Доменные имена №1(4) весна 2011

Доменные имена

RU center

весна 2011

Предоставляя услугу сокрытия персональных данных, мы даем пользователю выбор

Александр Панов,
управляющий партнер
Hosting Community

ГЕОдомены —

точные координаты вашего сайта

Вся ГЕОграфия доменов —
на **www.nic.ru**

msk.ru

vologda.su

ivanovo.su

spb.ru

karelia.su

pyatigorsk.ru

Содержание

Весна 2011, №1 (4)

Учредитель
ЗАО «Региональный сетевой информационныйц ентр»
123481, Москва, Свободы, 91, корп. 2, (495) 737 69 75

Издатель
Ателье «Афиши»
atelier.afisha.ru
ООО «Компания Афиша»
125009, Москва, Большой Гнездниковский пер., 7
(495) 785 17 00

Адрес редакции
123308, Москва, 3-я Хорошевская, 2, стр. 1, e-mail: info@nic.ru

Главный редактор
Александр Венедюхин

Редактор номера
Виктория Бунчук

Редакционная коллегия
Андрей Воробьев, Сергей Горбунов, Федор Смирнов

Ателье «Афиши»
Издатель
Наталья Стулова
Дизайн и верстка
Алексей Симонов, Виталий Шебанов
Автор макета, арт-директор
Алексей Симонов
Ответственный секретарь
Татьяна Князева
Фоторедактор
Ксения Манохина
Менеджер проекта
Алина Рябошапка
Цветоделение
Виктор Тишаков, Алексей Новиков, Александр Каштанов
Корректор
Светлана Кантонистова

Печать
ПК «Пушкинская площадь»
Тираж: 10 000 экземпляров

Редакция не несет ответственности за содержание рекламных материалов.
По вопросам размещения рекламы обращайтесь по адресу: info@nic.ru

Наш адрес в Интернете: dn.nic.ru

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия ПИ №ФС77-36679 от 22 июня 2009

Александр Венедюхин, главный редактор «ДИ»

Слово редактора

Уважаемые читатели!
«Доменные имена» отмечают пятилетие: издание в виде альманаха впервые вышло весной 2006 года. Редакция продолжает работу в обычном режиме. С момента выхода из печати прошлого выпуска журнала в Рунете на доменном рынке произошло много интересного. Конечно, среди главных событий опять оказался кириллический домен РФ: осенью 2010 года в нем открылась свободная регистрация имен — и разразился крупнейший за всю новейшую историю Рунета скандал, связанный с аукционами доменов. Поэтому на страницах журнала вы найдете статистику аукционов доменов .РФ, проведенных RU-CENTER (естественно, традиционно мы не прошли мимо общей статистики кириллического домена).

Главная тема этого номера — идентификация. Это одно из самых перспективных технологических направлений в современном Интернете. Киберпространство стало настолько разветвленным и густонаселенным, что без надежных механизмов идентификации пользователей, веб-приложений, программ-ботов, доменов, компьютерных зловредов, отправителей электронной почты, да и всех других многочисленных критически важных элементов Сети — Интернет просто не сможет расти дальше.

На страницах журнала вы найдете статьи о защите персональных данных, о технологических особенностях внедрения кириллических доменов в электронной почте, о росте влияния социальных сетей. А также о развитии геополитической роли системы доменных имен. Раздел «Соседи» посвящен нашумевшей ситуации со связанным с январской революцией отключением египетского сегмента Интернета. Похоже, понаблюдав за событиями на африканском континенте, старинную революционную последовательность можно модернизировать: «Почта, телеграф, телефон... Интернет». То ли еще будет.

RU center

www.nic.ru

Все домены мира

ICANN Accredited Registrar

Регистрируйте домены на любой вкус

.ru .su .me telnic dotMobi

.pro www.registry.pro Afilias SITA neustar

Андрей Воробьев, директор департамента по связям с общественностью RU-CENTER

Спокойствие, только спокойствие!

Уважаемые читатели!
А именно так хочется обратиться к читателям журнала «Доменные имена», которые вместе с нами уже четвертый выпуск подряд с интересом наблюдают за развитием доменной индустрии, а также эволюцией нашего журнала и (что уж там!) за самой компанией RU-CENTER.

За последние полгода произошло много событий. У всех на слуху ставшая скандальной история с началом открытой регистрации доменов .РФ и проведением аукционов за право владения доменами, на которые в ходе сбора предварительных заказов RU-CENTER получил две и более заявки. То, что во всем мире является обычной практикой, в России вдруг попытались объявить вне закона со всеми вытекающими проверками различных комиссий, созданных, похоже, не столько для решения имеющихся вопросов по существу, сколько для поддержания высокого градуса накала страстей... К финалу «кириллическая история» еще не подошла, но уже стала хрестоматийной для наших коллег, особенно из стран СНГ, многие из которых сейчас находятся у истоков создания собственных доменов с символами национальных алфавитов...

Второе событие, перевернувшее «внутренний мир» RU-CENTER и отечественный рынок регистрации доменов, — это объявление о вхождении RU-CENTER в состав группы компаний Hosting Community. Первый вопрос, который мы услышали от журналистов, партнеров, клиентов и коллег по цеху: «Что теперь будет?..» Все будет хорошо! В результате объединения клиенты RU-CENTER смогут получить все самое лучшее, что сегодня предлагается на рынках регистрации доменов и хостинга. Плюс ожидается мощный импульс в развитии новых перспективных проектов.

Кстати, один из таких масштабных проектов, который должен вывести не только компанию, но и доменное пространство страны на новый уровень, — Союз географических и культурно-лингвистических доменов России (RUCLID), задача которого — поддержка региональных инициатив по созданию доменов для городов, территориальных образований, культурных и языковых сообществ. В июне этого года корпорация ICANN должна одобрить правила появления таких и многих других доменов верхнего уровня, так что уже в следующем году нас ждет настоящий бум новых доменов. Граждане, не спешите выстраиваться в очередь, сохраняйте спокойствие!

Последние IPv4-адреса

Неизбежность скорого перехода интернет-сообщества к новому протоколу IPv6 ознаменовала торжественная церемония распределения последних пяти блоков IPv4-адресов между пятью региональными регистратурами, которая прошла 3 февраля 2011 года в Майами (США).

Далее распределение оставшихся адресов будет происходить внутри региональных регистратур между локальными регистраторами — операторами связи и хостинг-провайдерами. Как сообщает Дмитрий Бурков, член правления RIPE NIC, полностью эти адреса будут распределены, по разным оценкам, к середине лета 2011 года или ближе к осени.

День всемирного тестирования IPv6

Несмотря на то что свободных IPv4-адресов осталось менее чем на год, интенсивность перехода на IPv6 крайне мала. По статистике, в настоящий момент только 0,2% пользователей получили возможность прямого обращения к IPv6-сетям.

1338 **блоков IPv6-адресов уже получили европейские провайдеры**

Чтобы помочь ускорить внедрение IPv6, ряд крупнейших интернет-ресурсов, в число которых вошли Google, YouTube, Yahoo! и Facebook, намерены принять участие в проведении Всемирного дня тестирования IPv6, который состоится 8 июня 2011 года. В этот день в течение 24 часов все принимающие участие в акции ресурсы активируют IPv6 на своих сайтах. Подобное масштабное тестирование IPv6 в Сети пока не проводилось, и оно поможет в полной мере оценить готовность сетевых операторов обеспечить поддержку нового протокола и выявить возможные проблемы. По мнению специалистов, на 99,95% обычных пользователей подобный эксперимент никак не отразится, но у оставшихся 0,05% могут возникнуть проблемы из-за нарушения связности сетей или недоработок в поддержке IPv6 программным обеспечением.

Северная и Южная Корея: доменный занавес

Власти Южной Кореи потребовали заблокировать доступ с территории страны к домену Северной Кореи KP.

Согласно официальной информации это вынужденная мера, поскольку северокорейские сайты содержат «неправомерную информацию», которая попадает под действие законов о национальной безопасности и запрете коммунистической пропаганды. Интересно, что интернет-занавес между Северной и Южной Кореями был опущен всего через день после восстановления работоспособности DNS-серверов, поддерживающих работу домена KP (они были отключены, а доменные имена .KP, соответственно, недоступны с третьего квартала 2010 года).

Северокорейские домены вышли онлайн

Заработало то небольшое количество доменов, зарегистрированное в домене Северной Кореи KP. Они были недоступны с третьего квартала 2010 года. Виной всему — аварийное отключение DNS-серверов, поддерживающих работу зоны, причина которого выяснена не была.

Организация IANA указала новые серверы для домена KP — «kptc.kp», — вероятнее всего связанные с Почтовой и телекоммуникационной корпорацией Кореи, официального поставщика телекоммуникационных услуг в стране. По мнению специалистов, это упрочит позиции Северной Кореи в Интернете. Вообще, у пользователей Северной Кореи отключение DNS-серверов домена негатива, как и любых других эмоций, не вызвало. В стране параллельно функционирует так называемый Интранет — работа доменных имен поддерживается автономными (по сути, внутренними) серверами, не подключенными к официальной DNS. Рядовые корейцы не допускаются в Глобальную сеть согласно политике правительства данного государства по ограничению доступа (и, соответственно, влияния) информации из-за рубежа.

Картинки на TEL

С февраля 2011 года на доменах .TEL можно создавать рекламу и объявления, основанные не только на тексте, но и на изображении.

Ранее эта функция для владельцев .TEL была недоступна: на доменах разрешалось размещать только текстовую рекламу (в том числе ссылки). Визуальные объявления могут отображаться на экранах как компьютеров, так и смартфонов. В течение года планируется встроить эту функцию в панель управления доменом, для того чтобы позволить каждому владельцу .TEL создать собственный контент на нем.

ИЛЛЮСТРАЦИЯ: СЕРГЕЙ РАТНИКОВ

Опасный домен COM

Согласно исследованию компании McAfee, специализирующейся на создании систем кибербезопасности, домен COM занимает почетное второе место в списке рисковых доменных зон общего пользования, концентрируя 56% всех небезопасных сайтов.

В опасной пятерке национальных доменов: камерунский CM — 37% рисковых сайтов, китайский CN — 23,4%, самоанский WS — 17,8%, филиппинский PH — 13,1%. В список небезопасных ccTLD также вошли российский RU и армянский AM. Самые безопасные сайты в японском JP. Кроме этого, в пятерке, условно говоря, надежных национальных доменов верхнего уровня — ирландский IE, хорватский HR, люксембургский LU, вануатский VU. Практически не представляют риски сайты, зарегистрированные в доменах TRAVEL и EDU.

Уэльс уступил место

Домен верхнего уровня CYM получат Каймановы острова, хотя изначально на него претендовал Уэльс в рамках программы New gTLD.

Решение о резервировании домена CYM для островов приняла ООН. Определяющим стал тот факт, что бывшая британская колония имеет статус независимого государства, а Уэльс — лишь часть Великобритании. Теперь валлийское интернет-сообщество подумывает над альтернативным вариантом домена. Местные националисты надеются, что он не будет основан на англоязычном слове (так, .WALES признан неподходящим). Пока наиболее популярное среди интернет-пользователей этого региона буквосочетание .GWALIA — устаревшее романтическое название Уэльса.

Человечная New gTLD

Для того чтобы не исключать из процесса New gTLD (программы по созданию неограниченного числа доменов верхнего уровня) ряд категорий заявителей, в ICANN разрабатывается специальная система льгот: софинансирование заявок (но не более 50%), предоставление скидок заявителям и техническая поддержка.

В первую очередь льготы будут доступны претендентам на домены верхнего уровня из развивающихся стран, а также культурно-лингвистическим сообществам, некоммерческим организациям, предпринимателям из стран, где есть препятствия для развития бизнеса. Не смогут воспользоваться системой скидок желающие получить домены-бренды, географические домены и те, у кого есть более-менее значимая государственная поддержка. И если домен окажется успешным, от его администратора могут в дальнейшем потребовать вернуть вложенную субсидию, которая будет повторно реинвестирована в новые проекты, попадающие под льготы в рамках New gTLD.

Домен XXX: тройной приоритет

В марте 2011 года ICANN была одобрена заявка на создание домена XXX, предназначенного для размещения «взрослых» материалов. Регистрацию в ней планируется открыть в 2011 году.

В соответствии с международной практикой запуск XXX начнется с Sunrise-периода, однако не одного, а сразу трех. В первую очередь приоритет получат, конечно, владельцы «взрослых» товарных знаков. Затем к процессу внедрения «трех иксов» смогут присоединиться правообладатели товарных знаков, которые не используются в индустрии эротики (например, Disney): они смогут заявить о своих правах на то или иное обозначение, после чего соответствующее ему доменное имя будет внесено в специальный стоп-лист, что сделает невозможной его регистрацию кем-то еще. На третьем подэтапе пропуском в .XXX послужит уже существующий (функционирующий) «взрослый» домен в другой зоне (например, в COM и пр.).

ИЛЛЮСТРАЦИЯ: ИННОКЕНТИЙ КОРШУНОВ

FR: еще и IDN

13 января 2011 года во Франции был одобрен законопроект, который в том числе предполагает либерализацию регистрационных правил в национальном домене FR, что в перспективе открывает вход в зону и нерезидентам, жителям стран — членов Европейского Союза.

За этой радостной вестью последовала еще одна: в домене Франции будут сняты ограничения и на регистрацию имен с символами национального алфавита (IDN). Предполагаемая дата запуска IDN в .FR — вторая половина 2011 года.

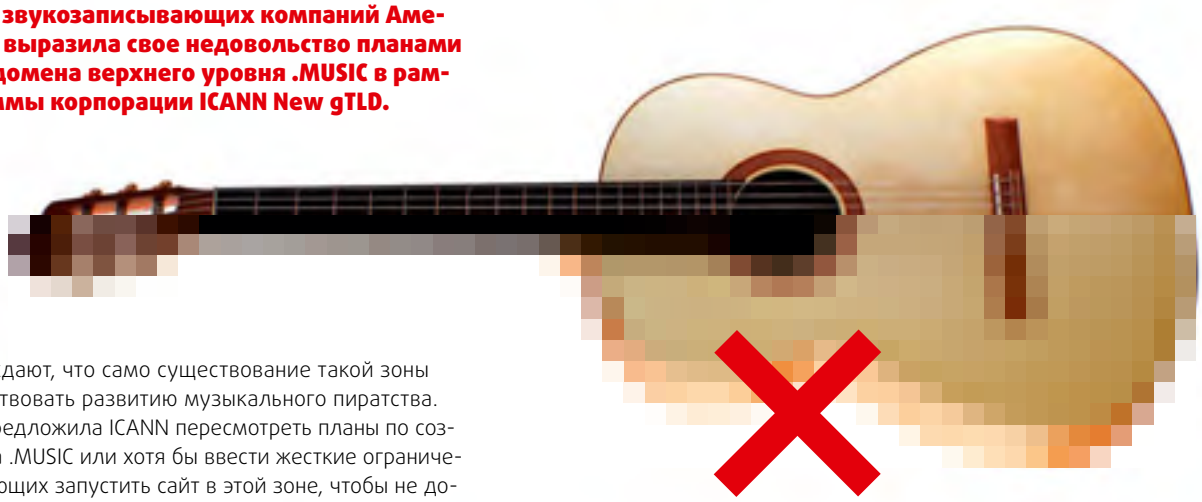
Бесплатные домены для нигерийцев

В домене Нигерии NG выделено 50 тыс. имен для бесплатной их регистрации жителями страны и местными компаниями.

Аттракцион неслыханной щедрости длился в течение 50 дней и завершился 21 марта 2011 года. Продление дареных доменов — платное. А те из них, которые не использовались в течение 6 месяцев, будут удаляться из реестра. По словам власть имущих, данная акция — это возможность «поддержать развитие домена NG как способа национальной самоидентификации в Глобальной сети». Сейчас в зоне зарегистрировано всего около 2 тыс. имен. Кроме того, администратор домена планирует обучать молодых нигерийцев веб-разработке. Будет ли безвозмездным и обучение — не уточняется.

.MUSIC — это зло

Ассоциация звукозаписывающих компаний Америки (RIAA) выразила свое недовольство планами по запуску домена верхнего уровня .MUSIC в рамках программы корпорации ICANN New gTLD.



В RIAA утверждают, что само существование такой зоны будет способствовать развитию музыкального пиратства. Ассоциация предложила ICANN пересмотреть планы по созданию домена .MUSIC или хотя бы ввести жесткие ограничения для желающих запустить сайт в этой зоне, чтобы не допустить «широкомасштабного нарушения авторских прав».

Wikileaks.org заблокировали

В декабре 2010 года делегирование доменного имени скандально известного ресурса Wikileaks.org, на котором публиковались секретные документы государственных органов США, было приостановлено сервисом EveryDNS.net.

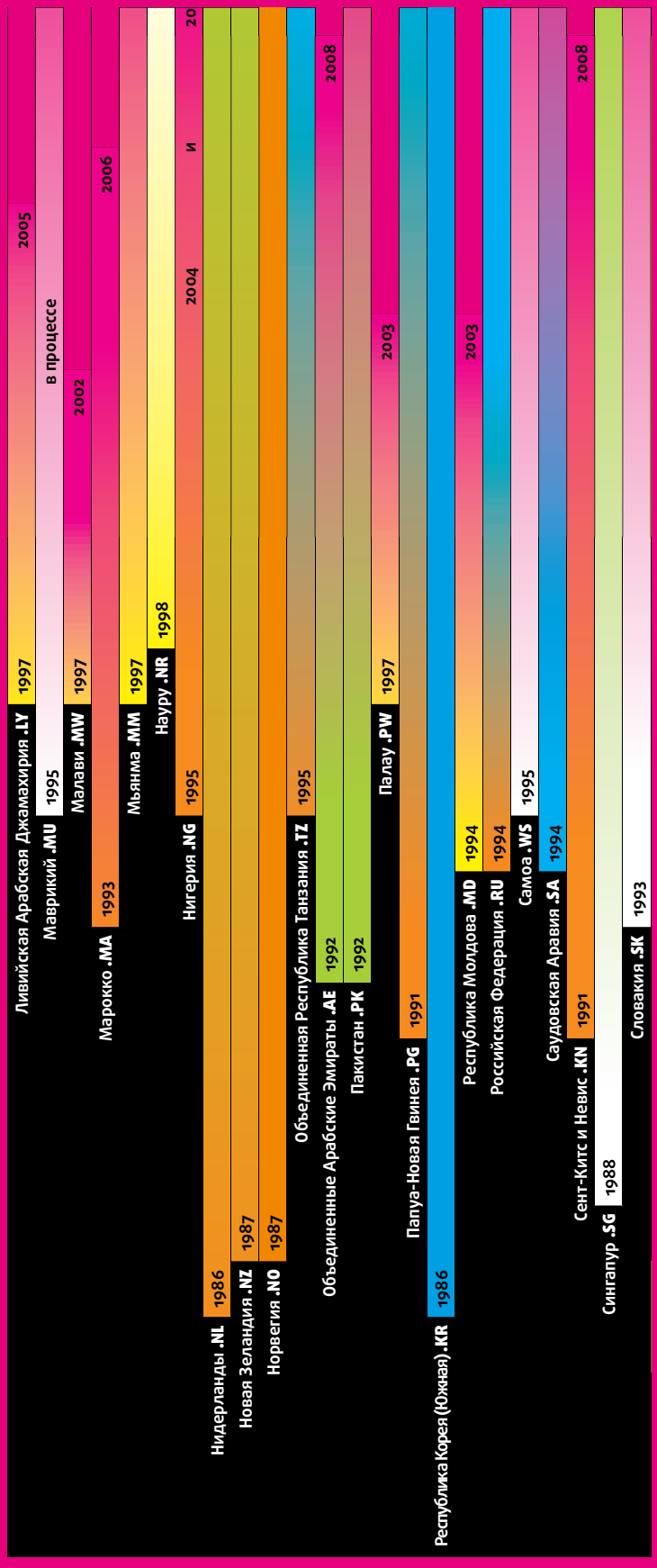
Представители Wikileaks подтвердили факт прекращения работы сайта в Twitter-блоге проекта: «Домен Wikileaks.org убит американским EveryDNS.net после массовых хакерских атак». В ноябре этого года хакеры уже блокировали работу Wikileaks. Как отмечалось тогда в микроблоге, в связи с атакой сайт был недоступен для пользователей США и Европы. Пока ресурс «живет» в домене INFO и в швейцарском .CH. Также на сайт можно зайти, набрав в строке браузера его IP-адрес (213.251.145.96).

26

14

С аукционов RU-CENTER за право обладания кириллическими доменами .РФ былор еализовано 23 113 имен, а средняя цена за домен составила 13 075 рублей

24



Синергетический эффект

В 2010 году RU-CENTER отметил свое десятилетие. Компания выросла из РосНИИРОС, организации, которая была первым администратором домена RU. С момента создания регистратора RU-CENTER началось развитие системы распределенной регистрации доменов в зоне .RU, итогом которой стало возникновение конкурентного рынка регистрации доменов в Рунете.

RU-CENTER — одна из крупнейших компаний в отрасли интернет-услуг, чей профессионализм давно заслужил самые высокие оценки экспертов. Наши компании более 10 лет идут бок о бок, нас связывают тесные партнерские отношения. Объединение усилий позволит достичь более высоких бизнес-показателей и будет полезным как обеим компаниям, так и интернет-сообществу в целом

Александр Панов,
управляющий партнер
Hosting Community

2011 год уже стал не менее значительным для истории компании, чем прошлый год, юбилейный. В марте 2011-го было объявлено о планах по вхождению RU-CENTER в состав группы компаний Hosting Community. Решение готовилось давно. Переговоры о слиянии компаний начались еще осенью 2010 года. Вхождение компании в группу является для нее наиболее логичным развитием — ведь RU-CENTER достиг того уровня, когда эффективно вести разветвленный высокотехнологичный бизнес в Интернете в одиночку уже невозможно.

Как говорится в пресс-релизе, посвященном вхождению RU-CENTER в группу Hosting Community: *«Участники сделки ожидают от объединения серьезного синергетического эффекта, увеличения рентабельности обеих компаний, а также укрепления лидерских позиций на рынке хостинга и регистрации доменов. Совместная деятельность даст партнерам возможность предоставлять более качественные услуги клиентам объединенной компании. Учитывая размер компании, наличие сложных программных и аппаратных средств, большие клиентскую и договорную базы, стороны договорились о введении в ЗАО «РСИЦ» должности управляющего. Эту позицию занял Александр Панов, управляющий партнер Hosting Community. Основной задачей господина Панова станет соблюдение интересов Hosting Community в процессе слияния, контроль финансовых потоков и любых существенных событий ЗАО «РСИЦ». Экс-гендиректор ЗАО «РСИЦ» Алексей Лесников перешел на должность советника управляющего».*

Сообщения об объединении компаний СМИ связал с громким скандалом в домене .РФ. Как известно, конец 2010 и начало 2011 года в российской доменной индустрии теперь навечно связаны с понятием доменных аукционов. Ведь именно аукционы доменов .РФ, проведенные ведущим регистратором RU-CENTER, стали краеугольным камнем конфликтной ситуации, в которой вторую ключевую роль сыграл Координационный центр национального домена.

Мы предлагаем нашим читателям обзор ситуации на мировых аукционных площадках, где совершаются сделки по доменным именам (в рамках как вторичного рынка, так первичного — на одном из этапов запуска новых или перезагрузки уже существующих доменных зон), а также итоговые статистические данные по выкупленным на аукционах RU-CENTER кириллическим доменам. АМ

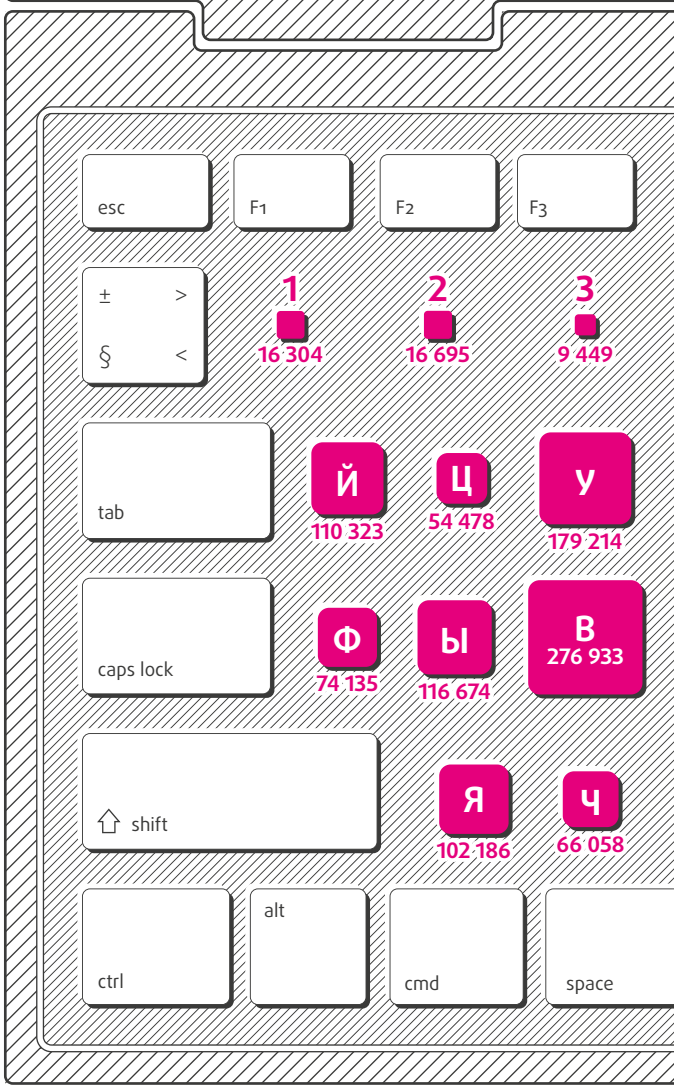
Мы искренне рады возможности в скором времени предоставить всем нашим партнерам и клиентам доступ к дополнительному набору услуг хостинга от признанного профессионала этого рынка — Hosting Community

Алексей Лесников,
советник генерального
директора ЗАО «РСИЦ»

ИЛЛЮСТРАЦИЯ: АЛЕКСЕЙ СИМОНОВ

С молотка

Слово «аукцион» вызывает образ человека с молотком, принимающего ставки из зала и считающего удары до победного «Продано!» Традиционная ассоциация. Для мира реального. В виртуальном — все несколько иначе. Особенно если на кону не вещь, а доменное имя.



Хотя эта поправка вовсе не отменяет тех вылазок в мир не ботов, но людей, которые совершают доменные инвесторы в поисках нового «вкусного» объекта вложения средств. Да. И виртуальное имущество можно приобрести, а в данном случае — выторговать, офлайн. Однако подобные мероприятия классифицируются скорее как шутки ради: серьезная игра на вторичном рынке доменных имен идет как раз на онлайн-площадках, близких к нему по сетевому духу.

Здесь не выкрикиваются суммы, не стучит молоток — торги проходят без шума и пыли. Главное — вовремя кликать мышью и следить за обновлением ставок на экране любого девайса, подключенного к Интернету. Однако так ли важно, как проходят торги? Ключевым в понимании силы аукциона должен стать ответ на вопрос «Для чего?»

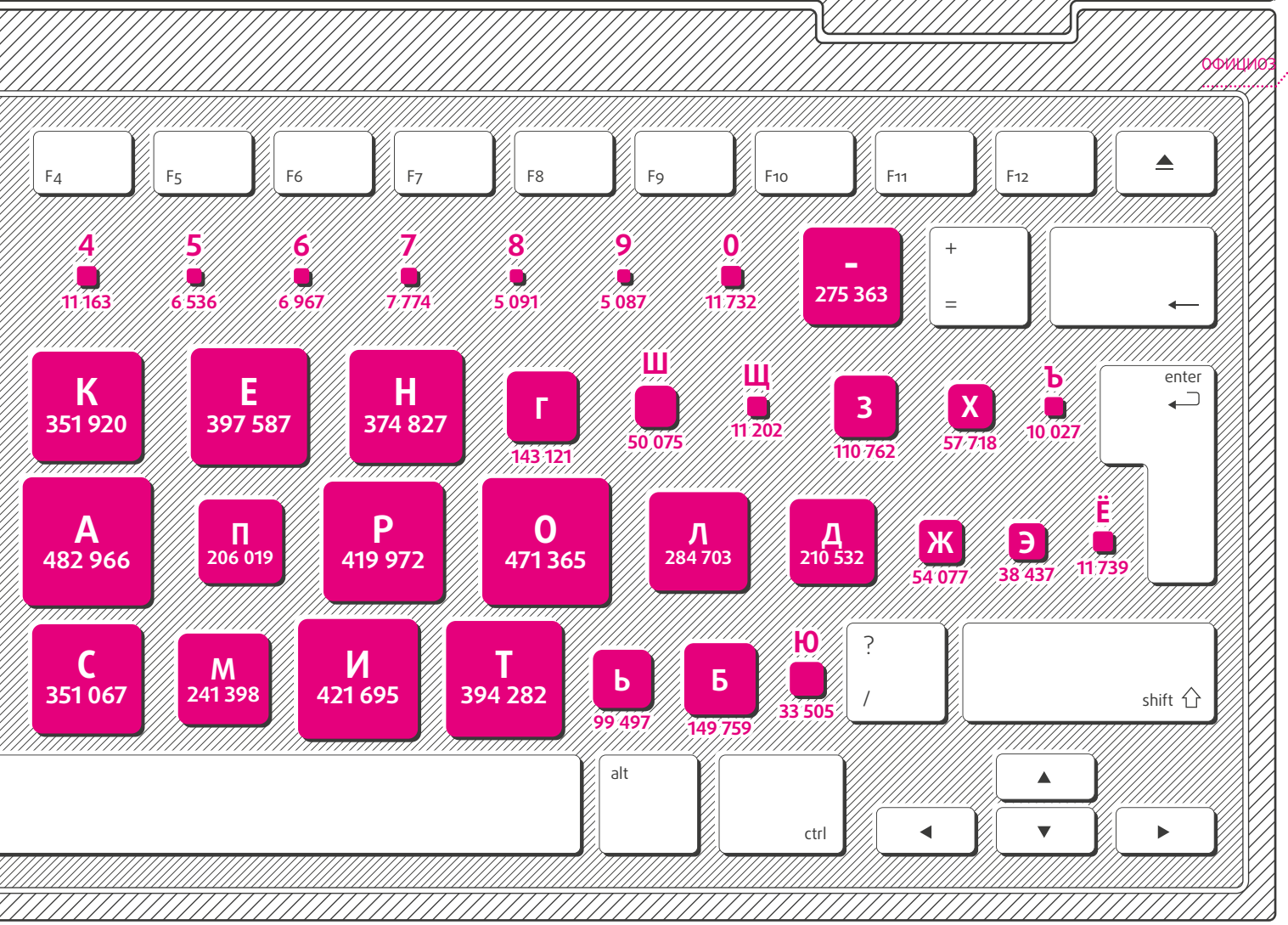
Цена вопроса

С растущей теснотой в доменном мире, когда уже не найти простое запоминающееся имя (иначе «ключевик» — словарное слово) не то что в классических доменах — «пионерах» DNS типа COM, ORG, NET, — но даже в национальных зонах, которые сегодня развиваются опережающими темпами, инструменты вторичного рынка как никогда актуальны. Именно на вторичном рынке можно найти премиум-домены на любой вкус и в любой интересующей вас зоне. В чем подвох? Цена вопроса.

В результате торгов (например, на аукционе) стоимость доменного имени может возрасти до... Трудно сказать, есть ли предел денежным возможностям покупателя, который во что бы то ни стало решил заполучить это имя, а затем использовать его для ведения сетевого бизнеса или (и так случается не редко) перепродать его в энный раз, когда в более-менее популярных доменных зонах станет еще теснее и единственной возможностью зарегистрировать «ключевик» будет невзрачный, ни с чем не ассоциирующийся у мирового сообщества, однако «малозаселенный»д омен типа ZW.

Так вот, насчет ценовых пределов. Долгое время титул самой крупной сделки на вторичном доменном рынке принадлежит домену Sex.com. Не слетела корона первенства с него и после того, как он чуть больше полугода назад был выставлен на торги повторно (в связи с банальным банкротством его владельца). В итоге в 2006 году за Sex.com, по разным источникам, была отдана сумма, равная $12–14 млн; в 2010-м — количество миллионов закрепилось на отметке $13 млн.

Нынешний владелец Sex.com, холдинг Clover, так комментирует сделку: «Мы постепенно по-



Число доменных имен .РФ, содержащих заданный символ (букву)

купали некоторые отраслевые домены, которые совпадают с ключевыми словами или названиями брендов определенных видов прибыльного онлайн-бизнеса и бизнеса, который, как мы полагаем, может стать прибыльным в будущем. Домен Sex.com подходит под эти критерии».

И вернемся к первой тройке условного списка доменов-миллионников: на втором и третьем местах в ней расположились Fund.com ($10 млн) и «собрат» лидера Porn.com ($9,5 млн).

И в качестве, и в количестве

Между прочим, количество букв, а также присутствие или отсутствие оных в доменном имени часто определяют его стоимость. Так в 2008 году некая компания из Великобритании приобрела на вторичном рынке доменных имен Cruises.co.uk более чем за $1 млн (отметим, что в Соединенном Королевстве это первая и единственная миллионная сделка по домену). Интересно, что к моменту совершения сделки

Домены, за которые когда-либо сражались на аукционах, за которые отдавались крупные суммы, — или словарные слова, или короткие и легкозапоминающиеся понятия

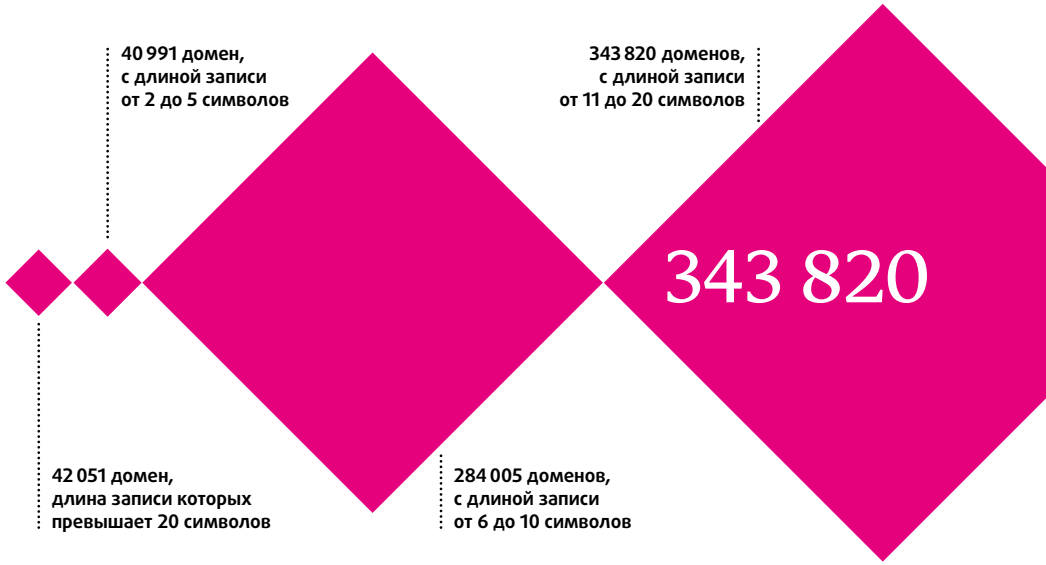
Под занавес 2010 года в этот «золотой» домен-чарт вклинился двубуквенник FB.com. В частном порядке он был продан за $8,5 млн. Казалось бы, что примечательного в этих двух буквах? Станет понятно, когда узнаете, кто заплатил за них эти бешеные деньги: крупнейшая и известнейшая социальная сеть Facebook. В планах создателей ресурса использовать короткий домен для неких «внутренних нужд». Некоторые источники указывают, что на нем будут размещаться электронные почтовые адреса пользователей социальной сети. Кстати, подобный подвиг в 2008-м совершила компания Yellow Pages, купив YP.com за $3,85 млн.

компания уже обладала доменом Cruise.co.uk — без буквы «s» в окончании, — но так хотела иметь его множественный вариант, что, не задумываясь, выложила миллион по сути за одну только букву «s». Вообще, миллионные сделки по доменным именам, зарегистрированным в национальных зонах, совершаются гораздо реже, чем, например, в уже упомянутом и знаменитом на весь интернет-свет COM (по данным некоторых исследований, предметом около 50% сделок, которые совершаются на доменных аукционах, являются именно домены .COM). Кроме «нацдомена» Cruises.co.uk в список доменов-миллионников входят «немцы» Shopping.de ($2,8 млн) и Kredit.de ($1,3 млн).

ИНФОГРАФИКА: НАДЕЖДА АНДРИАНОВА

Число доменов .РФ по регистраторам, на 01.03.2011

RUCENTER-REG-RF	232 082
REGRU-REG-RF	159 746
RUCENTRE-REG-RF	111 576
R01-REG-RF	97 343
REGISTRATOR-REG-RF	32 694
NAUNET-REG-RF	26 603
REGGI-REG-RF	23 597
REGTIME-REG-RF	21 578
CENTROHOST-REG-RF	17 773
NETFOX-REG-RF	14 865
SALENAMES-REG-RF	9072
AGAVA-REG-RF	5628
REGISTRANT-REG-RF	5080
101DOMAIN-REG-RF	4643
DOMENUS-REG-RF	4443
ELVIS-REG-RF	446
DEMOS-REG-RF	441
CC-REG-RF	238
RTCOMM-REG-RF	196
TCI-REG-RF	30
RELCOM-REG-RF	29
BEELINE-REG-RF	18
TESTMONITOR-REG-RF	2



Самые длинные домены:

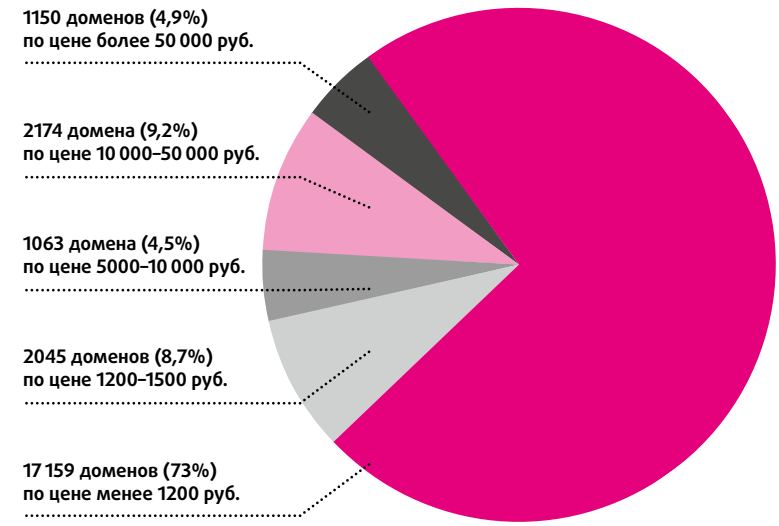
0000000000000000000000000000000000000000000000000000000000000000.рф
9999999999999999999999999999999999999999999999999999999999999999.рф
7777777777777777777777777777777777777777777777777777777777777777.рф
0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0.рф
Яяяя.рф
1111111111111111111111111111111111111111111111111111111111111111.рф
0----------0.рф

Стоимость доменов .РФ, выкупленных на аукционах RU-CENTER, данные на 21.12.2010, 12:00

13 075 руб.

— средняя цена за домен, выкупленный на аукционе

Инфографика подготовлена на основе данных на 1 марта 2011 года



Обоим доменам, ушедшим с молотка в 2008 году, дали звание героев вторичного рынка Германии. В 2010 году нескольких сотен тысяч долларов не дотянули до миллиона тезка одного из вышеупомянутых «немцев» Credit.fr ($850 тыс., Франция) и OnlineCasino.dk ($580 тыс., Дания).

Кстати, домены, связанные с азартными играми онлайн, очень частые гости аукционов. В начале 2000-х домен Casino.com ушел с молотка за $5,5 млн (в 2010-м за аналогичную сумму был продан другой азартный домен — Slots.com). Есть свое «казино» и в домене Германии: Casino.de с результатом $625 тыс. На третьем месте по количеству тысяч долларов за казино-домены стоит наш соотечественник Casino.ru ($235 тыс.), который кроме всего прочего открывает десятку крупнейших сделок, совершенных на вторичном рынке Рунета. За ним с довольно большим отрывом идут People.ru

ИЛЛЮСТРАЦИЯ: АЛЕКСЕЙ СИМОНОВ

($90 тыс.), Hi.ru ($80,6 тыс.), 2014.ru ($83 тыс.) и, конечно, Vodka.ru ($50 тыс.).

В общем, все перечисленные домены, за которые в свое время сражались на аукционах, за которые отдавались крупные суммы, — это либо словарные слова, либо короткие и легкозапоминающиеся понятия. (Нет, конечно, случаются и такие курьезы, как GamblingForumOnline.com, проданный за $1,1 млн. Специалисты почти уверены, что это утка. Во-первых, нелогично платить семизначную сумму за трехсложный, а потому неудобный и труднопроизносимый домен; во-вторых, еще можно найти пару звонких заменителей этого громоздкого нечто; в-третьих, владельцем домена стала компания BestOCG.com, простенький, утыканный партнерскими ссылками сайт, который не говорит о миллионных доходах учредителей.)

Однако неправильно будет ассоциировать аукционы только со вторичным рынком. Ведь изначально премиум-домены появляются на рынке первичном с первым же владельцем, успешно зарегистрировавшим таковой по стандартной процедуре через обычную компанию-регистратора. Но когда-то, на заре Интернета, о ценности доменного имени мало кто задумывался, считая его лишь удобным дополнением к сайту. Сегодня ситуация кардинально поменялась и за новые «вкусные» домены, которые прибывают вместе с открытием новой доменной зоны, так называемые киберсквоттеры готовы драться на самом первом этапе.

Аукцион — не аукцион

Осознавая всю значимость премиум-доменов, администраторы вновь открывающихся зон хотят уберечь их от банальной скупки пачками на первичном рынке по бросовой цене (что случается, если зона открывается сразу для всех желающих) лишь для последующей перепродажи. Такие домены, конечно, должны работать и приносить доход, но, пожалуй, не за счет бесконечного круговорота на вторичном рынке, однажды начатого киберсквоттером. Сегодня составляющая успеха компании, да и обычного пользователя, решившего проявить свои способности в Интернете, — сайт. И чем удачнее его доменное имя (читай — название), тем больше шансов, что его запомнят — заметят — начнут активно посещать. Дабы дать шанс обзавестись доменной роскошью всем, в новых доменах верхнего уровня проходят этапы премиальных регистраций. Или попросту аукционы с приемлемой стартовой ценой. С помощью аукционов распределялись премиум-домены, например, в зоне Черногории ME. На торги были выставлены такие имена, как Airport.me, August.me, Read.me, Save.me, Irina.me, Ankara.me и пр. Одну из самых высоких ставок получил домен Date.me — $70 тыс. Периодом премиальных регистраций предварялось открытие свободной регистрации для всех желающих в домене Колумбии CO. Крупнейшей стала продажа O.co за $350 тыс. Его владелец — онлайн-магазин Overstock.com. С однобуквенника сейчас идет переадресация на основной сайт ресурса. Подобная схема распределения доменных имен применялась и при открытии кириллического домена .РФ

Простая истина, что сегодня домен — это не только набор символов, придуманный для удобства обозначения IP-адреса, но и нематериальный актив, или, если уж совсем глобально, предмет первой необходимости. Он нужен для того, чтобы ты был в Сети. А не в Сети сегодня, пожалуй, только ленивый.

От редакции

Проворный запуск

Старта открытой регистрации в новом домене РФ ждали все, кто хоть как-то связан с российским сегментом Сети. Надежды и опасения, впрочем, были разными.

Кто-то полагал, что особенного всплеска регистраций ожидать не приходится. Кто-то считал, что спрос на кириллические домены окажется вполне ощутимым. Надо заметить, оптимисты представляли меньшинство. И едва ли кто-то предсказал то, что в итоге случилось. А случился рекордный бум.

11 ноября 2011 года в 12.00 по Москве открылся для приема заявок реестр домена РФ. Уже за первые два часа зарегистрировали около 80 000 доменов .РФ. За первые сутки — около 240 000. А спустя неделю новый домен РФ уже оказался в числе густонаселенных национальных доменов с числом регистраций, превысившим 500 000 (см. статистику по регистрациям на следующем развороте).

Часть новых доменов .РФ попала на аукционы RU-CENTER. Регистратор принимал от своих клиентов предварительные заявки на кириллические имена. Если на один домен претендовало более одного заявителя, то домен направлялся на закрытый аукцион, проводимый между этими заявителями. Конечно, для выставления домена на аукцион RU-CENTER должен был еще успеть его зарегистрировать раньше других регистраторов. Надо заметить, что регистратору это удалось в отношении большой части доменов клиентов.

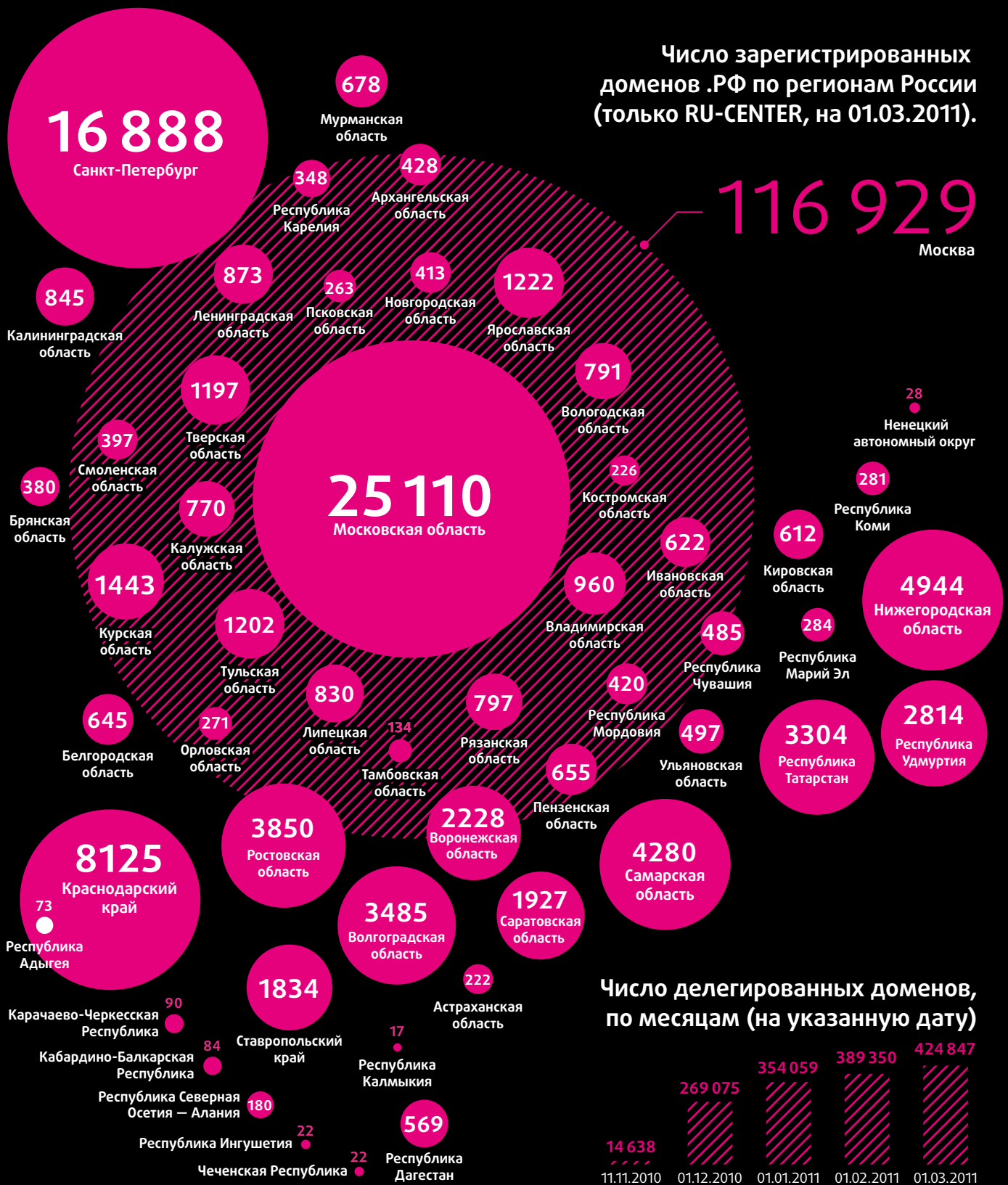
Для проведения аукциона RU-CENTER регистрировал доменное имя на себя — это решение, соответствующее опыту проведения аукционов на вторичном рынке доменов. Кроме того, RU-CENTER были достигнуты договоренности с другим регистраторами, аккредитованными в .РФ, для использования их квоты на доступ к реестру. Это было сделано для того, чтобы иметь возможность обработать максимальное число заявок, — у RU-CENTER наиболее многочисленная клиентская база.

Именно аукционы RU-CENTER составили основу очередного громкого скандала в домене РФ. Координационный центр предположил, что при проведении аукционов были нарушены правила регистрации доменов РФ. Разбирательство по этому вопросу затянулось, КЦ лишь постоянно переносил дату принятия решения, и даже в середине марта 2011 года (то есть спустя более чем четыре месяца с момента открытия свободной регистрации) никакой ясности в вопрос внесено так и не было.

Процесс проведения аукционов доменов .РФ в RU-CENTER постарались сделать максимально прозрачным. Так, на специальной странице info.nic.ru/auction/index.html публиковалась статистика хода аукционов.

Статистика регистраций домена .РФ

Источник: stat.nic.ru

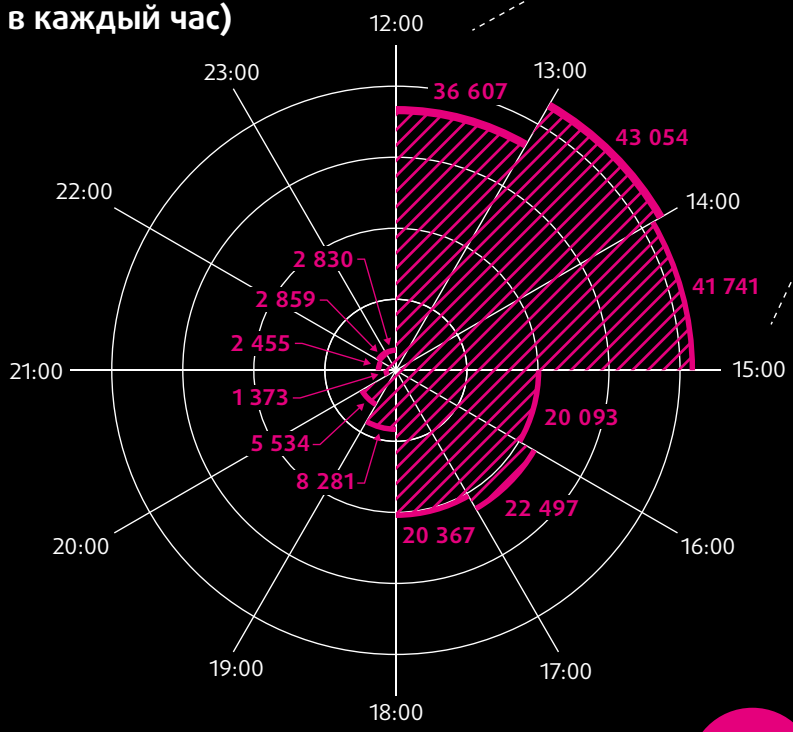


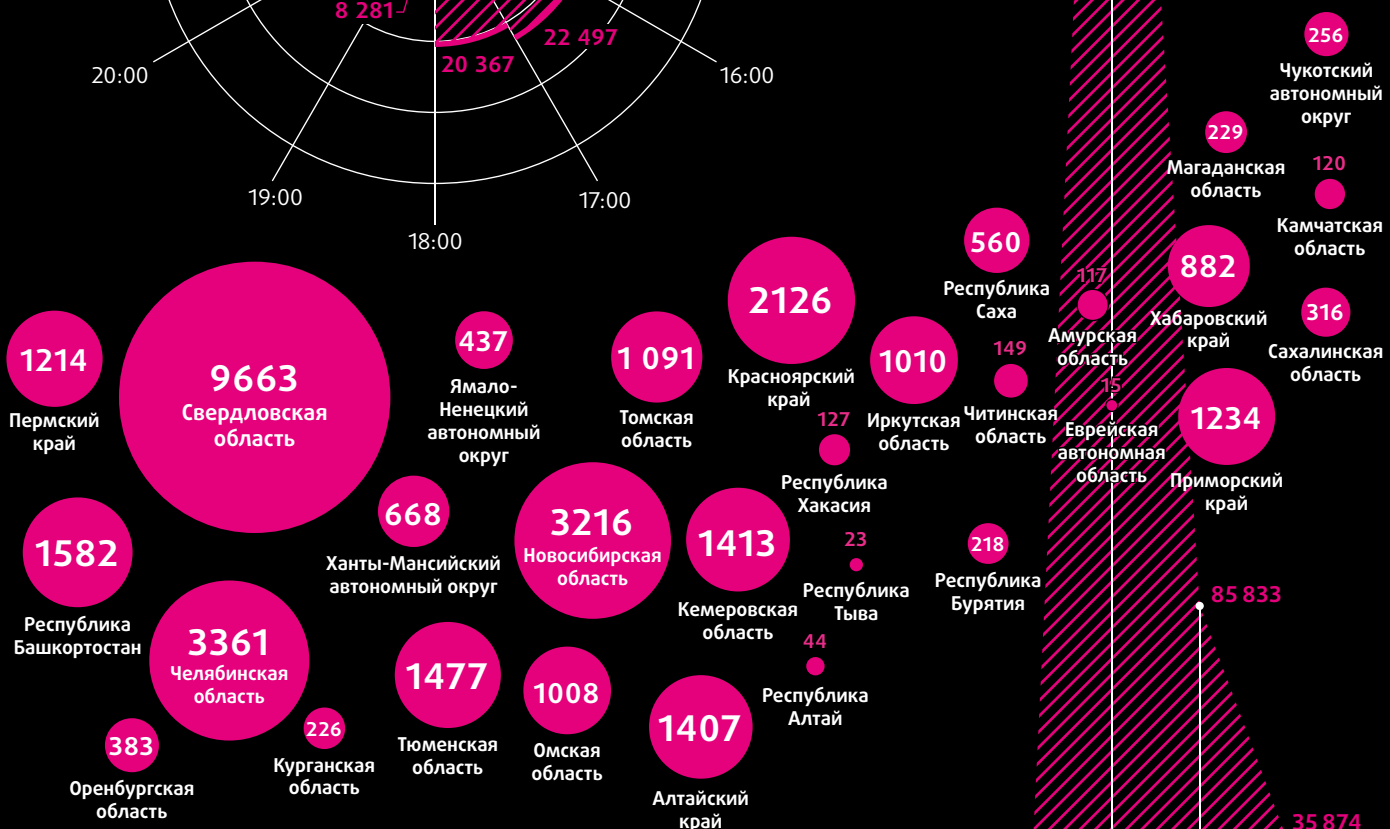
Всего доменов .РФ зарегистрировано (на 01.03.2011):

768 123

596 215
старт открытой регистрации

Регистрация доменов .РФ 11.11.2010 по часам (число доменов, зарегистрированных в каждый час)





Прирост зарегистрированных доменов .РФ по месяцам

ИНФОГРАФИКА: НАДЕЖДА АНДРИАНОВА

Дарья Баринова,
аспирант кафедры сравнительной политологии МГИМО

Автор выражает благодарность за помощь в написании статьи научному руководителю доктору политических наук, профессоруИ льину М.В.

Методы анализа информационной суверенности государства в национальных доменах

Национальные домены, созданные более 25 лет назад как технические коды, становятся важнейшими ресурсами государственной информационной инфраструктуры.

Введение

Когда мне предложили раскрыть тему информационного государственного суверенитета в свете национальных доменов, то я некоторое время пребывала в сомнениях: можно ли вообще употреблять словосочетание «информационный государственный суверенитет» применительно к Интернету? Традиционно суверенитет понимается как принцип, применяемый к территориальным образованиям, а мы ведем разговор об информации в Интернете — сетевом пространстве символов, где вместо территорий и физических границ — коды национальных доменов.К роме того, само понятие «суверенитет» вызывает споры, поскольку единогласия по поводу его употребления в современном дискурсе нет. Поэтому в данной статье я буду говорить не о суверенитете, а об информационной суверенности государства в Интернете; о том, как ее можно измерять и сравнивать по национальным доменам.

Когда мы говорим о суверенности — мы говорим о характеристике государства, а не о международном политическом принципе. Информационная суверенность государства как способность государства контролировать информационные потоки. Эта способность касается и военных, и многих других ресурсов, но в данном случае речь пойдет об информационных потоках, создаваемых такими ресурсами, как национальные домены.

Созданные чуть более 25 лет назад как технические коды для геолокализации в Интернете, сегодня эти цифровые ресурсы можно причислить к национальным ресурсам, составляющим основу информационной инфраструктуры. Такие источники, как CIA World Factbook, BBC Country Profile, включают данные о наличии у государства национального домена в один ряд с такими его атрибутами, как население, площадь, форма правления и ВВП. Наличие у страны национального домена свидетельствует о заинтересованности в получении видимости в Интернете и является важным показателем развития национальной Сети: это платформа для развития национальной экономики и национальных институтов в Интернете. Это позволяет гражданам, бизнесу, государственным и негосударственным институтам обозначить свою принадлежность к виртуальному представительству (национальному домену) данной страны.

Национальные домены можно рассматривать не только как ресурсы, но и как метод анализа распределения национальных доменных ресурсов, их уровня развития и принципов управления, позволяющий сравнивать между собой такие уникальные явления мировой политики, как современные государства. Эта статья о том, какие условия необходимы для проведения анализа информационной суверенности государства на уровне адресного пространства Интернета; о том, как оценить степень суверенности по количеству национальных доменов и по тому, кто ими управляет.

Признаки информационной суверенности государства

Для того чтобы государство могло контролировать свои информационные потоки в Интернете на уровне DNS, необходимо, чтобы выполнялись минимум два условия:

1) наличие информационного потока, то есть наличие у государства собственного национального домена;

2) наличие государственного контроля над потоком, создаваемым национальным доменом, то есть наличие у государства (государственного агента) статуса администратора национального домена.

Таблица 1. Примеры размещения сайтов официальных властных институтов непризнанных государств в Интернете

В национальных доменных зонах других стран

Сайт президента Южной Осетии	в национальном домене России, www.presidentrso.ru
Сайт президента Нагорного Карабаха	в национальном домене Армении, www.president.nkr.am
Сайт Министерства иностранных дел Нагорного Карабаха	в национальном домене Армении, www.nkr.am
Сайт президента Северного Кипра	в национальном домене Евросоюза, www.kktcb.eu

В доменных зонах общего пользования

Сайт президента Абхазии	www.abkhaziagov.org
Сайт Республики Южная Осетия	www.republicofsouthossetia.org
Сайт правительства Косово	www.rks-gov.net
Сайт парламента Косово	www.assembly-kosova.org
Сайт президента Косово	www.president-ksgov.net
Сайт премьер-министра Косово	www.kryeministri-ks.net
Сайт президента Приднестровья	www.pmr-gov.org
Сайт правительства Приднестровья	www.vspmr.org
Сайт правительства Нагорного Карабаха	www.karabakh.net
Отдел внешней информации Северного Кипра	www.trncinfo.com/TANITMADAIRESI

Эмпирический анализ показал, что сегодня национальные домены есть практически у всех существующих стран и зависимых территорий. Всего в Сети действует 247 национальных доменов, из которых 192 — домены стран-членов ООН и 53 — домены разных территориальных образований. Можно говорить о том, что пространство национальных доменов воссоздает сетку международной политической системы в Интернете — с той разницей, что в киберпространстве функцию базовых ячеек выполняют не государства, а национальные домены, основанные на кодах стран.

Результаты исследования показывают *неравномерное распределение доменных ресурсов* по странам.

Своих национальных доменов нет у шести непризнанных государств: Косово, Абхазии, Южной Осетии, Северного Кипра, Нагорного Карабаха и Приднестровья. Властям этих стран приходится размещать официальную информацию о себе либо на национальных доменах дружественных стран, либо в доменах общего пользования (*Таблица 1*).

При этом у непризнанных государств есть интерес в получении своего «представительства» в DNS. Так, год назад ко мне обращались представители властей Нагорного Карабаха с вопросами по процедуре получения национального домена. В свое время представители Абхазии и Южной Осетии обращались в ICANN с просьбами делегирования доменов — AB или AP для Абхазии и OS или SO для Южной Осетии[1]. Однако ICANN их просьбы рассматривать отказалась, предпочитая дожидаться реакции мирового сообщества. При этом свои домены есть у Тайваня, Палестины и Западной Сахары. То есть при картировании политического пространства Интернета по внешнему признаку (национальному домену) информационная суверенность Тайваня и Палестины окажется равной суверенности, скажем, Китая или Израиля: Тайвань (.TW) и Палестина (.PS) будут отмечены такими же двубуквенными кодами, как и Китай (.CN), и Израиль (.IL).

Как уже было сказано вначале, наличие домена — минимально необходимое условие для развития информационной суверенности в Интернете. Будет ошибкой утверждать, что все государства, обладающие национальным доменом, имеют равный суверенный статус в Сети. Нужно учитывать, способно ли государство создавать условия для развития своего доменного ресурса (онлайн-платформы). Например, домен Западной Сахары .EH существует более 10 лет, но так до сих пор и не был делегирован по причине нерешенного вопроса политического статуса самойЗ ападной Сахары, и, как следствие, домен остается необжитой платформой, не создающей информационного потока. В то же время в домене Тайваня около 500 000 регистраций, а с 2010 года страна получила две дополнительные платформы для развития в Интернете — домены на национальных языках. Это пример того, как экономическая состоятельность страны влияет на ее информационный суверенитет, несмотря на де-юре непризнанный статус Тайваня. Стоит выделить и группу территориальных

В последние 10 лет мы наблюдаем, как коммерческие «доменные войны» уступают место политическим: государства формируют онлайн-присутствие через национальные домены

[1] *Виртуально не признанные республики. Журнал «Ъ-Власть» №38 от 29.09.2008 — www.kommersant.ru/doc-rss.aspx?DocsID=1031505*

Мнение

Влияние международного права

Андрей Воробьев,
директор департамента по связям
с общественностью RU-CENTER

На регистратуры и регистраторов национальных доменов все более существенное влияние оказывают международные режимы защиты прав интеллектуальной собственности: традиционный, основанный на Бернской и Парижской конвенциях и координируемый Всемирной организацией интеллектуальной собственности (ВОИС), и новый режим Всемирной торговой организации (ВТО), в основе которого лежит Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS). Так, под влиянием этих документов с 2008 года изменено российское национальное законодательство в области охраны интеллектуальной собственности: впервые в Гражданском кодексе Российской Федерации доменное имя соотнесли с другими средствами индивидуализации. Российская судебная практика разрешения доменных споров пока крайне противоречива, но регистраторы неукоснительно исполняют вступившие в законную силу решения суда.

образований, получивших благодаря своим национальнымд оменам статус «виртуальных стран», однако в реальном мире далеко не равновеликих по политическому статусу: это особое территориальное образование — Евросоюз, нейтральная территория — Антарктида, и многочисленные зависимые территории.

История Интернета знает случай, когда создание информационной суверенности государства предшествовало формированию его политической суверенности. В 1997 году был делегирован домен .TP. Так Восточный Тимор стал первым «виртуальным государством», а независимость он получил в 2002-м (в 2005 году, как

Наличие национального домена — минимально необходимое условие для развития информационной суверенности государства в Интернете

следствие изменения названия страны с Portuguese Timor на Timor Leste, название домена изменили на TL; этот домен передали под управление правительства Восточного Тимора). И хотя мы не можем утверждать, что создание домена и получение Тимором независимости не были случайным совпадениями, можно предположить, что создание домена для непризнанных государств до получения ими статуса международно признанных будет способствовать усилению их информационной суверенности и, возможно, ускорит их вступление в клуб международно признанных государств. Важно обратить внимание политиков на то, что необходимо заранее просчитывать последствия получения национального домена.

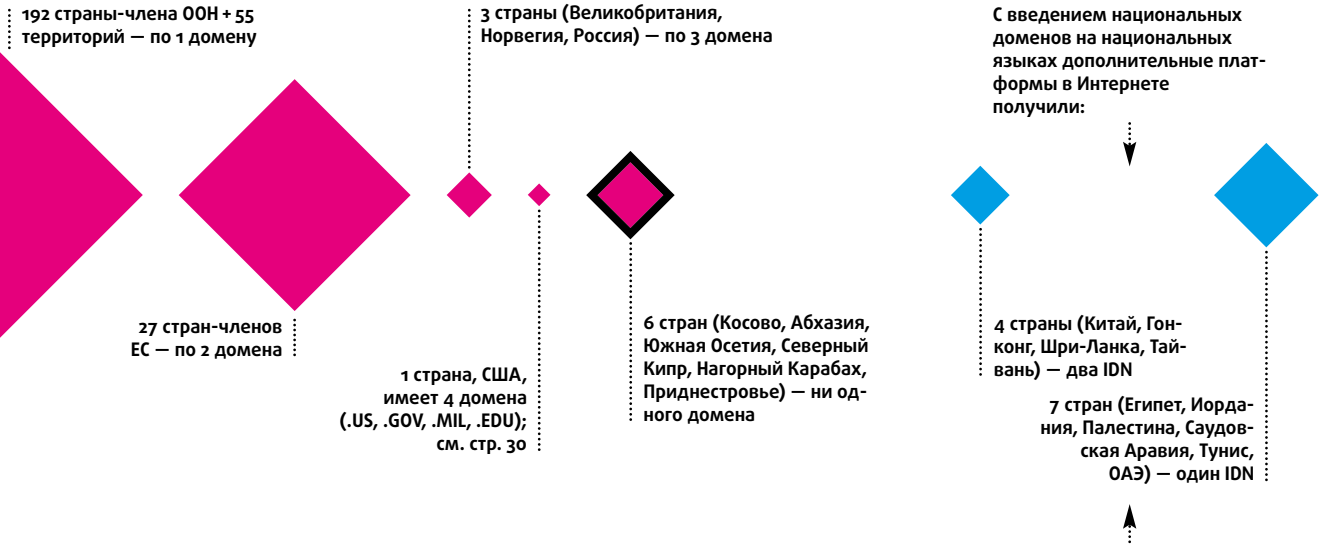
Анализ показал, что у некоторых стран есть *несколько национальных доменов* (*Таблица 2*). Можно предположить, что наличие дополнительных доменов создает для страны преимущество в международной информационной среде.

Участие государства в управлении своими доменами

Вторым минимальным условием для формирования информационной суверенности государства является контроль над информационными потоками. Вопрос: всегда ли государство участвует в управлении своим национальным доменом? Как может государство осуществлять этот контроль? Все ли страны и территории, у которых есть национальные домены, способны контролировать информационные потоки, создаваемые в доменных зонах?

В Таблице 3 (стр. 24) представлены результаты эмпирического исследования, целью которого было выявить тенденции в управлении адресным пространством Интернета. Полученные данные показывают, что пространство национальных доменов формировалось на протяжении 10 лет, с 1985 по 1995 годы, в «доICANNовский» период, и управление осуществлялось по принципу «снизу-вверх»: так из 192 стран-членов ООН лишь в 25 странах государство сразу подключилось к созданию и развитию национального домена, но в основном инициаторами выступали академические институты (в 70 странах), либо волонтеры (в 20 странах), либо неправительственные организации (в 29 странах). Второй период управления начинается с нулевых: по Таблице 3 мы видим всплеск интереса государств к управлению национальными доменами, о чем явно свидетельствует волна переде-

Таблица 2. Неравномерное распределение доменных ресурсов по странам



гирований (в 80 странах). Хотя не во всех странах в результате переделегирования функции администратора доменной зоны получает государство, но сама процедура переделегирования инициируется государством, и новый администратор назначается с согласия не только ICANN, но и государства. Любопытно, что половина переделегирований проходила официально (есть данные отчетов IANA), а половина — неофициально (нет данных в базе отчетов IANA).

Если первые 20 лет существования Интернета за онлайн-присутствие (доменные имена и сайты) борьбу вели в основном представители бизнеса, в то время как для государств использование экономических и политических ресурсов Сети было периферийным делом, то за последние 10 лет Сеть стала типичным примером критической информационной инфраструктуры по значению и использованию — и мы наблюдаем, как коммерческие «доменные войны» уступают место политическим: государства, в частности Россия, формируют онлайн-присутствие уже не только через сайты, но и через национальные домены, платформы для развития национальных институтов и экономик в Интернете.

Два потока

Наличие национального домена является условием создания информационного потока, при этом национальный домен позволяет создавать сразу два потока:

1) верхний — поток, создаваемый самим кодом домена;
2) нижний — поток, создаваемый пользователями, регистрирующим домены в данной национальной зоне.

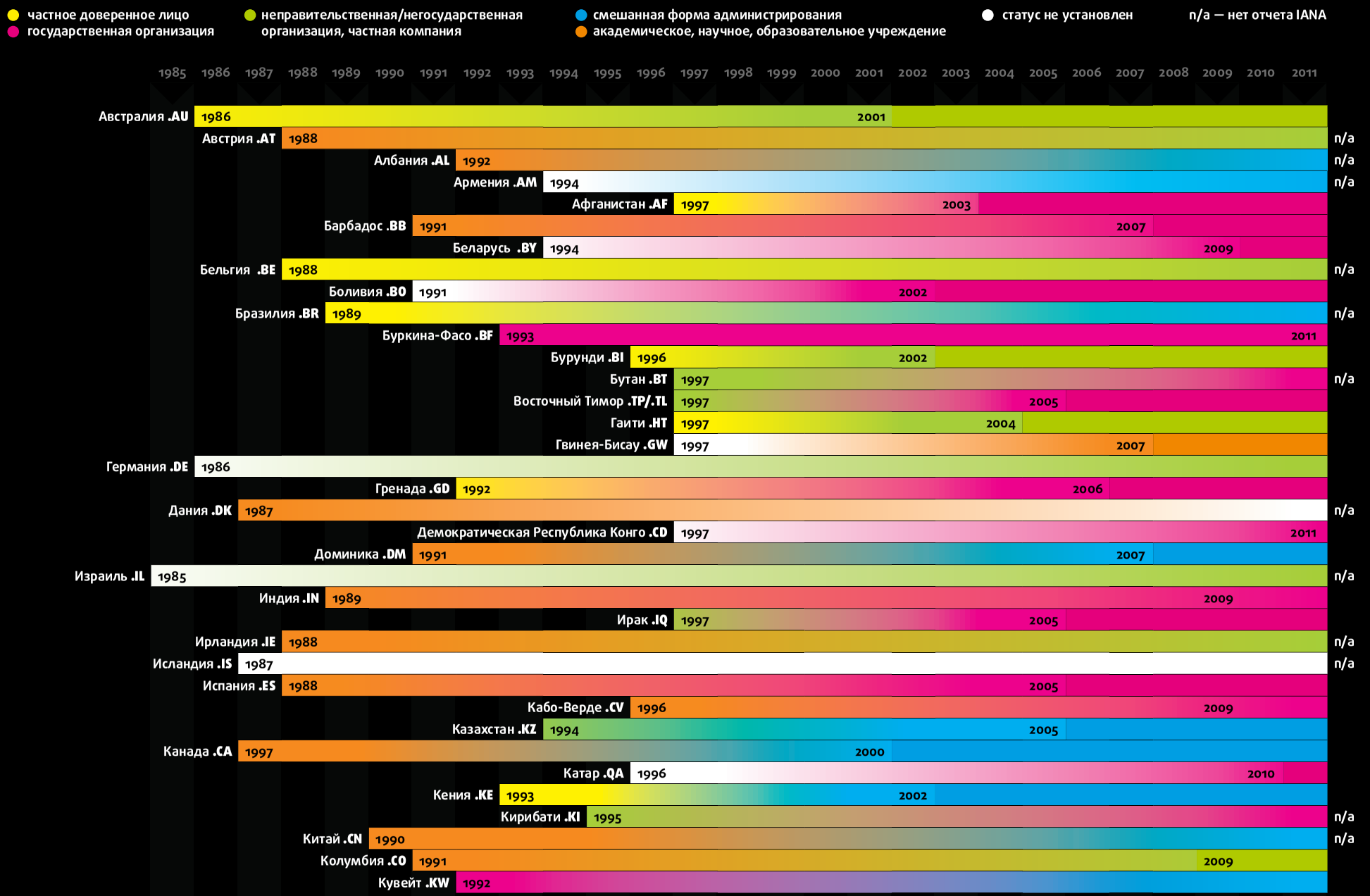
Верхний поток дает возможность стране существовать в Интернете. Государство получает возможность администрировать свою кибертерриторию, маркировать ее, проводить в ней свою политику. Наличие домена также позволяет государству представлять свои интересы как участника международной интернет-системы в различных международных институтах по управлению использования Интернета, таких как ICANN, RIPE, CENTR и пр.

Администрирование домена не является достаточным условием для контроля над информационным потоком. Существует и нижний поток, который характеризуется такими показателями, как виртуальное население (количество регистраций в национальной доменной зоне), национальный состав населения (соотношение резидентов страны к нерезидентам), а это напрямую связано с проблемой состоятельности (то, что в международном политическом дискурсе называется stateness problem), то есть с проблемой лояльности граждан своему государству, которая, в свою очередь, зависит от позитивного имиджа государства, от способности государства создать надежную информационную инфраструктуру, условия для развития интернет-бизнеса, обеспечить кибербезопасность пользователей в своей национальной доменной зоне — то есть от реальной состоятельности государства. Если у государства слабая состоятельность, как у Нигерии, то оно не сможет контролировать ни нижний, ни верхний информационные потоки в своем доменном пространстве.

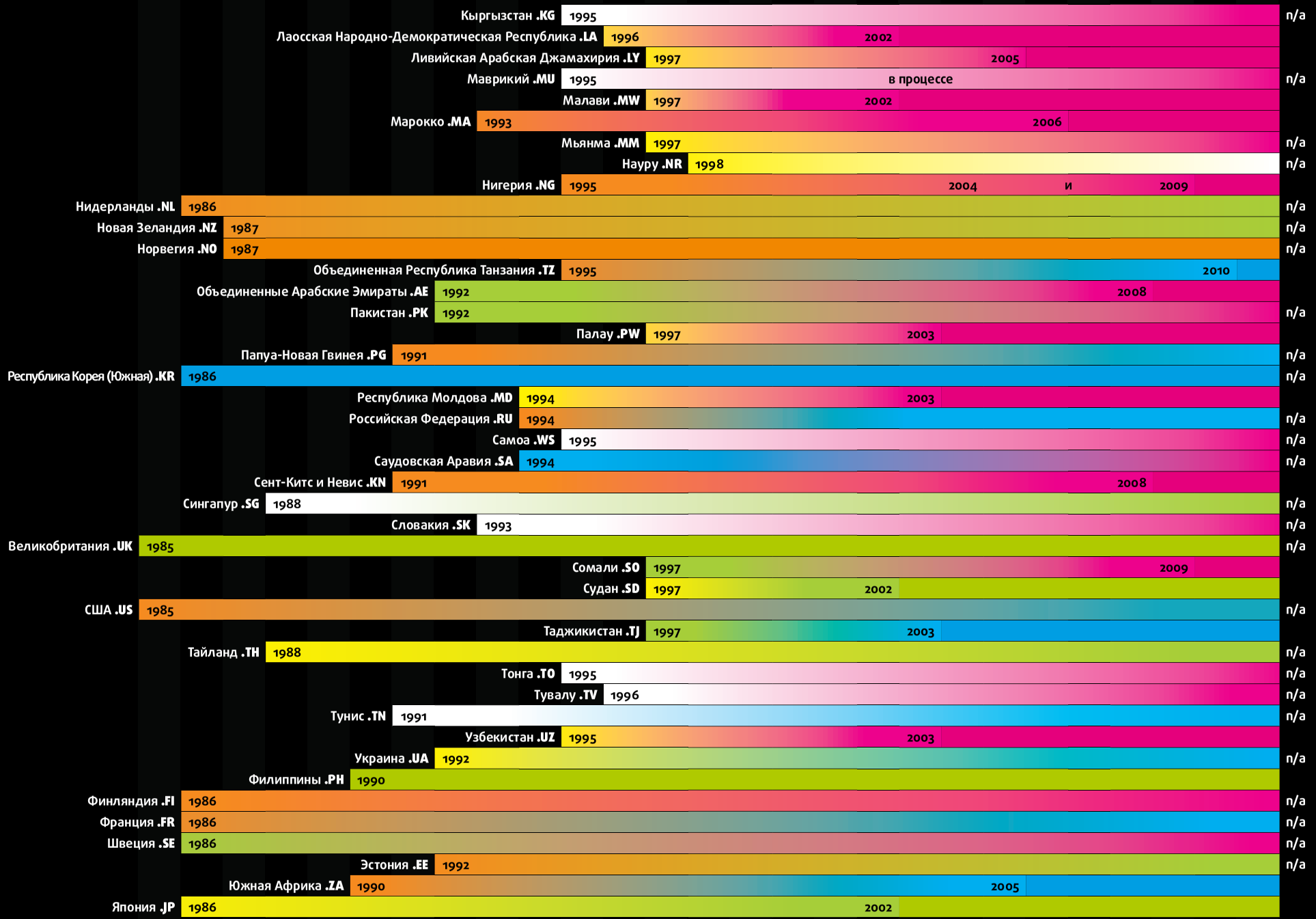
Заключение

Сами по себе национальные домены — это лишь возможности государства. Необходимо создавать условия, чтобы они приносили пользу. Гарантией успешной реализации политического курса правительства России по созданию единого национального информационного пространства в Интернете будет создание нормальных условий существования в этом пространстве для пользователей, проведение образовательных курсов. Понимание организации политического пространства Интернета, умение его визуализировать и анализировать будут также этому способствовать. Описанный здесь подход может быть использован как вспомогательный инструмент при разработке программ по развитию национального Интернета.

Временная шкала ределегирования управления некоторыми национальными доменами



ИНФОГРАФИКА: АЛЕКСЕЙ СИМОНОВ



Источники — базы данных IANA Root Zone DB, ccNSO, CENTR, Wikipedia, справочник по доменам RU-CENTER

Андрей Воробьев,
директор департамента по связям
с общественностью RU-CENTER

Устали ждать, но по-прежнему верим...

В марте в Сан-Франциско прошла 40-я конференция ICANN. Совет директоров ICANN одобрил «дорожную карту», предусматривающую итоговое утверждение новых правил создания доменов верхнего уровня в июне этого года.

Итак, завершилась 40-я международная конференция 18 марта. И проходила она в самом сердце IT-технологий — в Кремниевой долине (из-за неправильного перевода в народе она более известна как Силиконовая долина), что не замедлило сказаться на программе мероприятия: перед участниками конференции выступили 42-й президент США Билл Клинтон, в годы президентства которого и была основана ICANN, и отец-основатель Интернета Винт Серф. Оба авторитетных докладчика высоко оценили роль интернет-технологий в современном мире и в своих выступлениях остановились на гуманитарных аспектах развития Сети. Так, Билл Клинтон назвал доступ в Интернет одним из основных всеобщих прав человека. «Когда я занял свой пост в 1992 году, было всего около 50 сайтов в Интернете. Когда я покинул свой пост через восемь лет, их было уже примерно 36 миллионов», — сказал мистер Клинтон, дав оценку ICANN как уникальной некоммерческой многосторонней организации, созданной для координации глобальной системы адресации в Интернете. Говоря о будущем ICANN, экс-президент подчеркнул, что корпорация должна оставаться независимой и открытой для сотрудничества.

На конференции ICANN был обнародован план, в соответствии с которым процесс окончательного утверждения программы New gTLD должен завершиться на внеочередном заседании совета директоров ICANN 20 июня 2011 года

Пройдемся по ключевым моментам...

Ключевой темой очередной конференции было заявлено финальное обсуждение и утверждение программы New gTLD, предусматривающей существенное увеличение числа доменов верхнего уровня и упрощение процедуры их появления. Ожидалось, что именно в Сан-Франциско завершится многолетнее обсуждение правил создания новых доменов верхнего уровня, так называемого «Руководства претендента на общий домен верхнего уровня». В этом документе подробно описывается весь процесс подачи заявки на домен, а также сопутствующие этому процессу процедуры — в частности, по разрешению возможных конфликтных ситуаций, например, в случае получения нескольких заявок на один домен от разныхз аявителей. Однако документ так и не был утвержден.

ICANN заявляла о том, что ей потребуется около 2–3 месяцев на маркетинговые действия, связанные с программой New gTLD. Выходит, первые заявки на новые домены верхнего уровня будут получены ICANN не ранее осени 2011 года

XXX — домен такой домен...

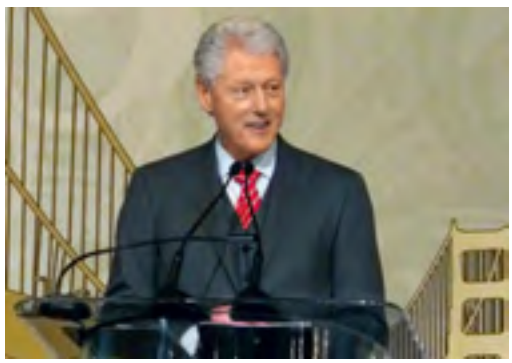
Напомним, в 2006 году совет директоров ICANN принял решение об отказе от подписания соглашения с ICM Registry на управление доменом для взрослых. Позже соглашение было доработано, однако и в новой редакции оно не удовлетворило GAC. В итоге в марте 2007 года совет ICANN и плох, что договориться, как показывает практика, удается далеко не всегда. В лице GAC корпорация ICANN приобрела настоящую головную боль. Однако уже в последний день конференции на итоговом заседании совета директоров ICANN показательным утверждением домена XXX (против появления которого выступил GAC) руководство корпорации отчетливо продемонстрировало, что можно найти средство для избавления от любой боли.

Для США исключений из общего правила о равноправии участников процесса управления Интернетом сделано не будет, даже несмотря на огромную роль Штатов в его создании

Запуск программы вновь отложен, на этот раз из-за существенных разногласий ICANN и GAC.

GAC — это Комитет правительственных советников ICANN, международный консультативный орган, в который входят официальные представители почти 100 стран мира, в том числе и России. Именно расширение полномочий GAC в свое время позволило ICANN продемонстрировать всему миру желание сделать процесс управления адресным пространством Интернета более интернациональным и отменить монопольное право США на управление Глобальной сетью. Влияние правительства США действительно было ослаблено, однако переход на коллегиальный принцип принятия решений тем окончательно отклонил заявку ICM. Казалось бы, судьба домена XXX была решена. Однако ICM Registry не собиралась опускать руки.

Представители компании решили оспорить решение ICANN и с этой целью инициировали процедуру его независимой экспертизы, предусмотренную уставом корпорации. По итогам разбирательства позиция ICANN была признана необоснованной. Выводы экспертов были приняты к сведению советом ICANN, в результате чего работа над внедрением домена XXX была продолжена. Однако главным противником реинкарнации идеи создания домена XXX выступил GAC. Несмотря на то что в финальной версии соглашения на управление доменом были



Слева вверху: Винт Серф, отец-основатель Интернета, в своем выступлении остановился на гуманитарных аспектах развития Сети

Слева внизу: Билл Клинтон, 42-й президент США, назвал доступ в Глобальную сеть одним из основных всеобщих прав человека

Справа вверху: Род Бекстром, президент ICANN: «Мы верим в принцип: все, кто имеет интересы в Интернете, обладают одинаковым правом быть услышанными при формировании его политики управления»

Справа внизу: Несмотря на отсутствие поддержки со стороны GAC (Правительственный комитет ICANN), 18 марта 2011 года договор с компанией ICM Registry на управление доменом XXX был одобрен советом ICANN

Вопрос

Довод о том, что домен XXX поддерживается далеко не всеми представителями индустрии для взрослых, в ICANN сочли незначимым. Мол, доменная зона внедряется в интересах того сообщества, к которому относит себя претендент на нее, в данном случае компания ICM Registry. А считать или не считать себя членом этого сообщества — личное дело каждого, и к созданию домена этот вопрос никакого отношения не имеет. Из итоговой резолюции ICANN по домену XXX складывается устойчивое ощущение, что путем его утверждения корпорация просто решила обрести дополнительный источник дохода. Возражения о высокой стоимости доменных имен .XXX в ICANN парировали, отметив, что вопросами ценообразования не занимаются.

В то же время, оценивая возможный эффект от предстоящего внедрения XXX, в корпорации удовлетворенно заявили, что доходы от регистрации во «взрослой» зоне пойдут на развитие деятельности ICANN.

учтены все вопросы, которые возникали у правительственного комитета ранее, 16 марта 2011 года GAC опубликовал резолюцию, в которой говорилось о том, что комитет не поддерживает внедрение домена для взрослых.

Несмотря на отсутствие поддержки со стороны GAC, 18 марта 2011 года договор с компанией ICM Registry на управление доменом XXX был одобрен советом ICANN. Объясняя свою позицию, совет корпорации весьма категорично подчеркнул, что для одобрения домена XXX не требуется обязательного согласия со стороны правительственного комитета.

ICANN, равноправие, братство

Вместе с тем на церемонии открытия конференции президент корпорации ICANN Род Бекстром подчеркнул важность сохранения многосторонней модели управления этой международной организации. «Мы верим в простой принцип: все, кто имеет интересы в Интернете, обладают одинаковым правом быть услышанными при формировании политики управления Глобальной сетью, — сказал Род Бекстром. — Когда все голоса услышаны, ни один голос не может доминировать».

В сентябре этого года истекает текущий контракт между ICANN и правительством США, регулирующий исполнение функций IANA, поэтому в своей речи Род Бекстром особо подчеркнул, что даже для правительства Соединенных Штатов исключений из общего правила о равноправии участников процесса управления Интернетом сделано не будет, несмотря на огромную роль США в создании Глобальной сети. Стоит отметить, что о выходе на новый уровень отношений с правительством США Род Бекстром говорил еще в 2010 году на конференции ICANN в Брюсселе, отмечая тогда, что тесная кооперация ICANN с Минторгом США будет продолжена, но уже в новом международном контексте. Любопытно, что при обсуждении крайне неудобного для ICANN вопроса о независимости корпорации секретарь Торговой палаты США Лоуренс Стриклинг раскритиковал нынешнее устройство коллегиальной модели управления

В сентябре 2011 года истекает действующий контракт между корпорацией ICANN и правительством США (Минторгом), регулирующий исполнение функций IANA

ICANN. По его мнению, корпорация недостаточно прозрачна, а членам Комитета правительственных советников ICANN следует дать больше шансов быть услышанными и принимать решения, основываясь на компромиссе между всеми участниками процесса.

Опять двадцать пять!..

Увы, к этому самому компромиссу ICANN и GAC в Сан-Франциско так и не удалось прийти. Из-за разногласий между ICANN и GAC «Руководство претендента на общий домен верхнего уровня» вопреки ожиданиям одобрено не было. Немного позитива в эту грустную картину добавило обнародование плана дальнейших действий, в соответствии с которым процесс окончательного утверждения программы New gTLD должен завершиться на внеочередном заседании совета директоров ICANN 20 июня 2011 года перед началом конференции ICANN в Сингапуре. Напомним, что разработка регламентирующих появление новых доменных зон документов началась еще в 2008 году. Стоит отметить, что сейчас рассматривается уже пятая версия правил. Глава корпорации ICANN Род Бекстром подчеркнул, что в финальной версии правил разработчики постарались предусмотреть интересы всех заинтересованных сторон.

В официальном сообщении Координационного центра национального домена сети Интернет по итогам конференции ICANN дается экспертный прогноз развития дальнейших событий: «В случае, если ICANN будет придерживаться расписания и объявит об утверждении «Руководства претендента» на сессии в Сингапуре, новые домены появятся еще не скоро: учитывая, что ICANN потребуется около двух-трех месяцев на маркетинговые действия (организация заявляла об этом ранее), первые заявки будут получены ICANN не ранее осени 2011 года. Если принять во внимание среднюю скорость обработки заявки на домен, существующую сейчас, от получения первых заявок до делегирования доменов может пройти полгода-год. После делегирования пройдет еще какое-то время, отпущенное на приоритетную фазу регистрации, — а это означает, что домены, запущенные в рамках новой программы, фактически не будут доступны широкой общественности до 2013 года. Стоит отметить, что все вышесказанное верно для доменов, которые не вызывают споров, тогда как заявки, по которым у ICANN или третьих лиц могут быть возражения, безусловно, будут обрабатываться значительно дольше. Кроме того, нельзя забывать, что программа вызывает массу возражений у GAC, надзорного правительственного комитета, и до тех пор, пока все разногласия не будут решены, руководство претендента на новый домен не получит официального статуса».

Мнение

New gTLD вопреки...

Сергей Горбунов,
главный специалист по международным связям RU-CENTER

По итогам консультаций, состоявшихся в Сан-Франциско, в текущую редакцию New gTLD будут внесены определенные изменения. И затем, согласно представленной «дорожной карте», в ICANN намерены во что бы то ни стало утвердить программу создания новых доменов верхнего уровня .Впрочем, как уже не раз бывало, эти планы могут быть скорректированы.

Очевидно, что измененная версия New gTLD может вновь не удовлетворить GAC. Что тогда будет делать ICANN — пока неясно. Но твердая решимость одобрить программу внедрения новых доменов верхнего уровня может заставить корпорацию действовать вопреки мнению GAC. То, что такое возможно, уже доказано на примере домена XXX, который был утвержден без согласия правительственного комитета. Этот случай весьма показателен и заставляет задуматься о том, насколько международным можно считать процесс управления Интернетом. Ведь, как выясняется, при необходимости американская корпорация ICANN вполне может принимать решения по важным вопросам и без согласия GAC, который выражает мнение представителей многих государств мира.

По мнению ряда зарубежных экспертов, появление упрощенной процедуры введения новых доменов верхнего уровня должно в будущем привести к сокращению споров по поводу товарных знаков. Род Бекстром, президент корпорации ICANN, считает, что введение новых доменных зон снизит желание компаний и физических лиц бороться за уникальные веб-адреса: «Просто с запуском новых доменов верхнего уровня у физических лиц и компаний появится больше возможностей получить желанное доменное имя». Бекстром также отметил, что это позволит уменьшить привязку Интернета к англоговорящей аудитории: «Причин две: большее разнообразие среди западных языков, использующих латинский алфавит, а также новые возможности использовать другие символы».

* * *

И в общем, несмотря на все разногласия между ICANN и GAC, в интернет-сообществе теплится надежда, что эти двое смогут договориться и программа New gTLD стартует. Ближайшее место и время встречи — июнь 2011-го, Сингапур, канун 41-й международной конференции ICANN.

По мнению экспертов, деятельность ICANN не достаточно прозрачна, а членам GAC следует дать больше шансов быть услышанными и принимать компромиссные решения

Домены-космополиты

Каждый домен общего назначения (gTLD) уникален и обладает особой философией.

MOBI

Для сайтов и сервисов, ориентированных на работу с мобильными телефонами и беспроводными устройствами; домен, объединяющий Интернет и мобильные технологии.
www.mtld.mobi

TEL

Предназначен для хранения контактной информации (сайтов-визиток), данные публикуются непосредственно в DNS — создание веб-сайта и хостинг не требуются.

COOP

Для кооперативов и других совместных предприятий.
www.nic.coop

INT

Для регистрации доменных имен международными организациями. Решение принимается международной организацией IANA при условии соблюдения регистрантом целого ряда требований.

NET

Изначально домен NET создавался специально для организаций, связанных с сетевыми технологиями и развитием систем телекоммуникаций. NET входит в число первых доменов, появившихся в Интернете.

ORG

Изначально был создан специально для некоммерческих организаций; появился одновременно с доменами COM и NET — на заре внедрения системы доменных имен.
www.pir.org

MUSEUM

Для музеев, а также организаций, имеющих отношение к музейному делу. Кроме того, зарегистрировать домен в .MUSEUM могут и частные лица, профессионально связанные с этой сферой деятельности.

COM

Изначально домен COM предназначался исключительно для коммерческих организаций, однако со временем принятые в нем регистрационные правила стали весьма либеральными. Самый крупный домен в мире — в нем зарегистрировано около 90 млн имен.

INFO

Сокращение от повсеместно признанного термина information («информация»).
www.nic.info

Доменное пространство для организаций, работающих в сфере туризма. Регистрация домена в .TRAVEL требует подтверждения принадлежности к туристическому бизнесу.
www.travel.travel

Создан специально для авиации и авиационной индустрии; требует подтверждения принадлежности к аэроиндустрии.
www.information.aero

Специализированная доменная зона, созданная для общения работодателей и наемных работников.
www.goto.jobs

Предназначен для лицензированных специалистов. Имя в .PRO могут получить представители более 1100 профессий из разных стран; единственное требование — наличие документа, подтверждающего его специализацию в какой-либо области (фактически диплом).

Для коммерческих организаций, предприятий и корпораций. Считается альтернативой домену COM.
www.neustarregistry.biz

«Именной домен», позволяет зарегистрировать в качестве домена имя и фамилию; предназначен для персональных страничек.

Исключительно для федеральных государственных учреждений США.

Эксклюзивно используется структурами Минобороны Соединенных Штатов; здесь размещаются сайты организаций, имеющих отношение к военному ведомству США.
www.nic.mil

Для различных образовательных учреждений США (школ, университетов, колледжей с четырехгодичным курсом обучения и пр.).
educause.edu/edudomain

Для представителей лингвистического и культурного сообщества испанской провинции Каталония.
www.domini.cat

Создан специально для резидентов 73 стран Азиатско-Тихоокеанского региона и Австралии (в список потенциальных регистрантов в домене ASIA входят как экономически развитые страны — Япония, Австралия, так и государства пока развивающиеся — Корея, Индия, Китай).
www.registry.asia

ИЛЛЮСТРАЦИЯ: ИННОКЕНТИЙ КОРШУНОВ

Евгений Беспалов,
генеральный директор фонда «Дружественный Рунет», к.э.н.

Горячая линия «Дружественный Рунет»: результаты 2010 года

Фонд «Дружественный Рунет» реализует в России комплексную стратегию в области безопасного Интернета.

Горячая линия по приему сообщений о детской порнографии является необходимым элементом комплексной системы противодействия противоправному контенту. Она работает в связке с Управлением «К» МВД России, взаимодействует практически со всеми ведущими представителями отечественной интернет-индустрии: операторами связи, хостерами, регистраторами доменных имен. Кроме того, фонд является российской контактной горячей линией международной ассоциации INHOPE.

За 12 месяцев 2010 года на горячей линии было обработано 22 161 сообщение от граждан и организаций. По этим сообщениям было обнаружено 11 016 адресов, содержащих контент с признаками детской порнографии (порносайты или отдельные разделы/страницы с фото- и видеоматериалами на общетематических веб-сайтах). При посредничестве горячей линии фонда «Дружественный Рунет» удален контент с 9739 адресов (удалены сайты или контент с отдельных страниц). Из всей массы удаленных ресурсов 9248 адресов располагалось в России, и 491 — за рубежом.

По информации, полученной с горячей линии фонда, в течение 2010 года сотрудники подразделений «К» МВД России возбудили 24 уголовных дела по ст. 242.1 УК РФ. Для сравнения: в 2009 году, по информации с горячей линии, было возбуждено 9 уголовных дел по статье 242.1 УК РФ.

В 2010 году наблюдался существенный рост количества сообщений, направляемых пользователями на горячую линию фонда «Дружественный Рунет». Если в 2009 году аналитики горячей линии обработали 9693 сообщения, то в 2010 году было обработано 22 161 сообщение. Более чем двукратный рост количества сообщений связан, во-первых, с ростом доверия пользователей к горячей линии как к эффективному инструменту борьбы с распространением противоправного контента. Во-вторых, на объем входящих сообщений повлияла информационная кампания в СМИ и на городских щитах, совместно проводимая фондом «Дружественный Рунет» и Управлением «К» МВД России.

По-прежнему весьма велика доля информативных сообщений, то есть содержащих ссылки на контент с признаками детской порнографии. Нужно отметить, что в 2010 году произошел рост доли таких сообщений во входящей массе. Так, если в 2009 году доля сообщений со ссылками на детскую порнографию составляла 40%, то в 2010 году это значение увеличилось до 52%.

Одной из важнейших тенденций, выявленных при анализе содержательных сообщений, является рост использования популярных социальных сервисов — файл-хостингов, фото- и видеохостингов, социальных сетей — для хранения детской порнографии и привлечения к ней пользователей. По данным 2010 года основными объектами противоправного использования стали фото- и видеохостинги, в эту категорию попали 62% рекламных (т.е. с бесплатным доступом к контенту) доменов с детской порнографией.

Всего по информации, присланной от пользователей, в России были выявлены 106 хостинговых площадок, на которых публиковалась детская порнография (для сравнения в 2009 году — 109). Российским владельцам сетей были направлены извещения о 9321 ресурсе. Как и в 2009 году, лидером по количеству сообщений стали ресурсы «Вконтакте»: на них пришлось около 30% всех содержательных сообщений. По состоянию на 1 января 2011 года более чем в 99% случаях контент с детской порнографией был удален, либо сайты полностью заблокированы.

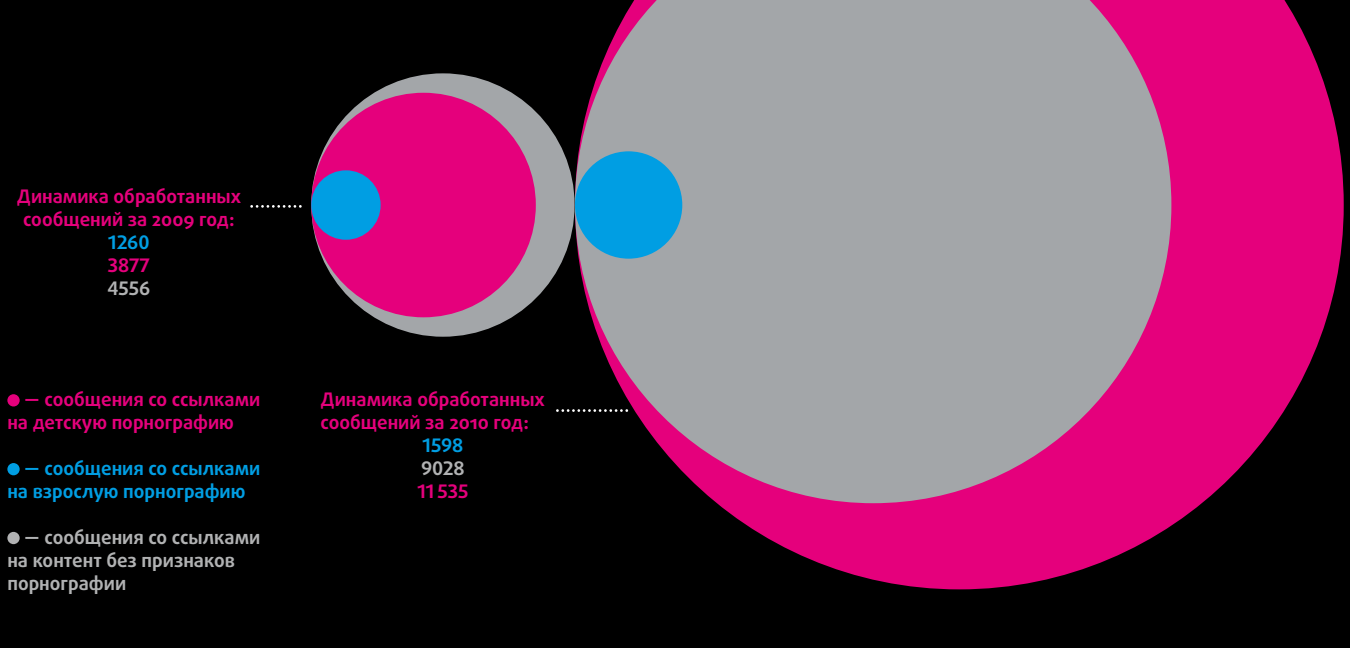
Приведенные цифры позволяют утверждать, что российская интернет-индустрия самым серьезным образом относится к проблеме распространения детской порнографии, в России сформированы и работают инструменты саморегулирования отрасли в рамках противодействия распространению противоправного контента в Сети. Однако пока не достигнут перелом ситуации. По-прежнему ведущие социальные сети и сервисы Рунета заражены детской порнографией.

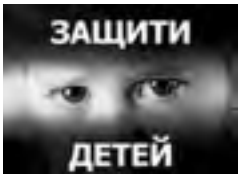
Распределение рекламных доменов с детской порнографией по специализации сайтов (фрагмент), %

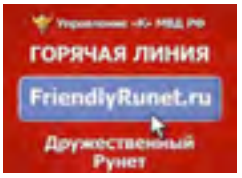
62	Фото-, видеохостинг
15	Доска объявлений (новостей)
11	Форум, чат, социальная сеть
9	Файл-хостинг

Источники сообщений о детской порнографии, %

67	Горячие линии
24	Граждане
5	Государственные ведомства
4	Коммерческие организации







Горячая линия работает в связке с Управлением «К» МВД России и взаимодействует с ведущими представителями отечественной интернет-индустрии

Топ-10 компаний, проявивших наибольшую активность в удалении детской порнографии, и количество исполненных ими сообщений

Vkontakte	3332
Ihome-net	2414
Совинтел	598
Radikal.ru	530
Агава	379
Juno.ru	317
Bashrtcomm-net	255
Яндекс	240
Rtcomm-colocation	224
Мастерхост	214

При поддержке Координационного центра домена RU российские регистраторы доменов также участвуют в работе по блокированию доступа к сайтам с детской порнографией. В течение 2010 года регистраторы сняли с делегирования 29 доменов с детской порнографией.

Кроме того, фонд «Дружественный Рунет» совместно с одним из ведущих регистраторов Рунета — компанией RU-CENTER — приступил к формированию дополнительного стоп-листа доменных имен из доменной зоны .РФ с целью исключения использования этой доменной зоны в аморальных и противоправных целях. В стоп-листе уже находятся десятки доменных имен с названиями, которые могут быть использованы распространителями детской порнографии. Для исключения возможности их регистрации потенциальными злоумышленниками эти доменные имена были зарегистрированы на фонд «Дружественный Рунет».

В течение 2010 года за рубеж, в том числе на горячие линии, входящие в ассоциацию INHOPE, были отправлены сообщения о 1695 ресурсах с детской порнографией. Больше всего сообщений было направлено в США. Из всего заявленного объема прекратил работу 491 ресурс. Таким образом, доля закрытия составила 29%. Особенно оперативно реагировали коллеги из Великобритании. На момент составления отчета они отработали 114 сообщений из 122 присланных. Для повышения эффективности международного взаимодействия фонд «Дружественный Рунет» постоянно контактирует со своими иностранными партнерами, что привело к отдельным улучшениям. Однако по-прежнему национальные нормы и правоприменительная практика других стран существенно затрудняют работу по противодействию распространению противоправного интернет-контента. Для ускорения работы по удалению детской порнографии из Сети с осени 2010 года горячая линия фонда начала устанавливать прямые отношения с компаниями украинской интернет-индустрии. Как результат, на момент составления отчета партнеры из Украины успешно отработали 91 сообщение из 98 присланных.

Как уже отмечалось, фонд «Дружественный Рунет» занимается научно-исследовательской деятельностью. В частности, в 2010 году было проведено исследование работы российских хостинг-провайдеров с сообщениями о противоправном контенте. Одной из целей исследования стало уточнение значимости вклада горячей линии в борьбу с детской порнографией в сети Интернет.

В ходе исследования было опрошено 11 организаций, по экспертным оценкам контролирующих примерно 50% российского рынка хостинга. Среди прочих в опросе участвовал и RU-CENTER. Участникам задавались вопросы о количестве и источниках сообщений о потенциально противоправном контенте.

Если проанализировать информацию об источниках сообщений о детской порнографии, то на горячие линии как источник приходится 67% сообщений.

Итак, основываясь на всех представленных данных, можно утверждать, что комплексная система противодействия детской порнографии, запущенная с участием фонда «Дружественный Рунет», основанная на общественно-государственном партнерстве и широком вовлечении в работу компаний интернет-индустрии, стала заметным и необходимым элементом борьбы с противоправным контентом в российском сегменте Глобальной сети.

44

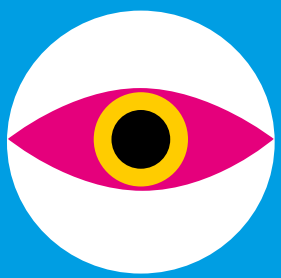
Вскоре логичной заменой генеральной темы для массовой интернет-общественности(темы безопасности) станет «идентификация» в Глобальной сети

39

Вопрос обеспечения достоверности и актуальности передаваемых и хранимых персональных данных остается одним из самых сложных

36

46



Кто? Где? Когда?

Современный Интернет связан с понятием «идентификация». А с ним — вопрос защиты персональных данных. Но без пользователя — все это было бы бессмысленным.

Кто все эти люди? Ответ на этот вопрос, заданный в разных вариантах, часто очень важен. Особенно в применении к Интернету. Конкретная реализация вопроса зависит от контекста. Например, рекламные агентства, продвигающие тот или иной товар в Сети, желают знать как можно больше о тех пользователях, которым показывают рекламу. Поисковые системы, все больше приспосабливаясь к потребностям и привычкам каждого пользователя, должны как-то этих пользователей узнавать, отличать их друг от друга. Все это задачи идентификации участников Сети.

Неразрывно связан с идентификацией пользователей вопрос защиты их персональных данных. Ведь, как известно, далеко не каждому пользователю Интернета нравится, когда его узнают рекламные сети.

С пользовательской стороны идентификация становится не менее важной задачей. Посудите сами: обычным пользователям Сети важно понимать, что они в настоящий момент работают именно с тем веб-сайтом, с которым планировали. Очень актуально для сайтов банков: самая популярная беда современного Интернета — фишинг — обязана своим существованием отсутствию механизмов уверенной идентификации сайтов пользователем. Да, задача определения достоверности веб-сайта в существенной части полагается на механизмы идентификации: сайт должен соответствовать некоторым эталонам, а проверка соответствия как раз относится к области идентификации.

Идентификация веб-приложений. Идентификация администраторов доменов. Областей, в которых идентификация важна, — много, и среди них — одни из самых быстро развивающихся направлений интернет-технологий. Потому что крепнет социальная составляющая информационных сервисов и требуется наконец автоматизировать ответ на вопрос: «Кто все эти люди?» Именно поэтому идентификация и стала темой очередного номера «Доменных имен».

«...У каждого есть право на конфиденциальность...»

Российский «Закон о персональных данных» готовился с 2006 года, вводился поэтапно, пережил несколько редакций... О ситуации вокруг него — в интервью с Александром Пановым*.

Как вы оцениваете актуальность действующей редакции закона о персональных данных?
По сути, закон актуален в том виде, в котором представлен сейчас. Подзаконные акты постоянно совершенствуются, и в них вводятся поправки. Однако есть один существенный момент, который потенциально способен затормозить его внедрение и существенно усложнить исполнение. Это требование подтвердить субъектом согласие на обработку своих персональных данных обязательно в письменной форме. С момента принятия закона технологии электронного документооборота постоянно развивались, и существующие на сегодняшний день уже позволяют отказаться от работы с бумажными документами — в частности, такие как технологии электронной цифровой подписи. В том случае если будет разрешено их использование, исполнять требования закона о персональных данных станет существенно проще.

Известно, что требования к операторам персональных данных очень разнообразны (существуют несколько сертифицирующих организаций — ФСТЭК, Минсвязи, ФСБ и пр.). Как это разнообразие влияет на деятельность регистраторов доменов и хостинг-провайдеров?
К сожалению, такой схеме получения всех необходимых разрешительных документов для обработки персональных данных сложно придумать какую-либо альтернативу просто потому, что каждая из сертифицирующих организаций занимается своей стороной вопроса. Федеральная служба безопасности занимается криптографией и защитой государственных тайн, вопросами безопасности информации при трансграничной передаче. ФСТЭК определяет правила того, как именно должны охраняться персональные данные, дает им определение и классифицирует их по категориям. Министерство связи задействовано здесь постольку, поскольку закон о связи превращает всех операторов связи в операторов персональных данных.

Есть мнение, что неукоснительное следование нормам закона о персональных данных вытеснит мелкие компании с рынка...
Требования к операторам очень сильно разнятся, и зависят они от категории персональных данных, с которыми работают. В соответствии с ФЗ 153 категория персональных данных, в свою очередь, определяется не только типом хранимой информации, но и количеством субъектов, которые доверили ее оператору. Чем меньше клиентов, тем ниже категория и тем менее строги требования к оператору. Соответственно, мелким компаниям не придется радикально перестраивать свою инфраструктуру, а значит, существенного передела рынка можно не опасаться.

Наибольшие трудности здесь испытывают, как ни странно, именно крупные операторы, для которых работа с персональными данными напрямую связана с основным видом деятельности (например, регистрацией доменных имен). Как правило, стоимость предоставляемых услуг невелика — соответственно, компании для успешного существования нужен большой оборот. Это автоматически влечет за собой повышение категории персональных данных и требует дополнительных технических и организационных мер по их защите.

Что делает Координационный центр национального домена сети Интернет для того, чтобы деятельность аккредитованных регистраторов была приведена в соответствие требованиям закона о ПДн?
Координационный центр рассматривает различные варианты работы над собственной инфраструктурой и над требованиями, предъявляемыми к регистраторам, однако о полном завершении этих работ говорить пока рано. Основные вопросы, которые сейчас стоят перед КЦ: какие именно данные и в каком виде передаются в реестр, и вообще передаются ли? И второй вопрос: каким образом защищать эти данные при передаче через публичные сети, в частности Интернет? Важно определить, будет ли что-то делаться для создания условий тем регистраторам, которые хотят передать права по обработке персональных данных самому КЦ, и если нет — будет ли КЦ предпринимать какие-то шаги, чтобы помочь этим регистраторам самостоятельно перестроить свою инфраструктуру. Как член совета КЦ могу отметить, что в настоящее время Координационный центр активно занимается приведением собственной инфраструктуры в соответствие с требованиями закона. На сегодняшний день им получены все необходимые разрешительные документы, касающиеся хранения и обработки персональных данных. Сейчас идет работа над передачей

Паспортизация в домене RU вывела разбирательства по ресурсам с противоправным контентом из-под юрисдикции регистратора и перевела их в судебную плоскость

* Александр Панов, управляющий партнер Hosting Community. Свою деятельность в телекоммуникационной отрасли начал в 1993 году. С 1995 года, работая в ООО «Гарант-Парк-Телеком», прошел путь от системного инженера до генерального директора

информации и получением ее от сторонних организаций — в частности, регистраторов.

Приходим ли мы обратно к анонимности в результате возможного закрытия большей части контактных данных?
Владельцы доменов не становятся вновь анонимными, просто потому что у них есть договорные отношения с регистратором доменных имен или его партнером. Персональные данные становятся скрытыми только из сервисов типа Whois. Однако по большому счету это ничего не изменит — регистраторы и раньше могли скрывать данные пользователя по его просьбе. Хорошо это или плохо — достаточно неоднозначный вопрос. Мы считаем, что у каждого человека есть право на конфиденциальность, и, предоставляя услугу сокрытия персональных данных, мы даем ему выбор: поступать так или нет. Кроме того, сокрытие, например, адреса электронной почты затруднит работу распространителей спама.

Как вы считаете, возможны ли дополнительные конфликты при трансграничной передаче данных (высказывается мнение, что различие в подходах к охране ПДн может привести к конфликтным ситуациям между российскими и зарубежными компаниями)?
Для того чтобы избежать подобных конфликтов, необходимо, чтобы было единое понимание принципов обеспечения сохранности данных при передаче и требований, предъявляемых к операторам связи. В настоящее время действует конвенция Совета Европы об охране персональных данных. Она выдвигает очень похожие требования к операторам связи, однако главное отличие в том, что там допускается предоставление пользователем согласия на обработку персональных

Разрешение использовать технологии электронной цифровой подписи в документообороте упростит исполнение требования закона о персональных данных

данных в любой оговоренной с пользователем форме. В США вообще нет понятия «охрана персональных данных» и отсутствует соответствующее законодательство. Все обязательства, накладываемые на оператора, прописываются в договоре с пользователем.

Однако конфликты действительно возможны, и наиболее показательной здесь является ситуация с российскими регистраторами, аккредитованными ICANN. ICANN требует передачи персональных данных пользователей сторонним компаниям — в частности, компании Iron Mountain, расположенной на территории США. Такая передача недопустима с точки зрения российского законодательства. В то же время невыполнение требований ICANN приведет к нарушению договорных обязательств с этой организацией.

Должны ли социальные сети (типа Facebook) менять свои подходы по обработке ПДн, предоставляемых российскими пользователями? И что можно в этом ключе сказать о российских соцсетях?
Особенность работы интернет-сервисов заключается в том, что любой ресурс должен соответствовать требованиям законодательства страны, на территории которой он зарегистрирован. Благодаря этому закон о персональных данных никак не отразится на работе иностранных сервисов, таких как Facebook, предоставляющих услуги гражданам России.

Что же касается российских социальных сетей, то тут необходимо учитывать несколько моментов. Во-первых, пользователь предоставляет информацию о себе добровольно, а значит, компания имеет право ее принимать. Кроме того, взаимоотношения социального сервиса и пользователя не регулируются договором. (По российскому законодательству он считается действительным или в том случае, если подписан в бумажном виде, или если произведена оплата, факт которой и является акцептом.) В этом случае в соответствии с законом о персональных данных такие ресурсы должны защищать предоставленную им информацию только от несанкционированного доступа. Необходимо также отметить, что социальные сети собирают обезличенную информацию, которая не позволяет однозначно идентифицировать пользователя (например, отсутствуют паспортные данные). Никто не мешает пользователю поместить другую фотографию и представиться другим именем. Соответственно, хранящаяся там информация не может быть в полной мере признана персональными данными.

Как влияет закон на системы контекстной рекламы, которые также могут собирать ПДн и использовать их для рекламного таргетинга?
Данные о пользователе, которые собирают системы контекстной рекламы, не являются персональными. По закону «О связи» информация об IP-адресе, с которого сделан тот или иной запрос, не является конфиденциальной, и по умолчанию все сервисы типа Whois показывают принадлежность адреса к маршрутизированному блоку адресов (то есть, по сути, принадлежность тому или иному провайдеру), но не дальше. Поэтому работе таких сетей закон о персональных данных не помешает.

Данный закон усложнит архитектуру информационных систем регистраторов доменов, сколько это стоит?

ФОТО: СЕРГЕЙ МЕЛИХОВ

Первое, с чего начинается построение информационной архитектуры оператора персональных данных, — это разработка модели угроз. Именно на основе этого документа определяются все те слабые места, над которыми в дальнейшем нужно работать, и список мер, которые необходимо предпринять.

Назвать конкретную цифру здесь сложно, потому что список изменений зависит от огромного количества факторов: организационной структуры, имеющихся технических резервов, квалификации сотрудников, метода обработки данных, распределения информационных потоков и т.д.

Как вы оцениваете итоги паспортизации в домене RU, которая проводилась в 2009–2010 годах?
Паспортизация изначально задумывалась для того, чтобы повысить скорость реакции провайдеров и правоохранительных органов на контент, размещаемый в Интернете. Она позволила вывести разбирательства по ресурсам с информацией, имеющей признаки противоправной, из-под юрисдикции регистратора и перевести их в судебную плоскость. Наличие скана паспорта позволяет, например, определить, является ли документ поддельным, и в этом случае ресурс подлежит закрытию как анонимный. Таким образом удалось закрыть несколько тысяч сайтов с противоправным контентом без ущерба для репутации регистраторов и хостинг-провайдеров.

Какие данные о владельцах доменов в идеальном случае должен собирать регистратор и как добиться того, чтобы эти данные были достоверные и актуальные?
Так как доменное имя по российскому законодательству является объектом гражданского права, владение которым определяется договором, то для его заключения требуются идентификационные данные, однозначно определяющие участников. На сегодняшний день для заключения договора подходят двенадцать видов документов, которые содержат достаточное количество сведений о предоставившем их человеке.

Некоторые признанные эксперты (Е.Касперский) говорят, что в Интернет нужно «пускать только по паспорту». Как вам такая инициатива?
Такое требование крайне трудно реализовать на практике. К сожалению, технически невозможно оснастить все возможные пункты доступа в Интернет техническими средствами проверки подлинности документов и укомплектовать персоналом, имеющим соответствующую подготовку. Такая система все равно не сможет гарантировать то, что злоумышленники не попадут в Сеть и не останутся потом безнаказанными.

На наш взгляд, проще и эффективнее было бы разработать систему быстрого удаления ресурса с противоправным контентом, информация о котором поступила бы по какому-либо каналу.

Не кажется ли вам, что государственная почта в .РФ, где электронный ящик должен быть приравнен к идентификатору в Сети, тоже своеобразная модель обработки ПДн?
Идея государственной почты, выступающей в качестве однозначного идентификатора, — очень хороша сама по себе. Однако способ реализации этой идеи оставляет желать лучшего. Внутри этого проекта не до конца проработаны средства защиты от подделки, существующие механизмы не гарантируют однозначного определения отправителя.

Кроме того, не до конца проработаны законодательные вопросы, касающиеся привязки почтового адреса к различным сущностям (как известно, электронная цифровая подпись может быть привязана только к физическому лицу и никак не будет отражать, например, его должность и полномочия). Естественно, такая почта будет в какой-то степени являться моделью обработки персональных данных, поскольку должна будет гарантировать их защиту, достоверность и неприкосновенность, однако ее нынешняя реализация далека от совершенства.

Поделитесь, пожалуйста, своим мнением о перспективах внедрения ЭЦП.
Закон «Об электронной цифровой подписи» действительно существует, и, на наш взгляд, у него хорошие перспективы в России. Однако для того чтобы он начал работать в полную силу, требуется проделать большую работу. Прежде всего надо устранить некоторые противоречия. Например, закон об ЭЦП говорит о том, что электронная цифровая подпись является полноправным аналогом собственноручной. В то же время закон «О связи» в некоторых местах прямо говорит, что допускается только бумажная форма документов.

Уже есть несколько прецедентов судебных разбирательств с сайтами, предоставляющими сервисы по построению генеалогического древа для пользователей, их пытались закрыть на основании закона о ПДн. Как вы считаете, будет ли эта тема развиваться?
В настоящее время их работа не всегда легитимна, просто потому что такой сервис должен опираться на какую-то базу данных. Как правило, это архивные базы различных ведомств. По российскому законодательству работа с персональными данными человека может вестись только спустя 50 лет после его смерти (если это не оговорено особо). Таким образом, неправомерность их работы заключается только в том, что они, вероятно, получают несанкционированный доступ к базам данных.

Как вы оцениваете полноту разработанной к закону государственной технической документации, регламентирующей устройство систем обработки и защиты ПДн, а также сертификацию операторов ПДн?
Техническая документация достаточно полно соответствует современному уровню развития техники. Однако не совсем обоснованным представляется требование использования только российских криптографических средств. И другие средства не попадают под определение средств защиты информации, а значит, не могут быть использованы при работе с персональными данными.

Закон предусматривает сложную, довольно жесткую (вплоть до письменной формы) схему получения согласия на обработку ПДн. Как это отражается на бизнесе, работающем с большим числом клиентов через Интернет?
Такое требование крайне сложно реализовать на практике, так как большие операторы столкнутся с целым рядом технических и организационных проблем. Многие бизнес-процессы станут просто невозможными, и это может спровоцировать людей на поиск обходных путей. По нашему мнению, это условие нуждается в доработке — его необходимо привести в соответствие с реалиями нашего рынка.

Каковы перспективы защиты ПДн в России?
Такие же, как и в любой другой стране. Мы уверены, что все заявленные цели достижимы и все трудности могут быть преодолены в ближайшей перспективе. Полноценное функционирование закона о персональных данных позволит вывести на новый уровень культуру электронной торговли и сделать очередной шаг к построению полноценного безопасного информационного общества.

Александр Венедюхин,
главный редактор «ДИ»

Нашествие виртуалов, или Социализация роботов

Влияние социальных веб-сервисов на офлайн за прошлый год выросло. Теперь за новым инструментом влияния пришли серьезные игроки.

Всякая достаточно продвинутая коммуникационная технология однажды становится востребованным социальным инструментом. Так, Интернет в современном мире — по крайней мере, в развитой его части — стал самым мощным транспортом для социальных взаимодействий.

В соответствии с базовыми принципами эволюции социальная функция Интернета начала обрастать новыми инструментальными дополнениями.

Надо заметить, что плотно увязанное в сознании современной массовой аудитории с Интернетом понятие «социальная сеть» в социологии известно с 50-х годов XX века. То есть Интернет в те годы только планировался и даже самые прозорливые из его создателей не могли предположить, во что это выльется. В социологии под социальной сетью понимают структуру из множества связанных различным образом людей (или людских групп), между которыми происходит обмен различными ресурсами. Ресурсы здесь не обязательно материальные. Для людских сообществ ресурсами также являются информация или эмоциональные состояния. Итак, это старые, офлайновые социальные сети. Они существуют в современной реальности. Многие из сетей не просто существуют, но эффективно работают. А небольшая часть обладает сокрушительной силой и ткет полотно судьбы этого мира.

Взглянем на офлайновые сети чуть подробнее. Такая социальная сеть — это неформальное одноранговое объединение, основанное на добровольной кооперации его членов (иногда кооперация не является строго добровольной в привычном понимании этого слова, а связана с давней традицией или складывается из общественного устройства). Одноранговость означает, что внутри социальной сети нет жесткой иерархии: ее участники просто согласились следовать некоторым правилам, соблюдать определенные обычаи. Социальная сеть предоставляет определенные преимущества своим членам: возможность получения новой информации, поддержку, в том числе связанную с общественным статусом, и так далее. Примеры офлайновых социальных сетей: студенческие сообщества; революционно настроенные граждане, создавшие тайный совет; политические общества; сообщества коллекционеров и футбольных фанатов.

В понимании современного Интернета социальная сеть — это иной феномен. Как правило, в Интернете под социальной сетью подразумевают веб-сервис, позволяющий зарегистрированным пользователям заводить собственные страницы-профили (где сообщается персональная информация), указывать социальные связи (механизм друзей) и обмениваться «ресурсами», информацией внутри сети (личные сообщения с различным уровнем доступа, механизмы подарков, поздравлений и т. п.).

Мощь и транснациональность социальной функции новых коммуникационных механизмов подтвердила череда африканских революций — Интернет обретает новый статус

При ближайшем рассмотрении интернетовские социальные сети — это особый инструмент, служащий для гибкого проецирования офлайновых социальных сетей в виртуальное пространство. Интернет усиливает классические сети, существовавшие в обществе раньше, делает эти сети сильнее, гибче, устойчивее.

Например, привычная всем современным интернет-пользователям простая функция «рекомендации связей» резко расширяет возможности роста социальной сети в офлайне. Возможно, два сотрудника компании «Имярек» никогда не встречались, так как работают в разных подразделениях. Однако инструмент автоматической рекомендации знакомых, доступный в социальной сети, сведет их через Интернет: «Ух ты! Работаем в одной компании и оба увлекаемся ядерной физикой!» Естественно, механизм автоматизированных рекомендаций френдов

(от англ. friend — «друг») — не единственное мощное онлайн-оружие, развивающее социальные сети с помощью интернет-механизмов.

Существует интересная структурная особенность. Предоставление только что описанных автоматизированных механизмов пользователям возможно лишь потому, что у социальной сети в Интернете появляется иерархия. И техническая, и административная. Техническая иерархия состоит в том, что для хранения баз данных с информацией об участниках сети, об их действиях и сообщениях используются «центральные серверы», полного доступа к которым у всех участников социальной сети нет по вполне понятным причинам.

Другой важной особенностью сервисов социальных сетей в Интернете является наличие в них администрации и модераторов, которые уже самим своим существованием вводят строгую иерархию: администрация, модераторы могут удалять какие-то сообщения участников сети и блокировать (удалять) профили участников целиком (исключая члена из социальной сети весьма радикальным образом). То есть из-за наличия иерархии социальные веб-сервисы в Интернете — это не социальные сети в классическом понимании, а лишь инструмент.

Технические механизмы Интернета позволяют в онлайне вводить правила контроля и методы ограничения обмена информацией, потенциальная неотвратимость которых не снилась офлайновыми мероприятиям. Действительно, если владельцы серверов социальной сети решат запретить данному конкретному пользовательскому профилю (аккаунту) общаться с остальными, то они сделают это одной кнопкой с эффективностью 100% — и никакая тайнопись не поможет. Учитывайте, что речь не об офлайновом прообразе профиля — он-то как раз может завести себе нового виртуала, — а о самом этом профиле, существующем полностью на подконтрольном владельцам серверов пространстве.

В начале статьи в качестве примера социальной сети упоминаются революционно настроенные граждане. Интернет увеличивает силу такой сети. Мощь и транснациональность социальной функции новых коммуникационных механизмов подтвердила череда африканских революций. Едва ли не в каждой из них Интернет и социальные сети играли одну из ключевых ролей в медийном пространстве (про события в Египте читайте в разделе «Соседи» этого номера на стр. 70).

Вспомним про жесткую техническую иерархию. У нее есть и второй аспект: да, профили могут удалять только владельцы серверов, но строить виртуалов, запускать в Facebook ботов — это под силу и группам энтузиастов, обладающих некоторой технической квалификацией. Здесь есть виртуалы — то есть поддельные персоны, за которыми скрываются живые люди, и боты — то есть поддельные персоны, за которыми стоят специальные «говорящие» программы. Такова реальность современных социальных сетей. Если разбирать только публичную историю, то окажется, что впервые эти технологии применили специалисты по продвижению товаров и услуг. Если боты здесь использовались для рассылки банального спама, то виртуалы писали в социальных сетях восторженные отзывы о новом товаре под продвигаемым брендом. Впрочем, не только восторженные, но и резкие критические. Только для того, чтобы другие виртуалы получили возможность включиться в дискуссию и при помощи весомых доказательств успешно переубедить виртуала-критика. «Да, я был неправ! Посыпаю голову пеплом! Это отличный утюг! » — признавал в итоге свою ошибку зачинщик горячего спора о товаре. Общественное мнение сформировано: покупатели любят делать выводы из дискуссий, прочитанных на просторах интернетовских социальных сетей. Агентства по продвижению в социальных сетях Интернета не только давно существуют, но и открыто бравируют развитыми технологиями использования ботов и виртуалов.

Весной 2011 года прессу взбудоражило сообщение об использовании ботов и виртуалов в социальных сетях военным ведомством США (являющимся технологическим отцом Интернета!). Пентагоновские боты и виртуальные персоны, как сообщалось в СМИ, послужат чем-то вроде лассо, которое позволит оседлать мощь социальных сетей в формировании общественного мнения. Эта новость породила волну обсуждений: кто и как станет использовать новый механизм развития социальных сетей теперь, когда о своем интересе открыто говорят из Пентагона?

Впрочем, довольно странно полагать, будто бы государственная пропагандистская машина США озаботилась использованием виртуалов в социальных сетях позже, чем этой технологией хорошо овладели обычные рекламные агентства. Решение с поддельными аккаунтами давно известно, о нем знали еще до появления Facebook. Скорее всего, специальные государственные службы уже пошли дальше.

Реальность

Борьба за живучесть

Благодаря своим структурным особенностям добротно построенные социальные сети очень живучи и практически неуязвимы для попыток их разрушения с помощью изоляции отдельных узлов или уничтожения центров. Интересно, что при отсутствии жесткой иерархии управляющие центры в социальных сетях могут формироваться и оказывать влияние на жизнь самой сети. Но при возникновении новых обстоятельств сформированные центры способны растворяться, а при необходимости — например, если часть сети утрачена — сетевое сообщество создает новые центры. Заметьте, что возникновение центра влияния вовсе не требует введения иерархии.

Исключительное преимущество социальных сетей в Интернете по сравнению с офлайном состоит в том, что они предоставляют автоматизированные механизмы «рекомендации связей»

Так никого уже не удивить использованием интернетовских социальных сетей для выявления связей между людьми, существующих в реальном мире, для сбора персональной информации об участниках этих сетей. Методы анализа описаны многократно, применяются и для розыска должников, и даже для розыска компьютерных мошенников. Но это аналитика первого порядка. Готовить ее относительно несложно. Для многих специальных коллективов — это просто рутина. Гораздо интереснее, важнее технологии второго порядка. О которых пока мало пишут. О чем идет речь? О ситуации, когда с помощью автоматизированных механизмов в социальных сетях создается такое информационное поле, что простые аналитики, честно и качественно работающие на первом уровне, вполне достоверно извлекают как раз ту информацию, которую посеял специалист, овладевший инструментами второго порядка. И для реализации такого механизма необходимы хорошо подготовленные боты, а также развитая сеть виртуалов.

Возможно ли сейчас или в ближайшей перспективе создать ботов, которые смогли бы более-менее самостоятельно общаться в социальных сетях, не рискуя быть разоблаченными? На первый взгляд, задача сложная. Но это только потому, что с ходу хочется применить офлайновый опыт: действительно, создать кибернетического двойника-робота даже для воображаемого человека пока что и близко не удавалось.

Но хитрость в том, что обычно в социальных сетях в Интернете массовые пользователи не предъявляют особенных требований к качеству письменных высказываний других пользователей. И чрезвычайно редко встретишь параноика, который специально проверяет всех френдов на предмет того, а не бот ли тут скрывается.

Заметьте, что даже некоторые программы-зловреды, распространяющиеся через, например, ICQ, успешно обманывают массового пользователя, прикидываясь его знакомым. «А это не вирус ты мне отправил? » — «Да не, ты что, это не вирус, просто прикольный ролик — открой!» Более того, в случае построения групп влияния в социальных сетях, речь должна идти об автоматизированных ботах, то есть о таких ботах, которые работают не полностью автоматически, а под контролем оператора-человека. Оператор не следит, конечно, за диалогом детально, но он, скажем, переключает ветки диалогов, подстраивает некоторые параметры «интеллекта» бота, все это — при необходимости. Что получается? Группа специалистов — среди них психологи, лингвисты, аналитики — работает с использованием программных инструментов, которые собирают поведенческую статистику целевых групп реальных пользователей в социальной сети. То есть, с одной стороны, здесь есть инструменты сбора информации и автоматического извлечения из нее нужных оценочных показателей. Вспомните, что уже давно созданы технологии автоматизированного, то есть с участием специалиста-человека, анализа текстов в Сети, с раскрашиванием по эмоциональной составляющей: положительный отзыв, недовольный клиент и так далее. Аналогичные системы применялись и применяются для анализа спама, для анализа корпоративной почты в системах информационной безопасности.

С другой стороны — работает система управления ботами. Это должен быть некоторый инструмент, который позволяет настраивать общие сценарии для групп ботов, задавая какие-то целевые характеристики. Например, активные отзывы о тех или иных онлайн-событиях, реакция на негативные сообщения и так далее. Результаты работы отслеживаются с помощью системы аналитики из предыдущего абзаца. Тут же используются виртуальные персоны, виртуалы, которые могут в критическом случае прийти на помощь запутавшемуся отряду ботов. Выступая от имени такого виртуала, группа психологов наверняка сможет разубедить «честного селянина», начавшего что-то подозревать, наткнувшись на группу роботов, орудующих в комментариях к его статусу в Facebook.

Кончено, администрация социальных сетей пытается вычислять ложные аккаунты (пусть это будут виртуалы, а не боты). Ведь тысячи таких аккаунтов используются для раскрутки страниц, товаров и так далее. Не в интересах владельцев социальной сети плотное заселение ее виртуальными персонажами, а тем более — ботами. Возможно, как раз администрация может вступать в особую переписку с подозрительными владельцами профилей и после теста Тьюринга выводить роботов из зала. Делается ли это на практике — не ясно. Может ли процесс чистки наблюдать рядовой пользователь? Не может. Естественно, вопрос, от чего защищать пользователей, а от чего не защищать, связан с политикой, которой придерживаются владельцы сети.

В обществе уже оценили возможности социальных сетей в разрезе реагирования на чрезвычайные обстоятельства. Именно с помощью интернет-механизмов, но силами выстроенных в офлайне социальных сетей из многих добровольцев были сделаны, например, общественные проекты, предоставлявшие и собиравшие информацию о лесных пожарах в Московской области, в России

Подписывающиеся на социальный веб-сервис пользователи не имеют возможности определять, кто и как будет модерировать данный сервис

Обсуждая бум социальных сервисов в Интернете, многие предрекают скорое схлопывание пузыря. Действительно, чисто коммерческая модель выживания социальных сетей — довольно мутная. Но, с другой стороны, вряд ли нашествие ботов убьет социальные сети в Интернете. А вот то, что именно конфликт между виртуальным населением социальных сетей и их возросшим офлайновым влиянием определит направление развития пузыря в ближайшие два года, — об этом можно говорить с уверенностью. Раскручивание описанных технологий влияния на общественное мнение ведет к одному важному изменению — к усилению механизмов идентификации пользователей, в том числе механизмов идентификации, доступных другим рядовым участникам сети.

РОЦИТ

ОБЩЕСТВЕННАЯ ПАЛАТА РОССИЙСКОЙ ФЕДЕРАЦИИ

СОПРОТИВЛЕНИЕ
правозащитное движение

ЦЕНТР БЕЗОПАСНОГО ИНТЕРНЕТА В РОССИИ

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ ЧАСТЬ

статьи, памятки, статистика, экспертное мнение

ГОРЯЧАЯ ЛИНИЯ

борьба с противоправным контентом

ЛИНИЯ ПОМОЩИ

советы и консультации

МОЛОДЕЖНАЯ ИНТЕРНЕТ-ПАЛАТА

сообщество молодежи за безопасный Интернет

ins@fe Член Европейской Сети Центров безопасного Интернета

A Member of INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES INHOPE Член международной Сети горячих линий

Специальные проекты:

НеДопусти — nedopusti.ru
против сексуальной эксплуатации детей

Хулиганам.Нет — huliganam.net
против киберунижения

Наркоманам.Нет — narkomanam.net
против пропаганды и распространения наркотиков

Моя безопасная Сеть — moya-set.ru
семейный конкурс по безопасности в Интернете

WWW.SAFERUNET.RU

Новые времена, новые интересы

Медийное пространство эволюционирует, изменяя конфигурацию центров конденсации внимания общественности, — в фокусе оказываются новые технологии. Популярная нынче тема безопасности — не исключение. Что ее ждет?

Скоро мы увидим результаты вторичной переработки медийного влияния темы безопасности: на популярных конференциях представители компаний начнут учить слушателей тому, как «можно заработать на обучении основам безопасности» (ну или чему-то в этом роде)

Безопасность во всех ее аспектах — одна из самых популярных тем публикаций, конференций, семинаров и книг. В том числе когда речь идет об Интернете. Технические аспекты безопасности занимают существенное место в массовом медийном поле, включающем в себя публикации СМИ, обсуждения в блогах, форумах. Редкая конференция по IT обходится без секции или ряда докладов по безопасности.

Более того, если говорить об Интернете, то большая часть важных технологических новинок последнего времени также напрямую связана с обеспечением безопасности. Например, самое значимое изменение в информационной инфраструктуре глобальной DNS, случившееся за четверть века, — внедрение технологии DNSSEC, затея, связанная с обеспечением безопасности. Конечно, развертывание DNSSEC — это уже не просто публикации в прессе. Но именно забота о безопасности пользователей Интернета находилась среди основных козырей, с помощью которых идея о необходимости DNSSEC продвигалась в массы.

Надо заметить, что безопасность не всегда была столь популярным, в смысле освещения в прессе и на конференциях, направлением. Естественно,о безопасности заботились и раньше. Но более тихо. Сейчас, так как речь идет о достаточно широкой аудитории, то и безопасность рассматривается в самом широком, словарном значении термина. Поэтому кто-то организует на конференциях секции по «защите веб-приложений», а кто-то занимается мерами по «контролю за неправовым контентом в Сети». И то и другое — это вопросы безопасности.

Проявления увлечения безопасностью в медийном пространстве разнообразны. Так, ши-

рота термина и популярность темы привели к тому, что в Интернете появилось много разных СМИ, освещающих вопросы безопасности на самых разных уровнях достоверности и технической компетенции. Появились разнообразнейшие регулярные семинары и круглые столы по безопасности, отдельные разделы в газетах и рубрики в телевизионных передачах. Не исключение и наш журнал «Доменные имена» — у нас соответствующий раздел называется «Под защитой», а темой осеннего выпуска 2009 года также была безопасность.

Тенденция налицо. Впрочем, медийное пространство развивается, а главные тренды меняются. Безопасность слишком важна для каждого, чтобы так просто уйти из перечня главных тем. И все же давайте попробуем заглянуть вперед и порассуждать о том, какая тема может прийти на смену теме безопасности в ближайшем будущем.

Очевидно, что это должно быть технологически богатое направление: потому что технологию может потеснить только технология. Логично предположить, что новый тренд вырастет из того или иного аспекта обеспечения безопасности — преемственность позволяет поддерживать эволюционное развитие. При ближайшем рассмотрении жизнеспособных вариантов замены не так много. Мы обнаружили только один.

Рискнем предположить, что логичной заменой генеральной темы для массовой сетевой общественности станет идентификация в Глобальной сети*. Идентификация опять будет рассматриваться в самом широком смысле: это и идентификация пользователей Интернета, и идентификация приложений (компьютерных программ, сервисов на разных сайтах и так далее), а равно — идентификация услуг/товаров/компаний.

Идентификация неразрывно связана с безопасностью. Точно так же с безопасностью связана и криптография, да и различные другие темы, от грузоперевозок (доставка взрывных устройств) до технологий обработки металлов (например, взлом сейфов). Но всеобъемлющая природа увлечения безопасностью никогда не мешала возникновению отдельных массовых тематических трендов: среди которых, скажем, увлечение шифрами, включающее и создание новых шифров, и взлом существующих.

У идентификации как термина «широкого назначения» намечается очень развитая проблематика. Давайте взглянем в первом приближении — очевидно, к области идентификации относятся такие медийно узнаваемые пучки технологий: «Интернет по паспорту», «персональные данные», «биометрический контроль», «кража личности», «обнаружение ботов, склоняющих рекламу», «обмен идентификаторами», «идентификация рисков». Естественно, список можно легко продолжить.

Задачи идентификации в самом широком смысле очень важны в современной Глобальной сети. Но их медийную значимость пока недооценивают

При этом задачи идентификации весьма важны в современном Интернете (как и в информационных технологиях вообще). Тему не нужно, что называется, притягивать за уши. А это означает, что налицо соответствие значимости предмета с потребностью «сменить тему» (вместо безопасности). Отличное продуктивное сочетание.

Не удивляйтесь, если скоро в программах крупных конференций появятся секции «по идентификации». Возможно, появятся даже отдельные специализированные конференции, ориентированные на широкую публику.

* С самой безопасностью от смены акцентов хуже не сделается; да и лучше — тоже

ИЛЛЮСТРАЦИЯ: АЛЕКСЕЙ СИМОНОВ

Персональные данные

Просто. Важно. И безумно привлекательно.

Используя Whois-сервис для поиска информации, пользователь соглашается с тем, что он будет использовать полученные данные только в законных целях; не станет рассылать спам по адресам электронной почты, факсу; не будет производить массовых выборок информации, превышающих разрешенные пределы. Запрещается использовать полученную информацию с целью ее дальнейшего распространения в коммерческих целях. Кроме того, есть технические ограничения на использование сервиса.

Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться сертифицированные в системе сертификации ФСБ России (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации) криптосредства.

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация...
(ФЗ от 27.07.2006 №152-ФЗ «О персональных данных»)

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться их конфиденциальность (за исключением обезличенных и общедоступных персональных данных).

(ФЗ от 27.07.2006 №152-ФЗ «О персональных данных»)

14 октября 2010 года, в день начала Всероссийской переписи населения-2010, в Интернете появился сайт — дублер официального сайта этого события. Лжересурс не только копирует содержание, но отчасти и домен. Если официальный сайт расположен по адресу perEpis-2010.ru, то дублер использует perIpis-2010.ru, то есть домен с опечаткой. По данному факту проводится проверка.

Закон о персональных данных затрагивает и интересы маркетологов. В частности проведение различных активностей, подразумевающих сбор персональных данных. К ним относится и выдача дисконтных карт (с предварительным заполнением анкеты). Теперь покупатель, которому заводят такую карту, также должен дать согласие на сбор и обработку своих персональных данных.

В январе 2011 года Роскомнадзор предпринял попытку закрыть известный сайт «Всероссийское генеалогическое древо» (www.vgd.ru), который уже 12 лет помогает россиянам изучать свою семейную историю. В Роскомнадзоре заявляли, что данное дело — часть общего процесса по - исполнению закона о персональных данных, в частности, права субъектов персональных данных на неприкосновенность частной жизни.

В итоге 2 февраля 2011 года Роскомнадзор и владелец интернет-портала vgd.ru заключили мировое соглашение. Учитывая устранение на «Всероссийском генеалогическом древе» обстоятельств, послуживших поводом для обращения в суд, Роскомнадзор отказывается от требований, выдвинутых в судебном иске. Владелец сайта берет на себя обязанность осуществлять деятельность в соответствии с законодательством о персональных данных.

В начале 2011 года Технический администратор национального домена Украины UA «Хостмастер» закрыл публичный доступ к информации о физических лицах, зарегистрировавших доменное имя, — так называемый Whois-сервис. Данная мера — необходимость для работы в соответствии с новым законом «О защите персональных данных», который запрещает передавать данные граждан третьим лицам без согласия пользователя.

Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе. Данное согласие может быть отозвано субъектом персональных данных. Однако предусматриваются случаи обязательного предоставления персональных данных — в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
(ФЗ от 27.07.2006 №152-ФЗ «О персональных данных»)

Сейчас для отображения в Whois-сервисе у клиента спрашивают ФИО, адрес, e-mail, телефон и, по желанию, номер факса. Зачастую злоумышленники используют Whois для сбора адресов электронной почты, чтобы потом рассылать спам или фальшивые письма от имени регистратора для перехвата контроля над доменом.

В 2009 году было зафиксировано наиболее частое появление в Рунете лжесайтов, имитирующих реальные веб-представительства российских банков. В мировой интернет-практике эту разновидность сетевого мошенничества называют фишингом. В целях противодействия распространению подобного негативного явления Банк России (www.cbr.ru) приступил к регулярному размещению на своем сайте в разделе «Информация по кредитным организациям» списка адресов/доменных имен официальных веб-ресурсов банков.

58

Обязанность преобразования многоязычных доменных имен в Punycode и обратно было решено возложить на клиентское программное обеспечение, такое как браузер

56

49

Число организаций, использующих IPv6 во внутренних сетях и для доступа в Интернет, возросло с 16 до 40%

60

59

©.com
♥.net
♫.org

RIPE по-итальянски

Сергей Горбунов,
главный специалист
департамента PR RU-CENTER

61-я конференция RIPE прошла в Риме с 15 по 19 ноября 2010 года. Началось мероприятие с самой актуальной в последние годы темы — процесса внедрения протокола IPv6. Напомним, он должен прийти на смену используемой сегодня адресной системе IPv4, ресурсы которой практически исчерпаны.

Кроме протокола IPv6 на конференции обсуждались и другие вопросы: роутинг, эффективное управление трафиком, развитие европейских Internet Exchange... На заседаниях рабочей группы, занимающейся развитием системы DNS, прозвучали доклады российских специалистов

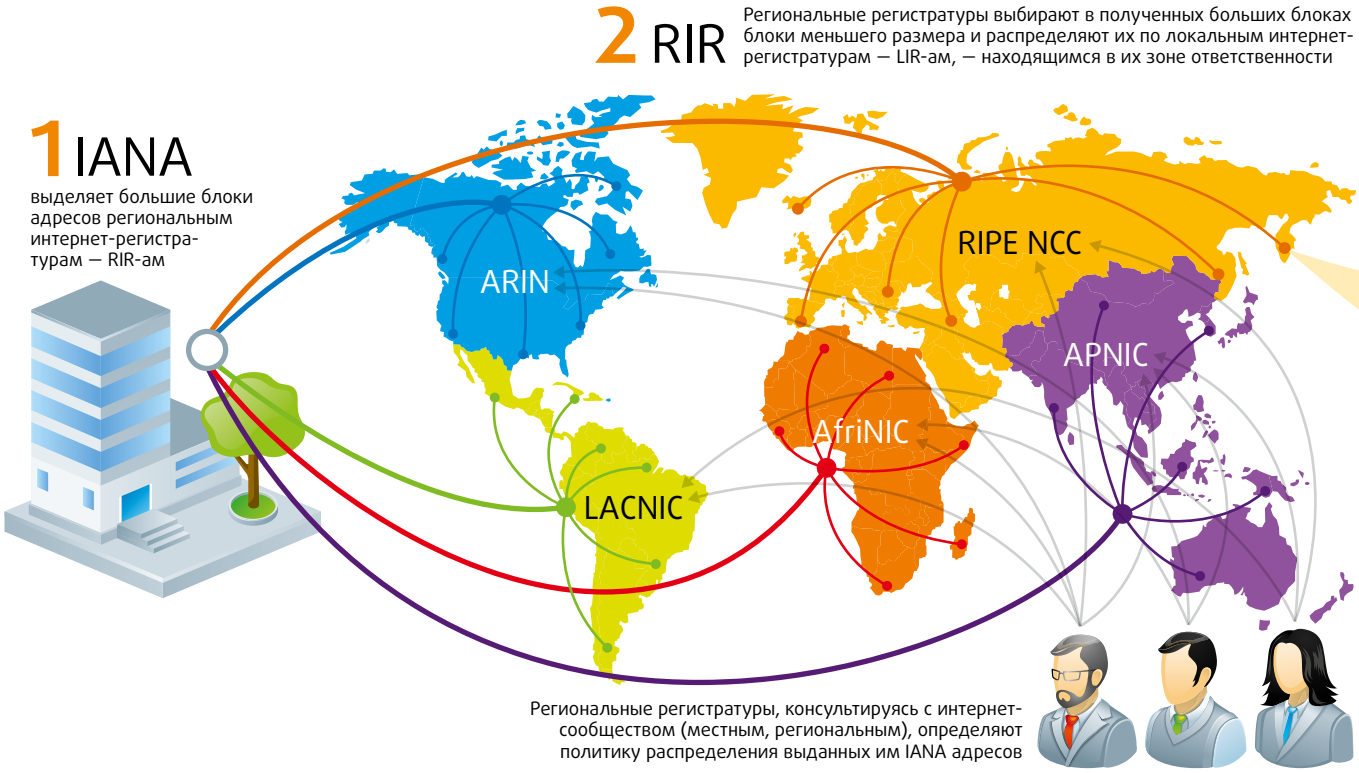
IPv6: ситуация сегодня

Вот только интернет-провайдеры не торопятся переходить к технологиям IPv6. Для них это попросту нецелесообразно: спрос на услуги на базе нового протокола слабый, информации по особенностям его внедрения недостаточно, оборудования с поддержкой IPv6 на рынке пока представлено мало, в то же время полноценный переход к использованию нового адресного пространства весьма затратен.

В итоге организация RIPE NCC и другие региональные интернет-регистратуры, отвечающие за распределение адресного пространства сети Интернет, вынуждены действовать методом кнута — в частности, ужесточать политику выделения последних блоков адресов протоколаI Pv4.

Постепенно к провайдерам приходит осознание неизбежности перехода к IPv6. На сегодняшний день самым популярным способом внедрения IPv6 пока что остается технология двойного стека, которая подразумевает способность устройства в зависимости от ситуации использовать IPv4- или IPv6-соединение.

Распределение IPv6-адресного пространства



На конференции RIPE 61 были представлены итоги опроса 700 европейских интернет-провайдеров. Исследование, в частности, показало, что двойной стек применяется в 94 случаях из 100.

Выбор в пользу двойного стека вполне объясним с точки зрения статистики. На сегодняшний день в сетях большинства провайдеров, принимавших участие в исследовании, доля клиентов, использующих IPv6, не превышает 1%. А по данным Google, только у 1,1% всех веб-сайтов есть адрес IPv6.

Даже в Европейском регионе, где новый протокол внедряется быстрее всего, 70% провайдеров до сих пор не получили ни одного блока адресов IPv6. В России эта цифра достигает 83%, это худший показателей среди всех европейских стран.

Ложка меда

Между тем о полном отсутствии прогресса во внедрении протокола говорить все же не приходится. По данным опроса, по сравнению с прошлым годом число провайдеров, которые не планируют продвигать IPv6 среди своих клиентов, сократилось с 43 до 9%. В то же время количество организаций, рассчитывающих получить адреса формата IPv6, возросло на 10%. Увеличилось и количество провайдеров, в сетях которых мало-мальски заметен IPv6-трафик. С 16 до 40% возросло число организаций, которые используют новый протокол во внутренних сетях и для доступа в Интернет.

IPv6 уже стабильно поддерживает большинство распространенных интернет-браузеров (Firefox, Internet Explorer, Safari). В адресном пространстве IPv6 способны работать и наиболее популярные веб-сервисы — Facebook и Google. Правда, поддержкой протокола пока не могут похвастать инстант-мессенджеры ICQ, AIM, MSN и приложение интернет-телефонии Skype, но очевидно, что это дело времени.

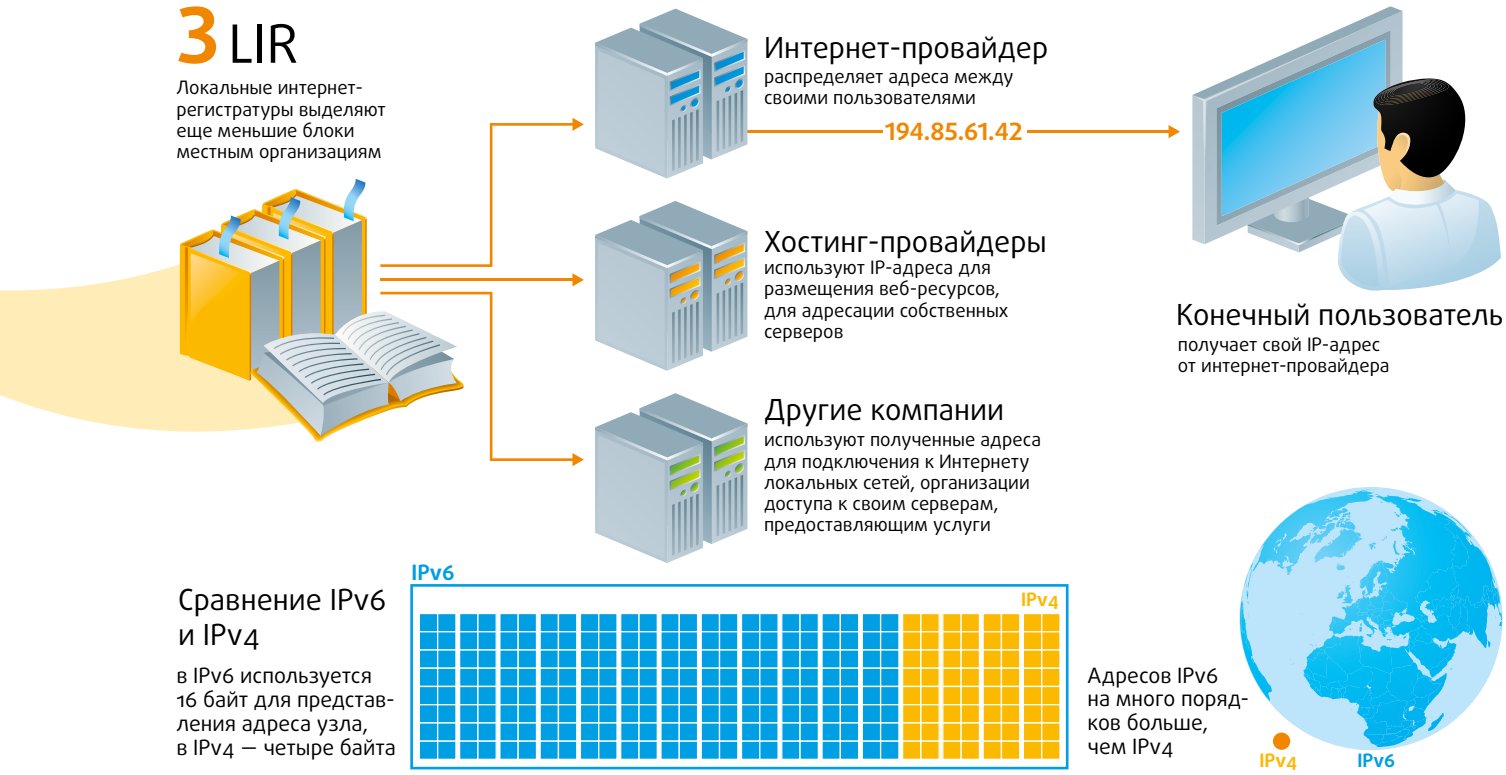
Появились и первые интернет-провайдеры, на практике занимающиеся продвижением IPv6 среди своих клиентов. Это прогресс — ведь раньше проблеме популяризации протокола уделяли внимание только международные организации вроде RIPE NCC и чиновники стран, наиболее продвинутых в области развития интернет-технологий. Между тем количество конечных пользователей, готовых перейти на протокол IPv6, может увеличиться в случае, если провайдеры начнут его рекламировать.

Об этом свидетельствует опыт голландской компания XS4ALL, которая ввела в коммерческую эксплуатацию услуги доступа в Интернет с использованием IPv6. Правда, провайдер среди прочего отмечает, что его клиенты не готовы тратить много усилий на настройку доступа в Сеть посредством нового протокола и в основном пока просто активируют поддержку IPv6-соединения, но на практике не используют его.

[Не]уязвимый IPv6

Кроме статистики и существующего опыта в области внедрения IPv6 на конференции

ИНФОГРАФИКА: НАДЕЖДА АНДРИАНОВА



RIPE 61 рассматривались и чисто прикладные аспекты перехода к использованию новой технологии. В частности, был затронут вопрос о безопасности IPv6. Надо сказать, что раньше этой теме уделялось слабое внимание. Вместе с тем эксперты не раз заявляли о том, что новый протокол далеко не идеален с точки зрения уязвимостей.

На RIPE 61 были даны рекомендации, выполнение которых позволяет повысить безопасность IPv6. В частности, меньше уязвимостей в тех сетях, где протокол используется напрямую, без каких-либо технологий совместимости с IPv4. Другой совет для тех, кто внедряет IPv6: не копировать алгоритмы безопасности, применявшиеся в сетях на базе IPv4, так как они могут быть неэффективны. Кроме того, в сетях на основе IPv6 следует тщательно продумывать адресную инфраструктуру и задействовать все средства штатной безопасности.

А что еще?

Кроме протокола IPv6 на конференции RIPE в Риме обсуждались и другие вопросы. Роутинг, эффективное управление трафиком, развитие европейских Internet Exchange — все эти темы были отражены в программе форума.

На заседаниях рабочей группы, занимающейся развитием системы DNS, прозвучали доклады российских специалистов.

В частности, Василий Долматов, представляющий компанию «Криптоком», рассказал о методах шифрования в DNSSEC, разработанных на базе отечественных стандартов ГОСТ. На сегодняшний день соответствующие алгоритмы описаны в ряде документов IETF — международного сообщества, которое занимается разработкой стандартов в области архитектуры Интернета. Принципы шифрования ГОСТ в DNSSEC оттестированы на базе домена ORG и одного из крупнейших регистраторов — GoDaddy, а также поддерживаются последними версиями программного обеспечения для DNS серверов — BIND и Unbound.

Ведущие специалисты национального регистратора доменов RU-CENTER представили доклад о российском опыте внедрения первого кириллического домена верхнего уровня РФ.

Также в рамках римского форума RIPE был дан официальный старт исследовательской программе RIPE Atlas. Она направлена на различные измерения адресного пространства Интернета. Принять участие в программе могут не только интернет-провайдеры, но и рядовые пользователи, имеющие проводное подключение к Сети. Для того чтобы присоединиться к исследованиям RIPE Atlas, необходимо обратиться в RIPE NCC и бесплатно получить специальное небольшое устройство для подключения, после чего подключить его к Интернету. Данные с устройства будут передаваться в RIPE NCC для последующей обработки. Таким образом, за счет большого количества участников в RIPE NCC рассчитывают в режиме реального времени получать статистические данные о состоянии и развитии системы адресации Интернета.

Эффект масштаба

О буме инноваций и будущем IT-индустрии — в интервью с Джеффом Хьюстоном.

Беседовал Евгений Кускевич, RU-CENTER

Джефф, в ходе пленарного заседания (на конференции RIPE 61. — Прим. ред.) состоялась интересная дискуссия о технологическом усложнении современных сетей. Почему вы считаете, что пришло время поднять эту тему?
По мере того как мы наделяем сети дополнительным функционалом, возникает вопрос, насколько сложными они становятся и особенно — остаются ли они при этом устойчивыми. Порой, когда вы реализуете новые возможности, вы отнюдь не увеличиваете надежность сети — наоборот, вы делаете ее менее надежной. Когда ваша сеть включает в себя различные сложные функции, такие как VPN, управление ресурсами, контроль пропускной способности и т.д., встает вопрос о том, насколько она функционально устойчива. Это называется проблемой усложнения сети.

В ходе упомянутой дискуссии инженер компании Cisco Майкл Беринджер представил результаты проведенного им опроса. Среди прочих пунктов там был вопрос о причинах критических аварий в сетях, и 75% респондентов указали в качестве одной из причин ошибку оператора. Кроме того, 70% участников опроса ответили, что в их компаниях случаются аварии, разобраться в причинах которых под силу только лучшим экспертам. Получается, несмотря на автоматизацию процессов, человеческий фактор по-прежнему очень важен. Будет ли возрастать роль человеческого фактора при управлении сетями по мере их усложнения?
IT — это огромная индустрия. Она работает на принципе эффекта масштаба. Когда вы предоставляете услугу миллионам пользователей, то вы не будете привлекать своих лучших экспертов к решению каждой мелкой проблемы. Вы будете полагаться на отработанные процедуры, которые можно поручить менее квалифицированным специалистам. Ошибки часто возникают по вине операторов. А оператор — это не системный архитектор и не ведущий инженер, который настраивал и внедрял систему. Оператор отвечает за свою узкоспециализированную область. Он может разбираться

Следующие пять лет будут весьма болезненными для индустрии: конец адресов IPv4 и переход на новый протокол — это не то же самое, что перейти на новую версию Windows

в какой-то одной из систем, например, в безопасности, в управлении ресурсами сети или в телефонии. И для него не всегда очевидно, какое действие на сеть оказывают другие области. Так что такая проблема действительно существует.

В последнее время в Интернете происходит бум технических инноваций. Внедряется DNSSEC, на подходе IPv6, добавляется множество функций безопасности, например, разрабатываются механизмы шифрования для протоколов маршрутизации. Считаете ли вы эти изменения в Интернете революционными или же их скорее можно назвать эволюцией?
Любая сложная инженерная система со временем развивается. Люди всегда пытаются улучшить то, что у них есть. Это в природе человека. Ему трудно оставить вещи в покое. Порой мы себя убеждаем, что некоторые вещи необходимы, но это становится неочевидным, если смотреть на них шире. Возьмем, к примеру, безопасность. Должна ли сеть быть безопасной или же конечные системы должны быть безопасными? А если делать безопасным и то и другое, то нам от этого станет проще или сложнее? Возможно, лучшим примером будет устойчивость к потерям. Изначально Интернет был сервисом с негарантированной доставкой данных. Пакет проходил или же мог не пройти. Был допустимый уровень потерь, и это было

Джефф Хьюстон — ведущий исследователь APNIC. Один из виднейших мировых аналитиков в области интернет-технологий. Посвятил множество работ теме исчерпания IPv4 (www.potaroo.net)

приемлемо. Но сейчас мы пытаемся создать сети, которые не теряют пакеты. Но это странно, так как большинство приложений используют такие протоколы, как TCP, которые устойчивы к потерям пакетов. Зачем создавать сети большей сложности и стоимости, чтобы избежать проблем, которые устраняются на уровне приложений? А именно это здесь и происходит. Каждый пытается улучшить свою частичку мира. Но зачастую, когда кто-то делает это в своей частичке Интернета, Интернет в целом не становится от этого лучше. Он становится сложнее и зачастую хуже, становится менее надежным, работающим менее эффективно, а стоимость его использования при этом возрастает. Таким образом, в инженерии сдержанность и принцип минимализма так же важны, как и сложность. Иногда делать меньше — более хороший подход. Но это непросто потому, что все требуют добавлять новые возможности. Трудно сказать «делай меньше».

Вы высказали интересную мысль на сессии. Насколько я помню, это звучало так: «Легко строить бизнес на сложности». Так вещи действительно должны быть сложными, или они делаются таковыми порой искусственно?
Я вообще думаю, что многие вещи являются более сложными, чем они должны бы быть. Делаются ли они таковыми в интересах бизнеса? Интересный вопрос. Потому что люди, продающие компьютеры, это не те же самые люди, которые торгуют сетями. И часто существует противоречие между тем, купить ли услугу у вашего сервис-провайдера или ее аналог в виде приложения для компьютера. Очевидно, что сетевые

Когда ваша сеть включает различные сложные функции (VPN, управление ресурсами, контроль пропускной способности и пр.), встает вопрос, насколько она функционально устойчива

сервис-провайдеры хотят предоставлять доходные услуги, хотят наполнить сеть функциями и опциями, за которые пользователи будут платить. Это вопрос выбора. Выбор состоит в том, что можно купить ту же самую функциональность в виде программного обеспечения для компьютера. VPN — классический пример. Вы можете использовать его как приложение и рассматривать сеть просто как IP-транспорт, пользоваться сервисом поверх сети. Или же вы можете купить VPN у сервис-провайдера. И поставщик приложения, и провайдер услуги заинтересованы в прибыли. И иногда встречаются клиенты, которые покупают и то и другое сразу. И этим делают свою жизнь сложнее. Да, все делают бизнес, двигаясь сложными путями. Возникает ощущение, что если я делаю что-то ужасно умное, то могу делать на этом деньги. Так происходит в сетях, в разработке ПО, во всей индустрии. Но если вы посмотрите на ситуацию с точки зрения конечного пользователя, то осознаете, что вам этого не надо. Все, что вы хотите, можно описать принципом — «мне нужно, чтобы это работало и чтобы это было дешево». Если вы согласны с этим утверждением, это значит, что вы хотите простые сети, потому что они дешевые и они работают. Иногда то, чего хотят люди, и то, что им хотят продать, находится на разных уровнях. Большинство компаний делают бизнес на сложности. Может показаться странным, но зачастую то, что нам действительно нужно — это простота. А строить бизнес на минимализме сложно. Простота дает простую работу.

На вопрос о причинах критических аварий в сетях 75% респондентов отвечают «ошибка оператора»; а 70% участников уверены, что в их компаниях случаются аварии, разобраться в причинах которых под силу только лучшим экспертам. Выходит, несмотря на автоматизацию многих процессов, человеческий фактор по-прежнему важен

Интернет был сервисом с негарантированной доставкой данных. Пакет проходил или же мог не пройти. Был допустимый уровень потерь, и это было приемлемо. Но сейчас мы пытаемся создать сети, которые не теряют пакеты. Но это странно, так как большинство приложений используют такие протоколы, как TCP, которые устойчивы к потерям пакетов

И последний вопрос. Каков ваш прогноз для IT-индустрии на ближайшие 5 лет? Какие тенденции, изменения нас ждут? С какими угрозами мы столкнемся?
Это очень интересный вопрос. В последние 10 лет в индустрии произошли серьезные изменения. Был узкий круг телефонных операторов, которые контролировали коммуникации. А Интернет с технологией коммутации пакетов создал большую конкуренцию. Был предпринимательский малый бизнес. А те, кто проповедовал эффект масштаба, имел в своем распоряжении технологии. Интернет — это мейнстрим, и сейчас там есть только крупные игроки. Экономика масштаба доминирует. Но сейчас мы задаем этим людям сложные вопросы. Мы просим их осуществить переход от IPv4 к IPv6. Мы просим самых больших игроков быть подвижными и инновационными. А они этого не любят. Для них это неестественно. Так что следующие пять лет будут весьма болезненными для индустрии. Потому что конец адресов IPv4 и переход на новый протокол — это не то же, что перейти на новую версию Windows. Это непросто. Нет обратной совместимости. Это такой же большой переход, как от телефонии к Интернету. Но люди пока не осознают масштаб события. Так что следующие пять лет обещают быть весьма интересными. Интересными, потому что я думаю, облик индустрии и ее игроки через пять лет будут не такими, как сейчас. Я подозреваю, что мы увидим крах ряда компаний, появление новых больших игроков. Этот переход потрясет мир.

«Не осваивать IPv6 — большой бизнес-риск», — заявил в интервью журналу «Доменные имена» Марко Хогевонинг.

Марко, сколько лет вы занимаетесь IPv6?
Почти 10.

Что вы можете сказать об эволюции IPv6 за эти 10 лет?
Мы были одними из первых на точке обмена трафиком AMS-IX, кто начал эксперименты с IPv6-пирингом, используя бета-версии программного обеспечения Cisco. С ним тогда было много проблем, все время что-то ломалось. На мой взгляд, прогресс экспоненциальный. Разработки ведутся все стремительнее, по мере того как все больше людей развертывают IPv6. Устраняются недочеты, которые существовали в течение последних пяти лет. По мере освоения IPv6 находятся и исправляются многие ошибки. Мы наблюдаем значительную активность, но надо отметить, что возникла она сравнительно недавно.

Как изменилось отношение людей к IPv6?
Все больше интереса от интернет-операторов. Но управленцы тормозят процесс. Когда разговариваешь с техническими специалистами, они понимают проблему и осознают, что нужно двигаться к IPv6. Но обычно это стремление застревает на уровне руководителей, потому что они не понимают важность IPv6. Для обычной публики — это просто слово, IP как понятие — просто слово, потому что люди не покупают IP-адрес. Они покупают доступ в Интернет, получают доступ к Facebook, но не осознают, что за окошком браузера есть еще целый мир.

Какие проблемы с внедрением IPv6 существуют сегодня?
До сих пор остается много ошибок в программном обеспечении. Протокол по-прежнему не слишком распространен, хотя мы уверены, что решили все наиболее серьезные проблемы, препятствующие его внедрению. И другая важная вещь — это то, что сейчас по ходу развертывания мы убеждаемся, что остается много вопросов, связанных не столько с самим протоколом, сколько с планированием по его практическому применению. По мере того как идет развертывание IPv6, люди сталкиваются с множеством мелочей, которые были описаны еще 5–6 лет назад, но когда с этими вещами начинают реально работать, они говорят: «Послушайте, а ведь это не очень здорово». По ходу знакомства с IPv6 люди начинают смотреть на документацию, связанную с протоколом, под другим углом. В ходе практических действий вылезает множество мелких проблем с планированием и непосредственной реализацией IPv6, которые, я уверен, будут исправлены. Но это займет некоторое время.

И последний вопрос. Что вы можете сказать тем IT-компаниям, которые до сих пор не уделяют должного внимания IPv6?
Займитесь этим сейчас, потому что иначе вы подвергаете свой бизнес серьезному риску. Когда эра IPv4 закончится и вы потеряете связь с частью Интернета, вы рискуете потерять клиентов. Потому что с точки зрения клиентов, если они просто не смогут зайти на нужный им сайт или не смогут встретиться в онлайне с кем им нужно, для них это все равно, что сервер сломался. Вы не сможете просто объяснить им, что, мол, есть такая штука — IPv6. В ответ вы получите резонный вопрос: почему не решили проблему с внедрением протокола раньше, если знали о ней заранее?

Не осваивать IPv6 — большой бизнес-риск. Думаю, сегодня любой технический специалист, работающий в крупной компании, должен сообщить ее руководству и даже ее акционерам, что в IPv6 необходимо вкладываться. Потому что если компания не сделает этого сейчас, то через пару лет она попросту вылетит из бизнеса. Чтобы начать внедрять IPv6 — можно рекомендовать отправиться на сайт www.IPv6actnow.org.

Марко Хогевонинг — ведущий IP-инженер компании XS4ALL, co-chair рабочий группы IPv6 в RIPE NCC, один из ведущих европейских специалистов по IPv6

Почта без кириллицы

Сергей Баукин,
руководитель департамента
хостинга RU-CENTER

Домену РФ год, однако полноценная кириллическая электронная почта до сих пор недоступна. Для запуска первых решений требуется переработать большое число документов, описывающих интернет-стандарты.

В настоящий момент кроме классических адресов, включающих латинские буквы, цифры и некоторые знаки пунктуации (user@example.com), поддерживаются гибридные адреса с традиционной латинской записью локальной части до знака @ и кириллической или смешанной записью имени домена после @, например, user@пример.испытание, user@пример.com. Использовать для работы с электронной почтой адреса вида «почта@ник.рф» — не выйдет. Такую ситуацию нельзя назвать нормальной, особенно если учитывать, что когда затевали домен .РФ, то основным аргументом в его пользу было удобство кириллических адресов для русскоязычных пользователей. Очевидно, существующая смесь кириллицы и латиницы не делает систему удобной.

Несколько лет назад предложена система IDN (Internationalized Domain Names — многоязычные доменные имена), позволяющая использовать нелатинские письменности для записи имен доменов. Многоязычные домены с помощью кодирования Punycode преобразуются в специальные последовательности стандартных ASCII-символов (26 букв латинского алфавита, цифры от 0 до 9 и дефис). Таким образом доменному имени «президент.рф» соответствует последовательность «xn--d1ab-bgf6aiiy.xn--p1ai», которая, конечно, выглядит как абракадабра, но при этом вполне понятна интернет-маршрутизаторам и коммутаторам, передающим запросы интернет-пользователей по всей Глобальной сети.

Преимущество использования Punycode в том, что не требуется модификации большинства функционирующих в Интернете программ для поддержки нового типа доменных имен. Программы продолжают работать со старыми, привычными наборами символов латиницы. Исключение составляют веб-браузеры и почтовые клиенты, которые должны принимать от пользователя доменные имена в «нестандартном» написании, производить их перекодировку для дальнейшей передачи по Сети, а при получении закодированного с помощью Punycode доменного имени преобразовывать его для корректного представления пользователю.

Далеко не все почтовые клиенты и веб-интерфейсы электронной почты корректно работают с адресами в уже существующих кириллических доменах (речь пока что идет о «гибридных» адресах типа «mail@президент.рф», а не о полностью

ИЛЛЮСТРАЦИЯ: СЕРГЕЙ РАТНИКОВ

русскоязычных почтовых адресах). Например, Microsoft Outlook начиная с версии 2007 полностью корректно работает с русскоязычными IDN-адресами, а Thunderbird 3.0 их не поддерживает.

Мы исследовали готовность популярных почтовых веб-сервисов к обработке кириллических адресов (см. таблицу). Целью исследования являлась проверка того, насколько сейчас может пользоваться электронной почтой обладатель почтового адреса в русскоязычном домене .РФ. Типичные задачи такого пользователя: чтение полученных сообщений, составление и отправка собственных сообщений, работа с адресной книгой и фильтрация входящей почты. А если у такого пользователя есть собственный IDN-домен, например, в зоне .РФ, то он должен иметь возможность авторизоваться на почтовом сервере и сообщить ему о существовании своего домена.

Так, пользователь почтовой службы Gmail компании Google сможет прочитать сообщение, отправленное из IDN-домена, но адрес отправителя он увидит в технологическом виде Punycode (т.е. «vasya@ XN--80A1ACNY.XN--P1AI», а не «vasya@почта.рф»). А вот послать сообщение обладателю адреса в IDN-домене нельзя — на экране появится сообщение об ошибке. С адресной книгой тоже проблемы: добавить в нее адрес «vasya@почта.рф» можно, а послать на него письмо — нет.

Gmail позволяет настроить почтовые фильтры, использующие русскоязычные адреса, но работать фильтры не будут, поскольку нет внутренней перекодировки адресов. Google предоставляет сервис создания почты на базе Gmail с использованием домена пользователя. Для обладателей русскоязычных интернет-доменов этот сервис Google работает, только если указывать домен в представлении Punycode и в таком же виде вводить его при авторизации в веб-интерфейсе. Однако все это касается только тех IDN-доменов первого уровня, которые находятся в традиционных зонах первого уровня (латинские двубуквенные национальные домены .COM, .ORG, .NET и т.д.). Домен .РФ в списке разрешенных в Gmail доменов — даже в виде Punycode — пока не значится.

Почтовые сервисы Mail.ru и Rambler ведут себя хуже Gmail: здесь поддерживается только получение сообщения от отправителя из IDN-домена, при этом в строке «от кого» будет фигурировать последовательность символов Punycode, и понять, от какого корреспондента письмо, — непросто. Отправить письмо на адрес в IDN-домене из интерфейса Mail.ru или Rambler — нельзя. Внести такой адрес в адресную книгу и использовать его при настройке фильтров электронной почты тоже не получится. Нет и возможности привязки IDN-домена к почтовому сервису — впрочем, это в случае Mail.ru и Rambler относится к любому, даже традиционному домену из латинских символов, не только IDN.

На таком фоне «Яндекс.Почта» выглядит почти идеально. Поддерживаются и возможность чтения сообщения из IDN-домена (причем адрес отправителя будет выглядеть читабельно), и функция отправки письма получателю из IDN-домена. Полностью поддерживается работа с IDN-адресами в адресной книге. С настройкой и корректной работой фильтров электронной почты также проблем нет. Но есть некоторое неудобство для обладателей IDN-доменов, планирующих использовать почту «Яндекса» на своем домене: указывать IDN-имя в настройках сервера допускается, но авторизоваться с ним можно, только указав его технологическое представление Punycode.

Мы обсудили только работу почтовых сервисов с гибридными адресами. Когда же пользователи получат полностью русскоязычную электронную почту? Не скоро. К первой части адреса предъявляются другие требования, и они диктуют иной способ обработки нелатинских символов, нежели перекодирование в Punycode. И если адрес «vasya@почта.рф» всегда можно заменить на технологическое имя, то замены для адреса вася@почта.рф, записанного латинскими символами, не существует. А значит, нужно научить все сервисы, работающие с электронной почтой и ее адресами, обрабатывать национальные символы. Это касается как распространенных социальных сетей, интернет-магазинов, так и менее знакомых рядовому пользователю задач создания SSL-сертификатов, подписи электронных сообщений, систем фильтрации спама и других. Предстоит заново решить вопросы безопасности, связанные с графической схожестью написания некоторых латинских и кириллических символов.

Например, Microsoft Outlook начиная с версии 2007 полностью корректно работает с русскоязычными IDN-адресами электронной почты, а Thunderbird 3.0 их не поддерживает

В итоге реализация поддержки кириллических адресов требуетв несения изменений в 47 спецификаций и стандартов RFC, регламентирующих те или иные моменты функционирования Интернета. Изменение стандарта написания адреса электронной почты затрагивает много аспектов процедуры доставки сообщений. Ждать утверждения нового стандарта можно не ранее конца 2011 года. И хотя первые реализации, основанные на пока экспериментальных, неутвержденных стандартах, уже появляются, до возможности полноценного использования нового кириллического домена еще далеко.

Анализ популярных систем веб-почты на предмет работы с кириллическими адресами

	Gmail	Mail.ru	Rambler	Яндекс.Почта
Чтение сообщения (отправитель в IDN-домене)	Адрес отправителя в Punycode	Адрес отправителя в Punycode	Адрес отправителя в Punycode	Адрес отправителя читаемый
Отправка сообщения (получатель в IDN-домене)	Ошибка	Ошибка	Ошибка	Сообщение отправляется
Работа с адресной книгой	Добавить адрес можно, написать на него — нет	Не работает	Не работает	Контакт добавляется, сообщение написать можно
Настройка фильтров электронной почты	Не работает	Не работает	Не работает	Фильтры работают
Указание домена в настройках сервера	Принимает только Punycode для не-IDN-доменов первого уровня	Не работает	Не работает	Работает
Авторизация		Не работает	Не работает	С указанием домена в Punycode

Павел Кейно,
веб-разработчик,
программист

Punycode: от цифры к слову

Многоязычие в системе доменных имен появилось в результате кропотливой инженерной работы.

Технологические особенности

Представление IDN-домена для вычислительной машины и человека различно в отличие от обычных доменных имен, написанных на латинице. Для того чтобы перекодировать специальное представление домена в осмысленную последовательность символов и обратно, необходима поддержка Punycode в клиентской программе. Для преобразования символов в Punycode используется специальный алгоритм, который переводит строку Unicode в формат, содержащий только символы латинского алфавита, цифры и дефисы, согласно принятым стандартам, в записи доменного имени допустимы только эти символы. Так, адрес «москва.рф» в машинном представлении будет выглядеть как «xn--80adxhks.xn--p1ai».

Обязанность преобразования имен решено возложить на клиентское программное обеспечение, такое как браузер. Это решение является абсолютно безболезненным для традиционных доменных имен, а обеспечение доступности IDN целиком и полностью зависит от того, с каким браузером работает пользователь. На данный момент идет завершающий этап обновления программного обеспечения для возможности работы с такими доменами. Все современные браузеры уже полностью поддерживают IDN.

Алгоритм Punycode допускает к кодированию любой символ из Unicode. Можно закодировать не только символы национальных алфавитов, но и псевдографические знаки

Путь Punycode

Первоначально было предложено три варианта реализации многоязычной системы доменных имен.

Первый вариант — просто записать в файлы зон нестандартные символы. Однако такое решение привело бы к нестабильности всей системы DNS. Связано это с тем, что символы национальных алфавитов в различных реализациях протокола DNS и различных кодировках хранятся по-разному. Также возникли бы проблемы с сопоставлением домена в разных системах. Хотя даже если использовать универсальную кодировку Unicode, то можно столкнуться с трудностями совместимости версий этих кодировок. И, конечно же, многие используемые в Интернете протоколы отбросили бы любое доменное имя, содержащее символы, отличные от символов ASCII, даже если бы на стороне DNS никаких проблем не наблюдалось. К таким протоколам, например, относятся протоколы электронной почты.

Вторым вариантом было предложено использование классовой структуры DNS. Предполагалась постепенная миграция с используемого класса IN (который подразумевает только ASCII-представление) на класс с более либеральными правилами представления интернациональных символов. Предложение было отправлено в экспертное сообщество по DNS, но в конечном итоге эти спецификации так и остались в черновиках. Идея, основанная на классах, точно так же влекла за собой множество рисков, связанных с совместимостью установленного программного обеспечения. Различные DNS-классы использовались в прошлом, они применялись в широком спектре приложений, однако на сегодняшний день на практике используется всего лишь один класс DNS. Введение дополнительного класса могло бы внести путаницу в протоколы, затруднив выбор обработчиков запросов для разных классов в программном обеспечении.

Третьим вариантом была идея «над DNS», которая заключалась в том, чтобы все символы, не относящиеся к ASCII, могли быть одинаково представлены в том же ASCII-формате. Этот вариант рассматривался с позиции полной совместимости с DNS. Согласно алгоритму, строка в кодировке Unicode преобразуется в ASCII-последовательность допустимых символов. Серия таких кодировок получила название ACE (ASCII-совместимая кодировка; англ. ASCII-Compatible Encoding), а алгоритм — Bootstring.

Немалую роль при выборе решения сыграло то, что развертывание программы многоязычных доменов должно было произойти быстро и безболезненно для всей системы DNS. Всего было разработано около десятка алгоритмов ACE, такие как RACE, LACE и др. Версия за версией, они незначительно обновлялись и совершенствовались, пока на основе ACE не был разработан Punycode — частный случай Bootstring. Его и выбрали, как основной алгоритм представления многоязычных доменов.

Почему многоязычный домен начинается с «xn--»?

Любое имя, закодированное в IDN, начинается с префикса «xn--». Префикс является отличительной особенностью IDN. Тем самым клиентские программы определяют, нуждается ли доменное имя в перекодировании. Однако мало кто знает, почему был выбран именно этот префикс. Попробуем разобраться. Согласно переписке IANA и IETF (тактическая группа разработки интернет-технологий) в 2003 году, основными кандидатами на префикс были следующие двухбуквенные сочетания: AA, диапазоны от QM до QZ, а также от XA до XZ, и ZZ.

Во избежание путаницы были исключены все двухбуквенные сочетания, которые образовывали код страны по стандарту ISO 3166-1 (именно по этому стандарту присваивались обозначения для национальных доменов верхнего уровня). Были также исключены буквы, графически похожие на цифры (например,

Факты

Технологическая хронология IDN

Первые предложения по представлению IDN-доменов были озвучены в 1996 году Мартином Дюрстом в Университете Цюриха. Он предложил использовать кодировку UTF-5 для представления символов в ASCII-совместимой кодировке.

В декабре 1999 года стартовали первые коммерческие IDN-домены в зоне .COM, содержащие символы китайского письма. Были некоторые трудности с составлением таблиц для иероглифов, так как китайский язык имеет два варианта письма. Использовалась для этого кодировка RACE. Для нее использовался префикс «bq--».

В ноябре 2001 года создан комитет ICANN по многоязычным доменным именам. Комитет занимался выявлением проблем при использовании многоязычных доменов. Комитет подготовил целый ряд правил по регистрации многоязычных доменных имен, которым должны следовать регистратуры.

В том же 2001 году был предложен метод кодирования UTF-6 для представления многонациональных доменных имен. Кодировка имела размер 1 байт на символ. Перед закодированной строкой должен был использоваться префикс «wq--». Также была предложена кодировка LACE, усовершенствованный вариант RACE.

В 2003 году корпорацией ICANN совместно с IETF была утверждена спецификация IDN, в которой основным алгоритмом кодирования имен стал алгоритм Punycode.

В январе 2008 года корпорация ICANN внедряет тестовые домены верхнего уровня, использующие символы национальных алфавитов. Для России таким доменом стал «пример.испытание». Тестовые домены дали возможность обычным пользователям протестировать работоспособность этих доменов в различных браузерах.

В 2009 году корпорация ICANN одобрила создание национальных IDN-доменов верхнего уровня.

В 2010 году первые страны получили собственные IDN-домены верхнего уровня. Ими стали: ОАЭ, Саудовская Аравия, Египет. Четвертой страной в этом списке стала Российская Федерация с доменом .РФ.

буквы O, I, L, S могут быть перепутаны с 0, 1 и 5 соответственно). Исключены из списка были и те буквенные сочетания, которые когда-либо были использованы для обозначения кодировок более старых версий: BL, BQ, DQ, LQ, MQ, RA, WQ, ZQ.

Следующим шагом стал просмотр файлов зон доменов верхнего уровня на предмет наличия в них доменов второго уровня, начинающихся с оставшихся двухбуквенных сочетаний и имеющих после них два дефиса. Так из списка исчезли сочетания: AA, диапазон от QM до QZ, XA, XZ и ZZ. После этого в списке претендентов на префикс остался диапазон из 18 сочетаний: от XB до XY.

Последним шагом стал выбор префикса из этого множества непредсказуемым образом. Алгоритм случайного выбора был основан на вычислении специального представления строки (MD5-хеша), содержащей данные объемов торгов Нью-Йоркской фондовой биржи по некоторым акциям на определенную заранее дату. После преобразования полученной строки по заранее опубликованному алгоритму был получен порядковый номер префикса, и этот номер в таблице рассматривавшихся вариантов соответствовал XN.

Использованный алгоритм выбора имеет элемент непредсказуемости, так как привязан к биржевой статистике, но достоверность и непредвзятость выбора префикса впоследствии может быть легко проверена любым заинтересованным лицом, так как все нужные данные находятся в открытом доступе. То есть использованный метод выбора важного для интернет-сообщества префикса полностью прозрачен.

Итак, последовательность символов XN абсолютно ничего не обозначает и является лишь одним из 18 самых редко используемых двухбуквенных сочетаний, которое невозможно спутать по написанию ни с каким-либо другим. Двойной дефис после префикса служит для разделения префикса и закодированного имени.

Ограничения и допущения

Алгоритм Punycode допускает к кодированию любой символ из Unicode. Таким образом возможно закодировать не только символы национальных алфавитов, но и псевдографические знаки. Например, в некоторых зонах уже зарегистрированы вот такие экзотические имена ©.com (xn--gba.com), ♥.net (xn--g6h.net), ♫.org (xn--m6h.org). Конечно же, такие допущения возможны далеко не во всех зонах. Некоторые регистратуры ограничивают регистрацию только определенным набором символов. Например, в национальном домене Германии (.DE) разрешено регистрировать многоязычные домены, содержащие только символы немецкого (умляуты) и латинского алфавитов. А в кириллическом домене России (.РФ) допускаются только символы кириллического алфавита. Создано это в первую очередь для того, чтобы избежать появления фишинговых сайтов, домены которых используют графически похожее написание.

Кодирование нижнего и верхнего регистров (прописных и строчных букв) в теории также различно. На практике же регистратуры ограничивают регистрацию лишь прописными буквами по тем же причинам. Политика многих зон подразумевает запрет на регистрацию доменных имен, содержащих два дефиса подряд. Это означает, что в такой доменной зоне вообще запрещено регистрировать многоязычные домены.

Заключение

Возникновение многоязычных доменных имен — это целая эпоха, в рамках которой было разобрано огромное количество вариантов технической реализации, каждый из которых по-своему уникален. В конечном итоге при активном участии интернет-сообщества сформировался законченный алгоритм Punycode, который используется теперь повсеместно.

WebHiTech — конкурс технологического совершенства веб-сайтов Рунета

WebHiTech — первый технологический конкурс веб-сайтов в Рунете — в 2010 году прошел в третий раз. Церемонию награждения победителей провели в формате WHT Conf — мероприятия, основу которого составила традиционная конференция веб-разработчиков в статусе Web Standards Days.

Напомним, что претендовать на победу в конкурсе может любой из общедоступных веб-сайтов, ориентированных на русскоговорящую аудиторию. Победителей определяет жюри конкурса.

Конкурс проводится в трех номинациях:

- лучшее дизайнерское решение;
- лучшие потребительские качества;
- лучшее использование технологий.

Заявки на конкурс принимаются на официальном веб-сайте www.webhitech.ru. Традиционно отбор номинантов и голосование жюри, разделенное на два этапа, проводятся осенью. В 2011 году старт приема заявок также запланирован на конец лета. Конкурс активно развивается и уже превратился во флагманское мероприятие, под эгидой которого в течение года проводятся семинары и мини-конференции, посвященные веб-разработке.

Если же вернуться к итоговому мероприятию WebHiTech, можно отметить, что с каждым годом наблюдается смещение баланса этих компонентов в сторону полезного. В 2008 году конкурс WebHiTech завершился пафосной церемонией награждения, прошедшей в весьма экзотическом месте: в подземном бункере, находящемся под Таганской площадью в Москве. В 2009 году была впервые опробована идея совмещения церемонии награждения (столь же торжественной) с мини-конференцией для веб-разработчиков. И вот в 2010 году принято решение вообще отказаться от церемониальной части в привычном понимании этого слова, что позволило организаторам не распылять внимание и сосредоточиться на проведении конференции. Результатом все остались довольны. Так что не удивительно, что в планах на 2011 год помимо проведения самого конкурсного отбора значится и очередная конференция, возможно, чуть более масштабная.

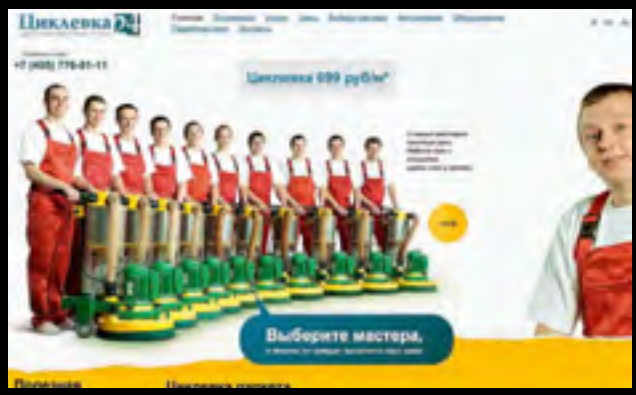
Итак, конкурс WebHiTech, впервые проведенный в 2008 году, уже успел стать заметным отраслевым мероприятием. Конкурс призван выявлять веб-проекты, способные убедительно доказывать и недвусмысленно демонстрировать широкому кругу практикующих разработчиков целесообразность применения новейших технологий в полном согласии с веб-стандартами. Мы публикуем список сайтов — победителей WebHiTech по версии 2010 года. (Да-да, в каждой номинации — по два третьих места, а в одной из номинаций еще и два первых места. Это не ошибка — просто следствие одинакового числа отданных за соответствующие проекты голосов жюри.)

Идея конкурса предложена в 2007 году Артемием Ломовым, известным идеологом веб-стандартов и председателем оргкомитета WebHiTech

Номинация «Лучшее дизайнерское решение»

При оценке работ, заявленных в данную номинацию, наибольшее внимание уделяется дизайну сайта в понимании искусства композиции, художественного оформления. Цель данной номинации — показать миру, что сайты, сверстанные с применением блочной модели CSS и созданные по правилам семантической разметки, уж точно ничем не хуже, а в большинстве случаев и гораздо лучше с точки зрения эстетического восприятия, нежели проекты, использующие сомнительное наследие консервативной школы табличной верстки и пренебрежение спецификациями технологий.

III место. BioTech Systems www.biotech-system.com.ua



I место. «Паркет 24» www.parket-24.ru

III место. «Азовтур» www.azovtour.com

II место. «Спортвилль-Дмитровка» www.sport-ville.ru

Финалист. Клиника «Панацея» www.klinikapanacea.ru

Факты

В 2008 году заявки на конкурс принимались полгода, в 2009 и 2010 годах — по 2 месяца. На количестве заявок сокращение сроков отразилось незначительно.

В 2010 году получено на 6% меньше заявок, чем в 2009-м, но в итоге номинантов было отобрано аж на 32% больше.

По итогам 2010 года номинантами конкурса стали 58% заявленных проектов, а лауреатами — 12% номинантов.

За последний день приема заявок в 2010 году на конкурс выдвинуто больше проектов, чем за весь август 2008-го.

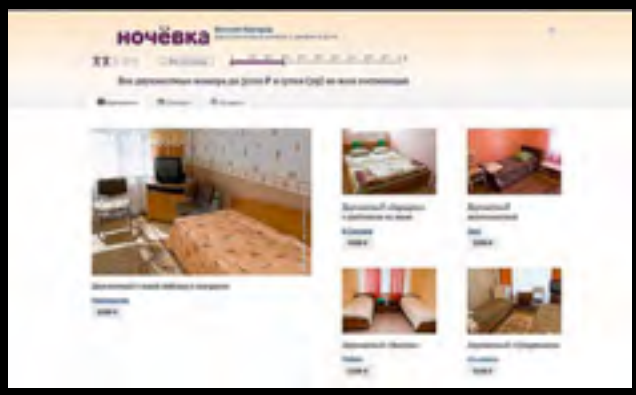
Номинация «Лучшие потребительские качества»

При голосовании в данной номинации предпочтения жюри отдаются проектам, отличающимся высоким уровнем пригодности к использованию (usability) и доступности контента (accessibility) для максимально широкого круга потенциальных пользователей. Оценивается скорость загрузки страниц, комфортность восприятия информации, продуманность системы навигации по сайту, доступность контента в условиях использования устаревших версий браузеров и портативных устройств, доступность всех сервисов сайта при отключенных JavaScript, ActiveX, Flash и пр., наличие и качество реализации альтернативных версий представления контента (для вывода на печать, для карманных компьютеров и т.п.).

II место. Откуда и куда.Ру www.otkudaikuda.ru

I место. Икра «Вкусно» www.ikravkusno.ru

III место. «Зона звука» www.zonazvuka.ru



I место. Ночевка www.hotels.nov.ru

III место. Сервис подбора наушников www.headphones.sony.ru

По итогам конкурса по версии 2010 года в каждой из трех номинаций вручены по два приза за третье место.

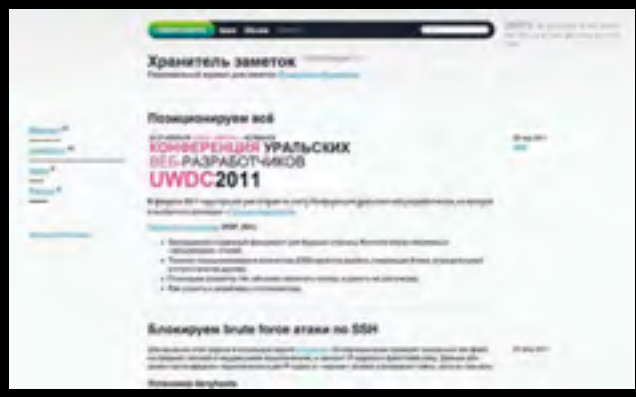
Первая церемония награждения была исключительно торжественной и проходила в довольно экзотическом месте — бывшем военном бункере.

Формат награждения изменился: теперь призы вручаются в рабочей атмосфере в рамках полезного мероприятия — конференции по веб-стандартам.

WebHiTech — это не только собственно конкурс, но еще и разнообразные конференции и семинары.

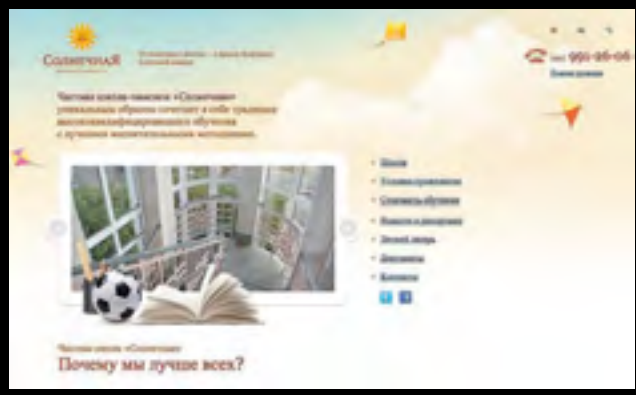
Номинация «Лучшее использование технологий»

Наибольшие шансы на победу в данной номинации имеют проекты, страницы которых: не содержат ошибок валидации в HTML- и CSS-коде; в максимальной степени соответствуют принципу разделения содержания и представления на уровне конечного кода веб-страниц, отправляемого сервером клиенту; выполнены в лучших традициях семантической верстки; эффективно используют микроформаты — в общем, являются красноречивой иллюстрацией продуктивного использования современных веб-стандартов.



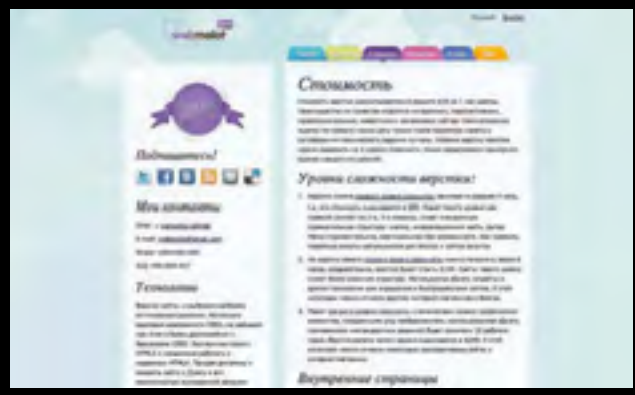
III место. Хранитель заметок www.noteskeeper.ru

I место. HippoApp www.hippoapp.ru



III место. Школа-пансион «Солнечная» www.sunpan.ru

II место. «Регион 18» www.pack18.ru



Финалист. Webmolot.com www.webmolot.com

В течение 2008–2010 годов организовано 2 конференции для разработчиков, 2 тематические секции на конференции «РИФ + КИБ», 5 учебных семинаров в вузах.

WebHiTech не только вручает, но и сам получает призы. В 2009 году конкурс стал мероприятием года по версии отраслевой премии РОТОР.

В жюри конкурса каждый год участвует 23–29 человек. Бессменными судьями на протяжении всех трех лет являются 14 участников жюри.

Существует добрая традиция приглашать в состав жюри авторов выдающихся конкурсных работ прошлых лет.

68

66

Многие пользователи предпочитают уничтожать разнообразие паролейв есьма опасным способом: они устанавливают на всех сервисах один и тот же пароль, которыйз апоминают

DNSSEC: столкновение с будущим

Обновление безопасности DNS провели в корневой зоне. Но проблемы только начинаются.

Летом прошлого года после тщательной подготовки в корневой зоне глобальной системы доменных имен развернули технологию DNSSEC (см. «ДИ», осень, 2010). Внедрение DNSSEC в корневой зоне — ключевой этап на пути развертывания этой технологии, без этого данная технология не может рассчитывать на дальнейшее уверенное развитие.

Кратко напомним азы: DNSSEC — это расширение протоколов «классической» DNS, вводящее с помощью криптографии механизмы удостоверения адресной информации и проверки достоверности полученных из DNS данных.

Может показаться, что с внедрением DNSSEC в корневой зоне пользователи Интернета стали жить в защищенном пространстве. Но все не так радужно. Действительно, теперь это защищенное пространство — новый безопасный дом — можно построить. Но по какому именно проекту будут строить? Пока что стройка далека от активной фазы. В лучшем случае можно говорить о закладке фундамента будущего здания.

Практическому развитию препятствует тот факт, что DNSSEC до сих пор не получила достаточного распространения в доменах второго уровня. Например, технология фактически никак не используется в зоне .RU.

Развертывание DNSSEC в доменах, находящихся уровнем ниже корня DNS, также гарантированно наталкивается и на технические, и на административные проблемы. Управление удостоверенными доменными зонами резко отличается от привычных, традиционных подходов. Изменения в доменную зону сложнее вносить, так как каждое изменение требует дополнительной процедуры подписания с использованием секретного криптографического ключа. При этом плотно населенные доменные зоны (то есть содержащие большое число записей) требуют существенного времени на генерацию

подписанной зоны. Осложняет ситуацию и то, что в данные зоны может вкрасться ошибка. И если зона с ошибкой в криптографической части будет опубликована на DNS-серверах, то это автоматически сделает домены данной зоны строго недоступными для навигации. Дело в том, что с точки зрения DNSSEC такие ошибки неотличимы от попытки подмены адресной информации злоумышленником.

Наверняка в реализациях DNSSEC возникнут новые уязвимости и дефекты, ранее вообще не свойственные DNS. Дело в том, что сложность протоколов DNSSEC гораздо выше, чем у «старых» протоколов классической DNS. Рост сложности приводит к росту риска возникновения уязвимостей.

В прошлом году и в начале этого, 2011-го, мы видели два шумных примера неприятностей, связанных с криптографическими механизмами в современном Интернете. Первый из этих примеров — компьютерный зловред Stuxnet, привлекший грандиозное внимание прессы благодаря тому, что он содержал код, нацеленный на атаку специального аппаратного обеспечения. Интересен тот факт, что Stuxnet для успешного внедрения в ядро операционной системы (ОС) Windows использовал электронные сертификаты, удостоверенные с помощью секретного ключа, принадлежавшего одному из производителей аппаратного обеспечения (по другим данным, использовались два ключа двух разныхп роизводителей).

При штатной эксплуатации подобные секретные ключи служат для удостоверения используемых в ОС Windows драйверов аппаратных компонентов. Предполагают, что для червя Stuxnet секретные ключи были похищены, что позволило сгенерировать соответствующие сертификаты и добиться возможности доступа к ядру операционной системы.

Второй пример касается компрометации системы выдачи SSL-сертификатов для веб-сайтов. Используя интерфейс одной из компаний-партнеров центра сертификации Comodo, злоумышленники смогли сгенерировать подлинные SSL-сертификаты для доменов, которыми не владели. Среди них оказались: mail.google.com, www.google.com, addons.mozilla.org и др. То есть, используя полученные сертификаты, можно создать веб-сайты, выдающие себя за соответствующие сервисы Google, Inc. и Mozilla Foundation. При этом «достоверность» подобных сайтов подтверждается подлинными сертификатами. (Проблема здесь в том, что компания Comodo не должна была через своего доверенного партнера выдавать сертификаты тем лицам, которые не контролируют соответствующие домены.)

Оба только что описанных события связаны с получением несанкционированного доступа к секретным криптографическим ключам. С их помощью удостоверялись мошеннические, вредоносные данные или программный код, как в случае со Stuxnet. Иными словами, практика очередной раз подтвердила, что безопасная и защищенная сама по себе технология не спасает от дефектов в способах применения этой технологии. Чем и пользуются злоумышленники. При этом рядовые пользователи оказываются в худшем положении, так как они начали ощущать себя в безопасной среде — но ощущение оказалось обманчивым.

Криптографические механизмы, действовавшие в обоих описанных выше случаях, математически эквивалентны механизмам, используемым в DNSSEC. То есть при краже секретных ключей от того или иного сегмента DNS злоумышленники смогут с легкостью злоупотребить повышенным доверием пользователей.

Можно с уверенностью предположить, что выбранные методы управления ключами в рамках поддержки DNSSEC не будут сильно отличаться от тех, которые применяются при работе с SSL-сертификатами или с сертификатами, удостоверяющими драйверы ОС Windows. То есть с распространением DNSSEC ключи от тех или иных доменов наверняка попадут к злоумышленникам. И множество пользователей, оснащенных новыми браузерами, однажды «попадут не туда», используя вполне доверенный канал работы с DNS.

Конечно, вряд ли такое может произойти с корневым ключом DNSSEC. По крайней мере, хочется на это надеяться.

С распространением DNSSEC станет ясно, насколько реальность далека от теории, описывающей безопасное будущее доменов. Основные трудности только появились на горизонте, и их пока никто не измерял.

Перспективы

DNSSEC — клиентская часть

Некоторое время назад предполагалось, что DNSSEC сосредоточит свое влияние на серверах интернет-провайдеров и не появится на пользовательском уровне. Все равно компьютеры рядовых интернет-серферов полагаются в плане преобразования адресов на провайдерские DNS-серверы. Теперь направление развития технологии поменялось: можно ожидать прихода DNSSEC на компьютеры пользователей. Более того, это наиболее вероятный следующий шаг. Поддержку защищенной версии DNS внесут в браузеры. Серьезных препятствий тут нет. Да, прогнозируются побочные эффекты: например, при условии, что изменятся алгоритмы кэширования адресной информации, может возрасти нагрузка на серверы имен, поддерживающие домены. Но это не препятствие. Осенью прошлого года уже была представлена специальная версия браузера Chrome и плагины для Mozilla Firefox, поддерживающие DNSSEC.

Более того, так как в распоряжении клиентского программного обеспечения появляется новый механизм удостоверения информации, размещенной в Интернете, то разработчики примутся этот механизм развивать и использовать для доверенной публикации в DNS сведений, используемых для аутентификации приложений и пользователей. Это может подстегнуть развитие DNSSEC.

Домен и сайт без опасности

Адресное пространство в Интернете давно уже является ценным ресурсом, а ценности, как известно, привлекают внимание недобропорядочных участников Глобальной сети.

Угоны доменов осуществляют самыми разными способами. При этом мастерство угонщиков, к сожалению, растет гораздо быстрее, чем информированность пользователей. Практика подтверждает всю плачевность ситуации, демонстрируя неутешительную статистику похищений доменов. И перехвата управления сайтами. Ведь веб-сайт, даже сам по себе, — ресурс ничуть не менее ценный для злоумышленника, чем доменное имя.

Наблюдения над обращениями пользователей в техническую поддержку того или иного крупного хостинг-провайдера, регистратора доменов регулярно доказывают один и тот же факт: львиной части взломов веб-сайтов или краж доменов не случилось бы, следуй пользователи правилам безопасного сопровождения в отношении своих онлайн-ресурсов.

Однажды заполучив «универсальный» пароль, атакующий сразу взламывает все сервисы, на которых этот пароль используется

На первом месте среди угроз, как всегда, находится перехват административных паролей. Не далее чем в прошлом году для выуживания таких паролей применительно к доменам использовали новый метод, хорошо автоматизированный. С помощью специальных программ-ботов автоматически просканировали записи в публичном сервисе Whois, отыскивая такие записи о доменах, где в качестве контактного указан адрес электронной почты на бесплатном почтовом сервисе.

У таких почтовых сервисов есть одна особенность: если почтовый ящик в течение продолжительного промежутка времени не используется — то есть не просматривается своим владельцем, — то он освобождается.

Освободившийся ящик можно зарегистрировать заново, ведь мы говорим о бесплатных почтовых сервисах (mail.ru, yandex.ru, gmail.com и др.).

Поэтому, собрав базу подходящих адресов, указанных в Whois, устроители атаки принялись также автоматически проверять, не оказались ли какие-то из этих адресов снова свободными. К сожалению, многие и многие администраторы доменов не следят за актуальностью своих контактных данных. Администраторы указывают при регистрации домена адрес электронной почты, о которой спустя год или два благополучно забывают. (Ничего удивительного: сервис же бесплатный!)

Регистрация же домена при этом регулярно продлевается. (Опять — ничего удивительного: домен гораздо важнее, чем какой-то почтовый ящик!)

Поэтому атакующим удалось найти немало освободившихся контактных адресов, которые тут же были ими зарегистрированы. Вероятно, уже не в автоматическом, а в автоматизированном режиме, то есть с применением ручного труда, так как популярные сервисы просят решить капчу при регистрации почтового ящика — это защита от ботов.

Следующий шаг атаки — использование механизма напоминания пароля в панели управления регистратора, через которого зарегистрирован домен с перехваченным почтовым ящиком. Очевидно, что после того как механизм напоминания сработал и выслал пароль на контактный e-mail, атакующий получает доступ к панели управления данным доменом на сайте регистратора. Теперь уже можно делать с доменом все что угодно, в том числе перенаправлять трафик с соответствующего домену веб-сайта.

Конечно, в схеме данной атаки часть вины лежит на регистраторе доменов, который должен был заранее более строго выстроить и сервис Whois, и систему напоминания паролей. Но пострадавшим пользователям от этого не легче. Тем более что они также нарушили одно из правил безопасной эксплуатации виртуальных ресурсов: нужно поддерживать свои административные контакты в актуальном состоянии.

ИЛЛЮСТРАЦИИ: СЕРГЕЙ РАТНИКОВ

Правило №1

Поддерживайте в актуальном состоянии контактные адреса e-mail, связанные с управлением доменами или другими сервисами. Удостоверьтесь, что к контактному почтовому ящику не имеют доступа посторонние лица.

Утратившие актуальность контактные данные, как мы видели выше, позволят злоумышленникам перехватить управление доменными именами администратора. А если кто-то лишь просто читает почту вашего ящика, он также может использовать систему напоминания паролей панели регистратора доменов для получения доступа к аккаунту.

В прошедшем году не менее распространены были фишинговые методы обмана пользователей. Хотя их нельзя назвать новым приемом. Так, проводятся массовые, но целевые рассылки, как будто от имени регистратора доменов или от хостинг-провайдера. Для злоумышленников установить списки адресов, которые, вероятно, принадлежат клиентам того или иного крупного хостера, регистратора, — не так уж сложно. Письмо, якобы отправленное службой технической поддержки, сообщает, что «ваш сайт временно заблокирован из-за превышения лимита нагрузки на сервер» или «регистрация вашего домена требует подтверждения»... Есть много других вариантов писем, но все они заканчиваются очень похожей фразой, предлагающей для осуществления какого-либо действия «кликнуть по ссылке, приведенной в конце письма».

Ссылка только имитирует адрес настоящего сайта компании, от имени которой якобы отправлено письмо. На самом деле кликнувший по ссылке пользователь направляется на подставной сайт, где ему предлагают ввести свои логин/пароль. Полученные данные тут же в автоматическом режиме используют для перехвата управления доменом или другим онлайн-ресурсом.

Правило №2

Всегда с подозрением относитесь к ссылкам, полученным в сообщениях электронной почты. Не переходите по ссылкам, в достоверности, правильности которых не уверены.

Необходимо обращать внимание на характер ссылок, получаемых по электронной почте, а также тщательно сверять с официальной информацией компании, указанной в отправителях, данные в заголовках писем, в их адресных полях, в поле «тема». Да и само содержание этих писем неплохо проверить, прежде чем слепо кликать по ссылкам. Интернет-компании редко не дублируют на своих сайтах важную информацию, касающуюся управления клиентскими ресурсами. Конечно, о блокировке одного-единичного сайта крупный хостер не пишет в корпоративных новостях, но вот в персональной панели управления наверняка сообщение разместит. Поэтому верным решением является следующее: при получении сомнительного письма не переходить по ссылкам в нем, а сперва проверить информацию по другим каналам. Заходить же в панель управления браузером нужно не по ссылке из электронной почты, а стандартным образом, воспользовавшись веб-сайтом компании — провайдера услуг.

При этом всегда тщательно проверяйте адреса интернет-серверов, запрашивающих логин и пароль от панели управления. Не следует вводить пароли от панели управления на незнакомых сайтах, адреса которых вызывают какие-либо сомнения (например, произошла неожиданная смена привычного URL, выдаются предупреждения системы безопасности браузера и т.п.). Обратите внимание, что обмен данными с веб-сайтом при вводе административных логина и пароля обязательно должен проходить по защищенному протоколу HTTPS.

В минувшем году в очередной раз обновился инструментарий разработчиков вирусов и троянских программ. Как известно, такой инструментарий позволяет быстро создавать специализированные троянские программы, нацеленные на сбор определенной информации. Новинкой оказался тот факт, что теперь к такой представляющей интерес информации

относят и пароли от регистраторских панелей управления доменами. И уже несколько лет специализированные троянские программы собирают на пользовательских компьютерах пароли от FTP-доступа к хостинг-площадкам.

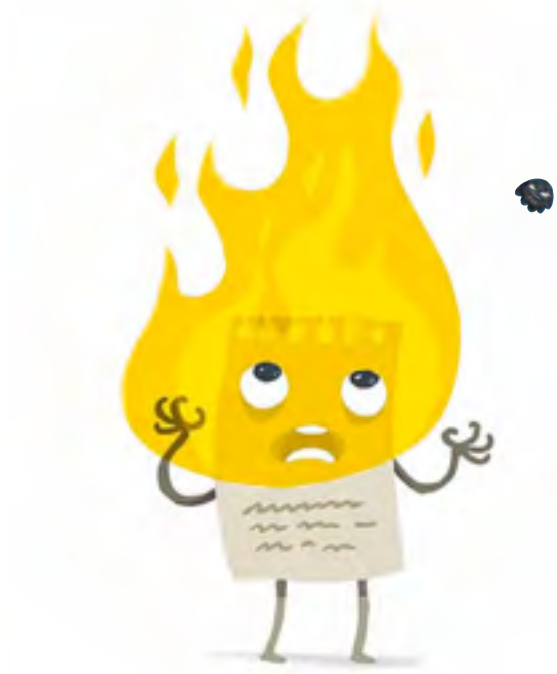
Пользователи привыкли сохранять пароли на диске компьютера. При этом многие программы, среди которых браузеры и FTP-клиенты, постоянно предлагают сохранить пароль для того, чтобы не вводить его следующий раз при посещении этого же сайта. При этом пароли часто сохраняются в незащищенном виде. То есть могут быть считаны троянской программой и отправлены злоумышленнику. Конечно, троянская программа может прочитать и вводимые с клавиатуры пароли. Есть одно отличие этих двух случаев в том, что при чтении с диска собирается сразу большое число паролей за короткое время. При перехвате клавиатурного ввода нужно еще дождаться, чтобы пользователю потребовалось ввести пароль.

Правило №3

Старайтесь не хранить нужные пароли на компьютере, если только это возможно.

О том, что необходимо соблюдать правила компьютерной безопасности и в части предотвращения попадания троянских программ на ПК, — мы только напомним в надежде, что уж к этим-то правилам читатели привыкли. Правда, от проникновения «троянцев» все равно никто не застрахован.

На практике следовать этому правилу сложно. В жизни современного интернет-пользователя существует слишком много паролей.



Правило №4

Если вы не можете запомнить все пароли, используйте для их хранения специальную программу-контейнер и мастер-пароль.

Такая программа сохраняет ваши пароли в удобном формате внутри зашифрованного файла. При этом для доступа к этому файлу используется мастер-пароль, к которому полностью применимо третье правило — этот пароль нельзя сохранять на компьютере. Примеров программ-контейнеров много, отметим две: KeePass и Password Safe.

Многие пользователи предпочитают уничтожать разнообразие паролей (а с ним и необходимость использования инструментов для хранения этих паролей) весьма опасным способом: они устанавливают на всех сервисах один и тот же пароль, который запоминают. Этот подход неоднократно играл на руку злоумышленникам. Опасность его в том, что, однажды заполучив пароль, атакующий сразу взламывает все сервисы, на которых этот пароль используется.

Традиционный способ выманивания универсального пароля — это добротный двухуровневый фишинг. Здесь пользователю не предлагают посетить поддельную страницу знакомого ему сайта, а напротив — приглашают зарегистрироваться на новом, незнакомом, но очень привлекательном сервисе. Сервис при этом создан лишь для того, чтобы заполучить пароль (с привязкой к конкретному пользователю). Более того, даже пароль осторожного пользователя может «утечь» из той или иной базы без всякого участия данного пользователя — просто по недосмотру администрации вполне добропорядочногоо нлайн-ресурса.

Правило №5

Не используйте один и тот же пароль для разных онлайн-ресурсов.

При этом, например, добавление цифр 1, 2, 3 и далее в конец одного и того же пароля не является достаточной мерой! Разные пароли должны быть действительно разными.

К сожалению, в случае с доменами и сайтами разнообразие паролей не может быть очень высоким по той простой причине, что под одними реквизитами доступа в панели управления обычно находится много доменов или несколько сайтов. Тем важнее становится соблюдение пятого правила — потеря пароля сразу от нескольких доменов только по той причине, что этот же пароль использовался на городском форуме, еще более неприятна.

Современный Интернет все еще остается средой открытой передачи данных. Подавляющая часть трафика с пользовательского компьютера не шифруется. Активно используются открытые сети Wi-Fi, а также пусть и защищенные, но незнакомые беспроводные сети. Даже если на вашем компьютере пароли от сайтов и доменов не сохраняются, их можно перехватить, если они передаются по сети в открытом виде. К сожалению, множество протоколов, употребляемых в повседневной деятельности администратора домена или сайтостроителя, как, впрочем, и любого пользователя Интернета, — используют передачу информации в открытом виде.

Правило №6

Для обмена данными применяйте защищенные протоколы, если только это возможно.

Откажитесь от применения устаревших, открытых протоколов там, где это возможно. Защищенные протоколы: HTTPS — для работы с Вебом, в том числе, что особенно важно, с системами авторизации веб-сайтов. Обязательно включите поддержку HTTPS для администраторского интерфейса вашего веб-сайта. В случае с панелями управления хостинг-провайдеров и регистраторов доменов использование HTTPS уже стало обязательным требованием.

Откажитесь от FTP для доступа к хостингу при редактировании файлов веб-сайта. Используйте SSH и SFTP — эти протоколы защищены. SSH (SFTP) сейчас поддерживается даже на платформе Windows. Порекомендуем известные клиенты: WinSCP, PuTTY.

Перехват управления веб-сайтом возможен не только с помощью кражи реквизитов доступа. Наличие уязвимостей в программном обеспечении, используемом на веб-сайте, может предоставить точно такой же полный доступ к управлению сайтом, как и администраторский пароль.

Правило №7

Тщательно следите за программным обеспечением, которое управляет вашим сайтом.

Конечно, уследить можно не за всем, особенно если вы пользуетесь услугами хостинг-провайдера, — в этом случае системное программное обеспечение и часть прикладного находятся вне вашего контроля и в большинстве случаев не выступают в роли источника неприятностей. А вот CMS (система управления контентом), дополнительные скрипты могут содержать ошибки, приводящие к возникновению уязвимостей. Не используйте незнакомые, полученные из непроверенных источников программы на ваших сайтах.

Наш свод из семи правил не включает в себя некоторые азы: например, мы не стали заострять внимание читателя на процедуре выбора «неугадываемого» пароля. Надеемся, что с основами безопасного управления интернет-ресурсами все читатели нашего журнала уже знакомы.

Египет: кто нажал «зеленую кнопку»?

Виктория Бунчук,
выпускающий редактор
info.nic.ru

Александр Венедюхин,
главный редактор «ДИ»

Отключение в Египте национального сегмента Интернета в общественном сознании оказалось среди ключевых аспектов последовавшей революции.

74

Как показали последние события — как в офлайн-, так и онлайн-масштабах, — рассуждения скептиков о виртуальном железномз анавесе, который опустится на страны с введением многоязычных доменов(например, того же многострадального .РФ), — лишь теория.

Впрочем, это отключение не осталось без внимания, его подробно обсуждали в профильных интернет-изданиях и онлайн-сообществах. В этом есть некоторая ирония технологической истории: наиболее свежую и подробную информацию об отключении Интернета в Египте получить можно было только через Интернет, доступный для большей части остального мира. Несмотря на то что подобных отключений Сети специалисты ожидали и ранее, именно египетский вариант станет отправной точкой нового движения в управлении глобальным киберпространством.

Как это случилось

Сейчас, изучая ситуацию по горячим следам, сложно выяснить во всех подробностях, с помощью каких именно административно-технических мер египетских пользователей отсоединили от Сети. Есть разные свидетельства, смысл которых варьируется от довольно банального «перерезания кабелей» до задейство-

Ирония технологической истории: наиболее свежую и подробную информацию об отключении Интернета в Египте получить можно было только через Интернет, доступный для большей части остального мира

вания сложной схемы директивных указаний, заранее подготовленной прошлым египетским государственным руководством. Наверняка в реальности сработал некоторый средний вариант: во-первых, очевидно, действовал административный ресурс правительства («звонок провайдеру»); а во-вторых, тем провайдерам, кто не успел или не пожелал вовремя среагировать, «отключили кабели».

Особенности устройства протоколов маршрутизации Интернета позволили не только констатировать то, что египетский сегмент Интернета погас, но и увидеть снаружи, сквозь туман локальной ситуации, как именно это происходило.

Когда Интернет проектировали в качестве научной компьютерной сети, то предполагалось, что все участники действуют в интересах поддержания связности

EGостичный домен

Несмотря на всю развитость экономики Египта до революции, национальный интернет-сегмент не был столь уж большим; этот простой факт позволил североамериканским аналитикам довольно быстро сделать вывод, что, например, в США египетский сценарий невозможен ввиду значительно большего количества интернет-провайдеров.

Так, проникновение Интернета в Египте (соотношение месячного количества реальных интернет-пользователей к общей численности населения) составляет чуть больше 21%. Об этом говорит статистика, приведенная на специализированном ресурсе Internet World Stats. По сравнению со странами-соседями по черному континенту — это вовсе не «ужас-ужас», вполне себе приличный результат. Лидирует по этому показателю Тунис, в котором 36% населения хотя бы раз в месяц приобщаются к миру Глобального. Неплохо в абсолютных цифрах выглядят такие экзотические государства, как Марокко (33%), Кабо-Верде (30%), Нигерия (29%). Остальные африканские страны набирают не больше 10% (а большая часть — в районе 1%).

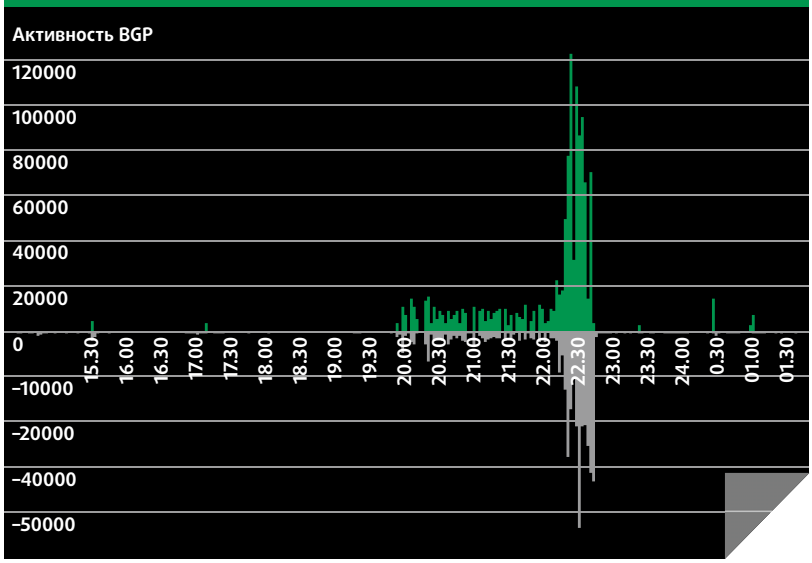
Однако в общемировых масштабах Египет явно уступает той же Германии, Китаю и даже России, об уровне «интернетизации» в которой все чаще говорят сквозь зубы и с явным пренебрежением: ну что взять с домена RU, если в нем «паспортизация» и на «анонимности» давно поставлен крест.

Определение «уступает» можно вполне применить и к национальному домену Египта EG, который относится к категории консервативных. Действительно, удивляет количество имен, зарегистрированных под суффиксом EG: всего 6 тысяч! По этому показателю Египет в явных аутсайдерах, опережает лишь Зимбабве, Мозамбик, Камерун и еще пару экзотических африканских стран. (К слову, самый мощный из доменов, соседствующих с Египтом на африканском континенте, — ZA, ЮАР — в нем функционируют рекордные 600 тыс. имен.) Официальная информация сайта администратора доменной зоны EG (Egyptian Universities Network — www.egregistry.eg) сообщает пользователю, что владельцем египетского домена может стать только резидент государства; иностранные организации должны подавать заявку на регистрацию .EG через компанию-резидента, египетского интернет-провайдера и/или иметь представительство в Египте. Существуют ограничения и на количество символов в домене: минимальная длина — 3 символа, максимальная — 22. Регистрация имен открыта только в поддоменах SCI.EG, EDU.EG, EUN.EG, NET.EG, ORG.EG, COM.EG. Еще одно ограничение,

* **Проникновение Интернета в Египте (соотношение месячного количества реальных интернет-пользователей к общей численности населения) составляет чуть больше 21%. А количество доменных имен, зарегистрированных в национальном домене этого государства EG, колеблется на уровне всего 6 тысяч**

EAST NEWS

Динамика отключения египетского сегмента Сети 27–28 января 2011 года по часам



Источник RIPE NCC: stat.ripe.net/egypt

которое сыграло злую шутку с «революционерами», задумавшими сменить власть (и весьма в этом преуспевшими, даже без поддержки радикальных исламистских группировок типа Аль-Каиды, которая «обвиняется» в причастности к аналогичному конфликту в Ливии), — name-сервера, поддерживающие работу EG, должны находиться в Египте.

Более подробную, свежую информацию о домене получить не удалось. Большая часть разделов сайта администратора зоны (а в этот перечень входят, например, раздел «Политика и правила регистрации в домене .EG», «Ценовая политика», «Список аккредитованных регистраторов») находятся «под реконструкцией». На данный момент (март 2011 года. — Прим.ред.) сайт египетского домена может быть полезен лишь whois-сервису, с помощью которого можно проверить, не зарегистрирован ли еще домен, на который вы положили глаз (если вы египтянин, конечно), и спискам целей, которые преследует администратор зоны ради «будущего ее процветания». Связана ли «реконструкция» сайта с революцией в стране или нет — можно только догадываться, однако домен EG был некоторое время «в отключке», и, пожалуй, этим все сказано.

Еще одним примером того, что Египет находится на грани глобального и локального — это новый национальный домен, записанный символами «местного» языка (IDN). Он был делегирован, то есть фактически заработал, одним из первых (в этот же день в DNS появились записи о домене Объединенных Арабских Эмиратов — امارات.; и Саудовской Аравии — السعودية.) — 5 мая 2010 года. Он выглядит следующим образом — مصر. По версии официальных источников, домен работает за счет исключительно вторичных серверов, которые находятся на территории страны, а посему отключить их и перекрыть доступ извне — еще проще. В этом случае как раз и имеет место быть так называемый «железный занавес», который совсем необоснованно приписывают российскому домену .РФ, попавшему в опалу технарей от бога и тех, кто «привык писать латиницей и не готов менять свои представления о классическом Интернете»...

Сеть, построенная на базе группы протоколов TCP/IP и самых современных принципов сетевой маршрутизации, вовсе не обязательно является действительно децентрализованной системой, не имеющей универсального «рубильника»

Действительно независимая?

Египет очень быстро и успешно исчез из Глобальной сети. Скорее всего, при этом нарушилась и связность локального Интернета. Но это уже не так важно. Причиной для отключения послужило желание лишить революционеров средства массовой коммуникации.

Раньше подобного массового директивного отключения не случалось. Важнейшая особенность тут в том, что ни методы административного управления системами адресации, ни распределенная DNS, но основы построения маршрутизации в Интернете — не могли предотвратить отключение и как-то ему помешать. То есть расхожий миф о распределенной и отказоустойчивой природе Интернета оказался не более чем мифом, это продемонстрировали на практике.

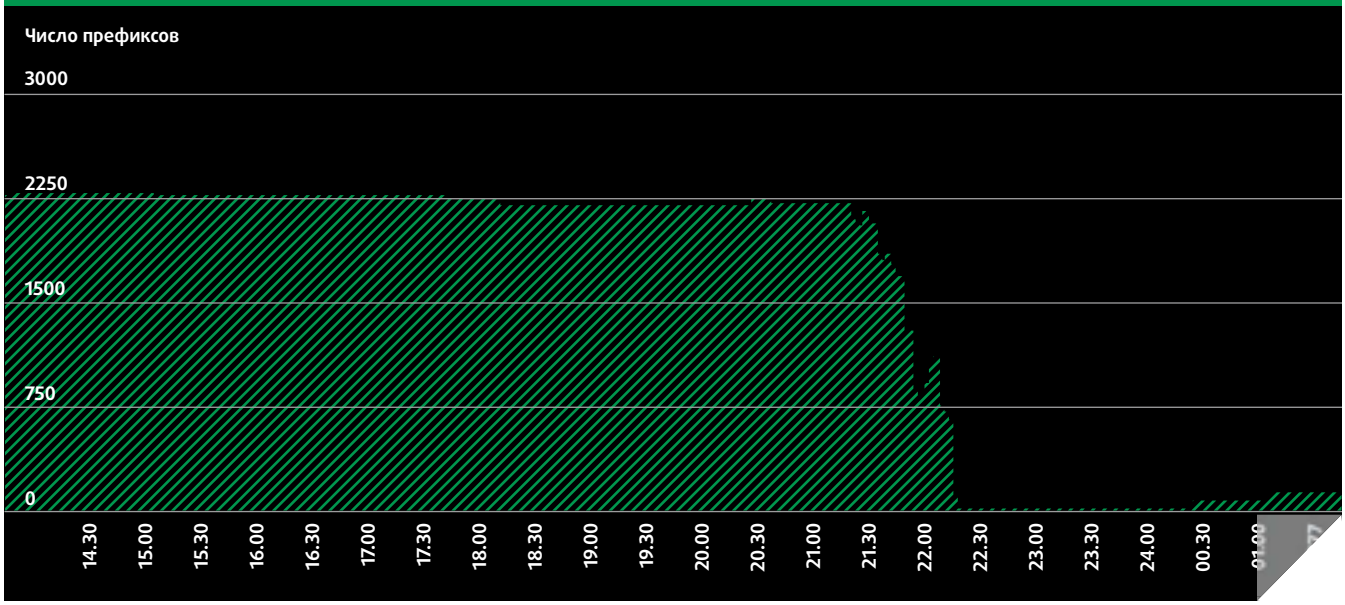
Казалось бы, «Интернет — децентрализованная независимая Сеть, построенная в виде распределенной структуры, где нет центрального управления». Действительно, такую сеть можно построить на базе протокола IP. Проект такой вычислительной сети ученые и показывали военному ведомству США, когда строили прототип Интернета в 70-х годах прошлого века. Но одно дело — возможности протокола и древний военный прототип. И совсем другое — практическая реализация базовых принципов в современном Интернете по всему миру.

Как ни странно, но сеть, построенная на базе группы протоколов TCP/IP и самых современных принципов сетевой маршрутизации, вовсе не обязательно является действительно децентрализованной системой, не имеющей универсального рубильника. Когда Интернет проектировали в качестве научной компьютерной сети, то предполагалось, что все участники действуют в интересах поддержания связности. Если же администраторы ключевых узлов по каким-то причинам не желают сохранять связность сегментов, а администрация сегмента не заботится о децентрализации, то имеющиеся технические протоколы не могут помочь рядовым пользователям — доступа к Сети у последних не станет, как не стало его в Египте.

Локальный рубильник

Эта история окажет заметное влияние на будущее Сети, сформируется новый тренд в управлении Интернетом. Теперь в первые ряды выйдет относительно новая тема: как глобально гарантировать всем землянам право доступа к Сети. Само это право на Интернет, его возможная неотъемлемость формируются как

Число египетских сетей, видимых в Интернете, в момент отключения сегмента 27–28 января



Источник RIPE NCC: stat.ripe.net/egypt

геополитические понятия уже несколько лет. Правда, до твердой фазы формулировок пока далеко.

Традиционным двигателем обсуждений принципов управления Интернетом был вопрос: а что делать, если США отключат национальный Интернет в той или иной стране, воспользовавшись неким главным рубильником? (Как известно, административное и техническое управление Сетью сосредоточены в США, а корпорация ICANN действует по законам штата Калифорния.) Теперь благодаря событиям в сфере египетских телекоммуникаций на повестке дня другой, не менее острый вопрос: а как бы, напротив, отобрать локальный рубильник, позволяющий быстро и осознанно отключить целый национальный сегмент от остального мира?

Кстати, о птичках. Альтернативный сервис, который бы помог бедным египтянам в охваченной революцией стране войти в Интернет и рассказать о том, что они в данный момент видят своими глазами, или поделиться мыслями на тему, а может, порассуждать о политических мотивах всего этого действа, предложил Google. Вот так просто — сориентировался и предложил (похоже на спекуляцию на чувствах и эмоциях), объяснив все это благородными мотивами помочь братскому народу.

Сервис, который предложил интернет-гигант (а точнее, небольшая группа инженеров-энтузиастов, занимавшихся его разработкой), можно назвать «голосовой Twitter».

Для того чтобы подключиться к этому сервису,н е требовалось интернет-соединения.

Из тех сил, которые могут отключить Интернет, вряд ли кто-то реально хочет это сделать. Разве что в самом крайнем случае, когда для выживания просто нет других вариантов

Проблема «красной кнопки», которой пугалась даже Еврокомиссия, превращается в проблему «зеленой кнопки».

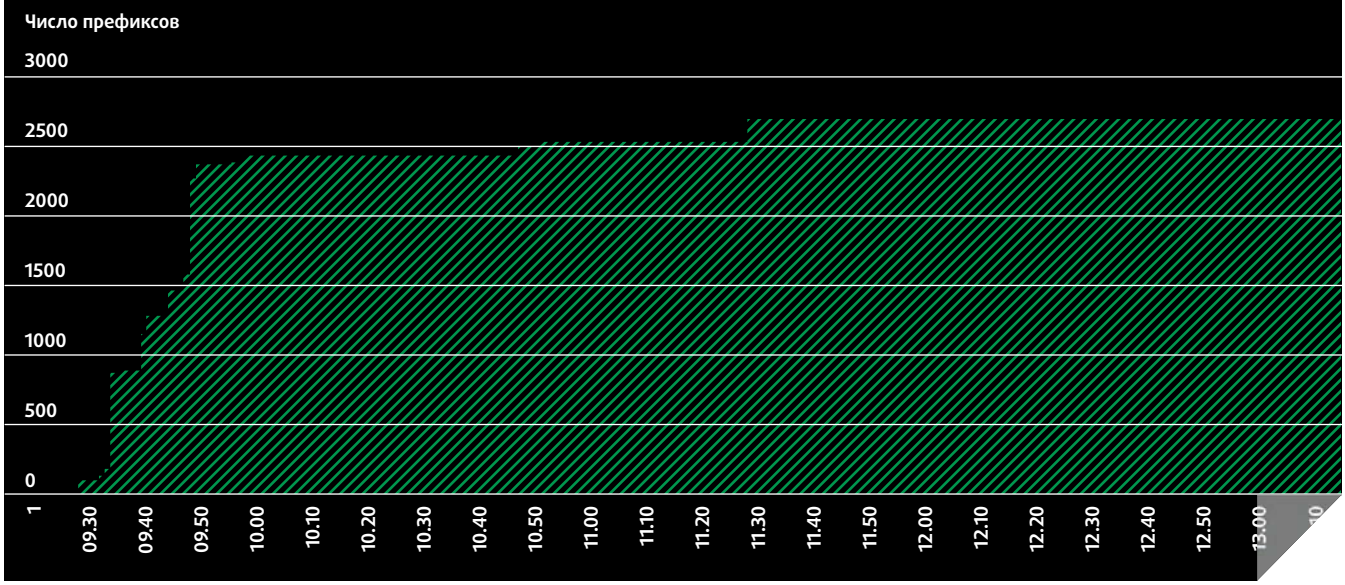
Интернет обрел невиданную силу. Значительная часть активных пользователей воспринимает сервисы массовой коммуникации, работающие на базе Интернета, — например, Twitter, Facebook, — как нечто само собой разумеющееся, как инструмент, встроенный в смартфон. Такое восприятие гарантирует легкое и естественное использование виртуального громкоговорителя, позволяющего элементарными методами поддерживать в режиме онлайн связь внутри группы из тысяч единомышленников. Ни радиосвязь, ни тем более другие дедовские методы революционеров вроде отправки гонцов-курьеров не идут ни в какое сравнение с новыми интерфейсами коммуникации.

Достаточно было оставить голосовое сообщение, дозвонившись на один из международных телефонных номеров (165 041 941 96, или 390 662 207 294, или 973 161 998 55), и далее служба, поддерживающая работоспособность данного сервиса, немедленно писала сообщения в Twitter, используя хэштег #egypt. Те, кто хотел бы ознакомиться с этими сообщениями, могли зайти на twitter.com/speak2tweet (как, впрочем, и сейчас может — сообщения на этой странице обновляются каждый час).

«Мы надеемся, что это хоть как-то поможет людям в Египте остаться на связи в столь трудное время. Наши мысли с ними», — сообщил Google, продавив очередной гибридный (офлайн-онлайн) сервис в среду, в которую чуть масла в огонь — и все... Вспыхнет так, что придется заботиться о дополнительных рейсах из Хургады или Шарм-эль-Шейха.

ИЛЛЮСТРАЦИИ: АНАСТАСИЯ УХИНА

Число видимых сетей в момент возвращения египетского сегмента Сети 2 февраля 2011 года



Источник RIPE NCC: stat.ripe.net/egypt

Интернет — это сила

Современность такова, что мало кто хочет отключать сильный Интернет (и готов, если что, его заменить чем-то похожим, главное, чтобы всегда — на связи). Речь о тех, у кого есть возможность это реально сделать, конечно. Интернет — ключевой транспорт для самой разной информации. Можно спорить о правилах, пытаться оттеснить друг друга от рычагов и штурвала. Но потерять Сеть — это только в самом крайнем случае, без всякого желания.

Но Интернет несравнимо мощнее, лучше, эффективнее этих старых «голосов». Глобальная сеть — интерактивная и позволяет организовать многосторонний обмен сведениями, новостями, информацией; позволяет построить обратную связь, собирать статистику в реальном времени. И при желании предоставляет все эти возможности каждому участнику. При одностороннем радиовещании такое просто невозможно. Более того, пользователи привыкли к механизмами коммуникации, которые работают на базе Интернета.

Египет очень быстро и успешно исчез из Интернета. Скорее всего, при этом нарушилась и связность локальной Сети. Причина — желание лишить революционеров средств коммуникации

Рубильники, «красные кнопки» — скорее инструмент устрашения, что-то из области доктрины стратегического сдерживания противников. Сама возможность отключения Интернета — это хороший козырь. Потому что принятие важных глобальных решений базируется на оценке именно возможностей другой стороны (а не ее «намерений», о которых твердят в прессе). Естественно, возможность должна быть реализуемой. Иначе элемент устрашения не сработает. Собственно, египетский вариант как раз и продемонстрировал на практике эффективность «красных кнопок».

У «зеленой кнопки» будет другая история. Здесь речь о принудительном внешнем навязывании Интернета на той или иной государственной территории. Можно вспомнить про «голоса» — радиостанции, вещающие с пропагандистскими целями на заданную территорию. Технология старая. В современном мире пропаганды ее реализуют на более высоком уровне: теперь вещать могут и радио-, и телевизионные станции, при этом передатчики возможно размещать на борту самолетов, на спутниках.

Конец первого десятилетия XXI века показал, что Интернет не просто информационный транспорт. Интернет — это механизм, позволяющий концентрировать и многократно увеличивать силу. Отключать Интернет где угодно можно, но не нужно. А вот взять в свои руки штурвал, получить возможность управлять — это годная стратегия. Если штурвал в руках, то на следующем шаге нужно позаботиться об инструментах, позволяющих продавливать информационное поле через границы офлайновых территорий, навязывать Интернет, если вдруг понадобится.

* * *

В общем, как показали последние события — как в офлайн-, так и онлайн-масштабах, — рассуждения скептиков о виртуальном «железном занавесе», который опустится на страны с введением многоязычных доменов (например, того же многострадального .РФ), — лишь теория. На практике — если и захотят отрезать государство от внешнего мира (в интернет-смысле), то отключат все и сразу. И международность статуса домена, локальность ли его характера — никакого значения для нажимающего на «красную кнопку» иметь не будут...

Род Бекстром, президент ICANN (запись из официального блога корпорации): «Операторы основных DNS-серверов .EG обратились с этой проблемой (отключения Сети. — Прим. ред.) в ICANN и через нас связались с операторами серверов вторичных, которые находятся за пределами страны, попросив их поддерживать существующий файл зоны, пока это необходимо»

RU center

www.nic.ru

Жизнь новая доменов исторических начинается

.net.ru

.pp.ru

.org.ru

Регистрация и продление

Слово за партнером

Многие из региональных партнеров RU-CENTER буквально выросли на наших глазах, превратившись в лидеров рынка. Наблюдать за их развитием — одно удовольствие, ведь партнерские связи давно переросли в дружеские.

Мы не выбирали RU-CENTER в качестве партнера, а получили его «по наследству» из РосНИИРОС. Но ничуть не в обиде на судьбу: за 10 лет сотрудничества RU-CENTER проявил себя надежным регистратором, помогал грамотно решать возникающие вопросы. Но по-настоящему партнерскую поддержку мы ощутили, когда начали проводить совместные семинары. Помимо того что мероприятия стали для нас важным маркетинговым инструментом, они позволили перейти на личный уровень в общении с RU-CENTER, что положительно сказалось на эффективности взаимодействия и по обычным рабочим вопросам. Особенно хочется поблагодарить в этой связи Федора Смирнова — как за частые визиты в наш город с докладами, так и за содействие в решении текущих вопросов.

Григорий Коган,
генеральный директор компании «Пиком» (Ижевск)

Компания «Хайтек Сервис» работает с RU-CENTER с 2005 года. В то время одним из основных направлений деятельности нашей компании была разработка веб-сайтов. А в этом деле очень важно подобрать хорошую площадку и интересное доменное имя. И мы выбрали в качестве компании — регистратора доменов — компанию RU-CENTER, одного из самых известных регистраторов на то время.

С развитием нашей компании у нас появляется новое направление — хостинг, или размещение сайта. И здесь уже без надежного регистратора было не обойтись. За все время сотрудничества с RU-CENTER у нас не возникало проблем с регистрацией и поддержкой доменов. Именно поэтому мы сотрудничаем с RU-CENTER по сегодняшний день.

Яна Белобородова,
исполнительный директор «Хайтек Сервис»(Пермь)

Евгений Молев,
генеральный директор компании Burbon.Ru (Нижний Новгород)

Если спросить у любой поисковой системы «регистрация доменного имени», то на самой первой строчке мы увидим компанию RU-CENTER. Это не случайно. RU-CENTER действительно первый среди аккредитованных в стране регистраторов доменных имен. Несмотря на широту возможностей, я всегда стараюсь регистрировать доменные имена исключительно в RU-CENTER. Меня не пугает разница в цене, так как гораздо важнее для меня надежность и качество обслуживания. Уверенность в работе с партнером — это гарантия, что наши собственные клиенты останутся довольны услугами, которые мы оказываем.

RU-CENTER — это не просто компания. Это всероссийский бренд. Сотрудничество с известной организацией придает определенный статус и ее партнерам. Мы поддерживаем все начинания RU-CENTER, участвуем в организации совместных мероприятий, которые всегда направлены на развитие рынка информационных технологий в России в целом, а значит — способствуют и нашему развитию как интернет-компании.

Первый зарегистрированный нами самостоятельно домен был еще в РосНИИРОС (RIPN). Вспомнить, какой именно, не удалось. Это пришлось на конец девяностых, когда нам потребовалось самостоятельно управлять доменами клиентов, которые периодически мигрировали от хостера к хостеру...

Потом (кажется, в 2000 году) была передача доменов на управление в АНО РСИЦ (под брендом RU-CENTER). Тогда же появилась очень интересная партнерская программа, удобный интерфейс управления, существенное снижение цен на услуги регистрации, приятная и оперативная техподдержка.

За более чем 10 лет совместного бизнеса мы ни разу не пожалели о сделанном выборе. RU-CENTER последовательно снижал цены на стоимость регистрации, расширял предложение по видам доменных имен, становился аккредитованным регистратором в популярных зонах (.COM, .INFO и другие), одновременно предлагая еще более низкие цены в своей партнерской программе.

Собственное доменное имя в зоне .RU (да и в других зонах) перестало быть роскошью и привилегией богатых. Практически любой российский бренд сегодня начинается с выбора удачного доменного имени, причем именно в зоне .RU.

На сегодняшний день все наши задачи по сопровождению доменов клиентов компания RU-CENTER успешно и быстро решает, предоставляя широкий ассортимент связанных услуг.

Отдельно хочется отметить и еще раз поблагодарить RU-CENTER за неоднократную поддержку при проведении нами региональных конференций и семинаров и делегирование на эти мероприятия своих ведущих специалистов.

От лица компании «Нэтбайт» (Netbyte) желаю компании RU-CENTER дальнейшего развития и процветания!

Игорь Андрианов,
генеральный директор компании «Нэтбайт» (Ставрополь)

С компанией RU-CENTER мы уже около трех лет успешно сотрудничаем в рамках совместного проведения семинаров для наших клиентов. Мы вместе привлекаем для участия представителей ведущих петербургских и московских интернет-компаний. В наших семинарах принимают участие руководители организаций, маркетологи, PR-специалисты и сотрудники рекламных отделов.

Отзывы участников говорят сами за себя: слушатели благодарят за интересную и актуальную для них информацию, связанную с продвижением их бизнеса в Интернете; RU-CENTER делится полезной информацией о правилах регистрации и защите доменов, а также о хостинге; специалисты Trinet приводят практические советы по созданию и продвижению интернет-проекта, анализу его эффективности. С коллегами из RU-CENTER всегда очень комфортно работать, так как мы с полуслова понимаем, как лучше наладить каждый процесс для проведения максимально эффективного для всех участников мероприятия. В ближайшие годы мы надеемся только развивать и укреплять сложившиеся благоприятные отношения для дальнейшего развития петербургского интернет-рынка.

Яна Ширикова,
PR-менеджер интернет-агентства Trinet (Санкт-Петербург)

Борис Беланов,
генеральный директор компании IntelSib (Новосибирск)

Компания IntelSib уже более двух лет тесно сотрудничает с RU-CENTER, и за это время никогда не было никаких нареканий — все быстро и оперативно. Нам и нашим клиентам приятно сотрудничать с такой крупной и клиентоориентированной компанией, которая является лидером в своей сфере. Просветительская деятельность в рамках общероссийских семинаров «Гуру про Интернет» принесла нашей компании немало клиентов и увеличила популярность в Сибирском регионе.

Дмитрий Батраков,
генеральный директор интернет-агентства Dextra (Челябинск)

Работаем с компанией RU-CENTER уже более 9 лет, с 2001 года. Очень радует постоянное совершенствование уровня обслуживания: развитие партнерских отношений, упрощение документооборота, улучшение работы сайта и введение новых сервисов, существенно облегчающих регистрацию доменов. С готовностью поддерживаем все начинания, рады развивать отношения за счет региональных мероприятий. Успехов!

Михаил Квачко,
руководитель интернет-агентства «Мибок» (Ростов-на-Дону)

При выборе регистратора доменных имен для наших клиентов нас прежде всего волновала гарантированность и качество оказываемых услуг. Сегодня на рынке доменных имен можно увидеть разницу в цене в несколько сотен рублей за регистрацию или продление регистрации доменного имени у разных регистраторов. Но в данном случае попытка сомнительной экономии не покрывает рисков: она никак не окупит тех проблем, которые могут возникнуть у владельца домена в случае некорректной работы или, не дай бог, прекращения работы регистратора.

За 10 лет сотрудничества с RU-CENTER мы убедились в надежности этой компании как поставщика услуг и ее динамичности. RU-CENTER занимает активную позицию на рынке, развивает его, повышает осведомленность населения, проводя семинары по городам России, расширяет линейку услуг. В общем, постоянно двигается вперед.

Благодарим за сотрудничество! Так держать!


ПРЕСС-ЦЕНТР


Доменные имена

Экология души

7 октября 2010 года в Центральном доме журналиста прошла презентация журнала «Доменные имена». Собравшиеся узнали о содержании очередного номера, о планах редакции на будущее, о новом оформлении издания. В рамках мероприятия удалось успешно совместить рассказ о журнале «Доменные имена» с литературными чтениями. А в финале эволюцию Интернета обсудили в рамках круглого стола. Дискуссия получилась довольно живой.

Поделимся отзывом одного из читателей журнала, который присутствовал на круглом столе. Итак, впечатления Георгия Асеева.

«К знаменательным событиям культурной жизни столицы по праву можно отнести презентацию журнала «Доменные имена. Осень 2010», состоявшуюся 7 октября этого года в Центральном доме журналиста на Никитском бульваре в Москве.

Презентация проводилась молодыми, преуспевающими на рынке IT-технологий интеллектуалами из компаний-организаторов: RU-CENTER — национальный регистратор доменов, издательский дом «Афиша», Русский литературный клуб, «ИКС-Холдинг» — ведущая издательская компания.

Квинтэссенция заключалась в гармоничном сочетании разноплановых мероприятий, проходивших в соседних роскошных залах старинного особняка: литературного вечера «Эволюция Интернета», круглого стола «Будущее системы адресации Интернета и эволюция Сети» и неформального (с аперитивом под звуки классической музыки в исполнении солистов Большого театра) общения читателей журнала «Доменные имена».

Футурологические, полемические выступления участников круглого стола побудили меня к серьезным размышлениям о роли творчества в нашей жизни.

Интернет — средство доставки информации. Развитие Рунета — перспективный бизнес. Всплеск активности по созданию и регистрации региональных геодоменов и корпоративных доменов ожидает в ближайшее время мировое сообщество.

Непрерывно возрастающий объем передаваемой СМИ «достоверной» информации по интерпретации какого-либо события или толкованию явления искажает благую суть земного бытия, создает виртуально-релятивистскую псевдореальность. Цвет (мрак или свет) окружающего мира есть зеркальное отражение нашей души.

Если мысли материализуются, то для всеобщего блага в условиях развития «субкультурного глобализма» нужен консенсус «в мире понятий и абсолютных истин».

Национальные культурно-лингвистические порталы, такие как Стихи.ру и Проза.ру, являются «жизнеутверждающими кровотоками», питающими здоровый организм народа и осуществляющими миссию духовного обустройства России — основы национального единства нашего Отечества. Пример тому — паломничество для авторов Стихи.ру и Проза.ру на Вяземское (тут проходили самые ожесточенные сражения осени 1941 года, в результате которых Красная армия и народное ополчение понесли крупные потери) ратное поле, где епископ Смоленский и Вяземский Феофилакт совершит освящение основания первого каменного Покровского храма будущего Одигитриевского женского монастыря.

Рунет — окно в мир правды и добра, должен стать эталоном «экологии души»!»

Георгий Асеев,
член Русского литературного клуба,
читатель журнала «Доменные имена»
2010

Несколько слов по теме

В ходе инициированной Министерством экономики и коммуникаций Эстонии реформы регистрационных правил в домене страны из Сети исчезло порядка 80% сайтов, адреса которых заканчивались суффиксом .EE.

В DNS появится новый национальный домен SX. В декабре 2010 года данный код был закреплен за островным государством Синт-Мартен, образовавшимся после раскола Нидерландских Антильских островов.

В марте 2011 года, через семь лет после запуска, домен для лицензированных специалистов PRO пересек символическую отметку в 100 тыс. регистраций

Компания Hitachi, производитель бытовой техники, планируется подать заявку на «одноименный» домен .HITACHI сразу после того, как ICANN начнет их принимать в рамках программы New gTLD.

1 марта 2011 года ICANN сообщила, что за Украиной забронирован национальный кириллический домен верхнего уровня УКР. В настоящее время домен УКР находится на стадии подготовки к делегированию.

Компания VeriSign выпустила новый статистический сервис Domain Tag Cloud, предлагающий информацию о наиболее популярных ключевых словах, используемых при регистрации доменных имен в.COM и.NET.

Отчет компании VeriSign «Domain Name Industry Brief» о развитии доменной индустрии в 2010 году сообщает, что к началу 2011-го в мире насчитывалось более 205 млн доменных имен.

Открыть регистрацию в домене XXX планируется в течение 2011 года. На данный момент подано более 300 тыс. предварительных заявок на .XXX

2 марта 2011 года домен ORG преодолел рубеж в 9 млн имен. Кроме того, с 2011-го в .ORG можно регистрировать домены на 20 языках мира, в том числе и на русском.

В колумбийском домене CO завершилась интеграция набора спецификаций, обеспечивающих безопасность информации, предоставляемой средствами DNS в корневую зону Интернета, — так называемого протокола DNSSEC.

Африка теперь претендует не только на домен .AFRICA, но также на его французский аналог — .AFRIQUE — и подумывает над его арабским вариантом. Это должно учесть интересы многоязычного населения континента.

Домен Sex.com, который был продан в ноябре 2010 года за $13 млн, попал в Книгу рекордов Гиннесса как «Самое дорогое доменное имя»