149
Глава 8. Встроенные модули системы	150
Электронная почта.....	150
Служба электронной почты	150
Ограничения	151
Переадресация почты	151
Фильтры	154
Проверка на вирусы	155
Безопасность	155
Настройка почтового ящика.....	156
Рекомендации и замечания по работе с почтой	156
Встроенный Firewall.....	157
Создание группы правил	157
Создание правила Firewall	158
Контент фильтр	161
Отключение Firewall.....	163
Внешний сайт организации	163

Виртуальные домены	163
Размещение сайта	163
Готовые примеры: CMS Joomla! и форум phpBB.....	164
Права доступа	165
Приложение А. Подключение к серверу Idecso ICS	166
Настройка VPN-соединения в Windows 2000/XP/2003.....	166
Настройка VPN-соединения в Windows 95/98/ME	167
Автоматическая настройка VPN-соединения в Windows.....	168
Настройка VPN-соединения в Mac OS X.....	169
Приложение В. Используемые технологии и ПО	170
Приложение С. Технические характеристики Idecso ICS	173
Приложение D. Контакты	174
Алфавитный указатель	175

Введение

Знакомство с Ideco ICS

Ideco Internet Control Server – это универсальный Интернет шлюз с межсетевым экраном, функциями учета трафика и биллинговой системой. Ideco ICS позволяет быстро и легко настроить качественный доступ в Интернет всем пользователям, делает работу с Интернет управляемой и безопасной.

Интегрированные Интернет сервисы позволяют сразу развернуть полноценную почтовую службу, веб-сайт, FTP-сервер. Встроенный VPN-сервер позволяет объединить несколько офисов в единую сеть, подключить удаленные подразделения и мобильных пользователей.

Ideco ICS – это высоконадежное и безопасное решение со встроенной и максимально защищенной операционной системой Linux, включает в себя полностью сконфигурированные и готовые к использованию компоненты. Система автоматически устанавливается и управляется через простой графический интерфейс.

Ideco ICS 2.5 имеет сертификат Минсвязи (ССС) № ОС-1-СТ-0125 на АСР «Ideco Internet Control Server» версия 2.5 (22/11/2006 - 22/11/2009).

Обзор возможностей

Контроль доступа

- Персональный полноценный доступ в Интернет для каждого сотрудника. Авторизация по логину и паролю через VPN, PPPoE или через Ideco Agent, авторизация по IP-адресу и по MAC-адресу.
- Возможность синхронизации и авторизации пользователей через Active Directory и LDAP-сервер.
- Контроль доступа к ресурсам Интернет, вся информация о действиях пользователя сохраняется.
- Возможность иерархической группировки пользователей идеально подходит к принятым структурным единицам: отделы, подразделения, офисы. Назначение ответственных лиц для управления этими группами.

Учет, планирование и ограничение расходов

- Планирование и ограничение расходов (лимитирование) по пользователям, отделам и предприятию в целом.
- Подсчет статистики в реальном времени, автоматическое предупреждение и отключение пользователя при превышении лимита.
- Статистика посещения ресурсов Интернет в Мб и денежном эквиваленте, статистика TOP 100.
- Распределение ширины канала между пользователями. Расстановка приоритетов трафика. Возможностью ограничения скорости скачивания файлов.

Защита и безопасность, межсетевой экран (Firewall)

- Защита компьютеров от атак из Интернет с использованием технологий NAT и встроенного Firewall.
- Блокирование IP-адресов и протоколов по заданным условиям.
- Защита от сканеров сети, защита от DOS-атак и блокирование чрезмерной активности
- Content фильтр. Возможность запрета типа скачиваемых файлов, например, MP3 и AVI. Блокирование рекламы. Блокирование любых протоколов по ключевым словам.
- Разграничение доступа к корпоративным ресурсам, создание общих и закрытых серверов сети.
- Защита от подстановки IP-адреса и прослушивания трафика, при авторизации через VPN и PPPoE каждому пользователю назначается личный IP-адрес.
- Шейпер. Ограничение скорости Интернет трафика для отдельных пользователей, компьютеров или протоколов.
- DNAT portmapper. Возможность прозрачного перенаправления адресов и портов на другой адрес. Например, для прозрачного прокси или для публикации внутреннего веб-сервера.
- Фильтрация межсегментного локального трафика.

Удаленное подключение, виртуальные частные сети

- Доступ сотрудников к сети предприятия из дома или командировки по защищенному каналу.

- Возможность объединить все удаленные подразделения в общую сеть на единой платформе по шифрованным протоколам VPN PPTP и СIPE.
- Возможность создать закрытые корпоративные серверы для ограниченного круга сотрудников.

Сетевые возможности

- Полноценный маршрутизатор, поддерживающий множество интерфейсов (как локальных, так и внешних). Поддерживаются виртуальные 802.1q VLAN интерфейсы, PPTP, PPPoE и СIPE интерфейсы. Возможность указать маршруты по источнику.
- Интеллектуальный QoS. Интеллектуальная приоритезация трафика по скорости и типу, резервирование полосы пропускания для важных приложений, возможность расставлять приоритеты вручную. Равномерное распределение канала между пользователями и между приложениями.
- DHCP-сервер – Автоматическое распределение IP-адресов в локальной сети. Возможность фиксированной привязки IP к MAC адресу компьютера. Возможность выдавать DNS, WINS и маршруты для DHCP-клиентов. Возможность указания разных диапазонов для различных интерфейсов и VLAN.
- PPPoE и PPTP сервер.

Подключение к провайдерам, резервирование каналов

- Поддержка нескольких каналов провайдеров и нескольких внешних сетей.
- Создание разных тарифных планов. Перенаправление трафика в разные подсети.
- Возможность полного разделения пользователей для выхода в Интернет через разных провайдеров.
- Автоматическая проверка связи с провайдером и переключение на альтернативного провайдера, в случае необходимости. Возможность указать резервный тарифный план.
- Подключение к провайдеру по Ethernet, PPTP (VPN) и PPPoE.

Интегрированные Интернет службы

Почтовый сервер с антивирусом. Ideco ICS включает сконфигурированный и настроенный почтовый сервер. Почтовый ящик создается автоматически при добавлении пользователя.

- Поддержка нескольких почтовых доменов, доверенные сети и домены.

- Поддержка протокола IMAP, шифрованных протоколов POP3S, IMAPS и общих почтовых папок.
- Удобный, полнофункциональный веб-интерфейс для работы с личной почтой, позволяет работать с почтой из любой точки мира по шифрованному каналу через обычный браузер.
- Предварительный спам-фильтр, отсекающий письма без получения тела письма позволяет значительно экономить трафик.
- Возможность переадресации, групповой рассылки, фильтрации по адресам и содержанию.
- Установка размера почтового ящика и размера письма.
- Возможность дублирования всей почты на один адрес, для контроля и архивирования корреспонденции.
- Возможность загружать почту с других серверов по протоколу POP3 и IMAP.

Многосайтовый Internet веб-сервер. Idesco ICS включает в себя полноценный веб-сервер. Сервер позволяет размещать внешний сайт организации или несколько различных сайтов. Поддерживается возможность создания динамических сайтов на PHP и Perl, а также поддержка БД MySQL. Готовые примеры CMS Joomla! с шаблонами сайтов и форум phpBB.

FTP-сервер. Idesco ICS включает в себя полноценный FTP-сервер. На этом сервере можно хранить общие документы и прочие файлы. Доступ к серверу может осуществляться как из Интернет, так и из локальной сети. Анонимный и авторизованный вход. Создание FTP-пользователей. Закрытая и публичная часть. Защита от переполнения диска. Возможность ограничения скорости скачивания.

Сервер точного времени. Idesco ICS включает в себя сервер точного времени, который может синхронизировать время через Интернет. Кроме того, есть возможность синхронизировать время компьютеров локальной сети с самим сервером.

DNS-сервер. Idesco ICS включает в себя кэширующий DNS-сервер для локальной сети и полноценный DNS-сервер BIND. Есть возможность указывать соответствие между доменным именем компьютера и его IP-адресом.

Преимущества Idesco ICS

Надежность и безопасность

- Idesco ICS построен на базе ядра Linux с применением уникальных технологий. Поэтому имеет беспрецедентную надежность и защищенность, сравнимую с аппаратными маршрутизаторами.

- Многоуровневая система защиты сервера.
- Надежность системы подтверждается фактами внедрения Idecos ICS крупными компаниями и безотказной работой в больших сетях.
- Встроенный модуль отказоустойчивости восстановит систему даже в случае сбоя.

Простота установки, настройки и сопровождения

- Не требует изменения существующей сети предприятия – достаточно установки одного сервера.
- Idecos ICS автоматически устанавливается на компьютер. Для работы Idecos ICS не требуется дополнительного программного обеспечения – все необходимое есть на диске.
- Не требует постоянного сопровождения – эксплуатационные расходы близки к нулю
- Удобный и понятный интерфейс администратора: управление пользователями, тарифными планами, установка ограничений, настройка Firewall и т.д. Управление системой возможно не только системным администратором, но и обычным пользователем.
- Веб-интерфейс пользователя: просмотр статистики, баланса, смена пароля и другой информации.
- Встроенный DHCP-сервер максимально упрощает развертывание на малых и средних предприятиях.
- Не требует установки нестандартного ПО на компьютеры пользователей.
- Прозрачность для всех сетевых протоколов: HTTP, SMTP, POP3, FTP и других.

Экономический эффект

- Учитывая экономию расходов, низкие эксплуатационные издержки и высвобождение времени специалистов – Idecos ICS окупается за несколько месяцев.
- Удобная схема лицензирования. Имеются версии для малых предприятий: 10-20 пользователей; средних: 50-200; и крупных компаний: 500 и более пользователей.

Что нового?

Новое в версии 2.5.8

Статистика, отчеты

- Удобный интерфейс для просмотра статистики прозрачного прокси-сервера, информация по URL, большим файлам и времени.
- Системный монитор в веб-интерфейсе, просмотр состояния сервера.
- Возможность смотреть трафик в реальном времени.

Новые службы

- DNS-сервер BIND с поддержкой зон.
- Сервер авторизации RADIUS.

Веб-сервер

- Сайт-шаблон dokuwiki.
- Поддержка запроса клиентских SSL-сертификатов.

Почтовый сервер

- Теперь удаленные пользователи могут пользоваться SMTP-сервером своей организации, используя свой логин и пароль. Авторизация SMTP-клиентов через SASL и шифрование TLS.
- Возможность добавления сертификата в браузер и почтовый клиент для удобства работы по шифрованному SSL каналу.

Безопасность

- Блокирование чрезмерной активности по классам трафика.
- Возможность отправки почты через Службу Безопасности с визуальной проверкой человеком.
- Новые правила-шаблоны в firewall.

Надежность, отказоустойчивость

- Обновлены драйвера популярных сетевых карт.
- Добавлен NMI Watchdog.

- Добавлена возможность резервного копирования по FTP и NetBIOS.
- Подключение и управление дополнительными IDE/SATA дисками.
- Новые алгоритмы авторизации, тарификации и шейпера позволяют быстрее подключаться пользователям и выдерживать серверу еще большие нагрузки.
- IdecAgent теперь может работать в сетях с большой потерей пакетов.

Удаленное подключение по VPN

- Теперь мобильные сотрудники при подключении из командировки могут иметь адрес локальной сети – ProxuARP для этих адресов будет добавлен автоматически при подключении.

Возможности для провайдеров

- Поддержка работы с СОРМ.
- Поддержка работы с банкоматами и платежными системами.
- Веб-интерфейс приема платежей для кассира.
- Ежедневное списание абонентской платы.
- Назначение динамического NAT-адреса из диапазона.

Новое в версии 2.5.5

Firewall, Шейпер

- Создание правил для пользователей и для групп
- Удобное распределение безлимитных каналов

Антивирус

- Обновление не только базы вирусов, но и библиотеки алгоритмов проверки

Тарифы

- Возможность задавать стоимость в зависимости от объема
- Возможность задавать стоимость в зависимости от времени суток
- Возможность задавать скорость в зависимости от объема
- Возможность задавать скорость в зависимости от времени суток

- Возможность тарификации превалирующего трафика
- Поддержка безлимитных тарифов

Новое в версии 2.5.4

Кэширование веб трафика, прокси сервер

- Прозрачное кэширование веб трафика пользователей
- Гибкие настройки кэширования позволяют экономить до 20% трафика
- Значительное увеличение скорости работы на медленных каналах
- Возможность скрывать присутствие прокси
- Возможность использовать обычный прокси режим

Антивирус для веб трафика

- Проверка на вирусы веб трафика
- Проверка на вирусы скачиваемых файлов
- Отмена скачивания файла при обнаружении вируса
- Проверка архивов и сжатых файлов
- Предупреждение пользователей о нахождении вируса

Новое в версии 2.5.3

Поддержка LDAP и Windows AD доменов

- Автоматическая синхронизация пользователей с группой LDAP/AD
- Авторизация пользователей через сервер LDAP/AD

Новые способы авторизации пользователей

- Новый способ авторизации - через программу агент
- Привязка MAC адреса к конкретному пользователю
- Возможность автоматически выдавать закрепленный за пользователем IP адрес по DHCP

Подключение к провайдерам

- Возможность перенаправления трафика по критериям в разные каналы, на разных провайдеров
- Исправлена ошибка при подключении PPPoE к некоторым провайдерам

Почтовая система

- Поддержка протокола IMAP и общих почтовых папок
- Поддержка шифрованных протоколов POP3S и IMAPS
- Удобный, полнофункциональный Веб-интерфейс для работы с личной почтой, позволяет работать с почтой из любой точки мира по шифрованному каналу через обычный браузер
- Предварительный спам фильтр, уничтожающий не менее 70% спама. Отсекание без получения тела письма позволяет значительно экономить трафик
- Возможность дублирования всей почты на один почтовый адрес, для контроля и архивирования корреспонденции.

DHCP сервер

- Возможность фиксированной привязки IP к MAC адресу компьютера
- Возможность выдавать DNS и WINS для DHCP клиентов
- Возможность выдавать маршруты для DHCP клиентов

Новое в версии 2.5.2

Подключение к провайдерам, резервирование каналов

- Добавлена возможность подключения к провайдеру по PPPoE и PPTP
- Возможность полного разделения пользователей для выхода в Интернет через разных провайдеров.
- Автоматическая проверка связи с провайдером и переключение на альтернативного провайдера, в случае необходимости. Возможность указать резервный тарифный план.

Сетевые возможности, расширенная маршрутизация

- Ideco ICS теперь стал полноценным маршрутизатором. Поддерживается маршрутизация на большом количестве интерфейсов. Возможность src-dst маршрутизации и установки правил Firewall для маршрутизируемых сетей.

- Поддержка множества сетевых интерфейсов одновременно: Ethernet интерфейсы, PPPoE – часто нужен для ADSL модемов, PPTP – для подключения по VPN. CIPE – для объединения в единую сеть подразделений.
- Поддержка VLAN – виртуальные Ethernet интерфейсы по технологии 802.1q
- Возможность раздельной маршрутизации между локальными интерфейсами и между внешними.

Объединение в единую сеть всех подразделений

- Улучшились возможности подключения удаленных подразделений. Появилась возможность создания защищенного зашифрованного и помехоустойчивого канала CIPE между серверами Ideco ICS, что позволяет объединить все удаленные подразделения в общую сеть на единой платформе. При этом можно создать закрытые корпоративные серверы для ограниченного круга сотрудников.
- Возможность подключения в корпоративную сеть удаленных серверов и сетей на базе Windows, Linux и других ОС по протоколам VPN PPTP и CIPE
- Возможность каскадирования серверов Ideco ICS

Новые способы авторизации пользователей

- Помимо авторизации по протоколу PPTP (VPN), поддерживает авторизацию по протоколу PPPoE.
- Авторизация по IP адресу компьютера, то есть прямой выход в Интернет без установки виртуального соединения, для оборудования которое не поддерживает авторизацию и для доверенных сетей.

Возможности электронной почты

- Поддержка нескольких почтовых доменов
- Возможность использования сервера в качестве почтового шлюза - релея.
- Возможность указания доверенных сетей

Безопасность

- Значительно улучшена защита от DOS-атак
- Firewall позволяет фильтровать межсегментный локальный трафик
- Возможность привязки IP-адреса к MAC-адресу

Новое в версии 2.5.1

Новая функциональность

Интеллектуальный QoS – интеллектуальная приоритезация трафика по скорости и типу, резервирование полосы пропускания для важных приложений, возможность расставлять приоритеты вручную. Равномерное распределение канала между пользователями.

Content фильтр - возможность запрета типа скачиваемых файлов, например, mp3 и avi. Блокирование рекламы. Произвольное блокирование любых протоколов по ключевым словам.

Шейпер – ограничение скорости Интернет-трафика для отдельных пользователей, компьютеров или протоколов.

DNAT portmapper - возможность прозрачной переадресации адресов и портов на другой адрес. Например, для прозрачного прокси или для публикации внутреннего веб-сервера.

Почта – возможность переадресации, групповой рассылки, фильтрации по адресам и содержанию. Установка размера почтового ящика и размер письма.

Многосайтовый Internet веб-сервер: поддержка динамической генерации страниц PHP, Perl. Поддержка баз данных MySQL и Firebird. Виртуальные домены. Готовые примеры CMS Joomla! с шаблонами сайтов, форум phpBB.

FTP-сервер – анонимный и авторизованный вход. Создание FTP пользователей. Закрытая и публичная часть. Защита от переполнения диска. Возможность ограничения скорости скачивания.

Синхронизации времени с Time-серверами, встроенный NTP-серверами для локальной сети.

DNS для локальной сети, hosts файл.

Дополнительно: абонентская плата, списание дополнительных услуг, отключение по дате, просмотр ограничений родителя, несколько IP-адресов на интерфейсе, ProхуАгр, расширено количество правил Firewall для стандартной версии.

Производительность. Надежность

Значительно улучшены показатели производительности при сильно загруженном канале и при большом количестве пользователей. Обеспечение 150 Mbit на один процессор 2.4 GHz.

Качественное время ответа для интерактивных приложений даже при 100% загрузке канала, при использовании интеллектуального QoS.

Планировщик задач ядра переведен в режим 1000 Hz - это значительно улучшило время отклика при большой нагрузке.

Решены проблемы фрагментации БД статистики src-dst, улучшено время получения статистики в веб-интерфейсе.

Устранена возможность создания отказа в обслуживании через внутренний сайт статистики, организована очередь запросов от пользователей.

Улучшены механизмы отказоустойчивости.

Безопасность и защита сервера

Все сетевые службы помещены в клетки chroot, нарушение безопасности одной службы не приведет к уязвимости сервера. Используется усиленный, по сравнению со стандартным, chroot, и даже суперпользователь не может покинуть такой chroot.

Запрет исполнения файлов с разделов с данными.

Запрет монтирования новых файловых систем.

Запрет монтирования rgs.

Максимальное ограничение возможностей (capabilities) для всех служб и процессов.

Система обнаружения и уничтожения exploit в ядре.

Новая усиленная схема защиты позволяет защитить систему даже от уязвимостей, которые могут обнаружены в будущем в Linux. Использование уникальных механизмов безопасности позволяет назвать Ideco ICS 2.5.1 одним из самых защищенных и надежных серверов на сегодняшний день.

Новое в версии 2.5.0

Ideco Internet Control Server 2.5 включает следующие нововведения, делающие его еще более надежным, простым, удобным и гибким в использовании:

Сервер

- Встроенный почтовый сервер
- Расширенный Firewall
- DHCP
- Кэширующий DNS
- Возможность удаленного подключения
- Учет времени
- Поддержка Pocket PC Windows Mobile 2002/2003
- Локальная консоль управления основными параметрами

- Система автоматического восстановления после сбоев
- Оповещение администратора по e-mail

Административный интерфейс

- Полностью новый удобный административный интерфейс
- Разделение полномочий администраторов
- Монитор пользователей
- Редактор новостей сайта
- Редактор правил Firewall
- Журнал операций
- Журнал аудита
- Возможность печати документов и редактирования шаблонов

Удобство использования

- Новый веб-интерфейс пользователя, статистика посещений и TOP100
- Мастер автоматической настройки VPN соединений
- Оповещение о превышении баланса по e-mail и winpopup
- Полностью автоматическая установка Ideco ICS на пустой компьютер

Отличия версий Ideco ICS

Ideco ICS выпускается в двух вариантах:

- Версия **Ideco ICS Standard Edition**
- Версия **Ideco ICS Enterprise Edition**. Обладает всеми возможностями версии Standard Edition, а также имеет ряд дополнительных возможностей.

Функциональность	Применение	Standard Edition	Enterprise Edition
VPN-сервер, PPPoE-сервер	Подключение пользователей, контроль доступа	X	X
Трансляция сетевых адресов (NAT)	Используется для защиты компьютеров пользователей от атак из Интернет, снимает ограничение на количество подключенных	X	X

Функциональность	Применение	Standard Edition	Enterprise Edition
	пользователей		
Модуль учета и контроля доступа	Подсчет текущего баланса, сохранение статистики	X	X
Статистика по сессиям	Анализ расхода трафика	X	X
Статистика по посещаемым ресурсам, детализированная статистика	Анализ посещаемых ресурсов Интернет	X	X
Веб интерфейс пользователя	Просмотр статистики, баланса, смена пароля и т.д.	X	X
Административный интерфейс	Управление пользователями, создание тарифных планов и другое.	X	X
Модуль отказоустойчивости	Автоматическое восстановление системы после сбоев	X	X
Система резервного копирования	Сохранение резервных файлов БД и конфигурации	X	X
Документооборот	Позволяет создавать и распечатывать отчетные документы	X	X
Кэширующий DNS сервер	Позволяет уменьшить количество внешних DNS-запросов и ускорить ответ на DNS-запрос	X	X
DHCP сервер	Автоматическое выделение IP-адресов компьютерам	X	X
Многосайтовый внешний веб-сервер	Позволяет создать внешний сайт организации	X	X
Интеллектуальный QoS и Шейпер	Позволяет автоматически распределять ширину канала и ограничивать скорость трафика	X	X
Content-фильтр	Позволяет фильтровать трафик по содержанию	X	X
FTP-сервер	Позволяет создавать на сервер общие файловые архивы	X	X
Встроенный Firewall	Установка дополнительных правил ограничений доступа, защита серверов сети	не более десяти правил	X
Возможность создания нескольких администраторов	Позволяет создавать выделенных администраторов для отдельных групп пользователей	не более четырех	X
Встроенный почтовый сервер	Пользователям автоматически создается личный почтовый ящик, переадресация почты	только у каждого пятого,	X

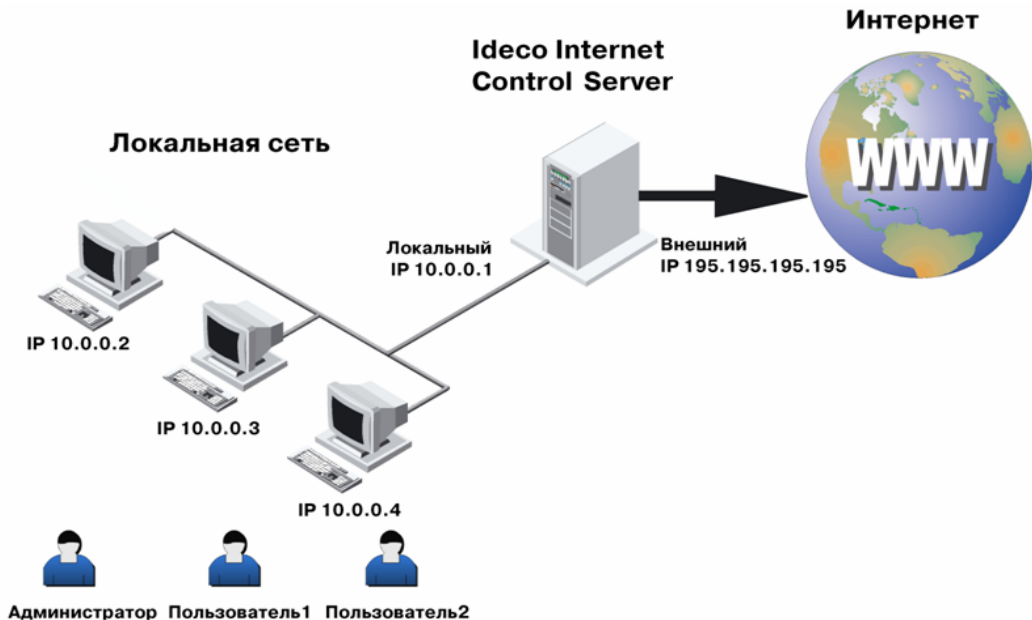
Функциональность	Применение	Standard Edition	Enterprise Edition
Карты оплаты	Позволяет организовать доступ по картам оплаты (Интернет карты)	–	X
Поддержка Active Directory/LDAP	Автоматическая синхронизация пользователей с группой LDAP/AD. Авторизация пользователей через сервер LDAP/AD	–	X

Глава 1. Основы Ideco ICS

В этой главе описываются основы Ideco ICS.

Назначение и принцип действия

Ideco ICS устанавливается на границе между локальной сетью предприятия и Интернет. И все взаимодействие пользователей с глобальной сетью осуществляется через Ideco ICS. Сервер имеет минимум два сетевых интерфейса: один интерфейс подключен к Интернет, а второй к локальной сети предприятия. Это позволяет полностью управлять Интернет трафиком, а также обеспечивать защиту локальной сети от внешних угроз.



В сети предприятия используются локальные IP-адреса, рекомендуются адреса из диапазона 10.0.0.2–10.127.255.255. На сервере создаются или импортируются пользователи и выбирается способ авторизации. После авторизации предоставляется доступ к Интернет с использованием технологии NAT.

При авторизации по логину паролю через VPN или PPPoE пользователь получает свой личный IP-адрес, который отличается от локального адреса компьютера. При таком способе авторизации пользователь выходит в Интернет от своего личного IP-адреса. Учет и ограничение идет по этому адресу. Данный способ авторизации является самым безопасным, так как устанавливается прямой защищенный канал от пользователя до сервера. Рекомендуется задавать пользователям адреса из диапазона 10.128.0.1–10.255.255.255, чтобы они не пересекались с адресами компьютеров.

При авторизации по логину паролю через Ideco Agent, IP-адрес пользователя совпадает с адресом компьютера и меняется при переходе на другой компьютер. Возможность сохранить логин пароль для автоматической авторизации.

При авторизации по IP или по IP + MAC компьютер с этим IP-адресом всегда имеет доступ в Интернет. При указании MAC-адреса компьютеры могут получать статические IP-адреса через DHCP.

При авторизации по IP + Ideco Agent компьютер с этим IP-адресом имеет доступ в Интернет только после авторизации пользователя через Ideco Agent. Пользователь при этом может работать только с этого компьютера.

Во время работы пользователя ведется статистика расхода трафика в соответствии с указанным тарифом и, если превышен лимит, то происходит отключение.

Примечания:

IP-адрес – уникальный адрес компьютера в сети. В системе Ideco ICS каждому пользователю назначается личный IP-адрес, и учет трафика ведется по этому IP-адресу, а не по IP-адресу компьютера. IP-адреса бывают двух типов: реальные Интернет-адреса и адреса для внутреннего использования в локальной сети предприятия. Рекомендуется для внутренних адресов компьютеров использовать диапазон 10.0.0.2 – 10.127.255.255, а для личных адресов пользователей использовать диапазон 10.128.0.1 – 10.255.255.255. Для Интернет-серверов предприятия задаются реальные IP-адреса, выданные провайдером. Сам Ideco ICS имеет три IP-адреса: внутренний (по умолчанию 10.0.0.1), защищенный (по умолчанию 10.128.0.0) и внешний, выданный провайдером.

VPN (Virtual Private Network). Для подключения пользователей к серверу Ideco ICS используется технология VPN. При подключении к серверу пользователь вводит свой логин и пароль. Пройдя авторизацию, пользователь получает доступ в Интернет. VPN обеспечивает прямой канал от клиента до сервера Ideco ICS, независимо от его нахождения в локальной сети. VPN соединение обеспечивает надежную защиту от подстановки чужого IP-адреса и прослушивания канала. Позволяет обеспечить удаленный защищенный доступ пользователей из дома или командировки, организовать защищенный канал связи с удаленными подразделениями. Для подключения к Ideco ICS используются стандартные VPN драйвера

Windows, Linux и других операционных систем.

NAT (Network Address Translation). Технология NAT защищает компьютеры пользователей от атак из сети Интернет. NAT скрывает компьютеры пользователей от доступа из внешней Интернет сети.

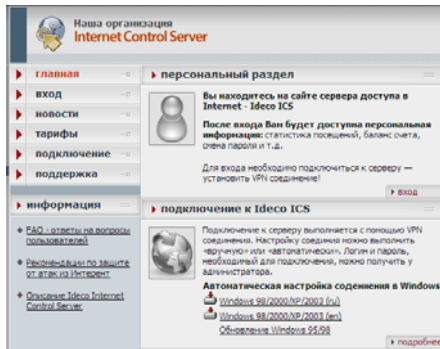
Ideco Agent – программа авторизации пользователя и отображения баланса, запускается на компьютере пользователя и находится в трее.

Состав Ideco ICS

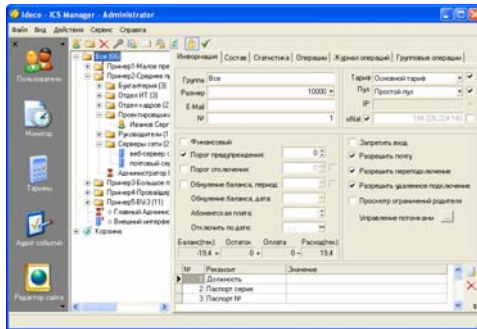
В состав системы Ideco ICS входят следующие основные компоненты:

- **Операционная система на базе ядра Linux.** Разработан специализированный дистрибутив с усиленными механизмами защиты.
- **Программное ядро системы** управляет подключением пользователей к серверу, выполняет алгоритмы тарификации, контроль доступа, собирает статистику.
- **База Данных,** хранящая информацию о пользователях и другие данные, необходимые для системы Ideco ICS.
- **Межсетевой экран (Firewall).** Фильтрует трафик по задаваемым правилам для защиты серверов и пользователей от Интернет-атак, запрещает заданные Интернет-ресурсы. Встроенный Firewall может ограничивать скорость соединений, правильно распределять ширину канала. Кроме того, есть возможность фильтровать трафик по содержанию.
- **Почтовый сервер с антивирусом.** Каждый пользователь может автоматически получить личный почтовый ящик.
- **Внешний WEB-сервер.** Полноценный многосайтовый WEB-сервер. Позволяет размещать внешний сайт организации или несколько различных сайтов. Поддерживается возможность создания динамических сайтов на PHP и Perl, а также поддержка MySQL.
- **FTP-сервер.** Полноценный FTP-сервер. Возможность хранить общие документы и прочие файлы. Доступ к серверу может осуществляться как снаружи, так и из локальной сети.
- **Сервер точного времени.** Синхронизация времени через Интернет. Возможность синхронизировать время компьютеров локальной сети.
- **DNS-сервер.** Ideco ICS включает в себя DNS сервер для локальной сети. Есть возможность указывать соответствие между именем компьютера и его сетевым адресом.

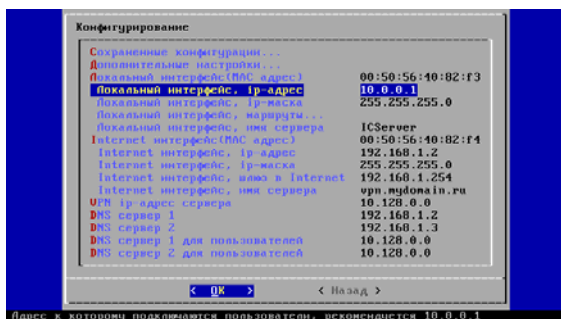
- **Веб-интерфейс пользователя.** Позволяет пользователю просматривать статистику, баланс, сменить пароль, получить справочную информацию.



- **Административный интерфейс (Ideco ICS Manager).** Приложение для управления Ideco ICS устанавливаемое на компьютерах администраторов.



- **Локальная консоль управления сервером.** Используется при установке сервера для первоначального конфигурирования. В локальной консоли включаются параметры безопасности, проводится сервисное обслуживание, включаются и выключаются службы. Имеется возможность удаленного доступа к локальной консоли через SSH.



Замечания:

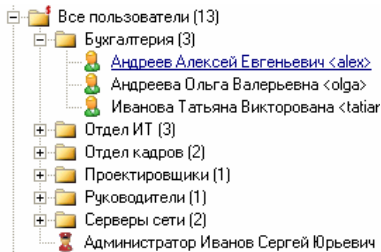
Все необходимое для функционирования Ideco ICS программное обеспечение входит в комплект поставки и устанавливается автоматически.

Пользователи и группы

Основным понятием системы Ideco ICS является пользователь.

Пользователь – регистрационная запись пользователя, получающего доступ в Интернет через Ideco ICS. Пользователем также может быть внутренний сервер предприятия или любое сетевое устройство.

Для удобства управления, пользователей объединяют в группы. Уровень вложенности групп неограничен. Такая древовидная структура позволяет легко отразить реальную структуру предприятия.



Группой может являться также и стороннее юридическое лицо, в случае оказания услуг доступа другим предприятиям. Для этого, создайте группу и передайте управление этой группой администратору этого предприятия. У таких групп необходимо устанавливать признак **финансовая**.

Основные параметры пользователей, такие как, пул IP-адресов, тарифный план, параметры ограничений и разрешений, по умолчанию наследуются от родительских групп.

Каждый пользователь и каждая группа имеют свой лицевой счет. Лицевой счет отражает текущий баланс.

Баланс(тек.)	Остаток	Оплата	Расход(тек.)
-5817,9 =	-5132,5 +	0 -	685,4

Система обеспечивает хранение информации об истории баланса, расходов за период, поступлениях за период, остатков на начало расчетных периодов. История отражена в журнале операций.

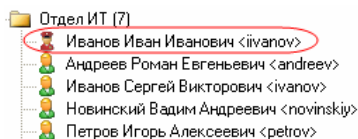
Для нефинансовых пользователей устанавливается лимит расхода за период, баланс обнуляется в начале периода и отсчет идет заново.

Для финансовых пользователей обнуление баланса не происходит, и оплата производится оператором.

Управление

Управление Ideco ICS осуществляется через Ideco ICS Manager. Эта программа устанавливается на компьютеры администраторов.

Администратор – это пользователь, имеющий права по управлению другими пользователями.



В системе может быть определено произвольное число администраторов с различными полномочиями.

Примечание: В версии Standard Edition может быть определено только четыре администратора (подробнее см. "[Отличия версий Ideco ICS](#)" на стр. 14).

После установки системы в ней зарегистрирован единственный администратор с именем **Главный администратор** и логином **Administrator**. Главный администратор имеет неограниченные права по управлению Ideco ICS. В дальнейшем могут быть созданы дополнительные администраторы.

Администратор может управлять всеми пользователями группы, в которой он находится сам, а также всеми подгруппами этой группы.

Удобный и понятный интерфейс Ideco ICS Manager позволяет управлять пользователями не только высококвалифицированным системным администраторам, но и простым пользователям.

Администратор может любого из пользователей группы назначить администратором группы. Тогда администратор группы сможет управлять пользователями своей группы, при этом он не сможет просматривать и изменять пользователей в других группах.

Учет, тарификация, ограничение доступа

В системе ведется учет расхода трафика по пользователям, группам пользователей и всего предприятия в целом.

Тарификация – это списание с лицевого счета пользователя условных единиц в соответствии с назначенным тарифным планом. Списание происходит в реальном времени.

Тарифный план определяет стоимость трафика в зависимости от направления.

№	Тарифный План	Вкл.	Правило	Цена Вх.	Цена Исх.
22	Тарифный план №1	<input checked="" type="checkbox"/>	Локальная сеть	0	0
18	Сторонние юр. лица	<input checked="" type="checkbox"/>	Сеть провайдера	0,01	0
27	Абоненты в домах	<input checked="" type="checkbox"/>	Внутригород	0,5	0
			Весь Интернет	3,5	0

Назва	Подсеть	Маска	Полити
	10.0.0.0	255.0.0.0	решено

В зависимости от потребностей предприятия может быть определено несколько тарифных планов. Поддерживается возможность смены тарифного плана, как для отдельных пользователей, так и для их групп.

В зависимости от состояния баланса пользователей или группы может происходить ограничение доступа. Например, если установить у пользователя порог отключения равным "-100", то при достижении балансом этого значения, пользователю будет автоматически закрыт доступ в Интернет. Также имеется возможность рассылки предупреждений о скором отключении доступа по электронной почте, winpopup и Ideco Agent.

<input type="checkbox"/>	Финансовый	
<input checked="" type="checkbox"/>	Порог предупреждения:	-40
<input checked="" type="checkbox"/>	Порог отключения:	-50
<input checked="" type="checkbox"/>	Обнуление баланса, период:	Месяц
	Обнуление баланса, дата:	01.08.2005

Защита и безопасность

Ideco ICS поддерживает принцип безопасности “Все, что не разрешено явно, то запрещено”. Обеспечивается максимальная безопасность, как пользователей, так и самого сервера.

Защита пользователей и локальной сети

Встроенный Firewall сервера изначально настроен на максимальную защищенность.

Ни один компьютер или другое устройство не может выйти в Интернет без авторизации. Все пользователи по умолчанию скрыты от внешних угроз технологией NAT.

Технология авторизации по VPN, PPPoE, Ideco Agent позволяет полностью устранить уязвимость подстановки чужих IP-адресов.

Встроенный Firewall позволяет гибко настраивать ограничения к Интернет ресурсам и защищать внутренние серверы с реальным IP-адресом от атак из Интернет.

Возможность создания зашифрованного канала для удаленного доступа сотрудников к сети предприятия из дома или командировки.

Возможность создания закрытых корпоративных серверов для ограниченного круга лиц.

Статистика пользователей также защищена, доступ возможен только после ввода логина и пароля.

Установка ограничений по расходам на все предприятие позволяет защититься от чрезмерного трафика во время вирусных эпидемий и Интернет атак.

Защита сервера

Ideco ICS содержит только надежные и хорошо зарекомендовавшие себя компоненты.

Все сетевые службы помещены в клетки chroot, нарушение безопасности одной службы не приведет к уязвимости сервера. Используется усиленный, по сравнению со стандартным, chroot. Даже суперпользователь не может покинуть такой chroot.

Изменение исполняемых файлов сервера возможно только при прямом физическом доступе к серверу.

Запрет исполнения файлов с разделов с данными, запрет монтирования новых файловых систем.

Максимальное ограничение возможностей (Capabilities) для всех служб и процессов.

Система обнаружения и уничтожения exploit в ядре.

Права администраторов четко ограничены в пределах своей группы на внутреннем уровне базы данных.

Глава 2. Установка и конфигурирование

В этом разделе описывается процесс установки и начального конфигурирования сервера Ideco ICS. Если Вам нужна первоначальная информация о начале работы с Ideco ICS, то рекомендуется обратиться к документу "Ideco Internet Control Server. Приступая к работе".

Порядок установки и конфигурирования

1. [Установка Ideco ICS](#). Ideco ICS устанавливается на отдельный компьютер. При установке будет автоматически установлена операционная система и все необходимые компоненты. Перед началом установки нужно ознакомиться с разделом "[Системные требования](#)" на стр. 25.
2. "[Начальное конфигурирование сервера](#)" на стр. 27. После установки нужно выполнить начальное конфигурирование сервера с локальной консоли: задать IP-адреса, DNS и т.д.
3. "[Конфигурирование локальной сети](#)" на стр. 28. При необходимости может потребоваться внести изменения в локальную сеть.

На этом установка сервера Ideco ICS заканчивается, далее необходимо:

4. Добавить пользователей и выбрать способ авторизации, отредактировать тарифный план. Подробнее см. "[Глава 3. Администрирование \(Ideco ICS Manager\)](#)" на стр. 37.

Системные требования

Требования к серверу Ideco ICS

Процессор	Процессор Pentium/Celeron/AMD 800 МГц или более мощный
Память*	256 МБ или больше
Жесткий диск**	8 Гб или больше, IDE/SATA

Сетевое оборудование	Две PCI сетевые карты. Рекомендуется 3Com905, Realtek 8139C+, Intel E100
Дополнительно	CD-ROM или DVD-ROM привод, монитор, клавиатура
Рекомендации	Системные платы на чипах Intel 945, Intel 965.
Замечания	Для SATA дисков необходимо в BIOS включить режим IDE LEGACY.

Примечания:

* В зависимости от количества пользователей (точнее, количества одновременно устанавливаемых VPN/PPPoE соединений с сервером), следует придерживаться следующего правила: на каждые 100 пользователей (одновременных соединений) рекомендуется дополнительно 256 Мб.

** В зависимости от объема трафика, а также продолжительности хранения детализированной статистики (статистики source-destination) может потребоваться увеличения объема жесткого диска. Например, объем трафика 100 Гб/Мес. соответствует приросту детализированной статистики примерно 3 Гб/Мес. При этом объем основной статистики увеличивается не значительно.

Для установки и работы Ideco ICS не требуется дополнительного программного обеспечения.

Компьютеры пользователей

Для подключения к серверу используются стандартные VPN/PPPoE драйвера Windows, Linux и других операционных систем, либо программа Ideco Agent. При авторизации по IP достаточно обеспечить связь с сервером по протоколу IP.

Установка Ideco ICS

Сервер Ideco ICS устанавливается с компакт диска на отдельный компьютер. При установке будет автоматически установлена операционная система и все необходимые компоненты.

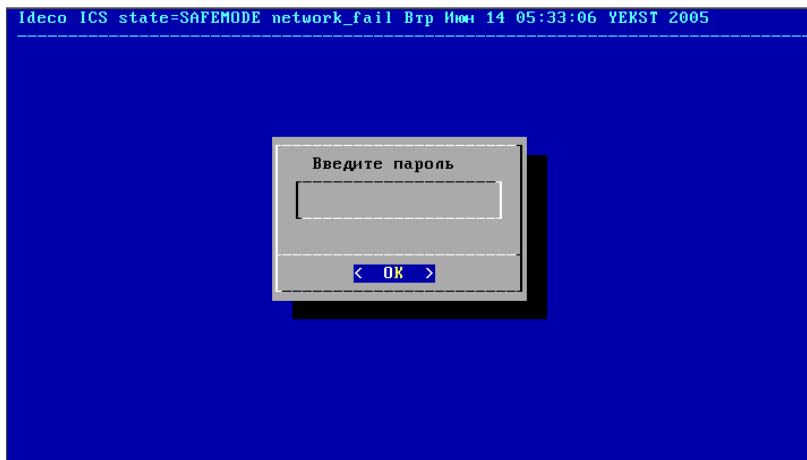
Важно! Перед установкой все данные будут уничтожены. Сервер Ideco ICS не поддерживает установку в существующую ОС или соседство с другой ОС.

1. Установите BIOS компьютера загрузку с CD-ROM и обязательно установите правильное время. Вставьте в CD-ROM установочный диск Ideco ICS.
2. Выполните загрузку с установочного диска.
3. Следуйте инструкциям мастера установки.

4. Перезагрузите сервер.

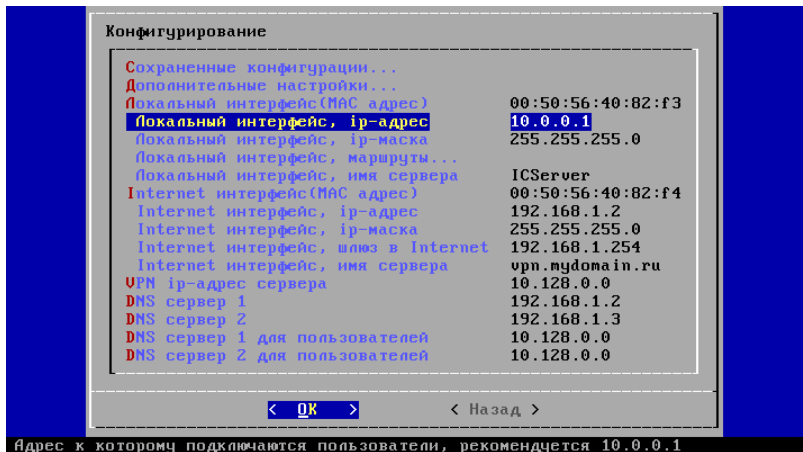
Начальное конфигурирование сервера

1. В верхней статусной строке показано, что сервер находится в режиме **SAFEMODE** и требуется его настройка.



2. Введите пароль "servicemode"

Войдите в раздел "Конфигурирование сервера", затем в раздел "Конфигурирование сети". Появится окно задания основных параметров. Задайте основные параметры: локальный IP адрес и параметры провайдера, и перезагрузите сервер. Подробнее о назначении параметров см. "[Сетевые параметры](#)" на стр. 94.



Конфигурирование локальной сети

Для правильной работы сервера, может потребоваться внести незначительные изменения в существующую сеть организации.

Плоская сеть (без маршрутизаторов)

1. Исключить возможность доступа пользователей в Интернет в обход сервера Ideco ICS. То есть физическое подключение к Интернет-провайдеру должен иметь только сервер Ideco ICS.
2. Проверить доступность сервера с компьютеров пользователей. Запустить команду строку, и выполнить команду

```
ping 10.0.0.1
```

вместо адреса 10.0.0.1 укажите тот, который вы установили для локального интерфейса при конфигурировании сервера.

3. Рекомендуется всю сеть перевести на диапазон IP-адресов 10.0.0.2 - 10.127.255.255. Это не является обязательным, но позволит избежать проблем расширения сети в будущем. Перевод компьютеров на новые IP-адреса можно выполнять постепенно.

Сеть с подсетями (с маршрутизаторами)

1. Исключить возможность доступа пользователей в Интернет в обход сервера Ideco ICS. То есть физическое подключение к Интернет-провайдеру должен иметь только сервер Ideco ICS. Некоторым серверам можно оставить прямой доступ в Интернет, но тогда рекомендуется отключить эти серверы от локальной сети организации, что бы избежать возможности пользователей обходного выхода в Интернет и исключить доступ в локальную сеть через эти серверы.
2. На всех маршрутизаторах организации прописать маршрут к серверу Ideco ICS.
3. Проверить доступность сервера с компьютеров пользователей. Запустить команду строку, и выполнить команду

```
ping 10.0.0.1
```

и

```
tracert -d 10.0.0.1
```

вместо адреса 10.0.0.1 укажите тот, который вы установили для локально интерфейса при конфигурировании сервера.

4. При авторизации по VPN/PPPoE, на компьютерах рекомендуется добавить маршрут локальной сети с указанием шлюза (маршрутизатора).

Например, для компьютеров подсети 10.33.1.x с маршрутизатором 10.33.1.1:

```
route -p add 10.0.0.0 mask 255.128.0.0 10.33.1.1
```

(Для компьютеров с ОС Windows 9x вместо ключа "-p" создать BAT-файл с этой командой и добавить его в автозагрузку.)

Для сети 10.16.x.x с маршрутизатором 10.16.0.1:

```
route -p add 10.0.0.0 mask 255.128.0.0 10.16.0.1
```

Добавление маршрута позволит избежать избыточного внутрисетевого трафика через сервер доступа. В противном случае после подключения к Интернет весь межсегментный трафик пользователей будет идти через Idesco ICS, что связано с особенностью ОС Windows.

Рекомендуется всю сеть перевести на диапазон IP-адресов 10.0.0.2 - 10.127.255.255. Это не является обязательным, но позволит избежать проблем развития сети в будущем. Перевод компьютеров на новые IP-адреса можно выполнять постепенно.

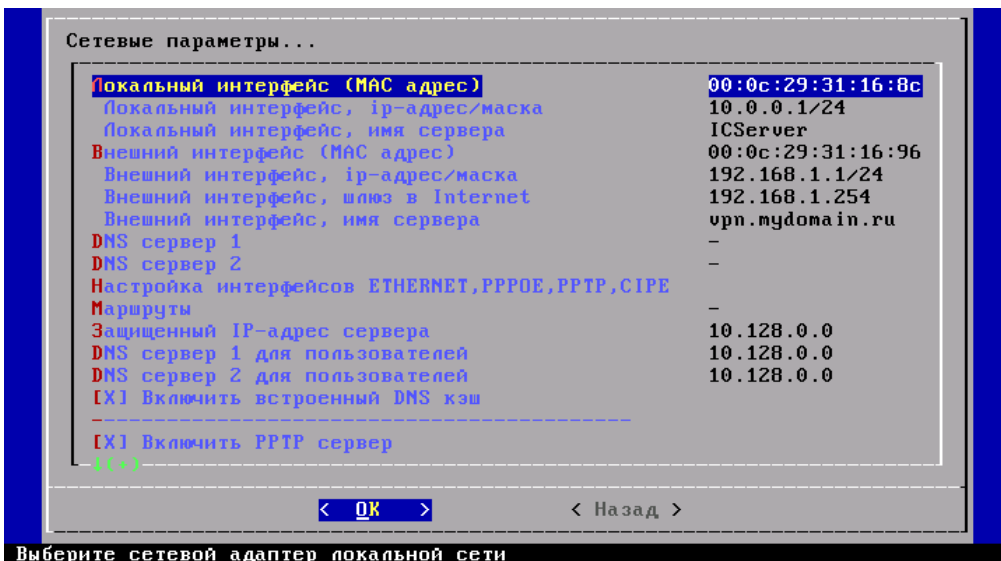
Сеть с контроллером домена

1. Настроить синхронизацию пользователей Idesco ICS и AD. Выбрать способ авторизации – рекомендуется Idesco Agent или VPN/PPPoE.
2. Отключить в настройках VPN/PPPoE-соединения на вкладке "Сеть" все компоненты кроме TCP/IP.
3. При использовании Idesco Agent рекомендуется расположить IdescoAgent.exe на общем сетевом ресурсе и установить в политике входа в домен запуск приложения IdescoAgent.exe с ключом --domain. Таким образом, запуск агента будет централизован и не потребует его установка на каждый компьютер.

Настройка подключения к провайдеру

Прямое подключение по Ethernet

Выберите в меню "Конфигурирование сервера" пункт "Конфигурирование сети".

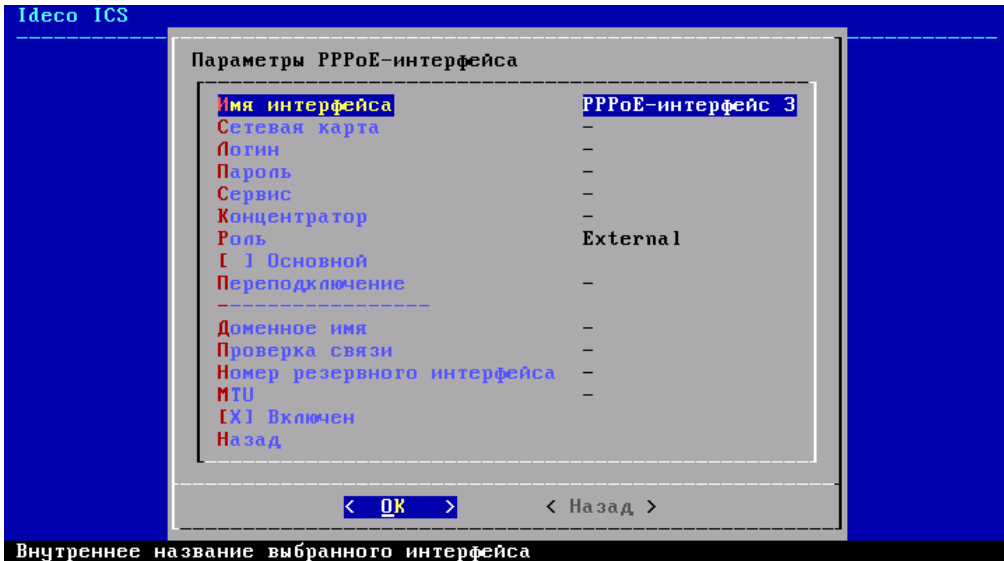


Необходимо выбрать сетевую карту, подключенную к провайдеру в пункте "Внешний интерфейс (MAC адрес)", указать IP-адрес, маску подсети, шлюз и два DNS-сервера провайдера.

Подключение по PPPoE

Для того чтобы подключить сервер Ideco ICS по протоколу PPPoE необходимо произвести следующее:

1. В локальной консоли открыть раздел "Конфигурирование сервера" – "Конфигурирование сети" – "Настройка интерфейсов 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. Отключить интерфейс с номером два – снять флажок "[] Включен".
7. Если провайдер требует указания имени сервиса и концентратора, указать их в соответствующих полях.
8. Сделать мягкую перезагрузку, а затем подключиться с помощью ICSManager к серверу.
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 NAT появился IP адрес выданный провайдером по PPPoE.

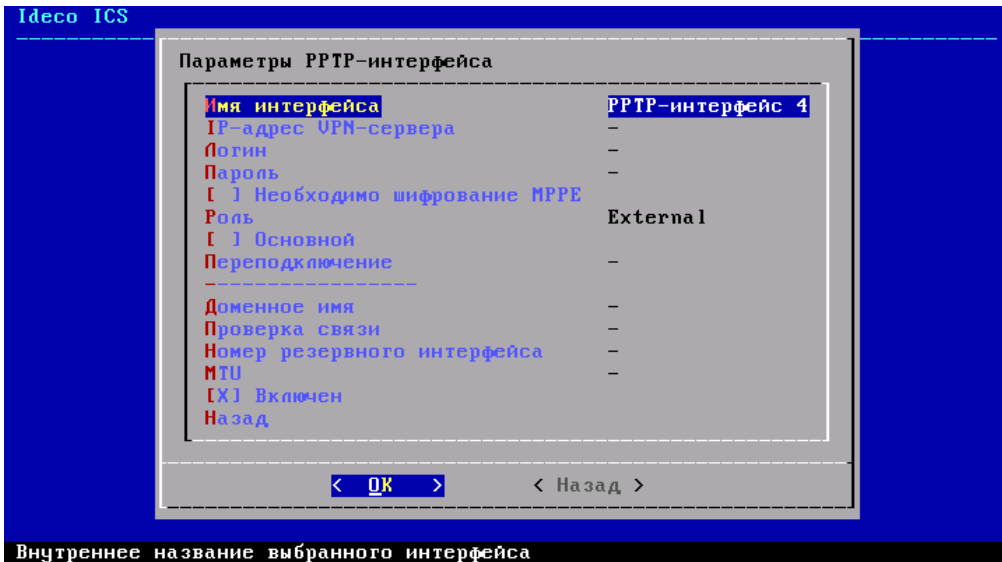
Важно! При подключении через ADSL, xDSL модем необходимо выяснить, в каком режиме настроен модем. Если модем настроен в режиме моста, то часто необходимо настроить PPPoE подключение к провайдеру на сервере Idecso ICS. Если модем находится в режиме NAT, то нужно сменить MTU/MRU на модеме, указать их равными 1000. Если модем в режиме NAT или в режиме

маршрутизатора, то необходимо настраивать Ideco ICS, как в разделе "Прямое подключение по Ethernet" и указывать локальный адрес модема в качестве шлюза для Ideco ICS. Необходимо обратить внимание на то чтобы адреса локальной сети не пересекались с адресами модема.

Подключение по PPTP

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

1. В локальной консоли открыть раздел "Конфигурирование сервера" – "Конфигурирование сети" – "Настройка интерфейсов Ethernet, PPPoE, PPTP, CIPE".
2. В этом диалоге создать интерфейс и указать тип "PPTP".



3. В поле "IP-адрес VPN-сервера" указать IP-адрес VPN-сервера провайдера
4. Указать 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>

8. Сделать мягкую перезагрузку, а затем подключиться с помощью ICSManager к серверу.
9. В корневой папке должен появиться пользователь, соответствующий созданному интерфейсу. В имени этого пользователя можно посмотреть 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 NAT появился IP адрес выданный провайдером по PPTP.

Подключение к нескольким провайдерам

Для подключения к нескольким провайдерам Интернет, необходимо сделать следующие настройки:

1. Для дополнительного провайдера сконфигурировать сетевой интерфейс (“Конфигурирование сервера” – “Конфигурирование сети” – “Настройка интерфейсов Ethernet, PPPoE, PPTP, CIPЕ”). 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 ICS Manager. Эти адреса будут выдаваться пользователям, выходящим в Интернет через дополнительного провайдера. Например, 10.230.1.0 / 255.255.255.0.
3. Создать маршрут вида:
 <выбранная подсеть> <0.0.0.0/0.0.0.0> <шлюз второго провайдера>.
 Например,
 10.230.1.0/255.255.255.0 0.0.0.0/0.0.0.0 шлюз.
 Если подключение ко второму провайдеру через интерфейс PPTP или PPPoE, то укажите в качестве шлюза номер этого интерфейса.
4. Сделать мягкую перезагрузку, а затем подключиться с помощью ICS Manager к серверу.
5. В разделе «Тарифы» 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» 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.

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 Ideco ICS с помощью ICSManager.
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. Произвести мягкую перезагрузку.

Авторизация пользователей на сервере Ideco ICS

Авторизация пользователей на сервере возможна через VPN, PPPoE, по IP-адресу и через программу IdecoAgent.

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».

На ПК пользователя убрать все настройки прокси в браузере.

Если при установке сервера, для администратора выбран тип авторизации по VPN, то для подключения администратора и запуска ICS Manager необходимо установить VPN-соединение. VPN-соединение рекомендуется оставить основным способом авторизации Администратора.

Авторизация по IP

Укажите в свойствах пользователя IP-адрес его компьютера.

На компьютере пользователя в настройках сетевой карты укажите в качестве шлюза и в качестве DNS локальный IP-адрес Ideco ICS.

Если необходима MAC привязка, укажите MAC-адрес в свойствах пользователя или нажмите кнопку "получить". Если нужно закрепить IP-адрес пользователя в DHCP, тоже сделайте MAC привязку.

Авторизация по VPN

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

1. Для автоматической настройки нужно скачать файл с первой страницы веб-интерфейса 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 ICS. Подробнее об автоматической настройке см. "[Приложение А. Подключение к серверу Ideco ICS](#)" на стр. 166, раздел "[Автоматическая настройка VPN-соединения в Windows](#)" на стр. 168
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. "[Приложение А. Подключение к серверу Ideco ICS](#)" на стр. 166, разделы:
 - "[Настройка VPN-соединения в Windows 2000/XP/2003](#)" на стр. 166
 - "[Настройка VPN-соединения в Windows 95/98/ME](#)" на стр. 167
3. Для серверов под управлением Windows 2000 и 2003 рекомендуется настроить VPN-подключение через службу "Маршрутизация и удаленный доступ".

Авторизация по PPPoE

Настройка PPPoE соединения производится через стандартный мастер создания сетевых подключений ОС, необходимо указать только логин и пароль.

Авторизация через Ideco Agent

Скопировать IdecoAgent.exe с локального сайта сервера в произвольный каталог. Однократно запустить, убедиться что подключение происходит успешно. При необходимости разрешить в Firewall компьютера 800 порт TCP.

На компьютере пользователя в настройках сетевой карты укажите в качестве шлюза и в качестве DNS локальный адрес Ideco ICS.

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 потребуются его установка на каждый компьютер. Подробнее см. "[Авторизация через программу агент – IdecoAgent](#)" на стр. 77

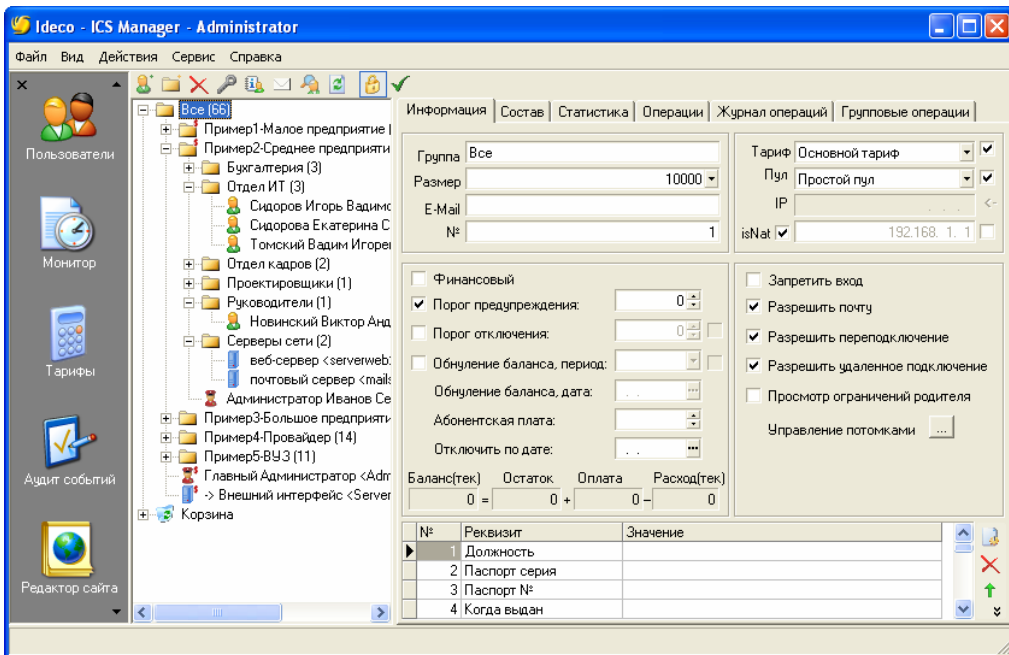
Глава 3. Администрирование (Ideco ICS Manager)

В этой главе содержится описание Ideco ICS Manager.

Ideco ICS Manager

Ideco ICS Manager – приложение под Windows для администрирования Ideco ICS, 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 ICS Manager позволяет управлять Ideco ICS не только опытным системным администраторам, но и обычным пользователям.



Установка Ideco ICS Manager

Системные требования

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

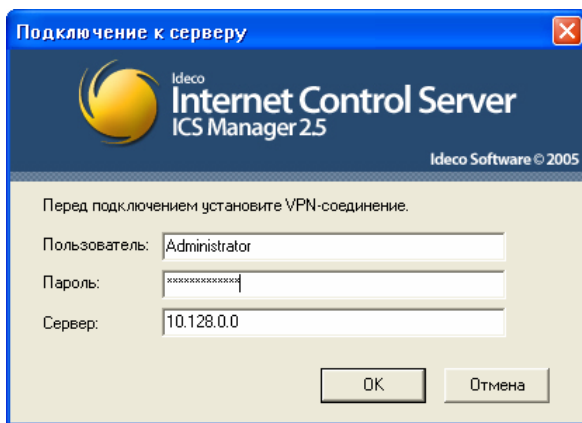
Установка

Ideco ICS Manager можно установить с компакт диска с дистрибутивом Ideco ICS:

1. Вставьте CD с дистрибутивом Ideco ICS, выберите пункт **Установка Ideco ICS Manager**, или вручную запустите файл **setup.exe** в каталоге **ICSManager** на установочном компакт-диске.
2. Следуйте инструкциям мастера.

Подключение к Ideco ICS

1. Установите VPN-соединение с сервером с логином администратора. Если VPN-соединение еще не установлено, то его сначала необходимо настроить и установить (подробнее см. "Авторизация пользователей на сервере Ideco ICS" на стр. 34).
2. Запустите Ideco ICS Manager. Появится следующее окно подключения:



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

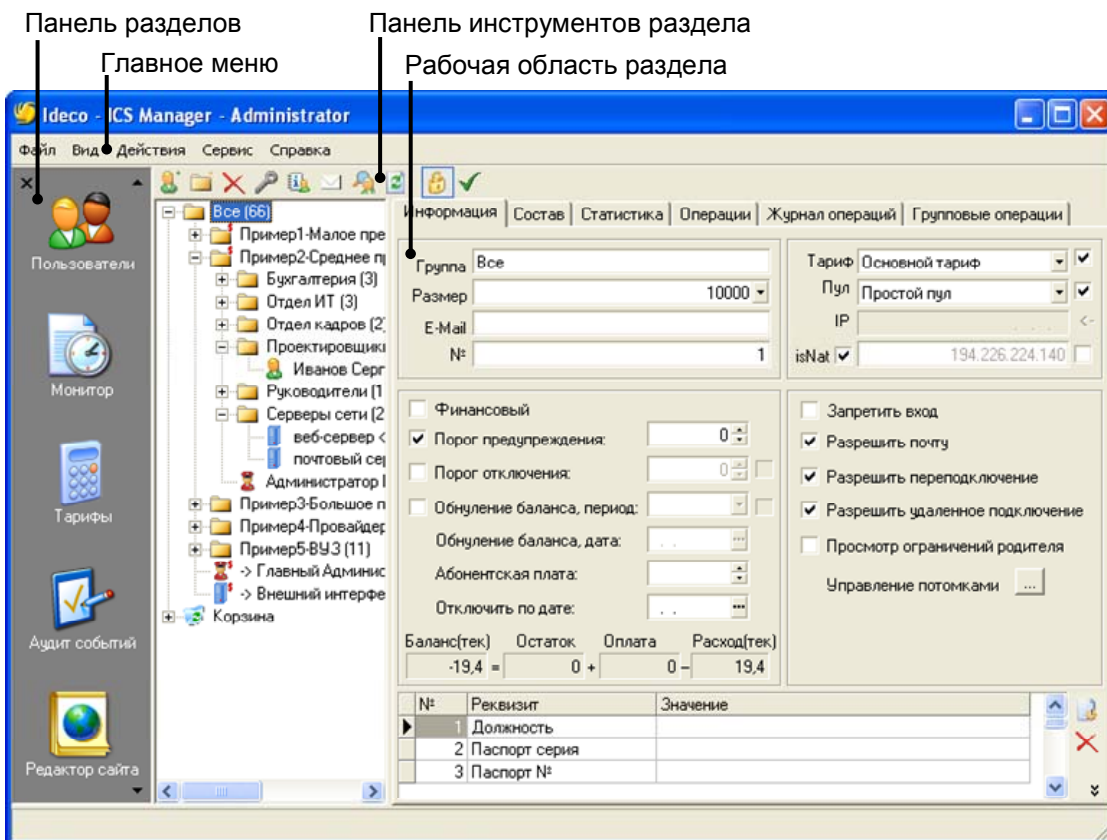
Замечания:

1. Перед подключением необходимо установить VPN-соединение с сервером Ideco ICS. В противном случае, подключение невозможно. Таким образом,

- обеспечивается защита передаваемых данных. VPN-соединение необходимо устанавливать под пользователем являющимся администратором.
2. Для подключения Ideco ICS Manager необходимо указать защищенный IP-адрес сервера (по умолчанию "10.128.0.0"). Обратите внимание, что это не адрес "10.0.0.1" к которому выполняется VPN-соединение.
 3. Для подключения используйте те же логин и пароль администратора, что и для установки VPN-соединения.
 4. Если Ideco ICS Manager запущен впервые после установки Ideco ICS, то в системе зарегистрирован только один администратор. Поэтому устанавливайте VPN-соединение и 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 ICS Manager – "10.128.0.0".
 5. Для работы Ideco ICS Manager используется TCP-порт **3050**. Поэтому, если на компьютере, с которого выполняется подключение, используется персональный Firewall, то в нем необходимо установить соответствующие разрешения.

Главное окно Ideco ICS Manager

Главное окно Ideco ICS Manager выглядит следующим образом:



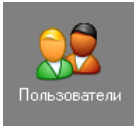


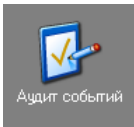
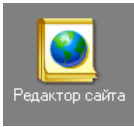
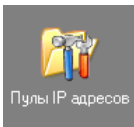

Главное окно Ideco ICS Manager состоит из следующих элементов:


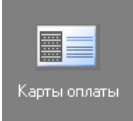
- **Панель разделов** расположена в левой части главного окна. Позволяет быстро переключаться между разделами с помощью соответствующих кнопок.
- **Главное меню.** Пункт меню "Действия" изменяется в зависимости от раздела, и содержит команды доступные в текущем разделе.
- **Панель инструментов раздела** 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	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	Монитор. Просмотр пользователей, которые подключены в настоящий момент.	Администратору группы показываются пользователи своей группы.
 Тарифы	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	Аудит событий. Просмотр действий и операций, которые были выполнены администраторами.	Администратор группы может видеть события только в своей группе.
 Редактор сайта	Редактор сайта. Позволяет редактировать информацию отображаемую в веб-интерфейсе пользователя: название организации, раздел "поддержка" и раздел "новости".	Раздел доступен только администраторам, находящимся в корневой группе.
 Пулы IP адресов	Пулы IP-адресов. Просмотр и редактирование пулов IP-адресов.	Раздел доступен только Главному администратору
 Firewall	Firewall. Управление встроенным Firewall.	Раздел доступен только Главному администратору

Раздел	Описание	Примечание
	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".

*Карты оплаты доступны только в версии в версии Enterprise Edition (подробнее см. "Отличия версий Ideco ICS" на стр. 14)

Администраторы

Администратор – пользователь, имеющий право управлять Ideco ICS через Ideco ICS 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 Ideco ICS. В дереве пользователей, в мониторе, в аудите событий и веб-интерфейсе 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](#)" на стр. 46 и "[Закладка "Информация" \(у пользователя\)](#)" на стр. 48).

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 использованием 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 версии 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**.

Управление пользователями

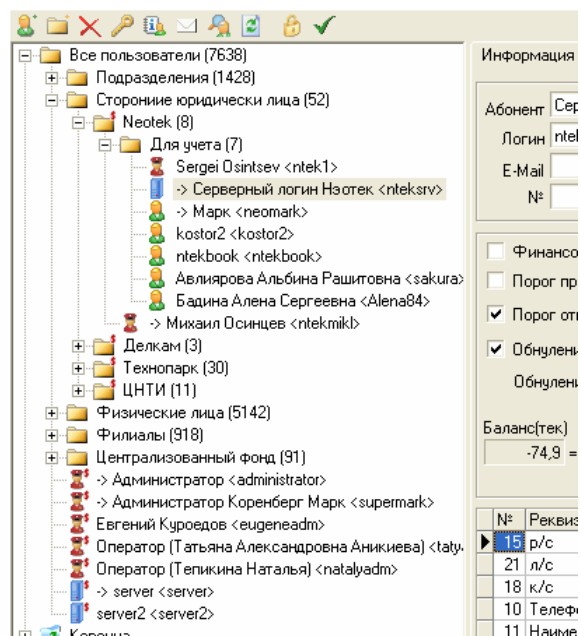
Дерево пользователей

Пользователи в Ideco ICS 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](#)" на стр. 65.



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"](#)" на стр. 65.



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

Ниже представлено описание кнопок Панели инструментов:



Создание нового пользователя. Подробнее см. "[Создание пользователя](#)" на стр. 46.



Создание новой группы. Подробнее см. "[Создание группы](#)" на стр. 46



Удаление пользователя или группы. Подробнее см. "[Удаление пользователей](#)" на стр. 68.



Восстановление пользователя или группы.



Смена пароля пользователя. Подробнее см. "[Смена пароля](#)" на стр. 72.



Проверка параметров пользователя и возможности пользователя выйти в Интернет. Подробнее см. "[Проверка пользователя](#)" на стр. 73



Отправить сообщение по e-mail и WinPopup. Подробнее см. "[Оповещение пользователей](#)" на стр. 74



Поиск пользователей. Подробнее см. "[Поиск пользователей](#)" на стр. 69.



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:

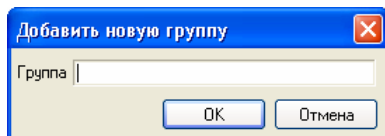
- ["Закладка "Информация" \(у пользователя\)"](#) на стр. 48
- ["Закладка "Информация" \(у группы\)"](#) на стр. 53
- ["Закладка "Статистика""](#) на стр. 59
- ["Закладка "Операции"](#) на стр. 61
- ["Закладка "Состав" \(у группы\)"](#) на стр. 62
- ["Закладка "Журнал операций"](#) на стр. 136
- ["Закладка "Групповые операции""](#) на стр. 137

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:



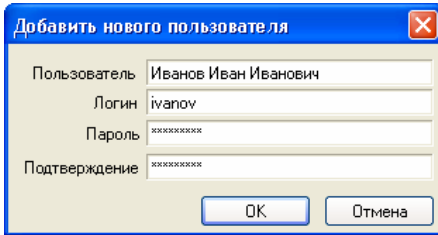
Заполните название новой группы пользователей. После создания группы, задайте остальные свойства группы на закладке "Информация" (подробнее см. ["Закладка "Информация" \(у группы\)"](#) на стр. 53).

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 ICS 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 веб-интерфейсе. В случае необходимости, администратор может сменить пароль.

Нажмите кнопку **ОК**. В текущей группе будет создан пользователь. При этом автоматически установлены следующие свойства:

1. **Тарифный план, адрес NAT, пул IP-адресов** унаследованы от родительской группы.
2. **IP-адрес** автоматически установлен из пула – выбирается первый не занятый IP-адрес в пуле.
3. 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" \(у пользователя\)](#)" на стр. 48).

Закладка "Информация" (у пользователя)

На закладке **Информация** отображаются параметры выбранного пользователя.

Информация | Статистика | Операции | Журнал операций

Абонент: Главный Администратор
 Логин: Administrator
 E-Mail:
 №:

Тариф: Основной тариф
 Пул: Простой пул
 IP: 10.128. 0. 57
 isNat: 194.226.224.140


Финансовый
 Порог предупреждения:
 Порог отключения:
 Формирование акта, период: Месяц
 Формирование акта, дата: 01.05.2006
 Абонентская плата:
 Отключить по дате:
 Баланс(тек) Остаток Оплата Расход(тек)
 -0,3 = 0 + 0 - 0,3

Запретить вход
 Включить почту
 Переадресовать почту
 Разрешить переподключение
 Разрешить удаленное подключение
 Просмотр ограничений родителя
 Администратор технический
 Администратор финансовый
 Администратор карт оплаты

№	Реквизит	Значение
1	Должность	
2	Паспорт серия	
3	Паспорт №	
4	Когда выдан	

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"](#) на стр. 49
- ["Параметры ограничений"](#) на стр. 50
- ["Параметры разрешений"](#) на стр. 52

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"](#) на стр. 137.

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**.

Общие параметры

Абонент	Иванов Иван Иванович	Тариф	Основной тариф	<input type="checkbox"/>
Логин	ivanov	Пул	Простой пул	<input type="checkbox"/>
E-Mail	ivanov@company.com	IP	10.128. 0. 1	<input type="checkbox"/>
№	222	isNat	<input checked="" type="checkbox"/> 192.168. 33. 4	<input type="checkbox"/>
		Вход по	Авторизация vpn pptp, pppoe	<input type="checkbox"/>

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:

1. 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.
2. Если у пользователя вручную установлен **Тарифный план**, то **Адрес NAT** по умолчанию ставится равным IP-адресу интерфейса указанного в тарифном плане.
 3. 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.
 4. 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**.

Параметры ограничений

<input type="checkbox"/>	Финансовый												
<input checked="" type="checkbox"/>	Порог предупреждения:	<input type="text" value="0"/>											
<input type="checkbox"/>	Порог отключения:	<input type="text" value="0"/> <input type="checkbox"/>											
<input type="checkbox"/>	Обнуление баланса, период:	<input type="text"/> <input type="checkbox"/>											
	Обнуление баланса, дата:	<input type="text" value=".."/>											
	Абонентская плата:	<input type="text"/>											
	Отключить по дате:	<input type="text" value=".."/>											
<table border="1"> <thead> <tr> <th>Баланс(тек)</th> <th>Остаток</th> <th>Оплата</th> <th>Расход(тек)</th> </tr> </thead> <tbody> <tr> <td><input type="text" value="0"/></td> <td>=</td> <td><input type="text" value="0"/></td> <td>+</td> <td><input type="text" value="0"/></td> <td>-</td> <td><input type="text" value="0"/></td> </tr> </tbody> </table>			Баланс(тек)	Остаток	Оплата	Расход(тек)	<input type="text" value="0"/>	=	<input type="text" value="0"/>	+	<input type="text" value="0"/>	-	<input type="text" value="0"/>
Баланс(тек)	Остаток	Оплата	Расход(тек)										
<input type="text" value="0"/>	=	<input type="text" value="0"/>	+	<input type="text" value="0"/>	-	<input type="text" value="0"/>							

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"](#)" на стр. 65.

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](#)" на стр. 74

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](#)" на стр. 63.

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](#)" на стр. 66.

У финансовых пользователей взамен "Обнуление баланса" есть функция "Формирование акта". Подробнее см. "[Автоматическое формирование акта](#)" на стр. 139.

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](#)" на стр. 63.

Замечания:

1. Как правило, признак **Финансовый** устанавливается у конечных пользователей только в случае, если предприятие оказывает услуги по доступу в Интернет физическим лицам.
2. 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.
3. 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**.

Параметры разрешений

<input type="checkbox"/>	Запретить вход
<input checked="" type="checkbox"/>	Включить почту
<input type="checkbox"/>	Переадресовать почту
<input checked="" type="checkbox"/>	Разрешить переподключение
<input checked="" type="checkbox"/>	Разрешить удаленное подключение
<input type="checkbox"/>	Просмотр ограничений родителя
<input checked="" type="checkbox"/>	Администратор технический
<input checked="" type="checkbox"/>	Администратор финансовый
<input checked="" type="checkbox"/>	Администратор карт оплаты

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 ICS Manager.

Включить почту

В случае если признак установлен, то пользователю автоматически создается почтовый ящик на сервере. Подробнее см. "[Использование почты](#)" на стр. 72.

В версии Standard Edition в качестве примера каждый пятый пользователь может иметь почтовый ящик, но не более 15-ти почтовых ящиков во всей системе (подробнее см. "[Отличия версий](#) Ideco ICS" на стр. 14).

Доступ к почте из Интернет

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. Подробнее см. "[Общие параметры](#)" на стр. 49 и "[Простая переадресация](#)" на стр 151

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. Простое соединение будет разорвано. Подробнее см. "[Переподключение](#)" на стр. 70.

Разрешить удаленное подключение

Означает возможность VPN подключения к внешнему адресу Ideco ICS. Например, в случае нахождения пользователя дома или в командировке. Подробнее см. "[Удаленное подключение](#)" на стр. 70.

Просмотр ограничения родителя

Разрешить пользователю просматривать ближайшее ограничение вышестоящих групп. "[Страница "Информация"](#)" на стр. 125

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](#)" на стр. 42.

Администратор карт оплаты

Пользователь сможет управлять картами оплаты. Доступно только в версии Enterprise Edition (подробнее см. "[Отличия версий Ideco ICS](#)" на стр. 14)

LDAP/AD-пользователь

Этот пользователь синхронизируется с доменом Windows. То есть 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.

Закладка "Информация" (у группы)

На закладке информация отображаются свойства группы выбранной в дереве пользователей.

Информация		Состав	Статистика	Операции	Журнал операций	Групповые операции		
Группа	Все					Тариф	Основной тариф	<input checked="" type="checkbox"/>
Размер	10000					Пул	Простой пул	<input checked="" type="checkbox"/>
E-Mail						IP		<-
№	1					isNat	<input checked="" type="checkbox"/>	192.168. 1. 1 <input type="checkbox"/>
<input type="checkbox"/> Финансовый						<input type="checkbox"/> Запретить вход		
<input checked="" type="checkbox"/> Порог предупреждения:	0					<input checked="" type="checkbox"/> Разрешить почту		
<input type="checkbox"/> Порог отключения:	0					<input checked="" type="checkbox"/> Разрешить переподключение		
<input type="checkbox"/> Обнуление баланса, период:						<input checked="" type="checkbox"/> Разрешить удаленное подключение		
Обнуление баланса, дата:						<input type="checkbox"/> Просмотр ограничений родителя		
Абонентская плата:						Управление потомками ...		
Отключить по дате:								
Баланс(тек)	Остаток	Оплата	Расход(тек)					
0 =	0 +	0 -	0					
№	Реквизит	Значение						
1	Должность							
2	Паспорт серия							
3	Паспорт №							
4	Когда выдан							


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](#)" на стр. 55
- "[Параметры ограничений](#)" на стр. 55
- "[Параметры разрешений](#)" на стр. 57
- "[Управление потомками](#)" на стр. 58

Внизу закладки Информация отображается таблица с **реквизитами**. Подробнее см. "[Реквизиты пользователя и группы](#)" на стр. 138.

После изменения свойств группы нажмите кнопку  **Сохранить** на панели инструментов.

Замечание: При сохранении некоторых свойств группы, соединения, установленные пользователями этой группы могут отключиться.

Общие параметры

Группа	Бухгалтерия	Тариф	Основной тариф
Размер	10	Пул	Простой пул
E-Mail		IP	0. 0. 0. 0
№	18	isNat	<input checked="" type="checkbox"/> 192.168. 33. 4
		Вход по	Авторизация vpn pptp, pppoe

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.

Параметры ограничений

<input type="checkbox"/>	Финансовый		
<input checked="" type="checkbox"/>	Порог предупреждения:	0	
<input type="checkbox"/>	Порог отключения:	0	
<input type="checkbox"/>	Обнуление баланса, период:		
	Обнуление баланса, дата:	
	Абонентская плата:		
	Отключить по дате:	
Баланс(тек)	Остаток	Оплата	Расход(тек)
0 =	0 +	0 -	0

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"](#) на стр. 65.

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"](#) на стр. 63.

Автоматическое обнуление баланса

Эта функция доступна только у нефинансовых групп. Позволяет с заданной периодичностью обнулять баланс группы. При этом поля остаток, расход и оплата обнуляются. Подробнее об использовании этой возможности см.

["Автоматическое обнуление баланса"](#) на стр. 66.

У финансовых групп вместо "Обнуления баланса" есть функция "Формирование акта". Подробнее см. ["Автоматическое формирование акта"](#) на стр. 139.

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"](#) на стр. 63.

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".

Параметры разрешений

Запретить вход
 Разрешить почту
 Разрешить переподключение
 Разрешить удаленное подключение
 Просмотр ограничений родителя
 Управление потоками ...

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](#)" на стр. 70
- "[Удаленное подключение](#)" на стр. 70
- "[Использование почты](#)" на стр. 72

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

Настройка синхронизации с LDAP/AD сервером

IP адрес сервера LDAP/AD

Имя домена

LDAP группа

Windows группа

Пользователь (binddn)

Пароль пользователя

Включить сервер в домен

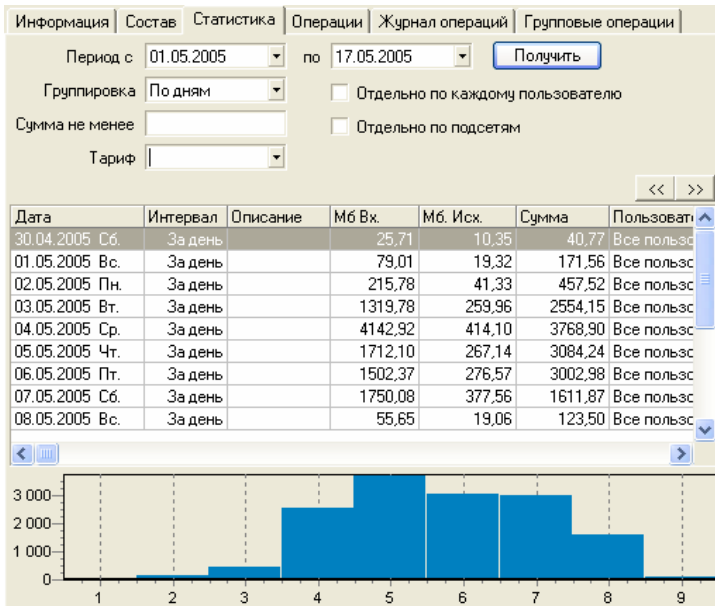
Запрос(basedn)

Фильтр

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.

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:

1. 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.

2. 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:

1. В Ideco ICS 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 (подробнее см. ["Глава 5. Веб-интерфейс пользователя"](#) на стр. 122.)
2. При выводе статистики учитывается незакрытые сессии пользователей, то есть сессии установленные в текущий момент.
 3. 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.
 4. **Основная статистика**, а также **Детализированная статистика** доступны в веб-интерфейсе пользователям. При этом пользователи могут посмотреть только свою статистику, а администраторы могут посмотреть статистику по всем пользователям своей группы. Подробнее см. ["Глава 5. Веб-интерфейс пользователя"](#) на стр. 122.

Закладка "Операции"

Ideco ICS 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 см. ["Глава 7. Дополнительные возможности Ideco ICS"](#) на стр. 132, разделы

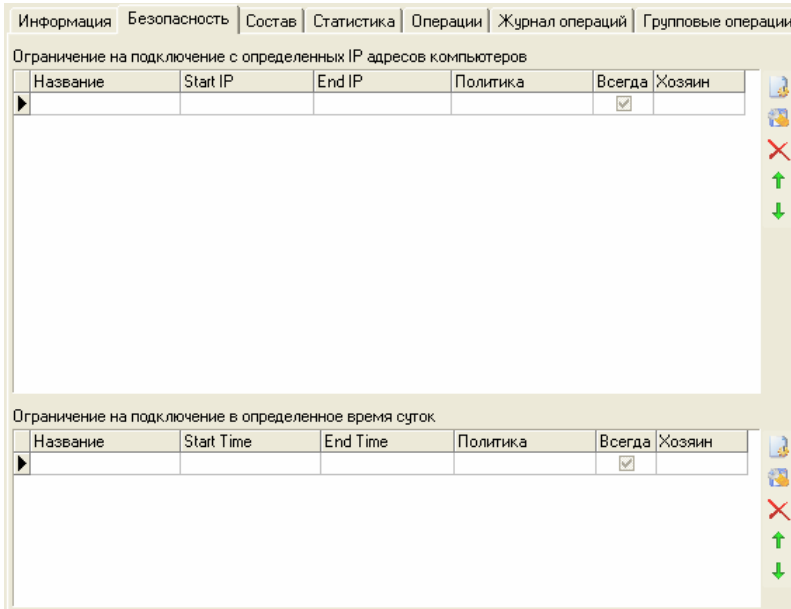
- ["Операции"](#) на стр. 132
- ["Закладка "Операции" "](#) на стр. 132
- ["Закладка "Журнал операций"](#) на стр. 136
- ["Закладка "Групповые операции" "](#) на стр. 137
- ["Реквизиты пользователя и группы"](#) на стр. 138
- ["Автоматическое формирование акта"](#) на стр. 139
- ["Шаблоны документов"](#) на стр. 141

Закладка "Состав" (у группы)

Информация	Состав	Статистика	Операции	Журнал операций	Групповые операции
N°	Наименование	Логин	Баланс	Неограничен	Фин.
▶ 259	Карпов В.М.	karvm	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
743	Карташов Вадим Викторович	h20dvz	-296,6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
457	Карфидова Надежда Сергеевна	naduha	-2	<input type="checkbox"/>	<input type="checkbox"/>
458	Карфидова Татьяна Николаевна	tanuha	-90,1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
377	Кассандров И.Н.	kass	0	<input type="checkbox"/>	<input type="checkbox"/>
751	Катаев Рудольф Федорович	250539	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
550	Катаева Н.Н.	katan	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
769	Кашкаров Александр Венедиктович	kwint	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
375	Кеда О.А.	keda	0	<input type="checkbox"/>	<input type="checkbox"/>
770	Кийко Валерий Васильевич	kiyko	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
427	Кириллов А.В.	kirilloff	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
514	Кирсанов Ю.Г.	kirsy	-37,6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
616	Кислов Алексей Николаевич	kislov	-37,1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
376	Клименко В.А.	kva	-16	<input checked="" type="checkbox"/>	<input type="checkbox"/>
378	Колмогорова Н.В.	kolm	0	<input type="checkbox"/>	<input type="checkbox"/>
343	Колобова А. В.	kolobova	0	<input type="checkbox"/>	<input type="checkbox"/>
321	Комп 29	29	0	<input type="checkbox"/>	<input type="checkbox"/>
322	Комп 30	30	0	<input type="checkbox"/>	<input type="checkbox"/>
381	Кондратьев В.В.	kondratev	0	<input type="checkbox"/>	<input type="checkbox"/>
655	Кондрашкина Наталья Николаевна	kondr	-17,9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
618	Конев Сергей Федорович	konev	-10,3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
601	Кононов Ю.А.	kononov	-48	<input checked="" type="checkbox"/>	<input type="checkbox"/>
341	Консультант	cons1	0	<input type="checkbox"/>	<input type="checkbox"/>
574	Копорущкин Павел	koporushkin	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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**.

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.

Баланс пользователя и группы, порог отключения

Баланс(тек)	Остаток	Оплата	Расход(тек)
3000 =	3500 +	1500 -	2000

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.

Баланс(тек.)	Остаток	Оплата	Расход(тек.)
-325	= 0	+ 0	- 325

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.

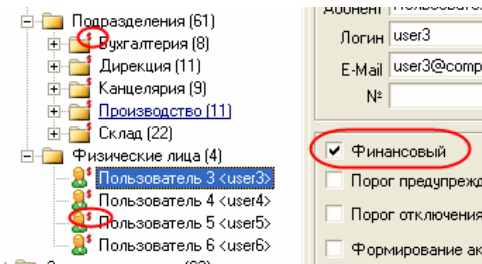
В конце месяца для финансовых пользователей рекомендуется проводить подведение баланса (списание дебета в "остаток на начало периода").

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".

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.

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.

Тариф: Тарифный план №1
 Пул: Первый пул
 IP: 10.129.0.3
 isNat: 195.195.195.195

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 ICS.

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.

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.

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:


The screenshot shows a dialog box with the following fields:

- Финансовый
- Порог предупреждения: []
- Порог отключения: -500
- Обнуление баланса, период: Месяц
- Обнуление баланса, дата: 01.07.2005

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 .

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 обнуляться: 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 подводится 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**.


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.

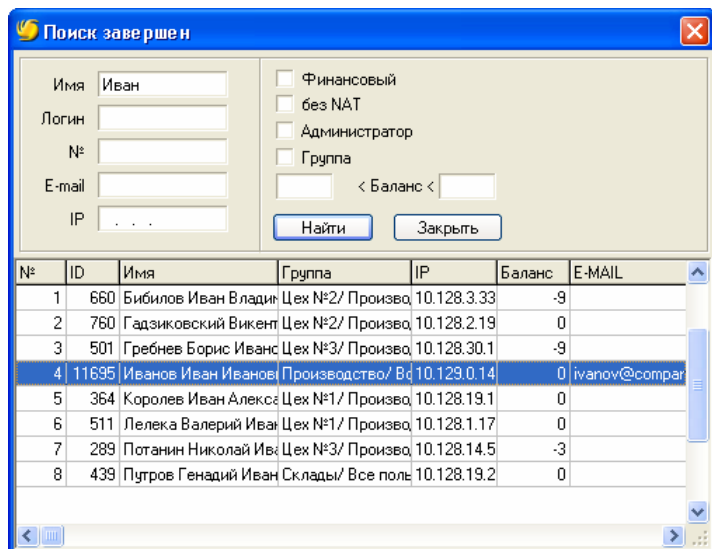
Замечания:

1. Удаление группы пользователей аналогично удалению пользователей. При этом вся группа перемещается в **Корзину**.

- При проведении операции "Закрытие периода" производится окончательное удаление пользователей и их статистики из БД.
- Параметры удаленного пользователя сменить нельзя.
- Для восстановления пользователя или группы, выберите нужного пользователя или группу в **Корзине** и нажмите кнопку  **Восстановить**.
- В Ideco ICS 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.
- Удаление пользователя не влияет на значение баланса вышележащих групп.

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**.



The screenshot shows a window titled "Поиск завершён" (Search completed) with a search criteria form and a table of results.

Search Criteria:

- Имя: Иван
- Логин: (empty)
- №: (empty)
- E-mail: (empty)
- IP: (empty)
- Финансовый:
- без NAT:
- Администратор:
- Группа: (empty)
- Баланс: < (empty) > (empty)

Buttons: Найти, Закрыть

Table of Results:

№	ID	Имя	Группа	IP	Баланс	E-MAIL
1	660	Бибилов Иван Владим	Цех №2/ Произво	10.128.3.33	-9	
2	760	Гадзиковский Викент	Цех №2/ Произво	10.128.2.19	0	
3	501	Гребнев Борис Иванс	Цех №3/ Произво	10.128.30.1	-9	
4	11695	Иванов Иван Иванович	Производство/ Вс	10.129.0.14	0	ivanov@compar
5	364	Королев Иван Алекс	Цех №1/ Произво	10.128.19.1	0	
6	511	Лелека Валерий Иван	Цех №1/ Произво	10.128.1.17	0	
7	289	Потанин Николай Ив	Цех №3/ Произво	10.128.14.5	-3	
8	439	Путров Геннадий Иван	Склады/ Все поле	10.128.19.2	0	

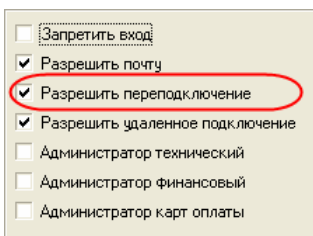
Задайте нужные параметры поиска и нажмите кнопку **Найти**.

Будет выведен список пользователей удовлетворяющих условиям поиска.

Для перехода к нужному пользователю в дереве пользователей выполните двойной щелчок мышкой на нужном пользователе. При этом окно поиска закроется.

Можно не закрывая окно поиска просматривать информацию по пользователям. Для этого можно перемещаться по результатам поиска и информация на закладках **Информация**, **Операции**, **Статистика** будут отображаться для текущего пользователя.

Переподключение



Запретить вход
 Разрешить почту
 Разрешить переподключение
 Разрешить удаленное подключение
 Администратор технический
 Администратор финансовый
 Администратор карт оплаты

Свойство пользователя **Разрешить переподключение** означает возможность пользователя установить соединения с сервером Ideco ICS, 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.

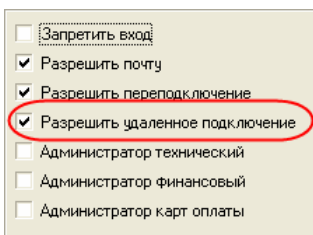
Рекомендуется использовать для пользователей, которые могут подключаться к Ideco ICS с разных компьютеров.

Замечания:

Свойство **Разрешить переподключение** устанавливается отдельно для каждого пользователя. Подробнее см. пункт "[Параметры разрешений](#)" на стр. 52 в разделе [Закладка "Информация" \(у пользователя\)](#).

На возможность администратора группы устанавливать своим пользователям это разрешение влияют соответствующие установки в свойствах группы. Подробнее см. пункт "[Параметры разрешений](#)" на стр. 57 в разделе [Закладка "Информация" \(у группы\)](#).

Удаленное подключение



Запретить вход
 Разрешить почту
 Разрешить переподключение
 Разрешить удаленное подключение
 Администратор технический
 Администратор финансовый
 Администратор карт оплаты

Свойство пользователя **Разрешить удаленное подключение** означает возможность пользователя подключиться к внешнему адресу Ideco ICS, 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](#)" на стр. 52 в разделе [Закладка "Информация" \(у пользователя\)](#).

На возможность администратора группы устанавливать своим пользователям это разрешение влияют соответствующие установки в свойствах группы. Подробнее см. пункт "[Параметры разрешений](#)" на стр. 57 в разделе [Закладка "Информация" \(у группы\)](#).

В Ideco ICS 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](#)" на стр. 105 в разделе "[Конфигурирование сервера](#)".

Особенности работы

Для использования удаленного подключения, нужно обратить внимание на следующие особенности, и по возможности информировать о них пользователей.

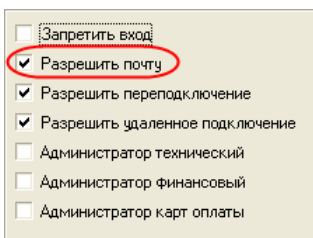
1. При удаленном подключении используется внешний (реальный) IP-адрес Ideco ICS. В то время как для обычного подключения из сети предприятия, как правило, используется внутренний IP-адрес Ideco ICS. Поэтому пользователям нужно сообщить внешний IP-адрес, а также уточнить, что уже настроенное соединение для работы из сети предприятия, например, на ноутбуке, не будет работать извне. Файл автоматической настройки соединения, находящийся в веб-интерфейсе, также настраивает соединение для работы только с внутренним IP-адресом.
2. Веб-интерфейс пользователя содержит инструкции по настройке VPN-соединения. При этом веб-интерфейс 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 веб-интерфейса.

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".

Использование почты

При установке флажка **Разрешить почту**, для пользователя создается почтовый ящик.



The screenshot shows a list of configuration options for a user. The first option is 'Запретить вход' (Disallow login) with an unchecked checkbox. The second option is 'Разрешить почту' (Allow mail) with a checked checkbox, which is circled in red. The third option is 'Разрешить переподключение' (Allow reconnection) with a checked checkbox. The fourth option is 'Разрешить удаленное подключение' (Allow remote connection) with a checked checkbox. The fifth option is 'Администратор технический' (Technical administrator) with an unchecked checkbox. The sixth option is 'Администратор финансовый' (Financial administrator) with an unchecked checkbox. The seventh option is 'Администратор карт оплаты' (Payment card administrator) with an unchecked checkbox.


Важно: Для использования почты необходимо в локальном интерфейсе установить параметр **Разрешить почту** и указать ваш почтовый домен. Подробнее см. "[Почтовый сервер](#)" на стр. 110

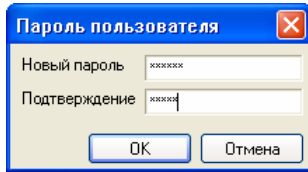
Подробнее о работе с почтой см. раздел "[Электронная почта](#)" на стр. 150.

Смена пароля

Пользователи могут самостоятельно изменять свои пароли в веб-интерфейсе. Если он забыл свой пароль то восстановить его нельзя, в этом случае сменить его может только администратор.

Для того что бы сменить пароль пользователя:

1. Выберите пользователя.
2. Нажмите кнопку  **Пароль** на панели инструментов, или Щелкните правой кнопкой мышки на пользователи и выберите пункт **Пароль**.
3. Появится следующее окно:




4. Введите пароль и подтверждение.

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:

1. 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**.
2. 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"

Оповещение пользователей

Idec ICS 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 Idec ICS, например, в случае переполнения жесткого диска, высылается сообщение **Главному администратору**.

Способ доставки

Сообщения пользователям могут доставляться по e-mail, по winpopup, а также пользователь может их посмотреть в веб-интерфейсе.


Для того чтобы задать способ доставки сообщений или отключить доставку сообщений:

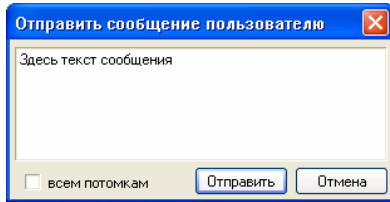
1. Выберите пункт меню **Сервис > Настройки**.
2. В появившемся окне выберите значение параметра **Оповещение пользователей**. Возможны три варианта:
 - Отключено
 - По e-mail
 - По e-mail и winpopup
3. Нажмите кнопку **ОК**.

Замечание: Сообщения в веб-интерфейс пользователя доставляются всегда, вне зависимости от вышеуказанных установок.

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".

Настройка синхронизации Ideco ICS с Active Directory или LDAP сервером

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»
2. Произвести мягкую перезагрузку
3. Подключиться с помощью ICS Manager к серверу
4. Создать новую группу пользователей. В параметрах группы установить флажок "Синхронизация с LDAP/AD".
5. Установить способ авторизации
6. Нажать на кнопку "Значения по умолчанию ..." и установить параметры, которые будут применены к создаваемым пользователям.

7. 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".
 - "Пользователь" и "пароль пользователя" – указать логин и пароль для подключения к LDAP серверу. От имени этого пользователя должна быть доступна на чтение "LDAP группа"
 - Нажать на кнопку "Проверить". Будет произведено тестовое подключение к серверу и проверка пароля.
 - Нажать ОК.
8. 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.
9. Настроить параметры пользователей, если это требуется.

Авторизация через программу агент – IdecoAgent

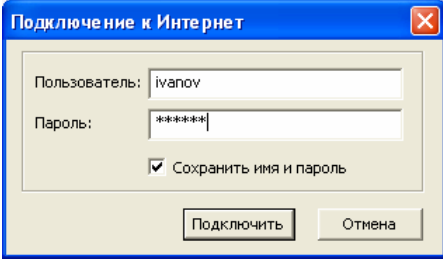
Для пользователей, у которых установлен способ авторизации "IdecoAgent" либо "IdecoAgent+IP" авторизация через программу агент позволит получить доступ в Интернет. Доступ будет обеспечен только в то время, когда пользователь авторизован с помощью этой программы.

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.

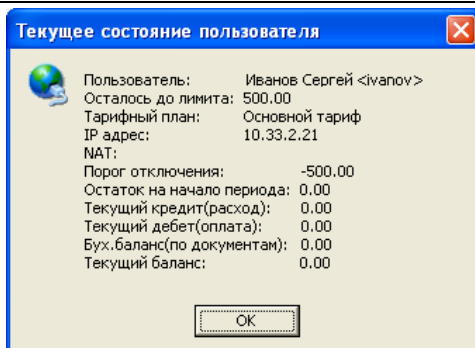
Для авторизации с помощью программы-агента необходимо с локального веб-сайта загрузить программу авторизации и сохранить ее в произвольный каталог. После запуска программы необходимо ввести логин и пароль пользователя. Состояние авторизации отображается иконкой в системном лотке. Возможные состояния:

-  – 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 отключения и т.д.

Пункт меню	Значение
------------	----------

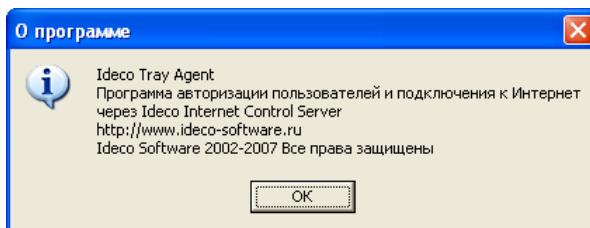


Запускаться при входе в систему

Установить автоматический запуск программы при входе в Windows.

О программе

Вывод информации о программе авторизации.



Рекомендации и замечания по работе с Ideco ICS Manager

В этом разделе содержатся рекомендации и замечания по работе Ideco ICS Manager, которые не вошли в другие разделы.


Интерфейс Ideco ICS Manager

1. Для ввода IP-адресов можно использовать копирование-вставку.

Поля для ввода IP-адресов используются в интерфейсе Ideco ICS 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 ICS 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 ICS 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 курсор 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.

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 ICS. 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.

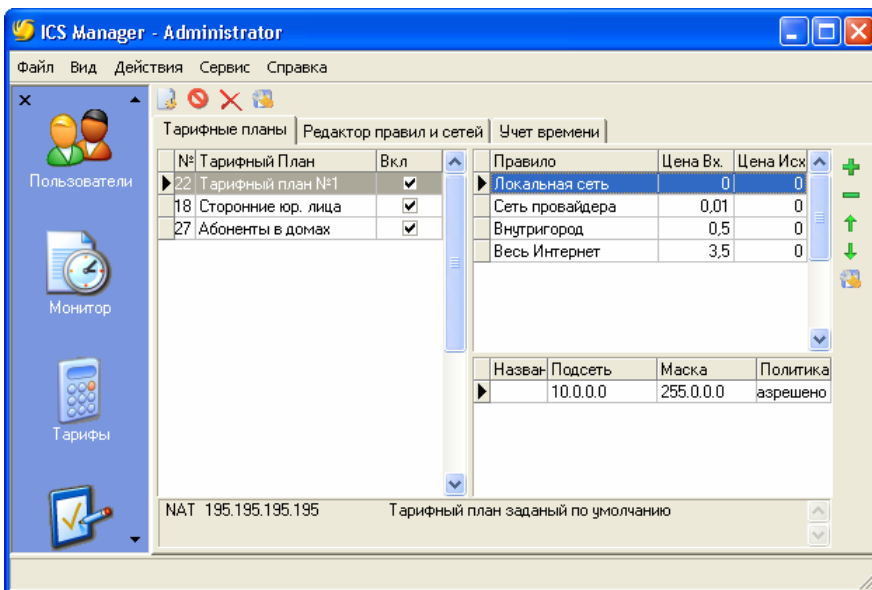
При подключении с чужих компьютеров следует иметь в виду, что на них может быть установлен клавиатурный шпион (Keylogger) и набранные пароли могут быть перехвачены злоумышленником.

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.

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 ICS 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.

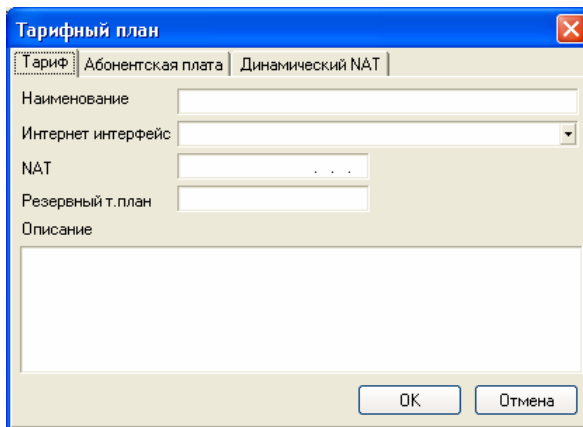
4. При редактировании тарифного плана, все соединения от пользователей подключенных на этот тарифный план разрываются.
5. В небольших организациях, как правило, используется один тарифный план. Использовать несколько тарифных планов целесообразно только в том случае, если для разных пользователей необходимо тарифицировать трафик по разным ценам. А также если используется возможность закрытия части ресурсов предприятия с использованием тарифных планов (подробнее см. "[Создание закрытых ресурсов](#)" на стр. 85).

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

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. При необходимости установите диапазон адресов NAT, которые будут выдаваться пользователям.

5. Нажмите кнопку **ОК**.
6. Теперь нужно добавить в тарифный план правила и указать стоимость.

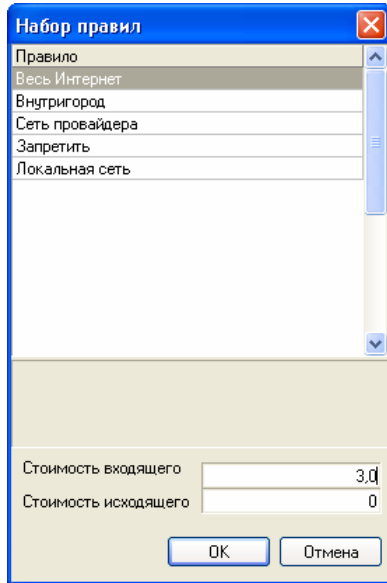
Добавление правил в тарифный план

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 **ОК**.



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](#)" на стр. 83.

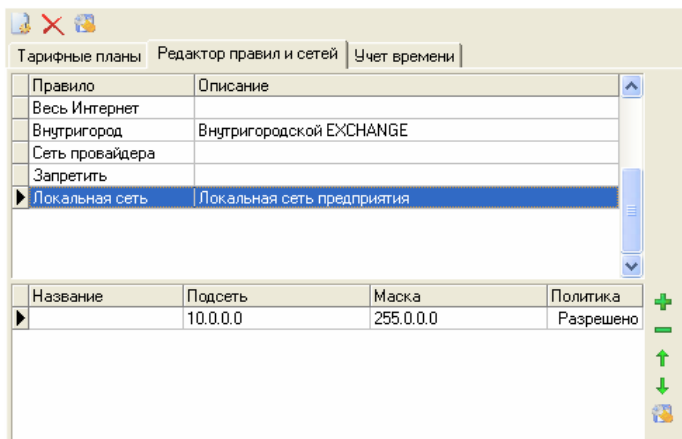
Обратите внимание, что:

- 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.

Редактор правил и сетей

Правила используются в тарифных планах. Правило в свою очередь состоит из списка сетей с указанием политики.

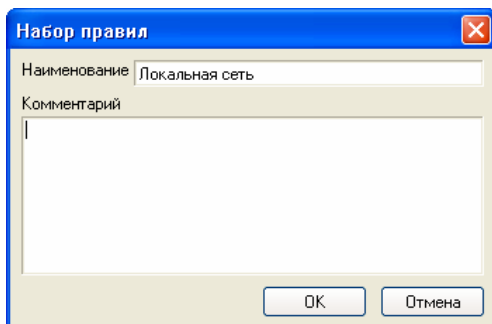
Для редактирования правил нажмите в разделе **Тарифные планы** на вкладку **Редактор правил и сетей**.




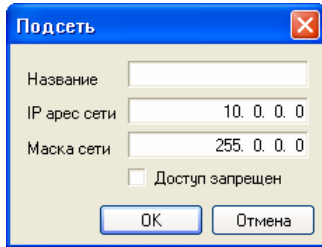
В таблице показаны все имеющиеся правила, а в нижней таблице все сети этого правила.

Для создания нового правила:

1. Нажмите кнопку  **Создать новое правило** на панели инструментов.



2. В появившемся окне введите название правила и описание. Нажмите кнопку **ОК**.
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**.

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 один 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](#)" на стр. 85.

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:

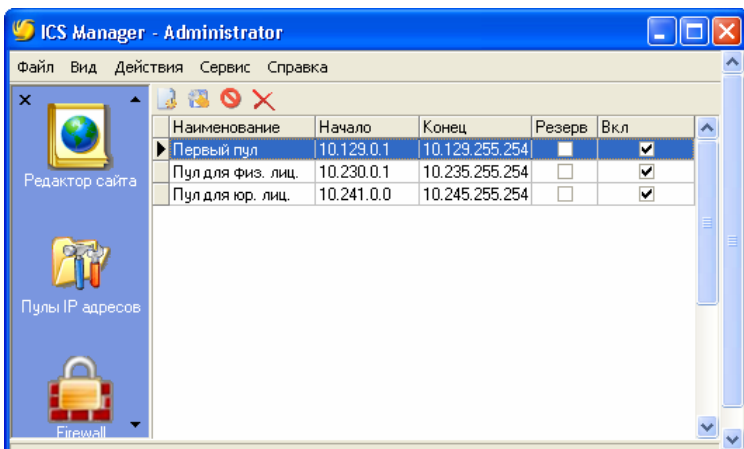
1. В тарифном плане назначаемом пользователя определить подсети доступ к которым должен быть закрыт и установить у них политику **Запрещено**. Этот тарифный план использовать для пользователей, которым должен быть закрыт доступ к указанным ресурсам. А в другом тарифном плане для этих подсетей установить 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 ICS. 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 ICS. Более развитые возможности по созданию закрытых ресурсов предоставляет встроенный Firewall (доступен только в версии Enterprise Edition). Подробнее см. "[Встроенный Firewall](#)" на стр. 157.

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 ICS.

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**.

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", то есть 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.

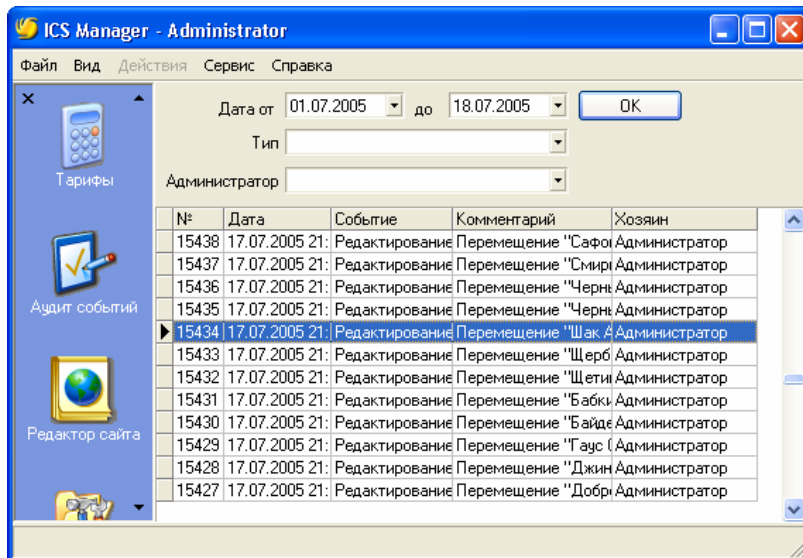
Включен – если признак не установлен, то пользователи, у которых установлен данный пул, не смогут выйти в Интернет.

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.

Аудит событий

Операции администраторов в Ideco ICS 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.

Монитор

Показывает список подключенных в настоящий момент пользователей.

IP-абонента – адрес пользователя, выдаваемый при VPN-соединении.

IP-компьютера – физический адрес компьютера

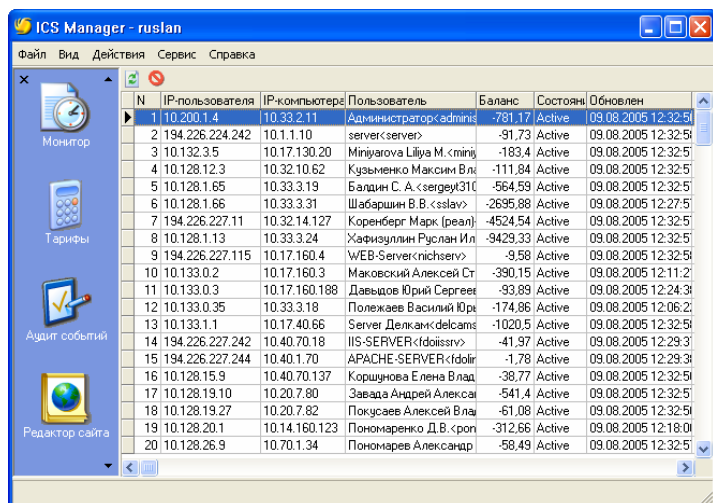
Пользователь – название пользователя

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



N	IP-пользователя	IP-компьютера	Пользователь	Баланс	Состояние	Обновлен
1	10.200.1.4	10.33.2.11	Администратор<admini>	-781.17	Active	09.08.2005 12:32:51
2	194.226.224.242	10.1.1.10	server<server>	-91.73	Active	09.08.2005 12:32:51
3	10.132.3.5	10.17.130.20	Minjugaova Liliya M. <minj>	-183.4	Active	09.08.2005 12:32:51
4	10.128.12.3	10.32.10.62	Кузьменко Максим Вла<	-111.84	Active	09.08.2005 12:32:51
5	10.128.1.65	10.33.3.19	Балдин С. А. <sergey310>	-564.59	Active	09.08.2005 12:32:51
6	10.128.1.66	10.33.3.31	Шабаршин В. В. <sslav>	-2695.88	Active	09.08.2005 12:27:51
7	194.226.227.11	10.32.14.127	Коренберг Марк (реал)	-4524.54	Active	09.08.2005 12:32:51
8	10.128.1.13	10.33.3.24	Хафизуллин Руслан Ил<	-9429.33	Active	09.08.2005 12:32:51
9	194.226.227.115	10.17.160.4	WEB-SERVER<nichserv>	-9.58	Active	09.08.2005 12:32:51
10	10.133.0.2	10.17.160.3	Маковский Алексей Ст<	-390.15	Active	09.08.2005 12:11:21
11	10.133.0.3	10.17.160.188	Давыдов Юрий Сергее<	-93.89	Active	09.08.2005 12:24:31
12	10.133.0.35	10.33.3.18	Полежаев Василий Юри<	-174.86	Active	09.08.2005 12:06:21
13	10.133.1.1	10.17.40.66	Server Делкан<delcanc>	-1020.5	Active	09.08.2005 12:32:51
14	194.226.227.242	10.40.70.18	IIS-SERVER<idoisrv>	-41.97	Active	09.08.2005 12:29:31
15	194.226.227.244	10.40.1.70	APACHE-SERVER<idolir>	-1.78	Active	09.08.2005 12:29:31
16	10.128.15.9	10.40.70.137	Коршунова Елена Влад<	-38.77	Active	09.08.2005 12:32:51
17	10.128.19.10	10.20.7.80	Завада Андрей Алексее<	-541.4	Active	09.08.2005 12:32:51
18	10.128.19.27	10.20.7.82	Покусаев Алексей Влад<	-61.08	Active	09.08.2005 12:32:51
19	10.128.20.1	10.14.160.123	Пономаренко Д.В. <ron>	-312.66	Active	09.08.2005 12:18:01
20	10.128.26.9	10.70.1.34	Пономарев Александр	-58.49	Active	09.08.2005 12:32:51

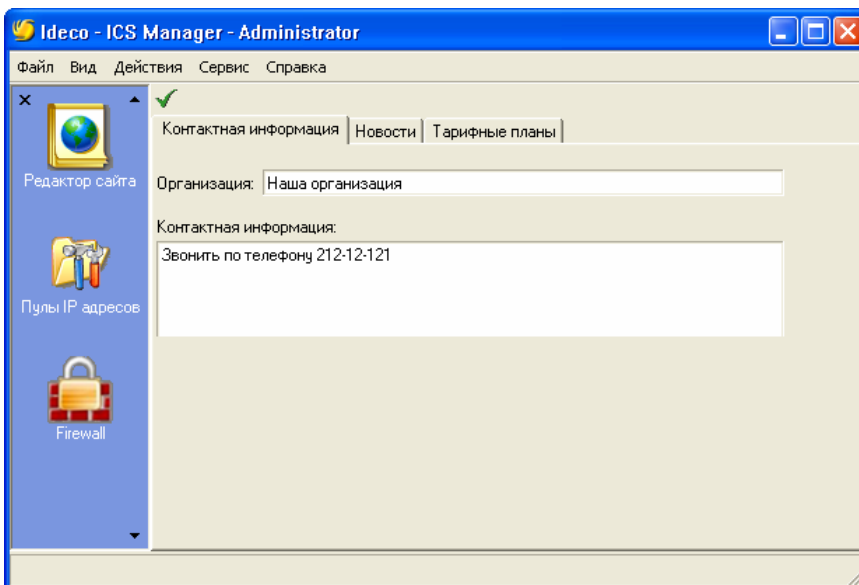
Редактор сайта

В разделе **Редактор сайта** редактируется информация, отображаемая в веб-интерфейсе пользователя.

Контактная информация

Организация – отображается в заголовке всех страниц веб-интерфейса. 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" веб-интерфейса 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".

Замечания:

При редактировании контактной информации и содержания новостей можно использовать форматирование HTML. При этом все тэги HTML должны быть обязательно закрыты. Например, "..." или так
.

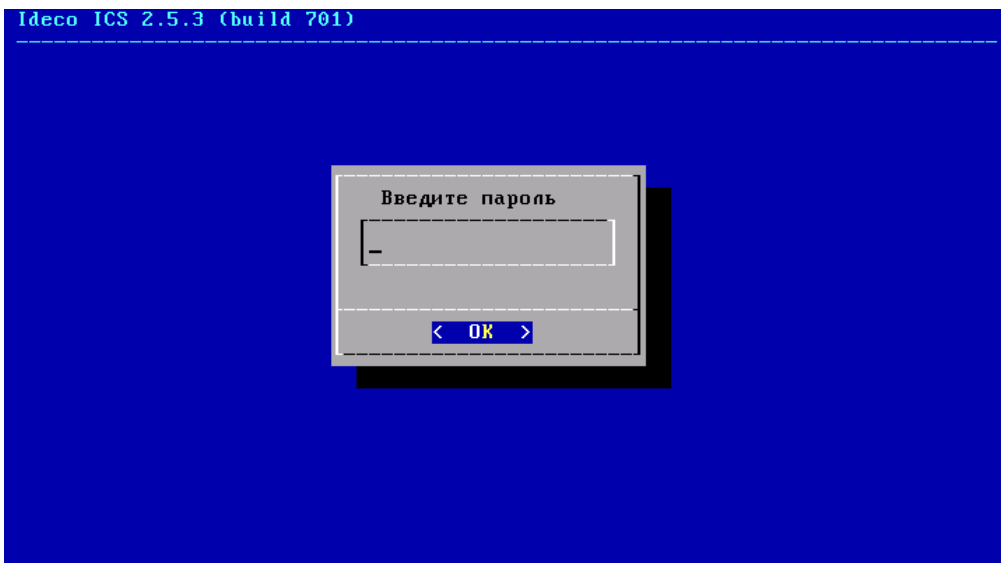
После редактирования информации в этом разделе обязательно проверьте правильность ее отображения в веб-интерфейсе пользователя.

Редактировать данные могут только администраторы, находящиеся в корневой группе.

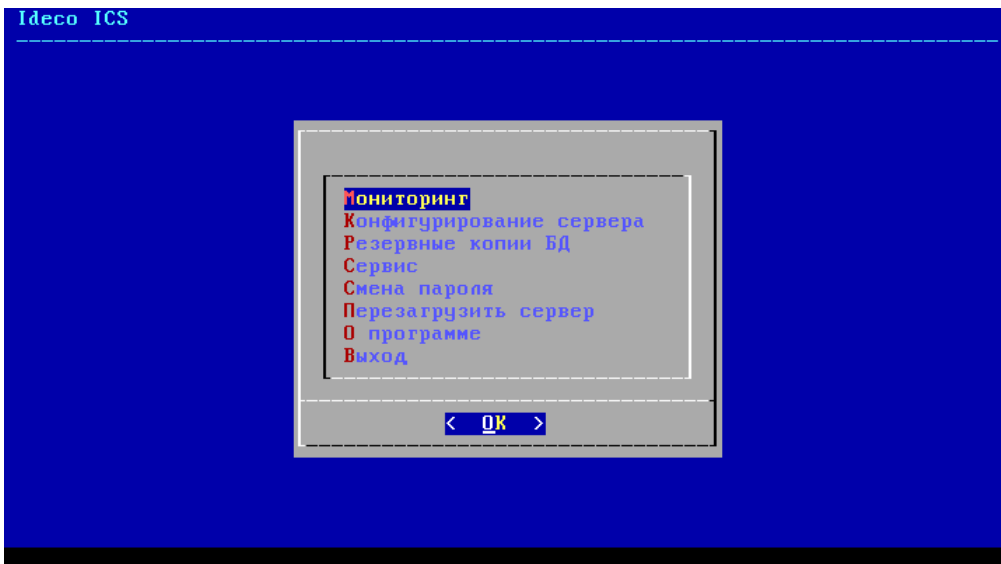
Глава 4. Локальная консоль сервера

Локальная консоль сервера предназначена для задания глобальных параметров сервера Ideco ICS 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 посмотреть текущее состояние сервера, перезагрузить систему и другое.

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



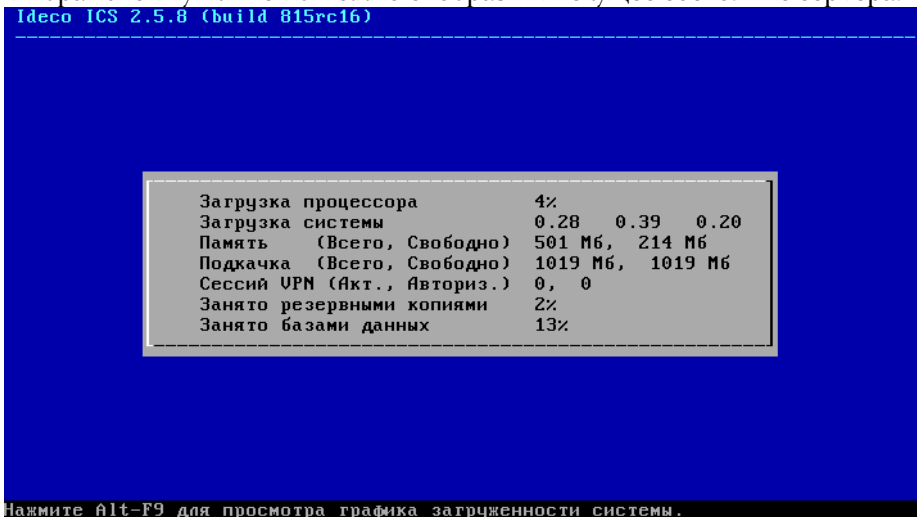
Пароль по умолчанию – **servicemode**. После ввода пароля доступно главное меню конфигурирования сервера.



Примечание: Доступ к локальной консоли можно получить удаленно, если заранее в ней включить параметр "Разрешить управление файлами по SSH". Подробнее см. "[Безопасность](#)" на стр. 105

Мониторинг

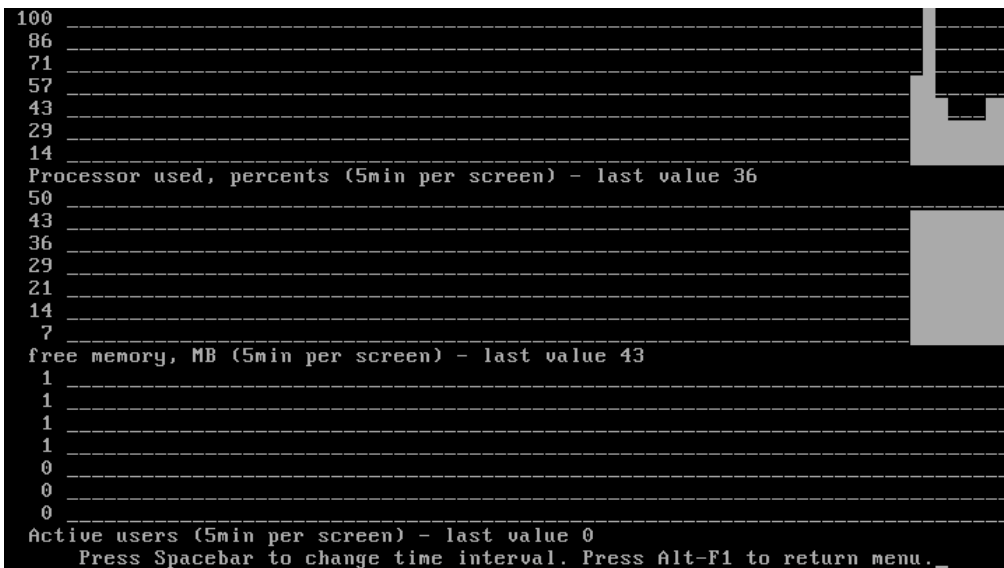
Выбрав этот пункт меню можно отобразить текущее состояние сервера:



- Загрузка процессора

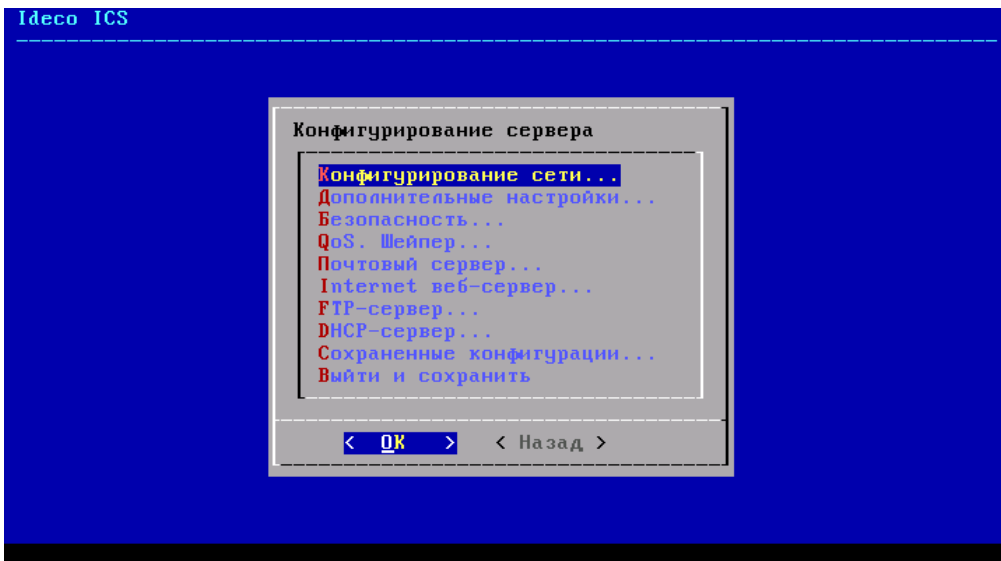
- Загруженность самой системы (за последнюю минуту, 5 минут и 15 минут соответственно)
- Загруженность памяти
- Загруженность раздела подкачки
- Количество подключенных пользователей (активных и подключающихся)
- Занятость диска для БД и диска для резервных копий

Просмотреть временную диаграмму загруженности сервера в реальном времени можно, нажав Alt-F9:



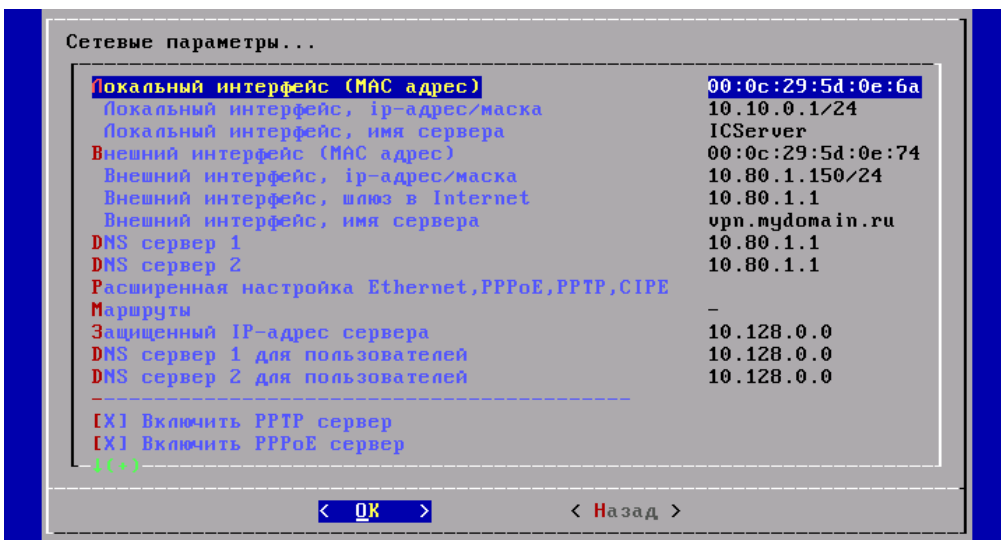
Поменять интервал просмотра можно клавишей пробел. Чтобы вернуться в меню конфигурирования, нажмите Alt-F1.

Конфигурирование сервера



С помощью этого меню можно настроить сетевые параметры, включить или выключить дополнительные сервисы (FTP, почта, веб-сервер и другие), установить параметры, связанные с безопасностью, загрузить или сохранить конфигурацию.

Сетевые параметры



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, CPE... – 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.

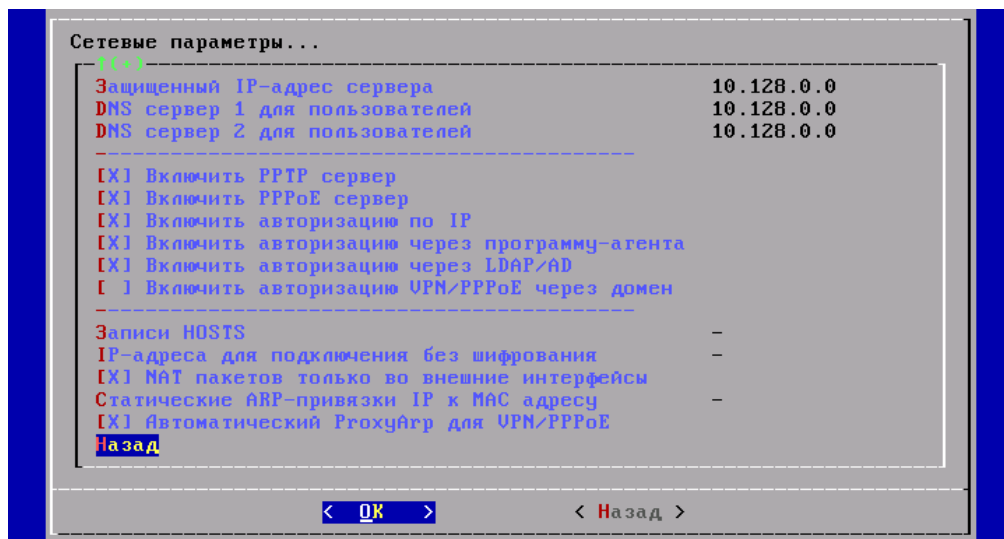
Защищенный IP-адрес сервера – адрес сервера внутри защищенных соединений, по умолчанию – "10.128.0.0". Адрес доступен только для авторизованных пользователей.

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.

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.

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.

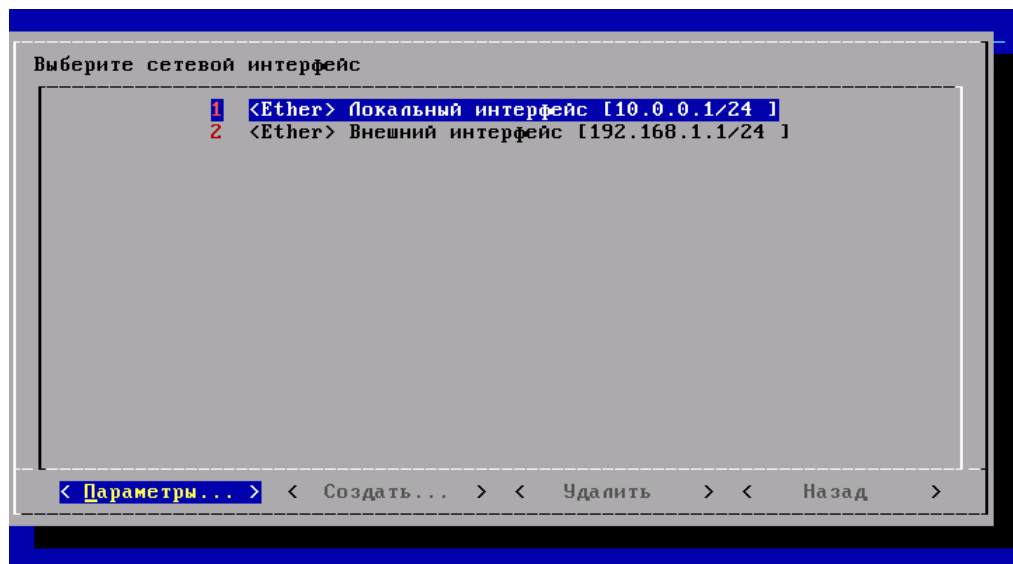
NAT пакетов только во внешние интерфейсы – Производить подмену адреса (NAT) только для соединений через внешние интерфейсы. При этом, для соединений через локальные интерфейсы будет работать обычная маршрутизация (если включена).

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.

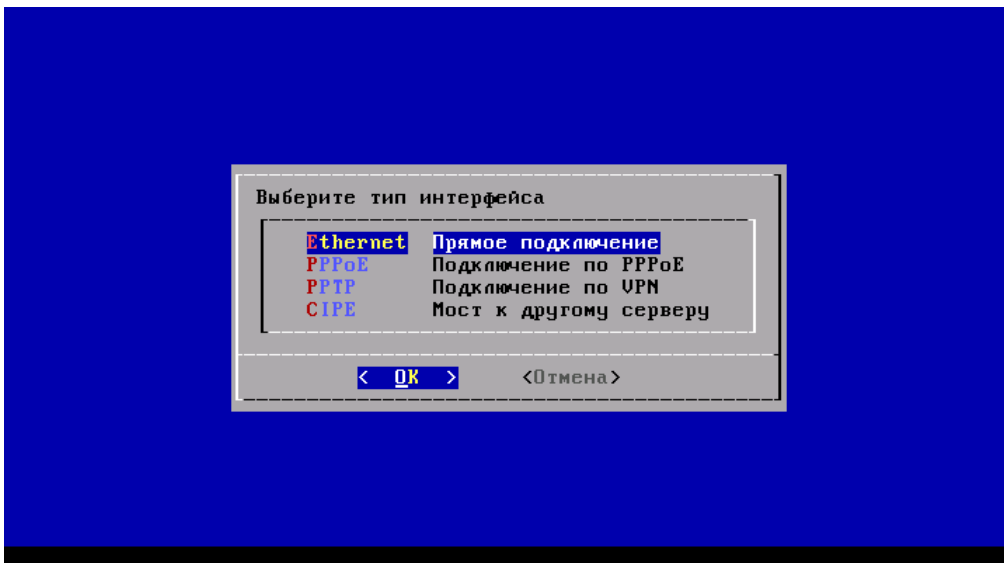
Автоматический Proxypg для VPN/PPPoE – при подключении из Интернет по VPN пользователь сразу попадет в локальную сеть.

Конфигурация сетевых интерфейсов

Выберите в меню "сетевые параметры" пункт "Расширенная настройка интерфейсов ETHERNET,PPPoE,PPTP,CIPЕ...". Появится следующий диалог:



В этом диалоге можно создать, отредактировать или удалить сетевой интерфейс. 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 CPE-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

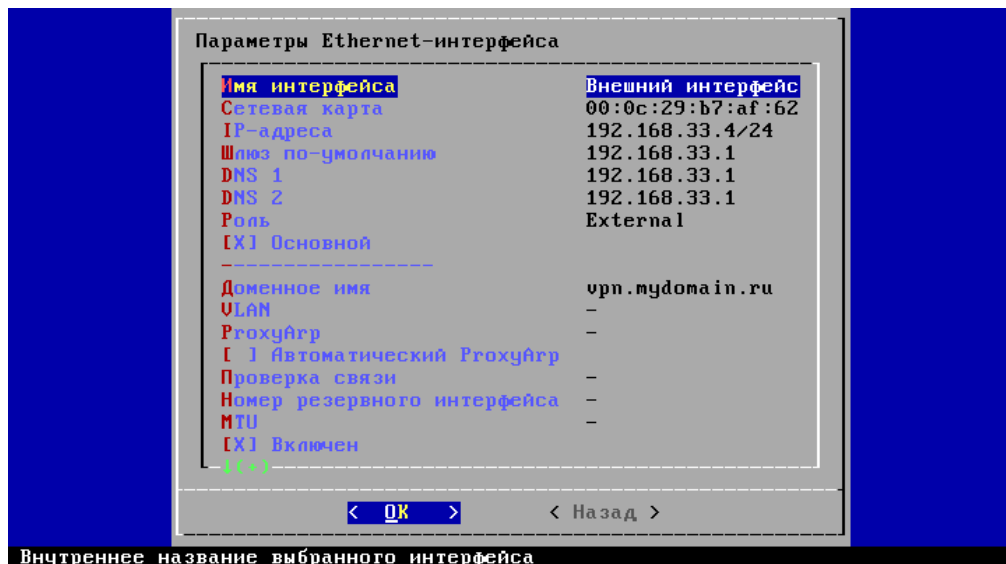
конкретный IP-адрес источника для проверок – для этого укажите его перед адресом назначения, например, "10.0.0.1 10.0.0.2:80".

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 в ICS Manager 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.

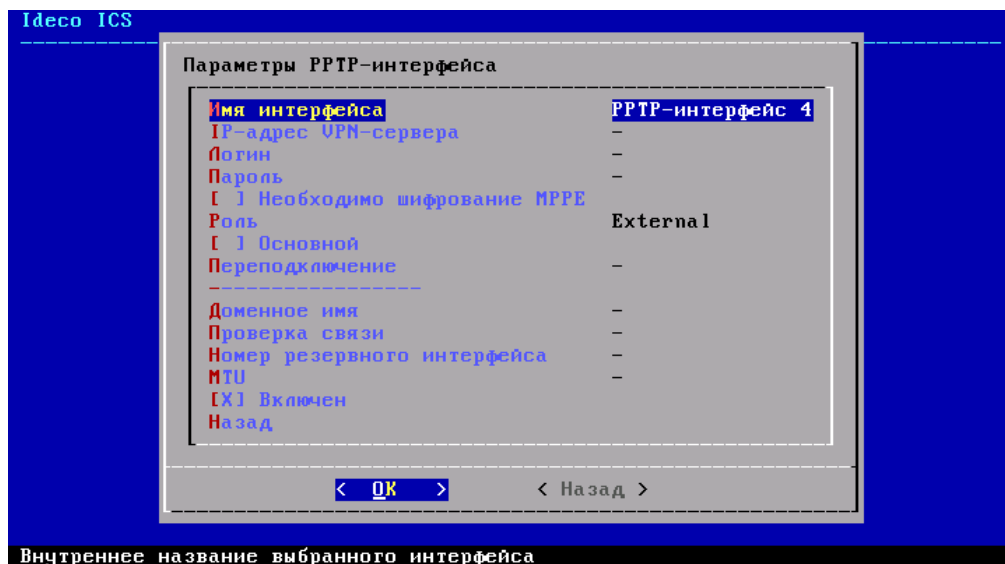
VLAN – Для того чтобы создать виртуальный 802.1q интерфейс, укажите VLAN ID в этом поле. В этом случае, интерфейс будут работать только с тегированными пакетами через выбранную сетевую карту. На одном физическом Ethernet-интерфейсе может быть сконфигурировано несколько VLAN-интерфейсов.

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.

Важно: Эти IP-адреса не будут назначены самому серверу, но их можно будет использовать для пользователей без NAT, указав им эти IP-адреса. Подробнее см. "[Общие параметры](#)" на стр. 49. Для большего удобства, можно создать отдельный пул из этих IP-адресов и назначать серверным логинам адреса из этого пула. Подробнее, "[Создание пула IP-адресов](#)" на стр. 87.

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

Параметры RPTP-интерфейса



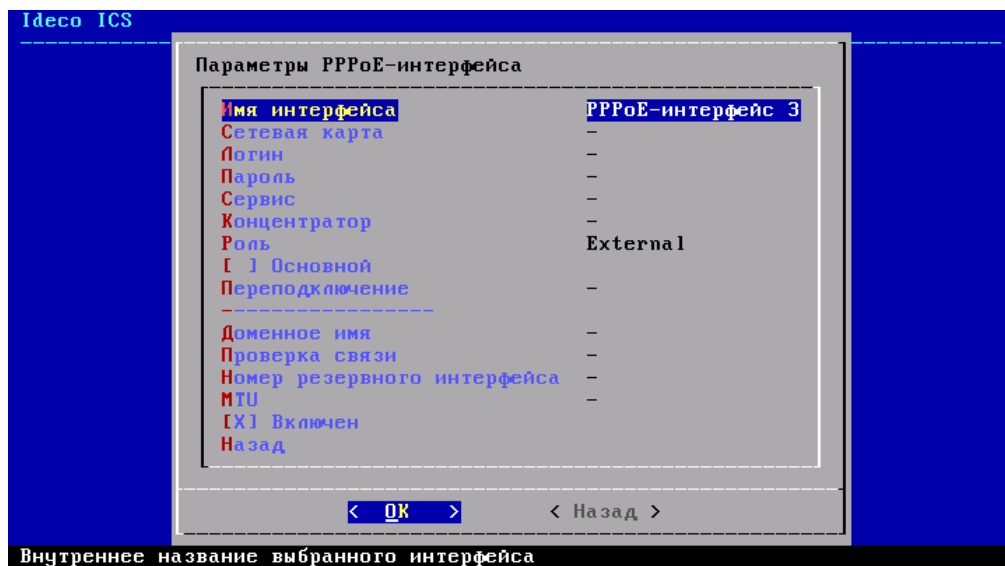
IP-адрес – Укажите IP-адрес сервера для подключения к провайдеру.

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



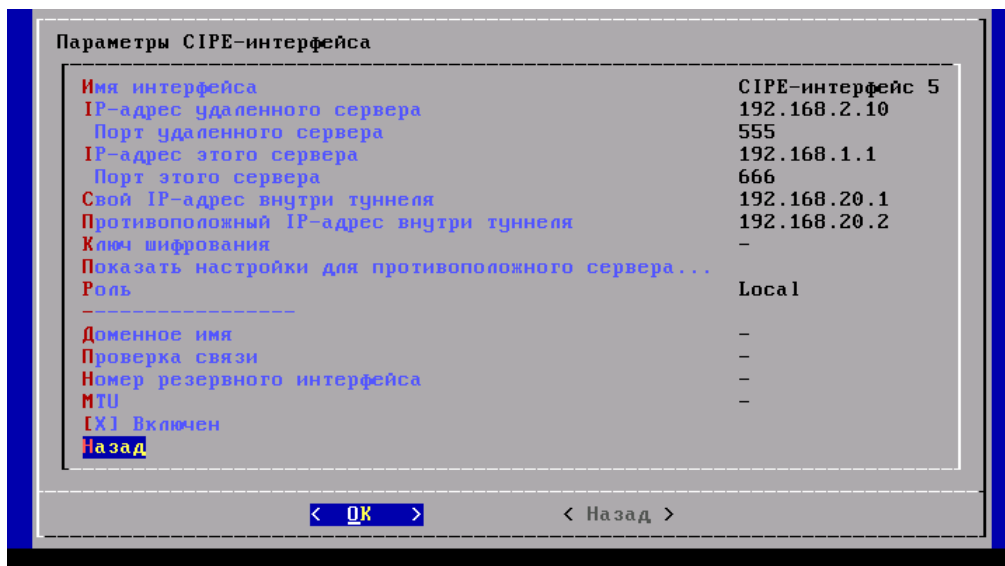
Сетевая карта – Укажите сетевую карту, через которую необходимо подключаться по PPPoE.

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 CIPЕ-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.

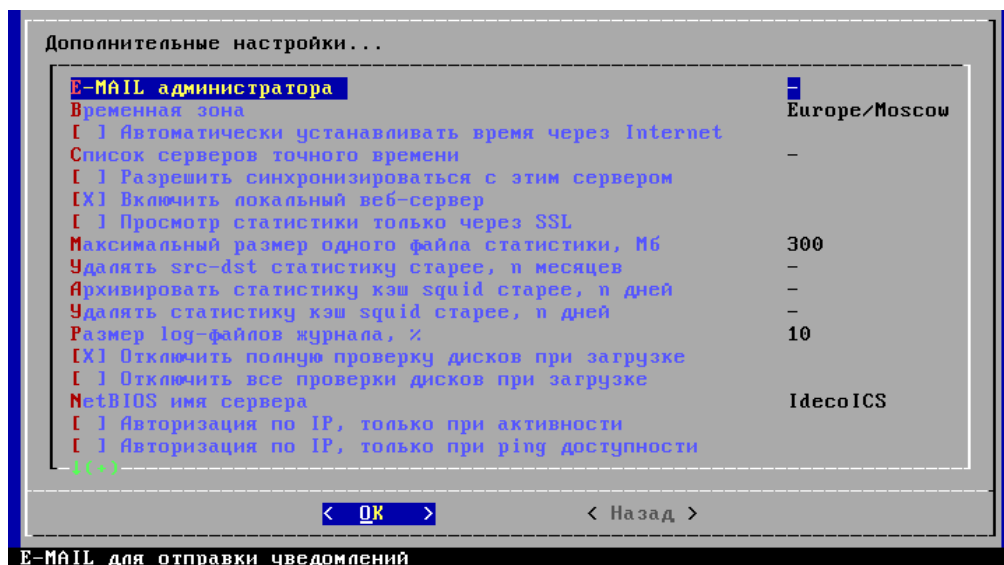
Свой IP-адрес внутри туннеля – Укажите IP-адрес этого сервера внутри туннеля.

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 на 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.

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 точного времени 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. "[Закрытая часть](#)" на стр. 124.

Просмотр статистики только через SSL – Разрешить просмотр статистики только через протокол с шифрованием – SSL. В браузере необходимо будет вместо "http://" набирать "https://". При подключении по VPN устанавливать эту опцию, как правило, не требуется, так как уже обеспечивается высокий уровень шифрования. Этот флажок имеет смысл устанавливать при подключении по VPN без шифрования или при авторизации по IP и IdecO Agent.

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 старше, 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. Как только свободного места на диске станет мало, системный администратор будет предупрежден

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

Удалять статистику кэш squid старше, 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.

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

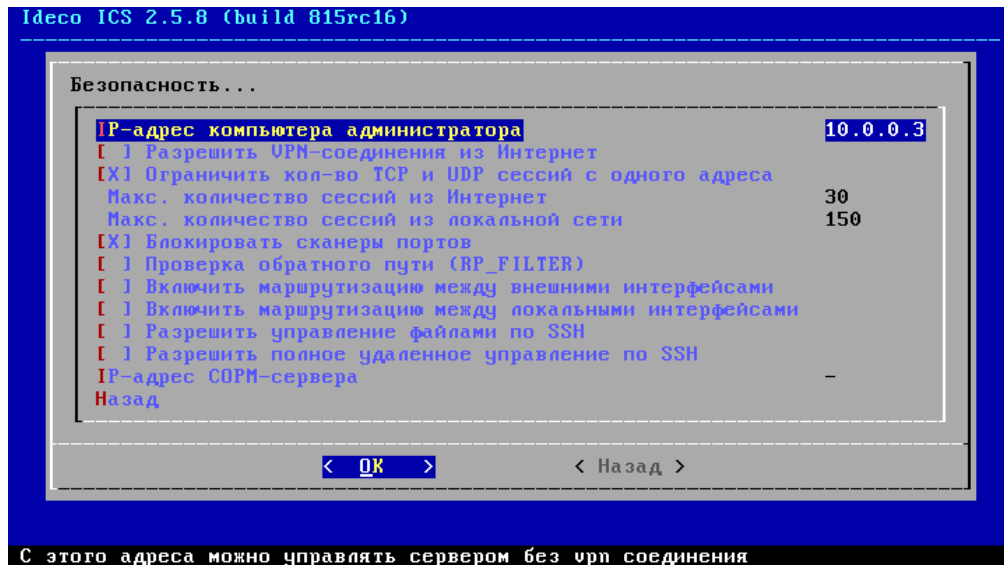
Авторизация по IP, только при активности – При включенной опции авторизация пользователей будет проходить только при наличии трафика от компьютера пользователя.

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.

Оптимизировать стек TCP/IP для P2P трафика – При большом количестве P2P-трафика будет работать оптимизация сетевых соединений.

Безопасность



IP-адрес компьютера администратора – Адрес компьютера, с которого можно управлять сервером без авторизации.

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.

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.

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

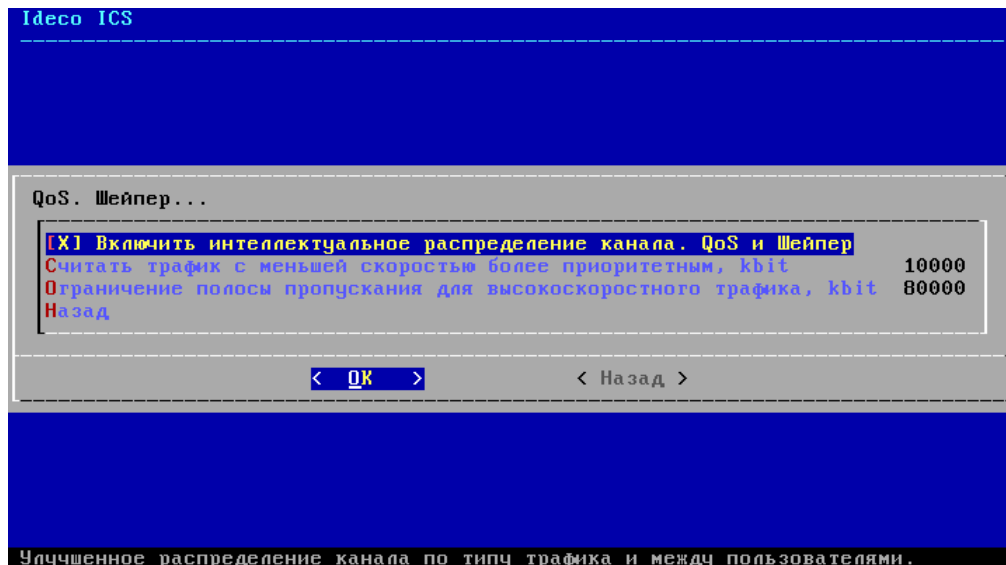
Включить маршрутизацию между локальными интерфейсами – Разрешить маршрутизацию между интерфейсами. Ограничения по IP-адресам и другим параметрам можно установить в разделе Firewall в ICS Manager.

Разрешить управление файлами по SSH – Разрешить подключения к серверу по SSH. Эта опция необходима для удаленного обслуживания сервера и удаленного доступа к меню. ("[Глава 6. Обслуживание](#)" на стр. 129)

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.

IP-адрес COPM-сервера – На этот адрес будет дублироваться весь трафик (необходимо для Интернет-провайдеров).

Qos и Шейпер



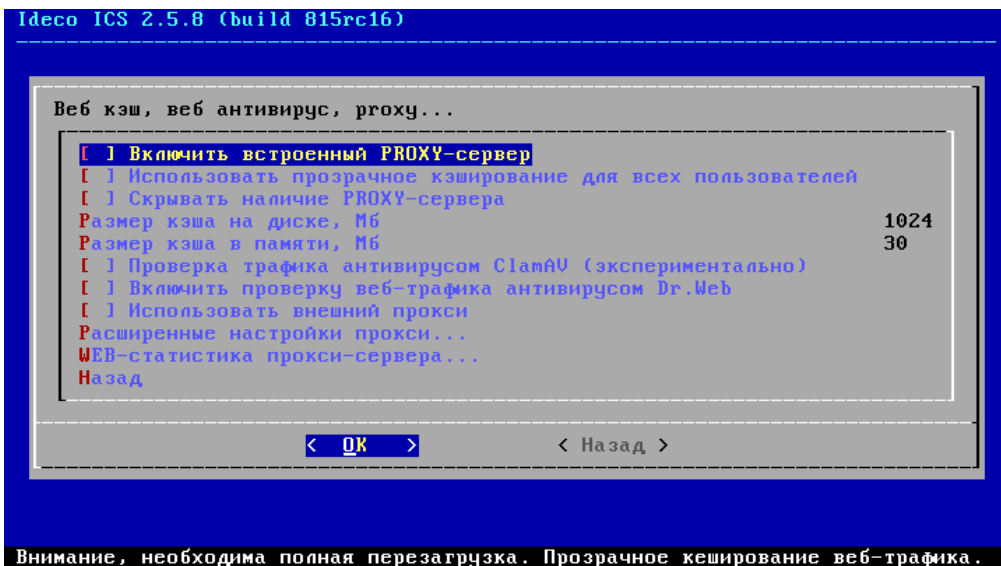
Включить интеллектуальное распределение канала. QoS и Шейпер. Эта возможность позволяет интеллектуально распределять ширину канала в случае его полной загрузки и равномерно распределить канал между пользователями. При включении этой опции интерактивный трафик становится более приоритетным, чем, например, 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 меньше указанной скорости, то приоритет такого трафика повышается. Приоритет трафика со скоростью больше этого значения понижается. Таким 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.

Веб кэш, веб антивирус, проху



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. Подробнее см. [“Создание правила Firewall”](#) на стр. 158.

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.

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

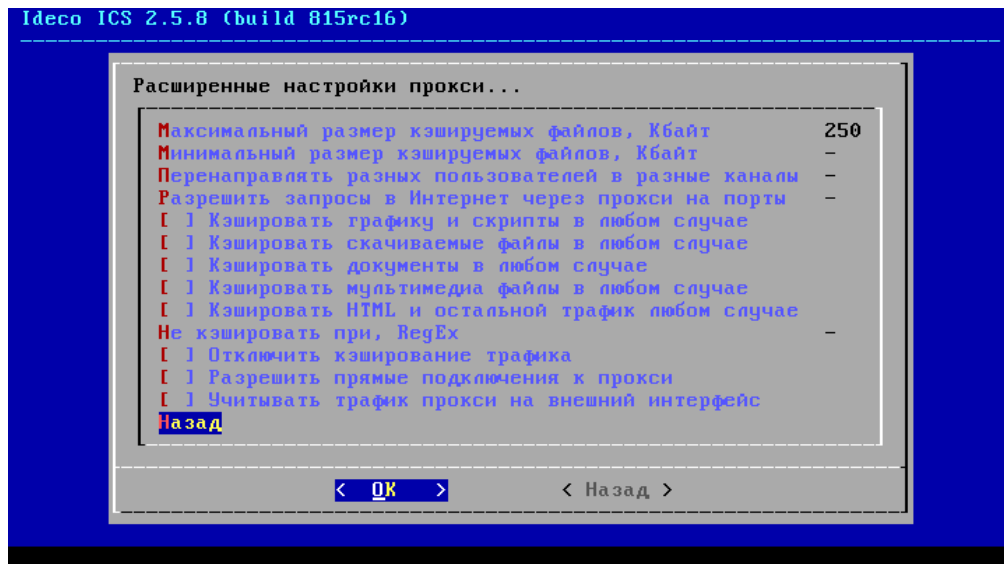
Проверка трафика на вирусы антивирусом ClamAV (экспериментально) – Проверка веб трафика встроенным антивирусом ClamAV. При включенной опции некоторые страницы могут отображаться неправильно. Если система обнаружит вирус, то в браузер выведется соответствующее сообщение и файл загружен не будет.

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.

Web-статистика прокси-сервера – Здесь можно задать параметры формирования веб-статистики прокси-сервера.

Расширенные настройки прокси



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.

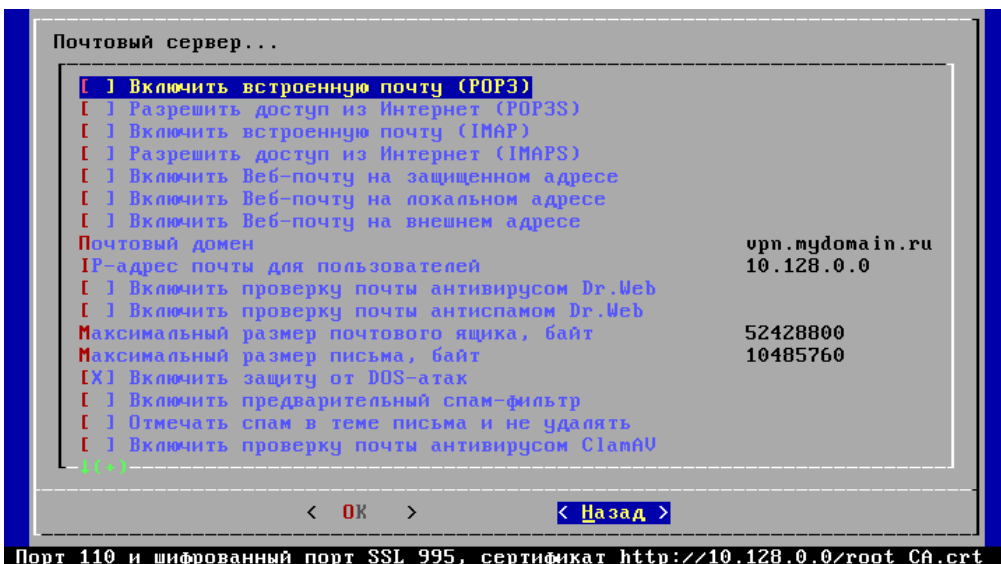
Кэшировать в любом случае – Укажите, какие файлы необходимо кэшировать вне зависимости от настроек запрашиваемого веб-сервера.

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 случаев это не требуется, так как программы должны работать напрямую, без прокси.

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

потребуется 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).

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 – Не принимать письма, идентифицированные как спам. Определение таких писем производится на основе анализа заголовков писем с помощью регулярных выражений. Это позволяет блокировать тривиальный спам, который составляет около 70% всего спама.

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

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

Расширенные настройки почты

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. Требуется для работы электронной почты при авторизации по IP.

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.

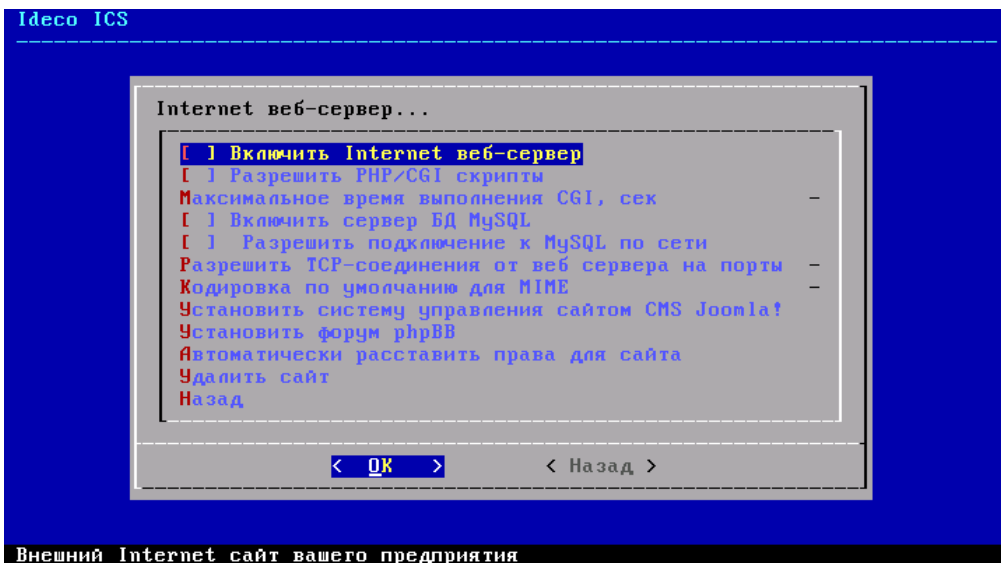
Интервал между проверкой почты (fetchmail), минут – Рекомендуется 5-15 минут.

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](#)" на стр. 163.

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)

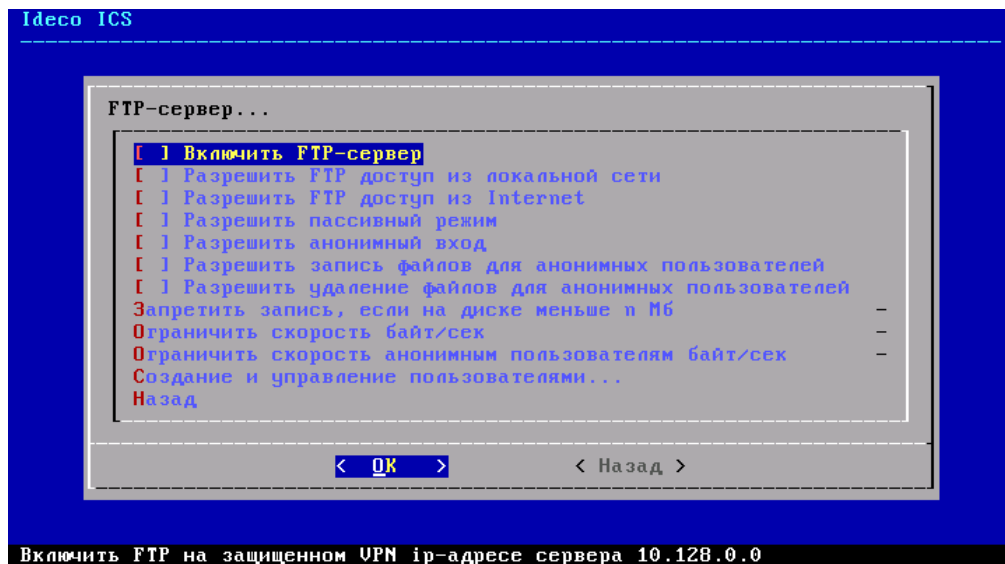
Установить форум phpBB – установить форум phpBB. По умолчанию, форум доступен по адресу внешнего доменного имени в каталоге forum. Например, <http://vpn.myorg.ru/forum>. Для установки форума необходимо включить поддержку MySQL, включить Internet веб-сервер и перезагрузиться (можно использовать мягкую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

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 будут 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).

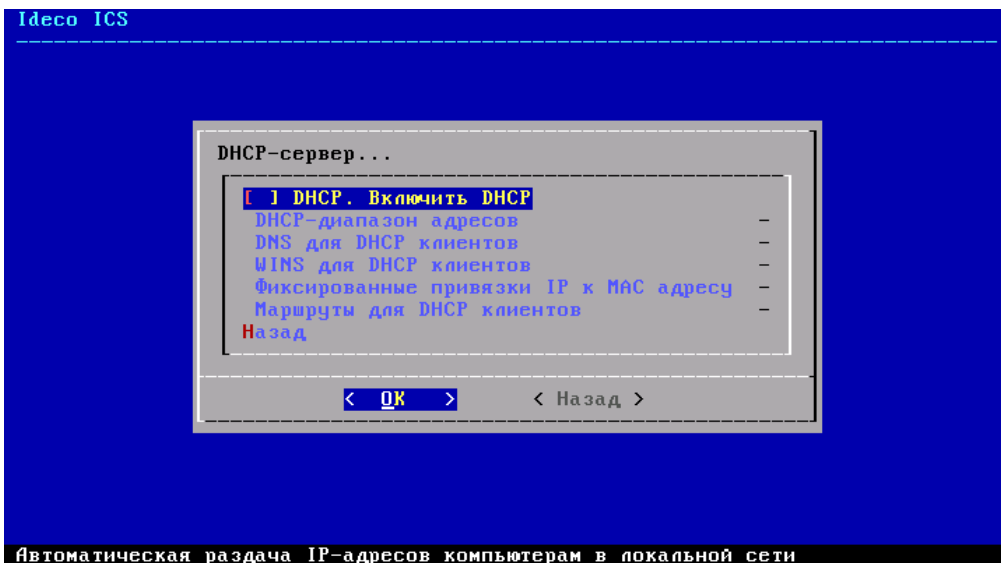
Запретить запись, если на диске меньше n Мб – Запретить создавать и выгружать файлы на сервер, если свободного места на диске меньше, чем указанное число мегабайт.

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.

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.

DHCP-диапазон адресов – диапазон адресов выдаваемых **компьютерам** сети. Эти адреса не должны пересекаться с адресами пользователей. Диапазон должен обязательно уместиться 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".

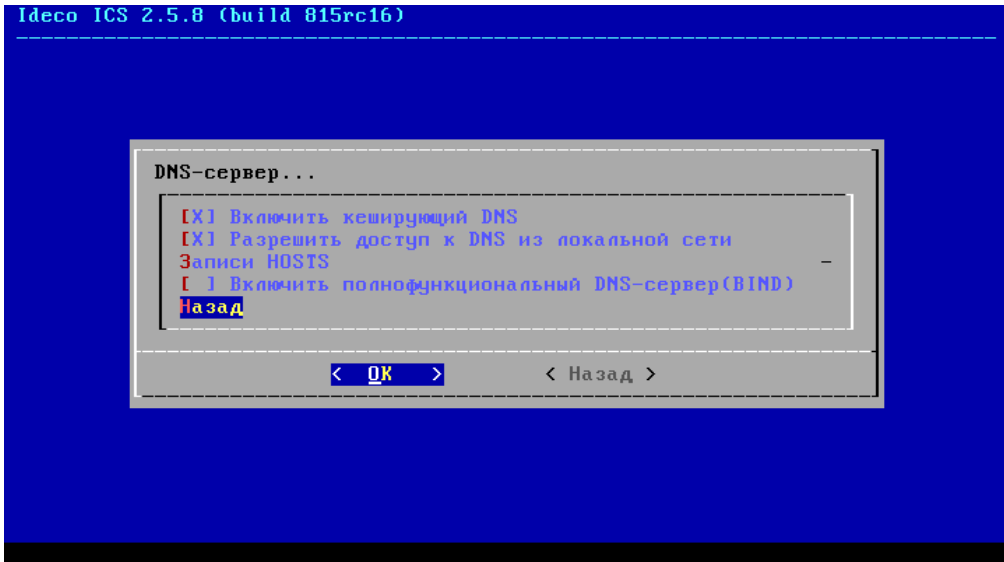
DNS для DHCP клиентов – Укажите DNS-сервера, которые должны быть выданы при автоматической настройке компьютеров по DHCP-протоколу

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

DNS-сервер



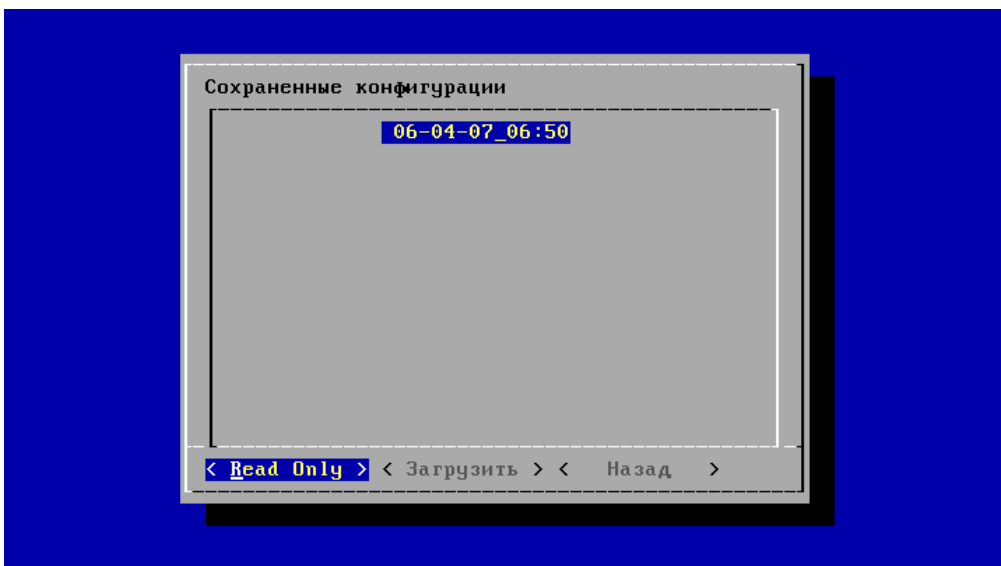
Включить кеширующий DNS – Включен по умолчанию. Используется для кеширования DNS-запросов из локальной сети.

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.

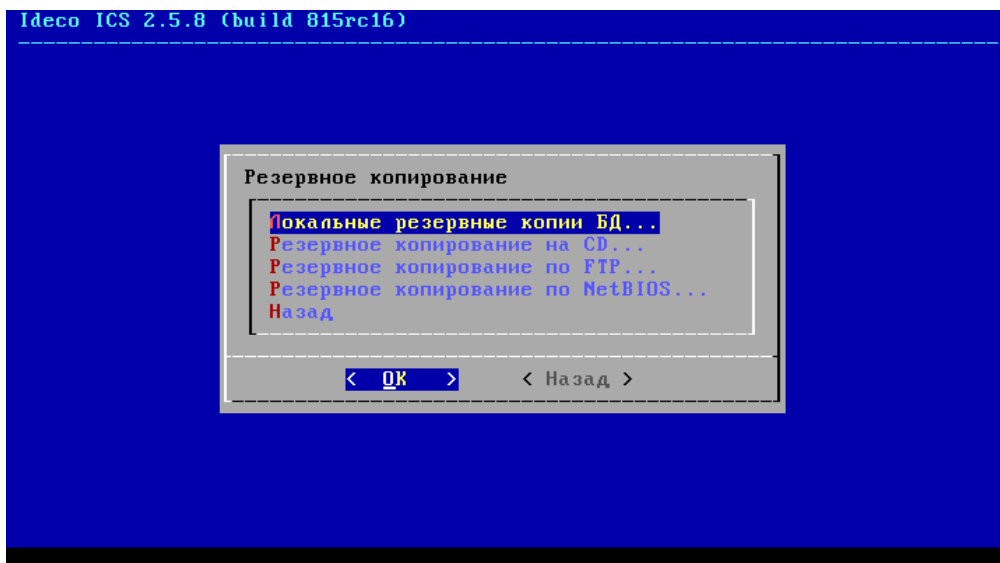
Включить полнофункциональный DNS-сервер (BIND) – Здесь можно указать настройки DNS, если сервер является держателем зоны.

Сохраненные конфигурации



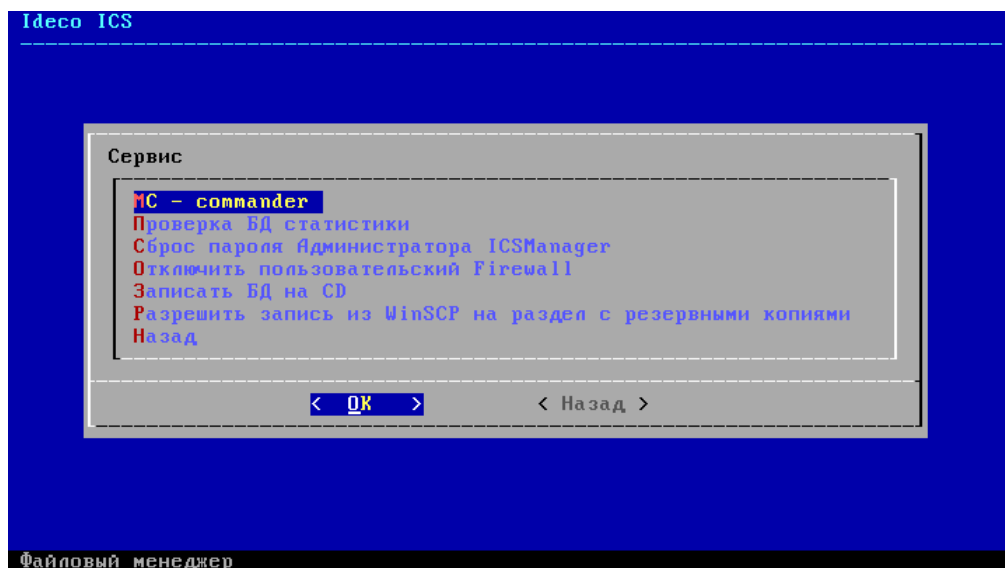
Здесь указан список последних 20 сохраненных конфигураций. При записи большего числа конфигураций самая первая из списка будет удалена. Если вы хотите, чтоб какая-либо конфигурации никогда не удалялась, установите для нее режим "Read-Only".

Резервное копирование



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

Сервис



Меню сервис содержит:

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 ICS Manager – если вы забыли пароль Администратора в Idesco ICS Manager, 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 Idesco ICS Manager.

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

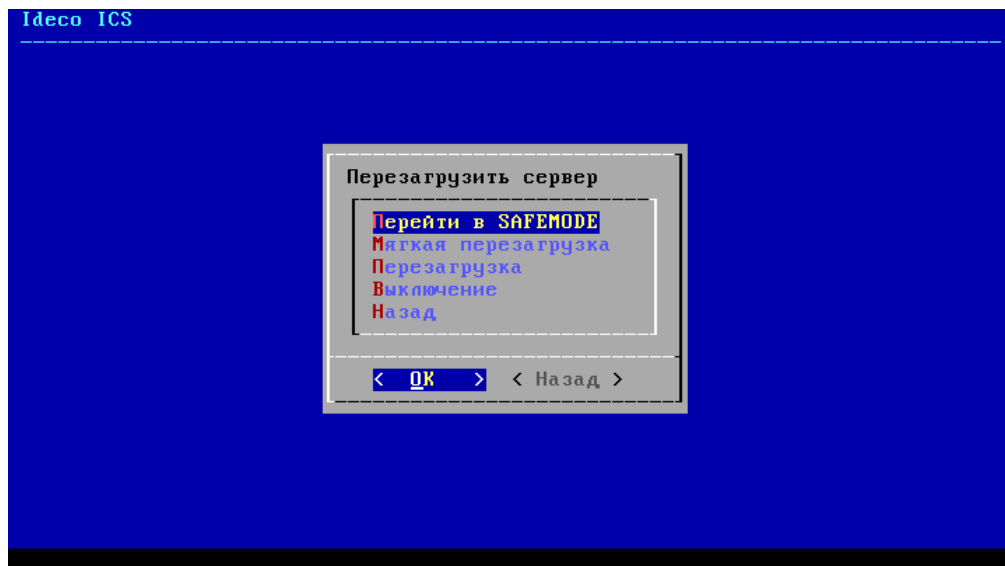
Разрешить запись из WinSCP на раздел с резервными копиями – Эта возможность позволит производить операции записи и удаления на разделе резервных копий через программу WinSCP.

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

Смена пароля

Этот пункт меню позволяет сменить пароль локальной консоли. Будьте внимательны, если вы забудете пароль, то восстановить его можно только полной переустановкой IdecO ICS. Этот пароль также используется для удаленного администрирования по SSH

Перезагрузка сервера



Перейти в SAFEMODE – перейти в режим минимальной загрузки компонентов IdecO ICS. 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.

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

Глава 5. Веб-интерфейс пользователя

Веб-интерфейс пользователя позволяет пользователям Ideco ICS просматривать статистику, сменить пароль, содержит информацию по подключению и т.д.

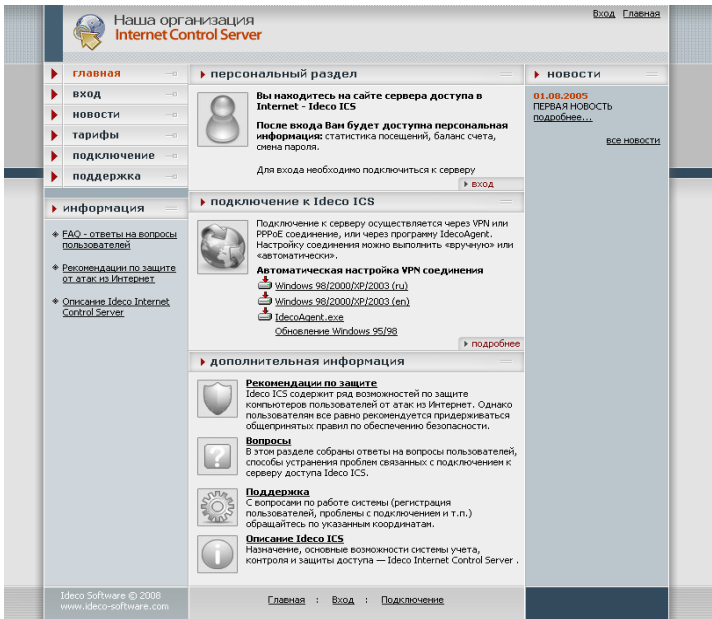
Веб-интерфейс пользователя делится на две части:

- **Открытая часть.** Доступна всем пользователям локальной сети. Содержит общую информацию, такую, как подключение, тарифные планы, новости, контакты и т.д.
- **Закрытая часть** (персональный раздел). Позволяет пользователю просмотреть свою статистику, операции, сменить пароль и т.д. Для входа в персональный раздел необходимо установить авторизованное подключение через VPN, PPPoE, или IdecoAgent, а также ввести свой логин и пароль.

Замечание: Адрес веб-интерфейса по умолчанию "http://10.0.0.1". По этому адресу находится открытая часть. Закрытая часть находится по адресу "http://10.128.0.0", который доступен только после авторизации через VPN, PPPoE, или IdecoAgent.

Открытая часть

Открытая часть веб-интерфейса пользователя выглядит следующим образом:



Страница "Главная"

Содержит информацию, которая может потребоваться пользователям в первую очередь:

- Как войти в персональный раздел.
- Как подключиться к Idesco ICS. Ссылки на файл с автоматической настройкой VPN-соединения.
- Программа авторизации – Idesco Agent.
- Новости.
- Дополнительная информация:
 - Рекомендации по защите компьютеров пользователей
 - Ответы на вопросы пользователей. Такие как, что делать в случае если не устанавливается соединение, или если соединение устанавливается, но при этом в Интернет не пускает.
 - Поддержка. В этом разделе указывается координаты куда могут обратиться пользователи в случае необходимости.
 - Описание Idesco ICS. В этом разделе пользователи могут ознакомиться с основными функциями Idesco ICS.

Страница "Вход"

Содержит ссылку на вход в закрытую часть.

Страница "Новости"

Список новостей. Новости выводятся также на главной странице. Новости редактируются администраторами в IdecO ICS Manager (подробнее см. ["Редактор сайта"](#) на стр. 89).

Страница "Тарифы"

Выводятся тарифные планы, имеющиеся в IdecO ICS. Выводить можно не все тарифные планы. Какие тарифные планы отображать в веб-интерфейсе пользователя, указывается администраторами в IdecO ICS Manager (подробнее см. ["Редактор сайта"](#) на стр. 89).

Тарифы выводятся в виде списка тарифных планов с указанием стоимости трафика по каждой подсети. Ниже выводятся сами подсети.

Страница "Подключение"

Содержит информации о подключении к серверу с IdecO ICS. Здесь доступны ссылки на файлы с автоматической настройкой соединения в ОС Windows 98/ME/2000/XP/2003, а также подробная информация по ручной настройке VPN-соединения, которую пользователи также могут скачать в виде файла в формате MS Word.

На этой же странице можно загрузить программу авторизации IdecOAgent.

Страница "Поддержка"

Здесь указывается координаты, куда пользователи могут обращаться по вопросам регистрации, по проблемам с подключением и т.п. Информация этого раздела редактируется администраторами в IdecO ICS Manager (подробнее см. ["Редактор сайта"](#) на стр. 89).

Закрытая часть

Для входа в закрытую часть, пользователю необходимо установить авторизованное подключение через VPN, PPPoE, или IdecOAgent, после чего открыть страницу входа:

Для входа введите данные:	
Имя пользователя (логин):	<input type="text" value="ivanov"/>
Пароль:	<input type="password" value="••••"/>
<input type="button" value="Вход >>"/>	

Ввести свой логин и пароль и нажать кнопку **Вход**.

После входа в закрытую часть открывается страница "**Информация**".

Страница "Информация"

На этой странице отображается основная информация о пользователе: Тарифный план, IP-адрес, состояние баланса, родительская группа и т.д. В этом разделе также отображаются сообщения, отправленные пользователю или группе.

Если вход осуществлен под пользователем с правами администратора, то будет отображено дерево пользователей его группы, как показано ниже. Если пользователь не является администратором, то дерево показываться не будет.

Наша организация
Internet Control Server

[Выход](#) [Главная](#)

Пользователь: **Administrator** (Главный Администратор)

[Информация](#)
▶
[статистика](#)
▶
[операции](#)
▶
[тариф](#)
▶
[выход](#)

Все

- [-] Пример1-Малое предприятие
- [-] Пример2-Среднее предприятие
 - [+] Бухгалтерия
 - [+] Отдел ИТ
 - [-] **Отдел кадров**
 - Петров Евгений Алексеевич <se...>
 - Сергеев Роман Романович <rom...>
 - [+] Проектировщики
 - [+] Руководители
 - [+] Серверы сети
 - Администратор Иванова Сергей Юрь...
- [+] Пример3-Большое предприятие
- [+] Пример4-Провайдер
- [+] Пример5-ВУЗ
- Главный Администратор <Administrator>
- Внешний интерфейс <Server>

Пользователь/группа	
Электронная почта	Отдел кадров
Тарифный план	Основной тариф
Пул IP адресов	Простой пул
Размер	5
NAT	
Порог отключения	-2000
Остаток на начало периода	0
Текущий кредит(расход)	0
Текущий дебет(оплата)	0
Бух. баланс(по документам)	0
Текущий баланс	0

Пользователи группы	Текущий баланс
Петров Евгений Алексеевич	0
Сергеев Роман Романович	0

Дата	Сообщение
------	-----------

[Download ICSManager.exe](#)

Ideco Software © 2006
www.ideco-software.com

Если у пользователя включена опция **Просмотр ограничения родителей** в параметрах разрешений для пользователя (см. "Параметры разрешений" на стр. 52), то на этой вкладке будет отображено ближайшее ограничение вышестоящих групп.

Замечание: Если вы вошли с логином администратора, то информация на страницах **Информация, Статистика, Операции, Тариф** будет выводиться по пользователю или группе, выбранной в дереве пользователей на этой странице.

Страница "Статистика"

После входа страница выглядит следующим образом:

информация ▶ статистика ▶ операции ▶ тариф ▶ пароль ▶ выход

Статистика по пользователю: administrator(Администратор)
Статистика посещений

Статистика за период

Дата от: 01.08.2005 до 15.08.2005

Группировка: день

Отдельно по подсетям

Запросить

Дата (время)	Длина	Описание	Получено,Мб	Передано,Мб	Стоимость
01.08.2005 Пн.	За день		27.41	19.38	30.74
02.08.2005 Вт.	За день		14.24	0.94	0.27
03.08.2005 Ср.	За день		9.42	0.43	0.01
04.08.2005 Чт.	За день		13.13	3.56	11.74
05.08.2005 Пт.	За день		12.58	20.15	23.56
08.08.2005 Пн.	За день		5.65	3.58	9.66
09.08.2005 Вт.	За день		8.65	12.99	16.85
10.08.2005 Ср.	За день		2.15	2.23	2.60
11.08.2005 Чт.	За день		0.10	0.02	0.19
12.08.2005 Пт.	За день		9.90	3.13	16.41
13.08.2005 Сб.	За день		128.49	60.17	175.97
15.08.2005 Пн.	За день		0.17	0.04	0.33

По умолчанию отображается основная статистика (по сессиям), сгруппированная по дням. Подробнее о том, как ведется основная статистика см. "[Закладка "Статистика"](#)" на стр. 59.

Страница "Детализированная статистика"

Детализированная статистика доступна по ссылке **Статистика посещений** со страницы **Статистика**.

информация ▶ статистика ▶ операции ▶ тариф ▶ пароль ▶ выход

Статистика по пользователю: administrator (Администратор)

Статистика по посещаемости top 100

Год: 2005 Месяц: Август Запросить

Подробная статистика посещений за месяц

Период: 01.08.2005 00:00 по 15.08.2005 15:28 Запросить

Входящий IP адрес: подробно по времени

Дата	Адрес	Объем байт.	Направление	Протокол (ваш порт <-> порт)	Описание
212.42.38.195		77,332,767	Входящий		
10.128.0.0		75,213,773	Входящий		
212.42.38.88		60,244,482	Исходящий		
212.42.38.88		35,710,409	Входящий		
62.168.231.161		29,883,408	Исходящий		medialt-231-161.utk.ru
195.58.6.12		24,616,248	Исходящий		
62.168.231.161		10,947,825	Входящий		medialt-231-161.utk.ru
82.94.246.33		7,604,451	Входящий		
195.58.6.12		7,515,273	Входящий		
213.202.214.219		5,508,520	Входящий		fragmaster.net
82.94.246.33		3,944,834	Исходящий		

Примечание: Детализированная статистика, в отличие от основной, отображается только в веб-интерфейсе пользователя и через IdecO ICS Manager недоступна.

Страница "Операции"

На этой странице отображается список всех операций с лицевым счетом пользователя или группы.

Также на этой странице пользователь может выполнить активацию карт оплаты.

Замечания:

Поля для активации карт оплаты доступны только **финансовым** пользователям. Подробнее о назначении и использовании признака **финансовый** см. "[Признак "Финансовый"](#)" на стр. 65.

Функции по работе с картами оплаты доступны только в версии IdecO ICS Enterprise Edition (подробнее см. "[Отличия версий IdecO ICS](#)" на стр. 14). Про управление картами оплаты см. "[Карты оплаты](#)" на стр. 145.

О формировании финансовых операций их назначении, особенностях работы см. "[Операции](#)" на стр. 132

Страница "Тариф"

На этой странице отображается вся информация по тарифному плану, который установлен для текущего пользователя или группы.

Замечание: В отличие от страницы "Тарифы" в открытой части веб-интерфейса пользователя, на этой странице тариф будет отображаться, даже если у

него не установлен признак **Показать в WEB** с помощью Ideco ICS Manager, разделе **Редактор сайта**.

Страница "Пароль"

На этой странице пользователь может изменить пароль, а также изменить e-mail, используемый для отправки сообщений.

Для смены пароля введите данные:	
Новый пароль:	<input type="password" value="••••••"/>
Введите новый пароль еще раз:	<input type="password" value="••••••"/>
	<input type="button" value="Изменить"/>
Изменить e-mail для оповещений	
E-mail:	<input type="text" value="ivanov@company.com"/>
	<input type="button" value="Изменить"/>

Глава 6. Обслуживание

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

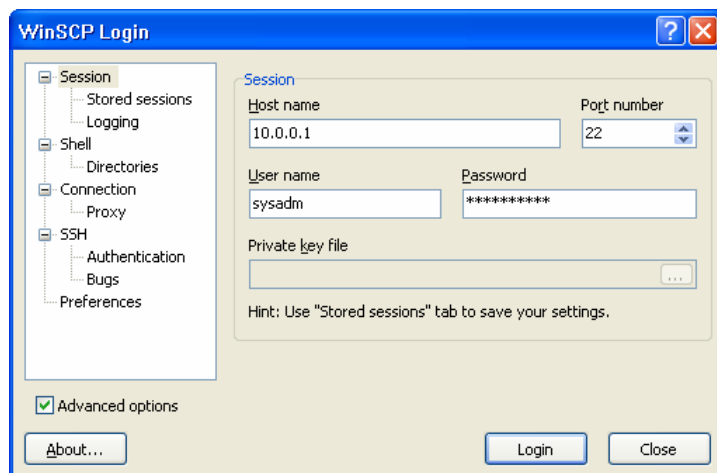
Резервное копирование

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

Однако аппаратные сбои могут привести к повреждению базы данных или всего жесткого диска, поэтому рекомендуется создавать резервные копии БД на другом носителе, например, скопировав их на компакт-диск через меню **Сервис** (см. "[Сервис](#)" на стр. 119) или с помощью программы WinSCP.

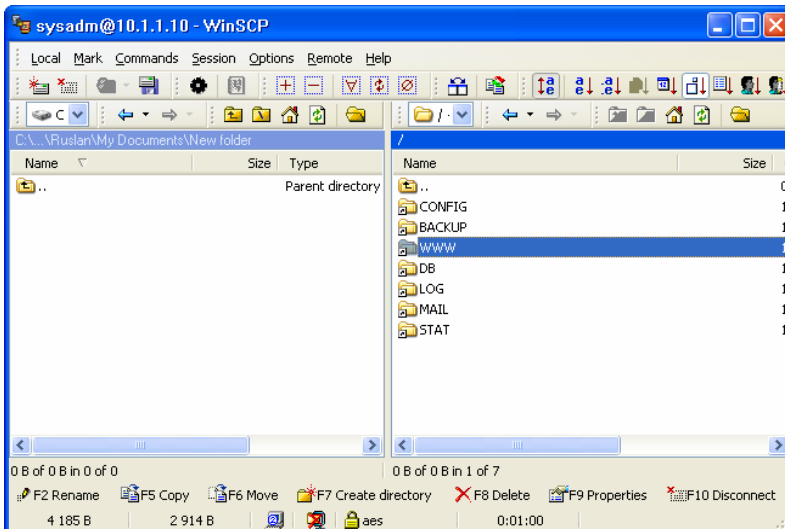
В локальной консоли в меню безопасность разрешите управление файлами по SSH.

Для того чтобы скопировать резервную копию на свой компьютер воспользуйтесь программой WinSCP, расположенной на диске с дистрибутивом.



Введите локальный IP-адрес сервера, логин **sysadm** и пароль, как в локальной консоли. Нажмите кнопку Login.

Зайдите справа в каталог **BACKUP**, а слева выберите ваш каталог и выберите резервную копию скопируйте клавишей **F5** или перетащите файлы мышью.

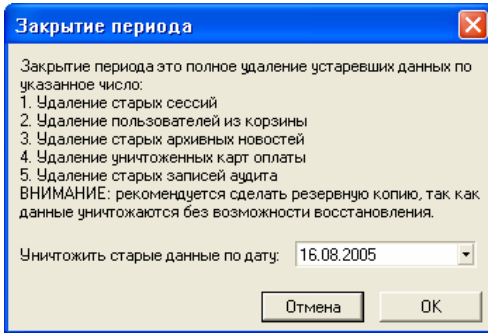


Удаление БД статистики посещений src-dst

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.

Закрытие периода

Со временем в основной базе данных накапливается много устаревшей информации, которая делает работу с IdecO ICS Manager неудобной. Поэтому рекомендуется минимум раз в год делать закрытие периода. Закрытие периода делается через IdecO ICS Manager в меню **Сервис > Закрытие периода**. При этом появится следующее окно с сообщением о том, какие операции будут выполнены.



Удаленный доступ к меню сервера

1. В локальной консоли в меню безопасность разрешите управление файлами по SSH.
2. Подключиться к серверу через программу putty, протокол SSH, порт 22. Указать логин sysadm, пароль как в локальной консоли.
3. Для вывода меню – команда menu, для запуска файлового менеджера - команда mc.

Глава 7. Дополнительные возможности Idecos ICS

В этой главе описываются возможности Idecos ICS используемые не всеми организациями. Например, функции связанные с расчетами с абонентами, работа с картами оплаты и т.д. А также возможности Idecos ICS, описание которых не было включено в другие главы. Большая часть данного раздела касается работы с Idecos ICS Manager.

Операции

Закладка "Операции"

Информация о состоянии лицевого счета

Кнопки формирования операций

Список операций

Информация	Состав	Статистика	Операции	Журнал операций	Групповые операции
Баланс(тек)	Остаток	Оплата	Расход(тек)	Приход	Обнулить баланс
-615,1 =	-433,1 +	0 -	182	Расход/Акт	Документы
Баланс(бук)	Остаток	Оплата		Подвести баланс	Счет на предоплату
-433,1 =	-433,1 +	0		Исправить баланс	

Номер	Тип	Описание	Дата	Сумма	Знак	Баланс(бук)	Оператор
1040	Расход	По расписанию: 2005-01-07-2005-01-07-2005	01.06.2005	512,15	-1	512,15	System
1182	Расход	По расписанию: 2005-01-07-2005-01-07-2005	01.07.2005	223,89	-1	-736,05	System
00032	Приход	01.07.2005-01.07.2005	01.07.2005	512,15	1	-223,9	Оператор (Тел
00026	Баланс	01.07.2005-01.07.2005	01.07.2005	-223,90	0	-223,9	Оператор (Тел
1337	Расход	2005-07-01...2005-07-31	01.08.2005	209,25	-1	-433,14	System

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	= Баланс (бух.) - Расход за текущий период

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 на 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 ICS 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](#)" на стр. 66 и "[Автоматическое формирование акта](#)" на стр. 139.

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 имеют 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...".

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:

Документ

Приход

Номер 00009 от 28.04.05

Описание 28.04.2005-28.04.2005

Сумма 100 Сформировать Отмена

Вывод на печать

№	Наименование
3	Приход

Печать

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.

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 операцию 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"](#) на стр. 141.

Примечание: О возможности выполнения операций одновременно по нескольким группам или пользователям см. ["Закладка "Групповые операции""](#) на стр. 137.

Совет: Выполнение операций Расход/Акт и Обнуление баланса можно автоматизировать. Подробнее об этом см.

["Автоматическое обнуление баланса"](#) на стр. 66 и ["Автоматическое формирование акта"](#) на стр. 139.

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"](#) на стр. 136.

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**.

Информация | Состав | Статистика | Операции | Журнал операций | Групповые операции

Период с 01.03.2005 по 17.07.2005 Тип

Финансовые абоненты

Группы

Финансовые документы

Запросить

Абонент	Номер	Тип	Описание	Дата	Сумма	Знак	Опера
Все пользователи	00001	Документ	04.04.05-04.04.094.04.2005	04.04.2005	0,00	0	Админ
Все пользователи	00001	Автоначис	30.04.2005-30.0410.04.2005	30.04.2005	31314,12	0	Админ
Все пользователи	00002	Автоначис	По расписанию: 11.05.2005	11.05.2005	1425,95	0	System
Все пользователи	00003	Приход	07.07.05-07.07.097.07.2005	07.07.2005	-9,00	1	Админ
Все пользователи	00017	Расход	17.07.2005-17.07.7.07.2005	17.07.2005	60732,50	-1	Админ
Все пользователи	00015	Приход	07.07.2005-17.07.7.07.2005	07.07.2005	70000,00	1	Админ
Все пользователи	00010	Баланс по	17.07.2005-17.07.7.07.2005	17.07.2005	9258,50	0	Админ
Telegin	00002	Автоначис	По расписанию: 11.05.2005	11.05.2005	0,00	0	System
Васев А. О.	00002	Автоначис	По расписанию: 11.05.2005	11.05.2005	0,00	0	System
Левый Андрей Мих	00002	Автоначис	По расписанию: 11.05.2005	11.05.2005	0,00	0	System
Лопалева Наталья С	00002	Автоначис	По расписанию: 11.05.2005	11.05.2005	0,00	0	System
Лошкарева Ольга	00002	Автоначис	По расписанию: 11.05.2005	11.05.2005	0,00	0	System
Карфидова Надеж	00002	Автоначис	По расписанию: 11.05.2005	11.05.2005	0,00	0	System
Пономарев Алекс	00002	Автоначис	По расписанию: 11.05.2005	11.05.2005	0,00	0	System
Воробьев Вячесла	00002	Автоначис	По расписанию: 11.05.2005	11.05.2005	0,00	0	System
Tana O sintseva	00006	Автоначис		10.04.2005	0,00	0	System

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**.

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.

Информация | Состав | Статистика | Операции | Журнал операций | Групповые операции

Все пользователи

Финансовые операции над потомками

Дата: 17.07.2005

Описание:

Расход/Акт Баланс Сброс баланса

Печать финансовых документов

Дата с: . . . по: . . .

Документ:

Печатать

Отчеты за период

Период с: 01.07.2005 по: 17.07.2005

Только финансовые абоненты
 Только финансовые документы
 Только должники
 Только группы

Вид отчета:

Печатать

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	

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"**.





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

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 помощью 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**.

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:

Баланс(тек)	Остаток	Оплата	Расход(тек)
0 =	0 +	0 -	0

Формирование акта, период – установите период формирования акта, обычно месяц.

Формирование акта, дата – укажите дату первого формирования акта, т.е. дата следующего формирования акта. Когда формирование акта работает, 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"](#)" на стр. 137

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 ICS Manager загружает из БД файл с шаблоном и заполняет его данными.

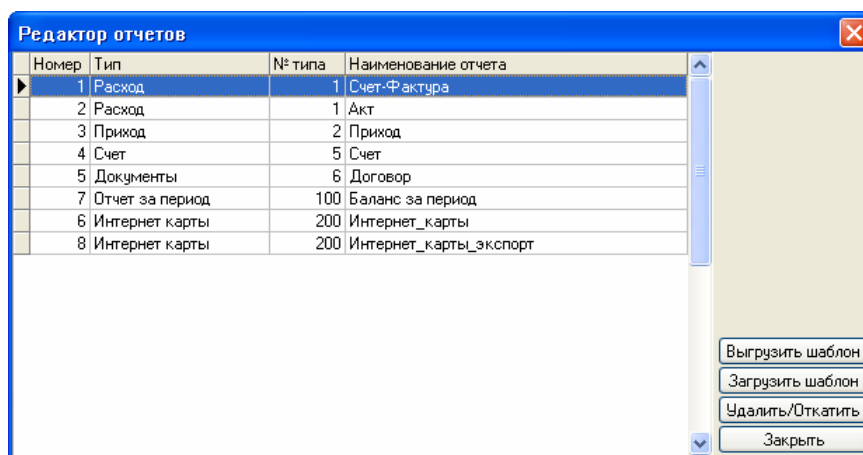
Замечание: Все генерируемые файлы MS Excel (*.xls) сохраняются во временной папке Windows. После закрытия Ideco ICS Manager они удаляются. Если требуется сохранить файл, то сохраните его в другой папке, для этого – выберите в MS Excel меню "**Файл > Сохранить как...**".

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 этот 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. Закрывать 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.

Расположение администраторов в дереве пользователей

В системе Ideco ICS 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 ICS 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.

Учет времени

Учет времени позволяет учитывать и тарифицировать время соединения пользователя с сервером.

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.


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.

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.

Карты оплаты

Доступно только в версии Enterprise Edition (подробнее см. "[Отличия версий Ideco ICS](#)" на стр. 14).

Ideco ICS Enterprise Edition 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 ICS 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.

Параметры карт оплаты

Создаваемые в системе IdecO ICS карты оплаты описываются следующими параметрами:

Код – секретный код карты, использующийся при проведении платежа по карте. Поддерживается уникальность кодов на всем времени жизни системы. Состоит из 9 десятичных цифр.

Серия – идентификатор серии, которой принадлежит карта. Номера серий создаются последовательно. Также используется для проведения платежа по карте.

Цена – номинал карты. Измеряется в условных единицах;

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.

Активирована – признак того, что карта использована.

Уничтожена – Признак полного уничтожения серии карт без возможности восстановления.

Управление картами оплаты

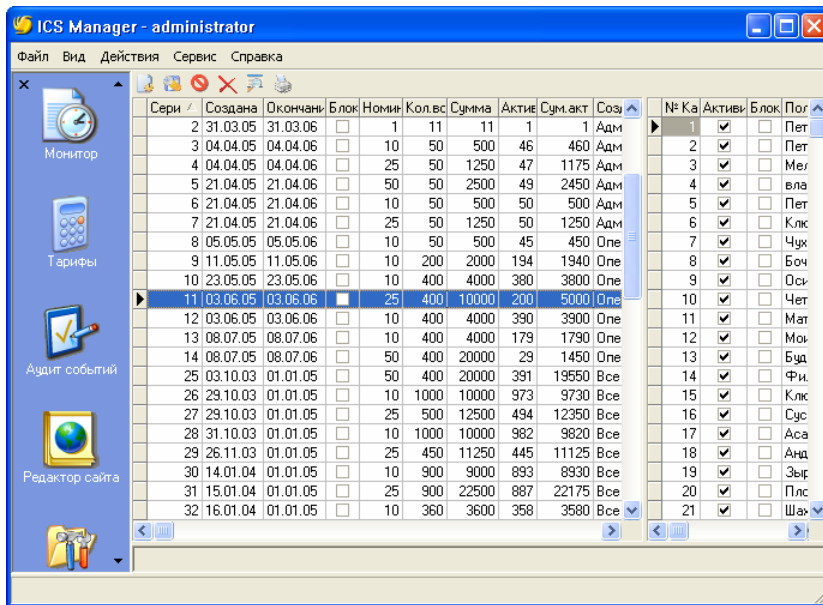
Генерирование карт оплаты, операции над картами оплаты выполняются в IdecO ICS Manager в разделе **Карты оплаты**.

Замечание: Функции для работы с картами оплаты доступны только **Главному администратору** и администраторам с установленным признаком "Администратор карт оплаты".

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**.

The dialog box 'Создать серию карт' has the following fields and controls:

- Номинал карты:
- Кол.во карт:
- Срок действия до:
- Комментарий:
- Buttons: and

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.

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**.

Печать карт оплаты

В системе имеется возможность вывода на печать сгенерированных карт оплаты.

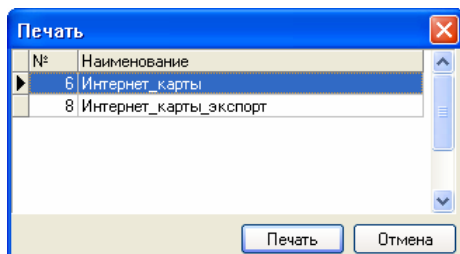
Замечание: В случае необходимости выпуска карт со стираемым полем эту возможность можно использовать для экспорта данных по картам и последующего их использования при выпуске в другом месте.

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"](#) на стр. 141.

Карты печатаются сериями.

1. Для печати выберите нужную серию, нажмите кнопку **Печать серии карт**.



2. Нажмите кнопку **Печать**.

Платежи по картам оплаты

Осуществляется пользователем из веб-интерфейса пользователя. При проведении платежа он вводит номер серии и секретный код карты.

The screenshot shows the web interface of the Internet Control Server. At the top, there is a logo and the text 'Наша организация Internet Control Server'. The user is logged in as 'Administrator (Administrator)'. A navigation menu includes 'информация', 'статистика', 'операции', 'тариф', 'пароль', and 'выход'. The main content area is divided into two sections: 'Пользователь (Administrator)' and 'Активация карт оплаты'. The 'Пользователь' section contains a table with various system parameters. The 'Активация карт оплаты' section has input fields for 'Серия' and 'Секретный код', and an 'Активировать' button. At the bottom, there is a table header for 'Финансовые операции с балансом' with columns for 'Дата', 'Тип', 'Сумма', 'Баланс', 'Описание', and 'Оператор'. The footer contains the copyright information: 'IdecO Software © 2005 www.ideco-software.com'.

Пользователь (Administrator)	
Электронная почта	
Тарифный план	Основной тариф
Пул IP адресов	Простой пул
IP адрес	10.128.0.57
NAT	192.168.1.2
Текущий кредит (расход)	0
Текущий дебит (оплата)	0
Прошлый остаток	0
Бух. баланс (по документам)	0
Текущий баланс	0

Активация карт оплаты	
Серия:	<input type="text"/>
Секретный код:	<input type="text"/>
<input type="button" value="Активировать"/>	

Финансовые операции с балансом					
Дата	Тип	Сумма	Баланс	Описание	Оператор

IdecO Software © 2005
www.ideco-software.com

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.

Глава 8. Встроенные модули системы

IdecO ICS содержит в себе дополнительные программные модули. Полноценное функционирование IdecO ICS, как сервера доступа, вполне возможно и без этих модулей. Они разработаны с целью упрощения развертывания новой сети и простого использования популярных сервисов. Модули оптимальным образом сконфигурированы и интегрированы в IdecO ICS. Все они имеют простую настройку, и их использование не требует постоянного администрирования. Следует иметь в виду, что если для организации требуется более широкие возможности, нежели предоставляемые этими модулями, то необходимо устанавливать отдельные серверы с другим программным обеспечением. IdecO ICS может быть сконфигурирован для использования других серверов. Например, если для внешнего WEB-сайта организации требуется более мощный WEB-сервер, то путем настройки DNAT можно перенаправлять запросы на отдельный WEB-сервер компании. Подробнее см. "[Создание правила Firewall](#)" на стр. 158

Каждая сетевая служба помещена в отдельную клетку chroot. Таким образом, даже потенциальное нарушение безопасности одной службы не приведет к уязвимости всего сервера. Каждую службу можно включить или выключить с помощью консольного меню. Каждый работающий дополнительный модуль отнимает ресурсы системы. Если сервер организации ограничен в ресурсах, не следует включать службы, в которых нет явной необходимости. Особенно к таким службам относится FTP-сервер.

Электронная почта

Служба электронной почты

IdecO ICS имеет встроенную почтовую службу. Эта возможность позволяет автоматически создавать для каждого пользователю личный почтовый ящик.

Почтовую службу можно глобально включить или отключить. Для этого зайдите в локальную консоль сервера и установите значение параметра

Включить встроенную почту. Кроме того, для правильной работы почтовой службы необходимо задать **Доменное имя**, используемое для почты. Это доменное

имя будет использоваться для e-mail адресов пользователей. Подробнее о задании этих параметров см. "[Почтовый сервер](#)" на стр. 110 в разделе [Конфигурирование сервера](#).

Каждому пользователю можно разрешить или запретить использовать встроенную электронную почту. Для этого зайдите на закладку **Информация** у пользователя и установите галочку **Включить почту**.

The image shows a list of user settings. The 'Включить почту' option is checked and highlighted with a red circle. Other options include 'Запретить вход', 'Переадресовать почту', 'Разрешить переподключение', 'Разрешить удаленное подключение', 'Просмотр ограничений родителя', 'Администратор технический', 'Администратор финансовый', and 'Администратор карт оплаты'.

Если для пользователя включена почта, то его e-mail будет иметь вид "<Логин>@<Доменное_имя>".

Ограничения

По умолчанию, в локальной консоли установлены следующие ограничения:

- Максимальный размер почтового ящика – 30Мб.
- Максимальный размер письма – 2 Мб.

Подробнее о настройке ограничений см. см. "[Почтовый сервер](#)" на стр. 110 в разделе [Конфигурирование сервера](#).

Переадресация почты

В Ideco ICS существует два вида переадресации почты.

1. **Простая переадресация.** Позволяет переадресовать почту со внутреннего почтового ящика на почтовый ящик, предназначенный для уведомления пользователя.
2. **Произвольная переадресация.** Позволяет настроить произвольную переадресацию почты.

Простая переадресация

Простая переадресация почты включается флажком **Переадресовать почту** в параметрах пользователя.

<input type="checkbox"/>	Запретить вход
<input checked="" type="checkbox"/>	Включить почту
<input type="checkbox"/>	Переадресовать почту
<input checked="" type="checkbox"/>	Разрешить переподключение
<input checked="" type="checkbox"/>	Разрешить удаленное подключение
<input type="checkbox"/>	Просмотр ограничений родителя
<input checked="" type="checkbox"/>	Администратор технический
<input checked="" type="checkbox"/>	Администратор финансовый
<input checked="" type="checkbox"/>	Администратор карт оплаты

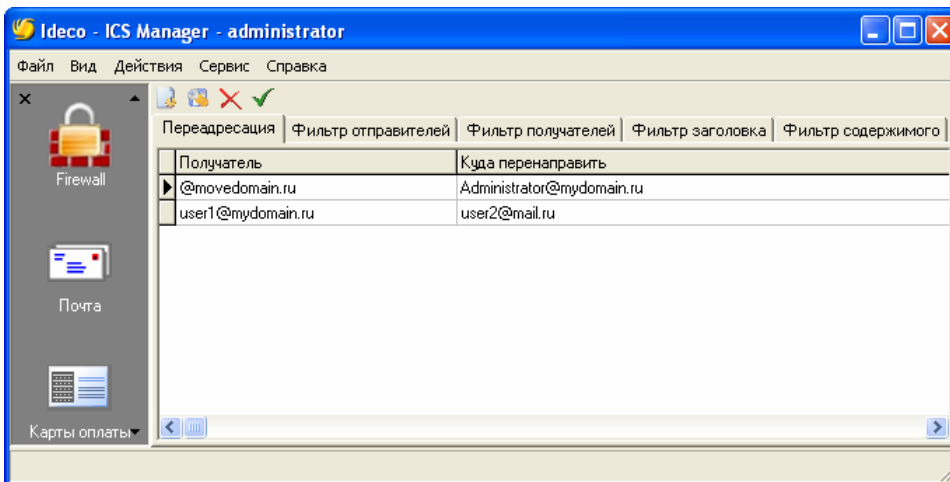
В этом случае, все письма, пришедшие на "<Логин>@<Доменное имя>", будут переадресованы на адрес, указанный в общих параметрах пользователя:

Абонент	Иванов Иван Иванович	Тариф	Тарифный план №1
Почта	ivanov	Пул	Первый пул
E-Mail	ivanov@company.com	IP	10.129. 0. 14
№	11635	isNat	<input checked="" type="checkbox"/> 195.195.195.195

Об указании общих параметров пользователя см. "[Общие параметры](#)" на стр. 49

Произвольная переадресация

Произвольная переадресация почты настраивается в разделе "Почта". Для перехода в этот раздел, выберите меню **Вид > Почта**, а затем вкладку "Переадресация".



На этой вкладке с помощью кнопок панели управления и контекстного меню можно создавать несколько записей переадресации почты. Для настройки переадресации необходимо ввести в столбец "получатель" и "Куда перенаправить" адреса, используя следующий синтаксис:

Адрес	Значение
user@domain	Конкретный адрес
user@	Указанный пользователь с любым доменом
@domain	Любой пользователь в указанном домене

Таким образом, возникает несколько вариантов переадресации, которые перечислены ниже:

Получатель	Куда перенаправить	Результат переадресации
user1@domain1.ru	user2@domain2.ru	С одного почтового ящика в другой
user1@domain1.ru	@domain.ru	С одного почтового ящика на другой, с таким же именем, но в другом домене
@domain.ru	user1@domain1.ru	Всех писем на выбранный домен на указанный почтовый ящик
@domain.ru	@domain.ru	Всех писем с одного домена на другой домен.
user@	user1@domain1.ru	Всех писем указанного пользователя на конкретный почтовый ящик
user@	@domain.ru	Всех писем указанного пользователя на другой домен

Примечание.

В поле "Куда перенаправить" можно указывать несколько адресов, указывая их через символ ";". Например, "user1@domain1.ru; user@domain2.ru". Не следует указывать одновременно несколько различных видов переадресации в одном правиле. Следует иметь в виду, что после произведения замены адресата, таблица переадресации просматривается вновь.

Если в поле "Куда перенаправить" встретится исходный адрес, то письмо будет доставлено по исходному адресу. Например, в случае перенаправления с "one@mydomain.ru" на "one@mydomain.ru; two@mail.ru", письмо уйдет в локальный ящик на домене "one@mydomain.ru" и продублируется в ящике на "two@mail.ru".

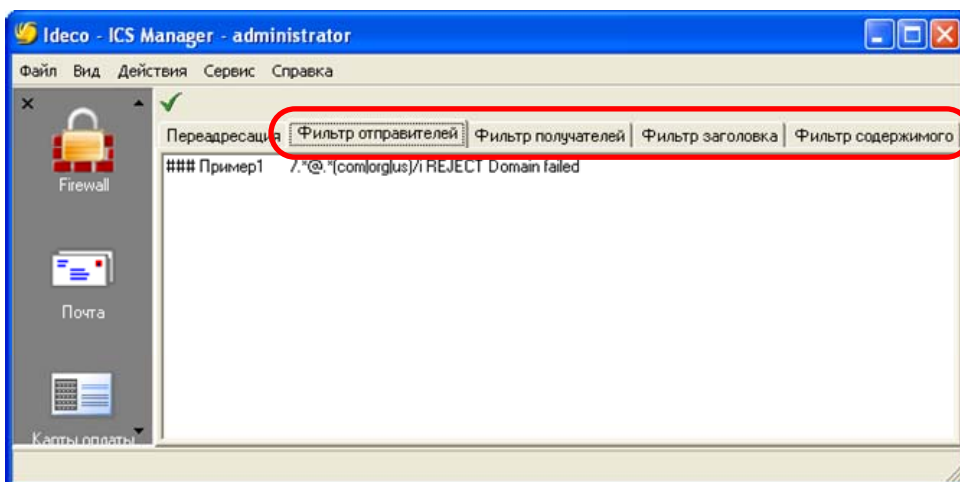
В качестве получателя и назначения можно указывать как адреса на почтовом сервере Idesco ICS, так и адреса на других почтовых серверах. Кроме того, в качестве получателя можно указывать несуществующие почтовые ящики.

Фильтры

Фильтрация почты предназначена для отсеивания писем, у которых, отправитель, получатель, заголовок или тело письма содержит текст, определяемый регулярным выражением.

Важно: Для того чтобы правильно настраивать фильтрацию почты рекомендуется обратиться к соответствующей литературе по почтовому серверу postfix (www.postfix.org) или к специалистам.

Фильтрация почты настраивается в разделе "Почта". Для перехода в этот раздел, выберите меню **Вид > Почта**, а затем одну из вкладок "Фильтр ...".



Всего есть четыре вкладки:

- **Фильтр отправителей.** Фильтрация отправителя письма.
- **Фильтр по получателей.** Фильтрация получателя письма.
- **Фильтр заголовка.** Фильтрация по полям почтовых заголовков.
- **Фильтр содержимого.** Фильтрация содержимого всего письма.

На каждой вкладке можно ввести один или несколько фильтров. Каждый фильтр разделяется новой строкой. Пустые строки и строки, начинающиеся с символ решетки ("#") игнорируются. Каждая строка имеет формат:

/искомое выражение/действие.

Например, чтобы запретить письма, в которых содержится фраза "Курсы английского", необходимо написать:

/курсы[:space:]английского/i REJECT We dont want spam.

Кодировка символов – WIN-1251. Для использования других кодировок необходимо произвести преобразование. Подробнее о синтаксисе фильтров можно узнать в Интернет по адресу: http://www.postfix.org/regexp_table.5.html.

Проверка на вирусы

Вся внутренняя почта, а также почта, отправленная через сервер Idesco ICS проверяется антивирусом. В качестве антивируса используется бесплатный антивирус ClamAV. Этот антивирус эффективен и может обнаруживать вирусы в почтовых сообщениях и вложенных файлах, в том числе архивах. Для включения этой возможности, в локальной консоли сервера включите флажок **"Включить проверку почты антивирусом"**. Для более эффективной борьбы с вирусами необходимо также установить флажок **"Включить автообновление антивирусных баз"**. Подробнее о настройке этих параметров см. ["Почтовый сервер"](#) на стр. 110.

Примечание: Почта, которая не принимается непосредственно с сервера Idesco ICS, не проверяется на вирусы. То есть, если почта проверяется с другого POP3-сервера в Internet, то она не будет проверена на вирусы. Сюда также входит почта, принимаемая через WEB-интерфейс, а также почта по протоколу IMAP.

Безопасность

Для того чтобы избежать потенциальных проблем с электронной почтой, которые могут возникнуть, например, при заражении вирусами, или при попытке отправить СПАМ, необходимо запретить пользователям отправлять электронную почту помимо почтового модуля Idesco ICS. Такой запрет гарантирует, что письма с вирусами не покинут организацию и не смогут навредить окружающим, так как вся отправляемая через почтовый модуль Idesco ICS почта проверяется на вирусы. Для этого необходимо во встроенном Firewall добавить следующее правило, запрещающее подключение к внешним SMTP-серверам:

- Протокол – TCP
- Source – 0.0.0.0, mask – 0.0.0.0, порт – любой (ALL)
- Destination – 0.0.0.0, mask - 0.0.0.0, порт SMTP (25)
- Действие – Запретить
- Путь – FORWARD

Настройка почтового ящика

Для работы с почтовой службой IdecO ICS, почтовая программа пользователя настраивается общепринятым способом.

- **Сервер входящей почты (POP3-сервер) – POP3.<домен>**, где <домен> – доменное имя сервера IdecO ICS. Вместо домена можно использовать IP-адрес, используемый для почты. Этот адрес настраивается в локальной консоли параметром **IP адрес почты для пользователей** (Подробнее см. ["Почтовый сервер"](#) на стр. 110). Этот адрес, как правило, совпадает с внешним IP-адресом сервера IdecO ICS.
- **Сервер исходящей почты (SMTP-сервер) – SMTP.<домен>**
- **Имя пользователя на POP-сервере** – логин пользователя в системе IdecO ICS (который указывается при подключении VPN-соединения), без значка "@" и названия домена.
- **Пароль** – Пароль пользователя в системе IdecO ICS.

Рекомендации и замечания по работе с почтой

Смена логина

Для пользователя создается почтовый ящик с именем логина. Таким образом, при смене логина у него будет новый почтовый ящик и новым e-mail адресом.

Очистка почты

При необходимости, может потребоваться очистка или удаление почтовых ящиков пользователей, которые перестали пользоваться своей почтой. Для этого в локальном интерфейсе зайдите в меню **Сервис > MC-Commander**. Зайдите в каталог **MAIL** и удалите неиспользуемый почтовый ящик. Вы также можете это сделать, подключившись удаленно с помощью Putty или WinScp. Подробнее см. ["Глава 6. Обслуживание"](#) на стр. 129

Тарификация почты

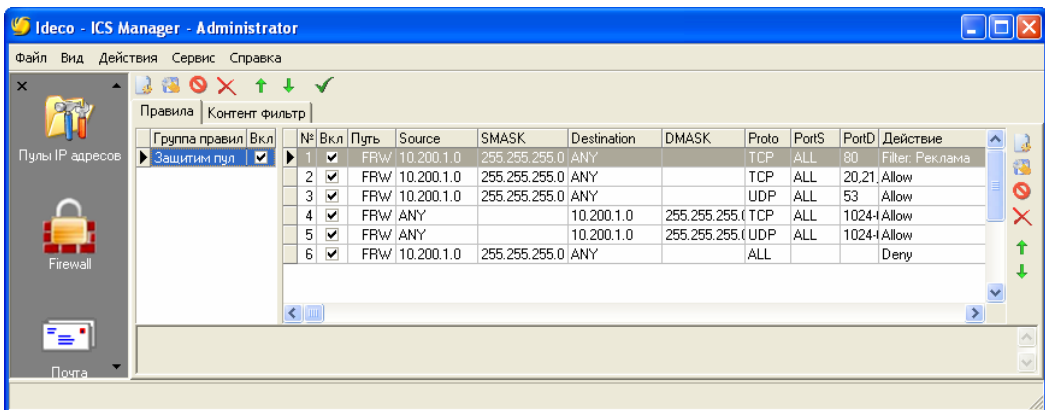
Как правило, не имеет смысла тарифицировать почтовый трафик пользователей. В случае, если это необходимо, необходимо назначить для почтовой службы отдельный IP-адрес. Подробнее об установке отдельного IP-адреса см. ["Почтовый сервер"](#) на стр. 110. В тарифном плане определить правило, например, с именем "Почта". В это правило включить соответствующий IP-адрес и указать стоимость входящего трафика. Тогда будет тарифицироваться весь трафик, входящий с этого адреса. При этом необходимо учитывать, и по возможности информировать пользователей, что почтовый трафик тарифицируется полностью, даже письма, отправленные самому себе.

Встроенный Firewall

По умолчанию, все пользователи Ideco ICS защищены технологией NAT, кроме этого возможно наложить различные ограничения для пользователей через Firewall.

Ideco ICS 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 ICS Manager.

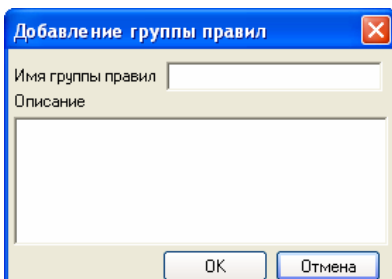
Важно: Для того чтобы правильно устанавливать правила Firewall рекомендуется обратиться к соответствующей литературе по безопасности или к специалистам



Во встроенном Firewall все правила объединяются в группы. Правила проверяются строго с верху вниз.

Создание группы правил


Для добавления группы правил, нажмите на кнопку  в верхней панели.

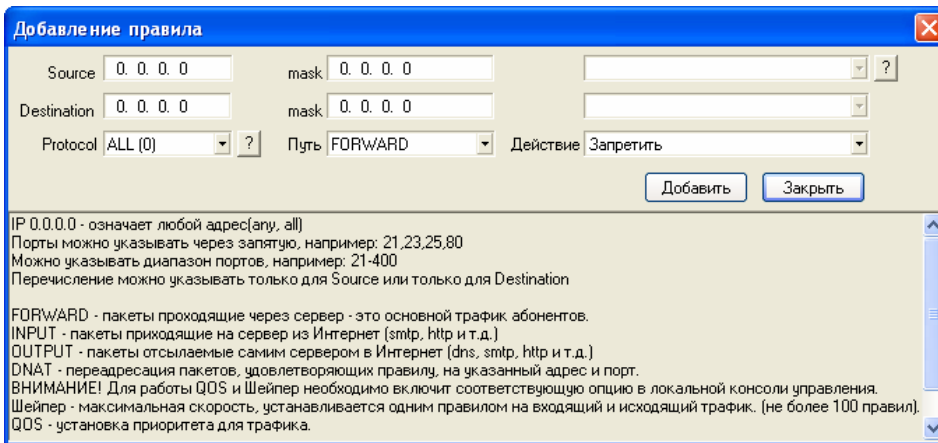


1. Введите **Имя группы правил** и описание (не обязательно).
2. Нажмите **ОК**.

После того, как группа создана, в нее можно добавлять правила Firewall.

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

Source, mask – IP-адрес и маска подсети источника пакетов.

Destination mask


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 ?

- ALL (0)
- ICMP (1)
- TCP (6)**
- UDP (17)

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.

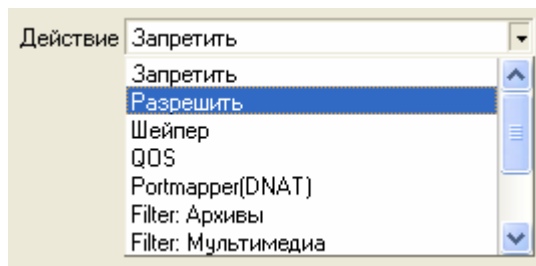
Замечание: При выборе протокола, отличного от **ALL** в верхней правой части окна появляются дополнительные опции правила

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 любые 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](#)" на стр. 106

Не рекомендуется создавать более 100 правил с действием **QOS** или **Шейпер**

Portmapper (DNAT) – Перенаправить трафик. При выборе этого правила, появятся поля: **Переадресовать на адрес** . . . **на порт** . 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 будут 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, проху](#)" на стр. 108.

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. "[Контент фильтр](#)" на стр. 161

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.

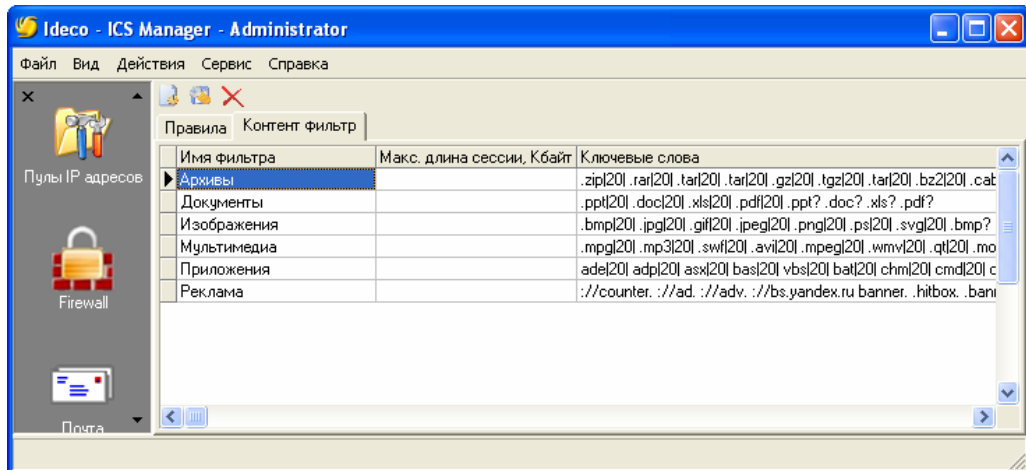
INPUT – Входящие пакеты, предназначенные для самого сервера.


OUTPUT – Пакеты, исходящие от самого сервера.

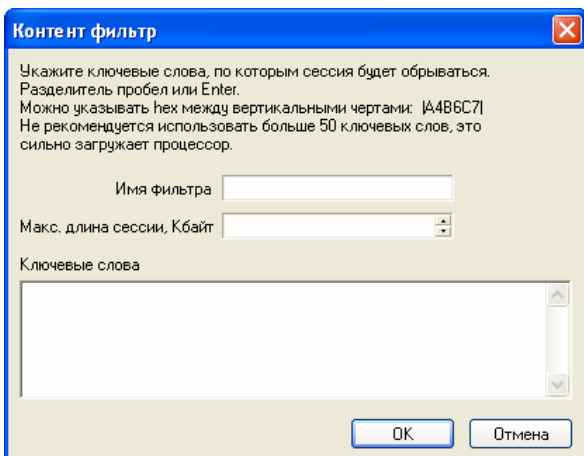
Если вы хотите ограничить доступ к серверу Idecso ICS, например, для блокировки серверов "спамеров", используйте путь **INPUT** и **OUTPUT**. Для ограничения доступа пользователя или нескольких пользователей к сайту, используйте путь **FORWARD**. Для более удобного ограничения нескольких пользователей 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.

Контент фильтр

Контент фильтр позволяет задавать правила для запрета трафика, в данных которого находится определенный текст. Контент фильтр настраивается в разделе Firewall на вкладке "**Контент фильтр**".



Во встроенном Firewall Idecso ICS можно создать несколько Контент-фильтров. Для создания такого фильтра необходимо нажать на кнопку  в панели инструментов. Появится окно:



Необходимо ввести следующие параметры:

Имя фильтра – Имя контент фильтра, 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.

Отключение Firewall

Если оказалось, что Firewall случайно сконфигурирован неверно и стало невозможным подключение к серверу с помощью IdecO ICS 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 ICS Manager и разобраться в ситуации.

Внешний сайт организации

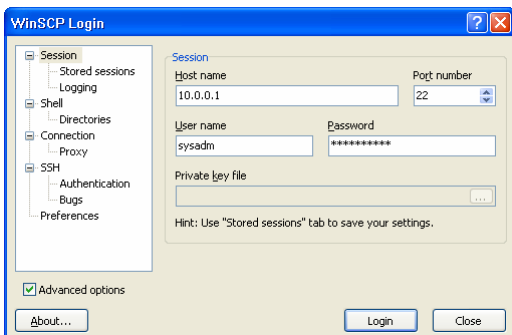
IdecO ICS включает в себя полнофункциональный многосайтовый веб-сервер. Он предназначен для размещения внешнего сайта организации. Сервер поддерживает динамическую генерацию страниц с помощью php, perl и других CGI программ. Кроме того, поддерживаются базы данных MySQL и Firebird.

Виртуальные домены

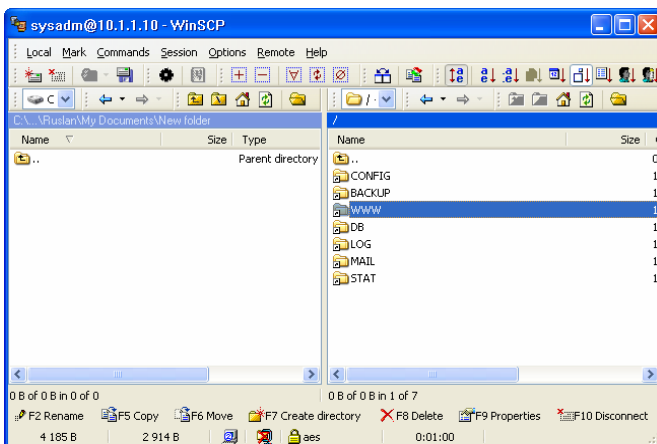
Встроенный в IdecO ICS внешний WEB-сервер позволяет размещать на нем несколько сайтов. Подробнее о регистрации доменов в зоне .ru см. сайт <http://www.nic.ru>. Для каждого сайта необходимо создать отдельный каталог в каталоге `/WWW/htdocs..` Каталог должен называться так же, как доменное имя сайта. Например, сайт www.myorg.ru необходимо разместить в каталоге `/WWW/htdocs/www.myorg.ru`. Если такой каталог не найден, то будет использована ссылка **Default**, которая по умолчанию указывает на каталог `/WWW/htdocs`. При желании, можно изменить ссылку так, что она будет указывать на определенный сайт. В случае, если многосайтовость не нужна, можно просто размещать файлы и каталоги сайта в каталоге `/WWW/htdocs`.

Размещение сайта

Для того чтобы разместить сайт на внешнем WEB-сервере, воспользуйтесь программой WinSCP, расположенной на диске с дистрибутивом.



Введите локальный IP-адрес сервера, логин **sysadm** и пароль, как в локальной консоли сервера. По умолчанию, пароль **servicemode**. Нажмите кнопку **Login**.



Примечание: Для работы этой возможности необходимо включить опцию "Разрешить управление файлами по SSH" в локальной консоли сервера. Подробнее см. "[Безопасность](#)" на стр. 105

Зайдите в правой панели в каталог **WWW**, а затем в каталог **htdocs**. В левой панели выберите каталог с вашим сайтом. Скопируйте клавишей F5 или перетащите файлы мышью из левой панели в правую. Индексный файл должен называться **index.htm**, **index.php** или **index.html**.

Готовые примеры: CMS Joomla! и форум phpBB

Вместе с WEB-сервером поставляются два open-source компонента: CMS **Joomla!** и форум **phpBB**. Установка этих компонентов полностью автоматическая – для этого в локальной консоли необходимо:

1. Включить поддержку MySQL

2. Включить внешний WEB-сайт
3. Произвести мягкую перезагрузку
4. Установить CMS Joomla! или форум phpBB.

Права доступа

При необходимости, можно настроить права доступа к файлам на WEB-сервере. Это можно сделать, если зайти в локальную консоль, затем выбрать пункт **Сервис > MC-commander**. Далее с помощью MC можно установить необходимые права доступа. Для установки корректных прав доступа необходимо обратиться к специалисту или прочитать соответствующую документацию.

Приложение А. Подключение к серверу IdecO ICS

При выборе авторизации пользователя по VPN, пользователи подключаются к серверу IdecO ICS с помощью VPN-соединения. При этом используются стандартные VPN драйвера. Настроить VPN-соединение можно вручную или автоматически. Для ручной настройки нужно знать адрес сервера IdecO ICS (**IP-адрес** или **доменное имя**). Для установки соединения нужно знать имя пользователя и логин. В этом разделе подробно описывается настройка VPN соединения в различных операционных системах, а также автоматическая настройка соединения.

Настройка VPN–соединения в Windows 2000/XP/2003

Информация этого раздела содержится также в Веб-интерфейсе пользователя

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 сервера IdecO ICS. 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**.

Настройка VPN-соединения в Windows 95/98/ME

Информация этого раздела содержится также в Веб-интерфейсе пользователя.

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 (Второго Издания) 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**. Поставьте 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 сервера IdecO ICS. 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**.

Автоматическая настройка VPN-соединения в Windows

В веб-интерфейсе пользователи могут скачать файл, с помощью которого выполняется автоматическая настройка VPN-соединения для работы с сервером IdecO ICS. Этот файл представляет собой профиль Microsoft Connection Manager.

При изменении с локальной консоли IdecO ICS 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 пользователями: 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 веб-интерфейс.

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 СМАК (Connection Manager Administration Kit – пакет администрирования диспетчера подключений), который входит в поставку серверных ОС Microsoft (Windows 2000/2003). Используя, СМАК вы можете создавать собственные файлы настройки соединений. При этом задавать свои настройки (адреса для подключения, графические элементы, иконки и другие параметры).

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 **ОК**. Это окно закроется. Нажмите кнопку **Connect** на главном окне.

Приложение В. Используемые технологии и ПО

Система базируется на ядре Linux из ветки 2.4. Дистрибутив создан с учетом всех требований системы. Принципиальное отличие – деление системы на изменяемую и константную (immutable) части. Система изначально построена так, что в ней невозможно изменить файлы, которые не должны меняться. То есть, даже если предположить возможность проникновения хакеров в систему, хакер не сможет изменить ни один системный файл, даже имея полные права в системе (root).

В Ideco ICS имеется модуль постоянного слежения за системой. Если какие-либо параметры работы системы выходят за определенные рамки, то система сама пытается предотвратить перегрузку сервера. При загрузке, система проверяет все параметры оборудования, состояние файловой системы и баз данных. Проверяется контрольная сумма всех неизменяемых файлов.

Вся информация о пользователях хранится в базе данных Firebird (Open Source реализация Interbase). Транзакционный подход обеспечивает стабильность хранения данных. База данных Firebird обеспечивает необходимую скорость работы и надежность хранимых данных.

В Ideco ICS предусмотрена система резервного копирования базы данных, в том числе на компакт-диски. Система может в автоматическом режиме записывать и перезаписывать компакт диски с резервными копиями, а также восстанавливать информацию из этих резервных копий.

При авторизации по VPN, происходит криптостойкое шифрование передаваемых данных. Таким образом, трафик VPN абонентов не может быть перехвачен или подставлен (spoofing) другими абонентами из локальной сети. Используемая при этом технология NAT исключает возможность подключения к компьютерам пользователей из сети Интернет.

Для подключения серверов можно убрать NAT для соответствующих учетных записей и использовать реальные IP-адреса.

Система построена так, что для каждого пользователя выделен персональный (и закрепленный за ним) IP-адрес. Таким образом, пользователь может выходить в Интернет с любого компьютера локальной сети, и учет трафика будет производиться только по этому пользователю.

Система хранит детализированную статистику каждого пользователя и каждой группы. В любой момент времени можно посмотреть, какие ресурсы Интернет посещал пользователь или вся группа. Информация агрегируется и сохраняется на лету.

С помощью встроенного WEB-интерфейса пользователи могут смотреть баланс, тарифный план, менять пароль, активировать карты оплаты, смотреть статистику.

Все настройки системы могут редактироваться с любой рабочей станции посредством Idecos ICS Manager'a. В том числе, создание, удаление, редактирование пользователей, тарифных планов, Firewall'a, просмотр статистики, редактор сайта и пр.

Самые основные системные параметры можно изменять только из локальной консоли серверного компьютера. Эти параметры, как правило, не изменяются. При изменении этих параметров необходима перезагрузка сервера. Из этой же консоли можно производить некоторые другие действия связанные с обслуживанием системы.

В систему встроена возможность удаленного управления по протоколу SSH. Также есть возможность подключиться по VPN из Интернет. При этом появляется возможность использовать локальную сеть из дома или командировки, а также управлять сервером с помощью ICS Manager'a.

В систему встроены Firewall, который позволяет запрещать или разрешать определенные виды трафика, базируясь на протоколе и номерах портов. В системе также имеется встроенная электронная почта. Для каждого пользователя системы может быть организован персональный почтовый ящик. Вся почта, приходящая на Idecos ICS проверяется встроенным антивирусом ClamAV. Есть возможность настроить автоматическое обновление антивирусных баз.

Встроенный DHCP сервер позволяет быстро развернуть систему в новой сети.

Безопасность и защита сервера

Значительно расширены стандартные механизмы защиты Linux:

- Все сетевые службы помещены в клетки chroot, нарушение безопасности одной службы не приведет к уязвимости сервера. Используется усиленный, по сравнению со стандартным chroot, и даже суперпользователь не может покинуть такой chroot.
- Запрет исполнения файлов с разделов с данными.
- Запрет монтирования новых файловых систем.
- Запрет монтирования rproc.
- Максимальное ограничение возможностей (capabilities) для всех служб и процессов.

- Система обнаружения и уничтожения exploit в ядре.

Усиленная схема защиты позволяет защитить систему даже от уязвимостей, которые могут обнаружены в будущем в Linux. Использование уникальных механизмов безопасности позволяет назвать IdecO ICS одним из самых защищенных и надежных серверов на сегодняшний день.

Ниже перечислены основные Open Source компоненты, входящие в состав IdecO ICS:

- **Linux kernel 2.4.24 i686 SMP**, с дополнительными исправлениями по безопасности.
- **squid 2.5.STABLE10.**
- **courier 4.1.1.**
- **poptop-1.2.1.**
- **pppd 2.4.3.**
- **thttpd 2.25b.**
- **postfix 2.1.5.**
- **openssh-3.5.**
- **firebird 1.0.3.972-0.64IO.**
- **iptables 1.2.9a-2.**
- **dnrd 2.17.**
- **dhcpcd 3.0pl1-23.**
- **php 4.3.8.**
- **vsftpd 1.1.3.**
- **ntpd 4.1.1c.**

Важно! Все перечисленные компоненты в дистрибутиве IdecO ICS настроены и сконфигурированы оптимальным образом. Дополнительное конфигурирование не требуется и во избежание проблем совместимости не рекомендуется.

Приложение С. Технические характеристики Ideco ICS

Параметр	Значение*
Погрешность определения момента срабатывания лимита при достижении порога отключения	Не более 1,5 Кб (один IP-пакет)
Интервал обновления статистики	В ядре real-time, интервал синхронизации с БД 100 сек
Интервалом агрегации детализированной статистики пользователей (src-dst)	30 мин
Открытые порты на внешнем интерфейсе	все порты по умолчанию закрыты
Открытые порты на внутреннем (локальном) интерфейсе	22, 25, 80, 1723
Открытые порты на защищенном интерфейсе	22, 25, 80, 110, 53, 3050 (только для администраторов)
Максимальное количество зарегистрированных пользователей в БД	Ограничивается только лицензионным соглашением
Поддерживаемое шифрование VPN канала	без шифрования, 40, 56 и 128 бит прре. По умолчанию шифрование включено
Погрешность определения стоимости трафика (при цене 1 у.е./1 Мб)	0,005%
Максимальное время потери информации о трафике при внезапном отключении питания	не более 100 сек
Время существования установленного авторизованного подключения	не ограничено
Количество одновременно установленных VPN и PPPoE соединений	2048
Время задержки пакетов в обычном режиме работы	<= 1 мс

*Значения некоторых параметров могут изменяться в зависимости от конфигурации.

Приложение D. 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 (343) 345-15-75.

Алфавитный указатель

A

Active 89
Administrator 22, 42

C

СМАК 169

D

daily 129
DHCP диапазон адресов 116
DHCP сервер 15
DNS сервер 1 95, 100
DNS сервер 1 для пользователей 96
DNS сервер 2 95, 100
DNS сервер 2 для пользователей 96

E

E-mail 49, 55, 74, 150
Enterprise Edition 14

F

Firewall 23, 86, 157
FORWARD 161
FTP-сервер 114

H

html 90

I

Ideco ICS 17, 25, 173
Ideco ICS Manager 22, 37, 132
index.htm 164
INPUT 161
Internet интерфейс (MAC адрес) 95

Internet интерфейс, IP-адрес 95
Internet интерфейс, имя сервера 95
IP-адрес 18, 85, 87, 166, 167
isNat 50, 55

J

Joomla! 164

K

Keylogger 79

M

MAC-адрес 49
Microsoft Connection Manager 168
Microsoft Excel 141
monthly 129
MS Excel 135, 141

N

NAT 24, 65
Network Address Translation 65
Not Active 89
nternet веб-сервер 113

P

phpBB 164
POP3-сервер 156
Portmapper (DNAT) 160
PPPoE-сервер 14
Protocol 159

Q

QOS 159
Qos и Шейпер 106

S

SAFEMODE 27
servicemode 27, 42, 91
SMTP-сервер 156
source–destination 60
Standard Edition 14
sysadm 164

V

VPN 24
VPN (Virtual Private Network) 18
VPN IP-адрес сервера 95
VPN-сервер 14
VPN-соединение 70, 71, 166

W

weekly 129
winpopup 74
WinSCP 129, 163

A

Абонент 49
Абонентская плата 51, 56
Автоматическая настройка VPN-соединения 168
Автоматическое обнуление баланса 51, 56, 66
Автоматическое создание акта 64
Автоматическое формирование акта 139
Авторизация по IP 35
Авторизация пользователей 34
Авторизация через IdecOAgent 77
Административный интерфейс
(IdecO ICS Manager) 20
Администратор 22, 143
 карт оплаты 43
 технический 42, 53
 финансовый 42, 53
Администратор карт оплаты 53
Администратор финансовый 133
Администраторы 42
Администраторы групп 44
Администрирование 37
Адрес веб-интерфейса 122
Активации карты оплаты 146
Активирована 146
Активированная 146
Аудит событий 88

Б

База Данных 19
Баланс 51, 56, 63
Баланс (бух.) 133
Баланс группы 63
Баланс пользователя 63
Безопасность 23, 105
Безопасность логинов и паролей 79
Блокирована 146
Блокирование
 отдельной карты 148
 серии 148

В

Ввод значений реквизитов 139
Веб-интерфейс пользователя 20, 122
Включен 87
Включить встроенную почту 150
Включить почту 52, 151
Внешний сайт организации 163
Восстановить 69
Восстановление пользователя 45
Время начала сессии 60
Всем потомкам 75
Встроенные модули системы 150
Встроенный Firewall 15, 157
Вход 125
Входящий 80
Вывод на печать 135
Выгрузить шаблон 142

Г

Главное меню 40
Главное окно IdecO ICS Manager 40
Главный администратор 22, 42
Группа 46, 55
Группа пользователей 44
Группировка 60
Групповые операции 137
Группы 21
Группы "Счетчики" 68

Д

Дерево пользователей 44
Детализированная статистика 60
Диапазон 87
Добавить подсеть в правило 84
Добавить правило 82

Документы 133
 Доменное имя 150, 166
 Дополнительные возможности Idecos ICS 132
 Дополнительные настройки 103
 Доступ запрещен 85
 Доступ к почте из Интернет 52
 Древоподобная структура 21, 44

Ж

Журнал операций 136, 137

З

Загрузить шаблон 142
 Закладка "Групповые операции" 137
 Закладка "Журнал операций" 136
 Закладка "Информация"
 у группы 53
 у пользователя 48
 Закладка "Операции" 61, 132
 Закладка "Состав" (у группы) 62
 Закладка "Статистика" 59
 Закрытая часть 122, 124
 Закрытие периода 130
 Закрытие ресурсов 85
 Закрытые ресурсы 85
 Закрытый 86
 Запретить вход 52, 57
 Запрещено 85, 86
 Зарезервировать 87
 Защита 23
 Значения по умолчанию для новых
 пользователей 58

И

Имя VPN-сервера 167
 Интервал обновления 173
 Интернет карты 145
 Интерфейс Idecos ICS Manager 78
 Исключение IP-адресов 85
 Использование NAT 65
 Использование почты 72
 Используемые технологии и ПО 170
 Исправить баланс 133
 исходящий 80
 Итого текущий баланс 133

К

Карты оплаты 16, 141, 145, 146

Код 146
 Кол-во карт 147
 Компьютеры пользователей 26
 Контактная информация 89, 124
 Контакты 174
 Конфигурирование 25
 Конфигурирование сервера 94
 Конфигурирование сети 28
 Копирование-вставка 78
 Корзина 68

Л

Лицевой счет 21, 133
 Логин 47, 49
 Локальная консоль сервера 20, 91
 Локальный интерфейс (MAC адрес) 95, 99
 Локальный интерфейс, IP-адрес 95
 Локальный интерфейс, имя сервера 95
 Локальный интерфейс, маршруты 95

М

Маршрутизация и удаленный доступ 35
 Маска сети 85
 Межсетевой экран (Firewall) 19
 Модуль отказоустойчивости 15
 Монитор 88
 Мониторинг 92

Н

Назначение 17
 Найти 69
 Настройка 167
 Настройка VPN-соединения
 в Mac OS X 169
 в Windows 2000/XP/2003 166
 Настройка почтового ящика 156
 Настройка синхронизации с LDAP/AD сервером
 59
 Настройка соединения 167
 Начальное конфигурирование сервера 27
 Начисление средств 64
 Нет финансово-ответственного 73
 Новости 90, 124
 Номинал 147
 Нумерация операций 134

О

Обновить данные 45

Обновлен 89
Обнуление баланса 64, 133
Обнуление баланса, дата 67
Обнуление баланса, период 67
Обнуления баланса 56
Обслуживание 129
Общие параметры 49, 55
Ограничение доступа 22
Ограничение расходов группы 67
Ограничение расходов пользователя 67
Окончание 146
Операции 61, 127, 132, 136
Операции над картами оплаты 147
Оплата 63, 133
Оповещение пользователей 74
Основная статистика 60
Основы Ideco ICS 17
Особенности работы 71
Остаток 63, 133
Остаток на начало периода 64
Отдельно по подсетям 60
Отключение файрвола 163
Отключить по дате 51, 56
Открытая часть 122
Открытые порты 173
Отправить 75
Отправить сообщение 45, 74
Отправка сообщений 74
Очистка почты 156

П

Панель инструментов раздела 40
Панель разделов 40
Параметры карт оплаты 146
Параметры ограничений 55
Параметры разрешений 52, 57
Пароль 47, 72, 128
Переадресация почты 151
Переадресовать почту 52, 151
Перезагрузка сервера 120
Переместить реквизит 139
Переподключение 70
Период 60
Персональный раздел 122
Печать 135
Печать карт оплаты 148
Платежи по картам оплаты 149
Плоская сеть 28
По каждому пользователю 60
По подсетям 60
По сессиям 60
Подвести баланс 133

Подключение к Ideco ICS 38
Подключение к виртуальной частной сети 166
Подключение к серверу Ideco ICS 166
Подключить к сети на рабочем месте 166
Подтверждение пароля 47
Поиск пользователей 45, 69
Политика 83
Пользователи 21
Пользователь 21, 46
Пользователь отключен 73
Пользователь с NAT 45
порог отключения 63
Порог отключения 51, 56, 64, 67
Порог предупреждения 51
Порог предупреждения 56
Порядок установки 25
Почтовые сервер 19
Почтовый сервер 110
Права доступа 165
Правило 80
превышен лимит 73
Предотвращение несанкционированного расхода трафика 68
Признак "Финансовый" 65
Принцип действия 17
Принцип работы 66, 144
Приход 133
Проверить 73
Проверка на вирусы 155
Проверка пользователя 73
Просмотр ограничений родителя 57
Просмотр ограничения родителей 53
Пул 49, 55
Пул IP-адресов 86
Пулы IP-адресов 86

Р

Рабочая область раздела 40
Разблокирование
отдельной карты 148
серии 148
Размер 55
Размер письма 151
Размер почтового ящика 151
Разрешено 86
Разрешить VPN соединения из Интернет 105
Разрешить переподключение 53, 57, 70
Разрешить почту 57, 72
Разрешить удаленное подключение 53, 57, 71
Расположение администраторов 143
Расход 63

Расход в денежном эквиваленте 60
 Расход за текущий период 133
 Расход коневой группы 64
 Расход/Акт 133
 Расходу за текущий период 140
 Редактирование списка реквизитов 139
 Редактирование шаблонов 142
 Редактор отчетов 142
 Редактор правил и сетей 83
 Редактор сайта 89
 Режим только для чтения 45
 Резервное копирование 129
 Резервные копии БД 118
 Реквизиты 138
 Рекомендации и замечания 78

С

Секретный код 146
 Сервис 119
 Серия 146
 сетевой интерфейс 81
 Сетевые параметры 94
 Сеть 83
 Сеть с подсетями 28
 Системные требования 25, 38
 Служба электронной почты 150
 Смена логина 156
 Смена пароля 72, 120, 128
 Событие 88
 Создание 146
 карт оплаты 146
 нового пользователя 45
 новой группы 45
 Создание группы 46
 Создание закрытых ресурсов 85
 Создание пользователя 46
 Создании пула IP-адресов 87
 Создание тарифного плана 81
 Создание тарифного плана по учету времени 145
 Создать группу 46
 Создать новое правило 84
 Создать новый реквизит 139
 Создать пользователя 47
 Создать серию 147
 Создать тарифный план 81
 Состав Idco ICS 19
 Состояние 89
 Сохранение изменений 45
 Сохраненные конфигурации 118
 Списание средств 64
 Список операций 136

Способ доставки 74
 Срок действия 147
 Статистика 59, 60, 126
 Статистика посещений 60
 Статистика расхода трафика 59
 Стоимость трафика 80
 Страница
 "Детализированная статистика" 126
 "Информация" 125
 "Операции" 127
 "Пароль" 128
 "Статистика" 126
 "Тариф" 127
 Страница "Вход" 124
 Страница "Главная" 123
 Страница "Новости" 124
 Страница "Поддержка" 124
 Страница "Подключение" 124
 Страница "Тарифы" 124
 Структуру предприятия 21, 44
 Счет клиента 146
 Счет на предоплату 133

Т

Тариф 49, 55
 Тарификация 22, 23
 Тарификация почты 156
 Тарифные планы 80, 90
 Тарифный план 23, 81, 85, 86, 124, 144
 Технические характеристики 173
 Требования к серверу 25

У

Удаление БД статистики посещений 130
 Удаление пользователей 68
 Удаленное подключение 70
 Удалить реквизит 139
 Удалить/Откатить 142
 Уничтожена 146
 Уничтожение серии карт 148
 Управление 22
 Управление картами оплаты 146
 Управление пользователями 44
 Управление потомками 58
 Установка 25
 автоматического обнуления 67
 Установка Idco ICS 26
 Установка VPN-адаптера 167
 Установка автоматического формирования акта 140

Учет 22

Учет времени 144

Ф

Финансовый 21, 51, 55, 65

 группа 65

 пользователь 65

Формирование

 акта

 период 140

 операции 134

Формирование акта 56

Формированиеакта

 дата 141

Х

Хозяин 88

Ц

Цена 146

Ш

Шаблон 141

Шаблоны документов 141

шифрование VPN канала 173

Э

Электронная почта 150