

## Оценка влияния спам-зомби на операторов широкополосного доступа в Интернет

### Введение

Спам, некогда воспринимавшийся чуть ли ни как простое неудобство, перерос в колоссальную проблему, которая затрагивает и пользователей Интернет, и операторов связи. Массовое распространение вирусов, червей и троянских программы попадает в заголовки новостей, однако спам, можно назвать более коварной угрозой, поскольку он прямо или косвенно затрагивает каждого пользователя сети Интернет. Спам нервирует пользователей, переполняя их электронные почтовые ящики большим количеством ненужных и бесполезных сообщений.

Помимо раздражения и неудобства, спам наносит пользователям и операторам связи реальный ущерб. Махинации с использованием «фишинга» заставляют излишне доверчивых пользователей раскрывать персональную информацию, например, номера кредитных карт или пароли, в результате чего они несут финансовые убытки, теряют время, а так же нарушается неприкосновенность их личной жизни. Спам может выступать переносчиком вирусов, содержащих вредоносный код, например, вирусы, используемые злоумышленниками для запуска распределенных атак типа «отказ в обслуживании» (DDoS). Со стороны оператора связи спам занимает ресурсы каналов передачи данных и перегружает серверы электронной почты, задерживая или блокируя передачу электронных сообщений. Спам оказывает влияние и на репутацию оператора связи, например, если оператор попадает в черный список как источник спама из-за действий его абонентов. Возможны и значительные негативные последствия в маркетинговом аспекте: репутация распространителя спама мешает оператору в борьбе за клиентов на конкурентном рынке услуг широкополосного доступа в Интернет.

### Возможность получить конкурентные преимущества

Хотя большинство пользователей воспринимают распространителей спама как мошенников (по меньшей мере), их гнев обрушивается на оператора связи. Типичный аргумент звучит так: «Мне неважно откуда это приходит, я хочу, чтобы вы это остановили!». По результатам исследований, 74% клиентов полагают, что их оператор связи несет ответственность за устранение проблем, связанных с распространением спама (источник Gartner Group). Несмотря на постоянное усовершенствование систем фильтрации электронной почты и приемов борьбы со спамом, среднестатистический пользователь, находящийся дома или в небольшом офисе, рассчитывает на то, что именно оператор связи обеспечит контроль над электронной почтой и очистит ее от спама. И этих людей никак нельзя назвать пассивным большинством: по данным журнала «PC Magazine», только AOL ежедневно получает 250 тысяч жалоб, связанных со спамом.

При этом спам открывает перед оператором возможность действенно и нетривиально подойти к решению проблемы. Оператор связи, покончивший со спамом, может не только переманить к себе клиентов, но и получить дополнительные доходы от сервисов,

помогающих бороться со спамом. В недавнем исследовательском отчете Gartner Group отмечается что:

- для сокращения объема получаемого спама 36% пользователей готовы поменять Интернет-провайдера;
- ни много ни мало – 24% пользователей готовы платить за услугу фильтрации спама.

### **Группа по борьбе со спамом Antispam Technical Alliance разрабатывает рекомендации для операторов связи**

Интернет-сообщество рассчитывает на то, что проблемы со спамом решат операторы связи. Группа по борьбе со спамом Antispam Technical Alliance разработала технические стандарты и стимулирует совместные усилия сообщества по решению этой проблемы. Исходный набор рекомендаций ("Antispam Technical Alliance Technology and Policy Proposal", версия 1.0 от 22 июня 2004 года) содержит конкретные указания по организации работы операторов связи, например:

- выявление и изоляция в карантинной зоне зараженных компьютеров абонентов, рассылающих спам;
- установка ограничений на исходящий от абонентов трафик электронной почты;
- внедрение соответствующих систем отчетности.

### **Спам как явление**

Спамеры первого поколения шли по самому простому пути: они рассылали тысячи или даже миллионы электронных сообщений с собственных электронных адресов. Операторы связи реагировали на жалобы столь же простым способом – заносили таких абонентов в черный список. Анализируя размеры писем, текста в заголовке и теле сообщений и рассматривая жалобы клиентов, оператор выявлял спамеров и блокировал им доступ в сеть. Эти простые приемы было несложно применять на практике.

Спамеры быстро взяли на вооружение другой прием: использование открытых SMTP-шлюзов (mail relay) и прокси-серверов. Проще говоря, открытый прокси-сервер допускает установку соединений, исходящих от любого сетевого адреса, действуя как слепой посредник при доступе практически к любому другому сетевому адресу. Получатель воспринимает спам как сообщение, исходящее от прокси-сервера. Этим путем достигается эффективная маскировка IP-адреса реального отправителя. Операторы связи отреагировали на этот прием черными списками второго типа. В эти списки попадали открытые прокси-серверы и SMTP-шлюзы, с которых рассылался спам. В ответ на эти черные списки спамеры изобрели еще более изощренный способ атаки – использование вирусов для рассылок спама.

Заражая вирусом незащищенные компьютеры, злоумышленники рекрутируют целую армию ни о чем не подозревающих союзников – пользователей, с компьютеров которых можно запускать рассылки спама. По своим характеристикам такая атака сходна с DDoS-атакой: большое количество атакующих компьютеров делает практически невозможным идентификацию источника атаки или принятие коррективных мер в реальном времени.

### **Зомби: зараженные компьютеры, используемые для рассылок спама**

Использование зомби – это гораздо более изощренный по сравнению с остальными изобретенными на сегодняшний день метод рассылки спама. Современные широкополосные сети особенно подвержены влиянию зомби-компьютеров, поскольку многие пользователи непрерывно подключены к сети.

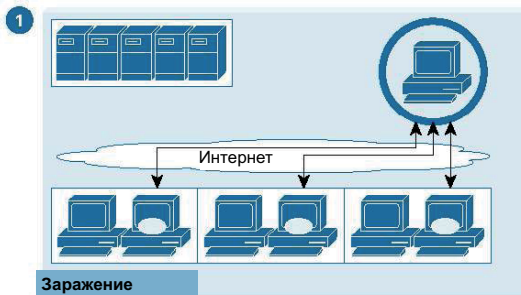
По оценкам отраслевых экспертов, доля зараженных ПК в широкополосных сетях, составляет, по меньшей мере, 1% и может достигать 10% (чтобы лучше понять механизм использования зомби, обратитесь к схеме “Как атакуют зомби” на рис.1).

### Блокирование спама у источника

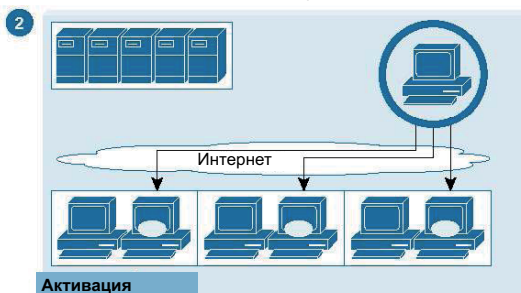
Поскольку спамеры стали активно использовать зараженные компьютеры для обхода существующих механизмов защиты от спама, Интернет-сообщество должно разработать и внедрить новые стратегии борьбы со спамом. Хотя существующие приемы защиты от спама, в частности, черные списки, анализ текста писем и фильтрация, позволяют отфильтровывать и удалять спам, поступающий на почтовые серверы, операторам широкополосного доступа необходимы эффективные решения, чтобы электронные сообщения, генерированные зомби, вообще не покидали сеть оператора. Такой подход сводит на нет значимое преимущество, которые приносят спамерам зараженные компьютеры: спамеры лишаются инструмента распространения.

#### Как атакуют зомби

Вирус попадает на персональный компьютер абонента, например, через вложение в электронной почте или с помощью уязвимости в операционной системе. Когда вирус заражает компьютер, он самостоятельно выходит на связь с ботнет-контроллером и ожидает дальнейших команд.



Злоумышленник инициирует кампанию по рассылке спама. С ботнет-контроллера всем вышедшим на связь зомби-компьютерам посылаются команды рассылать спам, включающая спам-сообщение и список адресов электронной почты, по которым необходимо произвести рассылку.



Затем, каждый зомби-компьютер инициирует массовую рассылку сообщений электронной почты по заданным адресам.

При этом пользователь зараженного ПК может и не догадываться о наличии вируса, рассылающего спам на всех этапах спам-кампании.

После завершения рассылки вирус переходит в неактивный режим, ожидая новых команд от ботнет-контроллера.



Рисунок 1. Как атакуют зомби

Идентификация становится возможной и более эффективной в широкополосной сети, которая выступает плацдармом для действия зомби. Решение, дающее возможность прозрачного мониторинга всего сетевого трафика и эффективной идентификации и блокировки спама, поступающего от зараженных компьютеров, без влияния на быстродействие и доступность сети открыло бы перед Интернет-сообществом новые пути борьбы с этой коварной агрессией.

### **Использование Cisco Service Control для борьбы со спам-зомби: экспертно-аналитический подход**

Наиболее эффективный подход к борьбе с спамом, рассылаемым с зараженных компьютеров: выявить нарушителей, т.е. те ПК, которые посылают спам. После того как зараженные компьютеры выявлены, оператор может поместить их в карантин (отказать в доступе в сеть), чтобы защитить сеть, а также уведомить пользователя о заражении, для того чтобы он мог принять меры по очистке своего компьютера от вирусов.

Каким образом выявляется источник спама? К счастью, хотя зомби и способны скрывать реального злоумышленника, они оставляют отчетливые следы в виде закономерностей поведения сетевого трафика. Их можно выявить с помощью экспертно-аналитических приемов, заложенных в решение Cisco Service Control. Их слабое звено – это количество SMTP-соединений, генерируемых с зараженного компьютера. Масштабные исследования операторов связи - клиентов Cisco - показали, что есть техническая возможность разработать сетевые правила, позволяющие с высокой степенью надежности идентифицировать активные зомби в реальном времени.

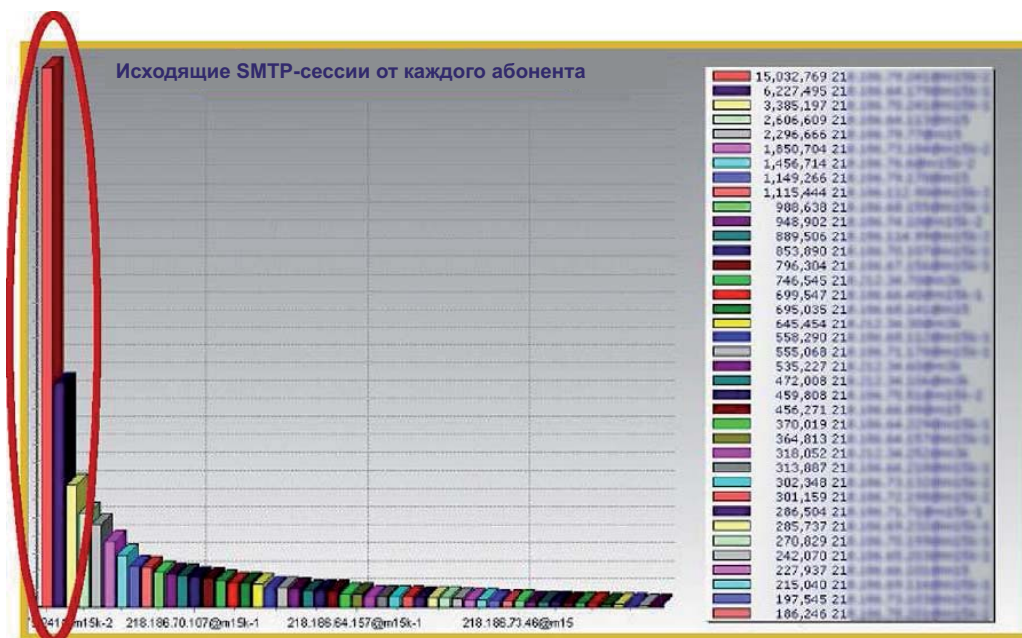
Для выявления источника спама, необходим сетевой элемент, который мог бы выполнять мониторинг сетевого трафика и обладал бы следующими ключевыми возможностями:

- *Глубокий анализ сетевых пакетов.* В решении должна быть заложена возможность глубокого анализа пакетов и классификации SMTP-сессий. С помощью глубокого анализа пакетов можно получить точную информацию принадлежности последовательности пакетов к одной SMTP-сессии, и выявить подозрительные закономерности, присутствующие в сетевом трафике.
- *Анализ сетевых сессий абонентов.* Когда установлено, что определенный поток пакетов относится к SMTP-сессии, необходимо отслеживать совокупное количество таких сессий, исходящих от конкретного абонента. Отслеживая количество SMTP-сессий, можно выявить пользователей, которые генерируют необоснованно большое их количество. Такая закономерность характерна для зомби, т.е. показывает попытку разослать сообщения большому количеству получателей.
- *Классификация потоков электронной почты на основании адреса назначения.* Для разграничения почтового трафика зомби и легитимной электронной почты необходима возможность отслеживать количество целевых почтовых серверов, на которые посылаются сообщения электронной почты в определенный период времени. Это помогает разграничить легитимные действия абонентов (использование собственных почтовых серверов Интернет-провайдера или небольшого количества внешних серверов) и деятельность зомби (использование большого количества внешних серверов).
- *Возможность контролировать трафик электронной почты и HTTP.* Для автоматизации процесса нейтрализации требуется, чтобы решение могло контролировать SMTP-трафик зомби путем установки ограничений или блокировки, а

также за счет использования возможностей переадресации по протоколу HTTP, чтобы информировать пользователей о том, что их компьютер заражен.

- *Ориентация на быстроедействие.* Для поддержания мониторинга и контроля над трафиком приложений, а также для немедленного реагирования на возможный спам, в сетевом элементе должна быть заложена возможность управлять потоками трафика под нагрузкой. Без такой возможности, учитывая растущие объемы трафика операторов связи, ресурсы решения по устранению спама в электронной почте очень скоро окажутся исчерпанными.

Глубокий анализ пакетов на уровне 4-7 модели ISO/OSI и способность контролировать состояние сетевых сессий – это мощный инструмент выявления аномалий в сетевом трафике, генерируемым спам-зомби. Учитывая состояние сессий, решение может отличить, например, тысячу сообщений размером в 1 кбайт, сгенерированных с использованием тысячи отдельных SMTP-сессий, от одной SMTP-сессии, передающей почту размером в 1 Мбайт. Решения, не учитывающие параметры состояния сессий, способны только подсчитать количество пакетов и не могут отличить серию небольших сессий от одной большой сессии. Более того, отслеживая состояние абонентов по множеству попыток входа, решение Cisco Service Control может выявить действия зараженных ПК, распространяющих спам, даже если используется большое количество сеансов подключения к широкополосной сети и различные IP-адреса. Учет параметров сетевых сессий и сеансов подключения абонентов позволяют оператору связи быстро выявить действия по рассылке спама, осуществляемые конкретным абонентом, заблокировать пересылаемую им электронную почту и переадресовать пользователя зараженного ПК на сайт, где содержится уведомление о заражении и инструкции по очистке компьютера от вирусов.



Анализ сессий электронной почты абонентов - данные Cisco Service Control

**Рисунок 2.** О наличии зомби говорит характерная закономерность: необычно большое количество сессий электронной почты исходящих от одного пользователя

## Защита широкополосных сетей от исходящего спама с использованием Cisco Service Control

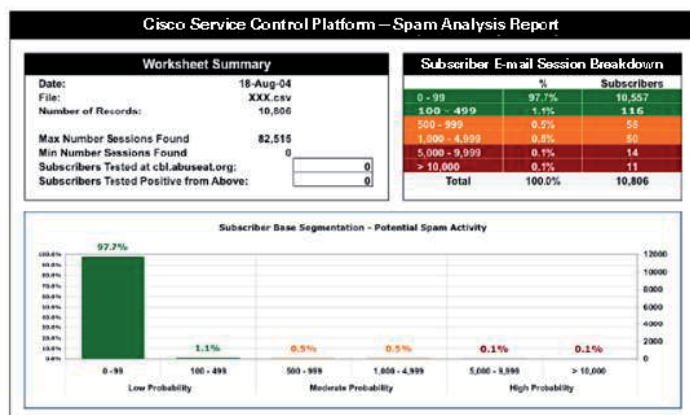
Спамеры переходят на использование более изощренных технологий, и операторы связи должны найти адекватный ответ. Устройства, работающие на уровне 3 модели ISO/OSI, не обладают достаточной интеллектуальной логикой для построения эффективной защиты. Здесь необходимо мощное сетевое устройство, учитывающее состояние сетевых сессий приложений, которое было бы способно выявить атаку, защитить сеть и уведомить пользователя. Технология Cisco Service Control предоставляет в распоряжение операторов связи готовый инструмент, который может существенно сократить в их сетях объем спама, генерируемого зомби, не требуя при этом значительных затрат на капитальную перестройку сетевой инфраструктуры.

Используя технологии глубокого анализа пакетов с учетом состояния соединений, решение Cisco Service Control вооружает операторов мощным инструментом борьбы со спамом. Это решение обладает интеллектуальной логикой и скоростью, необходимыми для выявления спама, защиты широкополосных сетей и уведомления пользователей:

- Решение должно учитывать и параметры сетевого трафика приложений, и параметры сеансов абонентов. Решение Cisco Service Control выполняет мониторинг и анализ трафика более углубленным образом по сравнению с устройствами, работающими на уровне 3, в частности, маршрутизаторами. Помимо этого, комплексная способность учитывать и контролировать состояние сетевых сессий открывает быстрый и эффективный путь к автоматическому выявлению и нейтрализации действий зомби, рассылающих спам.
- Решение должно работать на мульти-гигабитных каналах и обрабатывать большие объемы трафика без создания “узких мест”. Решение Cisco Service Control отвечает и этому требованию. Объединение в кластер нескольких устройств Cisco Service Control позволяет удовлетворить требованиям по высокой пропускной способности.

Подход Cisco Service Control к борьбе спам-зомби заключается в реализации трех этапов:

- *Выявление спам-зомби.* Решение Cisco Service Control может выявлять признаки, характерные для действий спам-зомби, на ранних этапах, во многих случаях уже на основании первых нескольких тысяч сообщений (как правило, это лишь небольшой процент от общего целевого количества спама).
- *Изоляция зараженных ПК в карантинной зоне.* Когда выявлена вредоносная активность в сетевом трафике, требуются немедленные действия для минимизации возможного ущерба. Благодаря быстрому формированию отчетов, администратор сети может вмешаться уже на ранних этапах атаки и ограничить количество спама, проникающего в сеть.
- *Уведомление абонентов.* Пользователи, компьютеры которых подверглись заражению вирусом, все-таки являются жертвами, а не злоумышленниками. Поэтому решение, должно не только изолировать зараженные ПК, но и оперативно уведомлять пользователей, чтобы у них была возможность принять меры по очистке ПК от вирусов. Такое сообщение наглядно демонстрирует качество предоставляемого сервиса, причем оператор связи получает возможность увеличить объемы продаж услуг безопасности абонентам, предлагая им самый высокий уровень сервиса.



### Следы, оставленные спам-зомби

Компания Cisco, работая совместно с рядом операторов связи, выявила ряд четких закономерностей, говорящих об активности спам-зомби на компьютерах абонентов. В ходе мониторинга на предмет проверки данных закономерностей совместно с одним оператором связи, были получены следующие результаты:

- 1% абонентов ШПД инициировали более 1000 SMTP-сессий за заданный промежуток времени;
- 0,1% абонентов ШПД инициировали более 10 000 SMTP-сеансов за тот же промежуток времени.

Затем, для подтверждения факта рассылки спама было выполнено сравнения списка IP-адресов данных абонентов с рядом публичных "черных списков" спамеров и баз репутации IP-адресов отправителей электронной почты. Большинство из тех, кто попал в группу "Более 1000" и практически все представители группы "Более 10 000" были упомянуты как спамеры.

**Рисунок 3.** Практический пример – значение решения Cisco по контролю над распространением спама. Типовое сообщение о анализе спама.

### Преимущества широкополосных сетей свободных от спама

Операторы связи более или менее успешно борются со спамом уже на протяжении многих лет. Хотя появление зомби можно рассматривать лишь как очередную из многих проблем в этой напряженно работающей отрасли, построение эффективной защиты приносит ощутимые преимущества:

- *Возможность получить конкурентные преимущества.* Когда клиентам предлагают на выбор самые разные услуги, возрастает важность дифференциации предлагаемых продуктов. Превентивные меры по сокращению спама – один из способов, с помощью которых операторы связи могут занять уникальную и прочную позицию, выделив себя на фоне конкурентов.
- *Защита от занесения в черные списки.* Если большое количество клиентов оператора связи заражены и вовлечены в рассылки спама, другие операторы связи могут отреагировать на это, занеся в черный список весь диапазон IP-адресов данного оператора, т.е. фактически не позволяя всем законопослушным пользователям отправлять электронную почту. Перебои в работе могут подорвать доверие пользователей к оператору и привести к уходу клиентов.
- *Повышение лояльности клиентов.* Если оператор связи предоставляет пользователям, пострадавшим от заражения вирусами, оперативные уведомления, онлайн-помощь и превентивную поддержку, это, неизменно, повысит уровень их лояльности.
- *Возможности для дополнительных продаж.* Процесс уведомления пользователей также открывает возможность предложить им услуги и продукты, связанные с обеспечением безопасности, в частности, антивирусную защиту и контроль доступа к определенным web-сайтам (услуга "родительский контроль").
- *Экономия вычислительных ресурсов и полосы пропускания.* По мере того как сокращается объем спама в сети, пользователям становятся доступны дополнительные ресурсы полосы пропускания, и при этом не требуется никаких капитальных затрат. Это преимущество заложено только в тех решениях, которые останавливают спам в самом источнике. Фильтры спама, действующие на компьютерах пользователей, могут сократить количество спама, которое видит пользователь, но практически не освобождают полосу пропускания.

## **Решение Cisco Service Control предлагает операторам связи не только контроль над спамом**

Помимо мощных механизмов, таких как блокирование спама, Cisco Service Control предлагает операторам связи широкие возможности по управлению трафиком приложений абонентов. Это оптимизация полосы пропускания с учетом типа и приоритета приложений, сокращение расходов за счет повышения эффективности работы сети. Cisco Service Control представляет собой специализированное программно-аппаратное решение, выполняющее мониторинг и классификацию трафика абонентов в режиме реального времени. Cisco Service Control – это комплексное решение, которое помогает операторам широкополосных сетей идентифицировать абонентов, классифицировать трафик приложений, устанавливать ограничения по использованию абонентами тех или иных приложений, учитывать объемы и начислять платежи за любые IP-сервисы, которые используют ресурсы сети оператора связи.

Основные возможности, заложенные в решении Cisco Service Control:

- Решение Cisco Service Control дает реальную возможность надежной и точной классификации трафика по приложениям и по абонентам.
- В решении заложены функции программирования, благодаря которым его можно адаптировать и расширить, учитывая новые сетевые угрозы.
- Все операции классификации выполняются в реальном времени. Это открывает уникальную возможность поддерживать гигабитные скорости в сетях операторов связи.
- Для развертывания интеллектуального и прозрачного сетевого решения в существующей сети требуется лишь минимальная реконфигурация сети. Благодаря этому, операторы могут свести к минимуму дополнительные инвестиции и окупить вложенные в решение средства, предлагая его большому количеству клиентов.

Используя технологию Cisco Service Control, операторы широкополосного доступа получают возможность более эффективно управлять сетевыми ресурсами, повысить быстродействие сетей и снизить операционные затраты, и, кроме этого, разрабатывать новые эффективные тарифные планы, и услуги для абонентов.

**Дополнительные сведения**

Cisco Series Service Control Engine:

<http://www.cisco.com/en/US/products/ps6151/index.html>

Personalized Subscriber Management Brochure:

[http://www.cisco.com/en/US/netsol/ns715/networking\\_solutions\\_white\\_paper0900aecd80581403.shtml](http://www.cisco.com/en/US/netsol/ns715/networking_solutions_white_paper0900aecd80581403.shtml)

Cisco Secure Broadband Brochure:

[http://www.cisco.com/en/US/netsol/ns734/networking\\_solutions\\_white\\_paper0900aecd806153ee.shtml](http://www.cisco.com/en/US/netsol/ns734/networking_solutions_white_paper0900aecd806153ee.shtml)



Cisco  
Россия, 115054, Москва,  
бизнес-центр  
«Риверсайд Тауерс»  
Космодамианская наб., 52,  
стр. 1, этаж 4  
Тел.: +7 (495) 961-14-10  
Факс: +7 (495) 961-14-60  
[www.cisco.ru](http://www.cisco.ru)  
[www.cisco.com](http://www.cisco.com)

Cisco  
Россия, 191186,  
Санкт-Петербург,  
бизнес-центр «Регус»  
Невский проспект, 25,  
этаж 2, офис 30  
Тел.: +7 (812) 346-77-17  
Факс: +7 (812) 346-78-00  
[www.cisco.ru](http://www.cisco.ru)  
[www.cisco.com](http://www.cisco.com)

Cisco  
Казахстан, 480099,  
Алматы,  
бизнес-центр «Самал 2»  
Ул. О. Жолдасбекова, 97,  
блок А2, этаж 14  
Тел.: +7 (327) 244-21-01  
Факс: +7 (327) 258-46-60  
[www.cisco.ru](http://www.cisco.ru)  
[www.cisco.com](http://www.cisco.com)

Cisco  
Украина, 03038, Киев,  
бизнес-центр  
«Горизонт Парк»  
(Horizon Park)  
Ул. Николая Гринченко, 4В  
Тел.: +38 (044) 391-36-00  
Факс: +38 (044) 391-36-01  
[www.cisco.ua](http://www.cisco.ua)  
[www.cisco.com](http://www.cisco.com)

Cisco  
Азербайджан,  
AZ 1065, Баку,  
бизнес-центр «Карат»  
Ул. М. Мухтарова, 201,  
этаж 2  
Тел.: +994 (50) 250-99-94  
Факс: +994 (12) 437-48-20  
[www.cisco.ru](http://www.cisco.ru)  
[www.cisco.com](http://www.cisco.com)

Cisco  
Узбекистан, 100000,  
Ташкент, бизнес-центр  
«Иконель»  
Ул. Пушкина, 75,  
офис 605.  
Тел.: +998 (71) 140-44-60  
Факс: +998 (71) 140-44-65  
[www.cisco.ru](http://www.cisco.ru)  
[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2007 Cisco Systems Inc. All rights reserved. Printed in Russia. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)