



# **РУКОВОДСТВО АДМИНИСТРАТОРА**

**«Интернет Администратор для Сети»  
версия 3.5, обновление 20**

<b>РАЗДЕЛ 1 – ВВЕДЕНИЕ.....</b>	<b>3</b>
<b>РАЗДЕЛ 2 – УСТАНОВКА.....</b>	<b>4</b>
РАЗДЕЛ 2.1. — СИСТЕМНЫЕ ТРЕБОВАНИЯ.....	4
РАЗДЕЛ 2.2. — ПОДГОТОВКА К УСТАНОВКЕ.....	4
РАЗДЕЛ 2.3. — ПРОЦЕСС УСТАНОВКИ.....	7
РАЗДЕЛ 2.4. – КОМПОНЕНТЫ ИНТЕРНЕТ АДМИНИСТРАТОРА.....	13
<b>РАЗДЕЛ 3 – НАСТРОЙКА СИСТЕМЫ.....</b>	<b>16</b>
РАЗДЕЛ 3.1. — НАСТРОЙКА СЕТЕВЫХ ПАРАМЕТРОВ.....	16
РАЗДЕЛ 3.2. — НАСТРОЙКА IADMIN PROXY.....	18
РАЗДЕЛ 3.3. — НАСТРОЙКА РЕЖИМА РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЯ НА КОМПЬЮТЕРАХ.....	20
РАЗДЕЛ 3.4. — НАСТРОЙКА ОТСЛЕЖИВАЕМЫХ ПОРТОВ ИНТЕРНЕТ.....	21
РАЗДЕЛ 3.5. — МОНИТОРИНГ ВЕБ САЙТОВ.....	21
РАЗДЕЛ 3.6. — ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ.....	22
<b>РАЗДЕЛ 4 – УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ.....</b>	<b>24</b>
РАЗДЕЛ 4.1. — ПОЛЬЗОВАТЕЛИ, ГРУППЫ И КОМПЬЮТЕРЫ.....	24
РАЗДЕЛ 4.2. — ЖУРНАЛ ДОСТУПА В ИНТЕРНЕТ.....	31
РАЗДЕЛ 4.3. — IADMIN WEB СЕРВЕР – СТАТИСТИКА И РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ.....	33
<b>РАЗДЕЛ 5 – КОНТРОЛЬ ДОСТУПА В ИНТЕРНЕТ.....</b>	<b>37</b>
РАЗДЕЛ 5.1. – СИСТЕМА ПРАВИЛ.....	37
РАЗДЕЛ 5.2. – КАК РАБОТАЮТ ПРАВИЛА.....	38
РАЗДЕЛ 5.3. – ЭЛЕМЕНТЫ ПРАВИЛА.....	39
<b>РАЗДЕЛ 6 – СЕРВИС.....</b>	<b>45</b>
РАЗДЕЛ 6.1. — ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ.....	45
РАЗДЕЛ 6.2. — ЛИЦЕНЗИРОВАНИЕ БАЗЫ КАТЕГОРИЙ.....	45
РАЗДЕЛ 6.3. – ОБНОВЛЕНИЕ БАЗЫ КАТЕГОРИЙ.....	46
РАЗДЕЛ 6.4. — НЕОТСЛЕЖИВАЕМЫЕ РАБОЧИЕ СТАНЦИИ.....	47
РАЗДЕЛ 6.5. — ОЧИСТКА БАЗЫ ДАННЫХ.....	48
РАЗДЕЛ 6.6. - ПОЛЬЗОВАТЕЛЬСКИЕ САЙТЫ В КАТЕГОРИЯХ.....	49
РАЗДЕЛ 6.7. – ПОИСК ПОЛЬЗОВАТЕЛЬСКИХ ИМЕН.....	50
<b>РАЗДЕЛ 7 – ОТЧЕТЫ.....</b>	<b>51</b>
РАЗДЕЛ 7.1. — ФОРМИРОВАНИЕ ОТЧЕТОВ.....	51
РАЗДЕЛ 7.2. — НАСТРОЙКА ОТЧЕТОВ.....	51
РАЗДЕЛ 7.3. — СПИСОК ОТЧЕТОВ.....	52
РАЗДЕЛ 7.4. — ЭКСПОРТ ДАННЫХ В ФОРМАТЕ W3C.....	52
<b>РАЗДЕЛ 8 – БАЗА ДАННЫХ И ПОДДЕРЖКА MICROSOFT SQL SERVER.....</b>	<b>53</b>
РАЗДЕЛ 8.1. — БАЗА ДАННЫХ ПО УМОЛЧАНИЮ.....	53
РАЗДЕЛ 8.2. — БАЗА ДАННЫХ НА MS SQL SERVER.....	53
РАЗДЕЛ 8.3. — РЕЗЕРВНОЕ КОПИРОВАНИЕ.....	57
<b>РАЗДЕЛ 9 – РАСПРЕДЕЛЕННЫЕ СЕТИ И КОЛЛЕКТОРЫ.....</b>	<b>58</b>
РАЗДЕЛ 9.1. — СОЗДАНИЕ ЦЕНТРАЛЬНОГО ХРАНИЛИЩА ДАННЫХ.....	58
РАЗДЕЛ 9.2. — УСТАНОВКА ДОПОЛНИТЕЛЬНЫХ КОЛЛЕКТОРОВ.....	58
РАЗДЕЛ 9.3. — УПРАВЛЕНИЕ И АДМИНИСТРИРОВАНИЕ.....	59

## РАЗДЕЛ 1 – ВВЕДЕНИЕ

Программный комплекс «Интернет Администратор для Сети» - предназначен для полного и всестороннего контроля доступа в глобальную сеть Интернет на предприятии. Программа осуществляет мониторинг за действиями пользователей в Интернет, ограничивает ресурсы пользователей и доступ к объектам сети Интернет.

Мониторинг обеспечивает предоставление информации о том, как используется Интернет на предприятии, а именно: Кто, Когда, Куда и Как осуществил доступ, сколько времени пробыл на данном ресурсе, сколько данных загрузил и отправил.

К ресурсам пользователя относятся трафик и время, проведенное в сети Интернет, которые могут быть ограничены за определенный период времени.

К объектам Интернет относятся: Категории базы URL, домены DNS, сайты, подсети, протоколы, время доступа, URL путь, страна сайта и тип контента.. Политика доступа реализуется на основе гибкой системы правил доступа и определяет Кто, Когда, Куда и Как может получить доступ. Наличие базы сайтов, разделенных на категории, позволяет наиболее гибко управлять доступом в Интернет.

В комплексе «Интернет Администратор для Сети» предусмотрены различные типы регистрации пользователей на рабочих станциях. Это может статическая привязка пользователя к компьютеру, пользователь будет зарегистрирован под доменным именем после входа в Microsoft Active Directory, либо пользователю необходимо будет ввести свое собственное имя и пароль.

«Интернет Администратор для Сети» работает на популярной платформе Windows, что позволяет применять данную систему в различных корпоративных сетях. Программный комплекс «Интернет Администратор» основан на технологии перехвата сетевых пакетов. Это позволяет устанавливать систему на сервер, не являющийся шлюзом в Интернет, если он подключен к зеркалирующему порту (monitoring port) коммутатора, а порт, где проходит Интернет-трафик, определен как зеркалируемый (monitored port).

«Интернет Администратор» выводит более 10 отчетов, наглядно показывающих характер использования корпоративного Интернет доступа. Выводимые отчеты можно распечатывать, сохранять, переводить в ряд популярных форматов и публиковать на веб серверах.

## РАЗДЕЛ 2 – УСТАНОВКА

### Раздел 2.1. — Системные требования

Системные требования, предъявляемые комплексом «Интернет Администратор для Сети» к программно-аппаратному обеспечению:

#### Операционная система:

Windows 7; Windows 7 Service Pack 1; Windows 8; Windows 8.1; Windows Server 2008 R2; Windows Server 2008 R2 SP1; Windows Server 2012; Windows Server 2012 R2

Примечание: поддерживаются только 64 разрядные ОС.

Процессор: x64 совместимый с Intel, имеющий частоту не ниже 1,5 ГГц.

Оперативная память: не менее 2ГБ, рекомендуется 4ГБ

Дисковое пространство: 4,2 ГБ дискового пространства

Другое:

- Сетевой адаптер без запрета на расширенный (promiscuous) режим работы. В расширенный режим может переходить любой сетевой адаптер, главное чтобы этот режим не был запрещен в настройках адаптера.

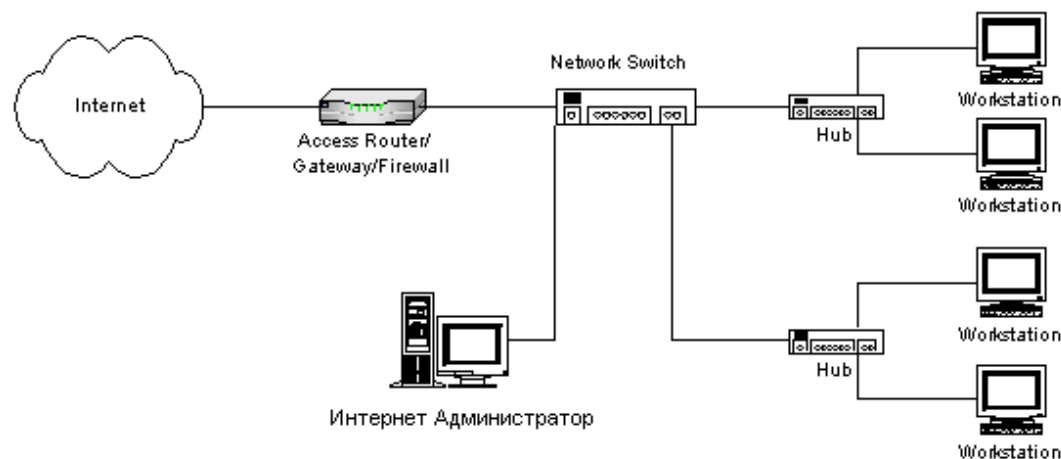
- Отсутствие на сервере программ-файрволов, способных ограничить поступление сетевых пакетов, не предназначенных для локального сервера, см. <http://www.iadmin.ru/products/?pid=40>

- Включенный Microsoft .NET Framework 3.5 с пакетом обновления 1 (SP1) или Microsoft .NET Framework 4.0.

### Раздел 2.2. — Подготовка к установке

Местоположение сервера с «Интернет Администратором» в сети является важным звеном. Так как принцип работы программы основан на перехвате сетевых пакетов, установку нужно производить на сервер, расположенный в том сегменте сети, где проходит трафик в Интернет.

#### Вариант 1 (рекомендуемый)



Представлена сеть с **управляемым коммутатором (Smart network switch) с поддержкой зеркалирования портов**. На управляемом коммутаторе нужно настроить зеркалирование портов, и указать порт, к которому подключен сервер с Интернет Администратором, в качестве зеркалирующего порта (monitoring port), а порт, через который идет Интернет-трафик, определить как зеркалируемый (monitored port). Таким образом весь трафик, проходящий в Интернет, будет попадать на сервер с Интернет Администратором для анализа.

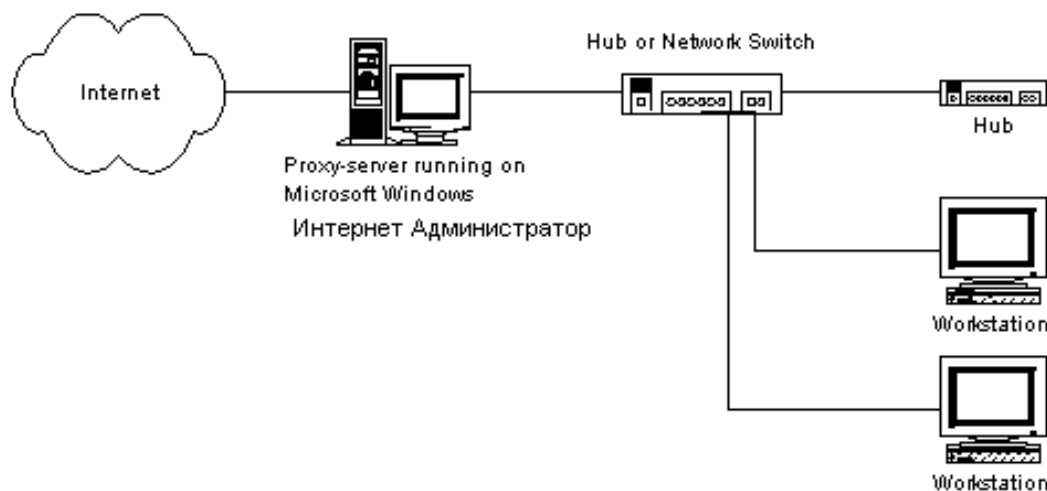
Этот вариант имеет 2 важных преимущества:

- в случае отказа сервера, Интернет продолжит работать!
- Интернет Администратор никак не влияет на сетевой трафик, не обрабатывает реальные пакеты и не затормаживает работу сети!

Интернет Администратор можно подключить и к **аппаратному маршрутизатору с поддержкой зеркалирования портов**, выполняющему роль шлюза в Интернет. Только в качестве зеркалируемых портов в этом случае нужно выбирать внутренние LAN порты, куда подключены пользователи интернета.

Блокирование TCP соединений осуществляется путем отправки специальных пакетов. В некоторых управляемых коммутаторах, например, CISCO, при конфигурации зеркалирования портов, на нем закрывается возможность отправки сетевых пакетов. То есть компьютер, подключенный к такому порту, не увидит сеть, а Интернет Администратор сможет только отслеживать трафик, а блокировка работать не будет. Для работы сети и блокировки используйте вторую сетевую карту на этом сервере, подключенную к обычному (не зеркальному) порту. В настройках Интернет Администратора необходимо будет указать данную карту как карту для блокировки.

## Вариант 2



Если в качестве шлюза для доступа в Интернет используется роутер, прокси-сервер или транслятор сетевых адресов (NAT) на платформе Windows, установку можно произвести прямо на этот компьютер. Однако с некоторыми программами есть несовместимость, подробнее о них <http://www.iadmin.ru/products/?pid=40>

Если используется Microsoft TMG Server 2010, то Интернет Администратор интегрируется с ним в процессе установки и будет получать трафик только от TMG сервера, а не из сетевого сегмента. Компонент IAdmin Proxy может быть использован независимо.

### Примечание.

Большинство текущих малых сетей подключаются провайдерами с помощью аппаратного оборудования, когда в сети установлен единственный неуправляемый коммутатор, к которому подключен интернет канал и другие компьютеры. Существует метод превращения такой сети в Вариант 2 без использования дополнительного программного обеспечения и без перестроения логической схемы сети. Это реализуется с применением возможности создания **моста** между двумя сетевыми картами в операционных системах Microsoft Windows. Мост не является шлюзом или роутером и пропускает трафик через себя всквозную, поэтому остальные компьютеры перенастраивать не нужно.

Для создания моста выполните следующее:

- Выберите компьютер из вашей сети, где будет работать «Интернет Администратор».
- Установите в него вторую сетевую карту.

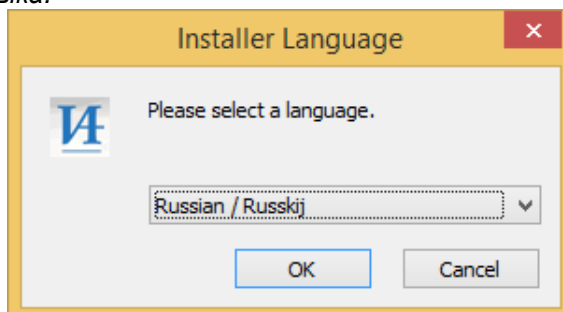
## Интернет Администратор для Сети версия 3.5, обновление 20

- В свойствах сетевого окружения выберите две сетевые карты и в меню по правой кнопке мыши укажите «Подключения типа Мост» (Bridge Connections).
- Задайте созданному мосту IP адрес и другие параметры протокола TCP/IP, которые были у первой сетевой карты.
- Извлеките сетевой кабель, идущий от провайдера в коммутатор вашей сети, и подключите его к новой сетевой карте.
- Проверьте работу Интернет с данного компьютера и с других рабочих станций.
- Учтите, что если данный компьютер будет выключен, то другие рабочие станции не получат доступ в Интернет.

### Раздел 2.3. — Процесс установки

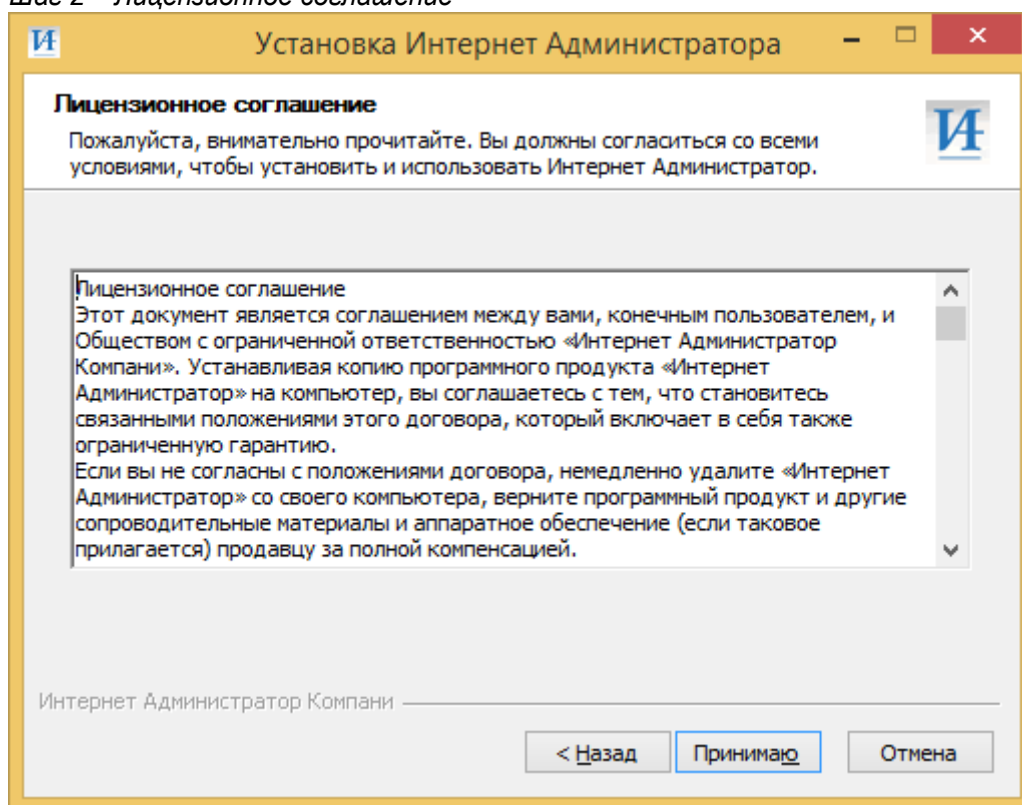
Для начала установки запустите файл инсталлятора, загруженный с сайта. В процессе установки Вы пройдёте несколько шагов, на которых вам будет предложено ввести необходимые данные или ознакомиться с информацией.

#### Шаг 1 – Выбор языка.



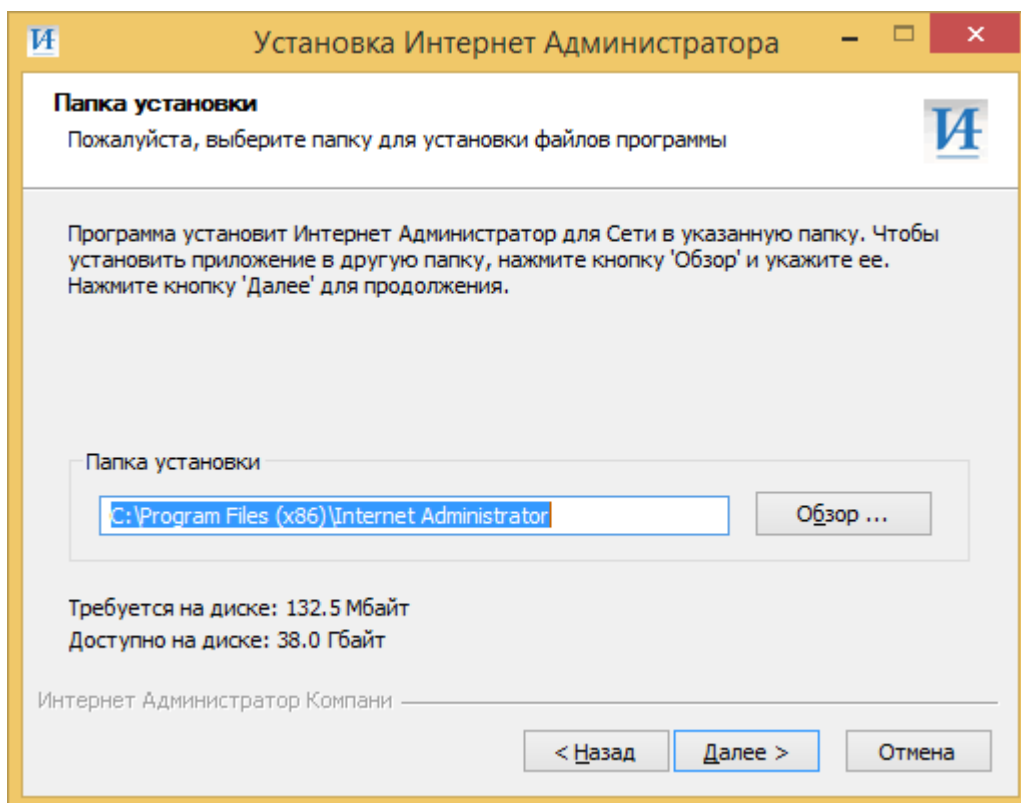
Интернет Администратор можно установить на русском или английском языках. Выбор языка будет доступен, если в системе установлена поддержка нескольких языков. Если у Вас английская версия Windows и не настроено использование языка по умолчанию для не-Юникод программ, то выбора языка не будет и программа установится только на английском языке.

#### Шаг 2 – Лицензионное соглашение



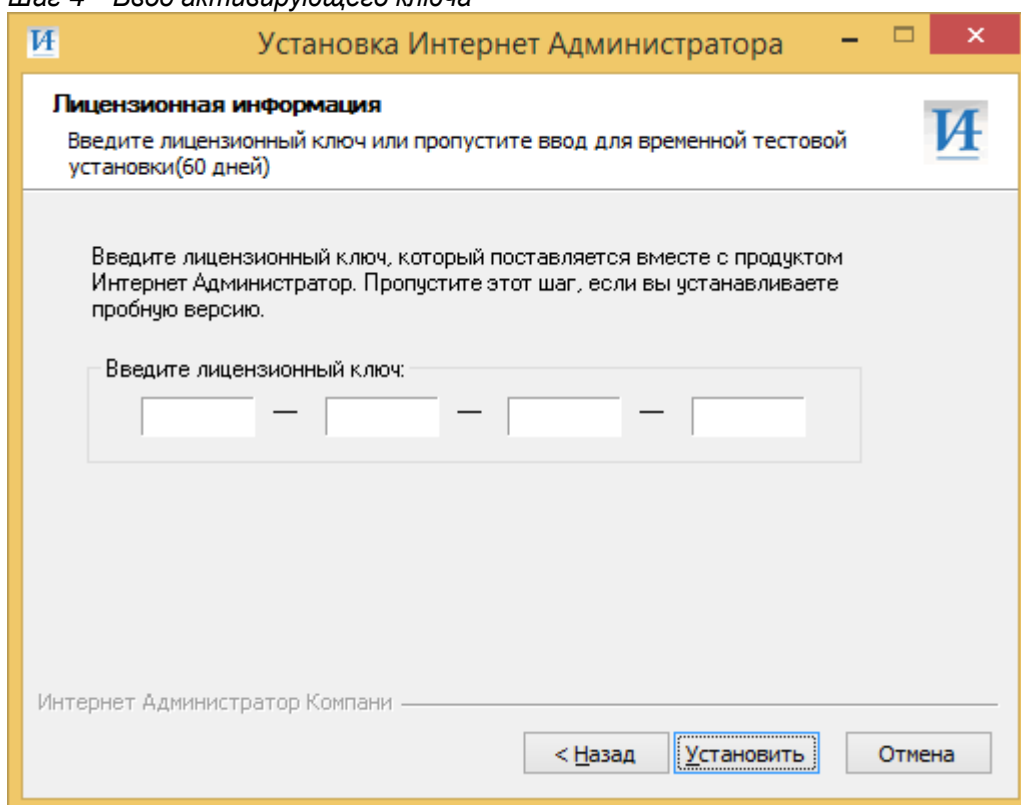
Ознакомьтесь с содержанием лицензионного соглашения, которое регламентирует порядок использования программного обеспечения и ответственность производителя и пользователя. Для продолжения установки Вам необходимо принять условия лицензионного соглашения, нажав кнопку **“Принимаю”**

#### Шаг 3 – Выбор каталога для установки



Выберите каталог, в который Вы желаете установить «Интернет Администратор». По умолчанию инсталлятор предложит Вам установить программу в подкаталог Internet Administrator каталога программных средств Windows, например, **C:\Program Files\Internet Administrator**.

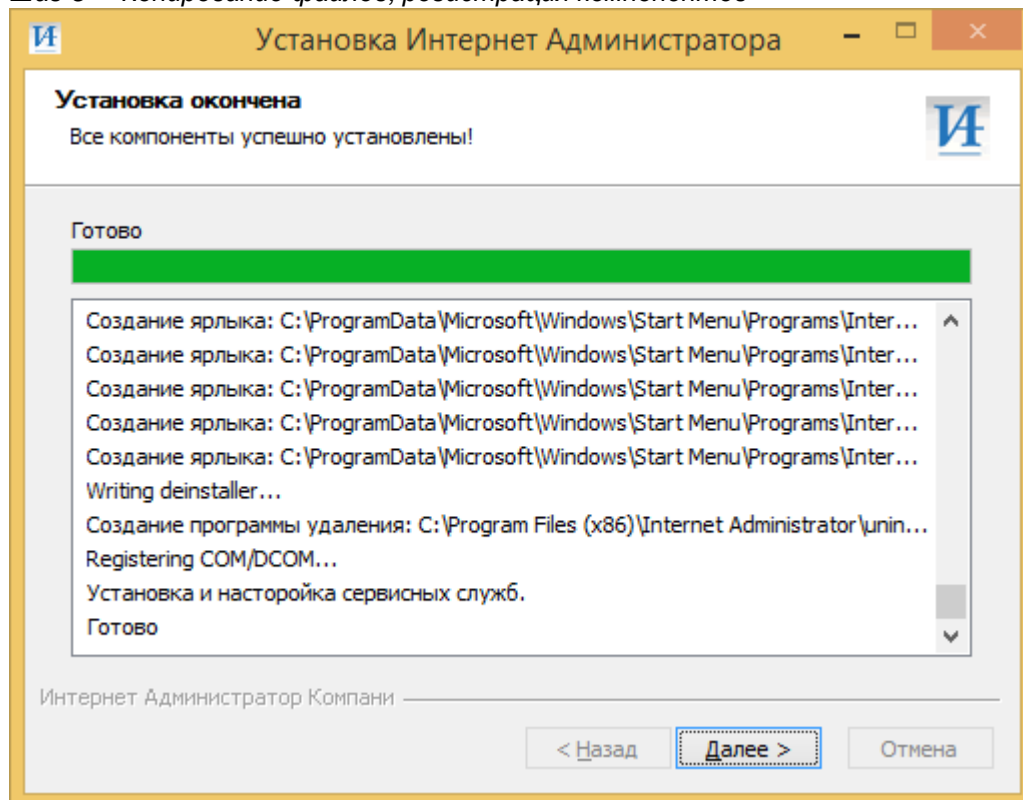
*Шаг 4 – Ввод активирующего ключа*





Если Вы приобрели копию программного обеспечения «Интернет Администратор», то на данном этапе Вам следует ввести лицензионный ключ, полученный после покупки программы. Проверка правильности ключа здесь не осуществляется. Если Вы устанавливаете «Интернет Администратор» в режиме испытания, то вводить ключ не надо. Однако при этом «Интернет Администратор» будет работать 60 дней с момента установки, после чего служба перестанет запускаться. Ввести лицензионный ключ Вы можете в любое время после установки.

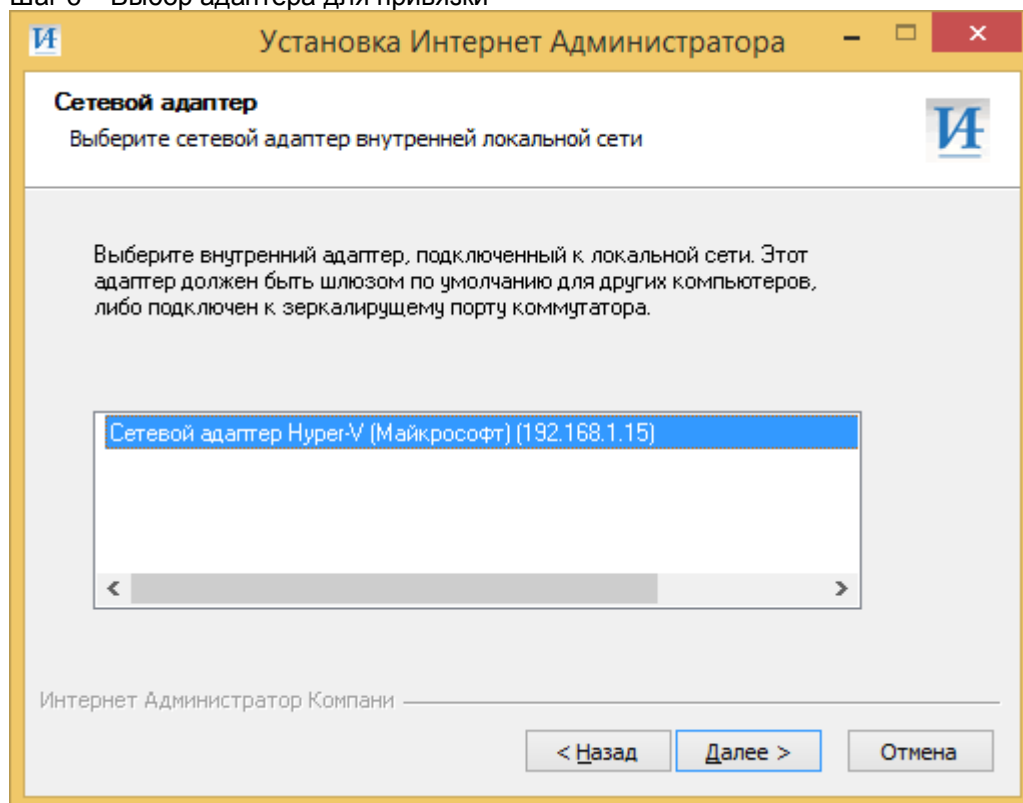
*Шаг 5 – Копирование файлов, регистрация компонентов*



На данном этапе инсталлятор копирует необходимые файлы в системный каталог «Интернет Администратор», регистрирует библиотеки и компоненты COM, устанавливает драйвер и службы.

Инсталлятор установит бесплатный Microsoft SQL Server Express 2014 в качестве СУБД и создаст новую базу данных. Если этот процесс окажется неудачным, то установку Microsoft SQL Server и создание новой базы данных необходимо произвести вручную. Смотрите раздел 8 – БАЗА ДАННЫХ И ПОДДЕРЖКА MICROSOFT SQL SERVER.

Шаг 6 – Выбор адаптера для привязки



Вам необходимо выбрать сетевой адаптер для работы. «Интернет Администратор» будет отслеживать трафик, проходящий только через один сетевой сегмент, к которому подключен выбранный сетевой адаптер. Например, если один сетевой адаптер работает с внешней сетью (Интернет), а другой – с внутренней, то выбирать следует адаптер, работающий с внутренней сетью, чтобы иметь возможность отслеживать Интернет активность каждого из пользователей. Если настроено зеркалирование портов, то выбираем адаптер подключенный к зеркалирующему порту (на который копируется интернет-трафик).

Шаг 7 – Ввод пула локальных IP-адресов

**Установка Интернет Администратора**

**Настройка сети**  
Пожалуйста, определите локальные адреса Вашей сети.

Интернет Администратор должен знать, какие IP адреса принадлежат Вашей сети, а какие нет. Пожалуйста, задайте адреса IP сетей, в которые входят все IP адреса Вашей внутренней сети.

IP сеть	Маска подсети
192.168.1.0	255.255.255.0

IP сеть (напр. 192.168.0.0):

Маска (напр. 255.255.255.0):

Введите IP адрес этого сервера и порт на котором будет работать веб сервер

IP адрес:  Порт:

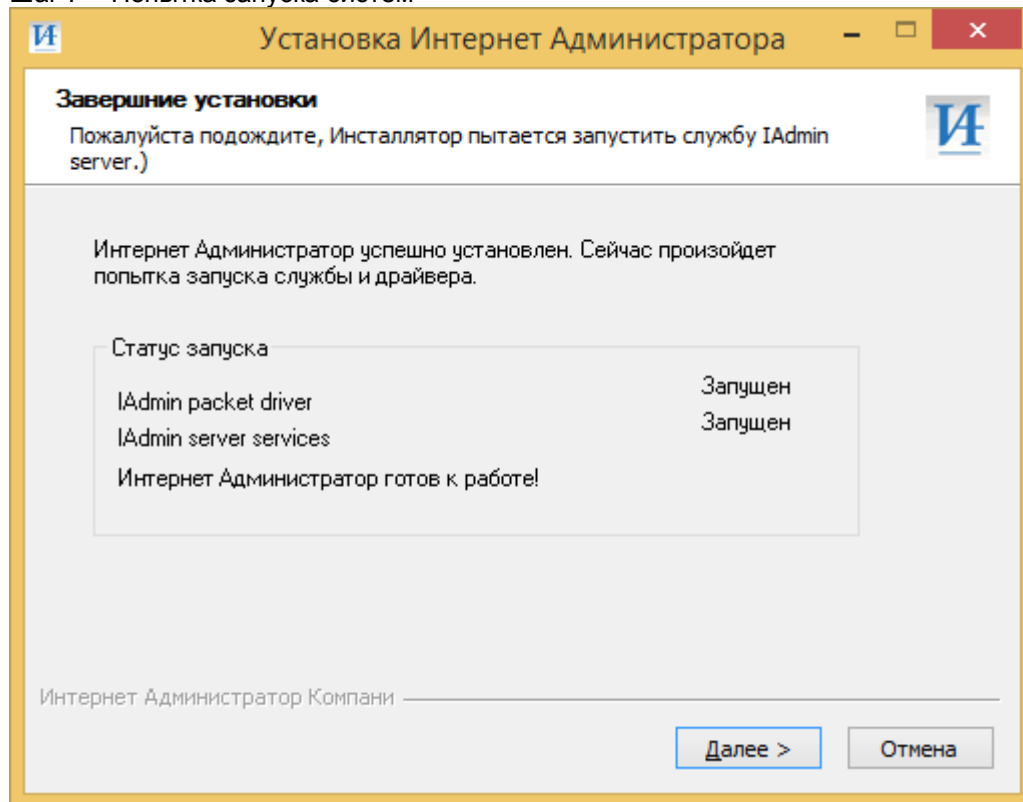
Интернет Администратор Компани

Инсталлятор сам определяет первоначальные данные, взятые с выбранного сетевого адаптера. Однако вы можете их изменить на этапе установки.

Для того чтобы «Интернет Администратор» мог корректно учитывать и анализировать Интернет трафик, ему необходимо указать компьютеры, принадлежащие Вашей сети, которые следует отслеживать. Для этого необходимо ввести адрес IP сети и маску по правилам TCP/IP, которые определяют Вашу сеть. Вы можете изменить данные настройки после установки с помощью утилиты «Администратор правил».

Здесь также нужно указать адрес и порт веб сервера. В качестве адреса должен быть указан IP адрес сервера, доступный для внутренних клиентов. В качестве порта может быть указано любое незанятое другими службами значение TCP порта.

Шаг 7 – Попытка запуска систем



На завершающем седьмом этапе программа установки производит попытку запуска пакетного драйвера и служб. В большинстве случаев запуск производится успешно, и Вы можете начать работу с системой сразу после этого при условии, что Вы указали необходимые параметры сети. Однако в случае неудачи вам необходимо проанализировать журнал событий Windows на предмет причин.

Если инсталлятор обнаружит предыдущую версию комплекса, он попросит удалить ее перед очередной установкой. При этом вы можете сохранить базу данных iadmin.mdb со всей информацией и затем заменить ее после новой установки. Если Вы используете базу на MS SQL сервере, то после установки воспользуетесь «Мастером базы данных» для выбора рабочей базы.

**ВНИМАНИЕ! Версия 3.5 будет совместима с базой данных от ранних версий только в случае использования базы на MS SQL Server и установки обновления 20!**

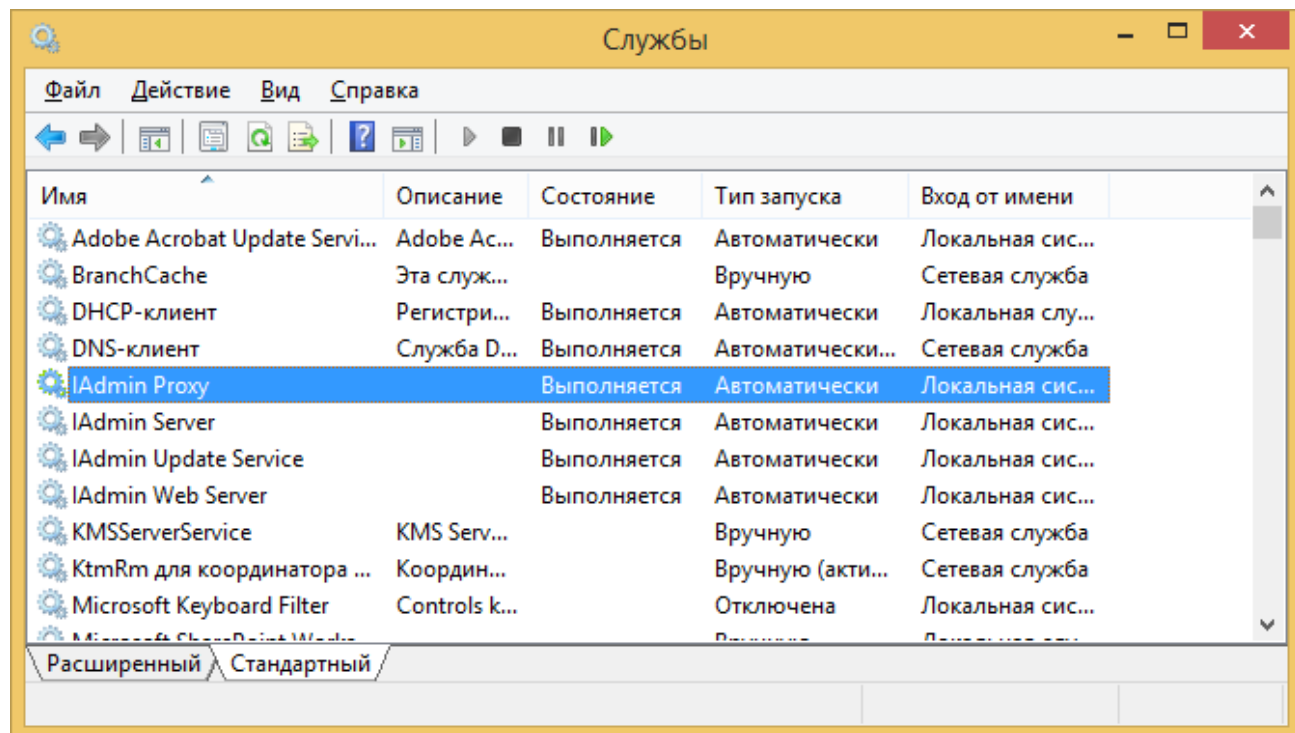
**Примечание.** Начиная с обновления 17, программа включает в себя собственный прокси-сервер IAdmin Proxy. Если у Вас в сети используется сторонний прокси-сервер на отдельном сервере, то его внутренний IP адрес, используемый для запросов клиентов, попадет в сегмент локальных адресов. Такой адрес необходимо сделать внешним с помощью административной утилиты «Администратор правил». Выберите в меню Сервис -> Настройка. На вкладке Сеть введите внутренний IP адрес прокси-сервера для исключения из локальных адресов. После изменений необходимо перезапустить службу IAdmin server.

**После установки «Интернет Администратор» начинает работу в режиме статической регистрации пользователей, и сам обнаруживает пользователей и компьютеры. Для обнаружения компьютер должен осуществить любой запрос в Интернет. Если новые пользователи не появляются после нескольких минут работы программы, проверьте, правильно ли выбран сетевой адаптер и указаны локальные IP сети.**

## Раздел 2.4. – Компоненты Интернет Администратора

После установки в системе появляются следующие рабочие компоненты:

1. Пакетный драйвер prf (файл prf.sys) – осуществляет работу с драйвером сетевой карты и обмен отслеживаемыми сетевыми пакетами.
2. Службы Windows:



- IAdmin Server – осуществляет основную работу по мониторингу и контролю доступа. Если эта служба не запущена, то программа не работает. Служба останавливается по окончании пробного периода и ее нельзя будет запустить без ввода ключа. Служба создает процесс iadmindsvcs.exe, который может занимать большой объем памяти, около 200 мегабайт. Такой размер памяти требуется для загрузки огромной базы категорий с сайтами.

- IAdmin Proxy – HTTP/HTTPS прокси сервер. По умолчанию принимает запросы от клиентов на всех IP адресах сервера на порту 8080. Осуществляет обработку TLS/SSL трафика с использованием собственных сертификатов, позволяет расшифровывать HTTPS, обрабатывать типы содержимого и более детальные параметры протокола HTTP.

- IAdmin Update Service – служебный сервис, который занимается обновлением базы категорий, а также очисткой рабочей базы данных по расписанию. Создает процесс iadminupdateservice.exe. Ведет журнал событий update.log в папке установки.

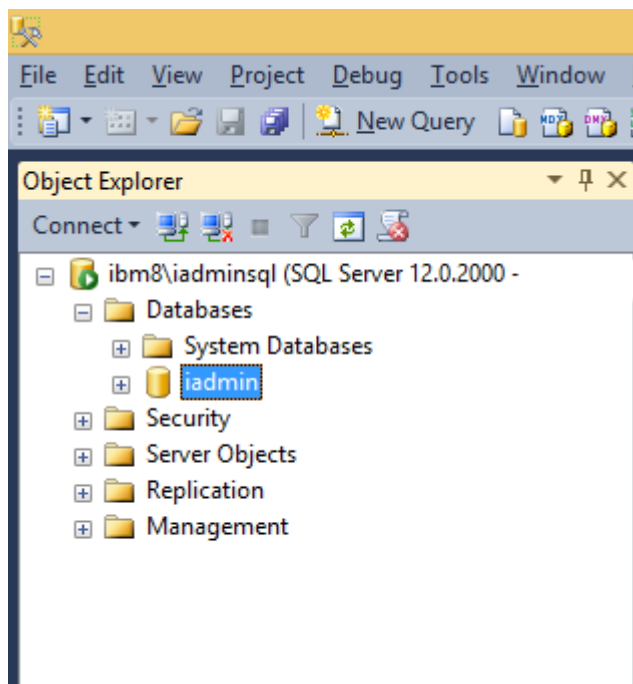
- IAdmin Web Server – веб сервер для вывода статистики пользователям и для осуществления регистрации пользователей в режиме входа в домен и по имени и паролю. Создает процесс IAdminWebSvc.exe.

3. Рабочая база данных по умолчанию.

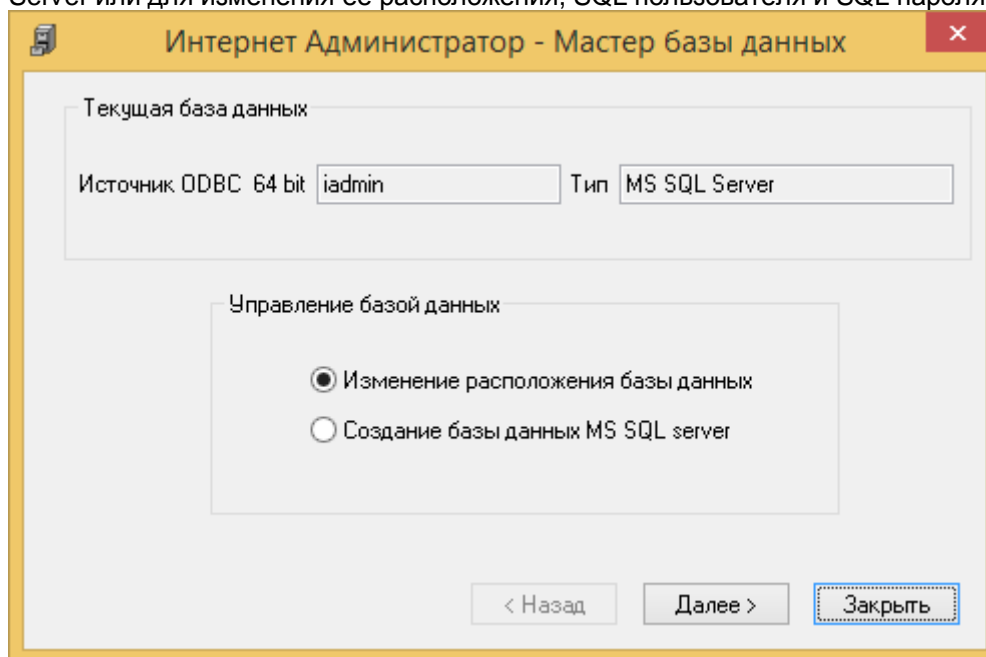
Версия 3.5 использует в качестве СУБД по умолчанию бесплатный Microsoft SQL Server Express 2014, дистрибутив которого входит в состав дистрибутива программы.

Для доступа к базе данных необходима дополнительная установка Microsoft SQL Server Management Studio, доступная для загрузки с сайта Microsoft.

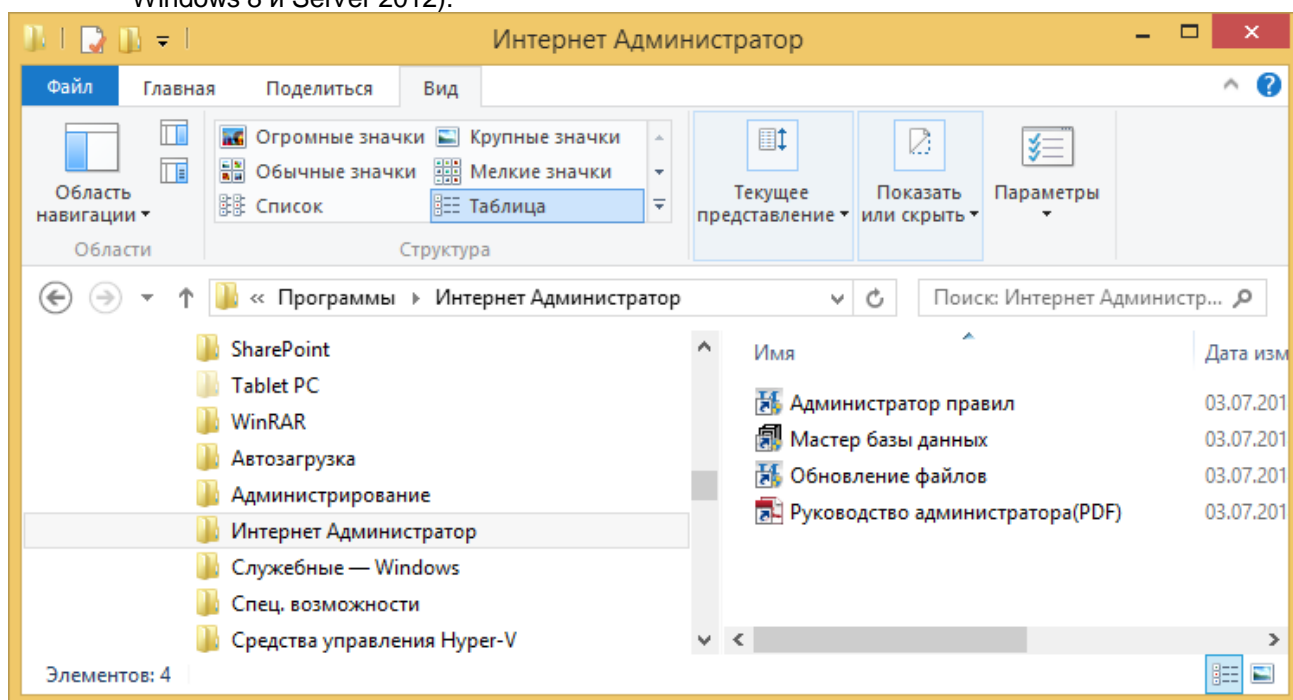
База данных располагается в экземпляре IADMINSQL на локальном сервере (SQL Server name: localhost\iadminsql). Пользователь Windows от имени которого происходила установка программы является администратором экземпляра IADMINSQL.



Для управления базой данных воспользуйтесь Мастером базы данных(в составе Интернет Администратора) для создания новой рабочей базы данных на MS SQL Server или для изменения ее расположения, SQL пользователя и SQL пароля.



4. Программная группа Internet Administrator.  
Здесь представлены административные утилиты, доступные для запуска через меню Пуск->Все программы, или Пуск->Приложения (в новой редакции Windows 8 и Server 2012).



Администратор правил – основная управляющая программа. Здесь указываются все настройки, осуществляется мониторинг и создаются правила доступа.

Мастер базы данных – программа для смены рабочей базы данных и создания базы данных на Microsoft SQL Server.

Обновление файлов – программа для автоматического обновления Интернет Администратора. При запуске Администратор правил проверяет наличие новых обновлений и стартует Обновление файлов, если обнаружена новая версия программы и администратор согласился его провести.

## РАЗДЕЛ 3 – НАСТРОЙКА СИСТЕМЫ

Настройка системы производится с помощью административной утилиты «Администратор правил».

### Раздел 3.1. — Настройка сетевых параметров

В системе «Интернет Администратор» имеются два параметра прямо влияющие на работу системы. Это сетевой адаптер, к которому привязана служба и описание локальных адресов внутреннего сегмента. При задании этих параметров с ошибкой, работа программы будет невозможна!

#### Сетевой адаптер

Привязка к сетевому адаптеру осуществляется в меню Сервис -> Привязка к сетевой карте.

В появившемся окне отобразится текущий адаптер вместе с его IP адресом, а также выпадающий список сетевых адаптеров, установленных на компьютере. После выбора адаптера будет перезапущена служба IAdmin Server. Привязку нужно осуществлять к адаптеру, через который проходит Интернет-трафик от компьютеров пользователей в Интернет. Если у Вас на шлюзе (роутере, NAT, прокси-сервере) два сетевых адаптера, то привязку необходимо осуществить к внутреннему адаптеру, подключенному к локальной сети. Если шлюз является сетевым мостом, привязку допускается сделать к внешней карте. Если для работы используется управляемый коммутатор, запрещающий отправку пакетов через зеркалирующий порт, то для работы механизма блокировки Вам нужно использовать вторую сетевую карту, подключенную к обычному порту и выбрать ее в качестве отдельного адаптера для блокировки. В этом случае кнопка ОК будет доступна только при выборе обоих адаптеров.

Сетевой адаптер

Выбор сетевого адаптера

Текущий адаптер: Сетевой адаптер Hyper-V (Майкрософт)

IP адрес : 192.168.1.15

Выберите новый сетевой адаптер для работы:

Использовать отдельный адаптер для отправки блокирующих пакетов

Адаптер для отправки

IP адрес :

Выберите новый сетевой адаптер для отправки:

Используйте отдельный адаптер для отправки блокирующих пакетов, если Ваше сетевое устройство на зеркалирующем порту запрещает отправку пакетов.  
Если используется карта для блокировки, отключите (снимите галочки) на основном адаптере все драйверы и сетевые службы в свойствах сетевого подключения Windows

ОК Отмена



## Локальные адреса

Настройка локальных адресов производится в меню Сервис -> Настройки на вкладке Сеть.

**Адреса локальных подсетей** определяют набор IP сетей, которые Вы используете в Вашей внутренней сети. Адреса задаются в стиле адрес IP сети (не хоста!) и маска подсети. Вы можете задать до 10 различных сетевых сегментов.

**Адреса, исключенные из локальных**, считаются внешними, то есть адресами Интернета. Любой запрос к таким адресам будет считаться доступом в Интернет. **Задание таких адресов необходимо при использовании прокси-сервера в Вашей сети, за исключением IAdmin Proxu.** Внутренний IP адрес стороннего прокси-сервера необходимо добавить в список исключенных IP адресов, иначе запросы пользователей через прокси не будут учитываться программой. Адрес IAdmin Proxu исключать не требуется, поскольку этот компонент обрабатывает трафик независимо от пакетного анализатора.

**Если DNS сервера расположены внутри локального сегмента, их также нужно исключить**, чтобы Интернет Администратор смог нормально распознавать названия хостов, обращение к которым идет по протоколам, отличным от HTTP.

**IP адрес IAdmin веб сервера** должен принадлежать серверу, на котором установлен Интернет Администратор, и быть доступным для внутренних пользователей. На этот адрес будут перенаправляться веб запросы для аутентификации, если пользователь не зарегистрирован. Порт определяет TCP порт, на котором Веб сервер ожидает запросы. Этот порт не должен использоваться другими программами! **Если Вы используете прокси-сервер, то адрес IAdmin Веб сервера обязательно должен быть добавлен в исключения «Не использовать прокси-сервер для локальных адресов» или «Не использовать прокси-сервер для адресов начинающихся с».**

### Раздел 3.2. — Настройка IAdmin Proxy

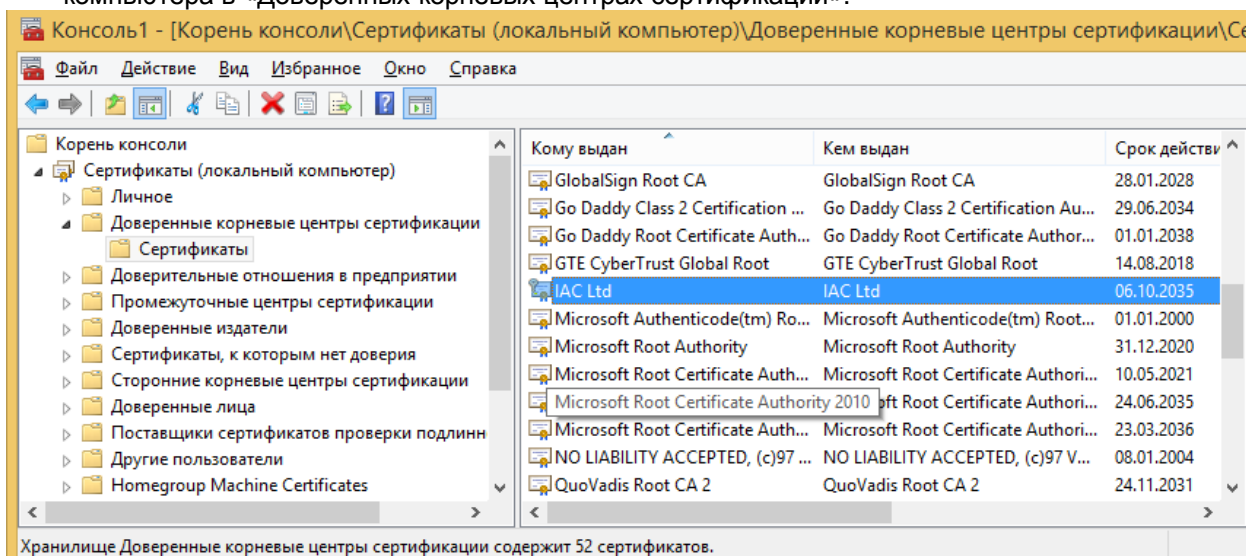
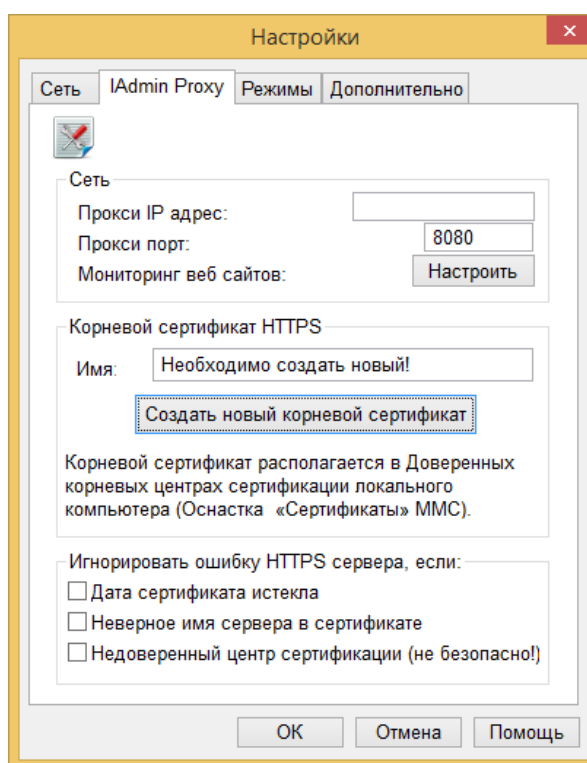
IAdmin Proxy является независимым сетевым компонентом по сбору трафика. Его внутренний IP адрес, к которому обращаются клиенты, должен принадлежать к локальным подсетям, а внешний IP адрес с которого происходят запросы в Интернет с сервера – не должен. Если на сервере с IAdmin Proxy одна сетевая карта, то необходимо логическое разделение на подсети: для внутренней сети и подсети, которая настроена на шлюз по умолчанию. Если используются 2 сетевые карты, то подсеть на внешней сетевой карте просто должна отсутствовать в списке локальных адресов.

Настройка производится в меню Сервис -> Настройка на вкладке IAdmin Proxy.

Прокси IP адрес и порт определяют параметры на которых прокси сервер ведет прием соединений. Если IP адрес не задан, то он может быть любым, установленным на сервере. Эти параметры указываются в настройках браузера пользователей для работы через IAdmin Proxy. Параметры могут быть установлены вручную, через групповую политику домена Windows Active Directory или методом автоматической конфигурации прокси сервера WPAD через ваш внутренний DHCP и/или DNS сервер.

Корневой сертификат является необходимым для работы HTTPS протокола. IAdmin Proxy не устанавливает прямой туннель, а использует метод «доверенный человек посередине» (англ. Trusted Man in the middle (Trusted MITM)). Корневой сертификат является сертификатом Центра сертификации, от его имени будут создаваться и подписываться сертификаты сайтов.

После первой установки необходимо создать свой собственный корневой сертификат. Нажмите соответствующую кнопку и задайте имя. Под именем подразумевается название организации, это имя будет определять созданный сертификат в снап-ине Сертификаты MMC. Сертификат создается в учетной записи компьютера в «Доверенных корневых центрах сертификации».



Экспортируйте этот сертификат и сохраните в виде файла. Экспортированный сертификат необходимо импортировать на все клиентские компьютеры, так же в раздел «Доверенных корневых центров сертификации». Это можно сделать вручную (двойным кликом по файлу сертификата с клиентского компьютера) либо используя групповую политику домена Windows Active Directory ([https://technet.microsoft.com/ru-ru/library/Cc731253\(v=WS.10\).aspx](https://technet.microsoft.com/ru-ru/library/Cc731253(v=WS.10).aspx)). Только после этого компьютеры начнут доверять сертификатам сайтов, подписанным Вашим корневым сертификатом, и не будут выдавать ошибку о недействительности сертификата. Пользователи будут видеть имя Вашей компании при наведении на свойство сертификата в браузере и при просмотре самого сертификата у каждого сайта в свойстве «Кем выдан». Это название будет гарантировать пользователям подлинность и безопасность соединения.

Сертификаты сайтов создаются и хранятся в разделе «Личное» в снап-ине Сертификаты MMC локального компьютера.

По умолчанию IAdmin Proxu будет устанавливать внешние соединения только с веб сайтами, у которых есть доверенный сертификат, не содержащий ошибок. В случае ошибки, например, просроченного сертификата, IAdmin Proxu выдаст в браузер клиента сообщение о соответствующей ошибке. В настройке «Игнорировать ошибку HTTPS сервера» можно указать, какие типы ошибок сертификата будут игнорироваться для установки соединения.

### Раздел 3.3. — Настройка режима регистрации пользователя на компьютерах

Настройка производится в меню Сервис -> Настройка на вкладке Режимы.

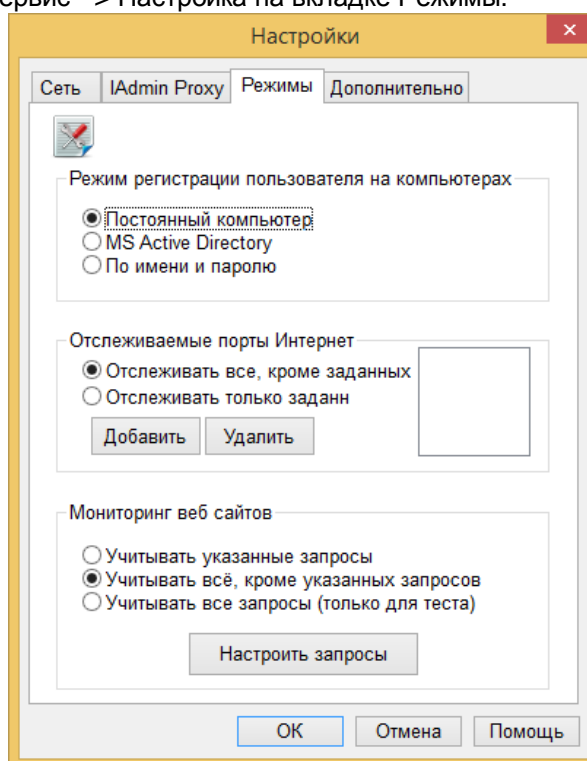
«Интернет Администратор» поддерживает три типа регистрации пользователей на рабочих станциях: «Постоянный компьютер», «Microsoft Active Directory» и «По имени и паролю». **Внимание! При установке режима отличного от «Постоянный компьютер», до прохождения процедуры регистрации доступ со всех компьютеров в Интернет закрывается! Если у Вас установлены серверы и другие устройства, которым не требуется регистрация, используйте галочку «Включить постоянную регистрацию в любых режимах» до перевода режима!**

При режиме «Постоянный компьютер» (установлен по умолчанию), пользователи регистрируются на своих рабочих станциях статично. Каждый пользователь соответствует той рабочей станции, на которой он был впервые обнаружен.

При режиме «Microsoft Active Directory» пользователь регистрируется на рабочей станции прохождения аутентификации через компонент IAdmin Web с использованием доменной учетной записи. Применяется встроенная проверка подлинности Windows.

Режим «По имени и паролю» предусматривает ввод регистрационных данных для регистрации на странице IAdmin Web. До тех пор, пока пользователь не пройдет процедуру регистрации, доступ в Интернет с рабочей станции блокируется.

Для более детального описания работы веб сервера смотрите раздел «4.3 IAdmin Web – статистика и регистрация пользователей».



### Раздел 3.4. — Настройка отслеживаемых портов Интернет

Настройка производится в меню Сервис -> Настройка на вкладке Режимы (смотрите скрин выше).

Отслеживаемые порты Интернет определяют, с какими портами (протоколами) работает комплекс «Интернет Администратор», то есть: отслеживает данные, ограничивает ресурсы и применяет политику доступа. Отслеживаемые порты предназначены прежде всего для работы с прокси-сервером. Так как прокси-сервер необходимо исключать из локального сегмента, любые запросы к нему будут считаться запросами в Интернет. Если на прокси-сервере установлены другие сетевые приложения, то порты, на которых эти приложения работают, нужно добавить в список не отслеживаемых. Если прокси-сервер предоставляет доступ по ограниченному набору портов (HTTP, FTP, POP3, SMTP), они настраиваются так, чтобы отслеживание велось только по ним, а остальные не учитывались. **Внимание!** Если Вы задали IP адреса в качестве исключенных, отслеживаемые порты будут применяться только для указанных исключенных адресов.

### Раздел 3.5. — Мониторинг веб сайтов

Настройка производится в меню Сервис -> Глобальные свойства на вкладке Режимы (смотрите скриншот выше).

Данная настройка определяет, каким образом будет осуществляться запись в базу данных отдельных запросов по HTTP протоколу, если не используется IAdmin Proху.

Учитывать указанные запросы.

При такой настройке учитываются запросы к головной странице сайта, а также к заданным страницам и файлам. Страницы и файлы задаются по их расширениям, например, .html или .zip. Для задания расширений нажмите на кнопку «Настроить» и в появившемся окне введите требуемые расширения. Все остальные, незадаанные страницы и запросы как отдельный элемент доступа учитываться не будут.

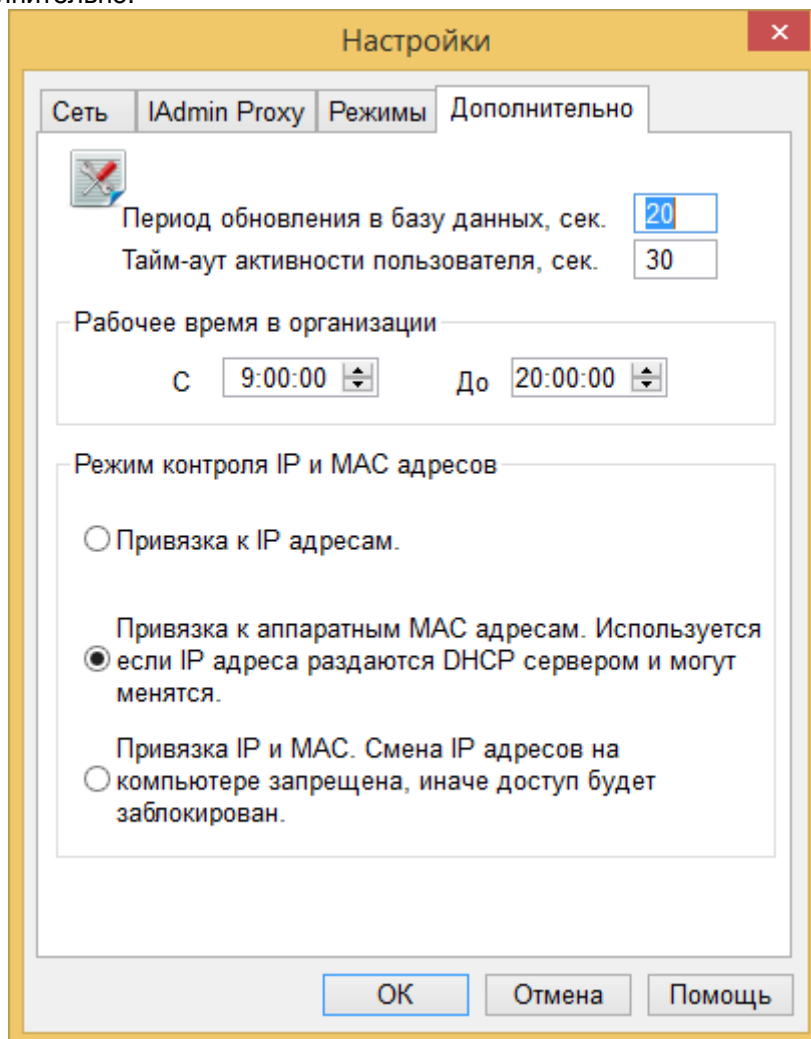
Учитывать всё, кроме указанных запросов (по умолчанию).

Здесь вы задаете расширения файлов запроса, которые не нужно учитывать. Это сделано для того, чтобы не записывать многочисленные рисунки (.gif, .jpeg) при открытии страницы, так как они не представляют особого интереса.

Учитывать все запросы. Учитываются любые запросы по протоколу HTTP. Данная настройка не рекомендуется, так как при этом база данных очень быстро наполняется, а служебные запросы к различным скриптам и изображениям не представляют информативности.

### Раздел 3.6. — Дополнительные настройки

Настройка производится в меню Сервис -> Настройки на вкладке Дополнительно.



**Период обновления в базу данных.** При своей работе «Интернет Администратор» оперирует с данными в оперативной памяти. Периодически он записывает данные в базу данных. По умолчанию значение периода обновления равно 20 секунд. Для более оперативного отслеживания его можно уменьшить. Не рекомендуется устанавливать этот параметр меньше 5 секунд. При большом количестве пользователей, чтобы снизить загрузку на процессор и жесткий диск, этот параметр можно увеличить. Тогда обновления в базу будут происходить реже.

**Тайм-аут активности пользователя.** Этот параметр определяет интервал, в течение которого осуществляется подсчет времени, проведенного пользователем в Интернет и на каком-либо сайте, хотя пользователь при этом не делает никаких запросов в Интернет. После истечения тайм-аута «Интернет Администратор» считает, что пользователь не активен. Тайм-аут помогает более точно отследить время работы. Пользователь может загрузить несколько страниц и просматривать их некоторое время.

**Рабочее время в организации.** Задаёт глобальное рабочее время для установки отдельных лимитов в рабочее и нерабочее время.

#### Режим контроля IP и MAC адресов.

**Привязка к IP.** Этот режим по умолчанию работал в прошлых версиях. Программа распознает компьютеры по только IP адресам. И если IP адрес на обнаруженном компьютере сменился на новый, Интернет Администратор обнаружит компьютер как новый. Этот режим не подходит для работы с DHCP сервером, который меняет IP адреса у одних и тех же компьютеров.

*Привязка к MAC.* Режим установлен по умолчанию, начиная с версии 3.0. В отличие от предыдущего режима, при смене IP адреса на компьютере, делает замену IP в системе. Может случиться так что компьютер получил IP адрес существующего компьютера, в этом случае с него снимается старый IP и в качестве адреса установится значение 0.0.0.0, до обнаружения нового IP адреса на этом MAC адресе.

**Внимание!** Режим Привязки к MAC имеет ограничение. Запрещается использовать внутри сети маршрутизаторы (роутеры) поскольку при маршрутизации они со своего MAC адреса передают пакеты с IP адресами маршрутизируемых компьютеров, стоящих за ними. Это не касается NAT или прокси-серверов, так как они шлют трафик со своего внешнего IP адреса.

*Привязка IP и MAC.* Этот режим необходим для защиты от смены IP адреса, и для установки существующего или нового адреса для обхода ограничений. При обнаружении смены любого параметра доступ будет заблокирован с IP адресов, которые не имеют MAC адрес на зарегистрированном в системе компьютере. Этот режим имеет такое же ограничение на использование относительно роутеров как и предыдущий.

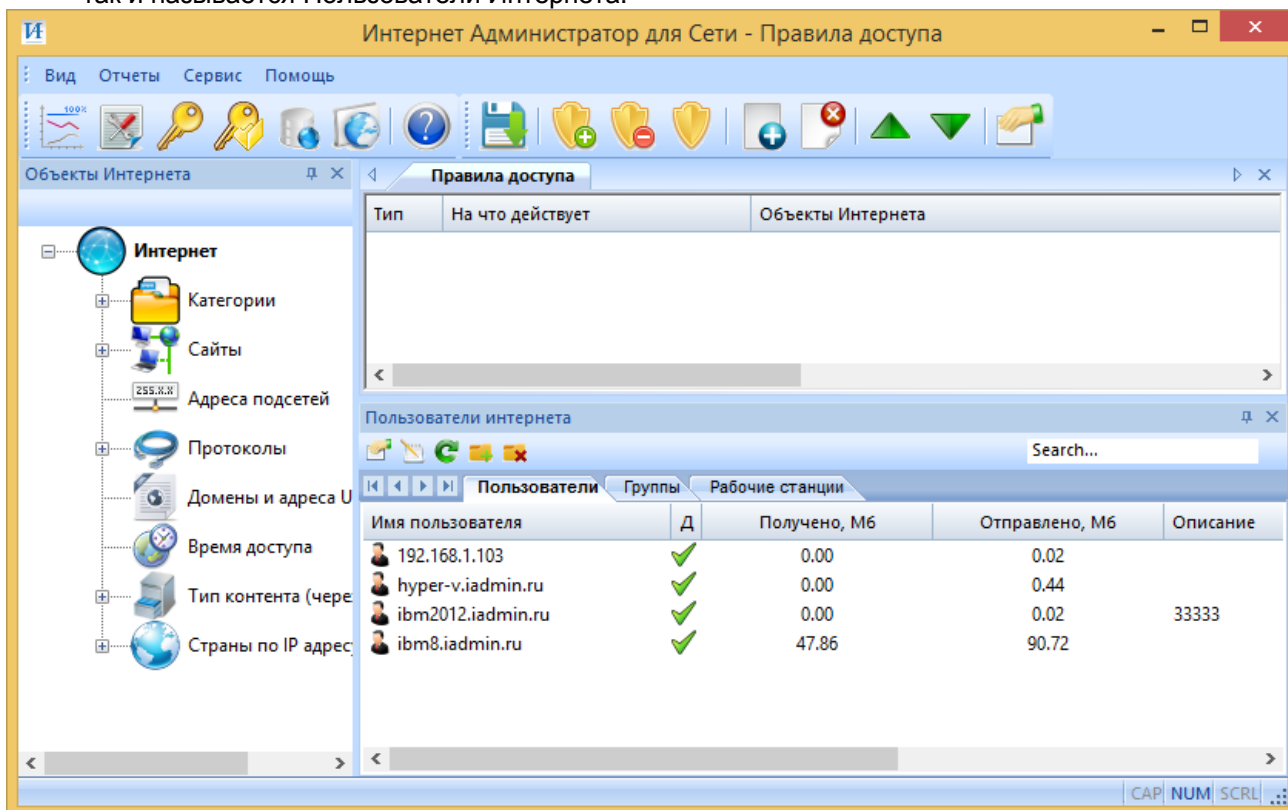



## РАЗДЕЛ 4 – УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

В данном разделе описываются методы управления пользователями, их группами, компьютерами. Все настройки, приведенные в этом разделе, выполняются из административной утилиты «Администратор Пользователей».

### Раздел 4.1. — Пользователи, группы и компьютеры

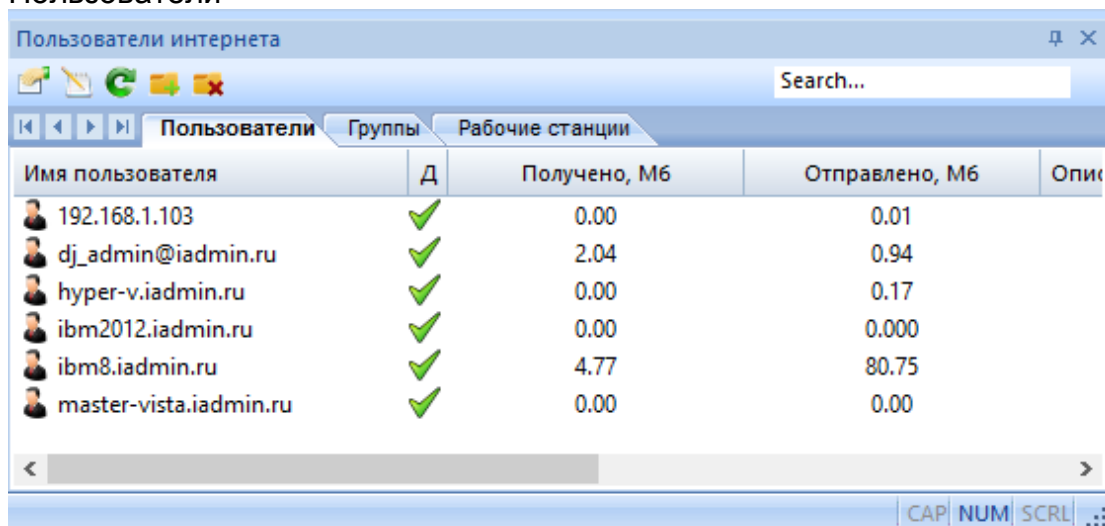
Управление описанными объектами осуществляется в главном окне Администратора правил. Пользователи располагаются в правой нижней зоне, которая так и называется Пользователи Интернета.



Здесь представлены три вкладки: Пользователи, Группы и Рабочие станции. Информацию в данных списках можно обновить с помощью кнопки  на локальной панели инструментов.







## Пользователи



Имя пользователя	Д	Получено, Мб	Отправлено, Мб	Описание
192.168.1.103	✓	0.00	0.01	
dj_admin@iadmin.ru	✓	2.04	0.94	
hyper-v.iadmin.ru	✓	0.00	0.17	
ibm2012.iadmin.ru	✓	0.00	0.000	
ibm8.iadmin.ru	✓	4.77	80.75	
master-vista.iadmin.ru	✓	0.00	0.00	

В данном списке представлена краткая информация о пользователе: Его имя, разрешен ли доступ в Интернет, сколько трафика он загрузил и отправил за сегодня и его описание.

Пользователей можно сортировать кликая по названию соответствующих колонок. Предусмотрен поиск пользователей по их имени. Для этого введите первые буквы имени пользователя в строку Search... на панели инструментов. Указатель в списке пользователей будет переходить к соответствующим пользователям.

С помощью кнопок на панели инструментов или из контекстного меню по правой кнопке мыши можно открыть  - свойства пользователя,  - журнал доступа в Интернет (см. раздел 6.1), а также  - удалить или  - добавить пользователя. Удаление пользователя приведет к удалению пользовательского объекта и всей связанной с ним информацией. Создание пользователя необходимо только при случайном удалении пользователя в режиме Постоянный компьютер или в режиме регистрации по имени и паролю для создания новых учетных записей для доступа в Интернет. При любых действиях с созданием или удалением пользователей необходима перезагрузка службы «IAdmin Server».

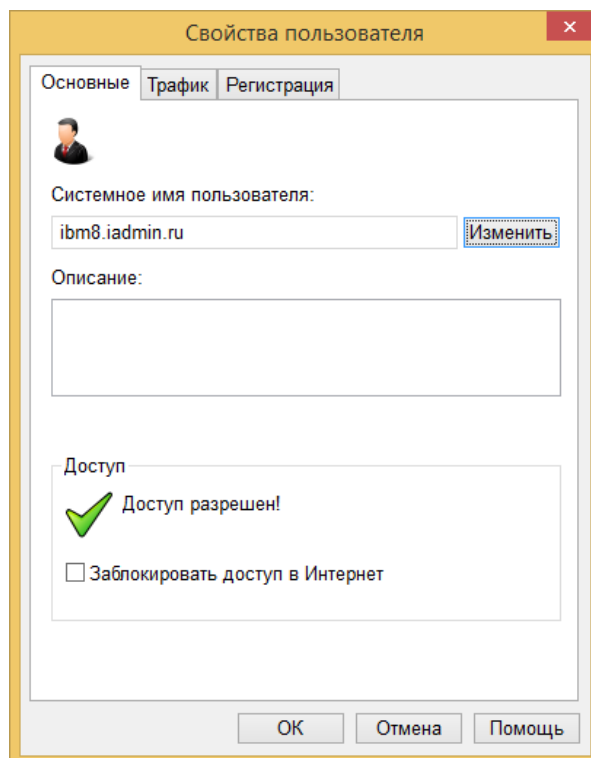
**Если выделить несколько пользователей, то можно задать некоторые свойства сразу целому списку.**

В свойствах пользователя отображаются три вкладки.

На вкладке «Основные свойства» можно изменить полное имя пользователя и его описание, а также вручную заблокировать пользователя – при этом доступ в Интернет ему будет закрыт принудительно.

Изменение системного имени можно производить для удобства отображения в отчетах. Системное имя – это имя пользователя, определенное системой при обнаружении рабочей станции. Это может быть доменное имя, имя компьютера, или IP адрес, если не удалось разрешить имя. При режиме регистрации MS Active Directory изменять системные имена нельзя, так как в таком режиме они являются доменными именами, и с ними происходит сопоставление зарегистрированного пользователя.

Если пользователь заблокирован системой, то перед разблокировкой нужно сначала увеличить доступные лимиты, иначе он заблокируется снова.



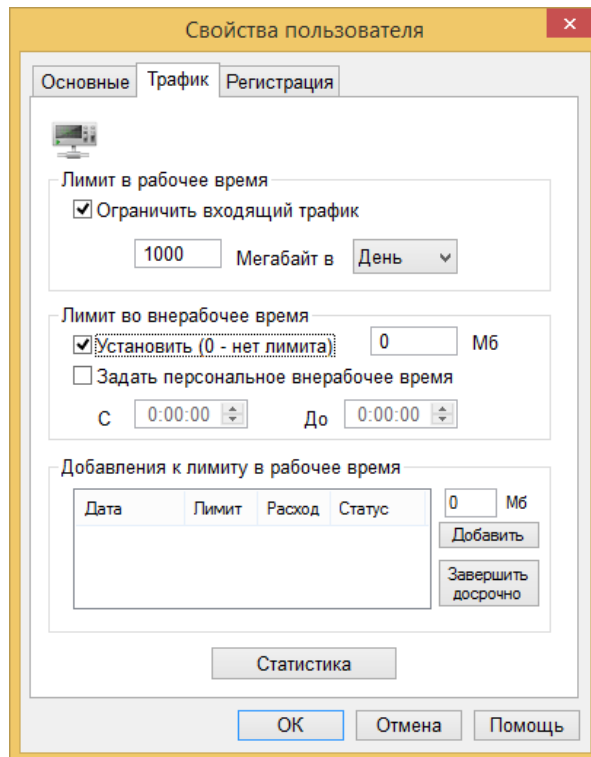
На вкладке «Трафик» задаются ограничения трафика по объему.

Для ограничения входящего трафика установите соответствующую галочку и задайте размер лимита и учетный период. Если не включен лимит во вне рабочее время, то данный лимит будет применяться в течение всех суток.

Учетный период – это время, в течение которого действует ограничение. При выработке лимита пользователь блокируется. При переходе в следующий интервал учетного периода, данные о выработке обнуляются. Если пользователь был заблокирован системой, то доступ ему открывается. Лимит по трафику задается в мегабайтах.

Вы можете задать отдельный лимит в нерабочее время. Если задать 0, то лимита в это время суток не будет. Глобальное рабочее время задается в настройках программы. Здесь можно указать персональное вне рабочее время.

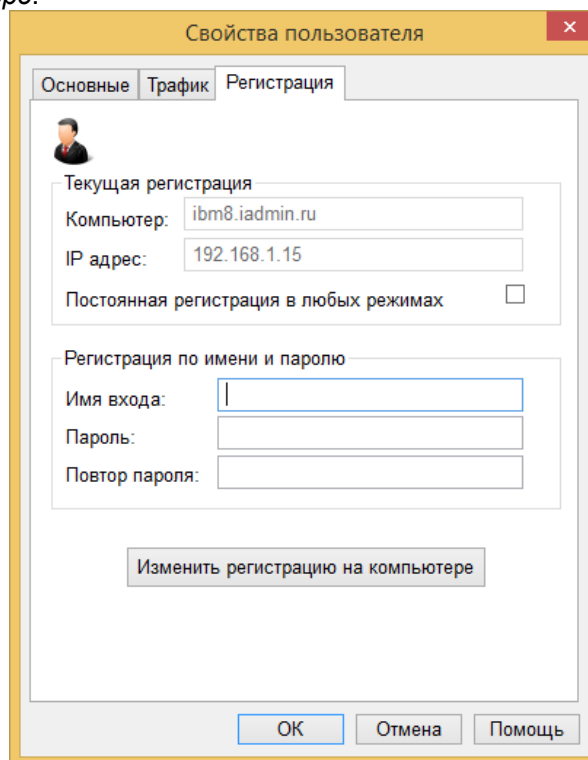
В случае окончания лимита в рабочее время и блокировки пользователя, вы можете добавить ему еще несколько мегабайт трафика в текущем учетном периоде ( в текущем дне или месяце).



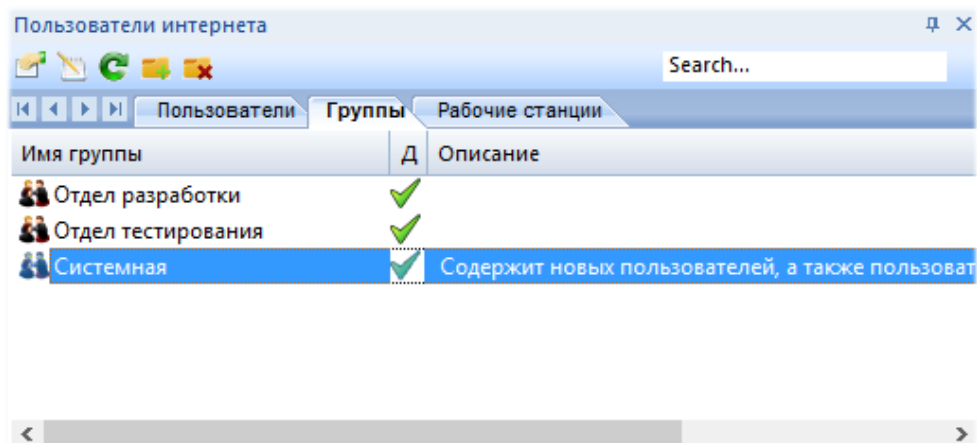
*Вкладка Регистрация на компьютере.*

Отображает текущую регистрацию пользователя и предназначена для задания имени и пароля пользователя для регистрации при соответствующем режиме.

Допускается вручную изменить регистрацию. Это необходимо для постоянной регистрации серверов, при случайном удалении пользователя и создании его вновь, либо при переходе из других режимов регистрации в режим Постоянный компьютер. **Используйте галочку «Постоянная регистрация в любых режимах» для серверов и устройств, работающих без пользователей, перед переходом из режима Постоянный компьютер в другие режимы регистрации, поскольку без регистрации доступ в Интернет будет заблокирован!**

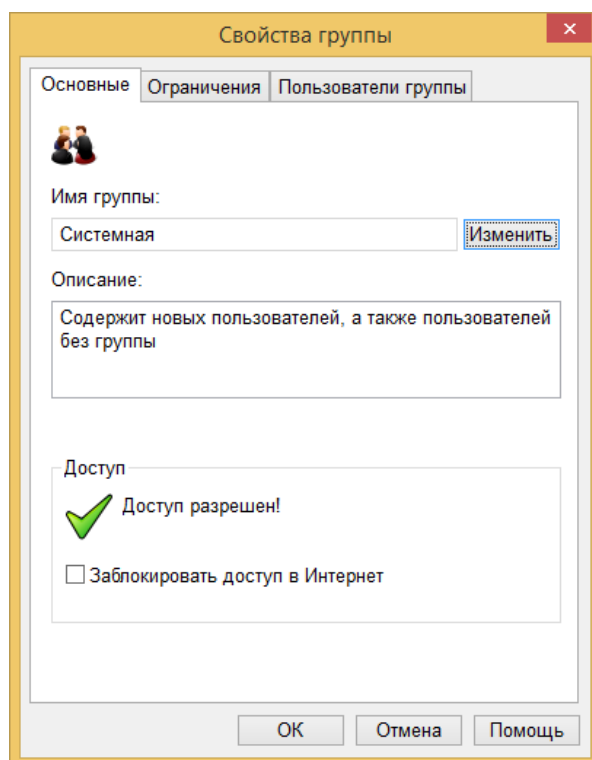


## Группы



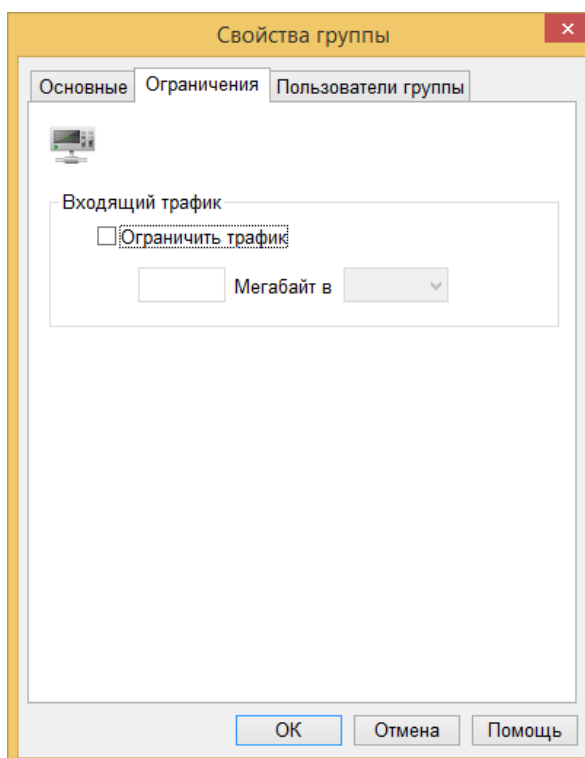
Группа объединяет несколько пользователей. Любые действия с группой относятся ко всем пользователям, входящим в нее в данный момент. Из панели инструментов или контекстного меню можно открыть свойства группы (📄), создать (➕), или удалить (✖) группу. Имя группы должно быть уникально. По умолчанию существует «Системная» группа, в которую входят пользователи, не являющиеся членами других групп. «Системную» группу переименовать или удалить нельзя.

В свойствах группы - три вкладки. На вкладке «Основные» отображается имя группы, описание. На данной вкладке можно принудительно заблокировать группу. При этом доступ всем пользователям этой группы будет закрыт.



На вкладке «Ограничения» задаются ограничения по объему загруженного трафика из Интернета всеми членами группы.

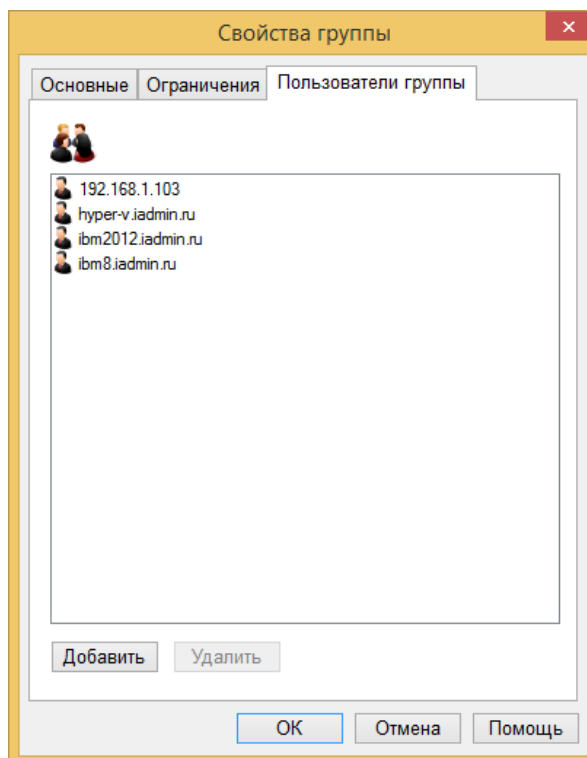
Работа каждого пользователя группы будет влиять на выработку лимита, даже один пользователь может стать причиной выработки. При достижении лимита блокируется группа и все пользователи, входящие в нее.



На вкладке Пользователи группы отображается список ее членов.

Отсюда можно удалять и добавлять пользователей. При добавлении пользователя он удаляется из группы предыдущего членства. При удалении он становится членом группы «Системная». Пользователь не может быть членом двух и более групп, он может только перемещается между существующими группами.

По умолчанию все пользователи при обнаружении попадают в группу «Системная». Используйте ее, если вы хотите автоматически блокировать всех новых пользователей. Для этого переместите пользователей по другим группа и заблокируйте группу «Системная». При обнаружении доступ в Интернет для новых пользователей будет закрыт.




## Рабочие станции (компьютеры)

Имя компьютера	IP адрес	MAC Адрес	Пользователь
192.168.1.103	192.168.1.103	5cf3fc3c4654	192.168.1.103
hyper-v.iadmin.ru	192.168.1.10	5cf3fc3c4650	hyper-v.iadmin.ru
ibm2012.iadmin.ru	192.168.1.11	00155d016800	ibm2012.iadmin.ru
ibm8.iadmin.ru	192.168.1.15	00155d016803	ibm8.iadmin.ru

В данном списке отражены все обнаруженные рабочие станции Вашей сети. Здесь представлена информация об имени рабочей станции, ее IP и MAC адресах, а также о пользователе, который в данный момент на ней зарегистрирован. С помощью контекстного меню компьютер можно перевести в список не отслеживаемых рабочих станций, для которых запросы не учитываются. Также в контекстном меню по правой кнопке мыши рабочую станцию можно удалить или открыть ее свойства.

В свойствах рабочей станции вы можете записать ей описание, а также изменить ее учетные данные, такие как Имя, IP адрес и MAC адрес. Делать последнее необходимо только в случае крайней необходимости.

**Раздел 4.2. — Журнал доступа в Интернет**

Журнал доступа в Интернет доступен из главного окна в разделе Пользователей Интернет. Выберите интересующего пользователя, а затем в контекстном меню или по кнопке  откройте журнал.

Журнал доступа в Интернет

Период журнала и фильтр страниц

04.07.2014 — 04.07.2014

Показывать только сайты  
 Показывать сайты и страницы

Сайт	Хиты	Категория	Последнее обращение	Получ, Кб	Отправ, Кб
lb1.adriver.ru	3	Нет	04.07.2014 10:12:44	0,19	0,35
mc.yandex.ru	1	Нет	04.07.2014 10:10:47	2,13	5,14
meta.wikimedia.org	3	Нет	04.07.2014 10:12:24	21,33	4,40
pass.yandex.ru	3	Нет	04.07.2014 10:11:58	1,72	1,85
qip.ru	1	Веб порталы;	04.07.2014 10:12:44	0,06	0,12
r.rbc.ru	1	Нет	04.07.2014 10:12:42	96,78	19,87
redir-service-neon.rbc.ru	1	Нет	04.07.2014 10:12:41	0,06	0,12
ru.wikipedia.org	11	Справочная информация;	04.07.2014 10:12:24	50,40	11,69
static.yandex.net	2	Нет	04.07.2014 10:11:45	0,19	0,66
suggest.yandex.net	1	Нет	04.07.2014 10:11:52	0,06	0,12
suggest.yandex.ru	10	Нет	04.07.2014 10:11:55	10,47	14,77
text-lb.esams.wikimedia.org	17	Нет	04.07.2014 10:12:24	1,10	1,99
upload-lb.esams.wikimedia.org	8	Нет	04.07.2014 10:12:12	6,42	0,91
www.tns-counter.ru	15	Нет	04.07.2014 10:12:44	38,03	8,23
www.yandex.ru	3	Поисковые машины;	04.07.2014 10:11:45	151,21	8,63
www-gt-mrr06.www-split.rbc.ru	1	Нет	04.07.2014 10:12:41	0,06	0,12
www-natty.rbc.ru	1	Нет	04.07.2014 10:12:43	0,06	0,12
yabs.yandex.ru	5	Баннерообменные сети;	04.07.2014 10:11:58	1,04	2,39
yandex.ru	3	Поисковые машины;	04.07.2014 10:11:57	188,76	17,29

Журнал доступа к ресурсам Интернет показывает посещенные сайты. Наверху окна доступен фильтр по времени, а также 2 режима просмотра. В режиме «Показывать только сайты» отображается обобщенная информация о посещенных сайтах: имя, число запросов к нему, категория, дата последнего обращения, а также объем загруженных и отправленных данных. В контекстном меню сайту можно установить категорию, если она не задана, а также открыть его в браузере для анализа.

Режим «Показывать сайты и страницы» выводит более подробную информацию в хронологическом порядке.

## Интернет Администратор для Сети версия 3.5, обновление 20

Журнал доступа в Интернет

Период журнала и фильтр страниц

04.07.2014 — 04.07.2014

Показывать только сайты  
 Показывать сайты и страницы

Сайт	Страница	Категория	Протокол	Время доступа	Получ, Кб	Отправ, Кб
meta.wikimedia.org	/wiki/special:bannerrando...	Нет	HTTP	04.07.2014 10:12:24	3,09	0,72
ru.wikipedia.org	/w/index.php?title=media...	Справочная информация;	HTTP	04.07.2014 10:12:24	0,61	0,90
text-lb.esams.wikimedia.org	/	Нет	HTTP	04.07.2014 10:12:24	0,06	0,12
ru.wikipedia.org	/w/index.php?title=media...	Справочная информация;	HTTP	04.07.2014 10:12:23	0,61	0,93
bits-lb.esams.wikimedia.org	/	Нет	HTTP	04.07.2014 10:12:23	0,06	0,12
bits-lb.esams.wikimedia.org	/	Нет	HTTP	04.07.2014 10:12:23	0,06	0,12
ru.wikipedia.org	/wiki/Сниффер	Справочная информация;	HTTP	04.07.2014 10:12:23	16,00	1,98
ru.wikipedia.org	/w/index.php?search=Сн...	Справочная информация;	HTTP	04.07.2014 10:12:23	0,76	1,05
text-lb.esams.wikimedia.org	/	Нет	HTTP	04.07.2014 10:12:21	0,06	0,12
ru.wikipedia.org	/w/api.php?action=opens...	Справочная информация;	HTTP	04.07.2014 10:12:21	0,83	1,03
text-lb.esams.wikimedia.org	/	Нет	HTTP	04.07.2014 10:12:21	0,06	0,12
ru.wikipedia.org	/w/api.php?action=opens...	Справочная информация;	HTTP	04.07.2014 10:12:21	0,89	0,98
ru.wikipedia.org	/w/api.php?action=opens...	Справочная информация;	HTTP	04.07.2014 10:12:21	0,72	0,99
ru.wikipedia.org	/w/api.php?action=opens...	Справочная информация;	HTTP	04.07.2014 10:12:21	0,97	1,07
ru.wikipedia.org	/w/api.php?action=opens...	Справочная информация;	HTTP	04.07.2014 10:12:18	0,66	0,96
ru.wikipedia.org	/w/api.php?action=opens...	Справочная информация;	HTTP	04.07.2014 10:12:18	0,70	0,97
ru.wikipedia.org	/w/api.php?action=opens...	Справочная информация;	HTTP	04.07.2014 10:12:18	0,00	0,97
text-lb.esams.wikimedia.org	/	Нет	HTTP	04.07.2014 10:12:17	0,06	0,12
ru.wikipedia.org	/w/api.php?action=opens...	Справочная информация;	HTTP	04.07.2014 10:12:17	0,83	0,96
upload-lb.esams.wikimedia	/	Нет	HTTP	04.07.2014 10:12:17	0,00	0,12

Здесь мы видим запросы так, как их посещал пользователь. Кроме самих сайтов здесь отображаются служебные запросы, которые сам пользователь не осуществляет, но они являются частью сайта, поэтому браузер открывает их самостоятельно.

Если доступ к сайту был заблокирован, он выделяется красным цветом. Для более детальной информации используйте отчеты (Раздел 7).



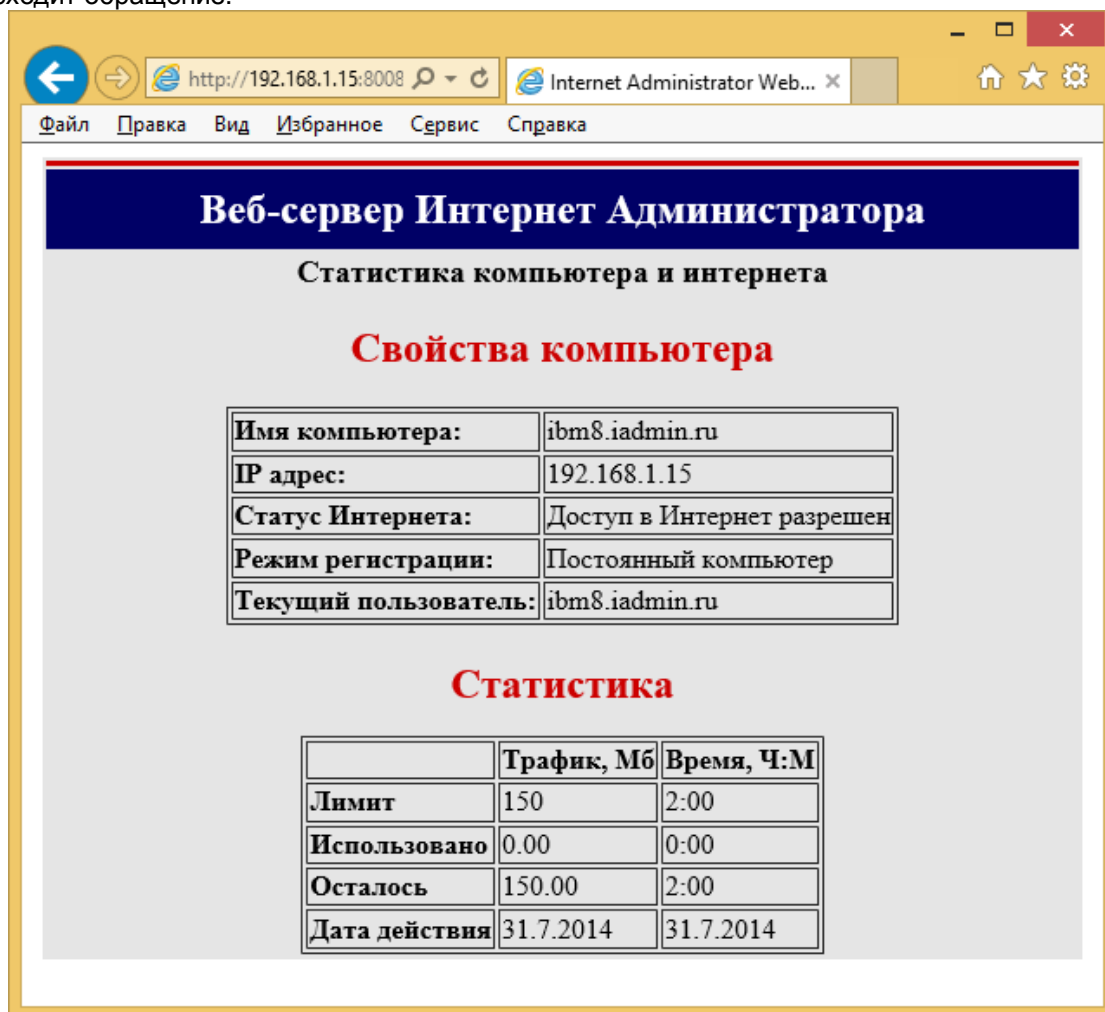
### Раздел 4.3. — IAdmin Web сервер – статистика и регистрация пользователей

Для настройки веб сервера см. раздел 3.1. IAdmin Web реализует 2 функции: вывод статистики компьютера и регистрация пользователей.

Обращение к IAdmin Web необходимо осуществлять с клиентских компьютеров. Для обращения к IAdmin Web используйте IP адрес или имя сервера, где установлен Интернет Администратор, а также порт, заданный в настройках (8008 по умолчанию). Адрес обращения выглядит примерно следующим <http://192.168.1.1:8008/>

#### Вывод статистики

При открытии Веб сервер выдает статистику по компьютеру, с которого происходит обращение.



The screenshot shows a web browser window with the URL <http://192.168.1.15:8008>. The page title is "Веб-сервер Интернет Администратора" and the main heading is "Статистика компьютера и интернета". Below this, there is a section titled "Свойства компьютера" containing a table with the following data:

Имя компьютера:	ibm8.iadmin.ru
IP адрес:	192.168.1.15
Статус Интернета:	Доступ в Интернет разрешен
Режим регистрации:	Постоянный компьютер
Текущий пользователь:	ibm8.iadmin.ru

Below the table is a section titled "Статистика" containing another table with the following data:

	Трафик, Мб	Время, Ч:М
Лимит	150	2:00
Использовано	0.00	0:00
Осталось	150.00	2:00
Дата действия	31.7.2014	31.7.2014

Отображаются данные компьютера, такие как имя и IP адрес. Статус показывает, есть ли блокировка доступа вручную или по выработке лимита трафика или времени. Режим регистрации выводит текущий режим регистрации пользователей, однако если для пользователя была установлена настройка всегда использовать режим Постоянный компьютер, то он и будет отображаться вместо глобального режима.

Статистика показывает данные по лимитам, если они заданы, и текущий остаток, аналогично данным в свойствах пользователя.

## Регистрация пользователей

В режимах MS Active Directory и По имени и паролю для доступа в Интернет пользователь должен пройти процедуру регистрации путем обращения к Веб серверу со своего компьютера. До процедуры регистрации доступ с компьютера в Интернет запрещен, а запросы по HTTP протоколу будут перенаправляются автоматически на Веб сервер.

Для выхода пользователю необходимо открыть Веб сервер с запросом logoff на конце (например, <http://192.168.1.1:8008/logoff>), либо нажать ссылку ВЫХОД, которая появляется после имени пользователя на странице статистики. Используйте политику домена, чтобы добавить открытие адреса logoff при выходе пользователя из домена, для автоматического выхода.

**Если не производить выход через Веб сервер, то следующий пользователь будет работать от имени предыдущего, поскольку в Интернет Администраторе сохранилась старая регистрация и новую он запрашивать не будет.**

## Регистрация через MS Active Directory

Если установлен режим MS Active Directory, то, до вывода статистики, Веб сервер пытается получить данные о зарегистрированном доменном пользователе на компьютере. Для этого используется встроенная проверка подлинности Windows, которая интегрирована во все современные браузеры. Проверьте что она включена в браузерах на рабочих станциях. Так выглядят свойства Internet Explorer для настройки проверки подлинности.

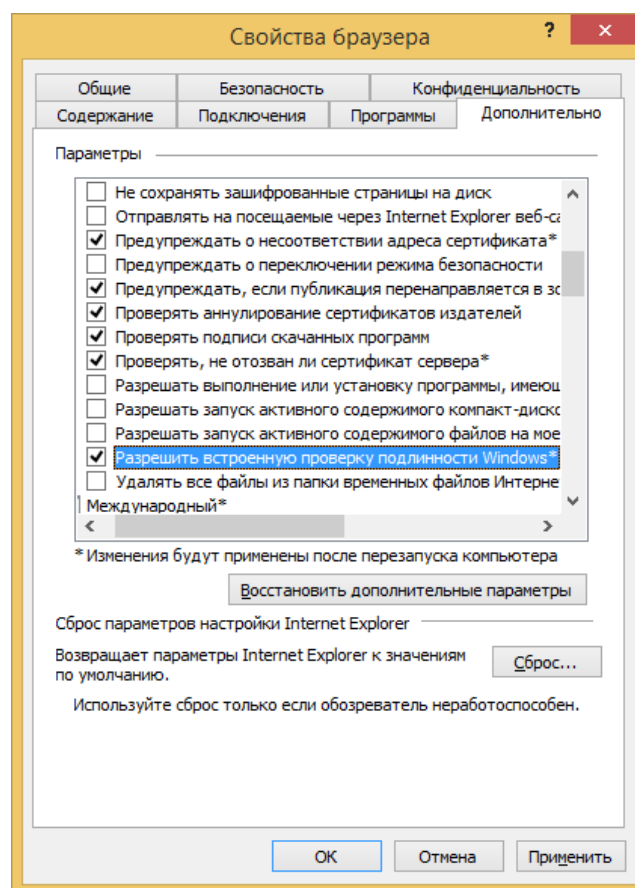
Указанная галочка должна быть включена.

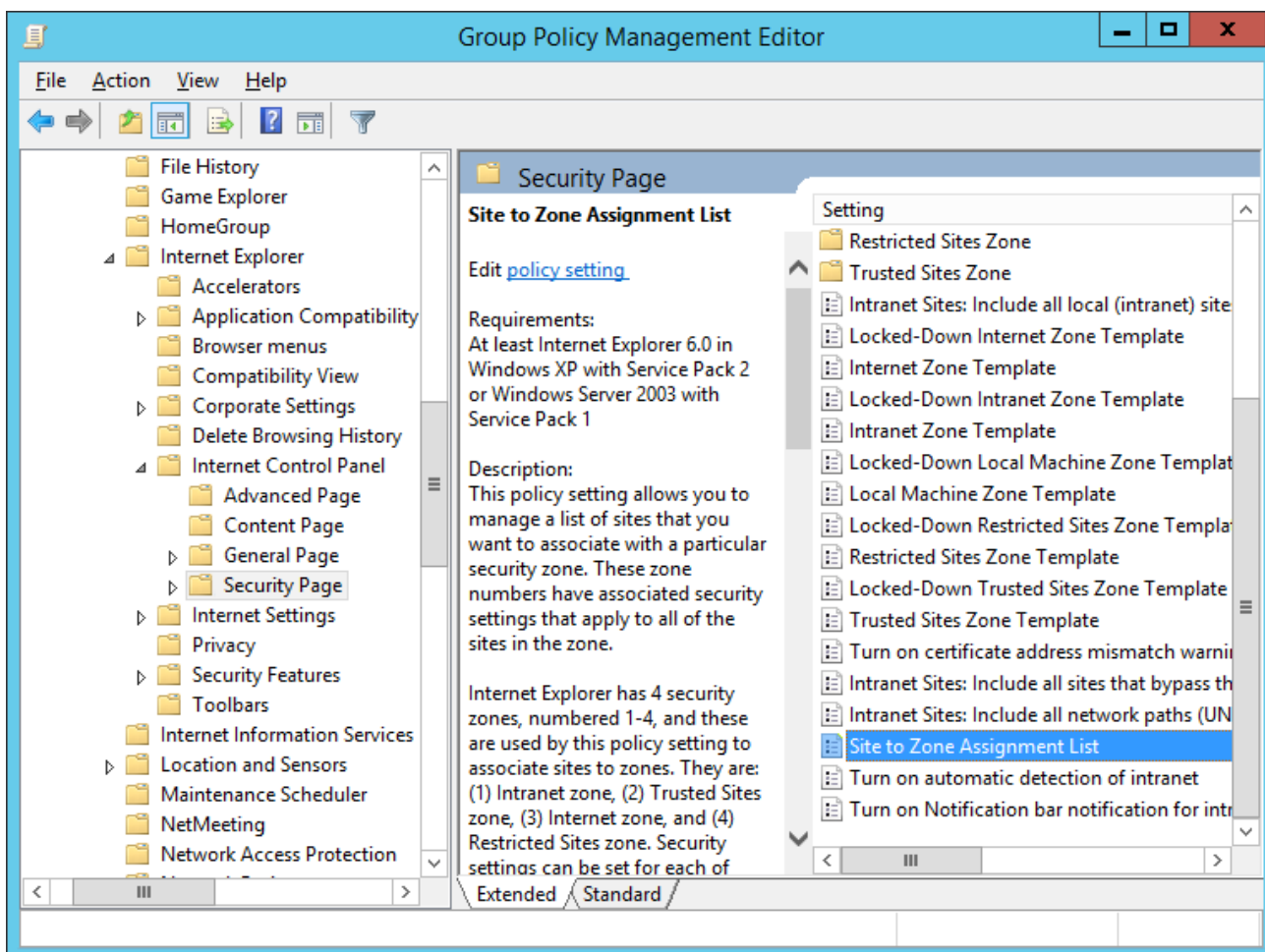
В проверке подлинности участвуют 3 компьютера: рабочая станция пользователя, сервер с Интернет Администратором и контроллер домена Active Directory. Контроллер удостоверяет, что на рабочей станции зарегистрирован доменный пользователь и передает его дескриптор безопасности, из которого Веб сервер получает имя пользователя для прохождения процедуры регистрации.

В случае если автоматическая проверка подлинности запрещена, в браузере выдается окно для запроса доменного имени и пароля. Эти имена и пароли не передаются на наш Веб сервер. Аутентификацией пользователя занимается контроллер домена, и только после получения от него данных о входе на компьютере под доменным пользователем, наш Веб сервер сможет произвести регистрацию!

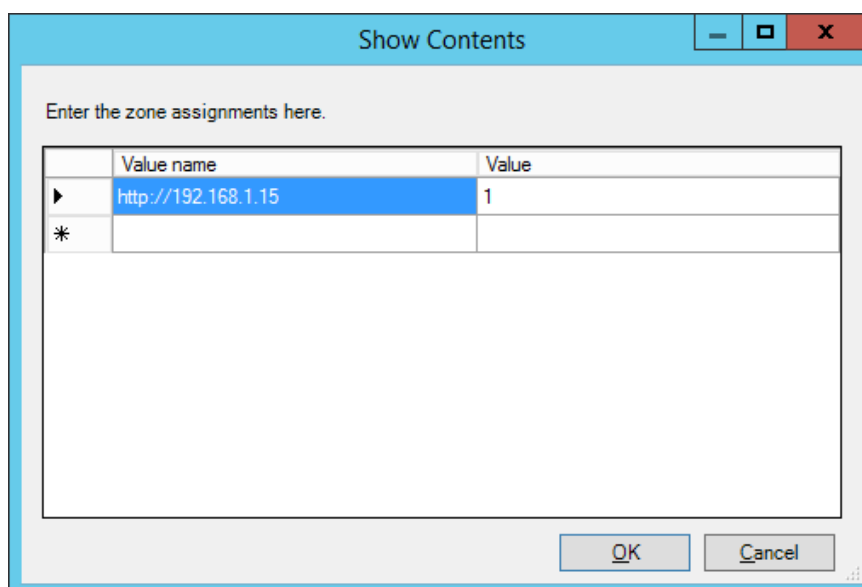
По умолчанию автоматическая проверка подлинности отключена, и окно с вводом имени и пароля будет возникать каждый раз в новой сессии.

**Для включения автоматической проверки подлинности**, чтобы пользователь не вводил свои доменные имя и пароль, добавьте адрес IAdmin Web в зону безопасности «Местная Интрасеть» на каждой рабочей станции. Централизованно это можно сделать через групповую политику домена. Настройка находится по пути Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page.



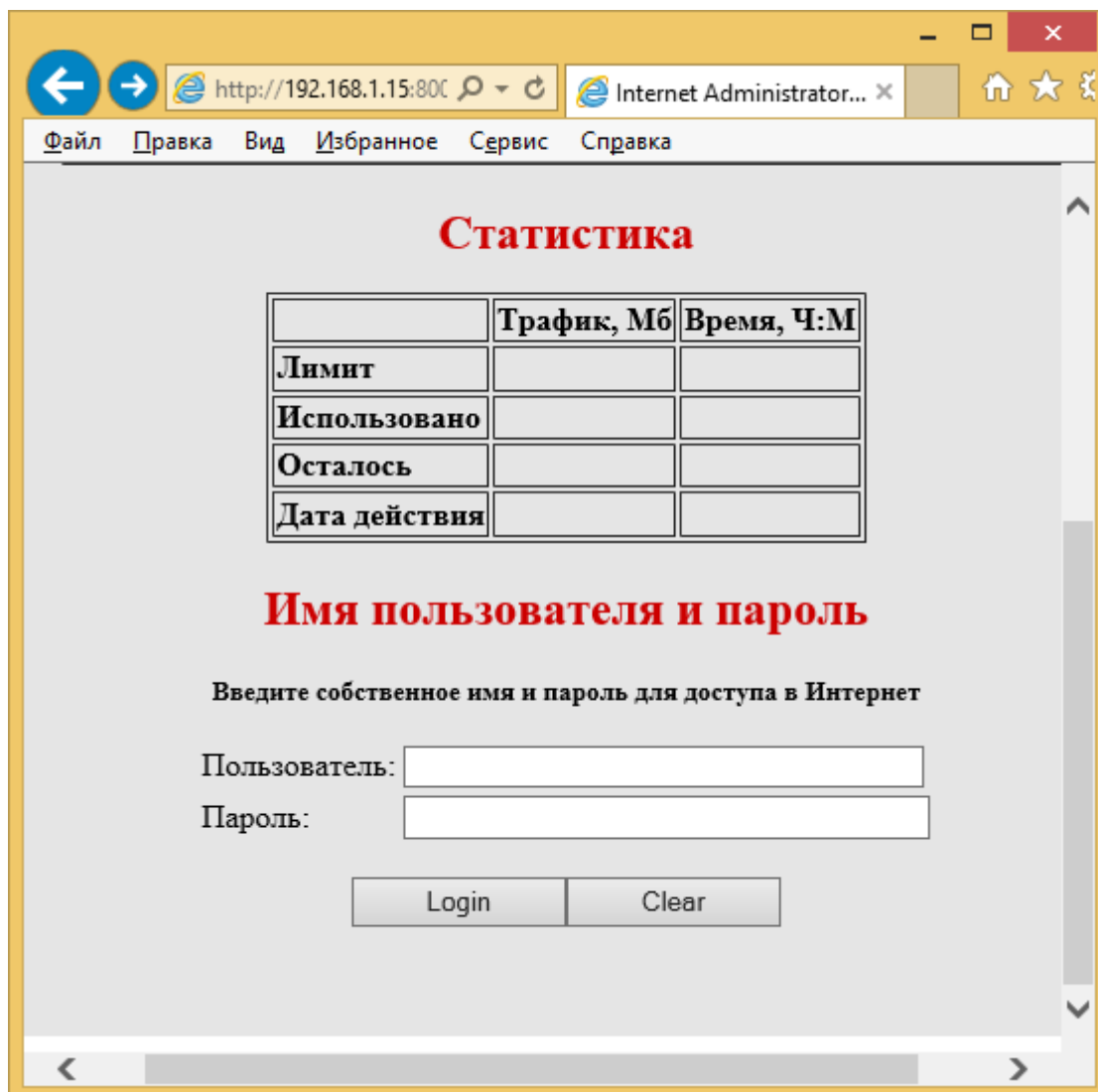


Добавьте в «Site to Zone assignment list» IP адрес веб сервера Интернет Администратора, на котором он работает, и установите значение типа сети 1.



### Регистрация по имени и паролю

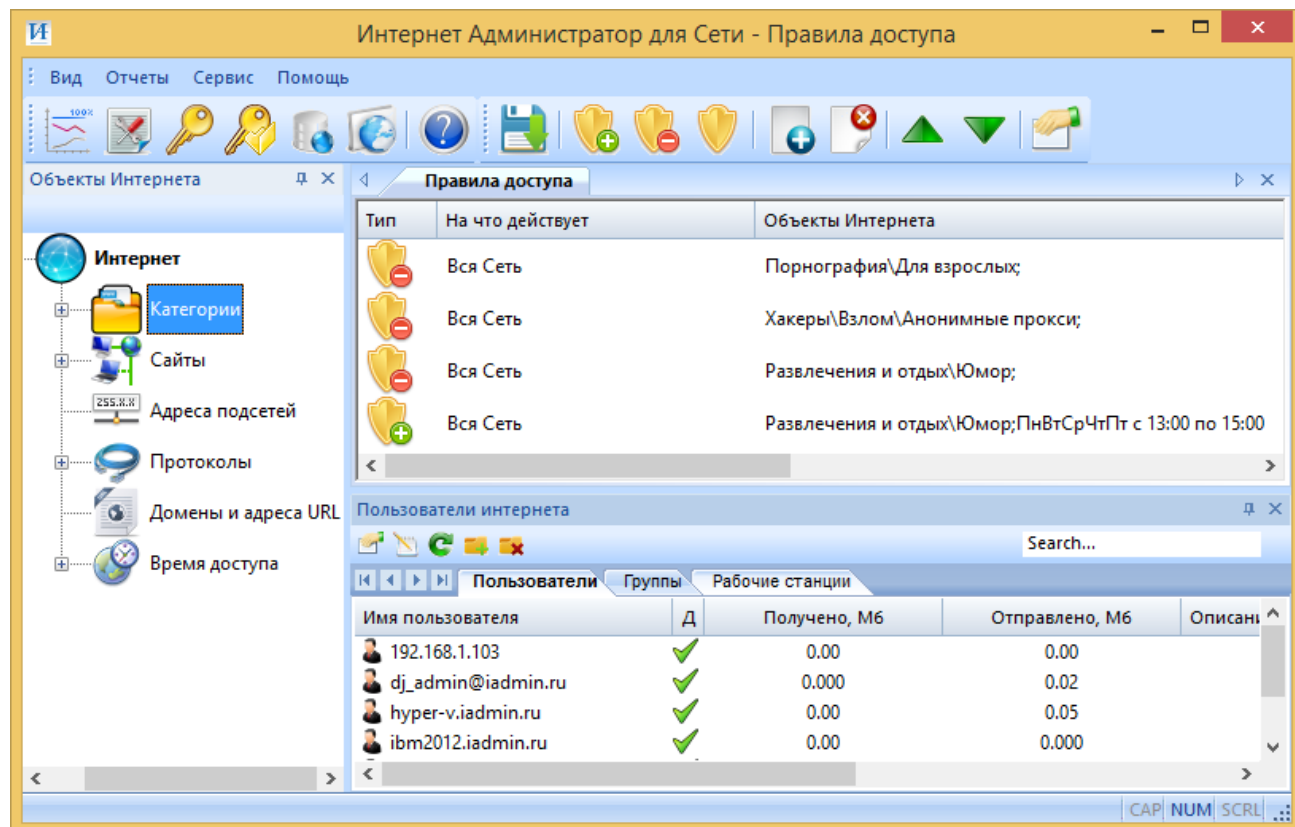
Если установлен режим По имени и паролю, то внизу на странице статистики Веб сервер выдет форму для ввода имени и пароля, которые заранее задаются в свойствах пользователя администратором.



После успешной регистрации, пользователь получает доступ в Интернет.

## РАЗДЕЛ 5 – КОНТРОЛЬ ДОСТУПА В ИНТЕРНЕТ

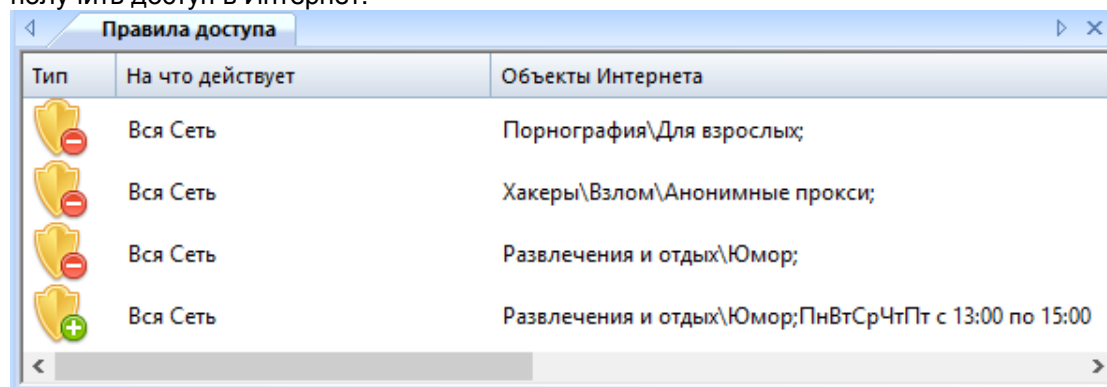
В данном разделе описываются методы управления ресурсами Интернет. Все настройки, приведенные в этом разделе, выполняются из «Администратора Правил».



В главном окне «Администратора правил» отображается список правил доступа, дерево объектов Интернета, а также список Пользователей Интернета.


### Раздел 5.1. – Система правил

Система правил определяет политику доступа – кто, когда куда и как может получить доступ в Интернет.

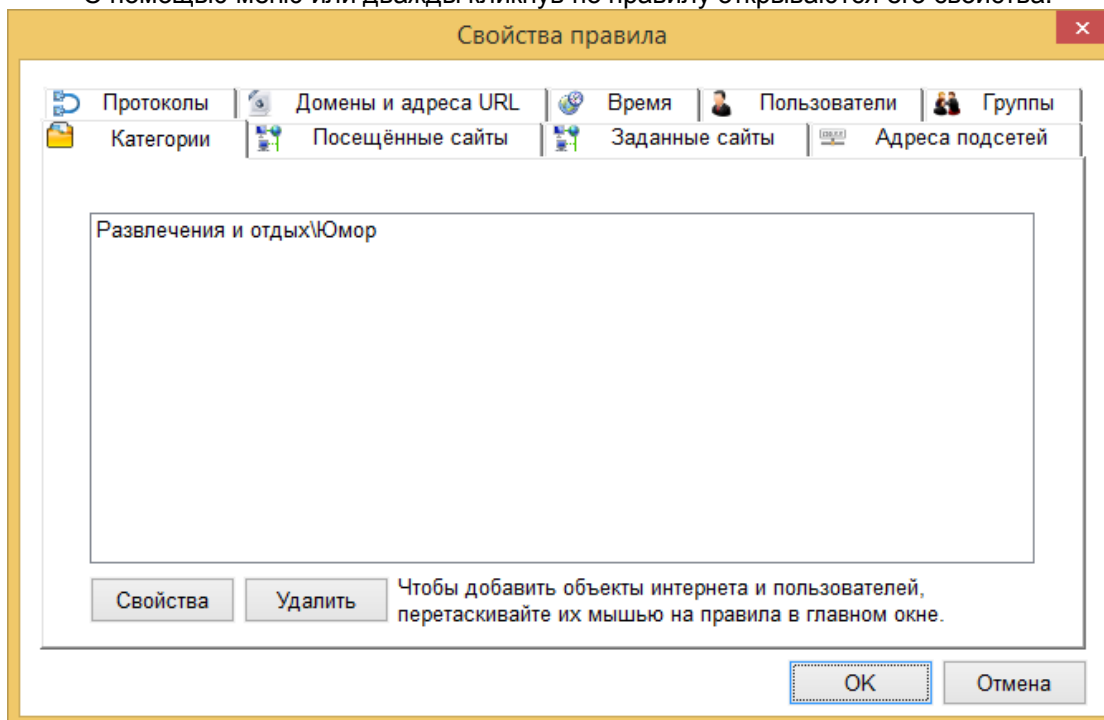


Правила работают по приоритету сверху вниз, наивысший приоритет имеет самое последнее по списку правило. Правило может разрешать или запрещать доступ и быть отключенным, при этом оно не учитывается в общей политике доступа. При отсутствии правил доступ неограничен.

Создать правило можно из контекстного меню, либо перенеся любой объект мышкой на свободное от текущих правил место в списке правил. Новое правило по умолчанию разрешает доступ ко всем ресурсам для всех.

Заполнение правил объектами происходит путем перетаскивания мышью. Для добавления нужный объект нужно захватить мышью (нажать и удерживать левую кнопку) и, передвигая его, опустить на нужное правило, либо на свободную область в правилах. Для вступления изменений в правилах в силу нужно нажать кнопку Сохранить  на главной панели инструментов.

С помощью меню или дважды кликнув по правилу открываются его свойства.







Здесь просматриваются и удаляются Объекты и пользователи Интернета, которые ранее были добавлены в правило, а также свойства

## Раздел 5.2. – Как работают правила

Правила работают по списку сверху вниз. Нижестоящее правило имеет приоритет над вышестоящим и может отменять ограничения, либо усиливать их. Система ищет сначала запрещающее правило и объекты в нем, а затем далее по списку разрешающее. Если разрешающего правила на данный ресурс не обнаружено, доступ блокируется. Если разрешающее правило найдено, ищется далее по списку запрещающее, и если оно не найдено для текущего запроса, доступ будет разрешен.

### Пример.

Тип	На что действует	Объекты Интернета
	Вся Сеть	Порнография\Для взрослых;
	Вся Сеть	Хакеры\Взлом\Анонимные прокси;
	Вся Сеть	Развлечения и отдых\Юмор;
	Вся Сеть	Развлечения и отдых\Юмор; ПнВтСрЧтПт с 13:00 по 15:00

В первых трех правилах на рисунке выше блокируется доступ к соответствующим категориям. Однако четвертое правило делает исключение, и разрешает доступ к Развлекательным сайтам в обеденное время с 13 до 15 часов. Однако, если бы существовало пятое правило, блокирующее доступ к определенному сайту из категории Развлечения, этот сайт был бы недоступен в любое время вне зависимости от 4го правила.

### Раздел 5.3. – Элементы правила

#### Пользователи и группы

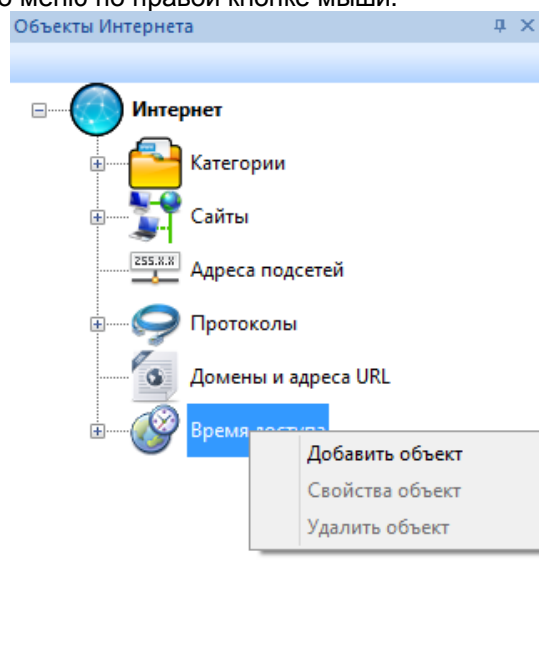
Пользователи и группы – это первый тип элементов, который определяет на кого распространяется правило. Если пользователи и группы не входят в правило, то оно распространяется на всю сеть.

#### Объекты Интернета

Объекты Интернета – это второй тип элементов, который определяет к чему правило будет блокировать или разрешать доступ. Если в одном правиле заданы несколько разных объектов Интернета, то их действие будет определяться совместно при решении вопроса об ограничении доступа. Например, если в одном правиле заблокирован определенный сайт и время, то доступ к этому сайту будет закрыт только в указанное время. Совместно в одном правиле могут быть объединены две группы:

- Сайты, Адреса подсетей, Протоколы, Домены и адреса URL, Время;
- Категории, Время.

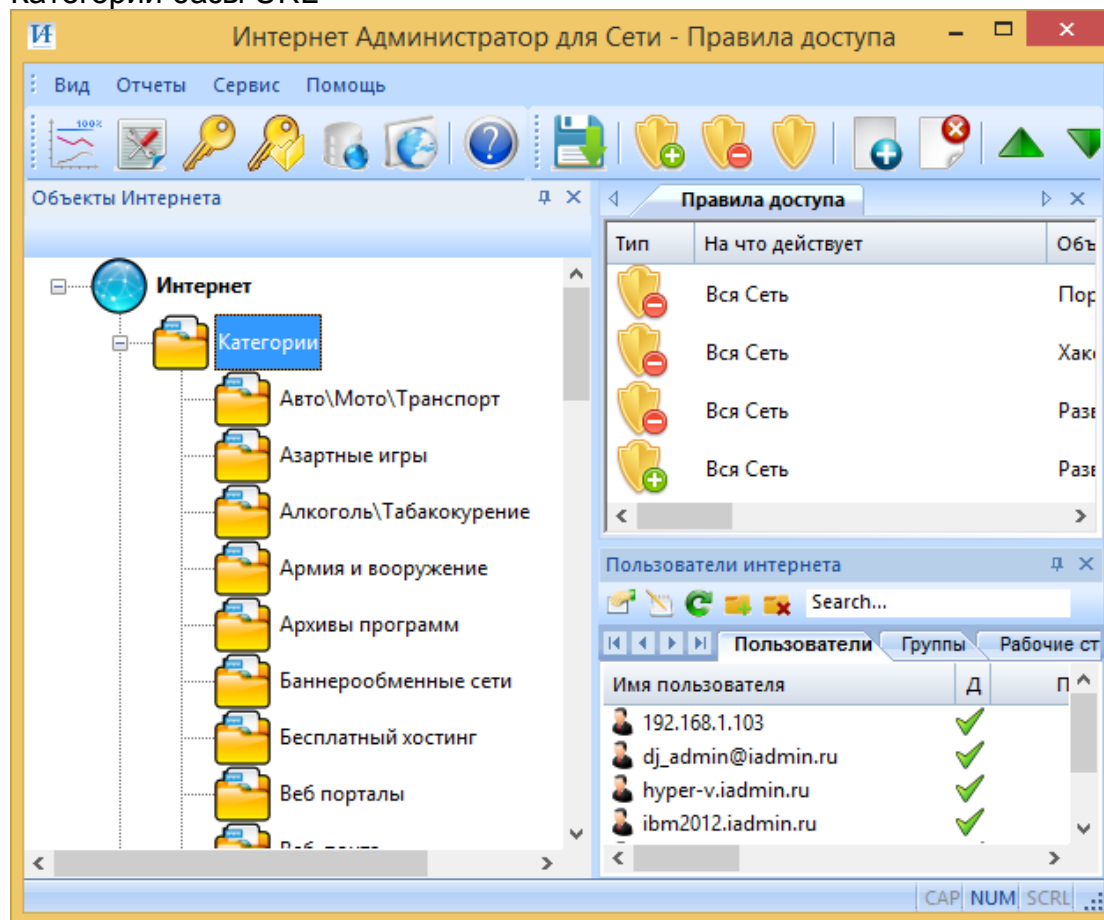
Добавление объектов Интернета в соответствующий список осуществляется с помощью контекстного меню по правой кнопке мыши.



В данном меню также можно просмотреть свойства объекта и удалить его, если меню открывается непосредственно при выделении Объекта.



## Категории базы URL



В списке представлено 38 стандартных категорий с более чем 3,5 млн. сайтов. Использование категорий доступно только после ввода ключа для Базы категорий и привязки его к текущему серверу. Смотрите Раздел 6.2. — Лицензирование базы категорий для дополнительной информации.

Описание стандартных категорий смотрите на сайте <http://www.iadmin.ru/products/?pid=7>.

**Сайты входящие в стандартные категории нельзя увидеть или редактировать.** Для проверки принадлежности сайта к категории используйте сервис проверки <http://www.iadmin.ru/support/urlchecker/>.

Кроме стандартных предусмотрено добавление пользовательских категорий. В такие категории администратор сам добавляет нужные сайты.



## Сайты

Сайты представлены двумя списками – посещенные и заданные. Посещенные сайты обнаруживаются при пользовательских запросах, эти те сайты, на которые был когда-либо осуществлен доступ. Заданные сайты добавляются администратором вручную.

Создание нового сайта

Введите имя сайта

www.ya.ru

Внимание! Если вы укажете IP адреса, то блокировка будет осуществляться как по имени так и по IP адресу хоста. В случае если на данном IP адресе есть несколько разных веб сайтов, все они будут заблокированы.

IP адреса

Получить IP адреса через DNS

Список IP

Ввести адреса вручную

Добавить Удалить

Создать Отмена

При этом указывается имя и IP адреса сайта. IP-адрес является необязательным параметром. Если он не задан, то ограничение будет осуществляться только по HTTP протоколу, в противном случае доступ будет блокироваться по IP адресам по любым протоколам. Адрес можно получить, используя механизм разрешения имен. Для этого нажмите кнопку «Получить IP адреса через DNS» в окне добавления хоста.

## Адреса подсетей

Свойства адреса подсети

Сетевой IP адрес и маска подсети

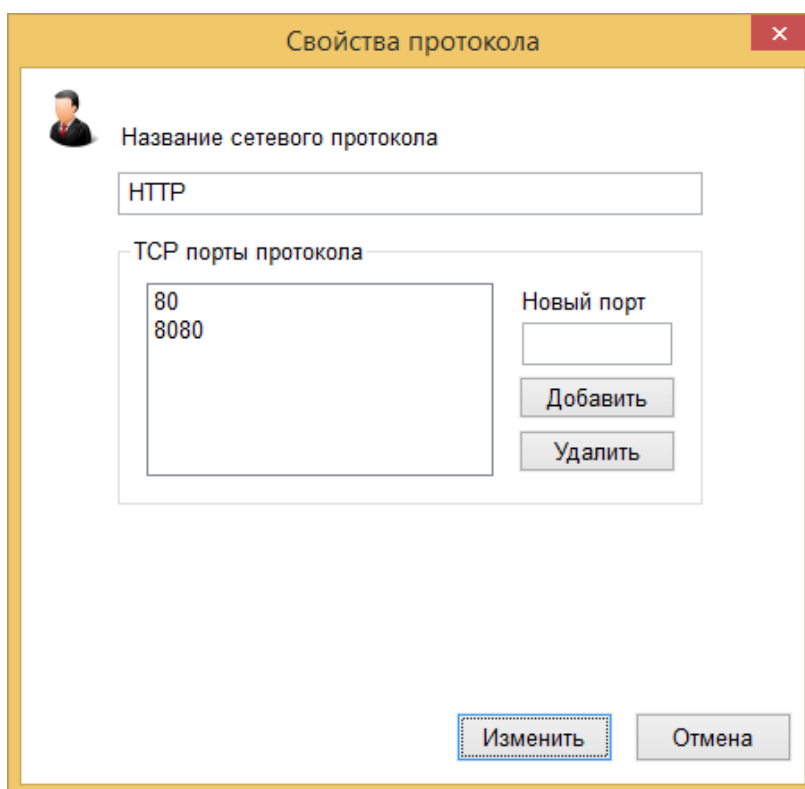
IP адрес 192 . 168 . 2 . 0

Маска подсети 255 . 255 . 255 . 0

Изменить Отмена

Этот объект определяет набор хостов Интернет по IP адресам. Адреса задаются в виде адреса IP-сети и маски.

## Протоколы



Протоколы связи содержат в себе список портов TCP/IP, по которым осуществляется передача данных между рабочей станцией и хостами Интернет. По умолчанию в этот объект добавлен список из некоторых стандартных протоколов.

## Домены и адреса URL

Объект Домены и адреса URL предназначен для задания поисковых строк, которые будут сравниваться с адресом запроса (адресная строка обозревателя) по протоколу HTTP.

Запрос URL имеет следующий формат

[http://имя\\_сайта.имя\\_домена.имя\\_корневого\\_домена/запрос.расширение?параметр1=значение1&параметр2=значение2](http://имя_сайта.имя_домена.имя_корневого_домена/запрос.расширение?параметр1=значение1&параметр2=значение2) и так далее.

Поиск производится в любом месте запроса, поэтому для анализа можно задать:

- Имя сайта, например [www.iadmin.ru](http://www.iadmin.ru)
- Домен, в том числе корневой, например [iadmin.ru](http://iadmin.ru) или [.com](http://.com)
- Страницу или каталог запроса, например [/product/](http://product/) или [/mypage.html](http://mypage.html)
- Названия и параметры запроса, например [porno](http://porno)

## Время доступа

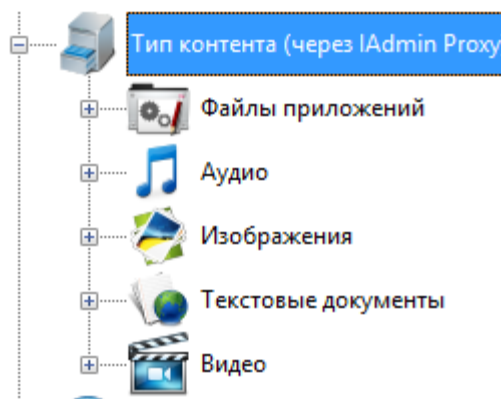
Данный объект определяет интервал времени, в котором сработает то или иное правило. Время доступа задается по дням недели и времени дня недели.

## Тип контента

**Внимание! Этот объект будет работать только для компьютеров, использующих IAdmin Proxy в качестве HTTP/HTTPS прокси-сервера!**

Тип контент показывает, к чему относится тот или иной ответ веб сервера. Здесь представлены файлы приложений, аудио и видео контент, изображения, а также веб страницы в виде текстовых документов. Тип контента определяется в соответствии с MIME типами по HTTP заголовку Content-Type.

Вы можете редактировать стандартные типы или создавать свои.



## Страны по IP адресу

Интернет Администратор определяет страну, в которой физически расположен хостинг сайта по IP адресу.

За каждой страной закреплены определенные IP адреса, по которым можно установить, где физически располагается сайт. Это дает гарантию, что материалы сайта находятся под юрисдикцией той или иной страны и обязаны соответствовать законам. Например, в России запрещено распространение порнографии, следовательно, ни один провайдер в России не позволит размещать такие материалы и можно гарантировать, что таких материалов Вы не увидите.


Однако стоит иметь в виду, что популярные сервисы могут располагаться за пределами нужных стран и станут недоступными, но к таким сервисам можно применять отдельные разрешающие правила!

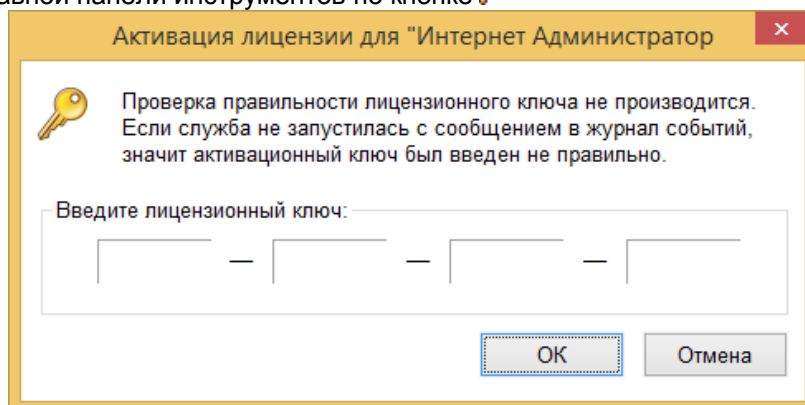


## РАЗДЕЛ 6 – СЕРВИС

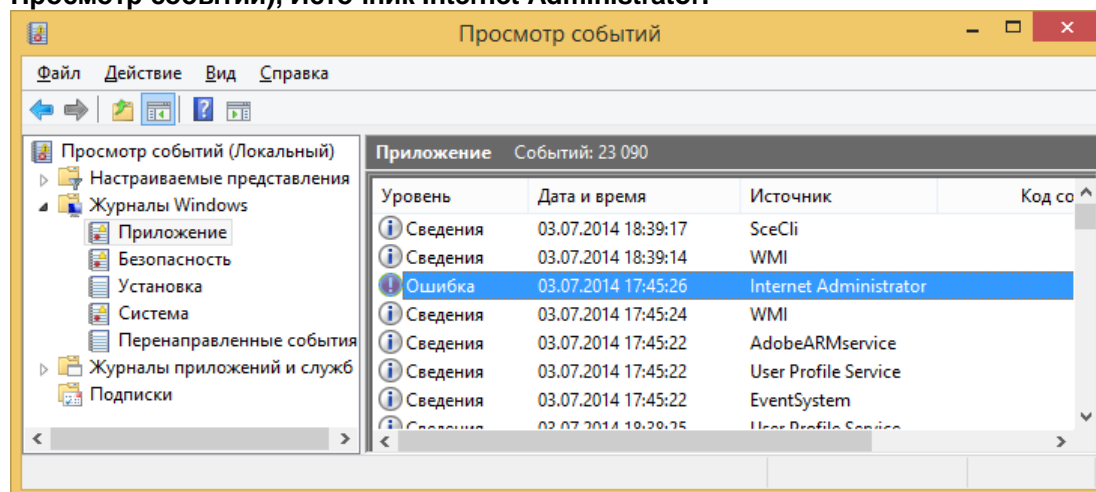
**Раздел 6.1. — Лицензирование программы**

Вы можете использовать «Интернет Администратор» без лицензионного ключа 60 дней с момента первой установки на сервере. После покупки программы Вы получите лицензионный ключ, который необходимо ввести для дальнейшей работы. Ключ определяет максимальное число компьютеров, с которыми будет работать программа и если это число будет превышено при обнаружении новых компьютеров, они будут автоматически попадать в Неотслеживаемые.

Ввод ключа осуществляется в главном меню Сервис -> Лицензионный ключ или на главной панели инструментов по кнопке 




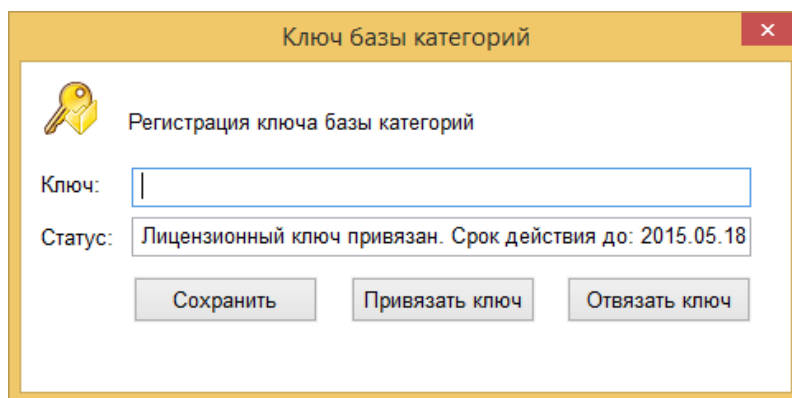
При вводе ключа проверка не осуществляется, пожалуйста, вводите его внимательно. Проверка происходит в процессе запуска службы IAdmin Server. Если служба не запустилась, то одной из причин может быть неверный лицензионный ключ. **В случае неудачного запуска служба записывает сообщение в раздел Приложение журнала событий Windows (доступен в Администрирование, Просмотр событий), Источник Internet Administrator.**



После ввода ключа, если программа работала в пробном режиме, службу IAdmin Server необходимо перезапустить, чтобы она перешла в нормальный режим работы.

**Раздел 6.2. — Лицензирование базы категорий**

Использование категорий доступно только после ввода ключа для Базы категорий и привязки его к текущему серверу. Ввод ключа осуществляется в главном меню Сервис -> Ключ базы категорий или на главной панели инструментов по кнопке 



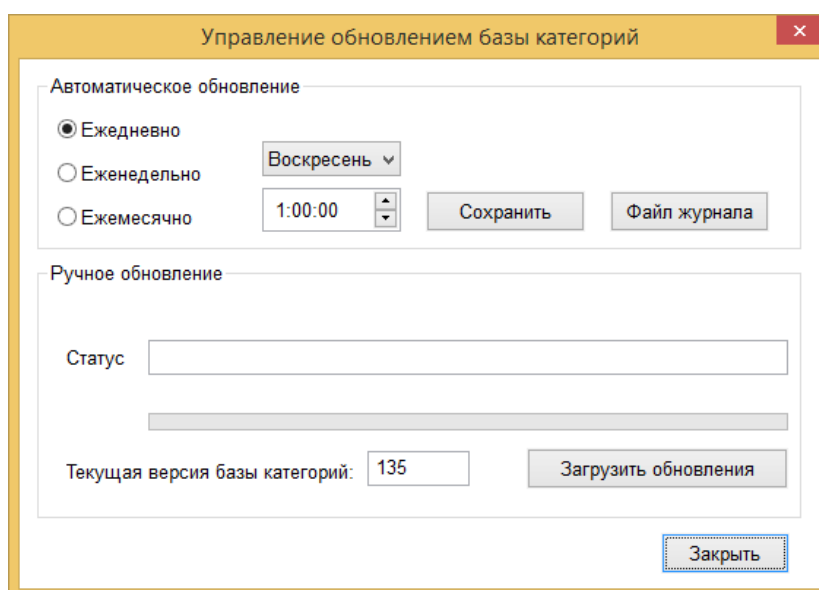
После вводу ключа нажмите кнопку Сохранить а затем Привязать. Произойдет запись, а затем подключение к серверу обновлений через Интернет для проверки ключа, и в случае успеха он будет привязан к текущему серверу.

Привязанный ключ невозможно использовать на другом сервере, для этого его необходимо отвязать на текущем сервере.

Категории работают ограниченное время, которое определяет ключ базы категорий. При первоначальной покупке ключ дает возможность использовать категории 1 год с момента продажи. За 30 дней до окончания срока программа будет предупреждать о сроке окончания ключа базы категорий. По истечении срока ключа для дальнейшего использования категорий необходимо оплатить использование базы категорий на следующий период (1 или 3 года) и получить новый ключ.

### Раздел 6.3. – Обновление базы категорий

Интернет Администратор Компани периодически выпускает обновления для базы категорий для поддержания ее в актуальном состоянии. Ежедневно обрабатываются тысячи новых порно сайтов, анонимных прокси-серверов и других вредоносных сайтов. Обновления доступны для загрузки только после ввода и привязки ключа базы категорий, который также имеет срок действия. Обновления добавляют сайты в базу, изменяют категорию уже имеющимся сайтам или удаляют сайты из базы категорий. Механизм обновления реализован посредством интерфейса управления и службы обновлений IAdmin Update Service. Интерфейс управления открывается через главное меню Сервис -> Обновление базы категорий.



В интерфейсе управления задается период автоматического обновления: Ежедневно, Еженедельно, Ежемесячно и указывается время суток. Данный период указывает, как часто служба обновлений будет связываться с сервером обновлений через Интернет. Результаты автоматического обновления записываются в журнал, который открывается по кнопке «Файл журнала».

В интерфейсе обновления возможно вручную произвести обновление по кнопке «Загрузить обновления». Статус выполнения и результат будут отображены в окне.

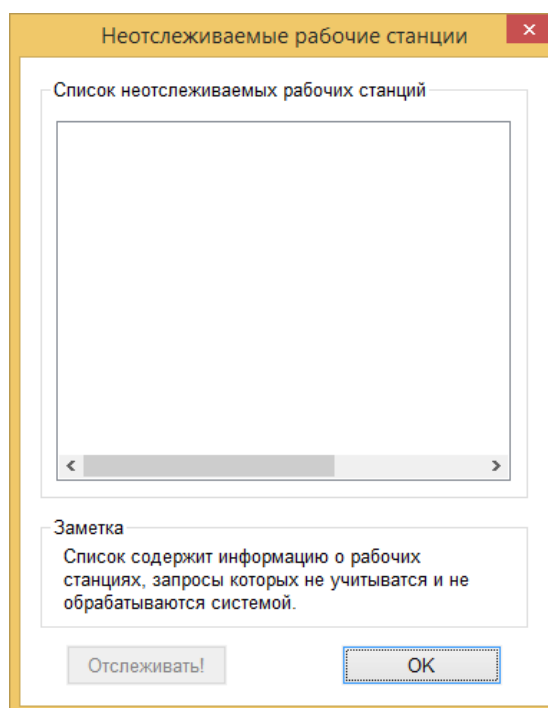
#### Раздел 6.4. — Неотслеживаемые рабочие станции

По умолчанию все рабочие станции отслеживаются и присутствуют в списке рабочих станций главного окна. Иногда существует необходимость игнорировать общую политику доступа для некоторых рабочих станций или серверов сети. Для неотслеживаемых рабочих станций не учитывается доступ и не применяются никакие ограничения.

Перевод рабочей станции в список неотслеживаемых производится из контекстного меню, выделив нужную рабочую станцию. В главном меню Сервис -> Неотслеживаемые компьютеры открывается список неотслеживаемых рабочих станций.

Отсюда можно перевести рабочую станцию обратно в основной список.

Если введен лицензионный ключ количество рабочих станций равно количеству лицензии, то все новые рабочие станции будут добавляться в список неотслеживаемых. **Если на момент ввода лицензионного ключа число рабочих станций превышает число, предусмотренное лицензией, то часть таких станций нужно перевести в список неотслеживаемых.** Комплекс будет отслеживать только то количество рабочих станций, сколько предусмотрено лицензией, даже если в основном списке их больше, чем лицензия. В этом случае будет трудно сказать, какие компьютеры отслеживаются, а какие нет.



## Раздел 6.5. — Очистка базы данных

Очистка базы данных

Ручная очистка

Удалить ВСЮ информацию

Удалить пользователей и компьютеры

Сохранить данные за:

За сегодня

За последнюю неделю

За последний месяц

За период С 04.07.2014

По 04.07.2014

Сохранить данные о трафике

Очистить

Автоматическая очистка

Включить

Еженедельно Суббота

Ежемесячно 2:00:00

Ежеквартально

Сохранять данные за:

За месяц

За квартал

За год

Сохранить

Закрыть

Для ускорения работы базы данных и для ограничения разрастания файла базы на физическом носителе Вы можете периодически удалить из нее устаревшую информацию. В меню «Сервис» выберите «Очистка рабочей базы».

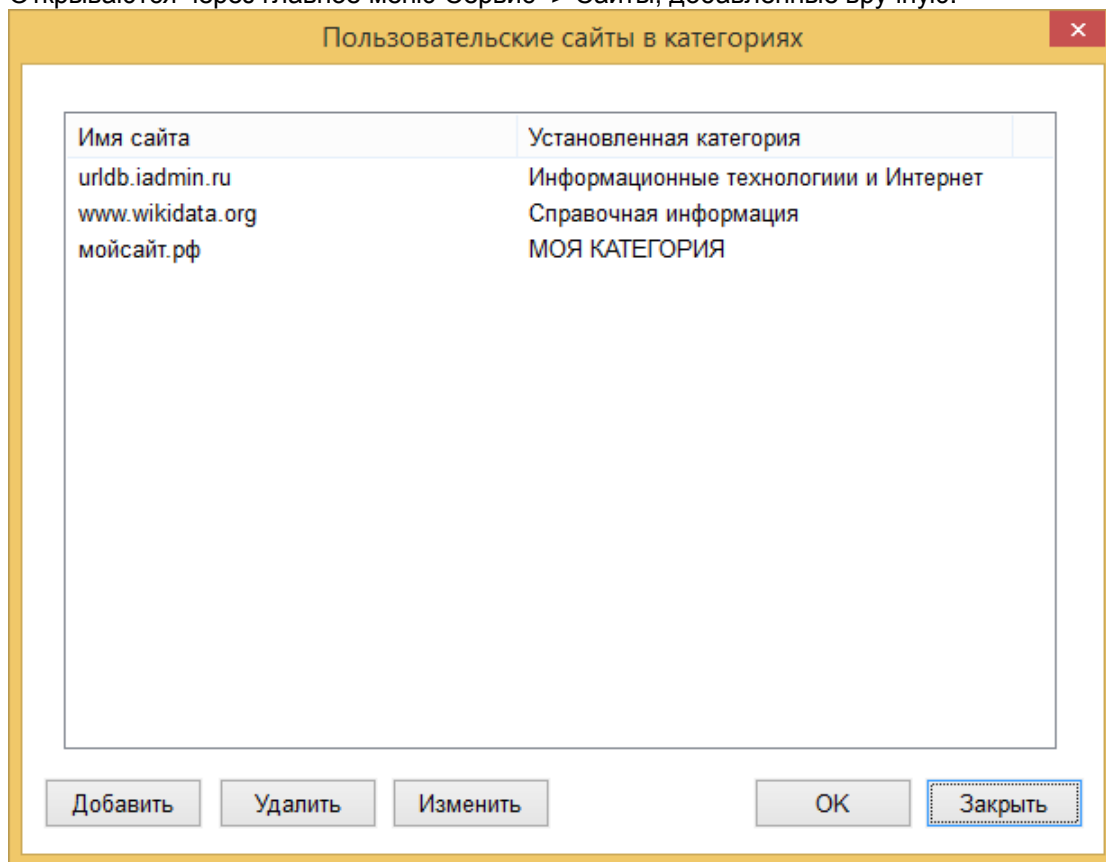
Вручную Вы можете удалить всю информацию с пользователями и рабочими станциями, либо указать временной интервал. Допускается Сохранить информацию за день, за последнюю неделю, месяц, либо указать интервал вручную.

Для настройки автоматического режима очистки, включите его, установив галочку, и задайте необходимые параметры очистки. Автоматическую очистку осуществляет служба IAdmin Update Service, результаты очистки записываются в файл update.log в папке установки программы.



## Раздел 6.6. - Пользовательские сайты в Категориях

Открываются через главное меню Сервис -> Сайты, добавленные вручную.



В окне представлен список сайтов и категория, заданные с помощью:

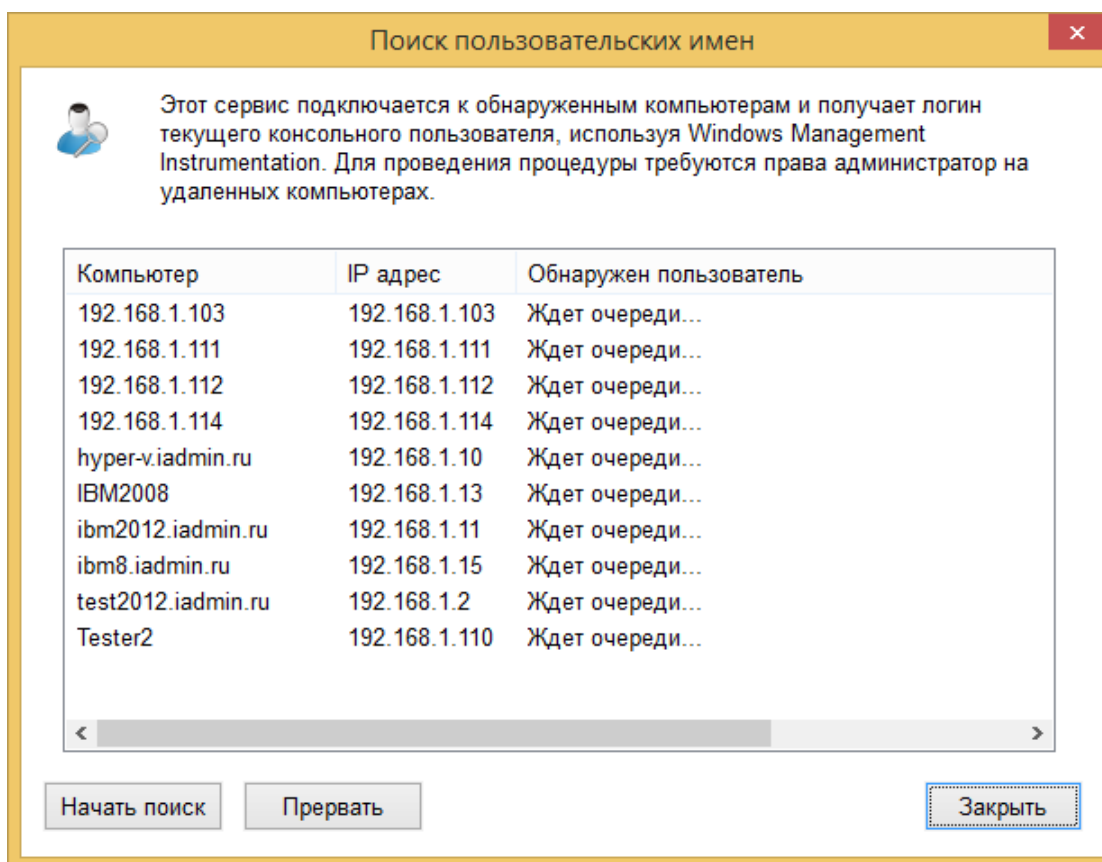
- Журнала доступа в Интернет и присвоения ему существующей категории.
- Добавления сайта в пользовательскую категорию.

При удалении сайта, он перестает принадлежать какой либо категории.

Вы можете добавлять любые сайты по имени и присваивать им стандартные либо пользовательские категории.

### Раздел 6.7. – Поиск пользовательских имен.

Поиск пользовательских имен доступен через меню Сервис -> Поиск пользовательских имен.




В статическом режиме в качестве имени пользователя используется обнаруженное имя компьютера. Для более наглядного представления используйте поиск для изменения имен пользователей в базе данных. Сервис будет связываться с каждым компьютером и запросит текущее имя пользователя. Для этого необходимы административные права на каждом компьютере, используйте этот сервис под именем администратора домена.

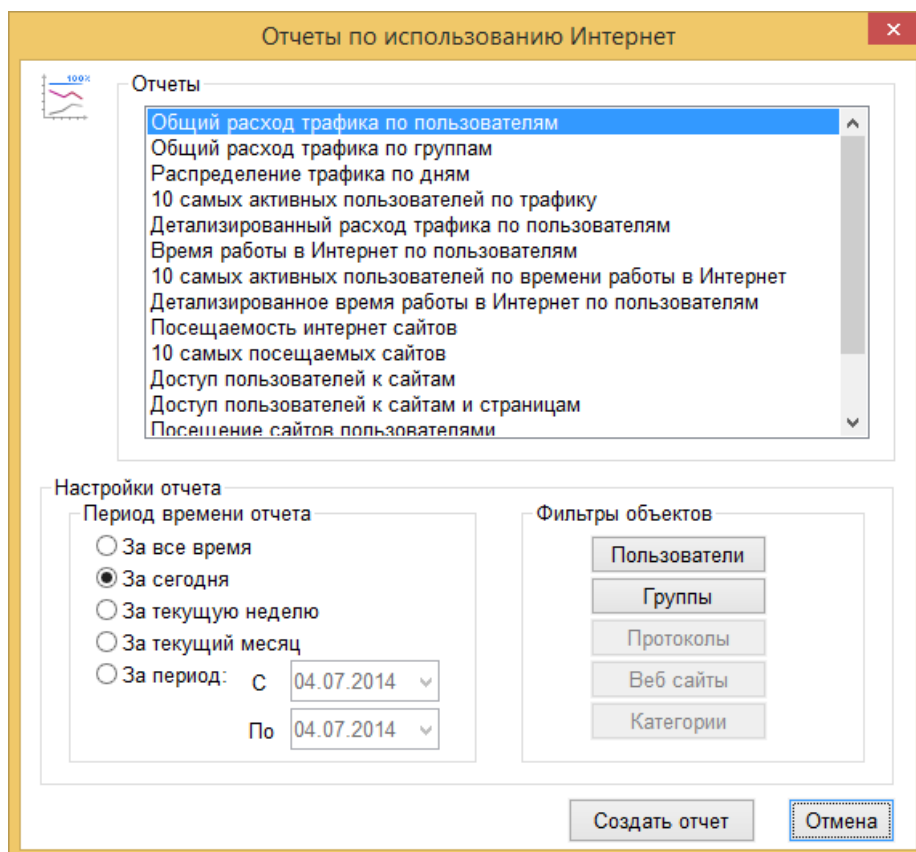
**Не используйте эту функцию в режиме MS Active Directory!**

## РАЗДЕЛ 7 –ОТЧЕТЫ

Система «Интернет Администратор» предоставляет широкие возможности в области формирования отчетов, отражающих динамику использования Интернет в Вашей организации.

### Раздел 7.1. — Формирование отчетов

Для открытия окна вывода отчетов Вы можете воспользоваться панелью инструментов кнопкой  или выбрать пункт «Отчеты» в меню «Отчеты».



Для построения выберите соответствующий отчет и укажите период времени данных. Помимо времени отчета здесь возможно указать фильтры объектов: Пользователи, Группы, Протоколы, Веб сайты и Категории.

### Раздел 7.2. — Настройка отчетов

Вы можете настраивать отчеты по следующим характеристикам.

- Пользователи, информация о которых будет использована при формировании отчета.
- Группы пользователей, информация о которых будет использована при формировании отчета.
- Период времени, за который будет использована информация о доступе в Интернет. Вы можете указать следующие периоды времени: за всё время, за сегодня, за текущую неделю или месяц, а также задав интервал вручную.
- Протоколы доступа.
- Категории веб сайтов.
- Отдельные сайты.

Данные о фильтрах будут содержаться в сформированном отчете.

### Раздел 7.3. — Список отчетов

Состав и описание текущих отчетов - <http://www.iadmin.ru/products/?pid=10>

### Раздел 7.4. — Экспорт данных в формате W3C

Кроме встроенных отчетов Интернет Администратор позволяет выгрузить свои данные в формате W3C для анализа сторонними программами построения отчетов. Для запуска экспорта в меню «Отчеты» выберите «Экспорт данных».

Укажите файл, куда будет произведен экспорт данных, а также задайте период времени для выгрузки данных, собранных Интернет Администратором. Формат данных в файле совместим с форматом лог файлов Microsoft ISA Server 2004.

Описание полей файла экспорта:

#Fields:	Описание
c-ip	Имя пользователя
cs-username	Имя пользователя
c-agent	Агент, всегда указан Unknown
date	Дата
time	Время
s-computername	Имя сервера, всегда указан IA_Server
cs-referred	Всегда указан -
r-host	Имя удаленного сайта
r-ip	IP адрес удаленного сайта
time-taken	Длительность запроса
cs-bytes	Отправлено байт
sc-bytes	Получено байт
cs-protocol	Порт
s-operation	Всегда GET
cs-uri	Запрос к серверу
x-action	Был ли доступ закрыт или разрешен
x-category	Категория удаленного сайта по базе категорий URL

## РАЗДЕЛ 8 – БАЗА ДАННЫХ И ПОДДЕРЖКА Microsoft SQL server

База данных «Интернет Администратора» является основным хранилищем информации. Сюда записываются данные об активности пользователей, хранятся правила и другие настройки программы.

### Раздел 8.1. — База данных по умолчанию

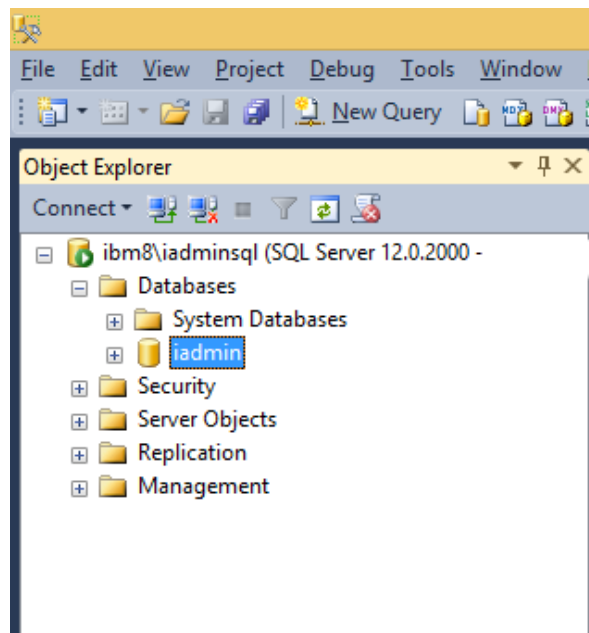
В процессе установки «Интернет Администратор» устанавливает Microsoft SQL Server Express, создает источник данных ODBC и новую базу данных на установленном Microsoft SQL Server Express.

Для доступа к базе данных, например, для резервного копирования, необходима дополнительная установка Microsoft SQL Server Management Studio, доступная для загрузки с сайта Microsoft.

База данных располагается в экземпляре IADMINSQL на локальном сервере (SQL Server name: localhost\iadminsql). Пользователь Windows, от имени которого происходила установка программы, является администратором экземпляра IADMINSQL.

Для подключения используется источник данных ODBC с именем iadmin, SQL пользователь - sa. В случае изменения пароля пользователя sa в экземпляре IADMINSQL, его необходимо изменить через Мастер базы данных.

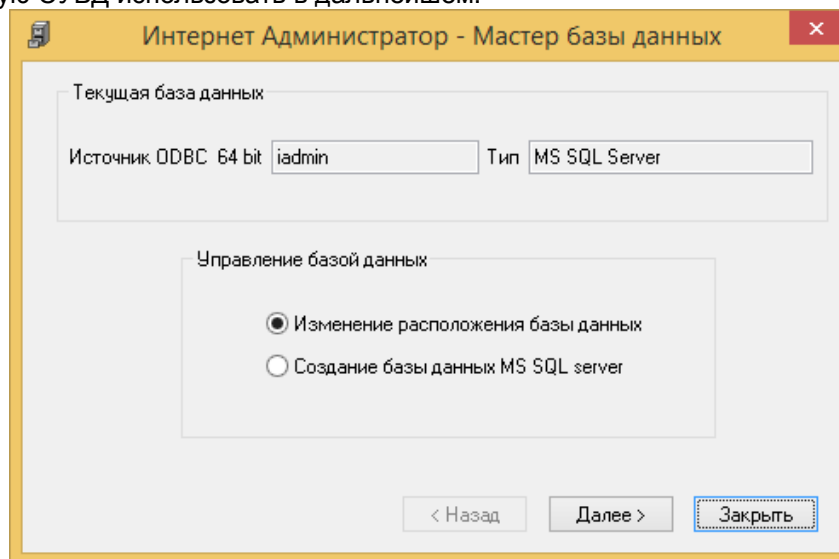
Microsoft SQL Server Express имеет ограничения: поддерживает 1 физический процессор, 1 ГБ памяти и 10 ГБ дискового пространства. В нем также недоступен SQL Server Agent и функции с ним связанные. Для снятия ограничений необходимо использовать полноценный Microsoft SQL Server.



### Раздел 8.2. — База данных на MS SQL Server

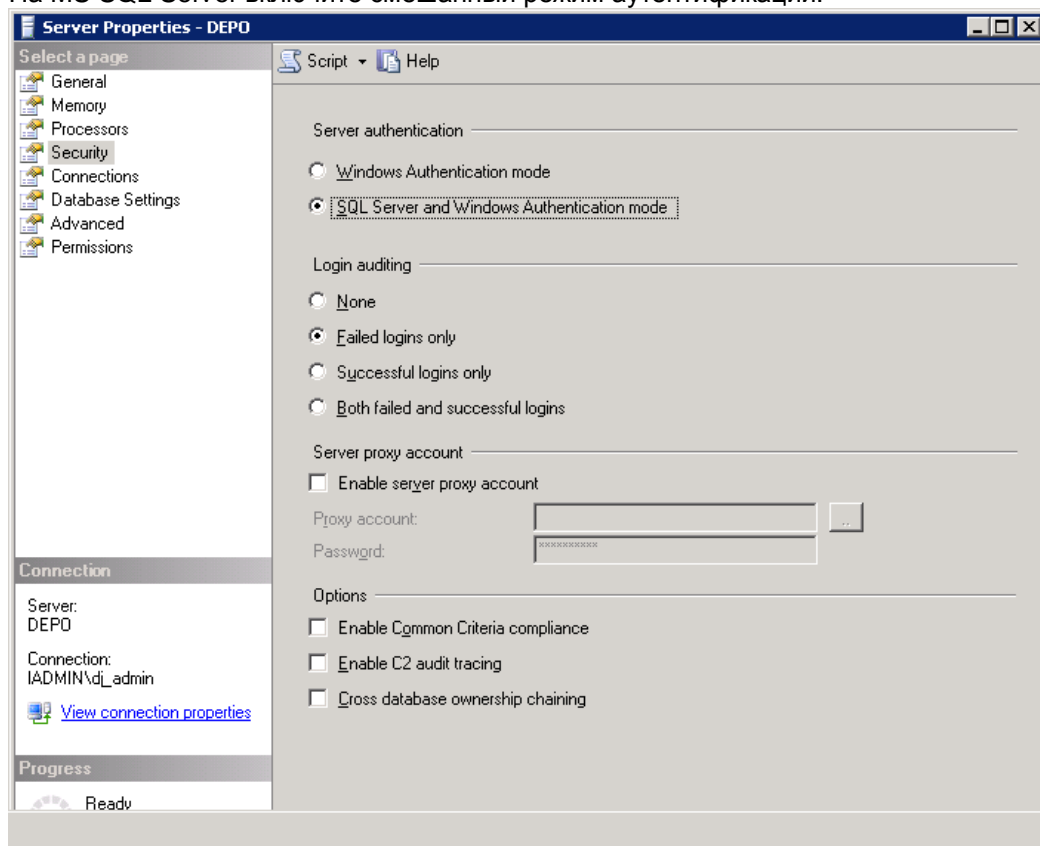
«Интернет Администратор» может использовать в качестве системы управления базой данных Microsoft SQL Server версии 2000 или выше. Данная СУБД рассчитана на базы данных масштаба предприятия и поддерживает базы данных с большим объемом информации.

В Интернет Администратор встроена специальная программа - «Мастер базы данных». С помощью Мастера можно создать новую базу данных на MS SQL Server, и выбрать, какую СУБД использовать в дальнейшем.

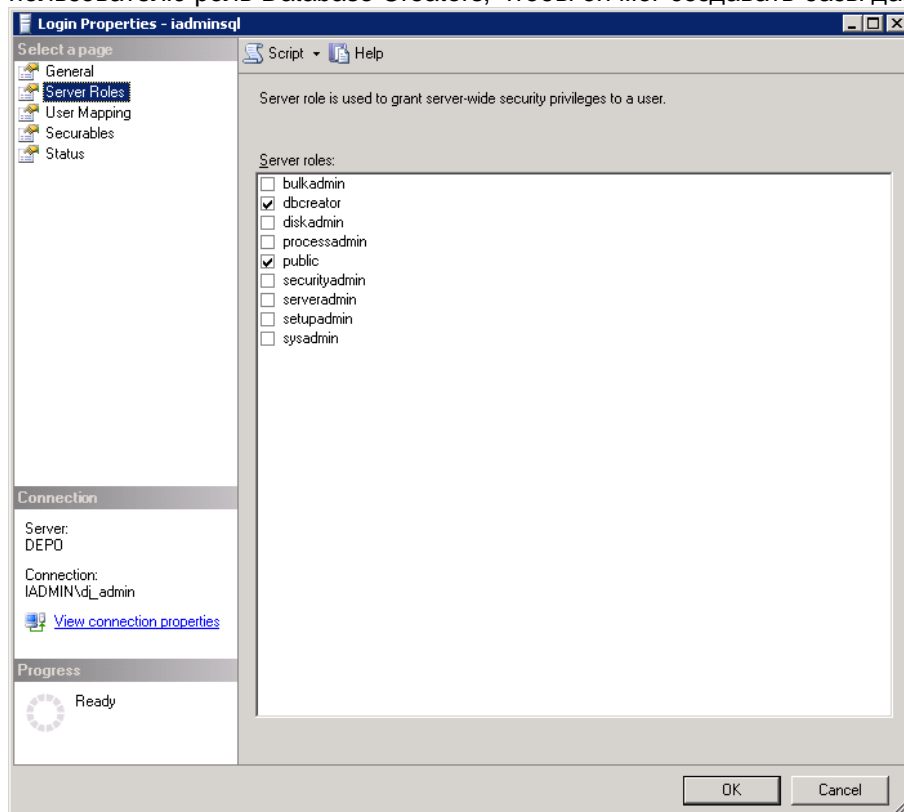


## Создание базы данных на MS SQL Server

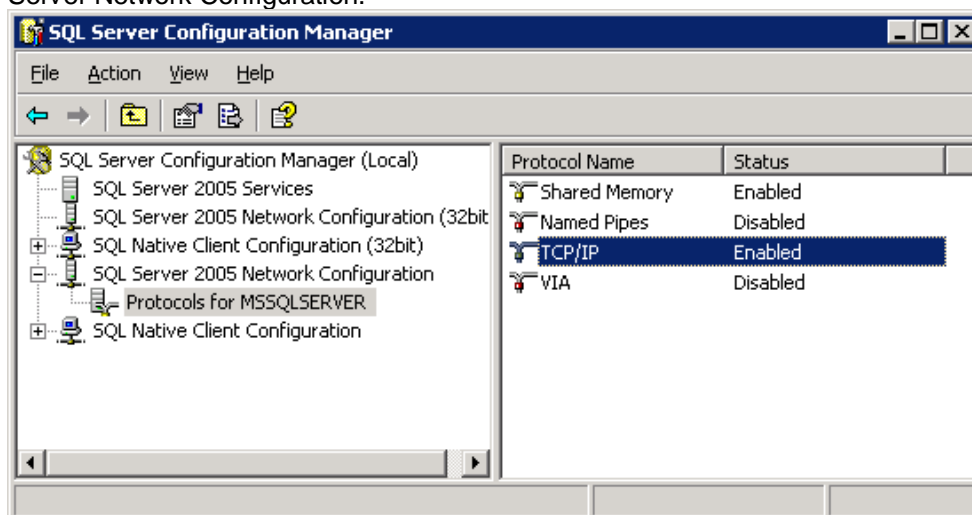
На MS SQL Server включите смешанный режим аутентификации.



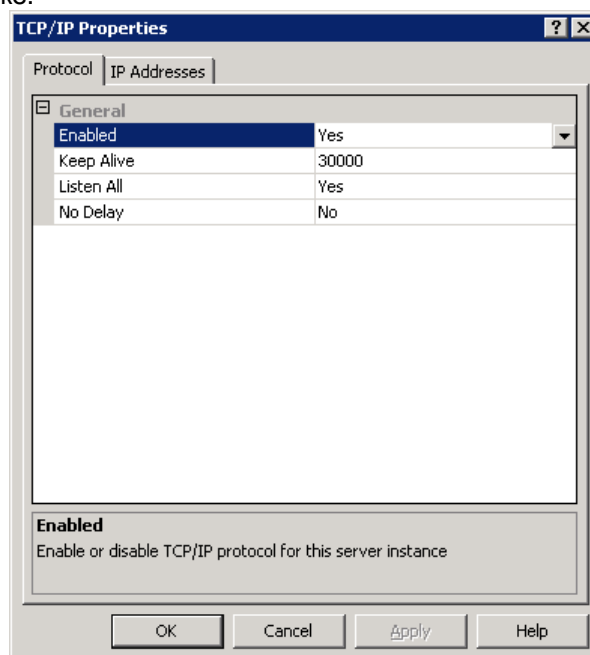
Создайте произвольного пользователя и на вкладке Server Roles включите пользователю роль Database Creators, чтобы он мог создавать базы данных.



Если SQL Server находится на удаленном сервере, то необходимо включить поддержку работы по сети. Запустите утилиту SQL Server Configuration Manager в программной группе SQL сервера, подгруппа Configuration Tools и раскройте SQL Server Network Configuration.



Откройте Свойства TCP/IP и включите его поддержку для удаленных подключений, если они отключены. Также включите TCP/IP на нужных IP адресах в соседней вкладке.



Теперь запустите «Мастер базы данных» и выберите «Создание базы данных MS SQL Server». На следующем экране укажите новое название базы данных, имя экземпляра SQL сервера, имя и пароль созданного выше пользователя. Название базы данных должно быть уникальным на выбранном экземпляре.

Интернет Администратор - Мастер базы данных

Создание базы данных MS SQL Server

Название базы данных: iadminsql

Имя MS SQL сервера: [ ]

Имя пользователя: [ ]

Пароль: [ ]

Проверить связь

Примечание: Пользователь должен иметь роль Database Creator.

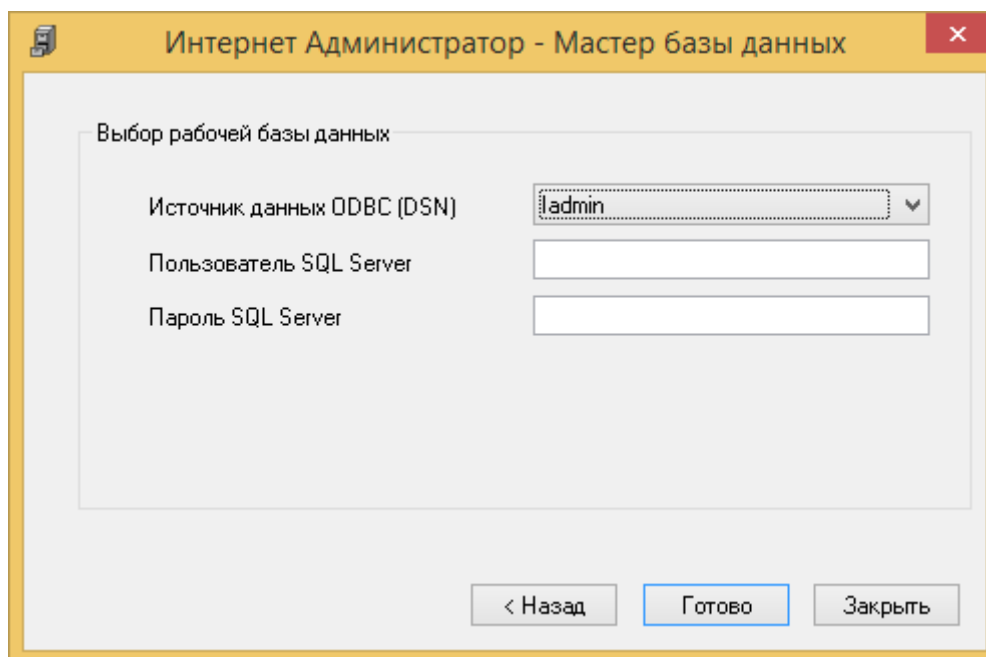
< Назад    Готово    Закреть

При нажатии на кнопку «Готово» мастер осуществит попытку создания базы и сообщит о результате. **Для вступления изменений в силу перезапустите службу IAdmin Server и программу Администратор правил.**



## Выбор СУБД

Для изменения параметров подключения к базе данных в «Мастере базы данных» выберите «Изменение расположения базы данных».



Источник данных для MS SQL Server создается при создании новой базы данных. Если источник ODBC создается вручную, его имя должно обязательно совпадать с названием базы данных. **Для вступления изменений в силу перезапустите службу IAdmin Server и программу Администратор правил.**

### Раздел 8.3. — Резервное копирование

Для сохранности данных, собранных комплексом «Интернет Администратор» в случае сбоя компьютера рекомендуется делать резервное копирование базы данных. Резервное копирование осуществляется средствами MS SQL Server. Для настройки и дополнительной информации обратитесь к документации на MS SQL Server.

## РАЗДЕЛ 9 – РАСПРЕДЕЛЕННЫЕ СЕТИ и КОЛЛЕКТОРЫ

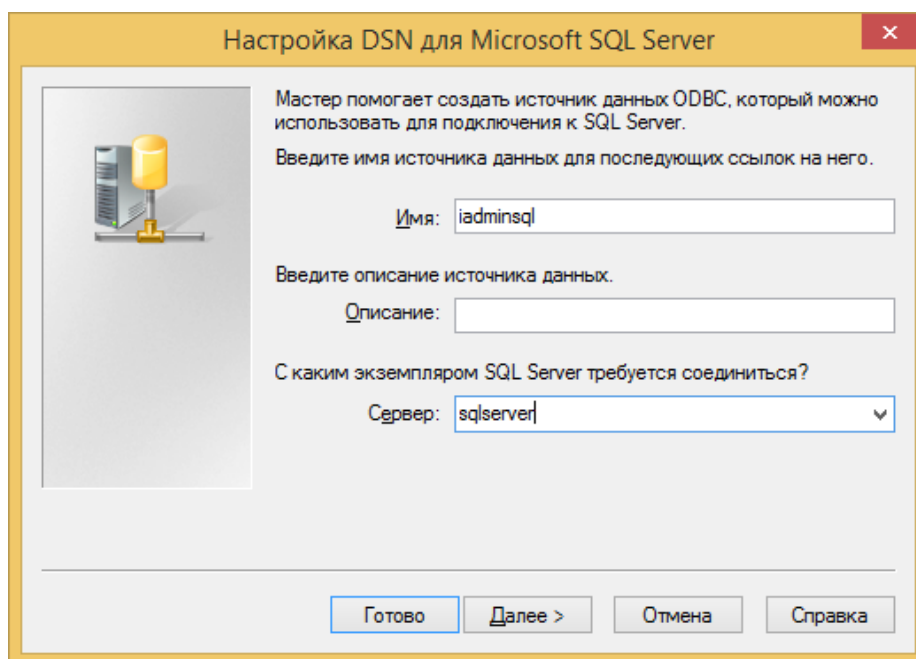
«Интернет Администратор для Сети» включает в себя средства для построения единой схемы мониторинга и управления политикой доступа в Интернет на предприятиях с распределенными сетями. Это обеспечивается путем создания центральной базы данных и установкой копий Интернет Администратора в каждую из контролируемых сетей или на каждый сервер, выполняющий роль шлюза. Под распределенными сетями подразумеваются сети, находящиеся в разных физических сетях, разделенных маршрутизаторами, в разных зданиях или имеющие разные выходы в Интернет.

### Раздел 9.1. — Создание центрального хранилища данных

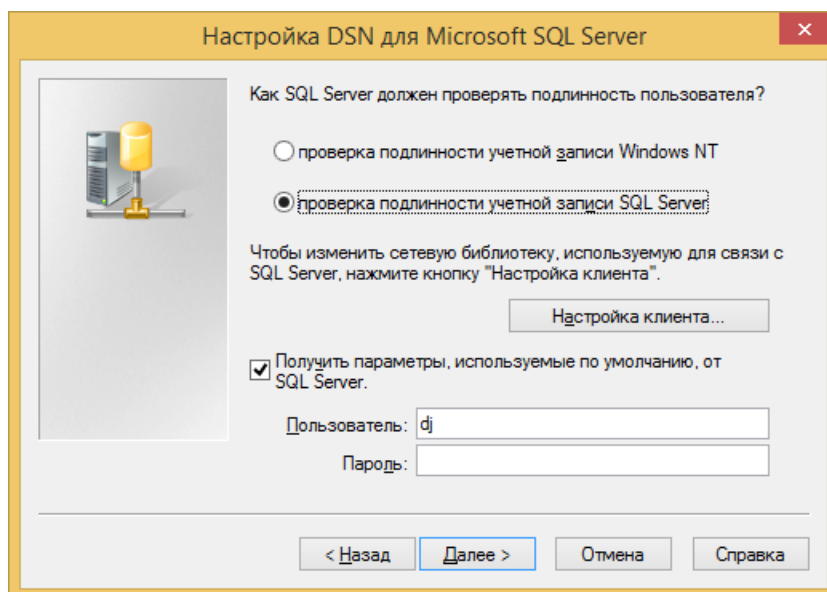
Для создания центрального хранилища необходимо провести первую инсталляцию в центральной сети и перенести базу данных комплекса на Microsoft SQL Server (см. раздел 8). На данной СУБД будет храниться вся информация, настройки и правила доступа для всех остальных коллекторов.

### Раздел 9.2. — Установка дополнительных коллекторов.

Установите «Интернет Администратор» в удаленной сети по обычной схеме, остановите службу Iadmin Server. Для подключения к центральному серверу базы данных будет необходим доступ к MS SQL серверу в центральной сети. Создайте два одинаковых источника данных ODBC для 32 и 64 битных приложений (Администрирование -> Источники данных ODBC (32-разрядная версия) и Источники данных ODBC (64-разрядная версия)) типа MS SQL server.



В качестве имени источника укажите название базы данных на центральном сервере. Если база данных называется Iadmin, то нужно не создать а изменить уже существующие источники Iadmin. В качестве сервера укажите имя MS SQL Server в центральной сети. Установите проверку подлинности пользователя SQL server.



Протестируйте источники данных перед созданием.

После этого, с помощью утилиты «Мастер базы данных», измените расположение базы данных и выберите созданный источник. Задайте имя и пароль, которые были введены при создании базы данных в центральной сети. Запустите службу Iadmin Server. Если служба запустилась без ошибок, то соединение с центральной базой данных установлено успешно.

**Примечание!** В удаленных сетях должна быть разная IP адресация. То есть не должно быть двух компьютеров с одинаковыми IP адресами, IP сети не должны пересекаться. При пересечении IP сетей одному пользователю будет записываться трафик со всех компьютеров других сетей с тем же IP адресом, который установлен на его рабочей станции.

### Раздел 9.3. — Управление и администрирование

После создания единой схемы управлять политикой доступа, а также просматривать статистику и создавать отчеты можно на любом коллекторе из любой сети. Но для нормальной работы с места администрирования необходимо, чтобы была связь со всеми серверами через DCOM по протоколу RPC. Желательно не фильтровать трафик по каналам VPN, так как RPC всегда использует динамические порты. Также необходимо настроить разрешение имен серверов, где установлен «Интернет Администратор». Лучше всего для этого использовать файл hosts (папка \windows\system32\drivers\etc). Задайте там IP адреса удаленных серверов и их имена компьютеров, так, как они называются в действительности.

При осуществлении некоторых действий в административных утилитах, скажем, блокировка пользователя, фиксация изменений в правилах и т.д. происходит связь с каждым коллектором Интернет Администратора. В случае, если такую связь невозможно установить, изменения произойдут только в базе данных, а удаленный коллектор применит их только после перезагрузки на нем службы Iadmin Server.