

ПРОЕКТ КОМПАНИИ

RUcenter
www.nic.ru

A large, stylized graphic of orange and red flames rising from behind the title.A white hand cursor icon pointing upwards towards the word 'ДОМЕННЫЕ'.

ДОМЕННЫЕ ВОЙНЫ

На прилагаемом
КОМПАКТ-ДИСКЕ —
журнал
«Доменные имена»,
таблицы
«Виды доменов»,
другие полезные
материалы



 **ПИТЕР**

А. Венедюхин



ВОЙНЫ

А. Венедюхин



Москва • Санкт-Петербург • Нижний Новгород • Воронеж
Ростов-на-Дону • Екатеринбург • Самара • Новосибирск
Киев • Харьков • Минск

2009

ББК 32.988.02
УДК 004.738.5
В29

Венедюхин А. А.

В29 Доменные войны (+CD). — СПб.: Питер, 2009. — 224 с.: ил.

ISBN 978-5-388-00728-5

Купля и продажа доменов стала в последние годы напоминать золотую лихорадку: каждый торопится застолбить лакомый кусочек, чтобы заработать на нем в будущем. Что и неудивительно, если учесть, за какие астрономические суммы продаются домены вроде sex.com. Книга подробно рассказывает о ключевом элементе Интернета — системе доменных имен. Большое внимание уделено доменному рынку, в том числе вторичному рынку доменных имен, а также истории и перспективам развития доменной системы адресации. На страницах книги читатель найдет сведения о том, как работают домены, кто и как ими управляет, как домены связаны с информационной безопасностью, какие правовые коллизии возникают вокруг них и что ждет доменные имена в ближайшем будущем.

Для широкого круга читателей.

На прилагаемом компакт-диске — журнал «Доменные имена» и другие полезные материалы.

ББК 32.988.02
УДК 004.738.5

Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

Информация, содержащаяся в данной книге, получена из источников, рассматриваемых издательством как надежные. Тем не менее, имея в виду возможные человеческие или технические ошибки, издательство не может гарантировать абсолютную точность и полноту приводимых сведений и не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-5-388-00728-5

© ООО «Питер Пресс», 2009

Оглавление

| | |
|---|----|
| От автора | 6 |
| Об авторе | 7 |
| От издательства | 8 |
| Предисловие. Домены древности и наших дней | 9 |
| Глава 1. Числа и Сеть сетей | 11 |
| Глава 2. Обнаружение адреса | 18 |
| Глава 3. Администраторы и реестры | 24 |
| Права и уровни доменов | 25 |
| Рассказы о владельце | 34 |
| Тысячи доменов | 40 |
| Глава 4. Виртуальная география, или Домен SU | 43 |
| Глава 5. Оплот Рунета — домен RU | 49 |
| Глава 6. Страны, коды и домены | 61 |
| Лингвистические фокусы | 64 |
| Трудности управления | 70 |
| Ликвидация | 74 |
| Глава 7. В первых доменных рядах | 78 |
| Живые древности | 79 |
| Новые времена и широкий брендинг | 82 |
| Первые дополнения | 88 |
| Виртуальность верхнего уровня | 92 |
| Нашли спонсора | 97 |
| Процедурный вопрос | 98 |

| | |
|---|-----|
| Глава 8. Национальные буквы | 101 |
| Технические трудности | 104 |
| На высшем уровне | 109 |
| Раздвоение личности | 110 |
| RUcские домены | 115 |
| Глава 9. Колесо Сансары, или Жизнь и смерть доменов | 124 |
| Рождение | 126 |
| Жизнь | 130 |
| Смерть | 133 |
| Зомби? Нет — перерождение | 136 |
| Циклы .ru | 136 |
| Глава 10. Вторичный рынок | 139 |
| Механизмы | 141 |
| Люди | 143 |
| Инструменты | 145 |
| Доходы | 156 |
| Глава 11. Безопасность и домены | 163 |
| Безопасное администрирование | 166 |
| Уверенный доступ | 173 |
| Достоверность: а туда ли я попал? | 175 |
| Заверено подписью | 180 |
| Глава 12. Право на домен | 195 |
| Отдай мой домен | 196 |
| Отвечать не желаю | 199 |

| | |
|--|-----|
| Заключение | 202 |
| Приложение 1. Перечень зарезервированных доменных имен в зоне .ru | 205 |
| Домены общего пользования | 205 |
| Домены, используемые для государственных нужд | 210 |
| Домены, зарезервированные в технических целях | 210 |
| Приложение 2. Национальные домены верхнего уровня | 211 |
| Приложение 3. Общие домены верхнего уровня (gTLDs) | 216 |
| Домены общего пользования | 216 |
| Специальные домены общего пользования | 216 |
| Домены ограниченного пользования | 216 |
| Специальные спонсируемые домены ограниченного пользования (Sponsored Top-Level Domains, sTLDs) | 217 |
| Приложение 4. Статистика доменов | 218 |
| Список литературы | 222 |

От автора

Эта книга рассказывает о настоящем и будущем одного из ключевых элементов Интернета — о доменных именах, составляющих для массового пользователя Глобальной сети основу навигации по сайтам и страницам. Доменные имена для Интернета придумали в начале 1980-х годов. С тех пор значение доменов для развития Сети неизменно растет и оказывает все большее влияние на Интернет в целом.

В книге вы найдете доступное описание принципов функционирования доменной системы имен (DNS), рассказ об истории доменов, о причинах их появления, о том, кто, почему и как управляет глобальной системой адресации, о том, что происходит на доменном рынке России сейчас и что ожидает его в дальнейшем.

Книга не появилась бы без поддержки компании RU-CENTER — ведущего российского регистратора доменов. Автор выражает признательность генеральному директору RU-CENTER А. Д. Лесникову за интерес к книге. Автор также благодарит А. А. Воробьева, директора Департамента по связям с общественностью компании RU-CENTER, и П. Б. Храмцова, ведущего аналитика компании RU-CENTER, за весьма ценные замечания по содержанию и структуре книги и за те плодотворные дискуссии, из которых, собственно, эта книга и возникла.

*Александр Венедюхин,
лето 2008,
Москва*

Об авторе

Александр Венедюхин — известный аналитик в области интернет-технологий, доменного рынка, систем адресации сетей передачи данных и специальных средств связи; автор научно-популярных публикаций; автор научно-технического блога <http://dxdt.ru/>.

От издательства

Ваши замечания, предложения и вопросы отправляйте по адресу электронной почты voevodin@msk.piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На сайте издательства <http://www.piter.com> вы найдете подробную информацию о наших книгах.

Предисловие. Домены древности и наших дней

В стародавние времена, когда люди еще не знали даже текстового Интернета, доменами назывались огромные королевские владения. Плодородные пахотные земли, реки, полные рыбы, деревни с работающими крестьянами, леса с тучными круторогими оленями — все это несметное богатство составляло королевский домен, переходивший по наследству.

Домен приносил доход, позволяя существовать королевскому двору. И именно из домена монарх жаловал земли и ресурсы своим вассалам, поддерживавшим его власть на территории государства силой оружия и убеждения. За домены шли кровопролитнейшие многолетние войны между королевствами и аристократическими домами. Эти войны и составили всемирную историю.

С тех пор прошли столетия. Появился Интернет. Времена изменились, и королей в реальном мире почти не осталось. Зато о доменах теперь можно услышать гораздо чаще, чем о королях.



В XXI веке доменом именуют владения в адресном пространстве Интернета. Реальные земли сменились виртуальными. Но домены Интернета, как и прежние, приносят доход своим хозяевам. «Короли» выделяют из доменов наделы «вассалам». «Вассалы» утверждают в домене свою власть и поддерживают власть «короля». За домены идут многолетние судебные споры. За контроль на доменами борются государства и транснациональные корпорации. Домены отбирают силой, уводят хитростью, покупают за астрономические суммы. Передел ресурсов нового виртуального мира еще только вступает в период расцвета.

С одной стороны, домен в Интернете предстает строкой из алфавитно-цифровых символов, обозначающей некоторый участок адресного пространства Всемирной сети. Например, .net, nic.ru, www.example.com, whois.rnp.net — это домены, или, как часто говорят, доменные имена. С другой стороны, за символами скрывается хитроумный клубок технологий, делающий использование доменов возможным для всего Интернета. А обе стороны создают новый объект, объединяющий виртуальный и реальный миры, — объект, ставший первопричиной изменений в законах больших государств и перевернувший жизнь многих и многих людей. Эта книга повествует о жизни доменов и жизни вокруг них.

Глава 1

Числа и Сеть сетей

Интернет создали в 1970-х годах в США на случай глобальной ядерной войны. «Сценаристы» Пентагона предсказывали очень неприятный расклад: после массированного ядерного удара по США инфраструктура систем связи будет разрушена и уцелеет лишь несколько командных центров-бункеров, разбросанных по огромной территории. Этим центрам нужно будет установить связь между своими компьютерными сетями, используя остатки инфраструктуры.

Невозможно заранее предсказать, какие кабельные и радиорелейные линии связи сохраняют работоспособность и какие пути окажутся доступными для доставки данных из одного командного пункта в другой. Более того, нельзя предвидеть, какие командные центры уцелеют после ядерного удара. Все это усложняло задачу, решение которой в итоге дало миру Интернет.

Другими словами, Интернет придумали как саморегулирующуюся сеть компьютерных сетей — сумму телекоммуникационных технологий, призванных обеспечивать надежность межсетевого взаимодействия в масштабе стран и огромных территорий.

Древний Интернет... Да, именно древний. Это вполне допустимый термин: по меркам суперскоростного прогресса в сфере информационных технологий Интернет действительно древнее явление. Итак, древний Интернет в плане адресации был числовым, потому что его придумали специалисты в области компьютерных технологий, а, как известно, компьютеры очень любят разнообразные числа и не любят слова и естественные языки. Более того, именно использование правильного числового представления позволило создать саморегулирующуюся сеть передачи данных. Числами обозначались адреса подключенных к Интернету компьютеров. С помощью преобразования чисел компьютеры находили пути доставки данных друг другу внутри Интернета.



В основе функционирования современного Интернета, конечно, также лежат числа. Однако современному массовому пользователю они не видны и скорее напоминают некий реликт, тайный артефакт, направляющий глубинные процессы внутри Глобальной сети.

КСТАТИ



Важно понимать, что все межкомпьютерные процедуры по обмену данными реализуются исключительно в числовом виде и могут быть сведены к математическим операциям по «превращению» одних чисел в другие и по установлению сравнительных отношений между числами (больше, меньше, равно). Когда речь идет о компьютерной технике, то буквенные обозначения всегда появляются лишь для удобства работающих с компьютерами людей. Но буквенные обозначения **рано или поздно появляются обязательно**.

Каждый компьютер, подключенный к Интернету, идентифицируется специальным адресом — так называемым IP-адресом. Проще говоря, IP-адрес позволяет отличить один узел от другого.

IP-адреса, конечно, задаются в цифровой форме — в современной версии они состоят из 32 бит. IP-адрес можно записать с помощью нескольких чисел в десятичной системе счисления. Например, 192.168.35.101 или 10.10.101.123. IP-адреса компьютеров соответствуют протоколу IP, являющемуся неотъемлемой частью группы протоколов TCP/IP. В свою очередь, TCP/IP — один из ключевых элементов, обеспечивающих передачу данных между сетевыми узлами Интернета.

Протоколы обмена данными — это некоторые стандарты, определяющие, каким образом компьютеры должны воспринимать и преобразовывать числа, представляющие собой передаваемые данные. Например, в определении протокола описано, какие части принятого (или переданного) пакета данных представляют собой служебную информацию, а какие — собственно полезные данные. Для успешного обмена данными компьютеры должны использовать совместимые протоколы, а если упростить ситуацию, то можно сказать, что компьютеры должны использовать один и тот же протокол.

Протокол IP, входящий в состав группы TCP/IP, определяет адресацию сетевых узлов в Интернете и задает правила доставки пакетов данных от узла к узлу. При этом на своем пути пакеты данных могут фрагментироваться (то есть разбиваться на части) и собираться вновь в единое целое.

Общие принципы, на которых строится процесс доставки данных в Интернете, можно представить с помощью такого примера. Предположим, что из одного города в другой перемещают крупный машиностроительный завод. Перевезти завод целиком невозможно: нет такого вида транспорта. Поэтому завод сперва «размонтируют», разбирают на составные элементы. Элементы перевозят к новому месту, где из них собирают завод.

При этом элементы завода можно перевозить самыми разными видами транспорта. Например, мебель из столовой отправляется на грузовике. Небольшие металлообрабатывающие станки — железнодорожным транспортом, потому что в грузовики они не

влезают. А для перевозки огромного парового пресса потребуются грузовое судно речного флота, так как для железной дороги этот пресс — негабаритный груз. Впрочем, если к месту нового расположения завода грузовое судно не может добраться, то для доставки пресса придется использовать другой вид транспорта.

Элементы завода прибывают к месту сборки в разном порядке, так как у различных видов транспорта разная скорость. При этом завод нужно собрать правильно.

Обмен данными в Интернете по протоколам TCP/IP происходит похожим образом. Только вместо различных видов транспорта здесь используются разные каналы связи (доступные в данный момент времени), и сборку-разборку пакетов данных осуществляет не бригада монтажников, а компьютерная программа, реализующая протокол обмена данными. Выбор путей доставки данных между двумя узлами происходит по весьма сложным алгоритмам, учитывающим множество факторов, среди которых, например, загруженность каналов связи на заданном направлении, стоимость доставки пакета данных.

Числа, составляющие IP-адрес, определяют не только узел Интернета, но и сеть, к которой принадлежит этот узел, ведь Интернет — это сеть сетей.

Впрочем, с увеличением числа пользователей компьютерных сетей выяснилось, что числа привычны лишь небольшой части пользователей. Поэтому неудивительно, что еще в начале 80-х годов XX века возникли трудности с практическим использованием чисел, определяющих адреса в Интернете.

Первопричиной прихода буквенных, точнее, алфавитно-цифровых обозначений в систему адресации Интернета стала электронная почта. Оказалось, что людям гораздо проще было бы представлять адреса электронной почты в виде, сходном с адресами обычной почты. Понятно, что удобство записи и запоминания адресов способствует росту эффективности использования

электронной почты. Поэтому на смену сложным комбинациям чисел пришли адреса вида alex.ivanov@test.ru.

Конечно, системы, преобразовывающие числовые адреса в символьные строки, в компьютерных сетях были известны и ранее, до возникновения электронной почты. Более того, некоторые из этих систем использовались даже до появления TCP/IP. Тем не менее именно межсетевое распространение электронной почты подтолкнуло инженеров к идее введения общей системы символьной адресации в Интернете. Так в 1983 году появилась система доменных имен Интернета — **DNS (Domain Name System)**.

DNS представляет собой сложный распределенный технологический механизм, позволяющий сопоставить символьному имени домена один или несколько числовых IP-адресов, определяющих соответствующий узел Интернета. Например, test.ru = 192.168.17.101, то есть доменному имени test.ru соответствует адрес 192.168.17.101.

Домены для Интернета придумал Пол Мокапетрис (Paul Mockapetris), ученый из США. Именно он разработал основополагающие для DNS документы — RFC 882 и RFC 883.

КСТАТИ



RFC (Request for Comments) — достаточно свободная форма определения тех или иных стандартов и протоколов работы Интернета, сложившаяся в результате исторического развития интернет-сообщества. Большая часть документов RFC, касающихся Интернета, — это описания новых интернет-технологий, добровольно принимаемые ко вниманию и исполнению всеми заинтересованными разработчиками.

В современном Интернете документы RFC 882 и RFC 883 (их тексты опубликованы на специальном сайте: <http://tools.ietf.org/html/rfc882> и <http://tools.ietf.org/html/rfc883>) не действуют — их заменили более новые версии RFC. Однако по фундаментальным принципам работы современная DNS Глобальной сети не отличается от системы, предложенной четверть века назад.

В наше время Интернет обычно ассоциируется с веб-сайтами. Большинство новых пользователей вообще не слышали о других технологиях Интернета, для них понятия веб и Интернет эквивалентны. Но если старые технологии типа Gopher давно умерщвлены всемогущим вебом, то DNS только окрепла, ведь именно символьные имена позволяют вебу виртуализировать понятия реального мира, отражая их в именах доменов.

Современные пользователи Интернета давно привыкли к символьным именам. Подавляющему большинству даже в голову не придет набирать в адресной строке браузера загадочную цепочку чисел вместо понятного <http://nic.ru/>. Текстовые имена проще воспринимаются в рекламе. Адреса сайтов, заданные в виде доменных имен, могут привязываться не только к названию бренда (что необходимо для корпоративных сайтов), но и к той отрасли, к тому сектору рынка, с которым связан сайт. Примерами подобных говорящих имен могут быть и auto.ru, и gramota.ru.

То есть без символьного именования сайтов Интернета никакого интернет-бума быть не могло: ни первого, ни второго. Скорее всего, после очередного «схлопывания инвестиционного пузыря» (а оно неминуемо наступит) в выигрыше останутся держатели доменного пространства как единственной технологии, позволяющей через языковые конструкции мертвым узлом привязать виртуальный мир к реальному.

Глава 2

Обнаружение адреса

DNS преобразует строки символов в IP-адреса. Неспециалистам, оперирующим «банальной эрудицией», этот процесс часто кажется простым. Действительно, возьмите таблицу соответствий «домен — адрес» и работайте по ней — предлагают они. Первые системы прото-DNS так и были устроены. Но в масштабах Глобальной сети это простое решение вполне предсказуемо оказывается неверным.

Например, изменяется соответствие IP-адресов и имен доменов. Для этого есть целый ряд причин. Скажем, домен может сменить владельца, и новый администратор захочет настроить соответствие имен и адресов таким образом, чтобы домен указывал на его сетевой узел, а не на узел старого владельца домена. В маленькой локальной сети из десяти компьютеров, содержащей два собственных домена, наверное, нет проблем с тем, чтобы разослать измененную таблицу соответствия всем десяти компьютерам. Но когда речь идет о сотнях миллионов доменов, помноженных на сотни миллионов компьютеров, разбросанных по всему земному шару, идея с рассылкой общей таблицы имен доменов оказывается, мягко говоря, абсурдной. А ведь нужно учитывать постоянный бурный рост Интернета. Так что реально работающая DNS устроена не просто.

Можно сказать, что IP-адресация формирует из множества узлов Интернета одноуровневую структуру. Узлы в ней соединяют различным образом проложенные линии связи.

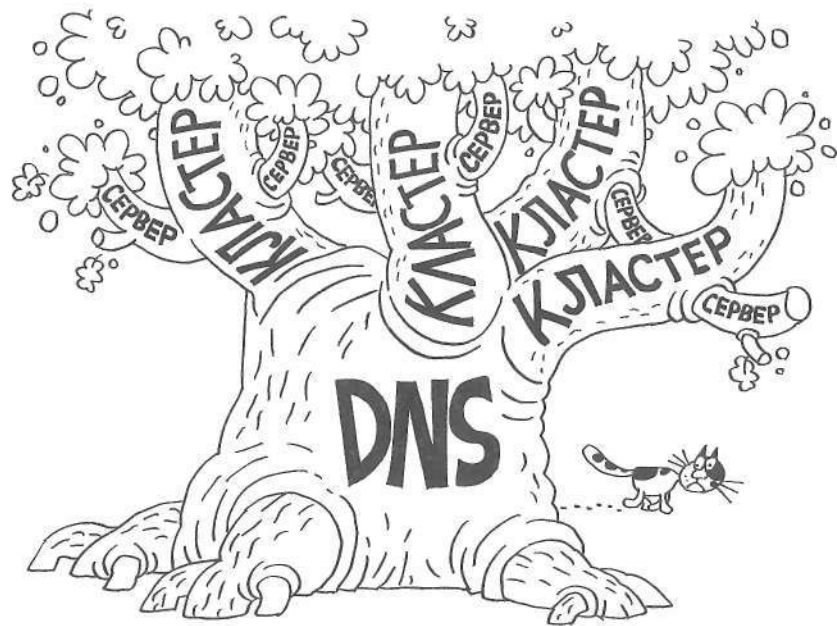
КСТАТИ



По-научному упомянутая плоская структура Интернета со связями между узлами называется графом. А методы успешной и эффективной передачи данных между узлами глобальной Сети помогают разработать в том числе и такую математическую дисциплину, как теория графов. Графы в качестве математического понятия появились задолго до возникновения Интернета — они служили удобным инструментом для исследования сетей электроснабжения.

DNS представляет собой иерархическую древовидную структуру, разбивающую одноуровневое множество узлов (или серверов) Интернета на «отдельные районы» — кластеры. Каждый такой кластер может состоять из многих тысяч серверов или включать в себя только один сервер. Кластеры могут пересекаться, то есть один и тот же узел-сервер может входить в несколько кластеров.

Несложно догадаться, что доменом является узел древовидной структуры DNS. В свою очередь, те серверы Интернета, которые попали в соответствующий узлу кластер, оказываются внутри данного домена. В древовидной структуре DNS каждому узлу дерева соответствует один кластер узлов Интернета. Можно сказать, что дерево DNS как бы добавляет адресной системе Интернета третье измерение, ведь в иерархии доменных имен кластеры вкладываются друг в друга, образуя несколько уровней.



Деление дерева DNS по уровням (первый, второй, третий и т. д.) — важнейшая особенность отношений, возникающих вокруг доме-

нов. DNS, как и всякое дерево, начинается с единственного корневого домена (нулевой уровень). Правда, современная реализация DNS позволяет не указывать корневой домен в адресной строке. Благодаря этому о существовании корневого домена сейчас помнят только специалисты.



КСТАТИ

Адресная строка с указанием корневого домена выглядит, например, так: `site.test.ru`. — здесь корневой домен отделен последней, крайней справа, точкой.

Адреса сайтов с использованием DNS записываются в виде последовательности, отражающей только что рассмотренную иерархию имен. Чем выше уровень домена, тем правее он записывается в строке адреса. Разделяются домены точками. Разберем, например, строку `www.site.nic.ru`. Здесь домен `www` — это домен четвертого уровня, а другие упомянутые в адресной строке домены расположены в домене первого уровня `RU`. Так, `site.nic.ru` — домен третьего уровня. Очень важно понимать, что привычный адрес веб-сайта, скажем, `www.test.ru`, обозначает домен третьего уровня (`www`), расположенный внутри домена второго уровня `test.ru`.

Работу DNS в масштабах всего Интернета обеспечивает распределенная система из многих серверов, которые образуют собственную иерархию. Каждый сервер DNS имеет свою зону ответственности, то есть за ним закреплен участок адресного пространства DNS, в котором этот сервер определяет соответствие IP-адресов и доменных имен. У каждого сервера DNS есть и свой набор клиентов — сервер предназначен для обслуживания именно их.

Основываясь на специальных правилах «доверия» и используя особые протоколы, серверы глобальной DNS обмениваются между собой информацией об изменениях в адресации. При этом изменения не отражаются на всех серверах моментально — напротив, для распространения информации об изменениях в адресации для того или иного домена по всему Интернету может потребоваться несколько суток.

Среди всех серверов DNS есть самые важные — корневые серверы системы, обеспечивающие работу DNS в целом. Таких серверов 13, и они принадлежат техническому центру корпорации ICANN, контролирующей адресное пространство Интернета (подробнее об ICANN и ее регулирующей роли я расскажу ниже).

КСТАТИ



Ни один из 13 корневых серверов DNS не является простым отдельным компьютером, как может показаться. В реальности они представляют собой сложные системы из многих компьютеров, способные одновременно обрабатывать огромное количество запросов. При этом выход из строя даже нескольких составляющих систему компьютеров не приводит к отказу системы в целом.

Ключевую роль играют также корневые серверы доменов первого уровня (например RU), обеспечивающие распространение по всему Интернету DNS-информации о домене, находящемся в их зоне ответственности.

Сложности в построении работающей DNS направлены на то, чтобы каждый из сотен миллионов разбросанных по всему миру компьютеров, подключенных к Интернету, имел возможность корректно преобразовывать адреса.

В упрощенном виде алгоритм работы DNS по поиску адресов веб-сайтов можно описать следующим образом. Когда пользователь вводит в адресной строке браузера адрес веб-сайта, например `http://site.nic.ru/`, компьютер «спрашивает» у того или иного известного этому компьютеру сервера DNS, какой IP-адрес связан с доменным адресом, указанным пользователем. В ответ сервер DNS, проверив соответствие по своим внутренним таблицам или выполнив запрос к другим серверам DNS, присылает искомым IP-адрес. Далее браузер устанавливает соединение с веб-сайтом уже по IP-адресу.

С DNS связано множество проблем безопасности, актуальных как для клиентских компьютеров, так и для Интернета в целом. Например, продвинутые хакеры могут проводить атаки на сервер

DNS, чтобы создать его перегрузку, что вызовет отказы в обслуживании. Подмена адресов в таблицах DNS может приводить к тому, что пользователи, набирающие в адресной строке привычное имя домена, ранее привязанное к одному сайту, будут соединяться с другим сервером, например с сервером злоумышленников, представляющим собой поддельный интернет-магазин, собирающий данные о кредитных картах посетителей.

Проблемы безопасности в DNS в основном связаны с тем, что в восьмидесятых, когда эта система создавалась, Интернет был другим. О многих атаках, ставших возможными теперь, в годы становления Глобальной сети даже не задумывались.

Тем не менее DNS активно развивается и, очевидно, продолжит оставаться ключевым элементом Интернета долгие годы. Несомненно, сохранится и определяющая роль DNS в привычных массовому пользователю механизмах адресации.

В настоящее время к услугам рядового пользователя Глобальной сети — три механизма перехода к тому или иному сетевому ресурсу.

- ❑ Во-первых, пользователь может набрать адрес интересующего сайта в адресной строке браузера.
- ❑ Во-вторых, можно перейти на сайт с помощью поисковой машины, нажав ссылку на странице результатов поиска документов в Интернете.
- ❑ Наконец, третий вариант — переход по ссылке с одного сайта на другой.

На практике в современном Интернете эти три механизма базируются на DNS и доменных именах.

Меняются технологии размещения информации в Интернете, развивается веб, появляются новые средства, позволяющие создавать все более оригинальные веб-сайты. Но пока ни одна из технологий не смогла предложить новых, столь же удобных пользователю механизмов адресации, способных потеснить систему доменных имен.

Глава 3

Администраторы и реестры

- ❑ Права и уровни доменов
- ❑ Рассказы о владельце
- ❑ Тысячи доменов

Права и уровни доменов

Доменов в Интернете очень много. Особое значение имеют домены первого уровня, среди которых принято выделять домены общего пользования (или **домены общего назначения**, как мы их будем называть далее) и **национальные домены**. Например, к доменам общего пользования относится самая популярная (по количеству зарегистрированных имен) доменная зона .com с практически ничем не ограниченной регистрацией. Примером национального домена является домен RU, выделенный России. Впрочем, в такой сложной и многогранной глобальной виртуальной среде, как Интернет, не следует ожидать жесткого деления доменов по классам. Напротив, временами оно весьма условное.

КСТАТИ



Среди доменов общего пользования есть такие, регистрация в которых фактически ограничена по государственной принадлежности лица, регистрирующего доменное имя. Например, домен первого уровня MIL на эксклюзивной основе «оккупировали» государственные военные структуры США.

Среди необычных национальных доменов широко известен домен первого уровня SU, который в свое время выделили Советскому Союзу. И вот советского государства не существует уже более полутора десятков лет, а домен SU остается в строю, демонстрируя рост числа регистраций, — настолько мощным оказалось международное правовое наследие СССР.

Итак, домен — это кусочек виртуального интернет-пространства. Любой подобный кусочек ценен, он дорожает вместе с интернет-пространством и может быть в той или иной мере полезен своему хозяину. Важно лишь правильно понимать, кто в домене хозяин.

Любая хозяйственная деятельность требует записей и отчетов. Домены не исключение. Автомобиль, дом или быстроходный катер как объекты вполне материальные учитываются с помощью

присвоения номеров и регистрации в соответствующих государственных структурах. С доменами дела обстоят несколько иначе, хотя регистрация также играет важную роль.

Прежде всего нужно разобраться, каким предстает домен с точки зрения компьютеров, обеспечивающих работу Интернета. Оказывается, для них домен — лишь запись в специальной базе данных, не более. Других форм существования у домена нет. Домен не компакт-диск, не кусок микросхемы. Домены не перевозят трехтонными грузовиками, как персидские ковры. Наверное, максимум физического воплощения домена, которое мог бы придумать лирик, — это некоторое множество электромагнитных импульсов, размазанных по кабелям и электронике Глобальной сети.



Однако внесение записи о домене в базу данных приводит к тому, что определенный кусочек Интернета начинает функционировать по-другому. Главное — правильно выбрать базу данных.

Параметры функционирования домена определяются соответствующими ему серверами DNS. А эти серверы, в свою очередь, определяет администратор домена.

Администратор домена — главное лицо в домене. Именно администратор обладает правами по управлению доменом и именно администратор определяет, какой веб-сайт или ресурс будет доступен под данным доменом.

Конечно, администратор не обязан владеть техническими навыками управления доменом, ведь он может поручить фактическое управление техническим службам с подходящей квалификацией. Точно так же владельцу грузового судна не обязательно быть капитаном дальнего плавания — капитана и команду можно нанять. (Главное — не ошибиться при выборе капитана, иначе он может увести корабль к пиратам.)

Как говорилось в главе 2, доменное пространство Интернета имеет иерархическую структуру. Соответственно, иерархическую структуру имеет и делегирование полномочий администраторам доменов.

В настоящий момент (2008 год) во главе иерархии находится корпорация ICANN (от англ. Internet Corporation for Assigned Names and Numbers, что означает буквально следующее: «Интернет-корпорация по распределяемым именам и числам»). Она управляет распределением всех адресных ресурсов Интернета. То есть в ведении этой организации не только домены, но и IP-адреса. Конечно, ICANN не работает с отдельными пользователями Интернета, а задает генеральную политику развития систем адресации. Например, специальная комиссия ICANN определяет, какие новые домены первого уровня вводить в глобальной Сети. Как упоминалось выше, в ведении ICANN находятся общемировые корневые серверы DNS, определяющие успешную работу Интернета в целом.

ICANN подконтрольна Минторгу США, а не является, как можно подумать, официальным международным органом управления

вроде ООН. Такая ситуация сложилась исторически, поскольку до появления ICANN адресным пространством Сети управляли правительственные организации США, поручавшие технические процедуры различным компаниям и учреждениям.

От ICANN ожидают действий в интересах Соединенных Штатов, и это неудивительно: Интернет был создан правительственными и исследовательскими лабораториями на средства налогоплательщиков США. На основании этого юридического факта правительство США, учреждая ICANN, подразумевало, что дальнейшее развитие Интернета будет приносить прибыль прежде всего коммерческим компаниям в США, таким образом возвращая налогоплательщикам «инвестированные» средства. Впрочем, на момент учреждения корпорации ICANN в 1998 году Интернет представлял собой вполне сложившееся глобальное явление, так что вопросы о том, почему общемировую Сеть должно контролировать одно государство, возникли задолго до появления корпорации. Но вопросы вопросами, а пока в руках североамериканских телекоммуникационных компаний находились все технические средства по управлению адресным пространством Интернета, спорить с США не было возможности.

Конечно, ICANN не может оказывать юридическое давление на ситуацию с развитием интернет-технологий за пределами США, а ее решения не имеют силы международных договоров или законов в других государствах, пользующихся Интернетом. Другими словами, решения и требования ICANN могут просто игнорироваться интернет-провайдерами других государств. Да, собственно, и провайдеров США ICANN не может принудить к каким-либо действиям.

Как же в таком случае осуществляется управление Интернетом? Довольно просто: ICANN, формально говоря, *рекомендует* другим участникам интернет-сообщества придерживаться некоторых правил и стандартов в работе с Глобальной сетью, а другие участники с этим *соглашаются*. Своего рода общественный до-

говор. Тех же, кто не соглашается с правилами, от Интернета могут отключить, ведь «главный рубильник» находится в руках ICANN.

КСТАТИ



Впрочем, ICANN зарекомендовала себя как очень и очень осторожная организация, всячески избегающая каких бы то ни было конфликтных ситуаций и умеющая лавировать по самым сложным фарватерам. При разрешении проблем ICANN демонстрирует грамотное владение широким набором дипломатических приемов, на зависть многим мировым министерствам иностранных дел. Например, в ход идет качественная работа с общественным мнением. ICANN всегда подчеркивала, что открытость для интернет-сообщества — одна из ключевых характеристик корпорации. Используются и обтекаемые формулировки официальных заявлений о позиции ICANN по тому или иному вопросу, и другие методы международной дипломатии.

Такой подход ICANN к управлению можно понять. Ведь обеспечение связности Глобальной сети, объединившей десятки государств мира, каждое из которых имеет свои исторические особенности, — дело далеко не простое, особенно если учесть, что Сеть нужно развивать. Именно из-за сложности объекта управления все стратегические решения (а тактикой ICANN и не занимается) принимаются корпорацией после многолетних консультаций и размышлений.

Итак, верхний уровень иерархии управления доменными именами занимает ICANN. Полномочия по управлению распределением имен внутри созданных доменов первого уровня ICANN делегирует другим организациям. При делегировании полномочий используются различные процедуры, зависящие от типа домена и иных факторов. Так, управлять доменом может одна организация или несколько, при этом взаимоотношения между этими организациями и лицами, которым они предоставляют права регистрации доменов, регулируются самым разным образом. Хотя, конечно, сложились определенные традиции.

ICANN назначает ответственных за домены первого уровня, а эти ответственные уже сами устанавливают правила игры внутри выделенных им доменов и обеспечивают исполнение правил. При этом ICANN сохраняет стратегическое управление в своих руках.

Таким образом, у каждого домена первого уровня есть администратор (обычно юридическое лицо), который обеспечивает взаимодействие с ICANN и задает правила игры внутри домена. Существует и такое понятие, как регистратор доменов.

Регистратор доменов — тот, кто предоставляет услуги по регистрации доменных имен во «вверенном» домене другим лицам (юридическим и физическим). Администратором и регистратором может быть одно лицо. Но возможна и ситуация, когда администратор у домена один, а регистраторов много, и они конкурируют между собой. Так, например, в домене RU на начало 2008 года действовало 16 компаний — регистраторов доменов.

КСТАТИ



В популярных доменах общего пользования, например в COM, ситуация несколько сложнее: там больше регистраторов, и отношения между регистраторами выстроены иначе.

Что такое регистрация доменного имени? Это внесение информации в связанный с данным доменом электронный реестр, фиксирующий распределение адресного пространства в домене. В реестр записываются само доменное имя и данные его владельца. То есть запись свидетельствует о том, что такой-то домен находится в управлении у такого-то лица, которое и является администратором домена. Данные о доменах в глобальной DNS формируются с учетом информации из реестров регистраторов.

Информация о регистрации домена может быть внесена в реестр, но сам домен при этом не будет доступен для DNS. Дело в том, что регистрация домена и размещение его в DNS — две различные процедуры.

Размещение домена в DNS называют **делегированием домена**. Если домен делегирован, то размещенные под ним сетевые ресурсы могут быть доступны для пользователей Интернета. Регистрация домена не подразумевает немедленное его делегирование в DNS.

Например, если Петр Иванов сумел зарегистрировать домен test.ru, то в реестре регистраций домена RU будет содержаться информация о том, что правом на управление доменным именем test.ru наделен Петр Иванов. А право на управление в случае с доменом подразумевает как минимум возможность привязывать домен к тем или иным серверам DNS (делегирование домена). И только с помощью правильно сконфигурированных серверов DNS домен может быть привязан к веб-сайту. Если у Петра Иванова есть нужные пароли, то он может разместить под доменом test.ru произвольный сайт.

КСТАТИ



Тут надо заметить, что домен и веб-сайт — это разные вещи, связываемые друг с другом посредством настройки DNS. Например, один и тот же веб-сайт можно разместить под несколькими совершенно разными доменами.

Администратор, получив в управление домен *второго уровня*, может не только привязать его к сайту, но и самостоятельно распределять доменные имена внутри своего домена. Скажем, только что упомянутый Петр Иванов, реализуя свое право на управление доменом test.ru, может независимо от администратора домена RU зарегистрировать домены *третьего уровня* www.test.ru, petrowich.test.ru.



Таким образом, мы рассмотрели иерархию администрирования доменов: **ICANN** — администратор домена первого уровня — администратор домена второго уровня. Конечно, иерархия продолжается и дальше. Например, тот же самый Петр Иванов может назначить администратором домена `petrov.test.ru` Ивана Петрова и установить с этим distinguished господином договорные отношения по управлению доменом `petrov.test.ru`. Понятно, что можно было бы продолжить построение иерархии и на четвертом, пятом, шестом уровнях. Есть ли предел такому росту вглубь?

Оказывается, есть. Пределы ставит сложившаяся практика. Обычно строгие и формальные отношения с администратором, закрепляемые тем или иным договором, устанавливаются для доменов первого (это особенно важные домены, здесь одной из сторон договора выступает ICANN), второго и, реже, третьего уровня. Последний момент в основном касается тех доменов верхнего уровня, в которых на регистрацию имен накладываются дополнительные упорядочивающие условия.

КСТАТИ



Примером домена, в котором юридические строгости уровня регистратора касаются доменов третьего уровня, может служить национальный домен Великобритании — UK. В нем регистрация имен возможна только в специально выделенных доменах второго уровня, например: `.co.uk` — для коммерческих структур, `.me.uk` — для персональных страничек, а `.org.uk` — для некоммерческих и общественных организаций.

Администратор домена более высокого уровня при желании может «отобрать» домен уровнем ниже, зарегистрированный в его зоне ответственности. Технические рычаги для осуществления этой операции даст DNS, позволяющая администратору переопределять адресацию в своей зоне произвольным образом. На практике «отобрать» домен можно, удалив записи о нем из DNS, — в этом случае все ресурсы, размещенные под этим доменом, просто перестанут быть доступны из Интернета. Можно «отобрать» домен, перенастроив DNS так, что домен будет указывать на совершенно другой сайт.

С юридической точки зрения лишение права администрирования домена должно регулироваться договором между сторонами, вовлеченными в использование домена, и правилами регистрации доменных имен. Но если с технической стороной процедуры все более или менее понятно, то с юридической иногда возникает ряд очень сложных коллизий, о которых я подробно расскажу в главе 12.

Итак, для рядовых участников доменной системы Интернета обычно наиболее важны процедуры, касающиеся управления доменами второго уровня (и иногда — третьего). Большая часть доменных «войн» и конфликтов также связана с доменами второго уровня.

Порядок использования домена определяет его администратор. Интересно, что администрирование домена — это право (может быть, и почетное). Это весьма важное уточнение: нельзя думать, что раз вы заплатили регистратору, то домен теперь куплен. Ведь мы уже разобрались, что домен не кольцо с бриллиантом, не холодильник и не дизайнерские солнечные очки. Домен нельзя

купить, но в обмен на денежный взнос можно приобрести у уполномоченной компании право на управление доменом и стать его администратором. При этом право приобретается на определенный срок, например на один год.

За честно купленное кольцо с бриллиантом не пужно платить второй раз. Право администрирования домена требует регулярного продления, за что придется заплатить, иначе право передат другим желающим поуправлять.

Таковы правила игры.

Рассказы о владельце

Реестр владельцев доменных имен в доменах первого уровня, который ведут уполномоченные регистраторы, предоставляет информацию для весьма важного сервиса, носящего название WHOIS.

С технической точки зрения **WHOIS** — набор баз данных и протокол доступа к ним. С практической точки зрения сервис WHOIS — весьма полезный инструмент, позволяющий пользователям Интернета получать данные о регистрации того или иного домена.

Сделав запрос с именем интересующего домена к WHOIS, можно узнать, свободен ли этот домен. Если домен уже кем-то зарегистрирован, WHOIS может сообщить дополнительную информацию о настройках DNS домена и о том, кем, через какого регистратора и когда домен зарегистрирован. Через WHOIS можно получить ту или иную контактную информацию владельцев домена или службы технической поддержки, обеспечивающей работу домена.

Впрочем, борьба за конфиденциальность персональных данных приводит к тому, что точные и полные сведения о владельце домена можно получить далеко не во всех случаях. В зависимости от действующего в той или иной стране законодательства и от предпочтений конкретного владельца домена на публикуемую в WHOIS информацию накладываются различные ограничения. Например, вместо имени владельца может быть указано просто

Private Person (частное лицо). Кроме того, информация в WHOIS может быть недостоверной, потому что далеко не всегда регистраторы тщательно следят за соответствием действительности публикуемых владельцами доменов данных.

Другие ограничения на использование WHOIS связаны с тем, что за различные домены первого уровня отвечают различные регистраторы и администраторы, которые могут вести свои собственные базы данных для WHOIS.

Использовать WHOIS для получения информации о доменах весьма просто. Большинство крупных регистраторов предоставляют доступ к WHOIS на своих веб-сайтах: на странице запроса к WHOIS достаточно ввести имя домена, в ответ сервер вернет информацию о состоянии этого домена. Кроме запросов через веб, использовать WHOIS можно и с помощью специальных программ-клиентов.

Попробуем исследовать домен test.ru с помощью сервиса WHOIS на веб-сайте регистратора доменов RU-CENTER. Форма отправки запроса находится по адресу <http://www.nic.ru/whois/>, и на момент написания книги она выглядела так, как на иллюстрации, приведенной ниже.

В ответ на запрос test.ru, введенный в форму, сервер возвращает страницу с довольно подробной информацией.

По данным WHOIS.NIC.RU:

```
% By submitting a query to RU-CENTER's Whois Service
% you agree to abide by the following terms of use:
% http://www.nic.ru/about/servpol.html (in Russian)
% http://www.nic.ru/about/en/servpol.html (in English).
```

```
domain:    TEST.RU
type:      CORPORATE
nserver:   ns3.nic.ru
nserver:   ns4.nic.ru
state:     REGISTERED, DELEGATED
org:       ANO Regional Network Information Center
phone:     +7 499 1967278
fax-no:    +7 499 1964984
e-mail:    lad@ripn.net
e-mail:    ru-ncc@nic.ru
descr:     test domain!
registrar: RUCENTER-REG-RIPN
created:   2005.08.16
paid-till: 2008.12.15
source:    RU-CENTER
```

Last updated on 2008.04.14 13:06:00 MSK/MSD.

По данным WHOIS.RIPN.NET:

```
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).
```

```
domain:    TEST.RU
type:      CORPORATE
nserver:   ns3.nic.ru.
nserver:   ns4.nic.ru.
state:     REGISTERED, DELEGATED
org:       ANO Regional Network Information Center
phone:     +7 499 1967278
fax-no:    +7 499 1964984
e-mail:    lad@ripn.net
e-mail:    ru-ncc@nic.ru
registrar: RUCENTER-REG-RIPN
created:   1997.05.23
paid-till: 2008.12.15
source:    TC-RIPN
```

Last updated on 2008.04.14 13:04:17 MSK/MSD.

Что же означают все эти буквы и цифры и какие выводы о test.ru можно сделать?

Главный вывод: домен test.ru занят, и зарегистрировать его нельзя. Об этом говорит уже наличие самой записи о домене в базе данных WHOIS. Если бы домен test.ru был свободен для регистрации, то в ответ на запрос WHOIS сообщил бы что-то вроде «Данных о домене не найдено!». Это важная особенность WHOIS: каковы бы ни были требования по охране персональных данных, запись о зарегистрированном домене нельзя полностью изъять из публично доступной базы данных регистраций (как, например, это можно сделать с телефонным номером и публичным телефонным справочником).

Кроме того, что домен занят, WHOIS рассказывает нам о владельце домена. В поле org: указано, что администратором домена является организация ANO Regional Network Information Center. А поля phone, fax-no и e-mail содержат контактную информацию,

актуальную для этого домена. Также из ответа WHOIS видно, что домен test.ru делегирован (поле state) и привязан к двум серверам DNS (поля nserver — ns3.nic.ru, ns4.nic.ru).

Несложно заметить, что в приведенном ответе сервиса WHOIS информация, по сути, продублирована. Почему? Дело в том, что информацию об одном и том же домене можно получить из нескольких источников. В нашем случае информацию о test.ru возможно получить из базы данных WHOIS регистратора RU-CENTER и из базы данных WHOIS технического центра домена RU. Сервис, обрабатывающий запросы о доменах на сайте RU-CENTER, вернул информацию из обоих источников. Кстати, информация о домене у регистратора и у технического центра вполне может отличаться. Мы не будем сейчас подробно разбирать все возможные поля в ответе WHOIS-сервиса, ограничимся таблицей, описывающей их в краткой форме (табл. 1).

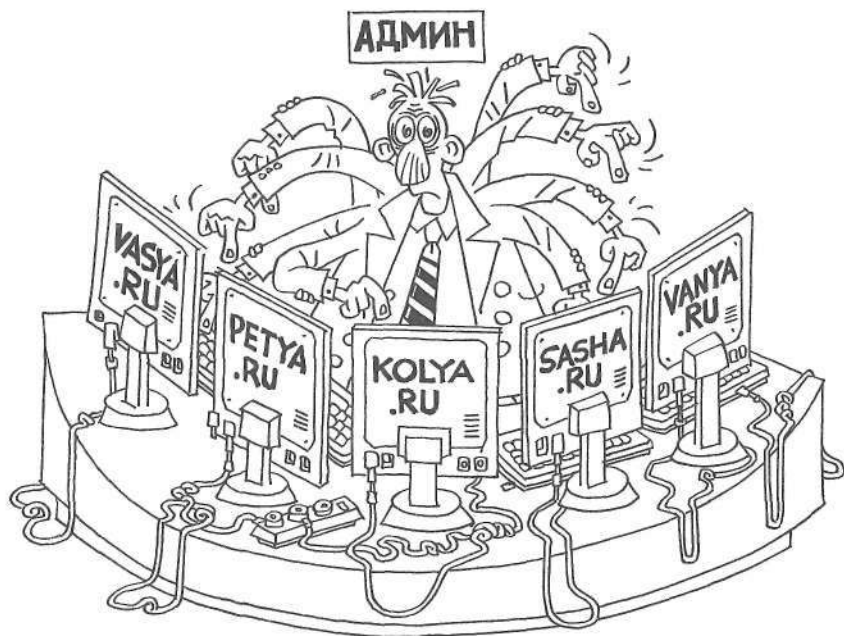
Таблица 1. Описание полей в ответах WHOIS-сервиса

| Поле | Описание |
|----------|--|
| address: | Контактный адрес физического лица (на английском языке) (необязательное) |
| admin-c: | Идентификатор представителя организации для административного контакта с РосНИИРОС |
| admin-o: | Идентификатор администратора домена |
| bill-c: | Идентификатор представителя организации, ответственного за оплату услуг по домену |
| changed: | Дата последнего изменения клиентом информации в объекте (приводит к запуску процесса тестирования зоны). Для доменов третьего уровня может указывать дату, когда начнется ежегодное автоматическое тестирование зоны, если не будет прислан запрос на обновление зоны (в формате YYYY.MM.DD, где YYYY — год, MM — месяц, DD — число) |
| created: | Дата регистрации домена; не изменяется при продлении срока регистрации, смене администратора или регистратора домена (в формате YYYY.MM.DD, где YYYY — год, MM — месяц, DD — число) |
| domain: | Доменное имя |

| Поле | Описание |
|------------|---|
| c-mail: | Адрес электронной почты |
| fax-no: | Номер факса (с международным кодом и кодом города) |
| free-date: | Дата освобождения домена (указывается для доменов с приближающимся сроком аннулирования регистрации) (в формате YYYY.MM.DD, где YYYY — год, MM — месяц, DD — число) |
| mnt-adm: | Организация или физическое лицо, которому принадлежит служба технической поддержки |
| mnt-by: | Идентификатор службы технической поддержки (службы авторизации), отвечающей за корректность информации о домене в базе данных РосНИИРОС |
| mntner: | Идентификатор службы технической поддержки в базе данных РосНИИРОС |
| nic-hdl: | Идентификатор объекта базы данных |
| nserver: | Список DNS-серверов, поддерживающих домен (если имя сервера содержит имя домена, то указываются также его IP-адреса) |
| org: | Название организации |
| paid-till: | Дата, по которую оплачена регистрация домена (в формате YYYY.MM.DD, где YYYY — год, MM — месяц, DD — число) |
| person: | Полное имя физического лица |
| phone: | Телефон(-ы) с международным кодом и кодом города |
| reg-ch: | Идентификатор регистратора, которому передается домен (если должен смениться регистратор) |
| registrar: | Идентификатор регистратора |
| remark: | Произвольные текстовые комментарии (поле необязательное) |
| source: | Источник информации |
| state: | Состояние объекта |
| tech-c: | Идентификатор контактного лица по техническим вопросам |
| type: | Тип домена |
| whois: | WHOIS-сервис регистратора |
| www: | URL-адрес сайта регистратора |
| x-freing: | Домен подлежит удалению из реестра в течение часа |

Тысячи доменов

Сколько доменов внутри домена первого уровня может находиться под контролем одного администратора? Пять? Десять? Пределы зависят только от правил регистрации, действующих внутри домена. Например, в некоторых национальных доменах на число имен, «отпускаемых в одни руки», наложены серьезные ограничения. Впрочем, правила регистрации могут быть и весьма либеральными, не накладывая вообще никаких ограничений на число доменов в управлении одного администратора. Скажем, таковы правила доменов COM и RU.



КСТАТИ

Важно напомнить, что в некоторых доменах первого уровня более или менее свободная регистрация доступна только для доменных имен третьего уровня. Помимо упоминавшегося



выше национального домена Великобритании — UK, аналогичная, но еще более жесткая ситуация наблюдается, например, в домене PRO. Домен PRO предназначен для регистрации адресов сертифицированными специалистами, и здесь имена регистрируются внутри доменов второго уровня, обозначающих принадлежность к тому или иному типу профессиональной деятельности. Например, имя вида name.med.pro в домене второго уровня med.pro может быть зарегистрировано практикующим врачом.

Итак, если правила позволяют, то найдутся администраторы, желающие получить в управление и десять, и сто, и тысячу доменов. И главное — не только желающие, но и имеющие возможность осуществить свое желание. Так, по официальным данным реестра доменов, в домене RU на начало 2008 года у одного из администраторов находилось в управлении более 10 тыс. доменных имен; около 50 администраторов имели в управлении более тысячи доменов. При этом около 10 тыс. администраторов имели в управлении от 11 до 100 доменов.

Цели, преследуемые администраторами больших доменных пулов, обычно относятся ко вторичному рынку доменов. Домены — ресурс ограниченный, и, застолбив «вкусное» имя по цене регистрации, можно в будущем перепродать права на управление этим доменом за гораздо большую сумму. То есть приобретение доменов в управление, очевидно, рассматривается как инвестиционная деятельность. А людей, профессионально играющих на вторичном рынке доменов, сейчас принято называть доменными инвесторами, или домейнерами.

Впрочем, на заре доменного рынка администраторов, массово столбивших домены, называли киберсквоттерами, то есть захватчиками пространства. Этот термин существует и сейчас, но теперь киберсквоттерами называют тех, кто захватывает домены в нарушение некоторых «правил приличия», сложившихся на рынке. Одним из характерных признаков киберсквоттера является приобретение доменных имен, совпадающих с названиями

раскрученных брендов. Застолбив такое имя, киберсквоттер предлагает владельцу бренда выкупить домен за внушительную сумму, порой даже угрожая передать домен конкурентам или разместить под ним порочащую бренд информацию.

Домейнеры же предпочитают действовать в правовом поле, придумывая интересные доменные имена и затем предлагая их всем желающим.

Глава 4

Виртуальная география, или Домен SU

В 1990 году, когда Советский Союз вливался в виртуальное пространство Сети, ему выделили виртуальный участок в глобальном адресном пространстве — так появился домен SU, который формально зарегистрировала Советская ассоциация пользователей UNIX (SUUG).

Советский Союз, некогда могучее государство, в конце 80-х годов переживал не самые лучшие времена. Времена эти оказались настолько «не лучшими», что в 1991 году СССР распался и исчез с политической карты мира.

Советский Союз исчез, а домен SU остался.

После распада СССР возникла закономерная идея о регистрации домена RU для России: многие сайты из доменов SU могли мигрировать в RU. Однако переговоры вокруг домена RU, сопровождавшиеся уточнением процедур и определением ответственных сторон, несколько затянулись. В итоге домен RU появился только в апреле 1994 года.

Практически одновременно с исчезновением Советского Союза с мировой политической арены возникли споры о будущем домена SU: следует ли его немедленно удалить или можно оставить? Надо заметить, что к 1994 году в домене SU располагалось несколько тысяч доменных имен (речь идет обо всех именах, а не только о доменах второго уровня). После появления домена RU администратор домена SU, РосНИИРОС (Российский научно-исследовательский институт развития общественных сетей, выросший из Курчатковского научного центра), прекратил регистрацию доменов второго уровня в SU. Тем не менее сам домен решено было сохранить: помимо политических причин, сохранения SU в течение переходного периода требовали и чисто технические моменты обеспечения работы российского сегмента Глобальной сети.

Сторонники ликвидации домена SU полагали, что вот-вот, через один-два года, все сайты из SU благополучно «разъедутся» по другим доменам, и виртуальное воплощение Советского Союза

можно будет вычеркнуть из глобальной системы доменных имен. Именно так случилось с доменом CS, который после распада государства Чехословакия в 1993 году довольно быстро опустел и был удален из реестра доменов первого уровня.

Однако SU оказался гораздо более живучим. Вместо того чтобы опустеть, домен вдруг принялся расти за счет доменов третьего уровня. Однако с 1998 года рост сменился сокращением, которое, впрочем, не давало оснований для удаления домена, ведь число размещенных в нем вполне живых и востребованных ресурсов все еще исчислялось многими тысячами.

В 2001 году полномочия по администрированию домена SU были частично переданы от РосНИИРОС Фонду развития Интернета, который сразу же предпринял шаги по возобновлению регистрации имен в домене SU.



Правда, заключив необходимые соглашения, Фонд начал развитие SU с установления невероятных запретительных цен на

регистрацию доменов второго уровня. \$15 000 за домен — весьма высокий порог вхождения на рынок доменов SU, доступный лишь избранным компаниям. Впрочем, цены довольно быстро падали. Так, с октября по декабрь 2001 года стоимость регистрации снизилась с упомянутых \$15 000 до \$1000. А уже весной 2002 года она составила \$100 в год — сумма, более близкая к адекватному на тот момент уровню цен. Сто долларов за домен — такой ценник сохранялся в SU несколько лет.

И все эти годы вокруг SU шли споры, по большей части направленные в сторону универсального арбитра — ICANN. Так, одни инициативные пользователи Интернета требовали от ICANN удаления домена SU, нарушающего принципы и правила создания национальных доменов: государства нет, а домен есть. Другие граждане доказывали ICANN, что домен реально используется, и параллельно искали для SU новое позиционирование: например, он мог бы стать доменом СНГ.

Свои домены есть у подавляющего большинства стран, отмеченных на политической карте. Например, островное государство в Карибском бассейне Тринидад и Тобаго владеет доменом TT. Из внутренних соображений, в борьбе против хаоса в адресной системе Интернета, ICANN иногда пытается отражать изменения реальной политической карты мира на виртуальной мировой карте, в которой, вообще говоря, совсем иная география.

Так, помимо упоминавшегося домена Чехословакии, с падением берлинской стены канул в Лету домен DD, ранее отражавший ГДР (Восточную Германию). ICANN просто взяла и отключила его, потому что она контролирует корневые серверы имен и технически может легко отключить любой домен верхнего уровня. Исчезновение зоны DD — случай прямой связи виртуальной и реальной географии.

С доменом SU вышло иначе. Несмотря на все требования о его удалении, это виртуальное воплощение пережило крах своего реального аналога уже более чем на 16 лет. Домен SU и сейчас живее всех живых.

Да, на протяжении всех «смутных лет» ICANN действительно несколько раз по разным поводам упоминала о своем намерении уничтожить все устаревшие имена. И по традиции под «устаревшие» попадал домен SU, содержащий тысячи сайтов. Но на виртуальной политической карте своя география, расстояния здесь измеряют иначе, и координаты все больше сверяют по ссылкам из Google. На адреса внутри домена SU ссылаются многие страницы из других стран, с других доменов. Уничтожение домена привело бы к нарушению связности в не очень большом, но все же исторически значимом кусочке веба.

Воевавшие вокруг домена SU стороны активно привлекали внимание общественности. Дело в том, что для влияния на ICANN, позиционирующейся в качестве открытой организации, общественное мнение — очень важный инструмент.

Кто же выиграл? Подводить итог еще рано: война не окончена. Тем не менее крупное сражение в 2007 году выиграл домен SU, который несколько неожиданным образом спасло мощное наследие Советского государства.

Выслушав спорящие стороны, представители ICANN официально заявили, что при создании национальных доменов ICANN руководствуется специальным международным стандартом — ISO 3166, описывающим двухбуквенные коды стран. И домен SU может быть удален не раньше, чем из этого стандарта исчезнет обозначение SU. То есть ICANN опять проявила чудеса дипломатии, умело переведя вопрос из политической плоскости в чисто техническую.

На протяжении нескольких десятков лет Советский Союз являлся одним из определяющих полюсов мировой политики, поэтому код стандарта ISO 3166 SU фигурирует в великом множестве важных официальных дипломатических документов и международных соглашений, которые не утратили силы и по сей день. Так что ожидать удаления кода SU из мировой дипломатической практики в ближайшие годы не приходится, а значит, сохранится он и в стандартах ISO.

Так что Советский Союз поддержал могучей дипломатической рукой свое виртуальное воплощение — домен SU — даже «с того света», если можно так выразиться.

В декабре 2007 года стоимость регистрации доменов в зоне SU резко снизилась: с 3000 до 600 руб. Снижение цены вызвало взрывной рост числа регистраций — зона SU в течение нескольких дней увеличилась почти в три раза, что только подчеркнуло: умирать самостоятельно домен SU вовсе не планирует. Более того, в апреле 2008 года в домене SU началась регистрация многоязычных доменных имен.

Глава 5

Оплот Рунета — домен RU

Союз Советских Социалистических Республик распался в 1991 году. Республики, ранее образовавшие единое государство, обрели самостоятельность, в том числе и во всемирной системе адресации Интернета. Правда, при изменении виртуальной географии домен СССР не исчез. То есть виртуальное отражение политической карты мира после распада СССР приобрело новые домены, сохранив нетронутым исходный домен SU.

Новые национальные домены в Интернете возникают не просто так, а в соответствии со сложившейся практикой присвоения государствам двухбуквенных кодов. Порядок использования этих кодов регулируют международные организации, ответственные за выработку единых стандартов. Для России как независимого государства, субъекта международной политики, код RU был введен в стандарты в 1992 году. Между тем домен первого уровня RU начал функционировать только в апреле 1994 года. Почему же возникла столь длинная задержка?

Дело в том, что к 1992 году у заинтересованных в Интернете российских компаний уже был накоплен некоторый опыт (еще советский) по использованию доменных имен. И конечно, как только на горизонте маячил новый домен верхнего уровня, заявки на его получение оперативно направили сразу несколько российских организаций.

В начале 1990-х годов распределением адресного пространства Интернета ведала такая организация, как **IANA** (от англ. **I**nternet **A**ssigned **N**umbers **A**uthority — Уполномоченная организация по распределению нумерации в сети Интернет). Сейчас она в качестве одного из подразделений входит в корпорацию ICANN. Но и во времена «до ICANN» IANA была организацией осторожной и сторонящейся всевозможных конфликтов. Поэтому конкурирующим за право администрирования нового домена RU компаниям пришлось прежде повоевать между собой и самим разобраться, кому же достанется новый кусок виртуального пространства.

В итоге споров, пересудов и разбирательств, длившихся почти два года, администрирование домена RU было решено доверить более

или менее нейтральной организации, устраивавшей все ключевые стороны «доменной войны». Ею оказался РосНИИРОС, управлявший и доменом SU, который, как ожидалось, должен был стать основным «донором» новых доменных имен в зоне RU. Ведь домен SU тогда собирались ликвидировать, и сразу после появления домена RU РосНИИРОС приостановил регистрацию имен второго уровня в SU.

Итак, домен новой России RU, запись о котором в реестр национальных доменов внесена 7 апреля 1994 года, достался в управление РосНИИРОС. А правила администрирования зоны .ru, которых должен был придерживаться РосНИИРОС, выработали с участием ключевых игроков рынка Интернета того времени. РосНИИРОС до 2000 года осуществлял функции по регистрации имен в домене RU, обрабатывая заявки от интернет-провайдеров или юридических лиц. Также за институт закреплялись обязанности по техническому сопровождению функционирования DNS национального домена.

Интернет тем временем активно развивался, превращаясь из академической среды общения в среду ведения бизнеса. Изменение рыночной ситуации требовало скорректировать правила регистрации доменных имен. Тем не менее домен RU долго демонстрировал чудеса консерватизма.

С ростом бизнес-значения доменных имен возросла и активность домейнеров (или, как этих предприимчивых господ поголовно называли в те времена, киберсквоттеров). Домейнеры приобретали «вкусные» имена по цене регистрации, инвестируя собственные средства, и позже предлагали заинтересованным лицам и компаниям выкупить у них права на управление привлекательным именем за сумму, значительно превышающую стоимость регистрации. А так как два одинаковых имени зарегистрировать нельзя, бизнесмены, успевшие застолбить домен ранее других, получали преимущество. Особенно интенсивно активность на рынке подобных перепродаж росла в конце 1990-х годов.



Между тем правила регистрации доменов в зоне .ru прямо запрещали подобную деятельность по «возмездной передаче» прав администрирования домена. Этот запрет был вызван желанием помешать массовому захвату доменных имен сквоттерами. Сторонники запрета полагали, что имена, которые удерживали сквоттеры-домейнеры, изымались из числа доступных ресурсов, однако при этом сквоттеры не использовали эти имена «по прямому назначению» (не размещали под доменами «живые» сайты), что в итоге могло пагубно сказаться на удобстве пользования Интернетом.

Впрочем, никаких серьезных рычагов воздействия на формировавшееся сообщество домейнеров у РосНИИРОС не было. Домейны интенсивно столбили желающие позже перепродать имя по выгодной цене. Попытка предотвратить возникновение вторичного рынка доменов привела лишь к тому, что он длительное время существовал в «серой» зоне.

Домены в зоне .ru становились все более важным активом, рост числа регистраций подстегивался планомерным снижением стои-

мости регистрации (от \$100 в год она снизилась сперва до \$50, а к 2001 году — до \$24).

КСТАТИ



Важно заметить, что в домене RU выделено значительное число доменов второго уровня, регистрация в которых осуществляется бесплатно. Это так называемые домены общего пользования, к которым относят, например, отраслевые домены, географические домены, домены для государственных нужд. Так, домен .com.ru предназначен для коммерческих организаций, и регистрация в нем имен (например, test.com.ru) должна быть бесплатной. В свою очередь, домен net.ru предназначен для проектов, так или иначе связанных с жизнью и развитием Интернета. Например, по адресу www.provider.net.ru расположен один из старейших узкоспециальных информационных ресурсов Рунета — «Независимый обзор провайдеров». По схожим в общих чертах с доменами .com.ru и .net.ru правилам управляются (а точнее, должны управляться) и другие отраслевые, географические, государственные домены второго уровня, полный список которых приводится в приложении 1 (<http://www.cctld.ru/ru/doc/acting/?id21=20&i21=8>).

К началу XXI века некоторые коммерческие фирмы находились в такой зависимости от своих сайтов, размещенных под узнаваемыми доменными именами, что ликвидация домена неминуемо привела бы к автоматической ликвидации всего бизнеса компании. Причем речь шла не только об интернет-компаниях вроде известных поисковых систем, но и о некоторых торговых, производственных фирмах.

Столь серьезные изменения рынка коснулись и базовых принципов управления доменом RU. Все возраставшее число конфликтов и просто спорных ситуаций вокруг доменов в зоне .ru, и особенно вокруг процедур их регистрации, привело к введению в 2000 году распределенной системы регистрации. Функции регистрации доменов от РосНИИРОС начали передавать конкурирующим между собой независимым регистраторам, которые предварительно получали аккредитацию.

Дальнейшее бурное развитие рынка привело к учреждению в 2001 году Координационного центра национального домена RU (далее в главе — Координационный центр), который должен был определить устраивающие игроков рынка правила игры, а точнее — правила регистрации доменов в зоне .ru. При этом РосНИИРОС, вошедший в состав учредителей Координационного центра, сохранил за собой роль технического центра, обеспечивающего функционирование домена RU. Функции же по регистрации полностью перешли к компаниям-регистраторам. Так, на начало 2008 года в домене RU действовало 16 аккредитованных регистраторов.

Одновременно под давлением реальности оформился легальный вторичный рынок доменов. Из Правил зоны .ru изъяли запрет на «продажу» доменов. Более того, весной 2004 года ведущий регистратор доменов RU — компания RU-CENTER — запустил официальный аукцион доменов. Появление аукциона, где гарантом сделки выступал аккредитованный регистратор доменов, наконец-то вывело вторичный рынок из «серой» зоны, дав продавцам и покупателям вполне законный механизм для совершения сделок по передаче права администрирования.

С 4 января 2006 года администратором домена RU официально стал Координационный центр. Необходимо заметить, что за время своего существования он зарекомендовал себя весьма инертной организацией, которой весомые решения, касающиеся судьбы домена RU, если и даются, то с большим трудом, а чаще вообще никак не даются.

Особенно остро инертность Координационного центра ощущается игроками рынка при возникновении конфликтных ситуаций. А разнообразных масштабных конфликтов вокруг доменов .ru становится все больше.

Так, в конце 2007 — начале 2008 года в домене RU сложилась довольно напряженная ситуация, связанная с минимальной стоимостью регистрации доменов. Суть проблемы составляло зафик-

сированное в правилах зоны .ru соглашение между регистраторами о том, что на розничном рынке минимальная цена регистрации домена составляет 500 руб. При этом, согласно тем же правилам, часть себестоимости регистрации домена для регистратора составляет платеж в пользу технических и административных служб домена RU, ведь поддержание функционирования DNS также требует существенных затрат. Впрочем, сумма этого платежа в несколько раз меньше 500 руб. и в 2008 году составляет 70 руб. (<http://cctld.ru/ru/doc/acting/?id21=165&i21=5>).

К 2007–2008 годам в условиях жесткой конкуренции на рынке доменов в розничном секторе появились предложения услуг по регистрации доменов в зоне .ru по цене, значительно меньшей 500 руб. Первые подобные предложения появились на закрытых интернет-форумах и не афишировались. Источником «новых розничных цен» послужили партнеры некоторых регистраторов, пытавшиеся развивать собственный бизнес, привлекая клиентов выгодными ценами.

В правилах регистрации доменов .ru нашлась лазейка: официальные правила и соглашения между регистраторами регламентировали только минимальную цену, по которой услуги регистрации оказываются *на розничном рынке* физическим лицам. Своим партнерам, проводящим «оптовые» регистрации, регистраторы могли предлагать и другую цену, меньше установленного предела. При этом компании — партнеры регистраторов, не являясь участниками регистраторских соглашений, как раз и предлагали на рынке домены по сниженным ценам.

Довольно длительное время ведущие регистраторы строго следили за деятельностью своих партнеров, пресекая попытки доменного демпинга и пытаясь сохранить в действии установленные правила. Участники рынка ждали, что Координационный центр вмешается и «прекратит безобразие», призвав тех регистраторов, которые позволяют своим партнерам нарушать правила игры, к ответу. Однако Координационный центр молчал.

На этом фоне регистраторы все больше ослабляли контроль за партнерами, и цены партнерских регистраций падали все ниже — до 300, 200 руб. А к 2008 году можно было найти предложения и по 100 руб. за домен.

Более того, в 2008 году бизнес регистраций по демпинговым ценам, охвативший партнеров всех сколько-нибудь крупных регистраторов, стал совершенно откровенным. Предложения о регистрации доменов «по 100 рублей» уже встречались не только на специальных закрытых форумах, но и в открытой рекламе.

КСТАТИ



Низкие фактические цены регистрации доменов .ru на розничном рынке были доступны и прежде, а довольно часто домены вообще предлагались бесплатно. Однако новизна ситуации 2007–2008 годов заключалась в том, что раньше дешевые домены предлагались в качестве бонуса к другим пакетным услугам крупных интернет-компаний, например при покупке хостинга или услуг доступа к Интернету. В этом случае клиент оплачивал другие услуги на сумму более 500 руб. и получал «домен в подарок», что с формальной точки зрения могло быть истолковано так: домен за клиента оплачивает компания, фактически предложившая скидку на пакет своих услуг, а не на стоимость регистрации домена. Различие между схемами с пакетом услуг и с простой регистрацией очевидно: во втором случае клиент без вариантов и юридического крючкотворства получает домен по демпинговой цене.

Важный аспект новых цен заключается в том, что клиент получает такие же права по управлению выбранным доменным именем, как и те администраторы, которые регистрировали домены по 600 руб. (500 руб. + НДС) у компаний, придерживавшихся правила минимальной цены.

Конечно, компании, предлагавшие регистрацию по низкой цене или бесплатно, получали существенное конкурентное преимущество перед теми регистраторами, которые придерживались буквы соглашения.

Формально у Координационного центра в руках находился рычаг воздействия на регистраторов, который не посвященному в скрытые механизмы доменного рынка наблюдателю может показаться эффективным. По крайней мере более эффективным, чем общественное порицание способствующих снижению цен регистраторов на заседаниях правления Координационного центра и в кулуарах. Этот рычаг — лишение аккредитации.

Действительно, согласно Правилам зоны .ru для осуществления регистраторского доступа к реестру доменов компания, желающая стать регистратором, должна получить аккредитацию у Координационного центра. По тем же правилам Координационный центр (в рамках неких формальных процедур) вправе лишить регистратора аккредитации. Однако на деле лишение аккредитации к регистраторам не применялось: Координационный центр по внутренним причинам не смог решиться на столь радикальную меру. Можно предположить, что Координационный центр действует подобным образом, опасаясь последствий и ответных судебных исков регистраторов, которые в результате лишения аккредитации понесут убытки. Так что эффективность единственного рычага давления мнимая.

Юридическая коллизия в том, что правила, по которым управляется зона .ru, являются не более чем «джентльменскими соглашениями», а точнее, договорами, заключенными между несколькими юридическими лицами. С точки зрения, например, судебной системы Российской Федерации соглашения и правила домена RU не имеют силы закона. Поэтому нарушение пункта правил о минимальной цене регистрации домена, да еще совершенное не регистратором, а его партнерами, может в худшем случае трактоваться лишь как невыполнение обязательств, взятых в рамках «джентльменского соглашения». В разрезе судебных разбирательств (если они возникнут) нужно также учитывать, что подобное нарушение не наносит непосредственно убытка другим сторонам соглашения. А вот лишение аккредитации непосредственно повлияет на бизнес компании-регистратора (собственно, этот бизнес остановится) и приведет к значительным прямым и косвенным убыткам у этой компании — очень весомые причины для судебного иска, правда?



С точки зрения деловых традиций отношение Правил зоны .ru к минимальной цене розничной регистрации доменных имен еще несколько лет назад представлялось вполне обоснованным и отражающим нормальную рыночную практику.

Например, действующие на рынке промышленных товаров компании-производители отпускают крупные партии продукции своим дилерам по специальной оптовой цене. Правда, подобные компании-производители обычно не договариваются о минимальной цене на розничном рынке (они там и не присутствуют).

Минимальная рыночная цена регистрации домена определялась регистраторами на основе анализа возможной себестоимости проведения транзакций по фиксации права администрирования и по дальнейшему сопровождению прав администратора на домен с учетом возможных рисков. Ведь регистратор не должен работать в убыток. Однако компании, для которых регистрация доменов не

является основным источником прибыли, могут себе позволить сделать эту часть своего бизнеса убыточной (бесплатные домены), зарабатывая больше на других услугах, по отношению к которым регистрация домена является сопутствующей.

Тут уместно привести пример из области страхового бизнеса (где, кстати, тоже встречаются соглашения о минимальной цене полиса по тем или иным видам страхования). Крупные страховые компании могут себе позволить страховать некоторые риски клиентов в убыток. Расчет здесь делается на то, что клиент, застраховавший по минимальной цене один риск, захочет приобрести другое, «пакетное» предложение, которое, напротив, приносит компании высокую прибыль.

Так что неверным будет считать договорное ограничение минимальной цены для розничной услуги исключительно сговором, направленным на получение сверхприбыли за счет доверчивых клиентов. Наоборот, такое соглашение могло бы послужить созданию стабильного рынка, противодействуя демпингу со стороны крупных компаний и монопольному захвату рынка. Однако на доменном рынке .ru в отсутствие реальных рычагов регулирования и при бездействии Координационного центра вышло иначе.

Отсутствие регулирующего механизма может привести к тому, что его предоставит государство. Логика здесь такова: если стоимость регистрации доменов упадет практически до нуля, все сколько-нибудь привлекательные доменные имена рискуют оказаться в руках игроков, которые профессионально занимаются доменным бизнесом. Они имеют большой опыт и технические инструменты, позволяющие им быстрее реагировать на появление новых имен по сравнению с рядовыми розничными покупателями прав администрирования. В результате снижения стоимости розничной регистрации крупнейшие профессионалы смогут расширить поле своей игры, вытеснив мелких домейнеров. В ситуации, когда рыночные механизмы не позволяют разумным образом отрегулировать распределение общедоступного ограниченного ресурса — доменного адресного пространства —

и рядовые потребители оказываются в заведомо проигрышном положении (а им в лучшем случае придется выкупать домены на вторичном рынке по спекулятивной цене), логичным является введение государственного регулирования.

В какой форме возможно такое регулирование? Хорошим примером служит распределение радиочастот в эфире. Радиоэфир — общее пространство. Для нормального обмена информацией необходимо закреплять радиочастоты за тем или иным вещателем (передатчиком). При этом, очевидно, сама по себе радиочастота ничего не стоит и технически вещание на данной частоте требует лишь наличия передатчика. Порядок в эфире регулируется путем выделения частот заинтересованным лицам особым государственным органом (комиссией при министерстве, например) и при помощи последующего контроля за использованием частот, также проводимого государством. Сходным образом можно распределять и домены, если рыночный путь оказался неподходящим.

Как сложится ситуация — покажет время. Как бы то ни было, в течение 2007–2008 годов домен RU продемонстрировал удивительный рост и продолжает бурно развиваться. Так, осенью 2007 года в нем было зарегистрировано миллионное доменное имя второго уровня, а уже к лету 2008 года прирост регистраций составил более 200 тысяч.

Глава 6

Страны, коды и домены

- ☐ Лингвистические фокусы
- ☐ Трудности управления
- ☐ Ликвидация

Национальными доменами называют двухбуквенные домены первого уровня, соответствующие кодам, обозначающим государства. Например, RU — национальный домен России; DE — национальный домен Германии; UZ — национальный домен Узбекистана.

ICANN называет национальные домены Country Code Top Level Domain (в ходу аббревиатура ccTLD). К доменам ccTLD относят не только домены общепризнанных государств мира, но и другие географические домены, обозначающие территории, автономии или объединения государств, например домен Евросоюза — EU. То есть ICANN по традиции проявляет дипломатическую гибкость, допуская исключения из правил. Впрочем, подавляющее число ccTLD, а их на начало 2008 года зарегистрировано 253, выделено именно полноценным государствам.



С давних пор при создании и дальнейшем сопровождении национальных доменов ICANN принимает во внимание международный стандарт ISO 3166, recommending двухбуквенные коды стран. Стандарт ISO 3166 используется не только ICANN и, конечно, не создавался специально для того, чтобы верно распределять домены. Собственно, он сформировался еще в конце 60-х годов XX века, то есть до возникновения Интернета. Именно благодаря своей долгой истории и очевидной независимости от ICANN стандарт ISO 3166 является очень удобным инструментом, позволяющим в нужный момент «переводить стрелки» в сторону от ICANN в случае возникновения конфликтных ситуаций.

Некоторые домены, относящиеся к категории национальных, ICANN распределила без привязки к стандарту ISO 3166 или не в полном соответствии с этим стандартом. Примером служит домен UK, в свое время выделенный Великобритании. В стандарте ISO Великобритания соответствует обозначению GB; домен первого уровня GB в настоящее время (2008 год) не используется и находится в списке зарезервированных имен. Угодил GB в этот список, не выдержав конкуренции с бурно развивающимся доменом UK. Проанализировав ситуацию с двумя национальными доменами Великобритании, ICANN решила сохранить один — хоть и нестандартный, но лидирующий.

В случае с доменом СССР SU (о нем подробно рассказывалось в главе 4) стандарт ISO помог прекратить очередной бурный конфликт: домен оставили в реестре, мотивируя решение тем, что обозначение SU сохраняется в стандарте.

КСТАТИ



Вообще же, ICANN старается отражать изменения на политической карте мира в системе национальных доменов. Правило «Нет государства — нет домена» скорее работает, чем дает возможность существовать исключениям.

Всякий домен первого уровня — ценнейший ресурс. Национальные домены не исключение. А за ценный ресурс всегда идет борьба той или иной интенсивности.

При этом Интернет на практике регулируется не международными соглашениями уровня резолюций ООН, а решениями корпорации ICANN. Поэтому ошибочно полагать, что национальный домен обязательно находится в управлении правительства того государства, которому выделен. Напротив, национальными доменами по большей части управляют либо негосударственные общественные организации, либо коммерческие структуры, либо иностранные (по отношению к соответствующему государству) бизнесмены.

Одна из причин такой ситуации кроется в том, что решение о назначении администратора национального домена принимает ICANN на основании рассмотрения заявок заинтересованных сторон. Так что некоторым зубастым акулам ИТ-бизнеса удалось получить в управление национальные домены ранее, чем правительства стран, названиям которых соответствуют домены, поняли, что такое Интернет.

Так произошло с доменом NU. Согласно стандарту ISO 3611 (как мы разобрались, от него можно, пусть и с небольшими оговорками, отталкиваться при определении букв национального домена) домен NU соответствует маленькому островному государству Ниуэ, расположенному в Тихом океане. По данным Центрального разведывательного управления США, на конец 2007 года в Ниуэ проживает около тысячи пользователей Интернета. Однако домен NU фактически находится в управлении у американского бизнесмена Уильяма Семича (J. William Semich).

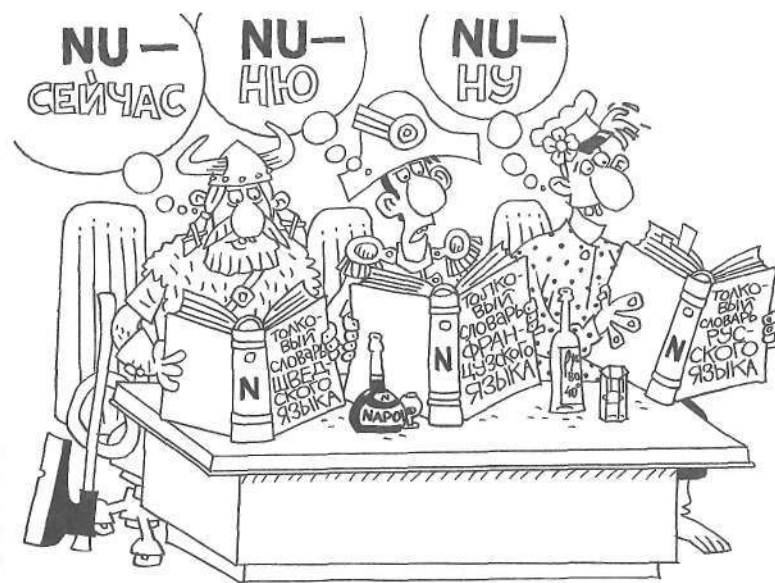
Лингвистические фокусы

По состоянию на 2008 год формальным администратором домена NU является организация под названием Общество пользователей Интернета Ниуэ (Niue Internet Users Society), которая делегировала компании Семича полномочия по техническому обеспечению функционирования домена. На практике же именно техническая служба занимается регистрацией новых доменов в NU и получает основную прибыль от этой деятельности, причем прибыль немалую.

Казалось бы, кому могут быть интересны имена в домене маленького Ниуэ? Очень многим. Виной всему один лингвистический эффект, актуальный не только для домена NU, но и для всех доменов первого уровня.

Дело в том, что *ни* на нескольких распространенных в развитых странах языках обозначает весьма привлекательные понятия. Например, в скандинавских языках (шведском, норвежском и датском) *ни* обозначает «сейчас», что само по себе полезно в качестве маркетингового хода, использующего интернет-адрес для продвижения бренда.

Более того, *ни* в переводе с французского — это еще и «ню», то есть «обнаженный». При этом само понятие «ню» интернациональное и легко воспринимается во многих современных языковых традициях, в том числе в русской.



Так что удачно выпавшие маленькому государству в Тихом океане две буквы NU оказались очень ценны для глобального Интернета и обрели популярность в скандинавских странах, Европе

и Латинской Америке. Конечно, большинство пользователей Интернета вряд ли слышали о Ниуэ и никогда там не побывают, но моментальная глобальная доступность в виртуальной географии сыграла свою роль, сделав национальный домен гораздо популярнее самого государства.

Неудивительно, что, разобравшись в ситуации, правительство Ниуэ принялось судиться с бизнесменом Семичем, требуя передать государству прибыль от регистрации имен в NU (эти деньги стали бы заметным вливанием в бюджет острова). Впрочем, к концу 2007 года Семич продолжал контролировать денежные потоки от домена в «стиле ню».

Созвучие национальных доменов с какими-то словами или аббревиатурами — черта, характерная не только для домена Ниуэ. Правда, большое значение подобные лингвистические фокусы приобретают лишь в тех государствах, где местный Интернет не развит и поэтому национальный домен оказался не востребован для использования по прямому назначению. Установив либеральные правила регистрации имен в своих доменах, некоторые из этих государств получают неплохую прибыль от продажи прав администрирования доменов, даже если никакое языковое созвучие с национальным доменом не связано.

КСТАТИ

Не так далеко от Ниуэ находится островная автономия Токелау (под управлением Новой Зеландии), которой выделен домен первого уровня TK. Маленькое государство успешно извлекает из этого домена существенную часть своего бюджета. Механизм довольно прост: компания голландского бизнесмена Йооста Цурбиера предлагает всем желающим бесплатно зарегистрировать домен в зоне .tk для размещения под этим доменом веб-сайта. Правда, бесплатная регистрация предполагает согласие на публикацию рекламы, а функционирование домена организовано таким образом, что в дальнейшем вместе с веб-сайтом показывается коммерческая реклама. Доходы от размещения рекламы получают и бизнесмен Йоост Цурбиер, и острова Токелау.

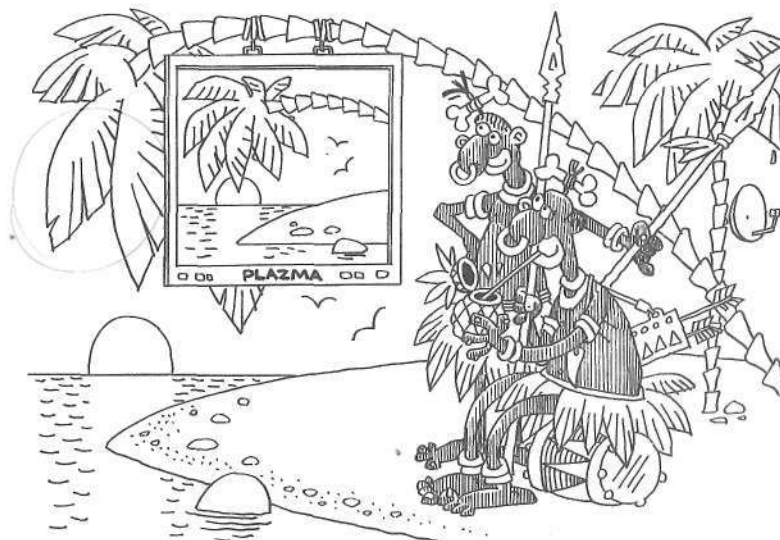
Классическим образцом использования для извлечения прибыли созвучия национального домена с узнаваемой аббревиатурой

остается домен TV. Несложно догадаться, что с формальной точки зрения за доменом TV стоит очередное микроскопическое островное государство в Тихом океане. Это государство Тувалу.

Тувалу занимает территорию около 26 квадратных километров. В 2008 году численность населения этой страны, по данным Центрального разведывательного управления США, составила около 12 тыс. человек.

Но одно дело — несколько островов в Тихом океане, получивших независимость от Великобритании в 1978 году, и совсем другое — аббревиатура TV, обозначающая телевидение и отлично узнаваемая во всем цивилизованном мире. Поэтому неудивительно, что домен TV довольно быстро оказался в управлении компании VeriSign — одного из крупнейших участников интернет-рынка.

За использование своего национального домена Тувалу получает лицензионные отчисления, которые составляют заметную часть государственного бюджета. Например, по данным аналитической службы ЦРУ, в 2006 году отчисления по домену TV в бюджет Тувалу составили более \$2 млн.



Домен TV официально и весьма жестко позиционируется компанией VeriSign как домен, связанный с телевидением и развлечениями. Например, на сайте официальной регистратуры доменов .tv (www.tv) телевидение на первом месте, а найти упоминания Тувалу непросто. Развитие домена Тувалу в направлении телевидения зашло так далеко, что многие пользователи Интернета полагают, будто домен TV был специально создан для мировых телекомпаний и популярных телепередач. Зарегистрировать домен в TV может любой желающий, а стоимость регистрации начинается от \$24,95 (2008 год).

В отличие от крохотного Тувалу, территория Туркмении составляет более 488 тыс. квадратных километров. Туркменский домен также неплох: аббревиатура ТМ — аналог интернационального обозначения знаков, зарегистрированных в качестве торговой марки.

В Туркмении Интернет пока не развит, поэтому и национальный домен ТМ, исторически более привлекательный для раскрученных торговых марок крупных компаний, чем для национального туркменского Интернета, администрирует коммерческая компания, базирующаяся в Великобритании. Домены второго уровня в зоне .tm регистрируются сразу на десять лет, а минимальная стоимость регистрации — \$1000, что немало, особенно по туркменским меркам.

Туркмения и Тувалу не одиноки: компанию им составляет, например, Молдова, чей национальный домен MD длительное время позиционировался как домен, привлекательный для организаций, так или иначе относящихся к медицине. Этот эффект вызван тем, что в англоязычной традиции аббревиатуру MD — Medical Doctor — обычно используют в качестве обозначения ученой степени квалифицированного практикующего врача.

Микронезия — очередное в нашем повествовании карликовое островное государство в Тихом океане. Микронезии достался домен FM, весьма привлекательный для радиостанций и радиовещательных компаний. Легко догадаться, что домен FM неавызовно позиционируется не как домен Микронезии, а как «Great Sounding

Web Address» (слоган регистратора FM компании dotFM), что в несколько вольном переводе означает: «Отлично звучащий адрес в вебе». То есть доменное имя весьма прозрачно увязывается с радиоиндустрией. И в этом нет ничего удивительного: от интернет-рынка Микронезии вряд ли стоит ожидать бурного роста, а вот всемирный рост популярности звукового вещания через Интернет (интернет-радио) палицо. Поэтому и маркетинг у домена FM соответствующий.

Ситуация с FM еще раз подтверждает фундаментальный тезис: был бы национальный домен в руках, а рынок для сбыта регистраций найдется в Глобальной сети.

Этот же тезис подтверждает и другой национальный домен — CD, который достался Демократической Республике Конго в качестве замены национальному домену ZR. Дело в том, что это африканское государство некоторое время (как раз тогда, когда распределялись национальные домены) называлось Заир. Позже в результате революций и радикальных государственных преобразований, типичных для африканского континента, на политической карте вместо Заира появилась Демократическая Республика Конго с очень привлекательным доменом CD.

КСТАТИ



Не следует путать Демократическую Республику Конго и Республику Конго: это два разных государства, которые, правда, имеют общую границу. Республике Конго с доменным именем не повезло: в ближайшие десятилетия домен CG вряд ли станет столь же популярным, как CD.

Аббревиатуру CD аудитория Интернета охотнее связывает с компакт-диском, чем с африканским государством, ранее известным как Заир. Именно поэтому национальный домен CD позиционируется как домен для веб-сайтов и других ресурсов Сети, так или иначе связанных с музыкальной и звукозаписывающей индустрией, с производством и распространением компакт-дисков. Несомненно, деятельность по развитию домена CD в этом направлении коммерчески выгодна для регистраторов.

Трудности управления

Как я уже упоминал выше, национальными доменами различных государств управляют самые разные общественные, коммерческие, некоммерческие и государственные организации, а иногда и фактически частные лица. Впрочем, в большинстве случаев администраторы крупных национальных доменов — это частные компании. Также заметное число администраторов — это подразделения научных и образовательных учреждений (тут ощущается влияние среды, в свое время породившей Интернет).

Управление национальными доменами осуществляется на основании самых разных правил. Так, в ряде национальных доменов действуют либеральные правила регистрации, не накладывающие серьезных ограничений на регистрируемые имена (такие домены часто называют открытыми). Другие национальные домены, наоборот, являются закрытыми: правила регистрации в них весьма строги.

Какие ограничения могут действовать в национальном домене? Оказывается, самые изощренные. Ведь доменные имена — ресурс ценный и весьма дефицитный: зарегистрировать два одинаковых имени невозможно. А распределение дефицитных ресурсов всегда порождает конфликты. Конфликты же, в свою очередь, порождают ограничения. Самым банальным является ограничение на максимальное количество доменов, которые может зарегистрировать одно лицо (такие ограничения действуют в национальных доменах Норвегии и Кипра). Это ограничение можно ослабить, сузив круг лиц, которым позволено регистрировать домены. Например, во многих национальных доменах регистрировать имена могут только резиденты соответствующих доменов стран. Иногда домен может зарегистрировать только юридическое лицо.

Довольно популярна политика принудительного разграничения регистраций доменных имен по доменам второго уровня. То есть рядовым пользователям позволено регистрировать домены только третьего уровня внутри зон, формируемых по назначе-

нию регистрируемого домена. Типичный пример: коммерческие компании принуждают регистрировать имена в зоне .com.cctld (где ccTLD — национальный домен).

Впрочем, практика показывает, что чем более закрытым является домен, тем медленнее он обычно развивается.

Так, китайский национальный домен CN после либерализации правил регистрации, которые в том числе разрешили иностранцам регистрировать домены, резко вырос и в 2007 году набрал 6,7 млн доменов, в то время как в 2005 году число регистраций в домене CN составляло около одного миллиона.

Пытаясь сделать регистрацию доменов максимально справедливой, некоторые администраторы идут на разнообразные ухищрения. Например, в домене Чили вновь поступившая заявка на доменное имя сперва публикуется на сервере регистратора, где доступна в течение 30 дней. Если за этот период поступает конкурирующая заявка на тот же самый домен, то решение по использованию имени принимается арбитром на основании анализа поступивших заявок. Впрочем, большинство регистраторов не мудрствуют и действуют проще, передавая право администрирования домена первому обратившемуся.

С другой стороны, при появлении новых доменов традиционно вводятся периоды так называемой приоритетной регистрации. В это время преимущественное право регистрации доменов предоставляется ограниченному (по тому или иному критерию) кругу лиц, например владельцам торговых марок или жителям региона, для которого предназначен домен. После того как те, кто действительно хотел заполучить по праву причитающиеся имена в новой зоне, реализовали свои права, регистрация открывается для всех желающих.

В домене Европейского Союза EU приоритетная регистрация продолжалась несколько месяцев (с начала декабря 2005 года по февраль 2006 года), что, впрочем, не спасло домен от весьма крупного скандала, случившегося уже через год. Захватчики доменов,

воспользовавшись несовершенством правил регистрации, сумели получить статус регистраторов и перехватить несколько десятков тысяч привлекательных доменов. В итоге администратору домена EU, компании EURid, пришлось постфактум отозвать регистрации более 70 тыс. доменов .eu — неслыханный провал для столь важного сегмента адресного пространства.

Несмотря на популярность рыночных методов во многих отраслях IT-бизнеса, регистрация имен в национальных доменах не всегда платная. Так, в домене Эстонии EE регистрация имен производится бесплатно (2008 год). Разумеется, чтобы список всех сколько-нибудь привлекательных имен в домене EE не исчерпался слишком быстро, потребовалось ввести строгие ограничения. Так, право администрирования домена второго уровня в EE может получить только организация, зарегистрированная в Эстонии. Но вполне вероятно, что подобный «интернет-коммунизм» в отдельно взятом национальном домене скоро закончится и за регистрацию доменов EE введут ежегодную плату.

КСТАТИ



Бесплатная регистрация доменов должна сопровождаться строгими проверками и контролем, иначе обязательно найдутся предприимчивые интернет-пользователи, которые с помощью методов автоматизированной подачи заявок на домены моментально застолбят тысячи интересных имен. Это важно не только для доменов второго уровня, но и для других зон. Например, ситуация с неверным управлением бесплатной зоной .com.ru чуть не сыграла с ней злую шутку, когда все ее «разумные» домены могли оказаться в руках одного активного киберсквоттера.

Национальные домены — одна из самых быстроразвивающихся областей в современном Интернете. Как мы уже видели, для бурного развития национального домена вовсе не обязательно, чтобы соответствующее ему государство являлось передовым в области информационных технологий. Хитрость в том, что Интернет — глобальное явление, в котором своя география, свои расстояния и свои мерки уровня развития. Оказывается, достаточно нацио-

нальному домену карликового государства попасть в руки к опытному бизнесмену, как число зарегистрированных в этом домене имен легко превысит число граждан «государства-донора».

Впрочем, развитие интернет-технологий, конечно же, способствует росту национальных доменов. Традиционный лидер по числу регистраций — домен Германии DE, в котором зарегистрировано свыше 11 млн доменов (2008 год). Он настолько популярен, что по числу регистраций среди всех доменов первого уровня уступает только домену общего пользования COM. Германия считается одним из европейских лидеров по численности населения, охваченного Интернетом. При этом численность населения Германии велика. Эти факторы вносят свою лепту в популярность национального домена. Поддерживают популярность и либеральные правила регистрации имен в DE. Так, при наличии представителя на территории Германии домены .de могут регистрировать иностранные граждане. В именах доменов, помимо символов латиницы, разрешены немецкие умляути. Немаловажную роль играет развитый вторичный рынок доменов, который поддерживает крупнейший участник этого рынка — компания Sedo.



Интересно, что домен COM, не являющийся национальным и с большим отрывом занимающий первую строку в мировом рейтинге по числу регистраций, стал причиной крайней непопулярности национального домена США. Последний настолько малоизвестен, что многие пользователи Интернета вообще не подозревают о его существовании. Между тем США имеют в своем распоряжении домен US. Однако жители Соединенных Штатов настолько привыкли считать весь Интернет собственностью своего государства, что предпочитают регистрировать свои сайты в зоне .com и других доменах первого уровня общего пользования, начисто игнорируя самый «патриотичный» домен. В 2008 году число регистраций в домене US приближалось к 1,3 млн (сравните с 11 млн доменов .de).

Ликвидация

Национальные домены появляются и исчезают. Во многих случаях за этим увлекательным процессом стоят соответствующие изменения политической карты мира. Например, после того как войска НАТО и США разрушили европейское государство Югославия, под виртуальным ударом оказался и его национальный домен YU.

Некоторое время вокруг домена YU велась дискуссия о том, не оставить ли его в качестве единого виртуального пространства для государств, ранее входивших в состав Югославии, а после раздела обретших независимость.

Сложно сказать, в какой степени на судьбу домена YU повлияла близость ICANN (главного органа «саморегулирования» в подобных спорах) к правительственным структурам США. Однако было бы довольно странно, если бы военное решение вопроса о существовании Югославии в реальности не повлияло на виртуальную сферу.

Как бы то ни было, в конце 2007 года ICANN приняла решение о ликвидации домена YU. Его решено «разделить» на два: RS (Сер-

бия) и ME (Черногория). А точнее, домены из зоны .yu должны быть перенесены в .rs и .me. На процесс переноса выделено не менее двух лет. После того как домен YU опустеет, его удалят из глобальной DNS.

Важно понимать, что технически домены представлены в Интернете всего лишь записями в специальных базах данных. Что такое удаление домена? С технической точки зрения это изъятие из компьютерной памяти (из базы данных) информации о домене. Правда, в соответствии с иерархической структурой DNS, чтобы домен совсем исчез из Интернета, запись о нем нужно удалить из памяти главного сервера, ответственного за распределение доменов соответствующего уровня. В таком случае спустя некоторое время (что связано с особенностями хранения информации в распределенной DNS) удаленный домен просто исчезнет, и по адресам, которые в нем содержались, уже нельзя будет обратиться.

Основные же технические трудности при удалении доменов первого уровня связаны с тем, что внутри этих доменов может находиться большое количество информационных ресурсов. На них ссылаются другие сайты, существующие в своих доменах. Ссылочная система, позволяющая очень просто с одной веб-страницы сослаться на другую, — основа современного веба. Именно гиперссылки определяют возможности навигации и поиска информации в нем. Если из обращения изъять домен, содержащий тысячи ресурсов, то ранее указывавшие на него ссылки с других сайтов окажутся «пустыми», а точнее, ведущими в никуда.

Казалось бы, если ресурсы, размещенные под доменами удаляемой зоны, заблаговременно переносятся в другой домен, проблему со ссылками можно решить, изменив соответствующие ссылки таким образом, чтобы они указывали на новый адрес ресурса. Однако реализовать такую схему в реальном Интернете очень непросто.

Дело вот в чем. Ссылки, ведущие на ресурс, которому предстоит переезд, расположены на других веб-сайтах. И вовсе не обязательно администратор переезжающего ресурса имеет возможность

как-то повлиять на эти ссылки. Более того, администратор может вообще не знать о части ссылок, не говоря уж о существовании эффективных механизмов изменения адресов.

На практике изменить содержание множества внешних ссылок в вебе можно только одним способом: для начала создается адрес в новом домене и туда переносится все содержимое веб-ресурса; затем на исходном сайте размещается особым (иногда довольно сложным) образом подготовленное сообщение о том, что ресурс доступен по новому адресу. После этого владельцу меняющего адрес ресурса остается надеяться, что администраторы, следящие за внешними ссылками, узнают об изменении адреса и исправят ссылки. Однако далеко не за всеми ссылками тщательно следят. И даже для того, чтобы изменить ссылки, находящиеся «под наблюдением», потребуется время.

Надо заметить, что речь пока шла лишь о ссылках в вебе. Между тем Интернет — это не только веб, и на ресурсы по имени домена могут ссылаться не только веб-страницы. Так, например, адреса электронной почты тоже включают в себя имена доменов, и в случае удаления домена почтовые ящики окажутся недоступны для корреспонденции. Все это усугубляет сложность изъятия доменов «из обращения».

Именно поэтому удаление всякого обитаемого домена первого уровня — болезненный процесс, требующий длительного времени для изменения ссылочной структуры.

Национальные домены — самый бурно развивающийся сегмент системы адресации Интернета. Одни национальные домены служат для развития Сети в соответствующих государствах; другие, напротив, способствуют не столько развитию Интернета, сколько пополнению бюджета «титularного» государства; а некоторые и вовсе, по сути, продаются иностранным бизнесменам. Одни из самых жарких доменных войн разгорались вокруг некоторых национальных доменов либо внутри них.

Тем не менее самый населенный домен верхнего уровня — COM — не является национальным, как и многие другие древнейшие домены, например NET, ORG. Они возникли на заре глобального Интернета и живут своей жизнью. Более того, за последние годы в полк так называемых доменов общего пользования прибыло изрядное пополнение. По-английски домены верхнего уровня, не относящиеся к категории национальных, называются Generic Top Level Domains (gTLDs). Мы (не забывая о популярном русскоязычном термине «домены общего пользования») будем называть их доменами общего назначения. Выбор терминологии объясняется тем, что среди доменов gTLDs есть и домены весьма ограниченного использования, например домен MIL.

Глава 7

В первых доменных рядах

- ☐ Живые древности
- ☐ Новые времена и широкий брендинг
- ☐ Первые дополнения
- ☐ Виртуальность верхнего уровня
- ☐ Нашли спонсора
- ☐ Процедурный вопрос

Изначальных доменов DNS восемь: COM, NET, ORG, GOV, INT, EDU, MIL, ARPA. Почему? Потому что именно такой набор доменов первого уровня, предназначенных для пользователей Интернета, был введен в строй вместе с самой DNS в 1984–1985 годах.

Принцип формирования списка ясен: каждой из масштабных областей деятельности человечества достался свой домен. Коммерция, сети телекоммуникаций, некоммерческие объединения, власть, международная деятельность, образование и наука, ведение войн и подготовка к ним — все получили по домену.

Особняком стоит домен ARPA. ARPA (Advanced Research Project Agency) — так раньше называлось Агентство перспективных разработок Министерства обороны США, в котором создали Интернет (в настоящее время оно называется DARPA — Defence Advanced Research Project Agency). Поэтому неудивительно, что создатели Интернета ввели собственный домен, который служил чисто техническим целям. Служит он им и сейчас, играя важную роль в малоизвестных среди рядовых пользователей внутренних протоколах организации информационной структуры Интернета.

Живые древности

Домен COM предполагалось использовать для коммерческих организаций всего мира. Сейчас он безоговорочный лидер по числу регистраций. Более того, во времена первого интернет-бума, случившегося в конце 1990-х годов, домен COM стал синонимом развития Интернета.

КСТАТИ



Например, новые интернет-компании, возникавшие во время интернет-бума столь же быстро, как и пузыри на городских лужах во время ливня, получили в профессиональной среде жаргонное название — «дот-комы». Это слово образовано от английского «dot COM», то есть «точка COM» в буквальном переводе. Причиной рождения термина явилось то, что новые

проекты обычно регистрировали имя в домене COM, и, как следствие, адрес сайта, если его произносить вслух, обязательно заканчивался словосочетанием «точка COM». Так что первый интернет-бум, закончившийся грандиозным провалом и кризисом рынка интернет-инвестиций, часто называют «бумом дот-комов».

Домен COM не утратил лидирующего положения и сейчас. По-прежнему именно в этом домене регистрируют адреса многие новые интернет-компании, ориентированные на западный или общемировой рынок. Популярен домен COM и у частных пользователей, размещающих в нем свои персональные сайты. Однако за длительное время существования домена COM все сколько-нибудь краткие и звучные имена в этой зоне оказались заняты. Более того, к началу 2008 года домен COM и вовсе исчерпал свободные четырехбуквенные сочетания: были зарегистрированы даже сочетания букв, представляющие собой полную абракадабру, например `xvqg.com`. «Словарные» домены длиной в четыре буквы закончились многим ранее.



КСТАТИ



Интересно, что первые в истории зоны .com четырехбуквенные домены `.ccur.com` и `.quad.com` зарегистрированы еще в 1986 году и являются одними из самых старых доменов Интернета. Таким образом, на то, чтобы в самой популярной зоне закончились четырехбуквенные имена, потребовалось 22 года. А всего возможно 456 976 вариантов четырехбуквенных доменов.

Домен NET изначально планировали для размещения ресурсов компаний и организаций, связанных с функционированием Сети и телекоммуникациями вообще. Однако довольно скоро регистрация в нем стала свободной, то есть теперь зарегистрировать домен NET может всякий желающий, вне зависимости от его связи с сетями и телекоммуникациями.

КСТАТИ



Интересно, что среди русскоязычных пользователей Интернета домен NET приобрел дополнительную привлекательность благодаря его созвучию со словом «нет». Ситуация в уменьшенном масштабе копирует положение дел с доменами NU или TV.

Несмотря на то что значение домена NET оказалось размытым, в нем, как и ранее, часто размещают свои сайты интернет-провайдеры или рабочие группы, связанные с телекоммуникациями.

Домен ORG предназначался для сайтов некоммерческих организаций, общественных объединений. Можно сказать, что по назначению он используется и сейчас, так как формально общественная организация может состоять из одного человека — администратора домена. Так что регистрировать имена в ORG позволено любому желающему. Но этот факт не мешает действительно крупным общественным, международным организациям размещать свои веб-сайты под доменами в зоне ORG, например, сайт ООН <http://un.org>.

Тремя перечисленными доменами: COM, NET, ORG — исчерпывается список действительно свободных для регистрации древнейших доменов. Дело в том, что домены GOV, MIL, EDU, INT, хоть их

иногда также называют доменами общего назначения (общего пользования), являются закрытыми, специальными.

Так, домен GOV предназначен для правительственных структур США, и только для них. Несмотря на глобальную доступность Интернета, размещать ресурсы в домене первого уровня GOV позволено далеко не всему миру. Примерами адреса .gov служат адреса NASA — .nasa.gov или ЦРУ — .cia.gov.

Аналогично устроен домен MIL. Здесь регистрируют только учреждения, организации и формирования, прямо связанные с оборонным ведомством США. Таков, например, центральный сайт пресс-службы BBC США — www.af.mil.

Домен EDU используется образовательными учреждениями США. Распределение имен контролирует правительственное агентство. Основную массу адресов в домене EDU занимают веб-сайты и другие ресурсы университетов и колледжей США.

Домен INT создан для международных организаций. Это единственный из изначальных специальных доменов, в котором возможна регистрация имени иностранной по отношению к США организации. Регистрацией ведаёт одно из подразделений ICANN, а чтобы получить в распоряжение имя в INT, организации-соискателю нужно представить множество официальных бумаг. Пример адреса в .int: www.esa.int — сайт Европейского космического агентства.

Новые времена и широкий брендинг

В начале 1980-х годов казалось, что нескольких доменов верхнего уровня общего назначения хватит навсегда. Ну, если не навсегда, то очень надолго. Не прошло и двух десятков лет, а ситуация изменилась настолько, что потребовалось вводить новые (причем не национальные) домены первого уровня.

Причиной появления новых доменов первого уровня (подчеркну, что речь сейчас идет не о национальных доменах) явился

вовсе не дефицит адресного пространства в существовавших ранее доменах, как можно подумать. Дефицита не было и нет. Даже если бы он и возник, его можно было бы легко побороть, используя домены третьего уровня. Более того, против «теории дефицита» свидетельствует тот факт, что короткие четырехбуквенные домены даже в самом «населенном» домене COM исчерпались только в 2008 году.

Дополнительные домены первого уровня ввели потому, что доменное имя стало мощным инструментом продвижения в массовое сознание тех или иных брендов. А во многих случаях доменное имя и есть бренд. Конечно же, домен первого уровня, обязательно входящий в состав имени, придавал бренду определенный оттенок. А раз так, то возникло желание чуть добавить индивидуальности адресному пространству, наделив его более детальной структурой, подходящей для продвижения с доменными именами отдельных секторов бизнеса и некоммерческой деятельности. Тем более что значение доменов COM, NET, ORG довольно сильно размылось. А кроме того, ICANN нужно было поддерживать развитие системы доменных имен, за которой, как вагоны за локомотивом, тянется весь Интернет.

Таким образом, в настоящее время развитие адресной системы Интернета, а в особенности системы доменных имен, в существенной мере определяется коммерческими интересами мирового бизнеса. Он не обязательно связан с интернет-технологиями напрямую, но использует их в собственных интересах. Поэтому система доменных имен интенсивно развивается в «ширину», если можно так выразиться, то есть путем увеличения «горизонтального» разнообразия.

Разобраться с особенностями коммерциализации доменного пространства можно на простом примере. Не так давно ICANN ввела домены верхнего уровня TRAVEL и MOBI. Первый предназначен для сайтов туристических фирм и агентств, связанных с путешествиями (то есть для коммерческих компаний); второй — для сайтов, ориентированных на использование мобильных средств коммуникации, прежде всего сотовых телефонных аппаратов.

Если к вопросу развития адресного пространства подходить с точки зрения только интернет-технологий, то ничто не мешало бы ввести домены .travel.com и .mobi.net (имена условные) и развивать туристические и «мобильные» сайты в этих доменах (третьим уровнем). Однако с точки зрения технологий брендинга, направленных на широкую аудиторию, а не только на технически продвинутых пользователей Интернета, применение в бренд дополнительных «сущностей» .com и .net ухудшало бы узнаваемость бренда.

Более того, в ситуации с использованием доменов третьего уровня компании, удачно разместившие свои сайты в домене уровня выше (второй уровень), получали вполне очевидное для маркетолога преимущество: домен вида .лучшая-компания.com воспринимался бы аудиторией как более общий, более весомый бренд по сравнению с сайтом внутри .travel.com.

Итак, коммерциализация Сети потребовала новых доменов первого уровня. В 2000 году ICANN инициировала процесс их добавления в глобальную DNS. Для выбора новых доменов была предложена довольно непростая процедура, начинавшаяся с подачи заявок на создание доменов первого уровня заинтересованными сторонами.

Заявки могли подавать и организации, и частные лица. В заявке, помимо предлагаемого имени домена и описания его назначения, требовалось указать причины введения нового домена, изложить планируемые принципы регистрации имен второго уровня. Кроме того, чтобы началось рассмотрение заявки, в большинстве случаев к ней нужно было присовокупить весомый денежный взнос (\$50 000).

КСТАТИ



Для чего потребовался денежный взнос? Вряд ли для обогащения руководства ICANN (слишком маленькая сумма). Взнос играл роль имущественного ценза, дающего некоторые гарантии серьезности намерений, стоящих за заявкой. Ведь если бы

взнос не взимался, ICANN просто завалили бы тысячи заявок на введение новых доменов от пользователей Интернета, желающих проявить свою «креативность».

Итак, в рамках первого подхода к введению новых доменов первого уровня ICANN получила 47 заявок от различных организаций. Заявки содержали самые неожиданные доменные имена, начиная от XXX (домен «для взрослых») и заканчивая лаконичным доменом I (единственная буква «i»). Многие заявки пересекались по составу предложений. Так, несколько заявок включали доменное имя INFO, популярностью пользовались SHOP и BIZ.



Естественно, рабочая группа ICANN выбрала несколько наиболее привлекательных предложений. В результате отбора заявок возник серьезный конфликт, так как многие были недовольны процессом. Впрочем, в ходе слушаний в Конгрессе США по вопросам деятельности ICANN представители корпорации в лучших традициях изложили довольно дипломатичное видение

проблемы. Так, по их словам (<http://icann.org/correspondence/roberts-testimony-14feb01.htm>), процесс приема и отбора заявок вообще не являлся «конкурсом», и определение каких бы то ни было победителей не являлось целью процесса, так же как его целью не являлось определение списка доменов первого уровня, которые будут незамедлительно введены в употребление (под управлением заявивших эти домены на конкурс компаний).

Для чего же заявки принимали? Для того, объяснили представители ICANN, чтобы с помощью интернет-сообщества выяснить, какие домены первого уровня можно было бы *без особенного риска* добавить в DNS. То есть, по мнению ICANN, проводился своего рода эксперимент, число участников которого ограничивалось с помощью установления «входной платы» в \$50 000, и резкое недовольство, высказанное некоторыми добровольными участниками эксперимента по поводу его результатов, только удивило руководство ICANN.

Тем не менее уже тот факт, что ICANN заговорила о возможности появления новых доменов верхнего уровня, привел к крупной «войне» вокруг них. Причиной послужило то, что ICANN не обладает статусом, позволяющим ей диктовать требования участникам мирового Интернета. Она может лишь рекомендовать правила игры. Воспользовавшись ситуацией, некоторые крупные интернет-провайдеры из разных стран и регионов решились надавить на ICANN.

Давление оказывалось следующим образом: провайдеры (или связанные с ними организации) самостоятельно учреждали новые домены верхнего уровня и включали их поддержку для своих клиентов, предлагая регистрировать имена. Принципы построения и функционирования DNS позволяют это сделать в достаточно прозрачном для конечного пользователя режиме. Организовав «альтернативный домен», его владельцы приглашали к сотрудничеству регистраторов и принимали другие меры для его популяризации.

В чем здесь давление на ICANN? Да в том, что эта организация не любит конфликтов и предпочитает закреплять в рекомендациях исторически сложившуюся ситуацию. Смелые IT-бизнесмены,

вводя без одобрения ICANN в оборот новые домены первого уровня, считали, что, если новые домены обретут большую популярность, ICANN будет вынуждена узаконить их в полном объеме. В таком случае, исходя из технических особенностей регистрации доменов второго уровня, администратором новой зоны пришлось бы назначить того, кто ее первым учредил и собрал больше регистраций. По крайней мере так полагали зачинщики «самопровозглашения».

Надо отметить, что полагали они так не без оснований. Дело, опять же, в том, как себя позиционирует ICANN. Ведь корпорация, позиционирующая себя в качестве проводника мнения интернет-общественности, должна однозначно реагировать на это мнение. В данном случае выразить мнение предполагалось с помощью бурного роста числа регистраций имен в «самопровозглашенных» доменах. Впрочем, нельзя упускать из виду, что ICANN, «одной рукой» проводя мнение общественности в жизнь, «другой рукой» участвует в формировании этого мнения, умело проводит закулисную работу и подготавливает почву для развития общественного мнения в нужном направлении.

В принципе, главными серверами DNS могут быть те серверы, которые признает таковыми большинство провайдеров, формирующих Интернет. ICANN контролирует главные серверы лишь до тех пор, пока за корпорацией стоит поддержка ключевых участников рынка доступа к Интернету. Однако несложно догадаться, что большинство системообразующих телекоммуникационных компаний пока играют на стороне ICANN, и не только по политическим причинам.

Со своей стороны, ICANN противодействует нелегальному введению новых доменов верхнего уровня, используя в качестве фундамента следующий тезис: принятие практики с простым фиксированием частных инициатив по введению доменов первого уровня приведет к краху единообразия DNS, и при этом заинтересованные компании будут бесконтрольно захватывать все сколько-нибудь интересные с точки зрения бизнеса домены первого уровня. Воцарится доменная анархия.

Такая позиция ICANN представляется очень грамотной и практически непробиваемой. Дело в том, что крупным игрокам рынка доступа к Глобальной сети выгодно, чтобы между ними стоял более или менее независимый арбитр — ICANN. А бои без правил, способные привести к полной неопределенности вектора развития доменного рынка, когда каждый «сам себе ковбой» с частными доменами, — наихудший для бизнеса вариант.

Первые дополнения

Итак, ICANN, умело лавируя между довольными и недовольными, опираясь на лидеров мнений и законодателей мод, рассмотрела силами рабочей группы поступившие заявки и в 2001 году приняла решение о введении семи новых доменов верхнего уровня общего назначения: BIZ, INFO, NAME, PRO, COOP, MUSEUM, AERO.

Домены BIZ и INFO представляют собой, условно говоря, развитие маркетинговой модели домена COM.

Домен INFO (от англ. information) позиционируется в качестве пространства для размещения веб-сайтов, рассказывающих о тех или иных товарах, услугах, персонах, а также для сайтов СМИ. Ранее веб-ресурсы подобного назначения традиционно размещались в домене COM либо в национальных доменах.

Домен BIZ (от англ. business) ориентирован на другую категорию пользователей, которым тесно в домене COM: на коммерческие компании и корпорации, плотно увязывающие свое доменное имя с бизнесом как явлением. Размытость восприятия интернет-аудиторией домена COM играет на руку домену BIZ.

Домены INFO и BIZ довольно популярны. Так, в 2007 году INFO насчитывает около 5 млн регистраций, а BIZ — около 1,7 млн. Для сравнения: в домене COM число регистраций превышает 70 млн.

Домены NAME и PRO — шаг навстречу персональным сайтам. Оба домена предназначены прежде всего для частных лиц. При этом

первый, NAME, создан для тех, кто желает зарегистрировать свои имя и фамилию в качестве доменного имени. По задумке, пользователи должны регистрировать имена вида имя.фамилия.name. Впрочем, сейчас в домене NAME возможна регистрация и доменов второго уровня имя.name.

Домен PRO — не простой, а специальный домен для «сертифицированных профессионалов». Основная идея, стоящая за ним, заключается в том, чтобы дать специалистам, которые работают в областях, требующих лицензирования и сертификации, возможность обозначить свою принадлежность к числу профессионалов с помощью доменного имени. Считается, что интернет-адрес в домене PRO будет лишним раз подтверждать легальность практики его обладателя. Вполне ожидаемым образом домен PRO в первую очередь ориентирован на врачей, юристов, бухгалтеров. Для классификации профессий внутри домена PRO созданы домены второго уровня, обозначающие профессиональную принадлежность владельца адреса. Например, для врачей — med.pro, для адвокатов — law.pro. Так, врач может зарегистрировать доменное имя JamesRClarke.med.pro.

Для регистрации имени в PRO, а точнее, в подходящем домене второго уровня администратору домена нужно документально подтвердить, что он обладает официальным правом оказывать услуги в соответствующей области.

Домен COOP — довольно оригинальный и столь же малоизвестный домен верхнего уровня. Он предназначен кооператорам, точнее, кооперативам. Что такое кооперативы? В международной классификации кооперативами называют добровольные объединения людей, созданные с целью совместного ведения хозяйственной деятельности. Решение о регистрации доменного имени в COOP на основании рассмотрения документов принимает компания DotCooperation LLC, управляющая доменом COOP. Помимо членов международных организаций кооператоров, претендовать на имя в домене COOP могут объединения, являющиеся кооперативами по местным законам. То есть, например,

российские товарищества собственников жилья или жилищно-строительные кооперативы могут смело подавать заявки на регистрацию имен в домене COOP.

Другой закрытый домен первого уровня — MUSEUM. Закрытым он (с некоторой долей условности, конечно) называется потому, что зарегистрировать имя в нем может не любое лицо, а лишь тот, кто докажет свою принадлежность к мировому музейному движению. То есть MUSEUM, как несложно догадаться по имени, — это домен для музеев и для тех, кто с ними связан.

Доменом MUSEUM управляет специальная ассоциация, в задачи которой входит и проведение жесткой политики по регистрации доменных имен, включающей тщательную индивидуальную проверку каждой заявки. В будущем администраторы домена планируют создать что-то вроде онлайн-каталога музеев. Например, российские музеи уже могут регистрировать имена в зоне .russia.museum.

Другой домен верхнего уровня с жесткой политикой регистрации — AERO. Он предназначен для авиации и авиационной индустрии, а зарегистрировать имена в нем могут те, кто способен подтвердить свою принадлежность к этой сфере (при этом регистрация доступна и физическим лицам, а не только организациям). Внутри домена AERO установлена дополнительная иерархия из зарезервированных доменов второго уровня. Она призвана помогать тематической рубрикации домена, облегчающей поиск нужного ресурса. Показателен пример с веб-сайтом российского международного аэропорта «Шереметьево». В домене RU сайт этого аэропорта расположен по простому адресу sheremetyevo-airport.ru, в то время как адрес sheremetyevo.ru занят транспортной компанией. В домене AERO за аэропортом «Шереметьево» оказывается автоматически и без всяких споров закреплен адрес svo.aero, построенный на основе уникального международного кода аэропорта.

Домены верхнего уровня с жесткой политикой регистрации, направленные на один, достаточно строго определенный сектор экономики, бизнеса или некоммерческой деятельности, — это,

помимо систематизации представления информации в Интернете, попытка придать DNS дополнительный статус, позволяющий использовать имя домена в качестве одного из элементов авторизации ресурса. Сам механизм выдачи адресов (доменных имен) в зоне .museum дает некоторые дополнительные гарантии посетителю сайта, подтверждая, что сайт по данному адресу действительно является сайтом музея (или имеет прямое отношение к музеям). Конечно, полной уверенности быть не может (потому что сама DNS, с точки зрения конечного пользователя, вовсе не является защищенной), но ситуация лучше, чем, скажем, в домене COM, где часто ни о владельце домена, ни о реальном состоянии сайта рядовому посетителю ничего не известно.

КСТАТИ



На идее о дополнительной защите пользователей Интернета от различных угроз виртуального пространства с помощью специальных доменов первого уровня базируется и предложение о введении доменной зоны для банков и финансовых структур. Для банков подошла бы зона BANK или SAFE. Доменные имена в новой зоне должны выдаваться только банкам и авторизованным финансовым организациям после документального подтверждения статуса. Пока ICANN не отреагировала на предложение (2008 год).

«Банковский домен» мог бы помочь бороться с фишингом, то есть с похищением реквизитов доступа к банковским счетам у клиентов банков с использованием поддельных сайтов, которые имитируют работу с банковской системой. Пользу от домена сложно отрицать, однако нужно иметь в виду, что уже довольно давно отработаны другие методы (криптографические) защиты банковских сайтов от подделки. Эти методы также позволяют авторизовать доменное имя без привязки к специальному домену первого уровня.

При этом понятно, что престижный «банковский домен», да еще и имеющий имидж сегмента Сети с «повышенной безопасностью», — лакомый кусочек для регистраторов и администраторов домена.

Все перечисленные новые домены первого уровня, введенные ICANN (BIZ, INFO, NAME, PRO, COOP, MUSEUM, AERO), уже внесены

в DNS и функционируют несколько лет, а регистрация в них открыта.

Проследив за реакцией интернет-общественности и за развитием бизнеса вокруг новых доменов, руководство корпорации ICANN поняло, что новые домены верхнего уровня — это хорошо. Поэтому началась выработка систематических правил, в соответствии с которыми можно подавать в ICANN заявки на введение новых доменов первого уровня. Более того, уже в 2005 году стало очевидно, что ICANN не собирается останавливаться, и доменов первого уровня, предназначенных для тех или иных областей человеческой деятельности, будет еще больше.

Виртуальность верхнего уровня

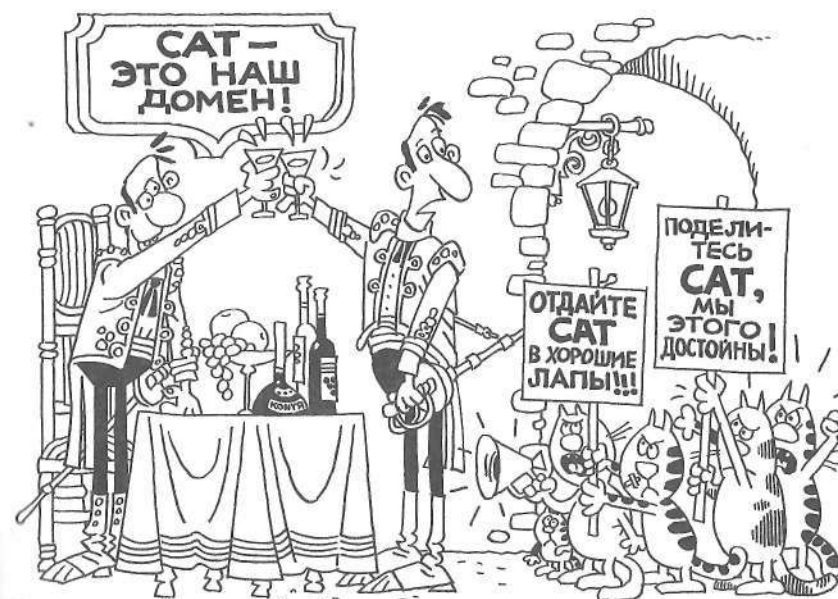
Итак, в 2005 году ICANN одобрила введение очередных новых доменов первого уровня. Это домены TRAVEL, JOBS, CAT, ASIA, MOBI, TEL.

Домен TRAVEL, как видно из названия, связан с путешествиями. В нем могут зарегистрировать доменное имя туристические компании и туроператоры. При этом потребуются документально подтвердить принадлежность к туристическому бизнесу. Для личных сайтов о путешествиях домен TRAVEL формально закрыт.

Таким образом, по своему назначению TRAVEL — яркий представитель бизнес-доменов, гораздо более яркий, чем домен COM. Впрочем, по популярности домен TRAVEL даже близко не подобрался к «дедушке» COM. Более того, в настоящий момент зона .travel находится на грани выживания, так как регистраций в ней крайне мало: около 25 тысяч на конец 2007 года.

Домен JOBS, предназначенный для размещения информационных ресурсов, связанных с наймом персонала. Идея использования JOBS проста: в этом домене размещается информация о вакансиях компаний, при этом «раздел» с вакансиями конкретной компании оформляется в виде домена второго уровня вида название_компании.jobs.

Самый «кошачий» домен Интернета — CAT (в переводе с английского — кошка) — на самом деле создан для каталонцев, а не для кошек. То есть это национальный домен, выделенный не государству, а языковой или, можно сказать, этнической общности — каталонцам (сейчас Каталония является провинцией Испании).



Если бы в домене CAT открыли свободную регистрацию, то, вероятно, многие имена быстро ушли бы к любителям кошек и производителям разнообразной кошачьей продукции. В пользу такого предположения говорит беглый взгляд на огромный и бурно развивающийся в западных странах рынок кошачьего питания, средств для ухода за питомцами и для их развлечения.

Отчасти по этой причине претендующий на домен в зоне .cat администратор (а им может быть и физическое, и юридическое лицо) должен соответствовать некоторым формальным требованиям. Например, домен в зоне .cat могут приобрести те, у кого уже есть веб-ресурс на каталонском языке. Также получить домен в пользование для создания познавательного ресурса на каталонскую

тематику помогут письменные рекомендации от трех других администраторов доменов в зоне .cat.

Надо заметить, что строгие требования к регистрации вряд ли позволят надолго удержать домен CAT от той или иной привязки к кошкам. Регистрация имен в этом домене началась в феврале 2006 года (в первые месяцы приоритет при регистрации имели владельцы торговых марок), а осенью 2007 года домен преодолел отметку в 25 тыс. зарегистрированных имен. Конечно, это не рекордные темпы, но домен связан с довольно развитым в плане информационных технологий регионом, который к тому же находится в Европе. Поэтому не приходится ожидать, что домен CAT повторит судьбу национального домена Тувалу TV, который сейчас однозначно привязан к телевидению.

Для истории развития глобальной DNS важно, что CAT — один из первых доменов верхнего уровня «особенного» назначения. Он в строгом смысле не является национальным доменом, но также его нельзя отнести к бизнес-доменам (как, например, TRAVEL) или к новым доменам широкого назначения (как, скажем, INFO). Кроме того, домен CAT, по крайней мере формально, нельзя назвать региональным или географическим. Мотивом создания этого домена послужила не территориальная обособленность Каталонии (что неудивительно, ведь это был бы чистой воды государственный сепаратизм), а языковая общность каталонцев. То есть домен CAT открывает историю «лингвистических» доменов, которых, конечно, будет больше. Так, следующий на очереди — домен LAT, представляющий Латинскую Америку.

К доменам CAT и LAT некоторым образом близок по своему назначению другой новый домен первого уровня — ASIA.

Этот домен ICANN ввела в октябре 2006 года для стран Азиатско-Тихоокеанского региона. Общедоступная регистрация имен в домене ASIA началась весной 2008 года. В одной из схем использования первый в истории региональный домен планируют поделить на географические поддомены, например создав домен второго уровня jp.asia для Японии. Очевидно, такая иерархия

повторит существующую систему национальных доменов азиатских стран, с той лишь разницей, что все домены окажутся выделены в новую зону .asia. Для чего же тогда нужен домен ASIA? Во-первых, введение первого в своем роде регионального домена позволит ICANN, да и Интернету в целом, понять на практике, нужны ли подобные домены. Во-вторых, азиатские производители и потребители играют серьезнейшую роль на мировом рынке информационных технологий, поэтому специальный домен, позволяющий четко обозначить «азиатскую принадлежность», привлекателен в качестве маркетингового инструмента. В-третьих, за тем, что именно Азии достался первый особенный географический домен первого уровня, несомненно кроется политическая подоплека.

Надо заметить, что приходящий на ум при обсуждении домена ASIA домен Евросоюза EU — не лучший пример. Дело в том, что домен EU выделен четко обозначенному политическому союзу государств. Азия не является подобным союзом: государства, расположенные в Азиатско-Тихоокеанском регионе, хоть и имеют некоторые общие черты, но при этом несравнимо более далеки друг от друга и по политическому устройству, и по своей культуре, чем государства, входящие в Евросоюз.

На момент написания этой книги домен ASIA был слишком молодым, чтобы можно было более или менее достоверно судить о его будущем. Тем не менее особых сомнений в том, что ASIA будет развиваться, а следом за ним появятся и другие региональные домены, нет.

Специальный домен первого уровня достался и такому революционному сегменту ИТ-рынка, как мобильная связь и мобильный доступ к информационным ресурсам Интернета. Домен MOBI создан для размещения веб-сайтов и других ресурсов, ориентированных на просмотр с мобильных телефонов. Такое позиционирование накладывает некоторые дополнительные требования на контент сайтов и используемые технологии. Например, плюсом является поддержка сервером доступа к сайту по протоколу WAP

(это специальная технология, облегчающая доступ с мобильных телефонов к контенту информационных сетевых ресурсов).

Интерес к домену MOBI поддерживается популярностью мобильной связи в мире: регистрация имен в нем открылась осенью 2006 года, а уже в 2007 года число регистраций превысило 500 тыс. имен. Развитию домена MOBI также может способствовать интерес к нему со стороны крупнейших представителей индустрии мобильной связи (например, со стороны компании Nokia).

Однако тенденции в развитии сотовой связи таковы, что современные коммуникаторы близки к тому, чтобы уверенно отображать на экране и контент обычных веб-сайтов, а не только тех, которые созданы специально для мобильных устройств. Поэтому у поставщиков интернет-контента остается все меньше причин специально сосредоточивать свои усилия на продвижении имен в зоне .mobi как ориентированных на мобильные устройства. Если у компании уже есть узнаваемый бренд, связанный, например, с доменом в зоне .com, то выделение ресурсов на развитие домена в MOBI может оказаться неоправданным.

В такой ситуации спасение для MOBI может прийти только со стороны крупнейших производителей мобильных телефонов и коммуникаторов. Например, если производители так настроят программное обеспечение массовых моделей телефонов, что по умолчанию поиск веб-сайтов будет происходить в домене .mobi, то и поставщики контента, борясь за аудиторию, будут вынуждены создавать ресурсы именно в этой зоне. Также развитие MOBI можно подтолкнуть, создавая внутри этого домена инфраструктуру имен, ориентированную на решение типичных задач, актуальных для пользователей мобильных средств связи. Одну из инициатив такого рода реализует компания dotMobi, администратор домена MOBI. DotMobi зарегистрировала около 650 доменов второго уровня .mobi, соответствующих крупным городам мира. Цель инициативы — создание информационных ресурсов для туристов. Действительно, путешественники, исследующие

достопримечательности городов мира, являются благодатной аудиторией для мобильных источников информации, рассказывающих именно о тех городах, в которых туристы находятся.

Другой новый домен первого уровня — TEL — с телефонами напрямую не связан, несмотря на название. Его планируют использовать в качестве основы для создания универсального онлайн-хранилища контактной информации. То есть пользователи адресов .tel могли бы создавать под своим персональным адресом что-то вроде электронной визитки, содержащей различные контактные данные (телефонный номер, адрес электронной почты, идентификатор в системе обмена мгновенными сообщениями и т. п.). Впрочем, домен TEL пока не работает, а его будущее выглядит неясным: сроки открытия домена для регистрации уже неоднократно переносились.

Нашли спонсора

В соответствии с определением ICANN сейчас сложилось два типа доменов первого уровня общего назначения.

- Новые домены первого типа вводятся ICANN на основании результатов обсуждения заявок глобальным интернет-сообществом. Далее эти домены управляются в соответствии с общественными процедурами ICANN. Примеры таких доменов: BIZ, INFO, PRO, NAME.
- Развитие рынка потребовало введения второго типа доменов — спонсируемых доменов первого уровня. Спонсируемый домен вводится ICANN в интересах достаточно узкой группы участников интернет-сообщества. Такой группой могут быть представители одного сегмента рынка. ICANN рассматривает заявку спонсирующей домен организации, которая «лоббирует» введение нового домена, представляя интересы связанной с ним группы пользователей. «Организация-лоббист» должна представить обоснование необходимости нового домена, а также проект политики регулирования регистраций в домене

и планы по его развитию. При этом вовсе не обязательно, чтобы домен создавался для чисто коммерческих интересов. Из новых доменов верхнего уровня спонсируемыми являются AERO, MUSEUM, COOP.

Процедурный вопрос

Новый домен первого уровня обычно вызывает живой интерес у пользователей, которые планируют зарегистрировать в нем имена. При этом имена в новом домене — ресурс ограниченный, требующий тщательного распределения. В ситуации, когда о введении нового домена становится известно заранее, требуются специальные процедуры, призванные противодействовать нездоровому ажиотажу, который может возникнуть в первые часы или дни после открытия регистрации.

Ажиотаж может быть вызван тем, что множество потенциальных администраторов доменов кинутся столбить все привлекательные имена, в том числе имена, важные для конкурентов по бизнесу, или имена, «родственные» известным брендам.

Чтобы регулировать поток заявок на доменные имена, а также предотвратить дополнительные судебные разбирательства, регистрация в новых доменах верхнего уровня обычно разворачивается поэтапно. Традиционная практика такова: в первую очередь право регистрации доменов получают обладатели торговых марок и фирменных наименований. Для них вводится начальный период приоритетной регистрации, обычно продолжающийся несколько месяцев.

Следующий этап — открытая регистрация, но по искусственно завышенным ценам. Он также может продолжаться несколько месяцев. Цель — дать возможность тем, кто готов раскошелиться, занять наиболее интересные имена. В некоторых случаях вместо этапа регистрации имен по завышенным ценам либо в дополнение к нему может проводиться аукцион доменных имен, на который попадают наиболее привлекательные имена.

Наконец, третий этап — полностью открытая регистрация по сниженным до определенного уровня ценам, то есть обычный режим функционирования домена.

Надо заметить, что различные ограничения, вводимые на начальных этапах регистрации доменов, призваны подогреть интерес аудитории к новому домену. Но, помимо этого, решается и чисто техническая задача распределения нагрузки на серверы регистраторов: огромные пиковые нагрузки довольно сложно обрабатывать, и при большом наплыве заявок на регистрацию имен система может отказать, а в результате увеличится число недовольных пользователей — ведь они останутся без «обещанных» доменов.

Если еще десять лет назад многие эксперты сомневались, что в ближайшей перспективе появятся новые домены верхнего уровня (кроме национальных), то сейчас никаких сомнений в появлении еще большего числа таких доменов не осталось. ICANN активно экспериментирует с региональными и особыми спонсируемыми доменами, развивая DNS. При этом разрабатывается четкая политика подачи заявок на новые домены верхнего уровня и рассмотрения этих заявок. То есть создаются механизмы для быстрого и безболезненного введения новых доменов.

Так, в 2008 году внутри ICANN созрел новый подход к созданию доменов первого уровня. Предлагаемая процедура немного напоминает проводившуюся ранее акцию по рассмотрению новых доменов (когда требовалось заплатить \$50 000 только за допуск заявки к рассмотрению комиссией, принимающей решение, и при этом действовали очень жесткие правила отбора). Серьезнейшее отличие новой процедуры, которую должны утвердить летом-осенью 2008 года, состоит в том, что планируется весьма либеральный подход к «утверждению доменов». Например, от компаний, претендующих на новые домены верхнего уровня, не требуется опыт в управлении реестрами доменов. Новая процедура обещает быть настолько либеральной, что можно ожидать не только появления доменов, связанных с сегментами потребительского рынка

(SHOP, CAR), но и доменов верхнего уровня для крупных корпораций (например, CISCO или BOEING). За рассмотрение заявки планируется взимать плату \$100 000, что не является сколько-нибудь заметной суммой ни для крупной компании, ни для богатого частного лица (\$100 000 сравнимы со стоимостью рядового автомобиля представительского класса). Судя по всему, при поступлении нескольких заявок на одно и то же имя (а так обязательно получится) возможно будет проведение аукционов. Хотя, если учесть практику выбора крупных подрядчиков государственными структурами в США, равновероятен и другой вариант — более тщательное рассмотрение поступивших заявок и по результатам объявление дополнительного тендера, в рамках которого заявки оценивает «экспертный совет».

Несомненно, в случае дальнейшей либерализации правил введения новых доменов верхнего уровня появятся домены для онлайн-сервисов, разработанных крупнейшими интернет-компаниями. Так, нешуточная борьба может возникнуть вокруг доменов PHOTO или MAIL.

Как бы то ни было, одним из самых серьезных нововведений обещает стать не какой-нибудь один домен, а целый новый сегмент доменов — домены верхнего уровня на национальных языках.

Глава 8

Национальные буквы

- ☐ Технические трудности
- ☐ На высшем уровне
- ☐ Раздвоение личности
- ☐ RUсские домены

Как мы помним, Интернет создали в США, где господствующий язык — английский. Поэтому в ходе исторического развития Глобальной сети английский язык стал основным и в ней. Действительно, английский язык принадлежит к числу самых распространенных языков мира, является одним из официальных языков ООН и входит в список языков международного общения. Если принять эти факторы во внимание, то господство английского в Сети уже не представляется столь удивительным.

Однако неясно, почему другим языкам даже не предоставили возможности конкурировать с английским в системе адресации Интернета? Ведь с получением глобального статуса Интернет наполнился информацией на множестве языков. Свое, и весьма существенное, место в Сети заняли русский, китайский, испанский, французский и многие другие языки мира. В национальных сегментах Интернета, предоставляющих своим пользователям контент на привычном национальном языке, наличие адресной системы, строго привязанной к латинскому алфавиту английского языка, уже не выглядит обоснованным.

Надо заметить, что одна из основных идей «философии» DNS состоит в использовании для обозначения адресов легко запоминающихся символьных строк, лучше всего — «словарных» слов. То есть система доменных имен позволяет использовать и ничего не значащие сочетания вроде `f1h1y212rfa1.com`. Однако DNS вводили как раз для того, чтобы вместо абракадабр (которыми для основной массы пользователей являются и числовые IP-адреса) использовать «человеческие» имена: скажем, `example.com` — домен, служащий для указания в качестве примера доменов (в переводе с английского `example` означает «пример»). Поэтому латинский алфавит в именах доменов используется прежде всего для записи осмысленных слов, аббревиатур и словосочетаний.

На начальном этапе развития Сети, когда основная масса ее пользователей состояла из ученых физико-математических специальностей, инженеров высокотехнологичных отраслей, технических специалистов, использование латиницы и английского для решения задач адресации казалось само собой разумеющимся, ведь

эти категории пользователей постоянно используют английский язык в работе, даже если живут в странах, где английский не является официальным языком.

Но как только Интернет, превратившийся в общедоступную, массовую сеть, стали заполнять «домохозяйки», у них возник резонный вопрос: почему же адрес набирается непонятной латиницей? Особенно рельефно проблема выглядела в странах, национальные языки которых не используют латинский алфавит в письменности (например, в кириллическом сегменте Интернета). Впрочем, во многих европейских странах алфавиты хоть и базируются на латинской графике, но включают дополнительные буквы, отсутствующие в английской письменности. Такова ситуация во всех скандинавских странах, во Франции, в Германии и др. То есть ограничения, накладываемые 26-буквенным английским алфавитом (а кроме него, разрешены только 10 цифр и знак дефиса), ощущаются и в близкородственных с английским языках.

Впервые идея о «расширении алфавита» возникла применительно к традиционным доменам первого уровня, а точнее, к национальным доменам. Администраторы некоторых национальных доменов еще в 1990-х годах решили самостоятельно пойти навстречу своим пользователям и разрешили регистрацию имен с символами национальных алфавитов, позволив тем самым использовать в качестве доменов привычные слова национальных языков. Впрочем, первые многоязычные домены работали с проблемами, требовали установки дополнительного программного обеспечения на компьютеры пользователей и проведения дополнительных настроек операционной системы. Тем не менее интерес к доменным именам на национальных языках был достаточно велик, чтобы в итоге побудить ICANN к запуску официальных процедур регистрации таких доменов. Произошло это в 2003 году.

Начался процесс с официального разрешения на регистрацию доменов второго уровня с национальными символами в тех национальных доменах, в которых администраторы проявили интерес к «многоязычию». В итоге домены с символами национальных алфавитов появились в национальных доменах Китая CN

и Японии JP. Также стала возможна регистрация многоязычных имен в доменах общего пользования — COM, NET, ORG, BIZ, INFO. К 2008 году регистрация «внелатинских» доменов разрешена в нескольких десятках национальных доменов.

Технические трудности

Введение многоязычных доменов связано с целым рядом технических трудностей, основная из которых состоит в том, что DNS может работать только с символами из набора ASCII.

Что такое ASCII? Это стандартный набор символов, который включает в себя в том числе буквы латинского алфавита, введенный еще до появления Интернета и DNS. Символы ASCII представлены в виде числовых кодов, а таблицы соответствия кодов и символов являются предметом этого стандарта.

Когда создавалась DNS, логично было использовать ASCII, ведь этот стандарт тогда лежал в основе компьютерной обработки символов, позволяя разным компьютерам и разному программному обеспечению одинаковым образом представлять символическую информацию. Надо заметить, что DNS использует далеко не все символы таблиц ASCII. Напротив, к использованию разрешены только 26 букв алфавита, 10 цифр и знак дефиса. То есть и без того узкий набор ASCII, не включавший, например, буквы кириллицы, сузили еще больше, выбрав некоторое подмножество символов.

Итак, стандартная современная система доменных имен использует урезанный набор ASCII-символов. Из чего состоит DNS? Из множества компьютеров-серверов, на которых работает специальное программное обеспечение, реализующее всю функциональность преобразования имен (преобразование, напомним, происходит между символическими строками и числовыми IP-адресами). Важных серверов DNS, работающих в Интернете, насчитываются многие тысячи. А управляют ими самые разные компании и администраторы, не имеющие централизованного начальства и находящиеся в разных странах мира.

Введение в таблицы преобразований новых символов и изменение алгоритмов преобразования — это самые радикальные изменения в программном обеспечении DNS, какие только можно представить. Понятно, что осуществить подобное на практике в глобальном масштабе просто невозможно. Дело в том, что любая попытка произвести «апгрейд» распределенной компьютерной системы мирового масштаба, включающей тысячи разных компьютеров и не имеющей центрального управления, имеет один наиболее вероятный исход — крах глобальной системы адресации Интернета.

Подобный исход вряд ли нужен пользователям Сети — им требуются лишь многоязычные домены разных уровней. Именно поэтому для введения многоязычия в систему адресации разработали технологию, позволяющую реализовать новую функцию поверх действующей годами и отлаженной DNS.

КСТАТИ



Нужно уточнить, что сперва для реализации многоязычных доменов было предложено несколько разных технологий. Некоторые из них подразумевали использование «альтернативной» системы доменных имен или предлагали другие подобные решения сомнительной ценности. После изучения вариантов и возможностей их реализации ICANN рекомендовала применить технологию, которая позволит с минимальными рисками поэтапно ввести в употребление доменные имена, допускающие максимально широкий набор символов самых разных алфавитов.

Суть технологии доменного многоязычия, рекомендованной ICANN, заключается в дополнительном преобразовании имен (например, на компьютере пользователя) до отправки запроса в DNS. В результате доменное имя с символами национального алфавита перекодируется в формат, допустимый для обычной обработки в DNS. То есть имя оказывается состоящим только из символов ASCII, разрешенных в классической DNS, а именно из букв латиницы, цифр и дефисов.

Другими словами, в рамках технологии многоязычных доменов старая и проверенная глобальная DNS остается нетронутой: она как бы и не «видит» новых алфавитных символов. Это освобождает интернет-сообщество от крайне рискованных усилий по «апгрейду» DNS.

Как же работают многоязычные имена? Введенное пользователем доменное имя на национальном языке преобразуется браузером по стандартному алгоритму в последовательность допустимых к использованию в DNS ASCII-символов. Эта последовательность начинается со специального префикса, позволяющего программам отличать многоязычные адреса. При этом с точки зрения старых программ, работающих с доменными именами, и с точки зрения DNS строка символов, полученная в результате преобразования, будет являться обычным именем домена. То есть старые программы, созданные до появления технологий многоязычия, также смогут обрабатывать новые адреса, правда, они не смогут правильно отобразить имена средствами национального алфавита.

Простой пример: русскоязычный адрес `руцентр.su` будет преобразован в ASCII-строку `xp--e1aqhcjdv.su`, где `xp--` — префикс, обозначающий мультязычное доменное имя, а `e1aqhcjdv` (самая настоящая абракадабра) представляет собой закодированную особым образом последовательность букв кириллицы «руцентр». Домен `SU` набирается стандартной латиницей, и его запись не преобразуется.

Итак, самое важное, что нужно понимать: технически многоязычные доменные имена вводятся на другом «уровне абстракции», поверх DNS. При этом необходимые преобразования символов осуществляются не DNS, а на компьютере пользователя Интернета (или на сервере, не участвующем в DNS, если такое преобразование требуется серверу) специальным программным обеспечением, а DNS передается результат преобразования, состоящий только из ASCII-символов.

Префикс `xp--`, обозначающий многоязычные доменные имена, согласно предложению ICANN, администраторы доменов верх-

него уровня могут зарезервировать, если они пока не хотят допускать регистрацию и использование многоязычных доменов в своих «зонах ответственности». Дело в том, что регистрация имени, начинающегося с префикса `xp--`, может оказаться технически эквивалентной регистрации того или иного доменного имени в многоязычном представлении.

Преобразование символов в описанной технологии, которая называется Punycode, происходит с использованием наиболее прогрессивной и универсальной современной кодировки символов — Unicode. Таблицы Unicode включают все мыслимые символы самых разнообразных алфавитов и используемых «при письме» знаковых систем, сколько-нибудь распространенных в мире.

Рекомендованная ICANN технология преобразования имен уже встроена в наиболее распространенные современные браузеры. Например, ее поддерживают браузеры Internet Explorer 7.0 и Firefox семейства версий 2.x. Пользователям этих браузеров (то есть подавляющему большинству пользователей Сети) не нужно прибегать к помощи дополнительных плагинов, чтобы воспользоваться многоязычными доменными именами. А если вспомнить, что технология многоязычия устроена не требующим перенастройки DNS образом, то окажется, что у администраторов существующих доменов нет технических препятствий для введения многоязычных доменных имен.

Предположим, администратор домена `test.ru` решил ввести внутри своей зоны ответственности доменные имена на русском языке. Оказывается, что для добавления в DNS доменного имени `привет.test.ru` администратору достаточно внести в управляющие записи сервера DNS домен `xp--b1agh1afp.test.ru`. Это доменное имя состоит только из допустимых в DNS символов и поэтому будет доступно и для современных, и для старых программных систем. Отличие лишь в том, что пользователи современных интернет-браузеров смогут обращаться к ресурсу под именем `привет.test.ru`. При этом администратору домена `test.ru` не придется получать разрешение на введение кириллических имен в своем домене у вышестоящих организаций.

Если с собственно DNS проблем во время внедрения многоязычных доменных имен, в том числе кириллических, возникнуть не должно, потому что, как мы разобрались выше, никаких изменений в DNS вносить не предполагается, то с другими программными системами, участвующими в работе веба, проблемы все же возможны. Они связаны не столько с собственно преобразованием адресов, сколько с разнообразным контролем вводимых данных и программными фильтрами.

Например, проблемы коснутся CMS (CMS — это система управления контентом, программный комплекс, обеспечивающий работу веб-сайта и помогающий редакторам сайта управлять публикуемыми материалами) и онлайн-сервисов вообще. Попробуем разобраться, что это за трудности.

Так, распространенной практикой является проверка данных, вводимых пользователем на сайте. Предположим, на веб-сайте присутствует форма для регистрации пользователей и в ней нужно указать адрес e-mail. При этом переданные пользователем данные проверяются на предмет соответствия заданному формату: если в поле формы должен быть адрес e-mail, то программное обеспечение на сайте проверяет, что это действительно адрес e-mail. Такую проверку возможно организовать с использованием специальных функций-фильтров, сравнивающих полученные символы с неким шаблоном. Так как электронная почта работает с использованием имен доменов, такие шаблоны строятся на основе допустимых в DNS символов.

Проблемы появляются, когда пользователь вводит адрес электронной почты, содержащий, к примеру, кириллический домен. Рядовой пользователь, конечно, не знает о потации xp-- и о стандартах преобразования, он вводит домен так, как привык — кириллицей. В результате программное обеспечение сервера, проверяющее вводимые данные относительно «старого» стандарта DNS, определяет, что адрес e-mail «содержит недопустимые символы», и не позволяет пользователю зарегистрироваться.

К сожалению, это весьма распространенная проблема. И она касается не только адресов электронной почты, но и адресов сайтов.

Так, многие онлайн-сервисы и даже поисковые машины (среди которых, по состоянию на 2008 год, были и русскоязычные) не позволяют вводить напрямую кириллические адреса сайтов в свои формы приема данных от пользователей.

С поисковыми машинами связаны и другие проблемы многоязычных адресов. Дело в том, что программы-роботы, индексирующие веб-страницы, придают большое значение ссылкам с одних страниц на другие. При этом с введением многоязычных доменов на страницах могут встречаться ссылки с адресами, записанными не латиницей. Однако если робот не умеет работать с многоязычными адресами, то он не сможет учесть эти ссылки и проиндексировать расположенные по ссылкам страницы.

С некоторыми проблемами, связанными с многоязычными доменами, могут также столкнуться сетевые инженеры. В повседневной деятельности по наладке сетей они используют специальное программное обеспечение, которое часто требует ввода тех или иных адресов, а адреса удобнее вводить в виде доменных имен. Однако многоязычные имена могут не поддерживаться классическими программами. Конечно, тут вполне допустимо использование тех же адресов в DNS-версии (то есть xp--...), но удобно ли будет инженерам оперировать той абракадаброй, в которую в данном случае превращаются осмысленные имена доменов, — это вопрос.

Впрочем, все описанные проблемы преодолимы. Для старого программного обеспечения выпустят исправления, а интернет-поисковики научатся обрабатывать многоязычные адреса в ссылках. Интересно, что в последнем случае лидером оказался Google, который уже полностью поддерживает кириллические адреса и в веб-формах, и в поисковой выдаче.

На высшем уровне

Описанная технология Punycode уже довольно тщательно испытана ICANN с точки зрения DNS. Так, в результате лабораторных испытаний выяснили, что нет препятствий для использования

этой технологии на корневых серверах DNS. То есть можно ввести домены первого уровня, записанные с использованием символов национальных алфавитов.

В рамках испытаний в 2007 году ICANN создала специальный проект, позволяющий пользователям Интернета протестировать многоязычные имена по полной программе. Для этого в «корневой системе» DNS Интернета были зарегистрированы специальные тестовые домены верхнего уровня, записанные символами различных национальных алфавитов. Так, для кириллических имен предназначен адрес <http://пример.испытание/>, под которым размещены веб-страницы, позволяющие пользователям не только проверить доступность адреса из того или иного браузера, но и оставить свои замечания, касающиеся использования технологии.

На базе отработанных технологий в 2009 году планируется ввести для России новый национальный домен — РФ, что позволит закрыть вопрос с кириллическими доменами в Интернете. Но об этом я расскажу чуть позже.

Раздвоение личности

Удобная технология работы многоязычных имен все же привела к возникновению некоторых организационных трудностей. Первая и, наверное, главная из них связана с тем, что с формально-юридической точки зрения всякое доменное имя, включающее символы национальных алфавитов, оказывается совокупностью двух имен. Точнее, двух представлений одного имени. Одно из этих имен — собственно имя домена, записанное с использованием «многоязычия». Второе имя — соответствующая комбинация ASCII-символов, используемая на уровне DNS. Связывает эти имена между собой только стандарт преобразования символов. Расщепление имени домена на два приводит к возникновению «войны доменных терминов»: какое имя считать первичным и самым главным?

В базе данных технического центра, управляющего доменом, очевидно, более важное значение приобретает внутренний вариант имени, то есть записанное ASCII-символами имя с префиксом `xp--`. Ведь именно оно размещено в базе данных и именно с ним фактически работает DNS.

С точки зрения администратора, зарегистрировавшего доменное имя на национальном языке, очевидно, главную роль играет представление домена символами национального алфавита. Ведь это имя заинтересовало пользователя, и это имя он планировал зарегистрировать. Абракадабра из латинских букв и арабских цифр, начинающаяся префиксом `xp--`, обладателя прав на домен `привет.ru` вряд ли интересует.

Сложностей в ситуацию добавляет и тот факт, что связь между двумя именами устанавливается не законами или юридическими процедурами, а лишь существующим алгоритмом преобразования. Если алгоритм изменится или кто-то предложит использовать другой алгоритм, то связь между именами в реестре доменов (внутри DNS) и именами, которые регистрировали пользователи, может прерваться.

В случае введения многоязычных имен в доменах первого уровня в самом сложном положении оказываются компании-регистраторы.

Техническая служба, осуществляющая администрирование домена, может легко избежать всех проблем, дистанцировавшись от многоязычия и занимаясь лишь регистрацией доменных имен с префиксом `xp--`. Для этого даже не понадобится вносить серьезные изменения в существующую систему приема заявок.

КСТАТИ



Нужно отметить, что по различным причинам возможно введение технических ограничений на использование тех или иных символов и последовательностей символов в именах `xp--`. И чтобы реализовать эти ограничения, технической службе,

обеспечивающей функционирование DNS домена, придется доработать свои программные системы, используемые для приема регистраций.

Для регистратора же доменов, как несложно догадаться, самым важным является представление доменного имени на национальном языке. Ведь возможность регистрации имен, записанных привычными для глаза символами национального алфавита, и является главной привлекательной для рядового пользователя Сети чертой введения многоязычия в системе адресации Интернета. А регистратор доменов ориентируется именно на рядового пользователя.

В итоге регистратор попадает в зависимость от действующих стандартов преобразования символов. Более того, он вынужден лавировать между собственными интересами, интересами своих клиентов и интересами технического центра, обеспечивающего функционирование домена.

Если регистрацию доменов для конечного пользователя производит та же организация, которой подчиняется технический центр домена, ситуация с национальными алфавитами несколько упрощается. Однако на практике подобное монопольное положение регистратора встречается далеко не во всех доменах первого уровня.

«Раздвоение» имен — далеко не единственная организационная проблема с многоязычными доменами.

Так, еще на раннем этапе обсуждения доменного многоязычия (в 1990-х годах) стало ясно, что расширение алфавита может сыграть на руку фишерам. Фишеры — это злоумышленники, использующие (помимо других систем и способов) Интернет для выуживания путем обмана у доверчивых граждан номеров банковских счетов, паролей доступа к этим счетам, а также другой ценной персональной информации.

Предположим, что в каком-то домене верхнего уровня открылась ничем не ограниченная регистрация имен с символами нацио-

нальных алфавитов. В таком случае умелый фишер может использовать графически похожие символы разных алфавитов для создания доменов-обманок.

Например, подлинный домен MYBANK записывается латиницей (представим, что под этим доменом размещается сайт крупного банка и для нас не имеет значения, в каком именно домене первого уровня расположен сайт банка). Фишер может зарегистрировать домен MYBANK, в котором буква *B* — это не заглавная латинская «би», а кириллическая буква «вэ». Во многих шрифтах латинская заглавная *b* и кириллическая заглавная «в» совпадают по начертанию.



Это означает, что при чтении пользователь не сможет отличить один домен от другого, хотя с точки зрения DNS и с точки зрения компьютера пользователя графически (то есть «на письме») похожие домены — два совершенно разных домена. Пользуясь тем, что графические представления имен доменов неразличимы, фишер может заманивать пользователей на свой сайт, который размещен

под ложным доменом, имитирующим известный пользователю адрес. Понятно, что на фишерском сайте от пользователя, полагающего, что он находится на официальном сайте банка, можно потребовать указать банковские реквизиты и пароли для доступа к системе управления банковским счетом.

КСТАТИ



Именно из-за графического сходства не стоит ожидать появления официального кириллического национального домена РУ для России. Дело в том, что при записи строчными буквами («ру») он неотличим от домена Парагвая — РУ (ru).

Для борьбы с фишингом вводятся различные ограничения на регистрацию многоязычных доменов. Одно из самых распространенных — запрет на регистрацию имен, содержащих вперемешку символы из различных алфавитов. Так, подобный запрет ставит крест на успехе изложенной схемы подделки адреса с помощью одной буквы. Другие ограничения могут включать приоритетную регистрацию имен на национальном языке для владельцев графически похожих «латинских» доменов.

Так, в действующем национальном домене России — RU — в период, когда введение кириллических имен оказалось близкой реальностью, в 2007 году, разработали специальную процедуру, направленную на предотвращение конфликтов вокруг графически похожих имен, записанных символами разных алфавитов.

Предполагалось, что администратором двух графически похожих доменов сможет быть только одно лицо. Чтобы формализовать процедуру определения графического сходства, подготовили таблицу соответствия, где перечислили графически сходные буквы латиницы и кириллицы. Например, домен сок.ru (здесь использованы кириллические буквы) по этой таблице признавался бы графически похожим на домен сок.ru (в «латинском» написании). Таблица графического соответствия была опубликована в открытом доступе.

Публикация таблицы привела к тому, что возник ажиотажный спрос на графически похожие домены. Предприимчивые пользователи, не дожидаясь открытия регистрации кириллических доменов, регистрировали привлекательные имена в «латинском» написании, надеясь позже, когда многоязычные домены зоны .ru будут доступны, претендовать на кириллический вариант. Всего за несколько дней после публикации таблицы соответствия были зарегистрированы сотни доменов, представлявших собой с точки зрения написания латиницей полнейшую абракадабру.

Впрочем, поторопившиеся доменные инвесторы крупно проиграла: кириллические имена в зоне .ru решено было не вводить, а зарегистрированные абракадабры так и остались абракадабрами, не обрета привлекательной рыночной цены.

РУсские домены

История с кириллицей в домене RU, несомненно, уже вошла в летопись Рунета и показательна сразу во многих аспектах.

О возможности введения кириллических имен в домене RU заговорили очень давно, еще в конце 90-х годов XX века. Более того, пока одни участники рынка только надеялись хорошо подготовить техническую базу и почву для введения кириллицы, другие, тогда еще не очень известные игроки, взялись решить задачу быстро. Тем более что из-за инертности ICANN в вопросах многоязычия самостоятельное введение национальных имен проводилось и локальными операторами в других странах.

В итоге через некоторое время в Рунете без оглядки на ICANN возникли альтернативные системы адресации, управляемые предприимчивыми компаниями-регистраторами. Эти системы действовали в «серой» зоне рынка, используя собственные плагины (программы-расширения для браузеров) и собственную альтернативную DNS, в которой появились кириллические домены верхнего уровня: РУ, КОМ, НЕТ, ОРГ.

Как я писал выше, в Интернете нет действенных механизмов, способных жестко ограничить введение новых услуг и систем адресации. Поэтому невозможно правовым способом запретить коммерческой компании предлагать на рынке услугу по регистрации доменов в самозванных (с точки зрения глобального Интернета) кириллических доменах. Услугу компания оказывает своими силами, вполне обычным образом используя каналы Интернета и специальное программное обеспечение для перенаправления пользовательских запросов на нужные IP-адреса, с использованием «расширения» DNS. Все это делается в рамках закона. В некотором противоречии с деловой практикой, впрочем, находится тот факт, что подобное расширение DNS интернет-сообщество не заказывало. Но ведь и многие другие нововведения, ставшие популярными, это же сообщество не заказывало. Живой пример — протоколы и технические решения для систем мгновенного обмена сообщениями по Интернету (особенно суперпопулярная ICQ), которые интернет-сообщество не «заказывало», что, однако, не помешало их повсеместному распространению, после того как все ощутили удобство использования.

Итак, кириллический домен РУ (как и его «братья» КОМ, НЕТ, ОРГ), введенный в 2000 году в ограниченный оборот силами одной компании («РегТайм»), начал принимать регистрации. С какой целью домен вводился в использование в обход традиционных процедур? Вероятно, чтобы позже, когда в новой зоне появятся регистрации, надавить на ICANN, требуя признать домен де-факто и ввести его глобальную поддержку уже стандартными процедурами, легитимизировать домен в мировом масштабе. Конечно, администратором домена осталась бы компания-создатель.

Если взглянуть на историю развития споров с участием ICANN, такой расчет не кажется совсем уж необоснованным. Более того, нужно признать, что хоть давление на ICANN и не позволило владельцам «неофициального» домена РУ достичь своей цели полностью, тем не менее существование РУ сыграло ключевую роль в судьбе кириллицы в национальном домене России.

История «давления на ICANN» давняя и уходит корнями еще в то время, когда ICANN не существовало (напомню, что корпорация появилась только в 1998 году). Основа подобных споров и конфликтных ситуаций довольно проста: локальные компании, предлагающие нововведения в Интернете, опираются на то, что с правовой точки зрения национальный сегмент Интернета не более чем совокупность каналов передачи данных и компьютерных сетей. Весомых межгосударственных дипломатических соглашений, признающих национальные сети связи элементами всемирного Интернета, не существует. Соответственно, нет и никаких правовых оснований для признания главенства ICANN, скажем, над российским сегментом Интернета.

Поэтому новый домен первого уровня, пусть и доступный только с использованием специальных программ, на территории России можно позиционировать как новую технологию, связанную с сетями передачи данных. При этом ICANN не имеет возможности запретить российской компании продвигать какие бы то ни было технологии на местный рынок. Более того, если корпорация начнет предпринимать резкие регулирующие действия, это обязательно вызовет конфликты и затяжные судебные разбирательства, что ICANN совершенно не нужно. В результате оказывается, что корпорация вынуждена либо придавать официальный статус сложившейся де-факто ситуации, либо, если внутри национального сегмента Интернета возникли противоборствующие группировки, затягивать принятие решения, всячески лавируя между сторонами «доменной войны».

Итак, официальное внедрение многоязычия в домене RU тянулось довольно долго. Общие правила регистрации кириллических имен в зоне .ru оформились только к 2006 году. А ключевой момент настал лишь в 2007 году.

Тогда процедура внедрения кириллицы в зоне .ru уже вступила в завершающую стадию, с технической стороны все было готово, оставалось лишь принять эпохальное решение силами Комитета

регистраторов Координационного центра домена RU и получить одобрение ICANN.

Уже на этапе подготовки решения создатели домена РУ использовали факт существования своего домена и наличия в нем регистраций для давления и на ICANN, и на Координационный центр, требуя признать домен РУ как уже действующий кириллический домен, вместо того чтобы вводить кириллицу в домене RU. Давление оказывалось с помощью публикации в прессе открытых писем и обращений. Использовались и другие подходящие для такой задачи методы.

Конфликт, помимо уже упомянутых причин, питало и полное сходство доменов RU и РУ с фонетической точки зрения: каждый из них является правильной транслитерацией другого. Этот аспект грозил правовыми коллизиями в том случае, если бы администраторы доменов в «неофициальной» зоне .ру стали подавать судебные иски в отношении администраторов аналогичных кириллических доменов в домене RU. Мотивировать подобные иски можно было тем, что используемые домены схожи по написанию и одинаково воспринимаются на слух.

Казалось, итоговое решение будет принято в пользу домена RU. Однако незадолго до решающего заседания в Координационном центре ICANN, опять проявив свою непростую дипломатическую природу, заняла весьма размытую, неоднозначную позицию в отношении наметившегося конфликта между сторонниками введения кириллических доменов в зоне .ru и администрацией домена РУ, в котором регистрация кириллических доменов проводилась уже долгие годы.

Сторонники русификации домена RU ожидали, что ICANN внесет ясность, четко обозначив приоритетный домен. Но этого не произошло. Тщательно избегая эскалации конфликта, ICANN, по сути, устранилась от решения проблемы, предложив сторонам «доменной войны» самостоятельно искать компромиссный выход, если они хотят получить одобрение ICANN на введение кириллицы.

Решение, найденное внутри страны, оказалось несколько неожиданным: Координационный центр постановил отказаться от введения кириллических доменов в зоне .ru, сославшись на то, что заинтересованным организациям пужно активнее лоббировать появление нового кириллического домена первого уровня — РФ. Конечно, речь идет уже об официальном кириллическом домене России, признаваемом ICANN.

Впрочем, домен РФ, появление которого ожидается не ранее 2009 года, оказывается даже удобнее домена .ru. В основном потому, что при наборе адреса пользователю не придется переключать раскладку клавиатуры. Более того, в отличие от домена РУ, домен РФ не конфликтует по написанию с доменами других стран. (Напомню, что кириллическое «*ру*» графически совпадает с латинским *ru* — доменом Парагвая.)

Хронология «кириллических» событий в домене RU достаточно показательна. Рассмотрим ее несколько подробнее.

□ 2001–2002 годы.

На фоне общего роста интереса к символам национальных алфавитов в доменных именах на сайте info.nic.ru (информационном центре доменной тематики), принадлежащем регистратору RU-CENTER, был открыт раздел «Многоязычные домены». Раздел включал информацию по правовым, историческим и технологическим вопросам введения многоязычных доменов в Интернете. Неофициальный домен РУ набирает обороты. Российское интернет-сообщество обсуждает перспективы кириллицы в доменных именах.

□ 13 ноября 2003 г.

Корпорация VeriSign провела в Москве конференцию «Русскоязычные домены в Интернете». Организовали конференцию РосНИИРОС и RU-CENTER. Компания VeriSign является одним из законодателей технологической моды Интернета. В 2003 году введение многоязычных доменов находилось в прямой зависимости от воли VeriSign. РосНИИРОС —

организация, управляющая техническим центром домена RU. RU-CENTER — крупнейший регистратор доменных имен в зоне .ru.

□ 10 декабря 2003 г.

По итогам кулуарного общения в рамках конференции, по запросу RU-CENTER в Координационном центре национального домена сети Интернет создана рабочая группа, которая должна была оценить целесообразность введения русскоязычных доменов в домене RU. Российское интернет-сообщество также обсуждает целесообразность появления символов кириллицы. Преобладает мнение, что вводить кириллические имена не нужно. Тем не менее существует и лагерь сторонников «доменов по-русски».

□ 29 декабря 2003 г.

Рабочая группа в кратчайшие сроки завершила работу, заключив, что введение символов кириллицы в имена доменов второго уровня RU целесообразно.

□ 21 января 2004 г.

Координационный центр начал разрабатывать план работ по введению кириллицы.

□ 15 апреля 2004 г.

Координационный центр принял план подготовительных работ по русскоязычным доменам RU. Завершение этих работ было запланировано на конец августа 2004 года.

□ 29 июня 2004 г.

Опубликован технический отчет о возможностях введения в домене RU доменных имен, содержащих символы кириллицы.

□ 30 мая 2005 г.

В Координационном центре национального домена сети Интернет создана рабочая группа по подготовке документов, регламентирующих порядок регистрации кириллических доменов. Проходят консультации с ICANN. В неофициальном

домене RU регистрируются имена, его владельцы также консультируются с ICANN.

□ 12 октября 2005 г.

Появились первые варианты документов, регламентирующих общий порядок регистрации русскоязычных доменных имен. Предусматривался период приоритетной регистрации для владельцев торговых марок.

□ 1 марта 2006 г.

Рабочей группе поручено доработать регламентирующие документы, так как эксперты обнаружили проблемы, касающиеся возможности фишинга.

□ Май 2006 года.

Координационный центр принял общие принципы регистрации в домене RU доменов с символами кириллицы и одобрил порядок регистрации.

□ Весна 2007 года.

Координационный центр утвердил правила регистрации кириллических доменов в зоне .ru. Правила включали пункт, разрешающий регистрировать графически похожие домены, построенные из символов разных алфавитов (латиница и кириллица), только на одно лицо. Вместе с правилами опубликована таблица соответствия букв двух алфавитов. Не дожидаясь вступления правил в силу и открытия регистрации кириллических имен, «доменные инвесторы» кинулись регистрировать графически похожие имена в «латинской» записи. Цель таких регистраций заключалась в том, чтобы позже претендовать на графически похожее привлекательное кириллическое имя.

Начинается заключительный этап консультаций с ICANN. Владельцы неофициального домена RU обращаются в ICANN с письмами и запросами. В профильной прессе разгорается шумиха по поводу грядущей русификации зоны .ru, в чем почти никто уже не сомневается.

□ 4 июня 2007 г.

Обратив внимание на возникшую конфликтную ситуацию, на неясность судьбы неофициального домена RU и на невящую позицию ICANN, правление Координационного центра домена RU приняло решение о том, что кириллических доменных имен в зоне .ru не будет. Интернет-сообществу предложено дожидаться появления официального кириллического домена первого уровня РФ.

КСТАТИ



Отмечу интересный факт: один кириллический домен в зоне .ru все-таки есть (2008 год). Это домен «кремль.ru». Если в адресной строке браузера набрать <http://кремль.ru/>, то можно попасть на официальный сайт Президента Российской Федерации (<http://kremlin.ru/>).

Если с доменом РФ на момент написания книги (2008 год) еще не все ясно, то в домене SU многоязычные имена уже появились. Произошло это 28 апреля 2008 г. Впрочем, администратор домена SU — Фонд развития Интернета — всячески дистанцировался от понятия «многоязычные домены». Формально Фонд лишь разрешил регистрацию в SU доменов второго уровня, начинающихся с префикса xp-- . Ранее такие имена считались зарезервированными и регистрация имен с двумя дефисами подряд запрещалась.

Если взглянуть на рекомендованную ICANN и поддерживаемую современными браузерами технологию многоязычных доменов, то станет ясно: допустив регистрацию доменов с префиксом xp-- , Фонд развития Интернета фактически разрешил регистрацию доменных имен с символами национальных алфавитов. Тем не менее в официальных сообщениях Фонда упоминаются только «возможность регистрации» (<http://www.fid.ru/?newsid=1206970140>). Установить соответствие между национальными алфавитами и доменными именами с префиксом xp-- внутри DNS предлагалось регистраторам.

При этом в домене SU регистрируются не только кириллические домены. Так как особо жестких ограничений на использование имен с префиксом xp-- введено не было, появилась возможность регистрировать и имена, записанные, например, буквами греческого алфавита.

КСТАТИ



Полный же список алфавитов, построенный в соответствии с таблицами Unicode, достаточно широк. Например, в мае 2008 года регистратор имен в домене SU (компания RU-CENTER) позволял регистрировать имена с использованием следующих алфавитов: латиница, греческий, кириллица, армянский, иврит, арабский, грузинский.

Надо заметить, что открытие регистрации многоязычных имен в домене SU подстегнуло его развитие: за несколько недель число зарегистрированных многоязычных доменов приблизилось к 10 000. Впрочем, многие из этих доменов регистрировались не с целью размещения сайта, а в качестве объекта инвестиции.

Глава 9

Колесо Сансары, или Жизнь и смерть доменов

- ☐ Рождение
- ☐ Жизнь
- ☐ Смерть
- ☐ Зомби? Нет — перерождение
- ☐ Циклы .ru

У всякого домена второго уровня есть жизненный цикл: домен появляется в DNS; под ним размещаются ресурсы, которые используют читатели сайтов и посетители сервисов; позже интернет-ресурс, связанный с доменом, может измениться или вовсе исчезнуть, а также может быть удален и сам домен, который, впрочем, затем опять может родиться.

Казалось бы, жизненный цикл домена можно описать тремя словами, составляющими простую и очевидную связку: «регистрация — работа — удаление». Действительно, трехэтапная схема существует в реальности, но является только приближением.

На практике все сложнее, и за каждым этапом кроется своя структура состояний.

Прежде чем исследовать эти структуры, еще раз договоримся о терминах. Надо заметить, что даже домены первого уровня имеют непростые жизненные циклы, в рамках которых возможно «рождение» замороженного домена или допускается существование «доменов-зомби», продолжающих действовать после смерти.

Мы подробно рассмотрели особенности жизни доменов первого уровня выше, в соответствующих главах книги. В этой же главе мы обсудим **домены второго уровня** (домены вида test.ru).

Жизненный цикл доменного имени второго уровня зависит от того, в каком домене верхнего уровня оно зарегистрировано. Хотя в разных доменах первого уровня можно выделить общие, фундаментальные черты «жизнедеятельности», в деталях картины будут различаться, порой до неузнаваемости.

Традиционным ориентиром в доменной индустрии считается домен общего пользования COM. На его примере мы и начнем исследовать особенности жизненного цикла доменов второго уровня.

Рождение

Итак, рождение домена в зоне .com начинается с периода так называемой предварительной регистрации (Add Grace Period). Он продолжается несколько дней, в течение которых регистратор ожидает поступления оплаты за регистрацию от администратора домена. То есть сперва домен регистрируется как бы в кредит (а по сути, бесплатно) и позже при непоступлении оплаты освобождается. Важно понимать, что подобная услуга доступна отнюдь не всем и далеко не во всех случаях, но она весьма распространена среди крупных игроков на рынке доменов и оказывается вполне официальный в соответствии с действующей политикой ICANN.

В чем главная особенность предварительной регистрации? Она позволяет желающим бесплатно тестировать домен в течение некоторого промежутка времени. С помощью подобного тестирования проверяется привлекательность домена для пользователей Интернета: если после регистрации на домене появляется достаточно большой трафик посещаемости, значит, домен стоит вложения средств в регистрацию. Понятно, что платное тестирование множества доменов сделало бы эту технологию невыгодной. Поэтому ключевое значение имеет тот факт, что испытания доменов можно проводить бесплатно.

Человеку, не посвященному в тонкости доменного рынка, может показаться, что вновь регистрируемый домен не способен обрести хоть какую-то посещаемость незамедлительно. Домен только что зарегистрирован, откуда же пользователи Интернета о нем узнают?

Однако на практике ситуация иная. Например, регистрируемый домен может быть не совсем новым, а являться «реинкарнацией» имени, ранее принадлежавшего какому-нибудь посещаемому сайту (скажем, домен не оплатили, и он был удален из реестра). Пользователи продолжают набирать запомнив-

шееся доменное имя в адресной строке браузера, создавая посещаемость домену. Более того, на ранее существовавший домен в Интернете может ссылаться некоторое число внешних страниц (иногда очень значительное), то есть посетители будут приходить по ссылкам. Дополнительные ссылки остаются в базах поисковых машин, и это еще один источник трафика посещений, причем данный трафик может оказаться очень ценным.

Некоторые совершенно новые домены могут привлекать посетителей потому, что связаны с какими-нибудь популярными офлайн-событиями, мероприятиями, происшествиями или, предположим, совпадают с названием популярного нового товара. Услышав новое название или прочитав его в газете, потенциальный посетитель домена может набрать его в адресной строке из чистого любопытства. На подобный источник популярности домена рассчитывают администраторы, регистрирующие имена, которые совпадают с именами и фамилиями звезд шоу-бизнеса или с названиями готовящихся к выходу литературных произведений из раскрученных книжных серий.

Хорошим примером служат истории вокруг романов о Гарри Поттере. За доменными именами, хоть в чем-то совпадающими с названием очередной книги сериала, шла настоящая охота. Чтобы предотвратить уход доменов в «нежелательные руки», агенты Джоан Роулинг (автора всех этих суперпопулярных романов) перед выходом очередного тома регистрировали множество доменных имен, перекликающихся с его названием. Например, до выхода в свет книги «Harry Potter and the Deathly Hallows» агенты писательницы регистрировали такие имена, как harrypotterandthedeathlyhallows.com и deathlyhallows.info (http://info.nic.ru/st/46/out_888.shtml). Конечно же, до появления в продаже новой книги эти домены не имели никакой привлекательности, однако после публикации романа сайтам под столь длинными именами обеспечен некоторый трафик, создаваемый поклонниками сериала о Гарри Поттере.



Итак, воспользовавшись периодом предварительной регистрации, потенциальный администратор домена может проверить, есть ли на этом домене трафик, и даже исследовать этот трафик с помощью статистики веб-сервера. Технология тестирования уже успела обрести историю, включающую несколько знаковых событий.

Например, технический центр, управляющий реестром доменов, имеет возможность автоматически отслеживать массовое тестирование имен регистраторами. Техническая сторона этого вопроса достаточно проста: любое изменение в реестре производится на компьютерах технического центра, который ведет довольно подробную статистику обращений к базам данных со стороны регистраторов (это делается и в целях балансировки нагрузки, и в целях правильного биллинга регистраторов). Так что наив-

ным было бы полагать, будто администраторы реестров домена COM не знали о массовом тестировании. Однако до 2002 года администраторы реестров, например компания VeriSign (лидер этого направления), закрывали глаза на сложившуюся ситуацию, полагая, что на падающем рынке (а интернет-рынок тогда просто обрушивался) любая активность на пользу.

Впрочем, в 2002 году, сославшись на вызванный тестированием большой рост нагрузки на реестры, VeriSign ввела технические ограничения, благодаря которым «окно массового тестирования» закрылось. Но не навсегда: уже в 2004 году тестирование доменных имен вновь оказалось возможным, так как VeriSign изменила технические условия доступа к реестру доменов. Основной причиной послужило то, что вторичный рынок доменных имен обрел новые инструменты (например, контекстную рекламу, соответствующую тематической направленности доменного имени), которые сулили большие прибыли техническим центрам реестров.

Однако к началу 2008 года над тестированием доменов вновь ступились тучи: корпорация ICANN предложила ввести небольшую плату (\$0,25) за предварительную регистрацию домена.

Следует кратко отметить и другой аспект управления доменами, связанный с тестированием. Это так называемый доменный кайтинг (kiting) (в некоторых публикациях в аналогичном значении также используется термин «скайтинг»). Данная технология состоит в том, что на протяжении бесплатного периода предварительной регистрации доменное имя регистрируется и практически тут же удаляется из реестра лишь для того, чтобы поставить то же самое имя на регистрацию вновь. Таким образом доменное имя может бесплатно удерживаться регистратором в течение некоторого времени, превышающего пятидневный период предварительной регистрации.

Несмотря на все особенности и хитрости начальной регистрации, рано или поздно домен оказывается успешно зарегистрирован администратором. Более того, при единичных регистрациях новых

доменов рядовым администратором все только что описанные перипетии обычно остаются за кадром, администратор может и не подозревать об их существовании. Тонкости регистрации касаются только компаний-регистраторов, технических центров, управляющих реестрами доменов, и тех, кто регистрирует домены массово.

После того как запись о домене внесена в реестр, начинается следующий этап в жизненном цикле домена.

Жизнь

В зависимости от правил администрирования домена первого уровня возможна регистрация имен на различные периоды времени. Например, в домене COM имена регистрируются на срок от одного года до десяти лет.

Обычно в течение первых 60 дней после регистрации смена администратора домена невозможна. Это означает, что вновь зарегистрированный домен нельзя будет сразу же продать, уступив права администрирования по спекулятивной цене другому администратору.

Многие домены сразу же после регистрации используются для размещения под ними различных ресурсов, например веб-сайтов. Некоторая часть зарегистрированных доменных имен так и останется неиспользуемой. Зарегистрированные домены не используются по разным причинам. Например, расторопные владельцы раскрученных торговых марок или веб-порталов могут столбить доменные имена, частично совпадающие с названием торговой марки или адресом портала, чтобы предотвратить тайпсквоттинг.

КСТАТИ



Подробнее о тайпсквоттинге я расскажу ниже. Пока же замечу, что этот вид «охоты за доменами» состоит в регистрации доменных имен с опечатками. Дело в том, что, набирая

в адресной строке имена доменов, пользователи иногда ошибаются. И если опечатки в адресе малопосещаемого, малоизвестного сайта не дают тайпсквоттеру существенного трафика посещений, то, например, «домен-опечатка», соответствующий адресу microsoft.com, может давать сотни посетителей в сутки.

Используемый для размещения веб-ресурса домен начинает «нагуливать вес». В зависимости от отношений ресурса с аудиторией домен может быстро набрать популярность, стать всем известным, а может так и остаться невостребованным. «Нагуливание веса» доменом выражается в нескольких факторах.

На размещенный под доменом ресурс приходят поисковые роботы (то есть роботы поисковых систем, например Google), собирающие информацию о веб-страницах, размещенных в Сети. Содержание найденных веб-страниц создает отпечатки в индексах поисковых систем, и позднее адреса этих страниц (очевидно, включающие доменное имя) могут выдаваться в результатах поиска, демонстрируемых поисковой системой своему пользователю в ответ на его запросы. Если по популярным поисковым запросам адреса веб-страниц, размещенных под данным доменом, выводятся на первых местах, то можно ожидать достаточно большого количества переходов с поисковой системы на данный домен (то есть можно ожидать трафика посетителей). Как мы выяснили выше, потенциальный поисковый трафик некоторое время сохраняется после удаления домена из реестра, а также после изменения контента веб-сайта.

Нужно заметить, что поисковые машины регулярно обновляют свои индексы, стараясь содержать их в состоянии релевантности, то есть максимально соответствующими реальности. Поэтому «мертвые» ссылки (ведущие на удаленный домен или на удаленную веб-страницу) через некоторое время изымаются из поискового индекса. Из этого следует простой вывод: даже если домен за время использования приобрел большой «поисковый вес», этот вес может быть быстро растрачен в случае удаления домена,

а значит, привлекательный удаленный домен должен быть «реанимирован» максимально быстро.

Домен, используемый для размещения того или иного привлекательного для аудитории веб-контента, также набирает «ссылочный вес». Владельцы других веб-ресурсов по различным причинам размещают на своих страницах гипертекстовые ссылки, которые могут давать данному домену существенный трафик посетителей. В отличие от поисковых индексов, потенциал ссылочного трафика обычно сохраняется в течение значительно большего времени: веб-мастера традиционно плохо следят за актуальностью ссылок. На некоторых сайтах встречаются ссылки на веб-страницы, которые были удалены многие годы назад.

«Ссылочный вес» домена плотно связан с его «поисковым весом». Дело в том, что поисковые машины для ранжирования результатов поиска в своих базах используют информацию о внешних ссылках, ведущих на данный домен с других веб-ресурсов. Однако подробный рассказ о таком разделе интернет-технологий, как поиск в вебе, остается за рамками этой книги.

Домен, под которым размещен веб-ресурс, также может приобретать популярность в офлайне, что прямо влияет на «вес» этого домена в онлайн. Наиболее ярким примером доменов, привлекательность которых в значительной степени определяется офлайном, являются домены, совпадающие с раскрученными интернет-брендами. Очевидно, что домены `yahoo.com`, `google.com` обладают в офлайне огромной известностью, которую они набрали именно в период регистрации.

Несмотря на то что веб сейчас является важнейшим аспектом Интернета, конкретный домен, доступный в DNS, может не использоваться для размещения веб-ресурса, а служить адресом для почтового сервера или для хранилища данных, доступного по протоколу передачи файлов FTP. Домен также может служить адресом сервера DNS (каким бы странным это ни показалось).

С другой стороны, в некоторых доменах верхнего уровня введены довольно строгие правила, регулирующие использование доменов. Так, в домене для мобильных сайтов `MOBI` настоятельно рекомендуется использовать зарегистрированный домен именно для размещения сайта, да еще не простого, а оптимизированного для просмотра с мобильного устройства связи, например с сотового телефонного аппарата.

На протяжении периода, когда домен является зарегистрированным, вне зависимости от того, делегирован ли он в DNS или нет, важнейшее с точки зрения доменного рынка событие, которое может приключиться с доменом, — это смена администратора. Смена администратора разрешается по истечении некоторого срока с момента регистрации домена; она лежит в основе вторичного рынка доменных имен, который возможен благодаря переуступке игроками друг другу прав по управлению тем или иным доменом. Подробно о вторичном рынке я расскажу в следующей главе.

Смерть

Права администратора на управление доменом требуют продления. То есть при каждой итерации домен регистрируется на некоторый срок, по истечении которого домен может быть удален из реестра. Удаление из реестра и есть смерть домена, потому что удаленный домен более не может быть доступен в DNS и использование его оказывается невозможным.

Обычно администраторы, заинтересованные в пролонгации своих прав на управление доменом, вносят очередной платеж регистратору, продлевая тем самым жизнь домену. Так может продолжаться очень долго: ограничений по числу продлений регистрации не вводится (за редкими исключениями, связанными, например, с удалением доменов первого уровня).

Однако то, что администратор не внес очередной платеж точно в срок, не означает, что домен будет удален моментально.

Напротив, чтобы забывчивые администраторы не оказались однажды утром без любимых доменов, введен специальный период, в течение которого администратор может вернуть себе «неоплаченный» домен по цене продления. В домене COM этот период называется Auto-Renew Grace Period.

В течение этого периода (а его продолжительность может варьироваться от нескольких дней до полутора месяцев) домен остается в DNS, однако вовсе не обязательно, что он будет продолжать указывать на ресурс прежнего администратора. Регламент зоны .com позволяет регистратору изменить информацию о DNS-серверах неоплаченного домена, перенаправив трафик посетителей на другие страницы. Иногда на такой странице размещается информация о том, что продление данного домена не оплачено и в скором времени он может быть удален из реестра. Однако главная польза этого периода для регистратора доменов в том, что с помощью перенаправления домена на новый сервер регистратор может провести тестирование трафика на домене.

Если администратор домена так и не оплатил продление, то в жизни (а в данном случае точнее будет сказать — в смерти) домена наступает новый период. В зоне .com это Redemption Grace Period. Запись о домене удаляется из DNS, то есть домен как бы уже мертв, однако в течение установленного срока (30 дней для доменов зоны .com) он может быть возвращен под управление прежнего администратора при условии, что последний оплачивает штраф, сумма которого значительно превышает стоимость продления регистрации. Продолжая аналогии, можно сказать, что возможна «реанимация» домена, но за нее, к сожалению, придется доплатить.

Если и в течение 30-дневного периода администратор не проявил желания заполучить управление доменом обратно в свои руки, домен должен быть удален из реестра. На это отводится некоторый срок — обычно пять дней. Удаление домена осуществляется регистратором.



Наиболее важной особенностью «предсмертного» состояния домена в настоящее время является то, что регистраторы и связанные с ними интернет-компании активно используют предоставленные регламентом возможности, чтобы предлагать домены на вторичном рынке. Если еще несколько лет назад для «брошенного» домена вполне реальной перспективой являлось простое удаление из реестра, то теперь интернет-компании заранее предоставляют списки освобождающихся доменов заинтересованным лицам, чтобы домен можно было вовремя «подхватить». Более того, предлагаются и услуги предварительной регистрации, в рамках которых регистратор принимает предварительные заявки от администраторов, желающих получить тот или иной зарегистрированный домен.

Домены также могут быть выставлены на аукцион, например, в том случае, если на данный домен предварительные заявки подали несколько администраторов.

Зомби? Нет — перерождение

После того как домен удален из реестра доменных имен, регистрация такого же домена оказывается доступна любому другому лицу; в стандартных случаях у прежнего администратора нет никаких приоритетов. Правда, подобные приоритеты могут возникнуть в результате судебных разбирательств, если выяснится, что домен был удален с нарушением регламента.

Спрос на доменные имена довольно велик, и многие домены, удаленные из реестра, через некоторое время наверняка вновь окажутся зарегистрированными. Возможно, тем же самым администратором, а скорее всего, другим. Таким образом, домен возрождается, и начинается новый виток его жизненного цикла. Возникновение и развитие инструментов вторичного рынка доменов поспособствовало тому, что процент возрождающихся к новой жизни доменов возрос.

Первый всплеск подобных «воскрешений» пришелся на время после схлопывания первого бума интернет-проектов, затронувшего на рубеже XX и XXI веков доменную зону .com. В период с 2001 по 2002 год разорилось множество проектов (так называемых дот-комов), ранее получивших инвестиции на волне интереса к интернет-сервисам и веб-технологиям. Оставшиеся от этих проектов доменные имена хлынули на вторичный рынок, дав ему решающий толчок к бурному развитию.

Циклы .ru

Жизненный цикл домена в зоне .ru довольно заметно отличается от циклов в зоне .com, хотя в общих чертах ситуации, конечно, схожи.

В домене RU фактически невозможно тестирование доменов без оплаты, так как отсутствует период предварительной регистрации — за внесение изменений в реестр доменов нужно заплатить.

Теоретически для тестирования доменов .ru можно использовать услугу по регистрации в кредит, которую предоставляют некоторые регистраторы. Однако на практике за такую услугу все равно придется заплатить, поэтому тестирование теряет смысл.

Регистрация доменов .ru производится сроком на один год. Разговоры о введении регистрации на более длительный период ведутся довольно давно, однако до сих пор решение об изменении соответствующей части Регламента зоны .ru не принято, а вокруг него идет дискуссия, у сторон которой есть аргументы и за, и против. Сторонники введения длительной регистрации говорят о том, что многим администраторам доменов было бы проще сразу оплатить домен на несколько лет, чем регулярно «возиться» с продлением регистрации. Противники изменения сроков считают, что разрешение многолетней регистрации приведет к захвату множества доменов предприимчивыми киберсквоттерами и к одномоментному выведению этих доменов из оборота на длительный срок.

В течение первых 60 дней с момента регистрации домена RU (или с момента смены администратора) не производится передача прав администрирования домена, то есть оказывается невозможной реализация домена на вторичном рынке.

После истечения годового срока регистрации домен в зоне .ru снимается с делегирования, то есть становится недоступным для адресации в DNS, однако в течение 30 дней администратор может продлить регистрацию по цене продления.

Если регистрация не была продлена, то в течение трех дней домен должен быть удален из реестра. Начиная с этого момента домен может быть зарегистрирован другим лицом. Некоторые регистраторы зоны .ru предлагают «забывчивым» администраторам услугу по восстановлению прав на управление доменом и после истечения 30-дневного регламентного периода. Для этого регистраторы после освобождения домена тут же регистрируют его на себя и предлагают администратору в течение некоторого срока

(например, 90 дней) выкупить права на домен, оплатив штрафные санкции.

Если все сроки прошли, а продление регистрации домена не оплачено администратором, то домен освобождается, а запись о нем удаляется из реестра доменов .ru. С этого момента доменное имя может зарегистрировать другой администратор (или тот же самый, если он вдруг вспомнит о необходимом имени и опередит конкурентов).

Глава 10

Вторичный рынок

- ☐ Механизмы
- ☐ Люди
- ☐ Инструменты
- ☐ Доходы

После прочтения предыдущих глав книги можно сделать верный вывод: сам по себе домен не может быть продан, так как не является материальным или даже нематериальным активом. Ведь домен — всего лишь кусочек виртуального адресного пространства Интернета. Как же тогда возник вторичный рынок доменов? Дело в том, что вторичный рынок доменов построен не на продаже доменов, а на переуступке прав управления тем или иным именем.

Впрочем, в прессе или просто в беседах, даже между специалистами, употребляется и термин «продажа домена». При этом, конечно, имеется в виду возмездная переуступка прав управления доменным именем. Далее я также иногда буду заменять юридически верный оборот «возмездная переуступка права управления доменным именем» разговорным словосочетанием «продажа домена».

Регистрация доменных имен не всегда была платной, да и сейчас она не обязательно платная. На заре Интернета за регистрацию доменных имен даже в зоне .com плата не взималась. Сейчас существует множество доменных зон различного уровня и типов, где регистрация имен бесплатна (в качестве очевидного примера можно вспомнить зоны второго уровня .net.ru, .com.ru, которые упоминались выше). Так что реальная стоимость регистрации, как и другие условия, сопровождающие регистрацию, определяются тем, в какой зоне регистрируется имя.

Бесплатная регистрация влечет за собой определенные проблемы, самая главная из которых — невозможность эффективного противодействия сквоттерству. Ведь если за имя не нужно платить, ничто не мешает заинтересованному администратору с помощью программы-бота занять все привлекательные имена в зоне. Это и произошло однажды в зоне .com.ru. Для предотвращения подобных ситуаций «исчерпания доменов» используют различные ограничивающие меры. Например, требуется написать заявку-обоснование на получение бесплатного домена или ограничивается максимально возможное число доменов, приходящихся на одного администратора.

О бесплатных доменах мы вспомнили не просто так. Оказывается, однажды занятый бесплатный домен запросто может стать платным для других желающих его получить: ведь за то, чтобы передать бесплатный домен другому администратору, администратор действующий вполне может потребовать некоторую «денежную компенсацию». Хотя, конечно, все зависит от конкретных правил.

Механизмы

Передача прав администрирования, или смена администратора домена, и есть базовый механизм, лежащий в основе вторичного рынка. Другими словами, вторичный рынок не мог бы возникнуть, если бы не существовало формально-юридических процедур, позволяющих администратору домена отказаться от своих прав в пользу другого конкретного администратора. Предположим, был бы возможен только отказ от администрирования домена, а после того как администратор отказался от своих прав, домен освобождался бы. Понятно, что после освобождения домена в большинстве популярных доменных зон его мог бы занять первый обратившийся. Гарантированная передача домена конкретному администратору была бы невозможна, соответственно, и платить дополнительную цену за понравившийся домен никто не стал бы.

Таким образом, инструменты вторичного рынка доменных имен строятся вокруг обслуживания механизма передачи прав администрирования. И пока этих инструментов не было, вторичный рынок не развивался и, можно сказать, пребывал на полулегальном положении. Например, в главе 5 я рассказывал о том, что длительное время правила зоны .ru прямо запрещали продажу доменов, несмотря на то что практика продажи имен вполне активно развивалась.

Относительно морально-этической стороны вторичного рынка — если только можно применить этот термин к подобному роду коммерческой деятельности — существует несколько точек зрения.

Среди них есть и строго запретительные, сторонники которых считают, что вторичного рынка доменов не должно быть в принципе. Одним из довольно сильных аргументов «запретителей» является такой: если пользователь Интернета набирает в браузере адрес `vezdehod.ru` (транслитерация слова «вездеход»), то этому пользователю должен быть показан либо сайт о вездеходах, либо сообщение о том, что домен не зарегистрирован и свободен для регистрации. Вариант, при котором домен не связан с сайтом о вездеходах и при этом зарегистрирован администратором, предлагающим его на продажу, представляется несправедливым. Эту позицию нельзя назвать нелогичной, ведь она опирается на вполне разумное предположение о том, что система адресации Интернета должна соответствовать некоторым «мнемоническим ожиданиям» типичного пользователя: набирает «вездеход» — значит, желает читать про вездеходы.

КСТАТИ



Интересно, что такая трактовка особенностей адресации в Интернете не чужда разработчикам различных поисковых систем, которые иногда используют буквальное значение доменного имени в качестве одного из факторов упорядочивания «поисковой базы».

Однако, к счастью или к сожалению, предположение о «мнемонических ожиданиях» не выдерживает столкновения с реальностью. Во-первых, Интернет коммерциализировался, и компании готовы платить за право получить то или иное привлекательное имя, сделав его тем самым недоступным для конкурентов.

Во-вторых, практически невозможно так формализовать правила использования доменных имен, чтобы на основании этих правил можно было уверенно судить: да, домен используется по назначению. Например, вовсе не ясно, о чем же именно должен рассказывать сайт `vezdehod.ru`. Если на нем размещен интернет-магазин, торгующий квадроциклами, — это использование по назначению или уже нет? А если это страничка о любимом коте администратора домена и Вездеход — кличка кота?

Однако курьезней всего (и это в-третьих) то, что изначально система доменных имен не создавалась для следования «мнемоническим ожиданиям» пользователей, как считают сторонники жесткого тематического регулирования. Исконное предназначение системы — введение удобных для использования людьми имен компьютеров Сети. А именем компьютера, так же как и кличкой кота, может быть любое слово. При этом кот Вездеход не обязан передвигаться на четырех колесах и иметь полный привод, точно так же и компьютер под именем `vezdehod.ru` не обязан рассказывать что-то о вездеходах.

Несмотря на такие, казалось бы, очевидные доводы, владельцы привлекательных доменов, застолбившие их в свое время, продолжают иногда получать от других желающих приобрести хорошее имя письма, в которых сообщается: «Доменное имя используется вами не по назначению; пожалуйста, передайте его нам».

Единственное более или менее реализуемое на практике правило, связанное с определением использования домена по назначению, могло бы требовать от администратора обязательной привязки доменного имени к веб-сайту. Впрочем, даже такое правило выглядит излишне жестким, так как рядовой администратор мог планировать использовать свой домен только для создания адресов электронной почты. При этом на вторичном рынке уже давно появились инструменты, позволяющие домену не простаивать, пока он продается: это сервисы паркинга доменов, о которых я расскажу чуть ниже.

Люди

Если еще несколько лет назад довольно большое число участников интернет-рынка неприязненно относились к людям, которые пытались зарабатывать на перепродаже «красивых» доменов, то сейчас ситуация изменилась. Вторичный рынок доменов набрал обороты, на нем сложились правила, в правовом отношении он по большей части вышел из серой зоны. Ранее владельцев

множества доменов, предлагавших свои владения на продажу, называли киберсквоттерами — словом с отрицательной эмоциональной окраской. Сейчас игроков вторичного рынка доменов уже делят на киберсквоттеров и домейнеров.

Домейнеры (или доменные инвесторы) — это люди, зарабатывающие на спекуляции доменами, но при этом не нарушающие некоторых неписаных правил хорошего тона. Так, домейнеры не столбят домены, совпадающие с торговыми марками, с целью последующего шантажа — такое делают только киберсквоттеры. Домейнеры же придумывают красивые, привлекательные имена, которые могут быть востребованы на рынке, и в дальнейшем предлагают их выкупить всем желающим по договорной цене. Чтобы угадать, будет ли имя востребовано, домейнеры часто изучают историю Глобальной сети, пытаясь предсказать тенденции. Иногда такая деятельность выливается в глубокие аналитические исследования.

Конечно, большинство крупных домейнеров — бывшие киберсквоттеры. И конечно, в домейнерстве есть много пограничных приемов, которые не так просто вписать в правила хорошего тона. Один из примеров — упоминавшаяся выше регистрация «опечаток» (доменов, представляющих собой раскрученные имена, набранные с опечаткой, например microsoft). Ведь если речь идет о торговых марках, то огораживание раскрученного домена сетью доменов-опечаток вряд ли можно отнести к справедливой игре.

На вторичном рынке доменов .ru есть игроки, управляющие многими тысячами доменов, а есть и те, у кого доменов всего несколько десятков. Так как имеются легальные и удобные инструменты по продаже прав администрирования доменов и поскольку финансовый порог вхождения на этот рынок невысок, домейнером-любителем может стать каждый. Ведь чтобы попробовать свои силы, достаточно зарегистрировать несколько доменов .ru и, подождав положенное время, выставить их на аукцион.

Однако чтобы стать профессионалом, нужно приобрести опыт и вложить некоторые весомые средства в формирование перво-

начального «инвест-пакета», состоящего из многообещающих имен. Действительно крупных игроков на вторичном рынке домена RU немного: весной 2008 года их число не превышало двух десятков. Всего же администраторов, которых можно отнести к домейнерам, в домене RU набиралось едва ли более двух сотен.

Инструменты

Во времена становления вторичного рынка особых инструментов на нем не было. Посмотрим на домен RU. Как я писал выше, длительное время продажа прав администрирования доменов здесь вообще была запрещена. Но права продавались.

Как это происходило? По «серой» схеме. Стороны, одна из которых права продавала, а другая приобретала, договаривались об «обмене». Например, сперва покупатель передавал продавцу деньги, после чего продавец запускал формальную процедуру по смене администратора домена, в которой, конечно, участвовал и покупатель. Продавец домена подавал регистратору доменов (в те времена регистрацией занимался РосНИИРОС) официальное заявление о смене администратора, где указывался новый администратор-покупатель. При этом в официальных бумагах регистратора стороны сделки не обозначались как «продавец» и «покупатель» и суммы не оговаривались.

В описанной схеме покупателю не давалось никаких гарантий, что домен действительно будет передан ему. В принципе, недобросовестный продавец, получив деньги, мог и не проводить процедуру изменения администратора либо воспользоваться другими уловками, с тем чтобы оставить домен за собой или своим сообщником. Понятно, что аналогичный риск угрожает и продавцу, если будет использована схема «сперва товар, потом деньги». Отобрать права администрирования у продавца до того, как домен перешел к покупателю, мог и регистратор, которому стало известно о нарушении регламента домена RU, явно, прямым текстом запрещавшего продажу прав и вводившего ответственность за нарушение.

КСТАТИ



Нужно заметить, что сделки по «обмену домена на деньги», нарушавшие регламент национального домена RU, вовсе не становились автоматически сделками, грубо нарушающими российские законы. Именно поэтому мы называем их «серыми». Регламент администрирования национального домена не только не имел силы закона или хотя бы подзаконного акта, но он по характеру практического действия на третьи стороны даже не был сравним, скажем, с отраслевой инструкцией Министерства связи. Нарушение регламента администратором домена в худшем случае являлось не более чем нарушением условий рядового коммерческого договора о предоставлении неких услуг. Собственно, обязанность администратора следовать регламенту и прописывалась в договоре оказания услуг. Конечно, нарушение условий подобного договора в теории может являться серьезным основанием для судебного иска, однако из-за этого сам договор вовсе не обретает силы закона.

В большинстве случаев нелегальным торговцам доменами не было никакого резона обманывать клиентов. Рынок был слишком мал, все друг друга знали, и возможные потери многократно превысили бы маржу от одной расстроенной сделки. Регистратор доменов также смотрел сквозь пальцы на нелегальные сделки по купле-продаже. Расследований и дознаний не проводилось, права администрирования практически никогда не отзывались, и длительное время РосНИИРОС вообще делал вид, что никаких продаж на вторичном рынке просто нет (хотя сделки на тот момент исчислялись многими десятками).

Если стороны, совершавшие сделку по домену, желали дополнительных гарантий, то даже несмотря на «серый» характер договоренности ничто не мешало им привлечь в качестве гаранта третью сторону, благо такие механизмы в бизнесе давно отработаны и используются довольно часто. Например, сделку можно было бы осуществлять через доверенную организацию (банк), которая передавала бы деньги продавцу только после того, как домен будет переоформлен на покупателя. Понятно, что продавец в таком случае начинал бы переоформлять домен только после того, как покупатель передал деньги доверенной организации. А в случае

неожиданного вмешательства регистратора посредник мог просто вернуть деньги покупателю. Впрочем, на заре вторичного рынка доменов .ru продавец все равно рисковал потерять доменное имя, которое продавал в нарушение регламента. Однако этот риск всегда был скорее теоретическим, а с внесением в Регламент зоны .ru «разрешительных поправок» и вовсе исчез.

Дополнительные трудности не способствовали росту вторичного рынка доменов .ru, по препятствий оказалось явно недостаточно для того, чтобы предотвратить его возникновение. Вторичный рынок рос, и уже в начале 2000-х годов его участники регистрировали домены на продажу тысячами, чему немало способствовало снижение стоимости регистрации, состоявшееся в феврале 2001 года.

Под давлением реальности регистраторы доменов поняли, что придется смириться с существованием вторичного рынка, а самым правильным выходом будет предоставление этому рынку необходимых инструментов для совершения сделок. В таком случае по крайней мере регистратор не упустит свой кусок пирога.

Первым регистратором, официально поддержавшим вторичный рынок доменов, стал RU-CENTER (крупнейший регистратор в зоне .ru). В 2004 году RU-CENTER предложил официальный аукцион доменов, тем самым вторичный рынок доменов окончательно вышел из «серой» зоны в «белую». Аукцион позволял администраторам выставить домен на продажу по некоторой начальной стоимости. Затем проводились торги на повышение, и домен передавался покупателю, сделавшему максимальную ставку, после ее оплаты.

Передачу прав управления доменом проводил регистратор RU-CENTER, таким образом выступая гарантом сделки. Аукцион не только позволял администраторам, желавшим передать права на свой домен, найти покупателя в более широком круге лиц, но и обеспечивал успешность сделки.

Очевидно, что регистратор мог выступать гарантом сделки лишь по тем доменам, которые у него зарегистрированы. В 2004 году в домене RU действовало несколько регистраторов, а аукцион

проводил только RU-CENTER, поэтому, чтобы воспользоваться удобным инструментом продаж, администратор должен был сперва перевести домен в RU-CENTER.

Нужно заметить, что, хотя появление официального аукциона доменов и сняло последние сомнения относительно легальности продажи доменов в Рунете, число сделок на аукционе RU-CENTER не впечатляло. Так, в 2004 году было проведено всего несколько продаж, а спустя три года, в 2007 году, число сделок за год едва превысило сотню. Тем не менее аукцион доменов RU-CENTER сыграл важную роль в становлении вторичного доменного рынка, да и в развитии доменных реалий Рунета вообще. В 2008 году свои аукционы запустили и другие регистраторы доменов.

КСТАТИ



Выше, в главе, рассказывавшей о жизненном цикле домена, я описал несколько вариантов событий, которые могут приключиться с доменом в зоне .ru по истечении срока его регистрации (1 год). В одном из вариантов домен освобождается. Этот вариант имеет важное значение и для аукционов доменов. Дело в том, что регистратор имеет технические возможности, позволяющие зарегистрировать домен сразу же после его освобождения. Реализация этих возможностей позволяет предоставить клиентам такую услугу, как регистрация освобождающегося домена (или отложенная регистрация). В рамках этой услуги клиент регистратора может заранее подать заявку на регистрацию того или иного доменного имени из *уже зарегистрированных*, в случае если данное доменное имя освободится.

При чем здесь аукцион? По очевидным причинам на уже зарегистрированный домен может быть подано несколько отложенных заявок от разных клиентов регистратора. Единственный осуществимый на практике и более или менее справедливый способ определить, кому же в итоге достанется домен, если он освободится, — это проведение закрытого аукциона между всеми подавшими заявки клиентами.

Регистрация освобождающегося домена не обязательно будет успешной. Если на домен поступило несколько заявок, то регистратору, предоставляющему услугу, придется сначала зарегистрировать доменное имя на себя, с тем чтобы после окончания торгов на закрытом аукционе передать домен победителю.

Услугу по отложенной регистрации освобождающихся доменов первым в Рунете также предложил регистратор RU-CENTER весной 2006 года. Введение услуги стало возможным после некоторых изменений в правилах удаления доменов.

Интересно, что необходимость регистрировать домен на регистратора для проведения аукциона некоторое время служила основанием для обвинений RU-CENTER в киберсквоттерстве. Обычно события «на обвиняющей стороне» развивались следующим образом. Потенциальный новый администратор освобождающегося домена, используя сервис WHOIS, замечал, что интересный для него домен находится на грани удаления из реестра (как я рассказывал выше, сервис WHOIS позволяет определить дату возможного освобождения домена). С этого момента пользователь Сети, запланировавший приобрести права на данный домен, принимался ждать удаления домена из реестра, периодически посещая сервис WHOIS, чтобы сразу же после удаления быстро, но обычным образом подать заявку тому или иному регистратору на регистрацию этого же имени.

Однако на практике пользователя часто ждало разочарование. Однажды он обнаруживал, что опоздал: едва освободившийся домен уже зарегистрирован на компанию RU-CENTER. Вообще говоря, такая ситуация означала, что привлекательный домен заинтересовал не только «пострадавшего» пользователя, а нескольких потенциальных администраторов, и они заблаговременно подали заявки на регистрацию освобождающегося имени в RU-CENTER. Естественно, возможности регистратора, имеющего прямой, автоматизированный доступ к реестру доменов, по оперативному «подхватыванию» удаляемого домена превышают возможности рядового пользователя, вооруженного «ручной подачей заявки», приблизительно настолько же, насколько возможности бульдозера по расчистке лесных завалов превышают возможности муравья. Поэтому освобождающийся домен достается прежде всего регистратору, но лишь для того, чтобы позже он передал имя участникам аукциона. Однако те, кто не подал заявки на аукцион, а надеялся «подхватить» домен собственными силами, ошибочно интерпретировав данные WHOIS, упрекали RU-CENTER в киберсквоттерстве: дескать, регистратор столбит домены в свою пользу.

Надо заметить, что механизмы автоматизированной регистрации доменов действительно использовались киберсквоттерами, причем намного раньше, чем RU-CENTER предложил услугу отложенных регистраций. Суть автоматизации состоит в том, что заявки на регистрацию доменов подает не человек, а компьютер,

который использует специальные списки доменов и соответствующие программы. Конечно, рядовой киберсквоттер или домейнер не может получить прямого доступа к реестру доменов .ru. Согласно правилам доступ к реестру технический центр домена предоставляет только аккредитованным регистраторам. Однако регистраторы предоставляют своим клиентам специальные программные интерфейсы, позволяющие автоматизировать операции с доменами. Можно сказать, что регистратор в данном случае служит неким «автоматическим мостом» между своим партнером и реестром доменов. Соответственно, киберсквоттер или домейнер может, став партнером регистратора, использовать программный интерфейс для автоматизации своей деятельности. Конечно, из этого нельзя делать вывод, что все партнеры регистраторов — киберсквоттеры.

Интересно, что если использование программного интерфейса партнером регистратора начинает противоречить интересам самого регистратора, то последний может ограничить партнерский доступ к интерфейсу. Например, ограничивается число регистраций доменов в единицу времени или периодичность получения полного списка зарегистрированных доменов.

Аукционы доменов как таковые не позволяют охватить все виды сделок на вторичном рынке. Они скорее относятся к инструментам, привлекающим новых игроков. Однако существенная часть сделок по доменам все равно будет проводиться администраторами вне аукциона. Наиболее очевидный вид сделок, для которых аукцион совершенно не нужен, — это сделки, в которых продавец передает домен одному конкретному покупателю. Такие сделки возникают не только по инициативе продавцов доменов, домейнеров. Напротив, в некоторых случаях покупатель сам находит продавца и уговаривает администратора понравившегося домена переуступить права за вознаграждение. Как мы разобрались выше, для таких сделок часто нужен доверенный посредник.

В 2005 году все тот же регистратор RU-CENTER представил сервис, позволявший осуществлять направленную передачу домена от одного администратора другому под гарантии регистратора. То есть третьей стороной — гарантом сделки — выступал регистратор продаваемого домена, что, конечно же, оказывалось очень привлекательным и разумным вариантом, ведь изменение

данных администратора домена также проводит регистратор. Направленная передача прав от действующего администратора другому администратору, тому, которого укажет действующий, проводится только после того, как покупатель исполнил свои финансовые обязательства, перечислив обозначенную сумму сделки RU-CENTER.

Коммерческий интерес регистратора, запускающего «вторичные» сервисы, отчасти заключается в том, что с каждой сделки он получает свой процент. Но это не единственный плюс. Так, предлагая инструменты вторичного рынка, регистратор привлекает новых клиентов, удерживает старых и получает возможность увеличить свою долю в общем числе зарегистрированных доменов. Привлеченные богатым инструментарием клиенты не только будут регистрировать новые домены у этого регистратора, но, возможно, перенесут к нему зарегистрированные у конкурентов домены.

Итак, в 2008 году многие регистраторы повторили шаги RU-CENTER и запустили свои аукционы. Однако общая тенденция на вторичном рынке доменов .ru уже была другой. К весне 2008 года на рынке действовало несколько крупных регистраторов доменов и множество администраторов. При этом реализация доменов на вторичном рынке хоть и обрела большее удобство по сравнению с тем, что было несколько лет назад, но все еще сталкивалась с рядом трудностей. Основная часть этих трудностей происходила от того, что клиентам по-прежнему требовалось посещать офисы регистраторов либо отправлять бумажные документы почтой, чтобы совершить некоторые операции над доменами.

Даже при использовании аукциона RU-CENTER (напомню, что это аукцион-первопроходец, законодатель рыночной моды) продавец, прежде чем получал возможность выставить домен на аукцион, должен был подать в RU-CENTER официальное заявление-поручение на бумаге. Заявление требовалось либо лично доставить в офис по работе с клиентами регистратора, либо прислать почтой; во втором случае к заявлению необходимо было приложить еще и нотариально заверенную доверенность.

С аналогичными проблемами сопряжена была и смена регистратора домена. Здесь в большинстве случаев администратору требовалось посетить офисы двух регистраторов (того, от которого домен забирается, и того, которому домен передается), лично подать два заявления: одно — с требованием передать домены другому регистратору, второе — с требованием принять указанные домены на обслуживание. При этом регистраторы могли еще потребовать нотариально оформленную доверенность на право осуществлять управление доменами.

Все эти юридические препоны возникли не на пустом месте. Так как право управления тем или иным доменом может стоить кругленькую сумму, регистраторы стремились обезопасить себя от возможного мошенничества, предотвращая неправомерные «угоны» доменов. Подробнее о правовых сложностях управления доменами мы поговорим в отдельной главе. Сейчас же отмечу, что необходимость разъезжать по офисам регистраторов с пачкой нотариально оформленных документов (а в особо сложных случаях — и вместе с нотариусом) не может добавлять легкости участию во вторичном рынке доменов. Особо печально документальная ситуация вокруг сделок с доменами выглядит на фоне повсеместного торжества систем электронных подписей и управления банковскими счетами через Интернет.

Поэтому важной тенденцией 2008 года на вторичном рынке доменов стало увеличение доступности сделок для клиентов. То, что ключ к развитию лежит не в запуске новых аукционов, а в удобных веб-интерфейсах и «магазинах доменов», не требующих личного присутствия покупателя и продавца в офисах регистраторов, стало понятно еще в середине 2007 года. А уже в 2008 году регистраторы стали упрощать процедуры управления доменами, стараясь сохранить безопасность и надежность сделок. Одни разрешали переводить домены к себе без лишней бумажной волокиты и посещения офиса, другие упрощали смену администратора.

Более того, весной 2008 года в Рунете появился первый в своем роде сервис, объединивший в себе и «магазин доменов», и единую панель управления для всех ведущих регистраторов доме-

нов. Проект «Дом доменов», который на момент написания книги еще проходил этап тестирования, заявлял о том, что его клиент сможет переводить домены от регистратора к регистратору и изменять администратора доменов без бумажного сопровождения операции. «Дом доменов» также позволяет (как обещано) регистрировать новые домены, причем не только в зоне .ru, и покупать уже зарегистрированные домены без присутствия в офисе — через единый веб-интерфейс.

Реализация подобных функций требует механизма, дающего гарантии, что сделка через веб-интерфейс действительно совершается с теми параметрами, которые заявлены клиентом. «Дом доменов» использует для создания таких гарантий парботки онлайн-платежных систем, в частности популярной системы Webmoney, которые при проведении платежей сталкиваются с теми же самыми проблемами проверки подлинности пользователей и «валидности намерений» этих пользователей.

Однако основное преимущество платежных систем как потенциальных партнеров «магазинов доменов» не в том, что они технически готовы обеспечивать гарантии достоверности исходных данных сделки. Нет. В конце концов, ведущие регистраторы доменов также имеют в своем распоряжении нужные технические средства. Преимущество платежных систем в том, что их владельцы и администраторы накопили огромный практический опыт по юридическому сопровождению проблемных сделок (а таковые неминуемо возникают в работе любой платежной системы) и по решению проблем, возникающих в результате совершения подобных сделок.

КСТАТИ



Поможет ли опыт платежного рынка на рынке доменном? Однозначного ответа здесь нет. При обнаружении платежей, неверно проведенных в результате мошеннических действий злоумышленников или в результате ошибки в программной системе, убытки (по крайней мере одной из сторон) часто могут быть покрыты из средств платежной системы (из специального фонда). В дальнейшем можно пытаться возместить потери фонда платежной

системы разными способами: разыскивая злоумышленников, возвращая товары и т. п. В случае с доменами ситуация гораздо сложнее: доменное имя — уникальный и дефицитный ресурс, а оперативно «возместить» домен, умело уведенный в результате мошенничества, невозможно. Отыграть проблемную сделку с доменом назад — также задача не из легких, иногда требующая привлечения к судебному разбирательству многих сторон (различных регистраторов, администраторов доменов, экспертов и, возможно, координационного центра домена RU).

Еще одной особенностью проекта «Дом доменов», которая отражает направление развития рынка и скорее всего будет достаточно быстро реализована другими игроками, является форма представления уже зарегистрированных доменов потенциальному покупателю. Здесь доменные имена собраны на «виртуальном прилавке» и упорядочены по их возможному назначению, а точнее, по тематике. Поскольку на вторичном рынке покупатель часто приобретает домен под какой-то проект, домены на «прилавке» представлены подобно книгам в книжном магазине: в одном разделе домены для интернет-магазинов, в другом — для фотогалерей, в третьем — для персональных страниц (например, домены-фамилии) и т. д. При этом домены, естественно, предлагаются по спекулятивной цене, которая, впрочем, иногда незначительно превышает стоимость прямой регистрации домена. Владельцы проекта в этом случае надеются заработать на количестве сделок, получая с каждой лишь небольшую прибыль.

Инструменты вторичного рынка не исчерпываются аукционами, направленной передачей прав и «магазинами доменов». Есть инструмент, который стоит несколько особняком, но имеет прямое отношение ко вторичному рынку, — это сервис паркинга (или парковки) доменов.

Паркинг доменов — сервис, позволяющий привязать доменное имя к некоторой веб-странице (или к нескольким веб-страницам), на которой будет демонстрироваться заранее и автоматическим способом подготовленный контент. Обычно это реклама, представляющая собой тематические объявления. Однако возможны и другие варианты (например, публикация ссылок на веб-сайты).

То есть зарегистрированный и «запаркованный» домен в случае, если пользователь набрал его в адресной строке браузера, приведет такого пользователя на страницу, где будет показана реклама. Содержание рекламных объявлений подбирается под тематику домена: демонстрируются контекстные объявления. Тематика определяется либо сервисом «парковки» автоматически, либо при участии администратора домена. В определении тематики может играть роль как семантическое значение домена (например, *vezdehod.ru* — сайт о вездеходах), так и содержание поисковых запросов, по которым посетители переходят на сайт под доменом из поисковых систем (эти запросы доступны для анализа на стороне веб-сервера).

Существенный трафик порой приносят «домены-опечатки», то есть доменные имена, которые пользователи набирают по ошибке. Например, пользователь может опечататься при наборе адреса популярного веб-ресурса (скажем, *odnokassniki.ru* вместо *odnoklassniki.ru*). Как я рассказывал выше, такие «домены-опечатки» могут давать большое количество посещений ежедневно.



Формально «припаркованный» домен связан с веб-сайтом, на котором размещается какая-то информация. Основное отличие паркинга заключается в том, что контент веб-сайта генерируется сервисом автоматически, а не создается администратором домена. Такой подход позволяет сделать сервис массовым: администратору достаточно лишь подключить свой домен к паркингу, а контент появится сам собой. При этом сервисы паркинга стараются сделать массовые автоматически генерируемые «парковочные веб-сайты» максимально похожими на настоящие веб-сайты штучной работы. Технологически развитые паркинги предоставляют сайты, содержащие целую иерархию страниц.

В подавляющем большинстве случаев цель «парковочных страниц» — отправить попавшего на эту страницу посетителя по рекламной ссылке (либо это будет ссылка из рекламного объявления, либо прямая ссылка на другой сайт). При этом за каждый переход рекламодатель выплачивает некоторое вознаграждение (в большинстве случаев подобная реклама оплачивается по схеме «за переходы»). Вырученные за размещение рекламы средства делятся между сервисом паркинга и владельцем домена, под которым размещаются «парковочные» страницы. Таким образом, зарегистрированный домен может приносить доход своему администратору.

Паркинг — один из самых удобных механизмов «монетизации». Если домен зарегистрирован не с целью размещения под ним какого-либо ресурса, то паркинг позволяет получать небольшой доход с домена без дополнительных затрат. При этом размещенный на паркинге домен может быть одновременно выставлен на аукцион.

Доходы

Стать участником вторичного рынка доменов довольно легко. Самый простой способ — зарегистрировать несколько интересных доменов и выставить их на аукцион. Не следует, конечно, надеяться на неминуемые огромные барыши. Вероятность того,

что на вторичной продаже удастся заработать миллионы (пусть не сразу, а хоть когда-нибудь), стремится к нулю. Взвешенно подходящие к вопросу люди — доменные инвесторы, или домейнеры — могут получать заметные доходы с доменного бизнеса, не более того.

Миллионные сделки за всю историю вторичного рынка единичны, даже с учетом того, что не вся информация о суммах сделок по доменам становится доступна публично. Хрестоматийной стала сделка с доменом *sex.com*, который сперва был украден у первоначального владельца, потом «походил по рукам», а в итоге был возвращен хозяину, который спустя несколько лет (в 2006 году) продал его за \$12 млн. В 2007 году за очень крупные суммы ушли домен *porn.com* (\$9,5 млн) и *computer.com* (\$2,1 млн).

Десятка самых дорогих доменов за всю историю вторичного рынка, насчитывающую уже более десяти лет, на момент написания книги (2008 год) выглядела не слишком блестяще.

1. Sex.com (\$12,5 млн).
2. Porn.com (\$9,5 млн).
3. Diamond.com (\$7,5 млн).
4. Business.com (\$7,5 млн).
5. Casino.com (\$5,5 млн).
6. Asseenontv.com (\$5 млн).
7. Korea.com (\$5 млн).
8. Wine.com (\$3,3 млн).
9. Creditcheck.com (\$3 млн).
10. Vodka.com (\$3 млн).

Подсчитывая количество нулей в ценниках, нужно понимать, что крупнейшие сделки по доменам — во многом элемент пиар-кампаний, ставящих своей целью и раскручивание площадок, торгующих доменами, и раскручивание самих доменных имен, и создание дополнительной «прессы» старым и новым владельцам

нашумевших доменов. Этим списком задачи по формированию общественного мнения, решаемые миллионными сделками по купле-продаже, конечно же, не исчерпываются.

Реальные масштабы сделок по доменным именам даже в популярной зоне COM не будоражат воображение. Типичная цена привлекательного домена второго уровня .com на вторичном рынке измеряется скорее сотнями и тысячами долларов, чем десятками тысяч и тем более миллионами.

Российский национальный домен RU ожидаемо уступает транснациональной зоне .com. Так, в 2007 году средняя сумма сделки по доменам .ru находилась в районе \$3000 (данные по сделкам, которые прошли через компанию RU-CENTER). Нужно учитывать, что это средняя цена домена и в ее формирование существенный вклад вносят единичные сделки с большими суммами. Согласно сообщению интернет-издания «Иифоцентр» (http://info.nic.ru/st/60/out_1629.shtml) за несколько лет на аукционе RU-CENTER проданы такие «дорогие» домены, как:

- ❑ Travels.ru (\$19 050);
- ❑ Valeria.ru (\$15 020);
- ❑ Rabotnik.ru (\$11 200);
- ❑ W1.ru (\$5656);
- ❑ Coach.ru (\$5000).

То есть практика показывает, что в лучшем случае можно надеяться реализовать домен за несколько сотен долларов. При этом все «словарные» домены (то есть домены, соответствующие распространённым русским и английским словам) в зоне .ru давно зарегистрированы, а некоторые из них даже проданы на вторичном рынке.

Оценивая возможные прибыли и убытки от доменных инвестиций, следует начинать с одного очень простого расчета: стоимость регистрации домена на год (без скидок, максимальная) в зоне .ru — 600 руб. (2008 год); если домен в год регистрации

удалось продать на вторичном рынке, выручив 1200 руб. (чистая прибыль около \$24), то доходность сделки составит 100 % годовых. И это немало. Однако при этом удачливый доменный инвестор сможет положить в карман лишь 600 руб. за год. А это немного.

На вторичном рынке продаж доменов возможны два основных подхода:

- ❑ доход формируется за счет единичных продаж «за большие деньги»;
- ❑ доход формируется за счет большого числа продаж «за небольшие деньги».

Долгое время преобладал первый подход, который можно даже назвать традиционным. Однако с развитием инструментов продаж доменов появляется надежда, что возможен и второй подход, который требует существенной автоматизации всего процесса передачи доменов. Автоматизация нужна для того, чтобы накладные расходы на осуществление каждой транзакции не съели прибыль: если для смены администратора в рамках сделки с чистой прибылью 500 руб. продавцу придется ехать в офис регистратора, тратя 500 руб. на такси, то вряд ли сделка имеет смысл (разве что она служила лишь поводом для личной встречи с покупателем).

Оба способа получения доходов от спекуляций доменами требуют соблюдения одного условия: домены должны быть в дефиците. Особенно это важно при стратегии «дорогих продаж». Ведь разумный покупатель всегда может рассмотреть альтернативные предложения. И если домен с условным именем «КрутойДомен.ru» продается на вторичном рынке по условной цене в один миллион рублей, а домен «СтольЖеКрутойДомен.ru» доступен по цене регистрации (600 руб.), то потенциальный покупатель может предпочесть вложить полмиллиона в раскрутку второго имени, предварительно зарегистрировав его за «смешные деньги». Другое дело, если «СтольЖеКрутойДомен.ru» уже занят и предлагается на вторичном рынке за два условных миллиона.



К счастью (или к сожалению), в домене RU, где к моменту выхода книги из печати, по мнению автора, будет более полутора миллионов регистраций доменов второго уровня, ощутимый дефицит привлекательных имен сложился сам собой. А из этого следует вывод: наступает вполне подходящее время для умелой игры на вторичном рынке. А с возможным появлением в ближайшие годы кириллического домена РФ возникнет и новое поле для игры на доменном рынке.

Принести неплохой доход даже в условиях дефицита имен способно планирование доменных инвестиций с «упреждающим анализом» офлайн-тенденций в развитии тех или иных отраслей хозяйства и сфер человеческой деятельности. Продемонстрирую на примерах, в чем состоит этот подход.

Предположим, доменному инвестору стало известно, что в ближайшее время (скажем, через год) возникнет огромный интерес к продажам скульптур из канадской березы через Интернет, хотя

на момент исследования никто такими продажами в Сети не занимался. Домейнер заранее регистрирует разнообразные имена доменов, пересекающиеся в семантическом плане со скульптурами и канадской березой. Например, доменные имена могут содержать конструкции наподобие *skulptura-kb*. Зарегистрировав множество «скульптурно-березовых» доменов (которые по причине отсутствия интереса на момент регистрации свободны), домейнер создаст дефицит подобных имен на будущее и в дальнейшем сможет продать некоторые из этих доменов по спекулятивной цене. Конечно, он может ошибиться в прогнозах, и интерес к продажам скульптур из канадской березы через Интернет не возникнет. В этом случае наш инвестор понесет убытки, поскольку занятые доменные имена не будут востребованы. Но таков весь инвестиционный бизнес: вложение денег здесь сопряжено с определенными рисками.

Приведенный пример — теоретический. Однако он подтверждается тем, что еще задолго до принятия Международным олимпийским комитетом (МОК) решения о проведении зимней Олимпиады 2014 года в Сочи были зарегистрированы практически все интересные домены в различных доменных зонах, содержащие оборот *sochi2014*. А спустя несколько месяцев после принятия МОК решения в пользу Сочи «олимпийские» домены начали уходить с молотка, в некоторых случаях за суммы в тысячи евро.

Паркинг доменов позволяет зарабатывать на доменах, составляющих инвестиционный портфель, пока они не проданы. Как упоминалось выше, паркинг приносит доход от переходов по рекламным объявлениям. В большинстве случаев трафик на «припаркованном» домене невелик, соответственно, невелик и доход от одного домена (хотя бывают и исключения).

Рассмотрим пример. Предположим, что размещенный на паркинге домен приносит ежемесячный доход в \$1 (\$12 в год). Микроскопическая сумма. При этом регистрация домена по полной стоимости обойдется в \$25 в год. То есть домен приносит убыток. Теперь попробуем подойти к вопросу с другой стороны.

Предположим, что домейнер регистрирует тысячу доменов. В этом случае он может рассчитывать на скидку и, скажем, каждый домен обойдется домейнеру уже в \$8 в год. Если каждый из этих доменов на паркинге приносит те же \$12 в год (\$1 в месяц), то домейнер уже не в убытке, а напротив, заработает не менее \$4000 в год. То есть доходность составит 50 % годовых. Неплохо. Конечно, это лишь теоретический пример. На практике не у всех есть тысяча доменов, но и не все домены приносят \$1 в месяц: с удачных имен можно получить многим более.

В заключение этой главы взглянем на показательную таблицу, в которой представлено распределение администраторов доменов в зоне .ru по числу доменов в управлении (данные предоставлены проектом stat.nic.ru).

Таблица 2. Распределение администраторов доменов в зоне .ru по числу доменов в управлении (по состоянию на 1 января 2007 г.)

| Число доменов в управлении | Число администраторов |
|----------------------------|-----------------------|
| > 10000 | 1 |
| 1001–10 000 | 47 |
| 101–1000 | 460 |
| 11–100 | 9912 |
| 1–10 | 447 563 |

Глава 11

Безопасность и домены

- ☐ Безопасное администрирование
- ☐ Уверенный доступ
- ☐ Достоверность: а туда ли я попал?
- ☐ Заверено подписью

Безопасность систем адресации Интернета — очень актуальная и живо обсуждаемая в профильных сообществах тема. Только по проблемам безопасности DNS за последние годы написано множество научных трудов. Это неудивительно: DNS лежит в основе большинства современных способов получения доступа к ресурсам Интернета со стороны пользователей, поэтому значительная часть хакерских атак так или иначе задействует DNS. Однако целью этой книги не является подробное освещение многочисленных проблем информационной безопасности в современном Интернете, так как решение подобной задачи потребовало бы и значительно большего объема материала и специальных математических знаний от читателя. Тем не менее мы в популярном изложении коснемся всех основных вопросов доменной безопасности с точки зрения администратора доменов и интернет-пользователя.

Так как DNS — один из краеугольных камней современного Интернета, от надежной и безопасной работы этой системы зависит буквально каждый пользователь Глобальной сети. Чтобы оказаться в роли пострадавшего от дыр в безопасности доменов, вовсе не обязательно быть администратором домена или иметь собственный сайт в вебе. Жертвами фишинговых атак, построенных с помощью поддельных имен доменов, в основном становятся рядовые пользователи Сети, скажем, использующие ее для доступа к системам онлайн-банкинга (это программные комплексы, позволяющие клиентам банков управлять своими счетами через веб-браузер или через другую программу, работающую по каналам Интернета).

КСТАТИ



Текущую ситуацию с безопасностью систем адресации в Интернете нельзя назвать хорошей. А классическая DNS вообще лишена каких бы то ни было механизмов обеспечения информационной безопасности. Причина в том, что, когда разрабатывалась DNS, многих угроз современного сетевого компьютерного мира просто не существовало, даже в лабораториях. Их тогда еще не успели разработать. Более того, четверть века назад Интернет не был столь агрессивным пространством,

в которое он превратился сейчас, в конце первого десятилетия XXI века, поэтому и о противодействии активным злоумышленникам, вмешивающимся в работу сетевых протоколов, думали не так много, как теперь. Выбранный путь развития требует решать проблемы безопасности с «древними» протоколами в основном с помощью надстроек. Однако заметны и попытки обновить базовые протоколы, приведя их в соответствие с реалиями (самый масштабный пример — новая версия протокола IPv6; это базовый «транспорт» Интернета, используемый в том числе и DNS).

Чтобы несколько упростить изложение, разделим вопросы доменной безопасности на три большие группы.

1. Управление правами доступа администраторов доменов.
2. Доступ к ресурсам, размещенным под доменами, со стороны всего остального Интернета.
3. Достоверность DNS и доверие к доменам со стороны пользователей Сети.

На чем основано такое деление? Прежде всего на том, что эти три группы различаются в техническом плане. Первая группа вопросов касается социальной инженерии, документооборота между регистратором и конкретным администратором домена. Вторая — технологий и принципов работы серверов DNS, непосредственно обслуживающих домен. Третья — технологий работы распределенной DNS Интернета и методов, используемых злоумышленниками «на стороне клиента» (то есть на компьютерах рядовых пользователей Сети).

Так, кража злоумышленником паролей доступа к папкам домена второго уровня у законного администратора — это проблема прав доступа, то есть проблема из первой группы. Отказ обслуживающих домен серверов DNS, приведший к недоступности размещенных под доменом ресурсов, — это проблема доступа из второй группы. Подделка записей, соответствующих доменному имени, в локальной DNS интернет-провайдера относится к третьей группе.

Попробуем взглянуть на ситуацию чуть более детально.

Безопасное администрирование

Как мы выяснили ранее, домены не продаются. Но за деньги можно приобрести право управления доменным именем. Права управления, полученные администратором домена, требуют надежного фиксирования и не менее надежных механизмов авторизации, иначе у администратора возникнут трудности с проведением прав в жизнь. Права по управлению доменом фиксируются в специальных базах данных, которые имеются у администраторов доменов первого уровня и у компаний-регистраторов.

Что угрожает администратору домена? Самая серьезная угроза — «угон» домена, то есть неправомерный переход домена под контроль злоумышленников. Как ни странно, «угон» может быть произведен с помощью разнообразных инструментов, причем некоторые из них вовсе не требуют использования высоких интернет-технологий.

Например, злоумышленники могут подделать нужные документы (заявления, доверенности) и выполнить процедуру смены администратора домена. Именно с целью предотвращения подобных проблем регистраторы в домене RU и требуют представления довольно большого количества бумаг и личного присутствия администратора домена в офисе. В некоторых случаях при сомнительных операциях по раскрученным и хорошо известным доменам регистратор может провести и дополнительную проверку «легитимности», скажем, перезвонив руководству компании — владельца домена по телефону и т. п.

Одна из самых больших проблем, создающих серьезные риски, — неверное делегирование полномочий по управлению доменом внутри компаний и официальных организаций.

Хрестоматийный пример касается корпоративных сайтов. Сейчас даже самая небольшая фирма считает нужным иметь свой сайт. У маленьких компаний нет ни юридического департамента, ни службы ИТ, поэтому корпоративный сайт поручают изготовить и запустить тому сотруднику, который, по мнению руко-

дителя фирмы, наиболее близок к Интернету. Нередки случаи, когда эта «почетная обязанность» достается секретарше директора, умеющей «поискать в Интернете». Также кандидатами на создание сайта часто оказываются «обобщенные программисты», дизайнеры, заместители директора по техническим вопросам, так называемые эникейщики и др. Несложно догадаться, что создание сайта достается случайному сотруднику, никак с сайтостроением не связанному.



Что в итоге? В итоге сотрудник, получивший задачу создать корпоративный сайт и выяснивший, что для этого потребуется домен второго уровня, регистрирует подходящий домен на себя. Как показывает практика, в подавляющем большинстве случаев сотрудник вовсе не имеет злого умысла — он просто желает избежать лишней бумажной волокиты. Более того, обычно он получает одобрение руководства на такую регистрацию: «Ну, ты же будешь сайтом заниматься, вот и регистрируй на себя».

Некоторое время с новоиспеченным «корпоративным» доменом все хорошо. Под ним работает корпоративный сайт, который при нынешних темпах роста Интернета вполне способен в скором времени стать важнейшей «витриной» компании. Но однажды сотрудник, зарегистрировавший домен, увольняется.

С этого момента с доменом начинаются большие проблемы. Он, по сути, находится «в угоне». Внести изменения в параметры работы домена, продлить его регистрацию — эти операции должны осуществлять либо сам администратор домена, либо его доверенное лицо. Оказывается, фирма не имеет практического контроля над «корпоративным» доменом, который уже стал важным элементом повседневного делового оборота (электронная почта, визитки, обмен прайс-листами и др.). Доменом может управлять только уволившийся сотрудник, и никаким способом нельзя убедить компанию-регистратора, что «на самом деле это наш корпоративный домен». Ведь регистратор действует согласно Правилам доменной зоны, а они четко прописывают роль администратора домена.

Администратор домена может просто не оплатить продление регистрации (действительно, зачем, если он уже не работает в компании?) — в результате домен будет освобожден, а фирма останется без корпоративного сайта.

Обиженный сотрудник, оказавшийся администратором «корпоративного» домена, может попытаться отомстить с его помощью, например, сделав с корпоративного сайта перенаправление на сайт конкурентов компании или (случай из жизни) разместив вместо корпоративного сайта веб-страницу, сообщающую изумленным клиентам и партнерам, заглянувшим по привычному адресу: «Извините, наша компания находится в процессе банкротства, а офис более не работает».

Мне не раз и не два приходилось помогать владельцам небольших компаний решать подобные «доменные проблемы». В каких-то случаях удавалось договориться с бывшим сотрудником компании (которого еще нужно было разыскать), являвшимся

администратором домена, и он соглашался передать права администрирования самой компании. Иногда, впрочем, делалось это за вполне весомое материальное вознаграждение («поймите, я же трачу на вас свое время!»). Кстати, если возврат «угнанного» домена производится через судебное разбирательство, то весомые преимущества компания может получить, только если имя домена совпадает с фирменным наименованием компании или, что еще лучше, с зарегистрированной торговой маркой (товарным знаком). Иначе домен остается ресурсом сотрудника-администратора, и отсудить его весьма сложно. В некоторых случаях просто не удавалось изыскать правовых способов решения проблемы. Пострадавшей компании приходилось регистрировать другой домен и сообщать всем клиентам и партнерам об изменении контактных данных. Тем не менее ситуация, в которой распоряжение правом администрирования корпоративного домена находится «в подвешенном состоянии», остается весьма распространенной и по сей день.

О том, как правильно зарегистрировать корпоративный домен, и о чисто юридических трудностях «владения» таким доменом я расскажу в главе 12, посвященной правовым вопросам. А сейчас взглянем на другие инструменты перехвата управления доменами.

На корпоративном уровне возможен спланированный «угон» домена директором компании. Так, если смена администратора домена может быть проведена регистратором на основании письма от генерального директора (или просто директора) компании, то ничто не мешает наемному работнику — директору «угнать» домен у владельцев компании. Для этого директор, действуя от имени юридического лица, производит смену администратора домена и передает домен либо себе, либо своему сообщнику. В результате владельцы компании, для которой доменное имя может являться важным, а иногда единственным ценным активом, его лишаются. Оспорить подобную операцию довольно трудно, если, опять же, имя домена не совпадает с фирменным обозначением или зарегистрированной торговой маркой.

Если для «угона» домена часто требуются бумажные документы, то перехватить управление можно и по «бесбумажной технологии». Так, регистраторы предоставляют своим клиентам веб-интерфейс, служащий для оперативного управления доменами через Интернет с помощью веб-браузера. Обычно доступ к веб-интерфейсу производится с авторизацией пользователя по паролю (используется пара логин/пароль; логин — системное имя, присвоенное данному клиенту). Злоумышленник, которому стал известен пароль (и логин) клиента регистратора для доступа к веб-интерфейсу, получает возможность перехватить управление веб-интерфейсом. Соответственно, все операции с доменами клиента, доступные через веб-интерфейс и не требующие дополнительной авторизации, оказываются в распоряжении злоумышленника.

Предположим, что добропорядочный клиент размещает под доменом свой веб-сайт. Злоумышленник, получив управление доменом через веб-интерфейс, может изменить записи DNS для домена таким образом, что домен будет указывать на другой сайт, например на интернет-ресурс, находящийся под контролем хакеров. Для чего это нужно злоумышленнику? В некоторых случаях лишь для того, чтобы потешить самолюбие, разместив под перехваченным доменом страничку с информацией о хакерской группировке, которая взломала сайт. Однако в более изощренных планах перехваченный домен может служить платформой для сложной атаки с подменой сайтов, состоящей из нескольких ступеней и имеющей своей целью вполне конкретные способы извлечения прибыли (незаконные, конечно).

Раскрытие пароля к веб-интерфейсу также возможно с помощью целой палитры наработанных методов. Во-первых, администратор домена может самостоятельно разгласить пароль, записав его на листке бумаги, прикрепленном к компьютеру: «Мой пароль для доменов: 31415926». Во-вторых, пароль можно узнать, используя электронную почту: либо просматривая почтовый трафик (если пароль пересылался в незашифрованном сообщении), либо перехватив управление почтовым ящиком атакуемого клиента и запросив пароль у сервера регистратора с помощью по-

пулярных механизмов напоминания пароля. В-третьих, пароль можно подобрать, задействовав автоматические программы, работающие с применением словаря (не у всех регистраторов есть эффективная защита от массовой проверки пользовательских паролей злоумышленниками). Существуют и другие способы.

Что делать администратору домена, чтобы уменьшить риски? Прежде всего, сохранять пароль в тайне и не пользоваться веб-интерфейсом с чужих компьютеров. Следующий шаг — узнать, не предоставляет ли регистратор дополнительных средств защиты веб-интерфейса. Среди таких методов:

- использование нескольких паролей, например технического и административного. Первый пароль может позволять лишь просматривать настройки доменов и выполнять только самые безопасные действия, а для внесения сколько-нибудь критичных изменений будет требоваться дополнительный ввод административного пароля;
- ограничение доступа к веб-интерфейсу на основании клиентского IP-адреса (способ довольно эффективный, хоть и не всегда удобный). То есть сервер регистратора позволяет использовать веб-интерфейс для управления доменом (даже при условии указания паролей и логинов) только с компьютеров, имеющих IP-адреса из разрешенного списка. Этот список клиент формирует самостоятельно и для активирования функции лично предъявляет регистратору.

Растет доменный рынок, а вместе с ним — и число компаний-регистраторов. Самым ожидаемым образом рост числа регистраторов приводит к тому, что ширится и разнообразие их подходов к ведению бизнеса. Например, в домене RU весной 2008 года действовало более десяти заметных регистраторов. Это компании, отличающиеся и формой собственности, и внутренней организацией, и деловым стилем. В дальнейшем также ожидается рост числа регистраторов.

Такая ситуация приводит к возникновению относительно нового аспекта в проблемах доменной безопасности, связанного

со степенью доверия к регистратору со стороны клиента: насколько можно быть уверенным в том, что у компании-регистратора не возникнет серьезных проблем, в результате которых клиент может лишиться своего домена. Степенью уверенности в большой степени определяется выбор регистратора.

Данная проблема характерна не только для домена RU. Нельзя, конечно, делать вывод, что все новые компании обязательно ненадежны. Накладки возникают и у старейших, крупнейших регистраторов. Тем не менее проблема существует, и рост числа регистраторов ее усугубит.

Наглядным примером может служить недавняя история с американским регистратором RegisterFly, который лишился аккредитации ICANN в 2007 году. У RegisterFly, работавшего в том числе с популярными доменами COM и NET, возник внутренний производственный конфликт в совете директоров. Из-за общей неразберихи и технических проблем компания попросту перестала выполнять свои функции по управлению доменами, в результате у клиентов этого регистратора возникли не просто технические трудности: несколько тысяч из них вообще остались без доменов.

Так как с точки зрения реестра доменов администратор конкретного имени оказывается представлен своим регистратором, то проблемы регистратора обязательно отразятся на администраторе и на его возможностях по управлению доменным именем. Поэтому, выбирая регистратора и заботясь о безопасности, администратору домена следует обратить внимание на историю компании и на методы ее работы, а не исходить из принципа «где дешевле».

Вернемся к домену RU. Как я писал в главе, посвященной национальному домену России, сумма, которую регистратор перечисляет в пользу реестра и технического центра домена RU, составляет 70 руб. (весна 2008 года) за каждую операцию регистрации домена. На эту сумму регистратор делает наценку, обеспечивая собственную прибыль. Например, домен для конечного пользо-

вателя может стоить 600, 500 или даже 200 руб. Из чего формируется регистраторская наценка? Из расходов регистратора по сопровождению доменного имени и взаимодействию с клиентом — администратором этого имени. Понятно, что уже оформление отдельного договора с клиентом и прием от него заявки на доменное имя потребуют затрат (оплата труда сотрудника, принимающего договор, и т. д.). В наценку также включаются расходы на обеспечение надежной работы регистраторских функций компании (ведение базы данных клиентов, работа с реестром доменов, предотвращение возможных сбоев).

КСТАТИ



Доменная наценка, очевидно, не связана напрямую с безопасностью доменов. С одной стороны, было бы странно ожидать, что надежность выполнения функций по управлению доменом клиента можно обеспечить за сумму, близкую к нулю рублей. С другой — понятно, что средства на управление доменами могут выделяться компанией-регистратором из доходов, получаемых от других видов деятельности.

Обеспечить гарантии клиентам регистраторов доменов могут дополнительные меры, принимаемые на уровнях администраторов национальных доменов или даже ICANN. Наиболее очевидные из этих мер:

- резервирование клиентских баз данных с привлечением независимых хранителей;
- обеспечение прозрачной и хорошо работающей процедуры перевода клиентов проблемных регистраторов к другим регистраторам с сохранением доменов.

Со своей стороны, администратор домена при выборе компании-регистратора должен принимать во внимание и ее надежность.

Уверенный доступ

Если под зарегистрированным доменным именем размещаются какие-то ресурсы, то домен нужно привязать к определенным

серверам DNS, обеспечивающим преобразование символьных имен внутри домена в адреса компьютеров, обслуживающих ресурсы. Например, адрес `www.test.ru` может соответствовать компьютеру, на котором работает веб-сервер, обслуживающий сайт `www.test.ru`. Регистрация домена сама по себе, как формальная процедура, не связана с последующим размещением каких-либо онлайн-ресурсов. Однако если такие ресурсы появились, то для их адресации будут использованы серверы DNS, которые связаны с конкретным доменом через общую, глобальную иерархию систем адресации.

Предположим, под зарегистрированным доменом размещается веб-сайт. Оказывается, чтобы обеспечить доступ к этому веб-сайту для пользователей, знающих его под доменным именем (а такая адресация уже давно стала единственно возможным вариантом не только для массовой аудитории Сети, но и для поисковых машин и прочих онлайн-сервисов), требуется надежное функционирование серверов DNS, связанных с доменом.

То есть сам сервер, на котором размещен веб-сайт, может работать бесперебойно, но, если откажут серверы DNS, достучаться к этому серверу по привычному адресу не получится. Таким образом, веб-сайт просто исчезнет из поля зрения его посетителей. Так что надежность серверов DNS играет важную роль в обеспечении доступности веб-сайтов и других онлайн-ресурсов, в том числе систем электронной почты. Домен должно обслуживать несколько серверов DNS, это позволяет повысить надежность: в случае недоступности одного из серверов на помощь придут другие.

Серверы DNS доменного имени могут быть выбраны более или менее произвольно, скажем, они вовсе не обязательно должны принадлежать регистратору доменов (хотя это довольно распространенная практика). Часто услуга размещения DNS предоставляется хостинг-провайдерами.

Итак, администратор домена должен использовать надежные серверы для организации DNS. При этом нужно иметь в виду, что

доступность домена также зависит от работоспособности вышестоящих серверов иерархии. Так, если нарушатся записи, соответствующие доменному имени второго уровня в базах серверов DNS, ответственных за домен первого уровня, то, очевидно, домен второго уровня также может оказаться недоступным. Правда, серьезные проблемы с DNS доменов верхнего уровня случаются довольно редко.

Серверы DNS часто служат объектом атак со стороны хакеров. Например, могут быть организованы атаки типа «отказ в обслуживании». Отказавшие DNS-серверы не смогут обслуживать запросы, и размещенные под соответствующим доменом ресурсы будут недоступны.

DNS-серверы, а точнее, программное обеспечение компьютеров, на которых работает конкретная DNS, могут быть взломаны хакером. В таком случае получивший доступ к серверу хакер сможет управлять и доменом (или несколькими доменами), обслуживаемым этим DNS-сервером. Это означает, что хакер может перенаправить трафик с ресурсов администратора на какие-нибудь свои ресурсы. С точки зрения пользователя Сети, новые хакерские онлайн-ресурсы будут доступны под теми же самыми доменами, которые ранее соответствовали легальным сайтам или адресам электронной почты. Другими словами, происходит «угон» домена в интересах хакера.

Итак, для обеспечения надежной работы своего домена администратор должен правильно выбрать серверы DNS. Желательно использовать услуги по аренде DNS, предоставляемые крупными регистраторами или хостинг-провайдерами. Хорошей практикой является одновременное использование нескольких DNS-серверов, находящихся у разных провайдеров.

Достоверность: а туда ли я попал?

Самым большим по количеству разнообразнейших проблем является класс доверия к доменам и DNS в целом. Причина в том,

что классическая DNS вообще не предусматривает эффективных способов проверки достоверности данных со стороны пользователя Интернета. При этом для неподготовленного пользователя адрес, переданный DNS, служит своего рода элементом психологического подтверждения того, что пользователь зашел именно на тот сайт, который обозначен адресом в адресной строке браузера. Этот факт наиболее активно эксплуатируется злоумышленниками, так что рассмотренные выше аспекты доменной безопасности для хакеров служат лишь фундаментом к использованию проблем из класса доверия.

Чтобы составить представление о том, насколько важна достоверность DNS, взглянем на один реальный пример (названия фигурирующих в этой истории компаний упоминаться не будут).

Несколько лет назад на рынке широкополосного доступа к Интернету г. Москвы появился новый игрок — один из крупнейших (впрочем, можно сказать, самый крупный) общегородских операторов связи. Новый провайдер, используя доступные практически в каждой квартире абонентские линии, предлагал широкополосный (то есть очень быстрый) и качественный доступ к Интернету по весьма и весьма разумной цене, да еще и построенный с помощью «верных технологий».

На момент появления этого игрока основными поставщиками широкополосного квартирного Интернета в столице являлись разнообразные домовые сети — небольшие компании (иногда даже не имевшие юридических оснований для своей работы), подключающие квартиры и дома к Глобальной сети с помощью технологий построения локальных вычислительных сетей, а именно Ethernet. Мы не станем сейчас обсуждать технические особенности сетей интернет-доступа и преимущества различных технологий. Нам важно отметить один момент: с приходом на рынок упомянутого крупного игрока домовые сети «почуяли», что грядет конец их существования. Особенно плохо себя почувствовали мелкие сети, так как начался стремительный отток клиентов: новый провайдер предлагал более выгодные тарифы и более качественные услуги, противопоставить которым было нечего.

Разумеется, у нового игрока имелся красивый корпоративный сайт, где рассказывалось о тарифах и способах подключения. Потенциальные клиенты, узнав о новом провайдере из рекламы (например, по телевидению), направлялись на корпоративный сайт, чтобы подробнее ознакомиться с услугами. Вполне естественный и понятный способ формирования клиентской базы.

Понимали это и владельцы — администраторы домашних сетей. А также они понимали, что их клиенты для доступа к корпоративному сайту провайдера-конкурента будут пользоваться домашней сетью: другого способа подключения к Интернету у клиентов нет.

Так вот, администраторы одной из домашних сетей (скорее всего, «находка» использовалась не только в этой сети) изменили записи своей локальной DNS таким образом, что доступ к сайту конкурента для клиентов этой сети оказывался невозможным. (Тут нужно отметить, что клиентов того или иного интернет-провайдера традиционно обслуживают его DNS-серверы. И конечно, настройки этих DNS-серверов целиком находятся в руках администраторов локальной сети.)

С точки зрения пользователя все выглядело так, будто сетевая неисправность находится на стороне корпоративного сайта конкурента домашней сети. Посетитель набирал в адресной строке браузера имя домена, увиденное в рекламе, и попадал на «испорченный» сайт, в итоге перебрасывавший браузер на веб-страницу головной компании холдинга, в который входил конкурирующий с домашней сетью оператор. При этом в адресной строке браузера отображался именно адрес из рекламы — домен корпоративного сайта провайдера — и пользователь был уверен, что все делает правильно.

Рассерженные пользователи из этой домашней сети, ничего не подозревавшие о подмене DNS, изливали гнев на интернет-форумах: «Ничего не понимаю! У них сайт не работает, ничего найти нельзя. Как же так можно! Бред! Я не стану пользоваться услугами оператора, который даже собственный сайт “из рекламы”

не умеет наладить!». При этом, подчеркнем, для всего остального Интернета сайт из рекламы конкурента домашней сети хорошо работал и внятно доносил до своих посетителей информацию об услугах. Эти посетители из других уголков Интернета долго вообще не могли понять, что имеют в виду их обозленные «коллеги» по общению на форумах. «Да как же? Вот же ссылка — все об услугах написано!» — возражали они, так как в их браузерах открывался совсем другой сайт, хоть и под тем же доменным именем. Обманутые же с помощью DNS клиенты домашней сети «попадали не туда», совершенно об этом не подозревая.



Целью акции, несомненно, являлось отпугивание клиентов от услуг конкурента. Понятно, что подобное мероприятие можно отнести лишь к разряду поступков «обезумевшего администратора». В итоге подлог довольно быстро раскрылся, ведь Интернет существует и вне «обиженной» домашней сети, а клиенты, узнав об истинном положении вещей (некоторых оно шокировало), полностью утратили доверие к нагло обманувшему их провайдеру. Домашняя сеть не «прожила» после этого и полугодя. Что, впрочем,

только подчеркивает важность проблемы с подделкой ответов DNS.

Администратор, официально зарегистрировавший домен, должен понимать: сам факт регистрации совсем не гарантирует, что другие пользователи Сети увидят под этим доменом именно тот веб-сайт, который разместил администратор. К сожалению, DNS, находящаяся в данном случае между владельцем домена и конечным пользователем Интернета, позволяет провайдерам на местах подделать соответствие домена и сайта.

Нужно отметить весьма важный момент: сама по себе DNS не является пособником хакеров, подделывающих сетевые адреса. Напротив, тщательное соблюдение стандартов и протоколов DNS приведет к тому, что все адреса будут настоящими, а система будет работать без сбоев. Корень проблемы в другом: DNS не позволяет противодействовать активным злоумышленникам, которые осознанно нарушают протоколы и стандарты. Другими словами, не являясь источником зла, классическая DNS этому злу попустительствует.

При этом действенных мер, позволяющих бороться с подделкой ответов DNS о сайтах, пока не выработано. Хотя проблема специалистам понятна и способы ее решения ищутся. Например, одним из методов противодействия подделке ответов DNS является технологическая инициатива DNSSEC (<http://www.dnssec.net/>), предлагающая набор мероприятий, которые позволят DNS-серверам, ответственным за тот или иной конкретный домен, подписывать ответ с помощью электронной подписи и механизма сертификации. Введение DNSSEC позволяет на стороне операционной системы компьютера конечного пользователя проверять корректность полученных от локального DNS-сервера ответов об адресах сайтов.

Другой способ, позволяющий помочь администратору домена удостовериться, что конечные пользователи будут видеть под доменом именно тот сайт, который разместил там администратор, — это введение дополнительных защищенных каналов связи

между браузером конечного пользователя и неким авторитативным сервером. Пользователя обязательно придется уведомить об этом по каналам, в той или иной мере независимым от провайдера, хотя бы с помощью защищенной электронной почты.

Конечно, общепринятые (но не имеющие юридической силы) правила работы в Интернете запрещают провайдерам нарушать связность сети и валидность DNS. А подделка сетевых реквизитов числится в ряду самых серьезных нарушений. Тем не менее провайдеры правила нарушают — с умыслом и без — по разным причинам: будь то цензура содержимого Сети (как в описанном выше случае с домовой сетью), системный сбой или хакерская атака. Радует только одно: такие нарушения пока не носят массового характера. Даже цензура в Интернете осуществляется (там, где она есть, например в локальных сетях крупных корпораций) не путем подделки адресов, а путем явного запрета доступа к тому или иному ресурсу с извещением пользователя о таком запрете.

Заверено подписью

Итак, у DNS есть множество хорошо известных специалистам проблем безопасности. Однако наиболее важная — это проблема с достоверностью адресной информации, что неудивительно, ведь определение адресов веб-узлов — та задача, для которой, собственно, DNS и создавали. Выше мы разобрали показательный пример с подделкой адресной информации на DNS-сервере, которому вынуждены доверять пользователи конкретного интернет-провайдера. Однако это лишь одно из воплощений проблемы, самое очевидное.

На первый взгляд может показаться, что для «подсовывания» конечному клиенту DNS дефектной информации об адресах узлов злоумышленник должен контролировать используемый атакуемым компьютером сервер DNS, ну, или по крайней мере находиться в одной сети с атакуемым компьютером. Но на практике дела обстоят гораздо хуже. Особенности реализации обмена запросами и ответами в DNS позволяют злоумышленнику атако-

вать даже весьма удаленные от его узла системы, и успешные атаки клиентских машин вовсе не требуют контроля над DNS-серверами. Однако в таком случае реализация атаки усложняется и требует параллельной работы нескольких «хакерских сетевых механизмов», которые, впрочем, хорошо изучены и отработаны.

Другими словами, у злых хакеров, хорошо владеющих интернет-технологиями, есть возможность направить по ложному адресу даже те пользовательские компьютеры, которые подключены к Интернету через добросовестных провайдеров, чьи сетевые администраторы следят за работой своих DNS-серверов. Более того, существует целый класс атак на DNS, которые используют особенности межсерверного взаимодействия внутри системы доменных имен. Здесь непосредственной целью являются сами DNS-серверы (а точнее — данные в их адресных таблицах), но конечная задумка практически всякой такой атаки — введение в заблуждение либо компьютеров конечных пользователей, либо других серверов (не имеющих отношения к DNS). Для чего? Обычно для того, чтобы получить доступ к закрытым информационным ресурсам, перехватить пароли для управления теми или иными сервисами, считать из удаленной и обособленной (в организационном плане) компьютерной сети какие-либо данные.

Атаки через уязвимости DNS могут быть чрезвычайно эффективны. Тем не менее системной защиты от них в Интернете пока нет (2008 год), она только конструируется. Впрочем, неверно думать, будто специалисты лишь недавно разгадали уязвимости DNS. О системных недостатках этого механизма адресации известно уже много лет, можно сказать, с самого рождения DNS.

Возникает вопрос: почему за все эти годы не внедрили какие-нибудь исправления протоколов, корректирующие ситуацию? Ответ на этот вопрос такой: только недавно практический ущерб от уязвимостей DNS стал выглядеть весомым в глазах достаточного числа специалистов, продвигающих и внедряющих новые интернет-технологии. Ранее возможные затраты на внедрение изменений в работе DNS в сумме с риском вовсе потерять связность доменной системы имен в процессе изменения протоколов легко

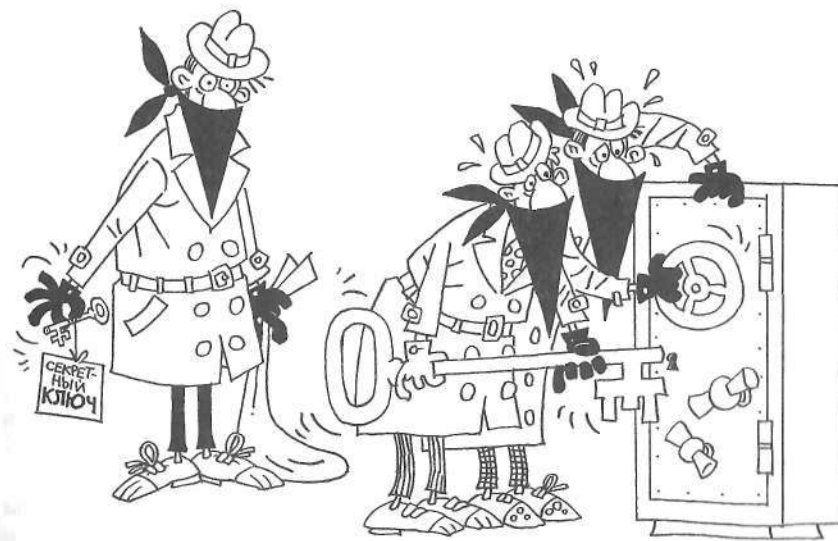
перевешивали практический вред от использования уязвимостей. Другими словами, довольно сложно убедить инертное провайдерское сообщество Интернета (у членов которого, будем говорить прямо, проблемы безопасности конечных пользователей не являются первоочередными) ввести ту или иную новую сложную технологию в дополнение к хорошо работающей и простой или вместо нее. Нужно заметить, что внедрение в DNS всякой функциональности «управления доверием» значительно усложняет систему, повышает требования к оборудованию и обслуживающему персоналу. То есть в конечном итоге защита DNS напрямую связана с прибыльностью провайдеров.

Впрочем, это лишь одна часть проблемы. Другая часть, не менее важная, связана с политическими факторами, как и следует ожидать в Глобальной сети. Подробнее о них — чуть ниже, а сейчас остановимся на том решении проблем безопасности DNS, у которого сейчас максимальные шансы на внедрение в Интернете.

Итак, для реализации «более безопасной DNS» предлагается такая технология, как DNSSEC, уже упоминавшаяся выше. DNSSEC позволяет, с одной стороны, удостоверять данные в адресных таблицах, а с другой — дает в руки конечным клиентам системы средства для проверки достоверности сообщаемой тем или иным сервером адресной информации. DNSSEC — расширение DNS, подразумевающее внесение изменений в структуры данных, используемые доменной системой, и в программное обеспечение, реализующее функции DNS на серверах и клиентах (то есть, проще говоря, на компьютерах обычных пользователей).

В рамках этой книги мы не станем подробно изучать криптографические механизмы, лежащие в основе DNSSEC, чтобы не перегружать читателя технической информацией. Однако для понимания принципов работы одного из главнейших обновлений DNS нужно в самых общих чертах представить себе основные понятия новой системы. Такие знания тем более полезны, что DNSSEC использует стандартные подходы, встречающиеся в большом количестве других современных систем безопасности.

Несколько десятков лет назад криптографами были разработаны методы, позволяющие создавать так называемые цифровые подписи, удостоверяющие подлинность заданного набора данных. Предположим, что у нас имеется запись о соответствии имени домена и IP-адреса. В рамках DNSSEC в строгое соответствие этой записи ставится специальная последовательность байтов, представляющая собой цифровую подпись. Главная особенность «подписывания» заключается в том, что есть простые и, самое главное, публично доступные (открытые) методы проверки достоверности подписи, а вот генерирование подписи для произвольных данных требует наличия секретного ключа в распоряжении подписывающего. То есть проверить подпись может каждый участник системы, а подписать что-либо, используя доступные вычислительные ресурсы и за разумное время (это очень важное дополнение), — только обладатель секретного ключа. На первый взгляд, это может показаться парадоксальным. Тем не менее именно так работают асимметричные системы шифрования с открытым ключом, лежащие в основе алгоритмов цифровой подписи.



Попробуем разобраться на очень простом примере. Следует иметь в виду, что этот пример лишь похож на операции в рамках DNSSEC, а не описывает их в деталях. Предположим, администратор зоны `fort.test.ru` хочет удостоверить с помощью цифровой подписи данные об адресации, хранящиеся на его DNS-сервере. У администратора есть пара ключей: секретный и открытый (публичный). Используя секретный ключ и данные об адресации (можно считать, что эти данные представляют собой простой компьютерный файл) в качестве исходных данных, администратор генерирует новый файл, содержащий цифровую подпись, соответствующую секретному ключу и исходным данным. Получив значение цифровой подписи (а она представима в виде набора байтов), администратор размещает эту подпись в публичном доступе вместе с адресной информацией.

Теперь для других участников DNSSEC доступна информация об адресации и связанная с этой информацией цифровая подпись. Для проверки подписи используется открытый ключ из пары, принадлежащей администратору, который также опубликован. Для проверки, которая выполняется по специальному, известному всем участникам DNSSEC, алгоритму, используются: файл данных об адресации, файл с соответствующей цифровой подписью и открытый ключ. Заметьте, что открытый ключ позволяет проверять достоверность подписи, но не позволяет за разумное время вычислять новые подписи для измененных данных. Важная особенность цифровой подписи в том, что при изменении подписываемых данных изменяется и сама подпись, поэтому просто скопировать подпись от одних данных и «прицепить» ее к другим не получится.

КСТАТИ



Нужно заметить, что в теории подписи у различных наборов исходных данных **могут совпадать**, однако на практике используются алгоритмы, сводящие вероятность такого совпадения к минимуму. По крайней мере, простые пользователи могут надеяться на то, что вероятность минимальна.

Если злоумышленник на каком-либо этапе обработки запросов с использованием DNSSEC изменил данные о соответствии доменов и адресов, то ему также потребуется изменить цифровую подпись, сопровождающую данные запросов. А для этого необходимо знание секретного ключа. Таким образом, потребитель адресной информации из DNS (или внутри DNS) может проверить достоверность данных с помощью подписи и не принимать к сведению недостоверные данные. Проблема решена? Не совсем.

Все бы хорошо, но, если чуть тщательнее обдумать предложенную только что схему, можно найти неприятный момент. Предположим, злоумышленник не только изменил адресную информацию, но еще и подписал ее, используя собственный секретный ключ, а соответствующий открытый ключ (для проверки подписи) подsunул ничего не подозревающей жертве вместе с обманными данными DNS. И вообще, каким образом получатель адресной информации может убедиться, что тот, кто ему эту информацию передает, действительно уполномочен управлять данным домом? Может, отвечающий сервер подставной? Сама по себе верность цифровой подписи не гарантирует того, что достоверно и содержание заверенных этой подписью данных. Выходит, даже внедрив «хитрые» подписи, мы остались все при тех же проблемах доверия?

Так и есть: одними подписями обойтись не удастся. Требуется механизм, позволяющий удостоверить полномочия источников этих подписей. В DNSSEC для создания этого механизма должна использоваться естественная иерархия прав, уже существующая в доменной системе имен. То есть на базе системы делегирования прав администраторам доменов, которая в подробностях описана несколькими главами выше, создается механизм подписывания ключей. Так, достоверность источника ключа для какого-либо домена удостоверяется с помощью цифровой подписи, исходящей от вышестоящего удостоверяющего центра, подпись этого центра удостоверяет другой, стоящий еще выше в иерархии,

а в итоге образующаяся «цепочка доверия» сводится с корневому домену и корневому ключу. Этот ключ должен быть распределен по всем участникам DNSSEC независимо от DNS. Например, он может быть встроен в операционные системы. Корневой ключ — главный ключ всей системы, позволяющий проверить достоверность любой подписи на всех прочих уровнях, — принадлежит той организации, которая отвечает за достоверность DNS в целом, и поэтому, строго говоря, этот ключ не может являться частью DNS.

DNSSEC позволяет участникам системы самим настраивать «цепочку доверия» и решать, какому именно удостоверяющему центру они готовы верить «на слово», без дополнительных проверок. В каких-то сетевых архитектурах конечным центром доверия может являться вовсе не корневой центр всего Интернета, а, скажем, некоторый локальный сервер. Но для всего Интернета важен именно общепринятый корневой центр.

Благодаря возможности вносить коррективы «в цепочку доверия» DNSSEC уже внедрена в некоторых доменах первого уровня. Есть множество доменов уровнем ниже, внутри которых также используется DNSSEC. Однако совершенно преждевременным было бы говорить, что DNSSEC развернута, до тех пор пока не будут «подписаны» корневые серверы имен, соответствующие корневому домену. (Как я рассказывал ранее, таких серверов 13, и в настоящий момент они в административном плане контролируются ICANN.)

Именно с «подписыванием» корневых серверов связаны политические проблемы в управлении Глобальной сетью. Они сводятся к довольно простому вопросу: у кого ключ?

Из соображений безопасности секретный ключ, с помощью которого подписывается информация в вершине иерархии доверия, должен являться самой охраняемой частью системы. Однако любое изменение в файлах корневой зоны требует использования секретного ключа для генерирования новой подписи. Изменения

же вносятся весьма часто, а многие из них носят чисто технический характер.

Сейчас контроль над верхушкой иерархии несколько «размазан». Фундаментальные решения принимает ICANN после согласования с соответствующими подразделениями Минторга США. Техническую сторону обеспечивают технические службы (например, корпорация VeriSign или такая организация, как IANA). При этом сами 13 корневых серверов вовсе не являются тринадцатью физическими компьютерами, а представляют собой большое количество сложных многокомпьютерных систем, разбросанных по дата-центрам разных стран. Понятно, что в управлении этими базовыми узлами DNS так или иначе задействовано большое количество различных телекоммуникационных компаний.

В случае если состоится «подписывание» корневых серверов, управление придется строго и однозначно привязать к корневому ключу. Окажется, что тот, кто распоряжается этим ключом, прямо контролирует адресное пространство доменной системы имен, без разных «дипломатических вариантов». Достанется ли ключ одной из коммерческих компаний США? Или его следует доверить общественной организации, подконтрольной правительству США? Или же подобный ключ от Глобальной сети должна держать в своих хранилищах некая международная организация наподобие ООН? Кто будет контролировать сохранность ключа? Кто станет следить за тем, чтобы ключ не был скомпрометирован? Подобные политические решения не принимаются быстро, и именно поэтому DNSSEC еще не развернута в Сети, несмотря на все усилия ее популяризаторов.

КСТАТИ



Между прочим, решая главную проблему «дырявости DNS», DNSSEC гарантированно создаст множество новых проблем. Так выйдет прежде всего потому, что DNSSEC устроена намного сложнее по сравнению с классической DNS. Уничтожая одни уязвимости, DNSSEC создает почву для других. Разработчики системы, конечно, знают об этом. В пример часто приводят то,

что внедрение DNSSEC создаст новые возможности для атак типа «Отказ в обслуживании» (DoS), ведь криптографические процедуры защищенной DNS гораздо более ресурсоемки в вычислительном плане. Злоумышленники при помощи отправки системам, поддерживающим DNSSEC, «дефектных» наборов данных смогут с большей, относительно классической DNS, легкостью занять все вычислительные ресурсы компьютера проверкой бессмысленных адресных данных. Кроме того, существенную трудность представляет распределение ключей, необходимых для генерирования цифровых подписей. Со временем ключи устаревают, и требуется производить их замену. При этом замена должна происходить с высокой надежностью, и все участники системы должны иметь возможность узнать, что конкретный ключ прекратил свое действие. Реализации сложных по сравнению с обычной DNS криптографических алгоритмов в программном обеспечении могут быть выполнены с ошибками, что создаст возможности для хакерских атак. Существует и множество других проблем. О некоторых из них наверняка сейчас еще ничего не известно, и раскроются они лишь после повсеместного внедрения DNSSEC. Однако при всех сложностях DNSSEC обещает значительно улучшить ситуацию с безопасностью в Интернете, создав платформу для «управления доверием».

Мы взглянули на комплекс проблем, связанных с достоверностью адресов, имен доменов и доверием к адресной системе, с одной стороны — со стороны администратора (владельца) доменного имени. Не менее многогранным предстает тот же комплекс с другой стороны — со стороны пользователей Сети, рядовых посетителей сайтов. Именно здесь «фокусы с доверием» вносят наибольший вклад в формирование реалий современного Интернета.

Мы уже касались важного момента, лежащего в основе множества хакерских атак, — ложного доверия к адресу: рядовые посетители веб-сайтов и других онлайн-ресурсов, связанных с доменами, склонны считать, что, если они набирают в адресной строке определенное доменное имя, браузер приводит их именно на тот сайт, который они ожидают под этим именем увидеть.

На доверии к сетевым реквизитам паразитируют так называемые фишеры. Фишинг — разновидность мошенничества, выманивание различными способами у ничего не подозревающего пользователя Интернета тех или иных критичных персональных данных, например номеров кредитных карт или паролей к системам управления банковскими счетами. Соответственно, фишеры — те, кто занимается фишингом. Фишинг не обязательно должен проводиться в Интернете, тем не менее мы рассмотрим именно сетевую часть.



Для обмана интернет-пользователей фишеры используют целый арсенал средств, на первом месте в котором — хитрости с DNS и именами доменов. Очень большой удачей для фишеров является выполненный тем или иным способом перехват управления доменом, под которым размещен сайт банка. Мошенники

заблаговременно готовят сайт-обманку, внешне неотличимый от официального сайта банка, и после получения управления доменом переводят домен на этот сайт-обманку. Клиенты банка, как и ранее, заходят на веб-сайт, набрав в адресной строке браузера привычное имя домена или воспользовавшись закладками браузера, что в данном случае имеет тот же эффект. Однако вместо настоящего сайта клиентов ждет поддельный, обычно предлагающий ввести реквизиты для управления банковским счетом. Мотивируется такая просьба самыми разными причинами: «обновление базы данных», «проверка и переучет пользователей системы онлайн-банкинга» и т. п. Клиент, искренне полагая, что находится на официальном сайте банка, делится нужными реквизитами с фишерами. Именно для подобных атак, весьма и весьма эффективных, фишеры и прибегают к услугам хакеров, помогающих «угнать» домен.

Впрочем, «угнать» домен банка даже временно удастся далеко не всегда. Поэтому фишеры используют и другие способы, также основанные на доменных именах, но не требующие хакерских ухищрений.

Например, фишеры регистрируют домены, по тому или иному аспекту похожие на домен атакуемого сервиса (атака не обязательно проводится на банк). Скажем, для атаки на сервисы известной поисковой машины «Яндекс», размещающей свои точки входа под доменом `yandex.ru`, предназначался домен `yanclex.ru`. В этом случае использовалось графическое сходство буквы *d* и последовательности букв *c, l*. Для атаки с использованием графически похожего домена пользователям рассылают поддельные сообщения электронной почты, в данном случае якобы от «Яндекса», при этом в тексте сообщений содержится приглашение зайти по указанной ссылке и ввести свои авторизационные данные. Здесь важную роль играет то, что пользователь не набирает адрес в строке браузера и не использует браузерную закладку для перехода на сайт «Яндекса», а нажимает предложенную ссылку, на глаз определяя ее как ведущую на «Яндекс».

Регистрация домена `yanclex.ru` вполне может вызвать некоторые подозрения у регистратора, хотя правовых оснований для запрета регистрации подобного домена нет. Но встречаются и куда более изящные с технической точки зрения решения, не вызывающие никаких подозрений вплоть до того момента, как начнется фишинговая атака. Например, в 2008 году фишеры атаковали пользователей платежной системы «Яндекс.Деньги». В этой атаке задействовали обыкновенный цифровой домен в зоне `.com` (эта зона, кстати, допускает весьма высокую степень «приватности» регистраций, затрудняющую в дальнейшем поиск злоумышленников правоохранительными органами).

Внутри цифрового домена с помощью DNS приписывалось несколько доменов более низкого уровня, цепочка начиналась с имен, совпадающих с адресом интерфейса платежной системы «Яндекс.Деньги», в результате получалась строка URL (ссылка) наподобие следующей: `http://money.yandex.ru.passport.idkey=354?18863&ncrnd=.92nnnnnnnn.com/`. (Здесь по понятным причинам большинство цифр в имени домена заменены на буквы *n* — см. *правый* конец строки.) Даже у искушенных в интернет-адресах пользователей не возникает сомнений, что их взору представлен домен в зоне ответственности «Яндекса» (`yandex.ru`). Дело в том, что обычный пользователь, обладающий наивным сознанием в области систем адресации Интернета, начинает разбор строки URL *слева направо* и, убедившись, что перед ним «ссылка на «Яндекс»» (`http://money.yandex.ru/`), уверенно на этой ссылке щелкает.

Хитрость в том, что URL разбирается компьютером, как положено по стандартам: с области, определяющей адрес сервера, — *справа налево* (терминальным, то есть отделяющим адрес сервера от других элементов URL, символом тут является *правый* символ «/»). Если теперь внимательно изучить представленный адрес *с точки зрения компьютера*, то окажется, что вся строка представляет собой адрес внутри домена `.92nnnnnnnn.com`, не имеющего никакого отношения к «Яндексу».

К сожалению, о правилах синтаксического разбора интернет-адресов компьютерами знают только специалисты. Пользователи же вынуждены доверять своему наивному сознанию. Добавим: в приведенной выше фишинговой ссылке умело эксплуатируется тот факт, что разработчики систем авторизации по неясным причинам (видимо, сложившимся исторически) постоянно используют в составе URL разнообразные цифры и буквы (обычно это идентификаторы сессий и разделов сайта), в большом количестве указываемые в качестве параметров. Именно поэтому использован цифровой домен, оказывающийся с точки зрения пользователя в конце строки. Пользователи постоянно видят эти цифры и буквы в адресе реального сайта, привыкают к ним и не пугаются абракадабры, лишь бы она начиналась со знакомого для глаз `http://money.yandex`. Опять действует доверие к адресу.

Фишеры атакуют все функции, касающиеся работы пользователя с интернет-адресами. Так, пользователям свойственно вводить адреса сайтов — имена доменов, вручную набирая их в адресной строке браузера. При этом пользователь может сделать опечатку. За «доменами-опечатками» охотятся не только так называемые тайпсквоттеры, но и фишеры.

Некоторые владельцы раскрученных торговых марок и посещаемых ресурсов щепетильно относятся к «доменам-опечаткам», заранее регистрируя их на себя. Другие, видимо, из-за недопонимания проблемы упускают момент, отдавая «опечатки» охотникам за доменами. Уходят «домены-опечатки» даже от известных ИТ-компаний, чей бизнес прямо связан с Интернетом. Например, в управлении у российской компании «1С-Битрикс» находится домен `bitrix.ru`, под которым размещен сайт известной в Рунете коммерческой системы управления сайтами (CMS) «Битрикс». При этом очевидный «домен-опечатка» `biRTix.ru` (из-за особенностей зрительного восприятия текста при беглом чтении этот домен неотличим от оригинала; «перестановка» специально выделена заглавными буквами) управляется вовсе не «1С-Битрикс» (по состоянию на 2008 год). Другой пример: компания «Яндекс» запустила сервис для веб-мастеров под до-

меном `webmaster.yandex.ru`. Менеджеры компании, прежде чем публично объявлять о запуске нового сервиса, не позаботились о перехвате «тайпсквоттерских» доменов. В результате очевидное доменное имя с опечаткой `webmasteryandex.ru` (без точки) оказалось под управлением опытных доменеров, сейчас под ним размещается что-то вроде поисковой системы.

Рост тайпсквоттерской активности в приобретении доменов наблюдается регулярно, как только какой-то новый (или не очень новый) интернет-проект вдруг обретает большую популярность. Например, как только в 2006–2007 годах набрал популярность проект «Одноклассники», размещенный под доменом `odnoklassniki.ru`, тут же началась регистрация десятков «доменов-опечаток», например: `odnoklasniki.ru`, `odnolkassniki.ru`, `ondoklassniki.ru` и т. п.

Все эти опечатки могут так или иначе использоваться фишерами. Не обязательно для прямых атак. Возможны многоступенчатые схемы: сначала пользователя заманивают на «домен-опечатку», выдавая размещенный там поддельный сайт за настоящий; далее пользователю предлагают перейти по той или иной ссылке, ведущей на внешний ресурс. Поскольку пользователь полагает, будто находится на сайте известной ИТ-компании, ему будет значительно легче «обмануться» и, особенно не задумываясь, перейти по рекомендуемой ссылке на ресурс фишера, например, изображающий официальный интернет-магазин той самой ИТ-компании.

Администратор домена должен принимать во внимание элемент подделки сайтов, особенно если речь идет о работе с важной пользовательской информацией, применять специальные дополнительные средства авторизации, позволяющие посетителю проверить достоверность сайта. Тем более что такие средства есть. Это системы SSL-сертификатов. SSL-сертификаты, используя криптографические методы, позволяют браузеру клиента проверить с привлечением независимых центров доверия, что сайт, с которым браузер соединяется, действительно является тем, за который себя выдает, и действительно размещен под указанным в адресной строке доменом.

Рассмотрение систем подобной сертификации сайтов выходит за рамки данной книги. Отмечу только, что сертификат должен быть размещен на защищаемом сайте, а процедура генерации сертификата должна сделать его копирование весьма затруднительным (можно сказать, нереальным) для злоумышленников. Впрочем, SSL-сертификаты лишь затрудняют деятельность по введению посетителей атакуемого сайта в заблуждение, но не делают ее невозможной.

В заключение этой главы еще раз подчеркну, что существенным подспорьем в решении проблем безопасности, очень актуальных для банковских сайтов и сайтов платежных систем, является заблаговременная регистрация всевозможных «доменов-опечаток».

Глава 12

Право на домен

- ☐ Отдай мой домен
- ☐ Отвечать не желаю

Доменные имена давно превратились в важный инструмент бизнеса. Нередки случаи, когда доменное имя представляет собой единственный действительно ценный ресурс той или иной коммерческой компании, а потеря домена эквивалентна потере всего бизнеса. Вокруг доменов возникают серьезные и весьма сложные в юридическом смысле судебные процессы. Некоторые из них, несмотря на кажущуюся очевидность, могут тянуться годами. Так, например, разбирательства вокруг домена kamaz.ru, зарегистрированного и использовавшегося частным лицом, а не известным на весь мир российским автопроизводителем, продолжались почти десять лет. Правда, в результате домен достался автозаводу.

Отдай мой домен

Что нужно знать начинающему администратору домена о правовых хитростях, окружающих доменные имена? Прежде всего необходимо уяснить для себя реальный статус доменов в российском законодательстве. Как ни странно, их статус можно довольно точно описать одним прилагательным: «расплывчатый». Статус доменного имени, как и само понятие «домен», в законодательстве хоть и упоминаются, но четко не прописаны.

С точки зрения российского законодательства регистрация доменного имени — это услуга, оказываемая юридическим лицом (скорее всего, коммерческой компанией) либо физическому лицу, либо другому юридическому лицу. Услуга, и не более. Документы и договоры, подтверждающие право управления доменом, и близко не равны по юридической силе действия каким-либо государственным правоустанавливающим документам.

Однако от этого право управления доменом не перестает быть правом. То есть администратор не покупает домен — он лишь получает право администрирования домена. Что это меняет? Как только дело дойдет до официальных юридических процедур, выяснится, что меняет это очень многое. Например, право на управ-

ление доменом нельзя наследовать. Если администратор домена умер, то коммерческая компания-регистратор вовсе не обязана передать право управления наследникам администратора. Ситуация во многом аналогична другим правам. Скажем, пенсионер может иметь право на бесплатный проезд в общественном транспорте. Но это право не переходит вместе с квартирой к наследникам данного пенсионера после его смерти (даже если пенсионер указал бесплатный проезд в завещании). Так и с доменом. Конечно, никто не запрещает компании-регистратору проявить добрую волю и передать право на домен наследникам умершего администратора, но регистратор не обязан так поступать.

Наследование доменов становится довольно важным моментом, как только они обретают серьезную ценность. В настоящий момент наиболее удобным способом передачи доменов по наследству является оформление их на юридическое лицо, владельцем которого является тот, кто заинтересован в корректном переводе доменов на наследников. В таком случае наследники унаследуют домены вместе с юридическим лицом: наследование долей в компаниях более четко регулируется законодательством.

Оформление прав управления доменом на юридическое лицо также должно проводиться с соблюдением определенных формальных правил. Так, особое внимание нужно уделить полномочиям генерального директора компании. Ведь директор — наемный сотрудник, имеющий при этом определенные права по управлению имуществом компании. В случае с доменом следует отдельно указать в договоре с директором и в учредительных документах компании, что директор не имеет права передавать права компании по доменным именам кому бы то ни было без согласия владельцев (более строго — учредителей). Это довольно важный момент: из-за новизны такого правового явления, как доменное имя, к юридическим аспектам управления им сейчас относятся без должного внимания. А между тем, как уже упоминалось, однажды доменное имя может стать единственным ценным ресурсом компании. В конце концов, другие ресурсы она может утратить и сохранить лишь раскрытый домен.

Интересно, что при разделе имущества обанкротившейся компании с доменными именами также возникают серьезные трудности. Если владельцев бизнеса несколько, раздел доменного имени между ними может оказаться весьма проблематичной задачей. Право управления доменом не набор мебели, включающий двенадцать стульев. «Разрезать» данное право на несколько частей не просто, а очень сложно. Особенно если претендующие на домен учредители компании находятся в конфликте. Решать задачу нужно с привлечением хорошего юриста.

Впрочем, основное содержание «доменных споров» обычно составляют конфликты между владельцами доменов и владельцами товарных знаков или фирменных наименований. Как правило, вторые пытаются отсудить домены у первых, часто успешно. Довольно просто отсудить домен, совпадающий в написании с зарегистрированной торговой маркой, которая не является тем или иным общеупотребительным словом. Если же доменное имя представляет собой общеупотребительное слово, то в случае существования совпадающей с ним торговой марки отсудить домен будет непросто. Особенно если администратор домена не использует его для деятельности, входящей в тот же класс товаров и услуг, для которых зарегистрирована торговая марка.

Домены, совпадающие с торговыми марками, могут регистрировать киберсквоттеры, чтобы в дальнейшем попробовать получить доход, предложив такой домен для выкупа владельцам торговой марки. Восприняв результаты судебных разбирательств, успешных для владельцев торговых марок, в последнее время киберсквоттеры уже не захватывают все доступные домены — торговые марки подряд, а кроме того, киберсквоттерами придуман целый ряд оригинальных мер, направленных на усложнение отсуживания доменов.

Например, киберсквоттер может зарегистрировать домен, имя которого совпадает с названием торговой марки, но не использовать его, то есть не делегировать. Теперь иск владельцев торговой марки о том, что киберсквоттер неправомерно использует торго-

вую марку в названии домена (а Гражданский кодекс в этом случае регулирует именно использование торговой марки), окажется неэффективным. Регистратор доменных имен также подтвердит в суде: действительно, домен даже не делегирован, а значит, не используется.

Впрочем, владелец торговой марки может подать и другой иск, сделав его предметом то, что киберсквоттер препятствует реализации прав по использованию торговой марки законным владельцем. Ведь доменное имя только одно, а факт регистрации домена, совпадающего с торговой маркой, не позволяет зарегистрировать и использовать второй такой же домен. Однако это уже совсем другой иск и другой состав разбирательства, не столь однозначно прописанный в законодательстве.

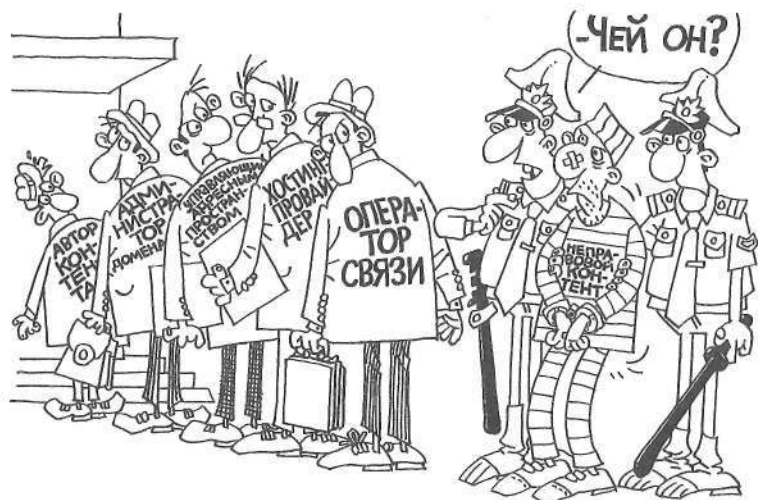
Киберсквоттеры наработали также целый арсенал мотивировок, почему они зарегистрировали именно этот домен, удачно, но совершенно случайно совпавший с названием известной коммерческой компании, и почему этот домен нужен им, киберсквоттерам. Впрочем, тенденция в судебных разбирательствах последних лет позволяет надеяться, что киберсквоттерам станет труднее защищать свои захваченные домены в судах.

Отвечать не желаю

Помимо конфликтов вокруг того, кому достанется право управления доменом, с системами адресации Интернета связан другой, весьма существенный по объему, пласт правовых вопросов. Они касаются ответственности за размещение «неправового контента».

В Интернете может быть опубликована информация, так или иначе нарушающая действующее законодательство. Доступ к ней осуществляется с использованием систем адресации, в том числе, очевидно, с использованием DNS и доменных имен. За размещение подобной информации кто-то должен отвечать. Кто же именно? Определить, оказывается, не всегда просто.

Обеспечивают доступность (то есть публикацию, доведение до всеобщего сведения) нарушающей закон информации в Интернете всегда несколько сторон. Во-первых, в публикации оказываются задействованы операторы связи, передававшие запросы пользователей и саму информацию в ответ на эти запросы. Во-вторых, виноваты хостинг-провайдеры, предоставившие место для размещения этой информации таким способом, что она через сети операторов связи оказалась доступна всем желающим. В-третьих, виноваты организации, управляющие адресным пространством Интернета, сделавшие так, что пользователи смогли найти путь к тем серверам, на которых хостинг-провайдеры выделили место таким способом, что через сети операторов связи оказался всем доступен «неправовой контент». В-четвертых, виноват администратор домена, который позволил включить свой домен организациям, управляющим адресным пространством Интернета, таким образом, что он указал путь пользователям к тем серверам у хостинг-провайдеров... В общем, получается песенка про дом, который построил Джек. При этом лишь где-то в конце цепочки появляется автор нарушающей законодательство информации, который и выложил ее в Сеть. Почему в конце? Потому что этого автора часто найти труднее всего. Впрочем, рано или поздно находят при содействии всех сторон из только что рассмотренной цепочки.



Так что если «неправовой контент» появился под доменом, находящимся в управлении того или иного администратора, это не означает, что именно администратор понесет всю тяжесть наказания. Ведь во многих случаях нарушающая законодательство информация может быть опубликована без участия администратора домена. Самый хрестоматийный пример — публикация сообщений на интернет-форуме на веб-сайте, расположенном под данным доменом. Однако администратор домена должен знать, что происходит на тех сайтах, домены которых он администрирует, иначе роль соответчика ему гарантирована.

Заклучение

В рамках этой книги мы окинули взглядом реалии и перипетии одной из важнейших систем адресации современного Интернета — доменных имен. При этом затрагиваются в основном проблемы доменного рынка, а не техническая сторона функционирования DNS. Нужно заметить, что техническая сторона (которая освещена в специальной литературе) весьма сложна и многогранна, хоть она и может показаться новичку прозрачной, как воздух. Впрочем, правильно настроенная DNS и будет подобна воздуху: столь же прозрачна и незаметна для «живущих» в Глобальной сети и столь же необходима им, потому что, если современный Интернет лишит DNS, большая часть «жителей» тут же «задохнется». Тем не менее сама DNS более не определяет развитие Интернета. Старые добрые времена канули в Лету. Наоборот, с наступлением окончательной и бесповоротной коммерциализации Глобальной сети именно коммерческие интересы игроков крупнейших бизнес-рынков (вовсе не телекоммуникационных!) диктуют направления дальнейшего развития систем адресации, и в особенности системы доменных имен.

Дело в том, что доменные имена представляют собой ту часть Интернета, которая прямым образом «проросла» в офлайновую реальность. Доменные имена позволяют коммерческим компаниям связывать онлайн-бизнес с офлайновыми реалиями, внутри которых живут потенциальные клиенты. Очевидный пример — реклама онлайн-сервисов на традиционных носителях (печать, щиты вдоль автострад и т. д.): практический смысл подобной рекламы целиком завязан на доменное имя. А раз в Интернете так важны доменные имена, то и перспективы развития доменного рынка определяются потребностями маркетингового инструментария.

Так, если в «классические» времена система доменных имен развивалась «в глубину», то в ближайшие несколько лет развитие системы неминуемо будет происходить «в ширину». Развитие «в глубину» — появление новых доменов на уровнях ниже первого, при том что доменов первого уровня немного и их список строго фиксирован. Развитие «в ширину» — появление все новых и новых доменов первого уровня. В последние годы происходит весьма бурный даже по меркам Интернета рост числа доменов верхнего уровня (вспомните NAME, INFO, JOBS и т. п.). Видимо, в следующие три-пять лет этот рост еще ускорится.

ICANN уже разработала специальные процедуры, подробно регламентирующие методы введения новых доменов первого уровня по заявкам интернет-общественности. Для чего нужна четкая регламентация? Нет, вовсе не для того, чтобы исключить доменные споры. Споры будут при любом регламенте. Четкая регламентация нужна для ускорения бюрократических процедур (они лучше идут в режиме «делай раз, делай два, переходи к пункту номер три»), что расширит дорогу новым доменам первого уровня. Коммерческие компании не желают мириться с тем, что у конкурентов есть привлекательный домен второго уровня в раскрученной зоне. Вполне понятно, что некоторым корпорациям из маркетинговых соображений (да и по «соображениям приличия») больше подошел бы собственный домен первого уровня. Например, BOEING. За такой адрес можно хорошо заплатить. Поэтому ближайшая перспектива доменного пространства — рост «в ширину». Насколько он будет успешным? Покажет время.

Другая важнейшая тенденция — рост доменного пространства в новом измерении: уже через несколько лет ожидается массовое появление многоязычных доменов верхнего уровня. Для России, скорее всего, будет выделен кириллический домен верхнего уровня РФ. Другие страны получают домены, соответствующие их языковой принадлежности. Интересно, что целому ряду стран ICANN, скорее всего, выделит сразу несколько нелатинских доменов верхнего уровня, так как в этих странах несколько

государственных языков. И здесь тенденция к появлению нового измерения поддерживает тенденцию к росту «в ширину».

По прошествии некоторого времени станет ясно, какие перспективы у самой корпорации ICANN, контролирующей адресное пространство Интернета. Ведь Интернет давно вырос из пределов США и стал гораздо более международным явлением, чем, например, Всемирная торговая организация. И такое положение дел, когда развитие Интернета контролирует структура, тесно связанная с правительством США, призванная проводить в виртуальную реальность интересы американских коммерческих компаний, уже далеко не всем кажется оправданным.

Попытки создать новый международный контролирующий орган, подобный хотя бы ООН, предпринимаются довольно давно. Что интересно: в свое время ICANN явилась неожиданным результатом одной из таких попыток. Поэтому полагать, будто США так легко откажутся от должности капитана Глобальной сети, весьма наивно. Для того же, чтобы по старому пиратскому обычаю низложить капитана, команде придется договориться, да еще предварительно обеспечить себе жесткий контроль над важнейшими магистралями обмена данными, благодаря которым сохраняется связность Сети. Вряд ли такое возможно в ближайшие несколько лет. Поэтому фактический контроль над Интернетом пока сохранится за США, хотя на словах, конечно же, будет «идти процесс формирования новой системы управления».

Итак, доменный рынок продолжает развиваться. Если говорить о коммерческой составляющей, которая и делает рынок рынком, то в российском сегменте Интернета намечается очередной доменный бум. Не упустите его.

Приложение 1. Перечень зарезервированных доменных имен в зоне .ru

Домены общего пользования

Отраслевые домены

Отраслевые домены предназначены для регистрации доменных имен третьего уровня с учетом отраслевой, ведомственной и другой подобной специфики.

К отраслевым доменам относятся:

- ❑ **ac.ru** — для научно-исследовательских организаций; высших учебных заведений; учреждений культуры, ведущих научные исследования;
- ❑ **com.ru** — для коммерческих организаций;
- ❑ **edu.ru** — для учебных заведений, имеющих лицензию на образовательную деятельность;
- ❑ **int.ru** — для международных организаций;
- ❑ **net.ru** — для организаций, осуществляющих реализацию проектов, связанных с развитием сети Интернет;
- ❑ **org.ru** — для некоммерческих организаций;
- ❑ **pp.ru** — для физических лиц.

Географические домены

Географическими доменными именами признаются сложившиеся обозначения субъектов Российской Федерации.

К географическим относятся следующие домены.

| | |
|---|-----------------------------------|
| adygeya.ru | Республика Адыгея (Адыгея) |
| — | Республика Алтай |
| bashkiria.ru | Республика Башкортостан |
| ulan-ude.ru, buriatia.ru | Республика Бурятия |
| dagestan.ru | Республика Дагестан |
| — | Республика Ингушетия |
| nalchik.ru | Кабардино-Балкарская Республика |
| kalmykia.ru | Республика Калмыкия |
| kchr.ru | Карачаево-Черкесская Республика |
| ptz.ru, karelia.ru | Республика Карелия |
| komi.ru | Республика Коми |
| mari-el.ru, joshkar-ola.ru, mari.ru | Республика Марий Эл |
| mordovia.ru | Республика Мордовия |
| yakutia.ru | Республика Саха (Якутия) |
| vladikavkaz.ru | Республика Северная Осетия-Алания |
| kazan.ru, tatarstan.ru | Республика Татарстан (Татарстан) |
| tuva.ru | Республика Тыва |
| udmurtia.ru, izhevsk.ru, udm.ru | Удмуртская Республика |
| khakassia.ru | Республика Хакасия |
| grozny.ru | Чеченская Республика |
| chuvashia.ru | Чувашская Республика - Чувашия |
| altai.ru | Алтайский край |
| kuban.ru | Краснодарский край |
| krasnoyarsk.ru | Красноярский край |

| | |
|-----------------------------------|-------------------------|
| marine.ru, vladivostok.ru | Приморский край |
| stavropol.ru, stv.ru | Ставропольский край |
| khabarovsk.ru, khv.ru | Хабаровский край |
| amur.ru | Амурская область |
| arkhangelsk.ru | Архангельская область |
| astrakhan.ru | Астраханская область |
| belgorod.ru | Белгородская область |
| bryansk.ru | Брянская область |
| vladimir.ru | Владимирская область |
| volgograd.ru, tsaritsyn.ru | Волгоградская область |
| vologda.ru | Вологодская область |
| voronezh.ru, vrn.ru, cbg.ru | Воронежская область |
| ivanovo.ru | Ивановская область |
| irkutsk.ru | Иркутская область |
| koenig.ru | Калининградская область |
| kaluga.ru | Калужская область |
| kamchatka.ru | Камчатская область |
| kemerovo.ru | Кемеровская область |
| kirov.ru, vyatka.ru | Кировская область |
| kostroma.ru | Костромская область |
| kurgan.ru | Курганская область |
| kursk.ru | Курская область |
| — | Ленинградская область |
| lipetsk.ru | Липецкая область |
| magadan.ru | Магаданская область |

| | |
|--------------------------------------|-----------------------|
| mosreg.ru | Московская область |
| murmansk.ru | Мурманская область |
| nnov.ru | Нижегородская область |
| nov.ru | Новгородская область |
| nsk.ru, novosibirsk.ru | Новосибирская область |
| omsk.ru | Омская область |
| orenburg.ru | Оренбургская область |
| oryol.ru | Орловская область |
| penza.ru | Пензенская область |
| perm.ru | Пермская область |
| pskov.ru | Псковская область |
| rnd.ru | Ростовская область |
| ryazan.ru | Рязанская область |
| samara.ru | Самарская область |
| saratov.ru | Саратовская область |
| sakhalin.ru, yuzhno-sakhalinsk.ru | Сахалинская область |
| yekaterinburg.ru, e-burg.ru | Свердловская область |
| smolensk.ru | Смоленская область |
| tambov.ru | Тамбовская область |
| tver.ru | Тверская область |
| tomsk.ru, tsk.ru, tom.ru | Томская область |
| tula.ru | Тульская область |
| tyumen.ru | Тюменская область |
| simbirsk.ru | Ульяновская область |
| chelyabinsk.ru, chel.ru | Челябинская область |
| chita.ru | Читинская область |

| | |
|----------------|--|
| yaroslavl.ru | Ярославская область |
| msk.ru | Город Москва |
| spb.ru | Город Санкт-Петербург |
| bir.ru, jar.ru | Еврейская автономная область |
| — | Агинский Бурятский автономный округ |
| — | Коми-Пермяцкий автономный округ |
| palana.ru | Корякский автономный округ |
| — | Ненецкий автономный округ |
| dudinka.ru | Таймырский (Долгано-Ненецкий) автономный округ |
| — | Усть-Ордынский Бурятский автономный округ |
| surgut.ru | Ханты-Мансийский автономный округ |
| chukotka.ru | Чукотский автономный округ |
| — | Эвенкийский автономный округ |
| yamal.ru | Ямало-Ненецкий автономный округ |

К географическим доменным именам относятся также сложившиеся обозначения ряда местностей, если статус этих имен был определен до введения в действие Положения.

| | |
|-------------|--|
| amursk.ru | г. Амурск, Хабаровский край |
| baikal.ru | Район озера Байкал |
| cmw.ru | Кавказские Минеральные Воды |
| fareast.ru | Дальний Восток |
| jamal.ru | Полуостров Ямал |
| kms.ru | г. Комсомольск-на-Амуре, Хабаровский край |
| k-uralsk.ru | г. Каменск-Уральский, Свердловская область |
| kustanai.ru | г. Кустанай |
| kuzbass.ru | Кузнецкий угольный бассейн |
| magnitka.ru | г. Магнитогорск, Челябинская область |
| mytis.ru | г. Мытищи, Московская область |
| nakhodka.ru | г. Находка, Приморский край |
| nkz.ru | г. Новокузнецк, Кемеровская область |

| | |
|---------------|---------------------------------------|
| norilsk.ru | г. Норильск, Красноярский край |
| snz.ru | г. Снежинск, Челябинская область |
| oskol.ru | г. Старый Оскол, Белгородская область |
| pyatigorsk.ru | г. Пятигорск, Ставропольский край |
| rubtsovsk.ru | г. Рубцовск, Алтайский край |
| syzran.ru | г. Сызрань, Самарская область |
| vdonsk.ru | г. Волгодонск, Ростовская область |
| zgrad.r | г. Зеленоград, г. Москва |

Домены, используемые для государственных нужд

Администрирование доменов, зарезервированных для государственных нужд, осуществляется в порядке и по правилам, установленным соответствующими государственными органами. К доменным именам, зарезервированным для государственных нужд, относятся:

- ☐ gov.ru — для федеральных государственных органов Российской Федерации;
- ☐ mil.ru — для организаций Вооруженных сил Российской Федерации.

Домены, зарезервированные в технических целях

Ряд доменных имен резервируется для технических и иных подобных целей (в частности, для использования в качестве примеров в описаниях и т. д.). К таким именам относятся test.ru — для использования в качестве примеров.

Приложение 2. Национальные домены верхнего уровня

- | | |
|---|---|
| .ad — Андорра. | .be — Бельгия. |
| .af — Афганистан. | .bf — Буркина-Фасо. |
| .ag — Антигуа и Барбуда. | .bg — Болгария |
| .ai — Ангилла. | .bh — Бахрейн. |
| .al — Албания. | .bi — Бурунди. |
| .am — Армения. | .bj — Бенин. |
| .ap — Антильские острова (Нидерланды). | .bm — Бермуды. |
| .ao — Ангола. | .bn — Бруней Даруссалам. |
| .aq — Антарктика. | .bo — Боливия. |
| .ar — Аргентина. | .br — Бразилия. |
| .as — Американские острова Самоа. | .bs — Багамы. |
| .at — Австрия. | .bt — Бутан. |
| .au — Австралия. | .bv — Буве, остров. |
| .aw — Аруба, остров (Нидерланды). | .bw — Ботсвана. |
| .az — Азербайджан. | .by — Беларусь. |
| .ba — Босния и Герцеговина. | .bz — Белиз. |
| .bb — Барбадос. | .ca — Канада. |
| .bd — Бангладеш. | .cc — Кокосовые острова. |
| | .cd — Республика Конго. |
| | .cf — Центральноафриканская республика. |

| | |
|---------------------------------|---|
| .cg — Конго. | .fi — Финляндия. |
| .ch — Швейцария. | .fj — Фиджи. |
| .ci — Кот-д'Ивуар. | .fk — Фолклендские острова. |
| .ck — Острова Кука. | .fm — Микронезия. |
| .cl — Чили. | .fr — Франция. |
| .cm — Камерун. | .ga — Габон. |
| .cn — Китай. | .gb — Великобритания. |
| .co — Колумбия. | .gd — Гренада. |
| .cr — Коста-Рика. | .ge — Грузия. |
| .cu — Куба. | .gf — Гвиана Французская. |
| .cv — Кабо-Верде. | .gh — Гана. |
| .cx — Остров Рождества. | .gi — Гибралтар. |
| .cy — Кипр. | .gl — Гренландия. |
| .cz — Чешская Республика. | .gm — Гамбия. |
| .de — Германия. | .gn — Гвинея. |
| .dj — Джибути. | .gp — Гваделупа. |
| .dk — Дания. | .gq — Экваториальная Гвинея. |
| .dm — Доминика. | .gr — Греция. |
| .do — Доминиканская Республика. | .gs — Южная Георгия и Южные Сандвичевы острова. |
| .dz — Алжир. | .gt — Гватемала. |
| .ec — Эквадор. | .gu — Гуам. |
| .ee — Эстония. | .gw — Гвинея-Бисау. |
| .eg — Египет. | .gy — Гайана. |
| .eh — Западная Сахара. | .hk — Гонконг. |
| .er — Эритрея. | .hm — Острова Херд и Макдо- нальд. |
| .es — Испания. | .hn — Гондурас. |
| .et — Эфиопия. | |

| | |
|--|---------------------------------------|
| .hr — Хорватия. | .lb — Ливан. |
| .ht — Гаити. | .lc — Сент-Люсия. |
| .hu — Венгрия. | .li — Лихтенштейн. |
| .id — Индонезия. | .lk — Шри-Ланка. |
| .ie — Ирландия. | .lr — Либерия. |
| .il — Израиль. | .ls — Лесото. |
| .in — Индия. | .lt — Литва. |
| .io — Индийская и Океанская территория. | .lu — Люксембург. |
| .iq — Ирак. | .lv — Латвия. |
| .ir — Иран. | .ly — Ливия. |
| .is — Исландия. | .ma — Марокко. |
| .it — Италия. | .mc — Монако. |
| .jm — Ямайка. | .md — Молдова. |
| .jo — Иордания. | .mg — Мадагаскар. |
| .jp — Япония. | .mh — Маршалловы Острова. |
| .ke — Кения. | .mk — Македония. |
| .kg — Кыргызстан. | .ml — Мали. |
| .kh — Камбоджа. | .mm — Мьянма. |
| .ki — Кирибати. | .mn — Монголия. |
| .km — Коморские Острова. | .mo — Макао. |
| .kn — Сент-Китс и Невис. | .mp — Северные Марианские Острова. |
| .kp — Северная Корея. | .mq — Мартиника. |
| .kr — Южная Корея. | .mr — Мавритания. |
| .kw — Кувейт. | .ms — Монтсеррат. |
| .ky — Каймановы острова. | .mt — Мальта. |
| .kz — Казахстан. | .mu — Маврикий. |
| .la — Лаос. | .mv — Мальдивы. |

| | |
|------------------------------|--------------------------------------|
| .mw — Малави. | .pt — Португалия. |
| .mx — Мексика. | .pw — Палау. |
| .my — Малайзия. | .py — Парагвай. |
| .mz — Мозамбик. | .qa — Катар. |
| .na — Намибия. | .re — Остров Воссоединения. |
| .nc — Новая Каледония. | .ro — Румыния. |
| .ne — Нигер. | .ru — Российская Федерация (Россия). |
| .nf — Остров Норфолк. | .rw — Руанда. |
| .ng — Нигерия. | .sa — Саудовская Аравия. |
| .ni — Никарагуа. | .sb — Соломоновы Острова. |
| .nl — Нидерланды. | .sc — Сейшельские Острова. |
| .no — Норвегия. | .sd — Судан. |
| .np — Непал. | .se — Швеция. |
| .nr — Науру. | .sg — Сингапур. |
| .nu — Ниуэ. | .sh — Остров Святой Елены. |
| .nz — Новая Зеландия. | .si — Словения. |
| .om — Оман. | .sj — Острова Свалбард и Джен Майен. |
| .pa — Панама. | .sk — Словацкая республика. |
| .pe — Перу. | .sl — Сьерра-Леоне. |
| .pf — Французская Полинезия. | .sm — Сан-Марино. |
| .pg — Папуа-Новая Гвинея. | .sn — Сенегал. |
| .ph — Филиппины. | .so — Сомали. |
| .pk — Пакистан. | .sr — Суринам. |
| .pl — Польша. | .st — Сан-Томе и Принсипи. |
| .pm — Св. Пьер и Маквело. | .sv — Сальвадор. |
| .pn — Остров Питкэрн. | .sy — Сирийская Арабская Республика. |
| .pr — Пуэрто-Рико. | |

| | |
|-------------------------------------|--------------------------------------|
| .sz — Свазиленд. | .us — Соединенные Штаты Америки. |
| .tc — Острова Текс и Кайакос. | .uy — Уругвай. |
| .td — Чад. | .uz — Узбекистан. |
| .tf — Французские южные Территории. | .va — Ватикан. |
| .tg — Того. | .vc — Сент-Винсент и Гренадины. |
| .th — Таиланд. | .ve — Венесуэла. |
| .tj — Таджикистан. | .vg — Виргинские острова (Британия). |
| .tk — Токелау. | .vi — Виргинские острова (США). |
| .tm — Туркменистан. | .vn — Вьетнам. |
| .tn — Тунис. | .vu — Вануату. |
| .to — Тонга. | .wf — Острова Уоллис и Футуна. |
| .tp — Восточный Тимор. | .ws — Западное Самоа. |
| .tr — Турция. | .ye — Йемен. |
| .tt — Тринидад и Тобаго. | .yt — Майотта. |
| .tv — Тувалу. | .yu — Югославия. |
| .tw — Тайвань. | .za — Южная Африка. |
| .tz — Танзания. | .zm — Замбия. |
| .ua — Украина. | .zw — Зимбабве. |
| .ug — Уганда. | |
| .um — Малые Отдаленные острова. | |

Приложение 3. Общие домены верхнего уровня (gTLDs)

Домены общего пользования

| gTLD | Предназначение |
|------|---|
| COM | Commercial (для коммерческих организаций) |
| NET | Networks (Интернет, телекоммуникационные сети) |
| ORG | Organizations (некоммерческие организации либо организации, не попадающие в другие категории) |
| INFO | Information (открытый для всех домен) |
| BIZ | Business Organizations (для организаций) |
| NAME | Personal (для частных лиц) |

Специальные домены общего пользования

| gTLD | Предназначение |
|--------|---|
| AERO | Air-transport industry (воздушно-транспортная индустрия) |
| COOP | Cooperatives (кооперативы) |
| MUSEUM | Museums (музеи) |
| PRO | Accountants, lawyers, and physicians — professionals (для специалистов — бухгалтеров, юристов и врачей) |

Домены ограниченного пользования

| gTLD | Предназначение |
|------|---|
| INT | International Organizations (международные организации) |
| EDU | Educational (образовательные проекты) |
| GOV | US Government (правительство США) |
| MIL | US Dept of Defense (Департамент безопасности США) |

Специальные спонсируемые домены ограниченного пользования (Sponsored Top-Level Domains, sTLDs)

| gTLD | Предназначение |
|--------|---|
| TRAVEL | Для турагентств, туроператоров, авиакомпаний, гостиничных сетей и всех, кто имеет отношение к индустрии путешествий, экскурсий, отдыха. Новый домен призван объединить в Интернете всю туристическую индустрию в едином доменном пространстве |
| JOBS | Для сайтов, устанавливающих коммуникации работодателей с наемными работниками |
| CAT | Для лингвистического и культурного сообщества испанской Каталонии |
| TEL | Для хранения и управления персональными и корпоративными контактными данными |
| MOBI | Для сайтов и сервисов, ориентированных на работу с мобильными телефонами и беспроводными устройствами |
| ASIA | Для сайтов и сервисов, ориентированных на граждан стран Азии |

Приложение 4. Статистика доменов

(по данным проекта stat.nic.ru)

Диаграмма 1. Рост домена RU:
число зарегистрированных имен
(январь 2005 — январь 2008 г.).

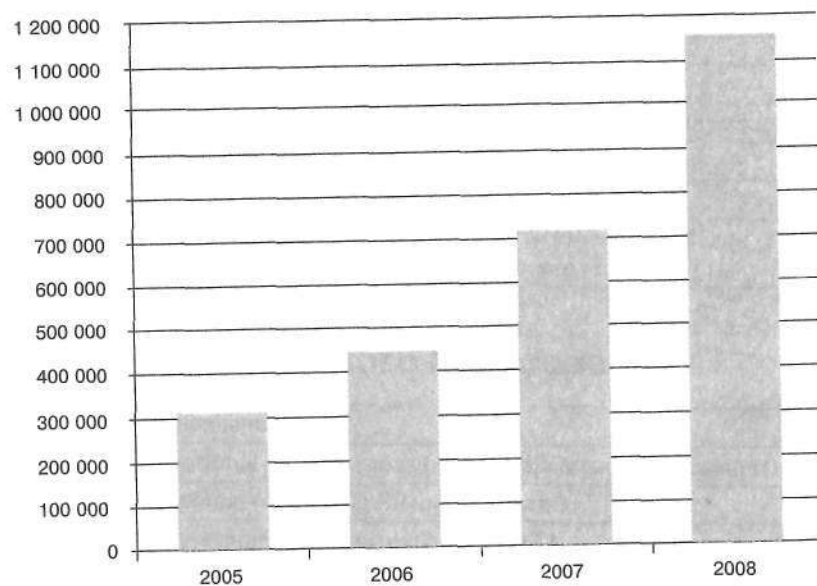


Диаграмма 2. Рост домена SU:
число зарегистрированных доменов
(январь 2005 — январь 2008 г.).

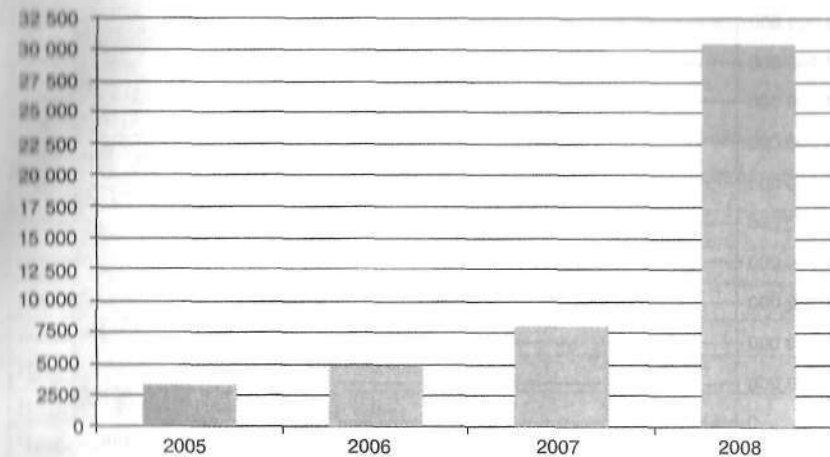


Диаграмма 3. Рост домена COM:
число делегированных доменов
(январь 2005 — январь 2008 г.).

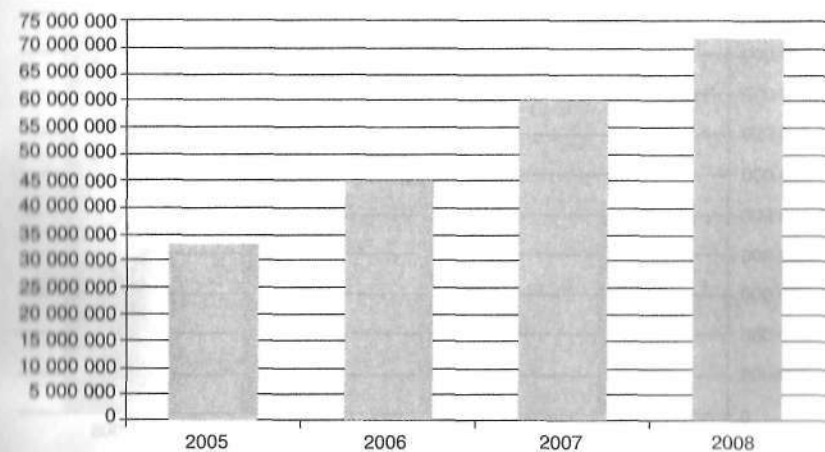


Диаграмма 4. Рост домена INFO:
число делегированных доменов в INFO
(январь 2005 — январь 2008 г.).

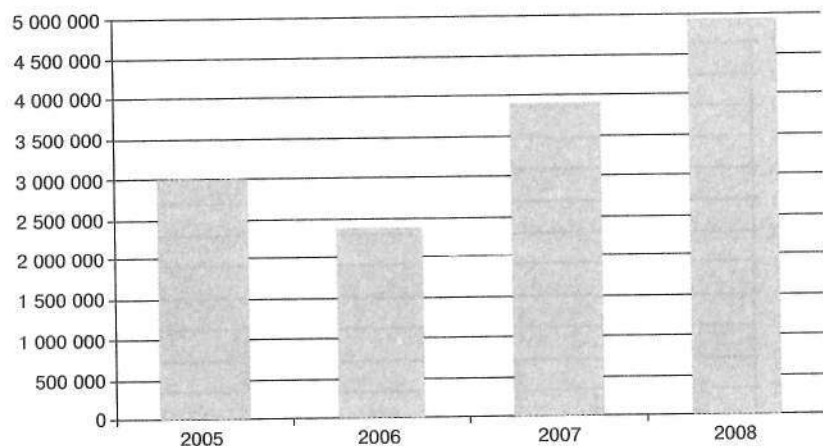


Диаграмма 5. Рост домена BIZ:
число делегированных доменов в BIZ
(январь 2005 — январь 2008 г.).

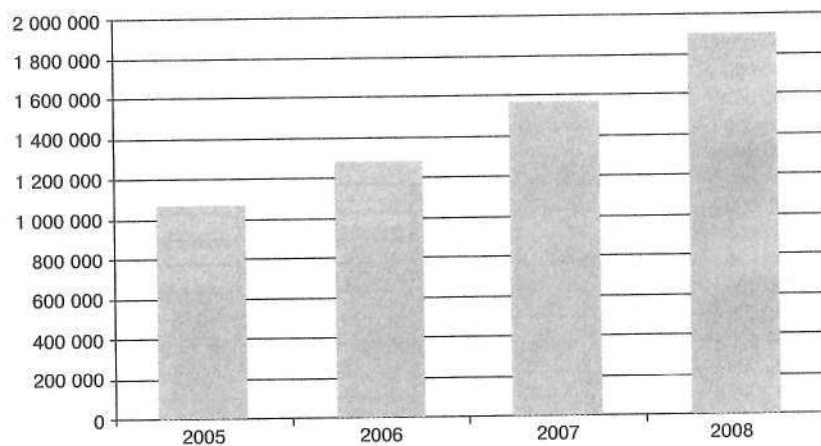


Таблица. Доли регистраций доменов .ru по странам администраторов,
для стран с числом регистраций более 0,1 %, на 1 января 2008 г.

| Страна | Доля доменов, % |
|---------------------------------|-----------------|
| Российская Федерация | 87,15 |
| Сейшельские острова | 6,49 |
| Белиз | 1,32 |
| Германия | 0,95 |
| Люксембург | 0,71 |
| Соединенные Штаты Америки | 0,49 |
| Украина | 0,47 |
| Франция | 0,23 |
| Нидерланды | 0,20 |
| Белоруссия | 0,16 |
| Швейцария | 0,15 |
| Виргинские острова (британские) | 0,13 |
| Чешская Республика | 0,12 |
| Италия | 0,12 |
| Австрия | 0,11 |
| Польша | 0,1 |
| Швеция | 0,1 |

Список литературы

1. *Альбитц П., Ли К.* DNS и BIND. — O'Reilly, 2006.
2. Альманах «Доменные имена, тенденции, 2007». — RU-CENTER, 2007.
3. Альманах «Доменные имена, тенденции, 2006». — RU-CENTER, 2006.
4. База соглашений по управлению ccTLD ICANN (<http://www.icann.org/cctlds/agreements.html>).
5. База WHOIS ccTLD (<http://www.iana.org/cctld/cctld-whois.htm>).
6. Документы ICANN (<http://www.icann.org/general/archive-bylaws/bylaws-06nov98.htm>, <http://www.icann.org/general/corporate.html>, <http://www.icann.org/general/bylaws.htm>).
7. Домены общего назначения, информация ICANN (<http://www.icann.org/registries/about.htm>).
8. Координационный Центр домена RU (<http://cctld.ru/>).
9. Общий список документов ICANN (<http://www.icann.org/cctlds/background.html>).
10. Перечень зарезервированных имен .ru: (<http://cctld.ru/ru/doc/acting/?id21=20&i21=8>).
11. Правила регистрации (<http://cctld.ru/ru/doc/acting/?id21=13&i21=1>).
12. Принципы управления национальными доменами (http://gac.icann.org/web/home/ccTLD_Principles.rtf).
13. Список документов по проблемам WHOIS (<http://gnso.icann.org/issues/whois/>).
14. Статистический бюллетень RU-CENTER (2006–2007) (<http://stat.nic.ru>).
15. *Храмцов П. Б.* Лабиринт Internet. — М.: Электронинформ, 1996.
16. CIA World Fact Book (<http://www.cia.gov/library/publications/the-world-factbook/>).
17. Council Report to the Board on WHOIS, 15 November, 2007 (<http://gnso.icann.org/issues/whois/gnso-council-report-board-whois-15nov07.pdf>).
18. DNS Security Introduction and Requirements, IETF RFC 4033 (<http://www.rfc-archive.org/getrfc.php?rfc=4033>).
19. DNS Threats & DNS Weaknesses, архив публикаций (<http://www.dnssec.net/dns-threats/>).
20. DNSSEC Research, архив публикаций (<http://www.dnssec.net/research/>).
21. *Lazear W.* RFC-1031. Milnet Name Domain Transition. — 1987. (<http://www.ietf.org/rfc/rfc1031.txt?number=1031>).
22. *Mockapetris P.* RFC-1034. Domain Names — Concepts and Facilities. — ISI, 1987. (<http://www.ietf.org/rfc/rfc1034.txt?number=1034>).
23. *Mockapetris P.* RFC-1035. Domain Names — Implementation and Specification. — ISI, 1987. (<http://www.ietf.org/rfc/rfc1035.txt?number=1035>).
24. Protocol Modifications for the DNS Security Extensions, IETF RFC 4035 (<http://www.rfc-archive.org/getrfc.php?rfc=4035>).
25. Resource Records for the DNS Security Extensions, IETF RFC 4034 (<http://www.rfc-archive.org/getrfc.php?rfc=4034>).
26. Summary of Public Suggestions on Further Studies of WHOIS including the GAC recommendations of 16 April Updated 10 May 2008 (<http://gnso.icann.org/issues/whois/whois-study-suggestion-report-10may08.pdf>).
27. *Weisstein E. W.* Graph. From MathWorld. — A Wolfram Web Resource (<http://mathworld.wolfram.com/Graph.html>).

Венедюхин Александр Анатольевич
Доменные войны (+CD)

Заведующий редакцией (Москва)
Ведущий редактор
Литературный редактор
Художники
Корректоры
Верстка

*И. Воеводин
М. Моисеева
Ю. Соболевская
О. Гуцол, А. Татарко
Т. Дранезо, Ю. Цеханович
Г. Блинов*

Подписано в печать 20.10.08. Формат 60×88/16. Усл. п. л. 15. Тираж 3000. Заказ 11698.

ООО «Питер Пресс», 198206, Санкт-Петербург, Петергофское шоссе, 73, лит. А29.

Налоговая льгота — общероссийский классификатор продукции ОК 005-93, том 2;
95 3005 — литература учебная.

Отпечатано по технологии СІР в ОАО «Печатный двор» им. А. М. Горького.
197110, Санкт-Петербург, Чкаловский пр., 15.

**Александр Венедюхин —**

известный аналитик в области интернет-технологий, доменного рынка, систем адресации сетей передачи данных и специальных средств связи.

Ведущий научно-технического блога www.dxdt.ru, автор научно-популярных публикаций.

Купля и продажа доменов стала в последние годы напоминать «золотую лихорадку» — каждый торопится застолбить «лакомый кусочек», чтобы заработать на нем в будущем. Что и неудивительно, если учесть, за какие астрономические суммы продаются домены вроде sex.com. Александр Венедюхин рассказывает о захватывающих сюжетах тихого регистраторского бизнеса.



На прилагаемом **КОМПАКТ-ДИСКЕ** —

журнал «**Доменные имена**», таблицы «**Виды доменов**», другие полезные материалы

Тема: **Интернет** | Уровень пользователя: **опытный**



www.piter.com — вся информация

Заказ книг: 197198, Санкт-Петербург,
а/я 619; тел.: (812) 703-73-74,
postbook@piter.com

61093, Харьков-93, а/я 9130;
тел.: (057) 758-41-46, 751-10-02,
piter@kharkov.piter.com



ISBN 978-5-388-00728-5

