НОМЕР 2(29)
МАЙ-ИЮНЬ
2017

СЕРГЕЙ ПЛУГОТАРЕНКО
ЕЛЕНА ВОРОНИНА
АЛЕКСЕЙ ПЛАТОНОВ
АЛЕКСАНДР ВЕНЕДЮХИН
ОЛЕГ ДЕМИДОВ
ВИКТОРИЯ БУНЧУК

12+

интернет

в цифрах

www.in-numbers.ru

Состояние безопасности

R:TA РАЭК

SOCIAL MEDIA MOSCOW

КОНФЕРЕНЦИЯ 12 ВДОХНОВЛЯЮЩИХ SMM КЕЙСОВ

7 ИЮНЯ, 10:00
ПРЕМЬЕРНЫЙ ЗАЛ К/Т «ОКТЯБРЬ»

СОДЕРЖАНИЕ

ЖУРНАЛ «ИНТЕРНЕТ В ЦИФРАХ»

Сайт журнала
www.in-numbers.ru
InNumbers Daily
www.facebook.com/innumbers

Главный редактор / Карен Казарян

Редактор / Ярослав Капустинский

Дизайн / Александр Груздев

Авторы / Карен Казарян / Ярослав Капустинский / Сергей Алимбеков / Олег Демидов / Антон Мелехов / Виктория Бунчук / Александр Венедюхин / Михаил Анисимов / Марина Рожкова / Дмитрий Афанасьев / Ирина Пыжова / Сергей Горбунов / Игорь Лидин / Денис Жилин / Дмитрий Дениськин / Сергей Плуготаренко

В журнале использованы материалы / РАЭК / ОСС/ Google / Qrator Labs / ФРИИ / Mediascope / Akamai / TheRunet / BuduGuru / ТЦИ / Qrator labs / КЦ .RU/.РФ / RTB House

В журнале использованы материалы с Freepik.com

Экспертная поддержка / Институт развития Интернета / РАЭК (Российская Ассоциация эллектронных коммуникаций)

Подписка на сайте
www.in-numbers.ru
По вопросам размещения рекламы пишите на
adv@in-numbers.ru

ВЫХОДНЫЕ ДАННЫЕ

Название издания:
«Интернет в цифрах»
Издатель: Ассоциация электронных коммуникаций (РАЭК)
Учредитель: Общество с ограниченной ответственностью «Интернет Медиа Холдинг»
Главный редактор (редактор):
Казарян К. Р.
Порядковый номер выпуска и дата его выхода в свет:
Выпуск № 29, дата выхода: май 2017 г.
Тираж: 1 500 экземпляров
Бесплатно
Адрес редакции и издателя:
123100, г. Москва, Набережная Пресненская, д. 12
Адрес типографии:
115114, г. Москва, Дербеневская наб., д. 7, стр. 2

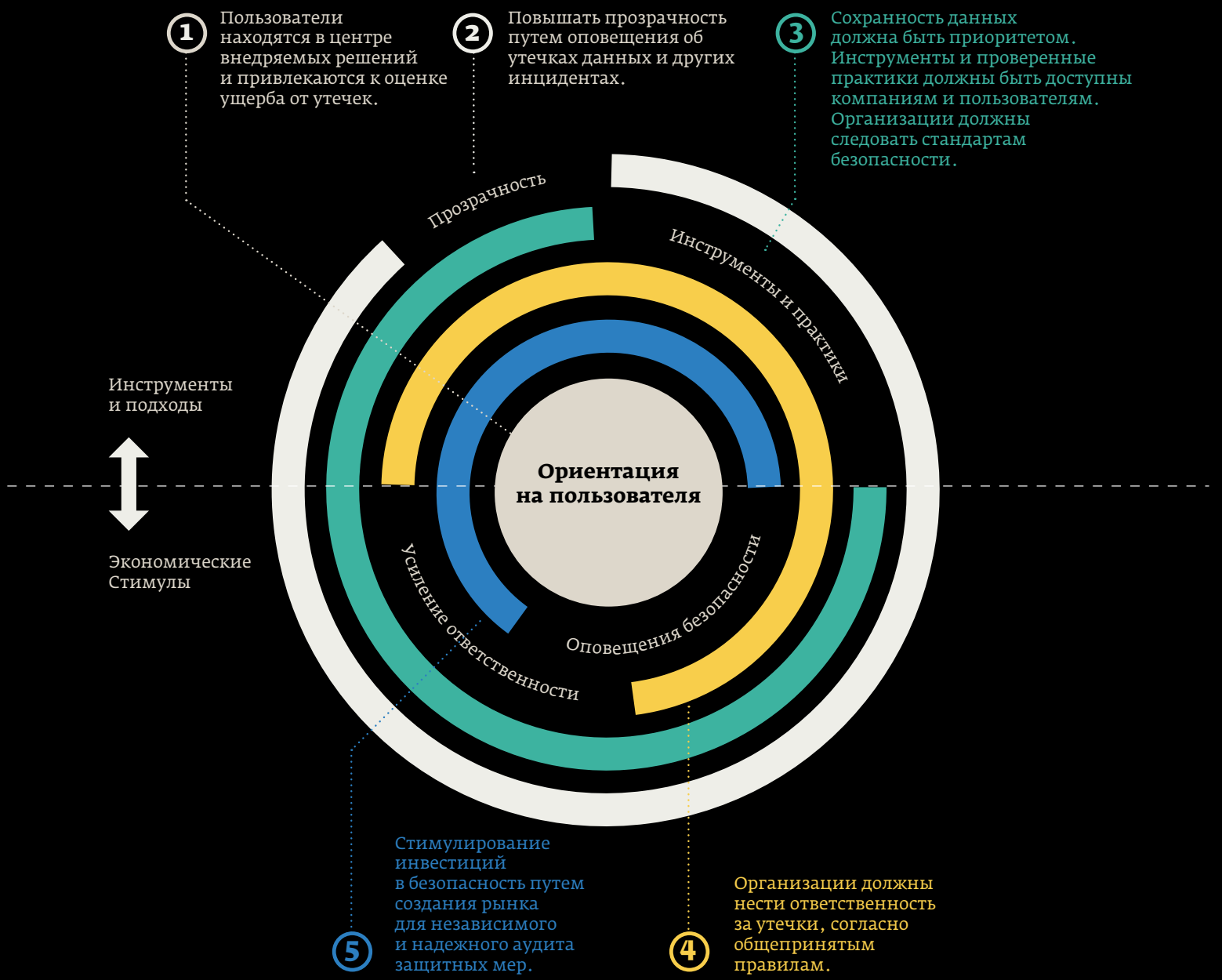
Журнал **«Интернет в цифрах»** зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Регистрационный номер ПИ № ФС 77–37895 от 19 октября 2009 г. (СМИ перерегистрировано в связи со сменой учредителя, регистрационный номер **ПИ № ФС77–42452** от 25 октября 2010 г.).

Редакция не несет ответственности за содержание рекламных материалов.

12+


do simple.
do smart.
BANDA
WWW.THEBANDA.RU
*ПРОСТЫЕ И УМНЫЕ ЛЕНДИНГИ
РЕКЛАМА

Основы безопасности



Говорить про важность кибербезопасности в условиях цифровой трансформации кажется уже банально, но тенденции к улучшению ситуации, к сожалению, не видно. Производители продолжают выпускать незащищенные устройства, которые взламываются через несколько минут после первого выхода в сеть. Ботнеты интернета вещей организуют гигантские ddos-атаки на объекты инфраструктуры глобального интернета, а эксперты прогнозируют еще более масштабные утечки данных. Но кажется, вопросы безопасности волнуют правительства в основном для закручивания гаек регулирования интернета, а не восстановления доверия. И даже спецслужбы занимаются эксплуатацией дыр в безопасности, а не их устранением.

Этот номер мы сделали совместно с Координационным центром национальных доменов .RU и .РФ. Управление интернетом координирующими организациями всегда было построено на принципах доверия и включения всех заинтересованных сторон. Так что неудивительно, что именно на этом уровне, чуть ли не единственном, ведется диалог между различными сторонами о том, как сделать интернет безопаснее, и сохранить при этом его базовые принципы, такие как свобода информации. Остается надеяться, что правительства придут к пониманию необходимости такого диалога раньше, чем инциденты в киберпространстве начнут приводить к человеческим жертвам.

Спасибо за внимание к Цифрам!

Карен Казарян, главный редактор

ЦИФРЫ КОРОТКО

АПРЕЛЬ

Комиссия Российского союза промышленников и предпринимателей (РСПП) по связи и информационно-коммуникационным технологиям подготовила заключение на доработанный Минкомсвязью проект постановления по реализации «закона Яровой». Предлагаемый Минкомсвязью способ реализации «закона Яровой» в несколько раз увеличивает потенциальные расходы, уверены в РСПП. На момент принятия закона операторы оценивали общий объем хранимой по нему информации в 157,5 эксабайт, а общие затраты на исполнение требований — в 5,2 трлн руб. По правилам же Минкомсвязи, с 1 января 2019 года объем хранимой информации только для одного крупного оператора может достигнуть около 20 эксабайт, что потребует примерно 1 трлн руб. Общие расходы всех участников рынка достигнут примерно 10 трлн руб.

Исследователи из Нью-Йоркского университета (NYU) и Университета штата Мичиган (MSU) доказали, что сканер отпечатков пальцев в смартфоне можно обойти при помощи современных технологий. Они создали «супер-отпечатки» (master prints), с помощью которых удалось пройти проверку сканера в 65% случаев. Дело в том, что сканеры на смартфонах довольно маленькие. Они сверяют только части отпечатка, а не весь рисунок. Это сделано для того, чтобы телефон можно было разблокировать одним прикосновением. Таким образом, для доступа к данным нужна лишь часть отпечатка. При этом многие люди используют в качестве ключей к одному устройству несколько пальцев, что еще больше увеличивает количество подходящих комбинаций. Ученые объединили части рисунков многих отпечатков в «супер-отпечатки». Каждый может имитировать пальцы нескольких людей.

Аналитики из Zendrive подсчитали, насколько часто американские водители используют свои смартфоны. За время исследования 3,1 млн человек, чьи данные об использовании телефона учитывала компания, успели проехать 9 млрд км пути. Выяснилось, что в 88% поездок водитель хотя бы раз отвлекался на свой смартфон. В среднем, за каждый час, проведенный в дороге, пользователи тратили на мобильное устройство 3,5 минуты или 5,8% времени. Отмечается, что в 6 из 10 штатов, где доля использования смартфонов минимальна, есть некие законы, ограничивающие использование смартфонов за рулем.

Министр связи и массовых коммуникаций РФ Николай Никифоров рассказал о прогрессе программы по устранению цифрового неравенства и о росте мобильной экономики в РФ. По словам министра, цифровая экономика делает важный вклад в рост экономики России и задача государства состоит в том, чтобы его ускорить. К настоящему моменту проект охватил 71 регион РФ. К сети подключено 4 тысячи населенных пунктов. Уже построено более 34 тыс. км оптики в маленькие населенные пункты. При этом стоимость доступа в интернет остается на достаточно низком уровне относительно других стран. Стоимость подключения со скоростью 10 Мбит/с составляет всего 45 рублей в месяц. В России по данным на конец 2016 года работало 120 тысяч базовых станций формата LTE.

МАЙ

Большинство российских пользователей, а именно, 91,5% предпочитают оплачивать товары и услуги онлайн. Об этом свидетельствуют данные исследования компании Mediascope. Отмечается, что 85,7% используют для этого компьютеры и ноутбуки, а 68,3% — смартфоны. Мобильные устройства

для денежных переводов в 2017 использует на 8,6% больше людей, чем в 2016. Доля тех, кто использует смартфоны для платежей по штрафам ГИБДД и налогам, выросла на 5,8%, для оплаты ЖКУ — на 5,3%. Другими словами, оплата через смартфоны набирает популярность, кроме того, с помощью мобильных приложений платят на 60% больше пользователей, чем через мобильные версии сайтов. 83% опрошенных хотя бы раз в год производят оплату с помощью интернет-банкинга, почти столько же, 82,8% расплачиваются банковскими картами, а 66,3% — электронными деньгами. Большинство оплачивает товары и услуги через Сбербанк Онлайн, на втором месте — банковские карты, а на третьем —Яндекс.Деньги. Также в пятерку лидеров вошли WebMoney и Qiwi. Бесконтактный способ оплаты со смартфона оказался на 10 месте. Через Apple Pay и Samsung Pay оплачивают 8,6% респондентов. В основном пользователи оплачивают с их помощью заказы в интернет-магазинах и доставку еды, третье место по популярности занимают сотовая связь и ЖКУ, также через такие сервисы часто производят денежные переводы.

Snap опубликовал данные о доходах впервые после размещения акций на бирже в начале марта. Количество ежедневных пользователей приложения выросло до 166 млн человек. Это на 5% больше, чем в прошлом квартале, но меньше, чем у Instagram Stories. Аудитория сервиса, который, по сути, является клоном Snapchat, составляет 200 млн. Финансовые показатели компании при этом выросли, доходы увеличились на 300% и составили $150 млн в первой четверти финансового года. Эта цифра оказалась ниже ожиданий аналитиков, на Уолл-стрит предсказывали цифру в $158 млн. При этом убытки компании более чем удвоились — до $2,2 млрд. По итогам торгов стоимость ценных бумаг компании снизилась на 25%.

Выступая на конференции Google I/O, исполнительный директор компании Сандар Пичай (Sundar Pichai) сообщил, что в начале недели количество ежемесячно активных пользователей платформы Android перевалило за 2 млрд, закрепляя за ней статус самой популярной мобильной операционной системы в мире. Прирост составил 400 млн пользователей со времени последней статистической сводки в сентябре 2015 года. Для сравнения, в январе 2016 года Apple объявила о миллиарде устройств (не пользователей), работающих под управлением iOS.

---

12 мая по всей планете началось мгновенное распространение вируса Wanna Cry. Меньше чем за два часа заражение было обнаружено в 11 странах мира: России, Великобритании, США, Китае, Испании, Италии, Вьетнаме, Тайване. К вечеру пятницы было зафиксировано 45000 попыток атак в 74 странах мира. Атакам подверглись около 40 клиник в Англии и Шотландии и одна из крупнейших телекоммуникационных компаний Испании Telefonica. Масштабное заражение произошло в России — о проблемах сообщали в Мегафоне, МВД (в ведомстве подтвердили блокирование порядка 1000 компьютеров).

Wanna Cry представляет собой программу под названием WanaCrypt0r 2.0, которая атакует исключительно ПК на ОС Windows. Программа использует для проникновения «дыру» в системе — Microsoft Security Bulletin MS17–010. По словам экспертов, с программой был совмещен шпионский инструмент Агентства национальной безопасности США (АНБ) ETERNALBLUE, который был выложен в открытый доступ хакерами Shadow Brokers 14 апреля 2017 года. Это не первый случай: с помощью одного из инструментов АНБ — бэкдора DOUBLEPULSAR из утечки Shadow Brokers хакерам удалось заразить более 47000 компьютеров ОС Windows в США, Великобритании, на Тайване. Из-за особенностей вируса, распространяющегося преимущественно в локальных сетях, от него, в основном, пострадали компании и государственные структуры. Под удар вируса попали телекомкомпании, железные дороги, организации здравоохранения, университеты, отделения почты, шоппинг-центры, офисные здания. По данным полиции ЕС, к 14 мая от вируса пострадали более 200 тысяч пользователей в 150 странах мира, включая Россию. В понедельник, 15 мая, атаки продолжились. Китай заявил о заражении в более чем 29 тыс. организаций. О большом числе кибератак сообщила Индия. В Европе, по данным Европола, распространение вируса стабилизировалось, несмотря на воскресный прогноз о возможном ухудшении ситуации в связи с массовым выходом сотрудников на работу в понедельник. Однако представители британской разведки посоветовали коммерческим организациям готовиться к новой масштабной кибератаке, которая может начаться на следующей неделе. Специалисты в области кибербезопасности считают, что более 1,3 миллиона компьютерных систем до сих пор уязвимы перед вирусом Wanna Cry.

Звезды YouTube вытесняют ТВ-кумиров, а сам YouTube заменяет молодым поиск в интернете, говорится в новом исследовании-сравнении российских миллениалов (Y) и центениалов (Z), проведенным международным коммуникационным агентством PBN H+K совместно с независимой исследовательской компанией MAGRAM MR. Один из главных выводов исследования — YouTube является ключевой платформой для поиска и потребления контента среди поколения Z практически по всем категориям. Если поколение Y информацию по темам ЗОЖ, технологии, бизнес еще продолжает искать в обычном интернет-поиске, то поколение Z по этим темам переехало на YouTube. Что важно — даже новости центениалы узнают на YouTube (46%). Миллениалы тоже не отстают от трендов: 40% опрошенных предпочитают получать новости на YouTube, здесь же они смотрят развлекательный контент (49%) и видео о технологиях (45%).

АНАЛИЗ МОБИЛЬНОЙ ИНТЕРНЕТ-ЭКОНОМИКИ В РОССИИ

ДАННЫЙ НЕЗАВИСИМЫЙ ОТЧЕТ БЫЛ ПОДГОТОВЛЕН КОМПАНИЕЙ OC&C STRATEGY CONSULTANTS, УПОЛНОМОЧЕННОЙ GOOGLE РОССИЯ ДЛЯ ИССЛЕДОВАНИЯ И ОПРЕДЕЛЕНИЯ РАЗМЕРА МОБИЛЬНОЙ ИНТЕРНЕТ-ЭКОНОМИКИ В РОССИИ СОВМЕСТНО С РАЭК. ИНФОРМАЦИЯ, ПРЕДСТАВЛЕННАЯ В НАСТОЯЩЕМ ДОКУМЕНТЕ, КОТОРАЯ МОЖЕТ ВКЛЮЧАТЬ РЕКОМЕНДАЦИИ, ПОДГОТОВЛЕНА И ПРЕДНАЗНАЧЕНА ДЛЯ ИСПОЛЬЗОВАНИЯ В КАЧЕСТВЕ ОБСУЖДЕНИЯ СПОСОБОВ ПОДДЕРЖКИ РОСТА МОБИЛЬНОЙ ИНТЕРНЕТ-ЭКОНОМИКИ.

I. ВКЛАД МОБИЛЬНОЙ ИНТЕРНЕТ-ЭКОНОМИКИ В РОССИЙСКИЙ ВВП И ЭКОНОМИЧЕСКИЙ РОСТ

Мобильная интернет-экономика — хотя и значительная по объему — обычно не отслеживается как отдельное направление экономической деятельности на рынке. Чтобы правильно оценить мобильную интернет-экономику, необходимо дать определение всей экосистеме мобильного интернета; в данном случае предлагаемое нами определение, включающее три слоя, является исчерпывающим и выходит за пределы того, что нам известно из деятельности самых известных мобильных компаний.

Слой 3 — Косвенный вклад

Прирост бизнеса: Коммерческие компании, деятельность которых стала возможной или более эффективной благодаря мобильным технологиям

Продажи/повышение эффективности работы компаний (предприятий малого и среднего бизнеса и промышленных предприятий) от других сегментов благодаря использованию мобильного интернета (например, бутики, водители такси и пр.) могут рассматриваться как «элемент» слоя 3

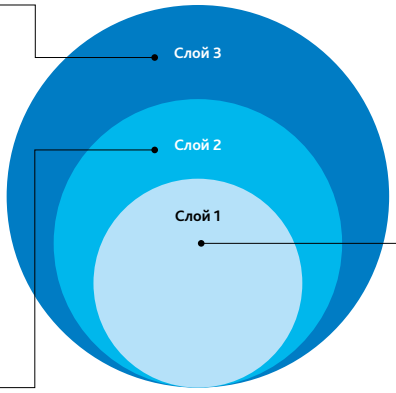
QIWI, Яндекс Деньги, Сбербанк, Delivery Club, Gett, Яндекс Такси.

Слой 2 — Косвенный вклад

Поставщики и провайдеры услуг для Слоя 1

Вспомогательные компании, которые поставляют продукцию/оказывают услуги ключевым компаниям – себестоимость реализованной продукции и операционные расходы Слоя 1 (выручка Слоя 2)

Microsoft, Staffline, Oracle, PWC, SAP, HH карьера.



Слой 1 — Прямой вклад

Прямой вклад мобильной экономики в ВВП

Слой 1 — ядро мобильной экосистемы — может быть разбит на ряд элементов, где тот или иной элемент является стержнем мобильной экосистемы. Добавленная стоимость, генерируемая данными компаниями, вносит прямой вклад в ВВП

- **Семейство элементов, связанных с устройством:** Изготовители устройств производят устройства, а поставщики операционной системы предоставляют операционную систему для того, чтобы устройство функционировало. Потребитель получает доступ к устройству через магазины, принадлежащие производителям устройств или через продавцов-посредников.
- **Семейство элементов, относящихся к связи:** Устройство «присоединяется» к «внешнему миру» посредством голосовой связи, текстовых сообщений или данных, предоставляемых мобильными операторами или поставщиками интернет-услуг и поставщиками инфраструктуры.
- **Семейство элементов, связанных с контентом:** Владелец устройства получает доступ в интернет через мобильные приложения, созданные разработчиками мобильных приложений и усовершенствованные провайдерами контента и компаниями, занимающимися мобильной коммерцией — эти приложения либо заранее установлены, либо скачиваются из магазинов приложений, в то время как компании, занимающиеся мобильной коммерцией, продают свою продукцию/услуги при помощи мобильного телефона.

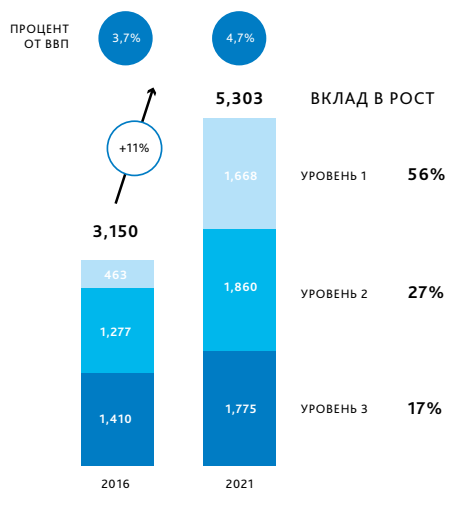
МТС, Эльдорадо, Связной, Евросеть, Ozon.ru, Yandex, Google, Apple.

1. **Слой 1, прямой вклад в ВВП, состоит из компаний, названия которых обычно приходят на ум, когда мы думаем о мобильной экономике. Это компании, предоставляющие устройства, связь и контент потребителям и коммерческим компаниям.**
   - **Семейство элементов, связанных с устройством**, производит мобильные устройства и создает операционные системы, обеспечивающие их работу, и, в конечном счете, поставляет готовое устройство клиентам. Производители устройств, провайдеры операционных устройств и розничные распространители электронных устройств — все это элементы данного семейства.
   - **Семейство элементов, относящихся к связи**, основано на возможности связи устройства с реальным миром посредством голосовой связи, текстовых сообщений или иного доступа к данным. Сетевые и инфраструктурные компании подготавливают то, что физически необходимо операторам мобильной связи и поставщикам интернет-услуг для обеспечения связи посредством своей инфраструктуры и внутренних систем связи. Дилеры операторов мобильной связи ответственны за дальнейшее оказание этих услуг через магазины, где можно приобрести сим-карты мобильных операторов или другие устройства связи. Операторы мобильной связи и поставщики интернет-услуг затем оптимизируют подключение и управляют подключением мобильного устройства через свои сети. Сюда включена часть деятельности поставщиков интернет-услуг, поскольку мобильные устройства могут быть подключены к их услугам через Wi-Fi, сеть и инфраструктуру, операторов мобильной связи, поставщиков интернет-услуг и операторов мобильной связи.

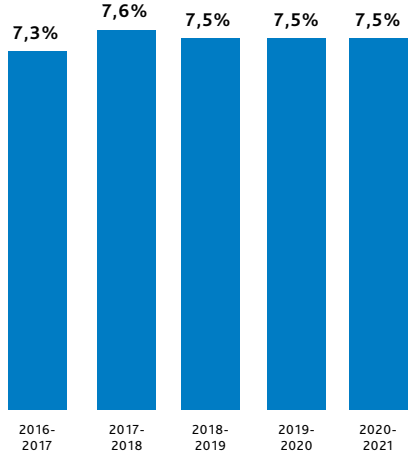
- **Семейство элементов, связанных с контентом**, в значительной мере зависит от приложений, созданных разработчиками мобильных приложений и усовершенствованными провайдерами контента и компаниями, занимающимися мобильными розничными продажами. Провайдеры контента извлекают финансовую выгоду из своей продукции посредством рекламы, покупок внутри приложений, подписок или одноразовой бесплатной загрузки. В то же время организации, занимающиеся мобильными розничными продажами, могут продавать свои услуги и продукцию с помощью мобильных телефонов. К этому семейству принадлежат компании, занимающиеся мобильными розничными продажами, компании по контенту и рекламе, разработчики игр, провайдеры контента, разработчики приложений и магазины приложений.

1. **Слой 2 участвует в косвенном вкладе в экономику и состоит из поставщиков и провайдеров услуг, которые обслуживают компании Слоя 1.** Поставщики предоставляют сырье, которое закупается и учитывается как себестоимость реализованной продукции компаний Слоя 1. Некоторые секторы, в рамках данного элемента, существуют только для того, чтобы обслуживать компании Слоя 1, поэтому поставщики образуют с ними симбиоз; они сильно зависят от их присутствия и роста. Поставщики сим-карт, изготовители запчастей и пр.— всего лишь несколько примеров таких компаний-поставщиков.
2. **Слой 3 представляет собой последний слой непрямого вклада мобильной интернет-экономики в общую экономику (ВВП)**. Он включает в себя **доходы от повышения эффективности работы и дополнительную выручку, получаемую предприятиями малого и среднего бизнеса и промышленными предприятиями благодаря существованию мобильных устройств**. Хотя и менее очевидный, чем Слой 1 и Слой 2, этот слой обеспечивает самый большой вклад в ВВП, поскольку он влияет на все дополнительные выгоды для бизнеса или государства, полученные от всех уровней экономики благодаря использованию мобильных технологий.

Мобильная интернет-экономика, 2016-2021 гг. (прогноз)
Источник: Росстат, вторичное исследование, финансовая отчетность компаний, анализ ОС&С



Доля мобильной экономики в росте ВВП
Источник: анализ ОС&С



Эта экосистема со всеми ее слоями формирует мобильную интернет-экономику, которая, в свою очередь, вносит существенный вклад в российскую экономику и, в числе других экономических активностей, будет становиться более значимой впоследствии, а также увеличивать свое воздействие на российский ВВП. Недавно проводившееся исследование OC&C Strategy Consultants при поддержке РАЭК показало, что доля мобильной экономики в ВВП, согласно ожиданиям, увеличится с 3,7% в 2016 г. до 4,7% в 2021, включая все указанные выше слои. Для некоторых станет неожиданной информация, что большая часть роста придется на косвенный вклад (Слой 3), т.е. коммерческие предприятия, которые были созданы/усовершенствованы/выросли благодаря существованию мобильных технологий.

В период с 2016 по 2021 гг. более 7,5% роста ВВП будет обусловлено исключительно мобильной интернет-экономикой. Рост ВВП в России в 2016–2021 гг. ожидается на уровне 6,0% (МВФ), при этом мобильная интернет-экономика вырастет на 10,7%.

СРАВНЕНИЕ ПО СЕКТОРАМ И В МЕЖДУНАРОДНОМ КОНТЕКСТЕ

В 2016 г. мобильная экономика занимала 11 место в России среди сфер экономической деятельности по объему, при этом другие направления экономической деятельности имели гораздо менее благоприятные прогнозы развития. Так, например, мобильная интернет-экономика опережает сельское хозяйство по объему вклада (4,5% в 2016 г.)

Источник: Росстат

ОТРАСЛЬ ЭКОНОМИКИ	ВКЛАД В ВВП
Операции с недвижимым имуществом	**17,2%**
Торговля	**16,0%**
Производство	**13,7%**
Добыча полезных ископаемых	**9,4%**
Государственное управление и обеспечение военной безопасности; социальное обеспечение	**7,9%**
Транспорт и связь	**7,8%**
Строительство	**6,2%**
Сельское, лесное хозяйство, охота, рыболовство и рыбоводство	**4,5%**
Финансовая и страховая деятельность	**4,5%**
Здравоохранение и социальные услуги	**3,8%**
Электроэнергия, газо- и водоснабжение	**3,1%**
Образование	**2,6%**
Прочие услуги	**1,7%**
Гостиницы, общественное питание	**0,8%**

Доля мобильной экономики в 2021 4,7%

Доля мобильной экономики в 2016 3,8%

Как абсолютная величина, размер российской мобильной интернет-экономики больше, чем ВВП большинства стран — например, в 2016 г. российская мобильная интернет-экономика по объему была равна всему ВВП Белоруссии (и около 15% ВВП Израиля в 2016 г.)

Общий объем ВВП в 107 из 190 стран мира ниже, чем отдельно взятая мобильная интернет-экономика России.

ВВП по странам, 2016 г.
Источник: МВФ, анализ ОС&С

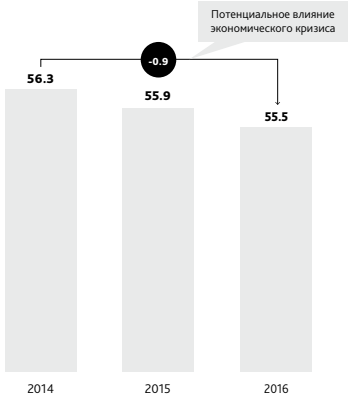
1. США	**18,561**
2. Китай	**11,392**
3. Япония	**4,730**
4. Германия	**3,495**
5. Россия	**1,268**
6. Израиль	**312**
7. Украина	**87,2**
8. Беларусь	**48,1**
9. Словения	**44,1**
10. Литва	**42,8**
11. Азербайджан	**35,7**

$48,2 млрд
Мобильная экономика России

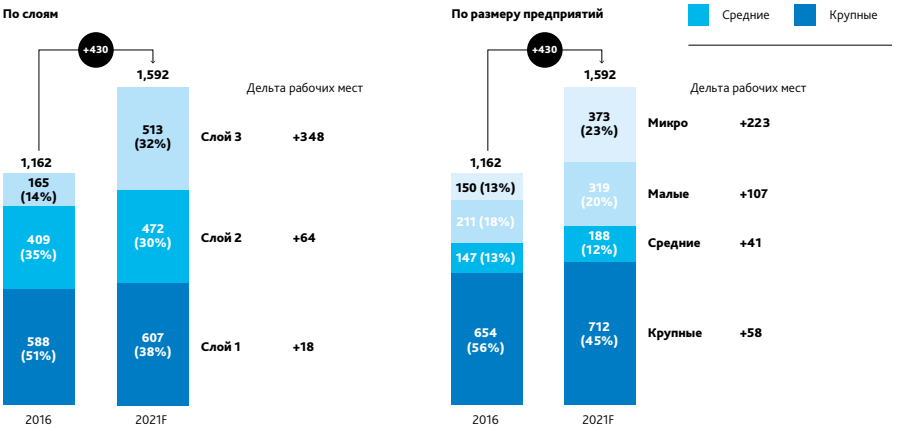
СОЗДАНИЕ РАБОЧИХ МЕСТ

Экономический спад, наблюдаемый в России в последние несколько лет, привел к увеличению количества безработных примерно на 0,9 млн (согласно данным Росстата — для юридических лиц и индивидуальных предпринимателей, т.е. исключая государственную и бытовую деятельность) в 2014–2016 гг., однако мобильные технологии способны оказать помощь и создать 430 тыс. дополнительных рабочих мест в ближайшие 5 лет, и около 350 тыс. из них будут связаны с компаниями слоя 3 (существует экосистема мобильного интернета, которая состоит из компаний, распределенных по различным слоям); компании 3-го слоя стимулируются исключительно мобильными технологиями и представляют собой, в основном, предпринимателей и микробизнес. Говоря коротко, мобильная экономика сама по себе ликвидирует почти половину этой потери.

Количество работающих по найму в России
Источник: Росстат, анализ ОС&С



Кол-во рабочих мест, создаваемых мобильной интернет-экономикой в 2016-2021 гг. (прогноз), тыс. *Источник: Росстат, GSMA, Euromonitor, Statista, кабинетные исследования, анализ ОС&С*



II. УНИВЕРСАЛЬНЫЙ ДОСТУП/ ДОСТУП ДЛЯ ВСЕХ

В отличие от многих других развитых рынков, в России очень низкая стоимость связи и устройств, что дает возможность мобильной экономике расти.

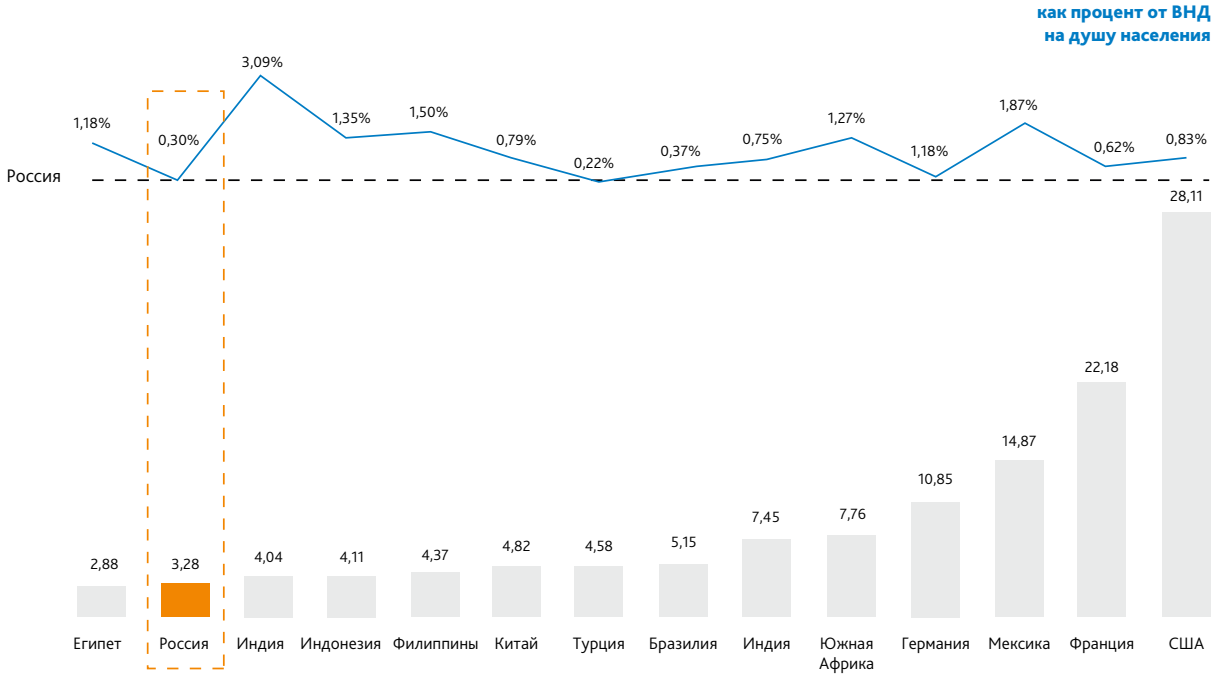
СТОИМОСТЬ СВЯЗИ

Цены на мобильную связь в России очень привлекательны для конечных пользователей как в номинальном выражении, так и по паритету покупательной способности, особенно цены интернет-трафика. В России цены на интернет — как широкополосной, так и мобильный — одни из самых низких, что является положительным мотивационным фактором для пользователей. Отчасти это связано с высоким уровнем конкуренции, а отчасти — с доступностью/культурой бесплатного интернета в стране.

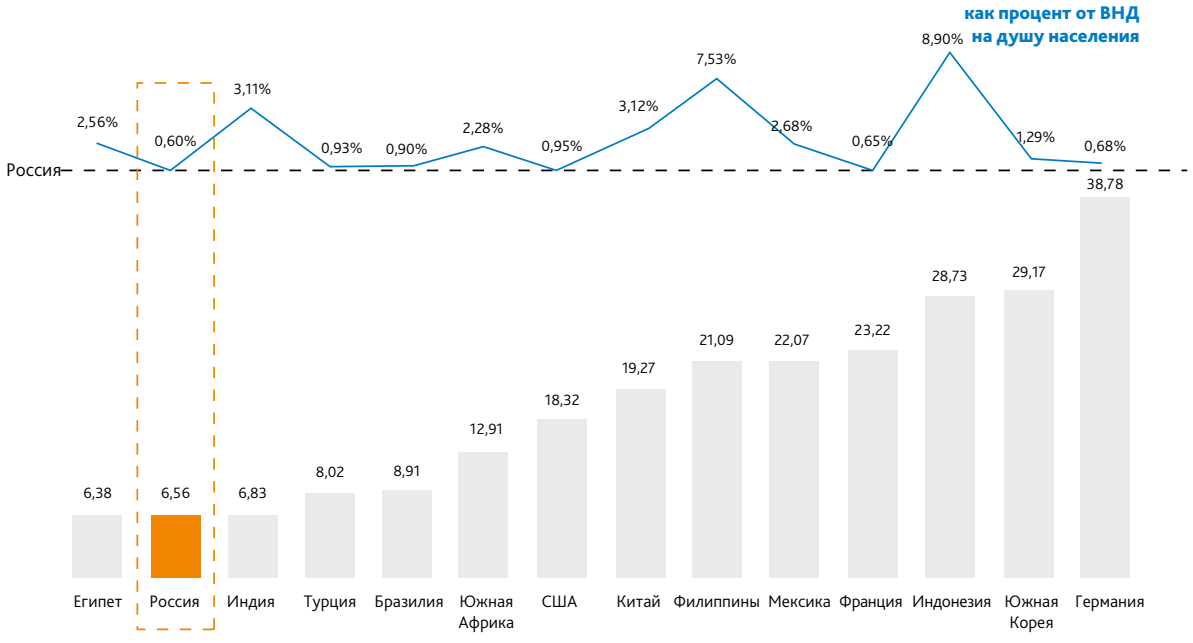
Но это также обусловлено инвестициями российского правительства в инфраструктуру и доступностью бесплатного интернета для каждого, что, безусловно, обращается в прибыль для всего рынка.

Хотя такая среда доступного интернета ведет к определенному давлению на операторов мобильной связи и поставщиков интернет-услуг (которые очень конкурентоспособны и ориентированы на цену) в том смысле, что клиенты в меньшей степени готовы платить за связь; мобильная экономика будет продолжать получать прибыль от недорогого/бесплатного интернета по мере того, как все большее количество услуг и контента станет доступными в мобильном формате.

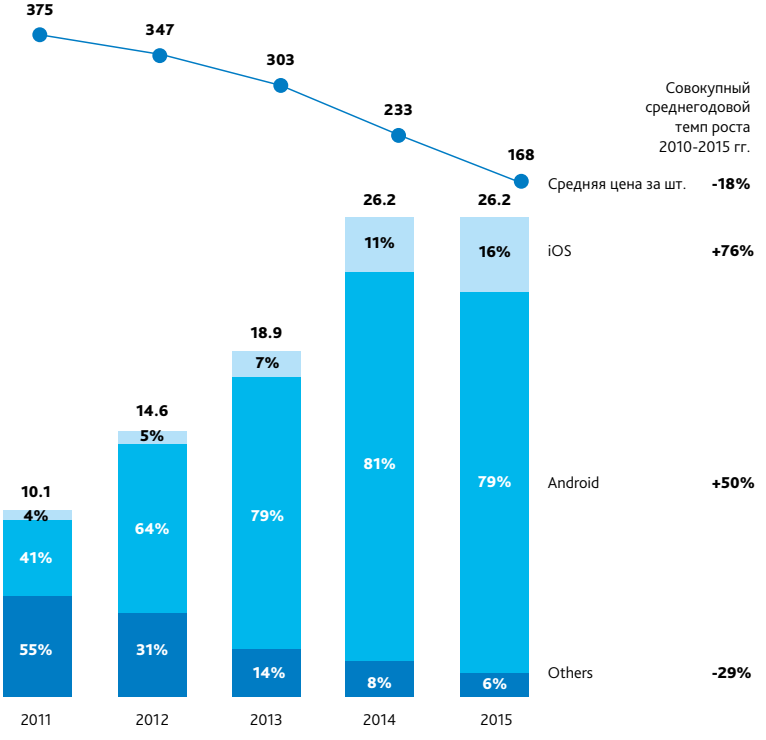
Стоимость 500мб данных по странам как доля от среднего дохода граждан, 2015, долл. США
Источник: ITU, кабинетный анализ, анализ OC&C



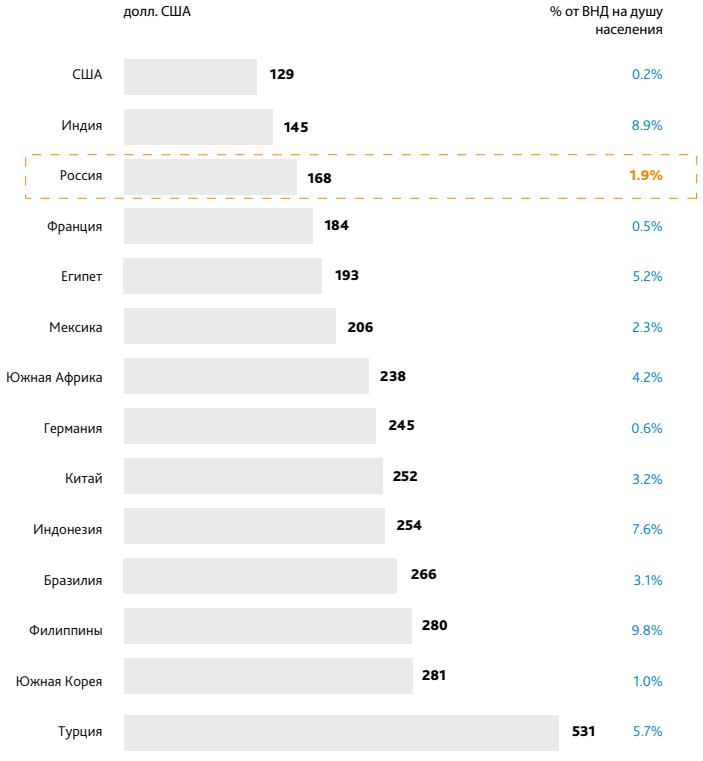
Стоимость субкорзины фиксированной широкополосной связи по странам и как процент от ВНД на душу населения, 2015 г.
Источник: ITU, кабинетный анализ, анализ ОС&С



Эволюция продаж смартфонов по категории, Россия, 2011-2015 гг. Млн шт., долл. США
Источник: Euromonitor, МВФ, анализ ОС&С



Средняя цена смартфона за шт. по странам



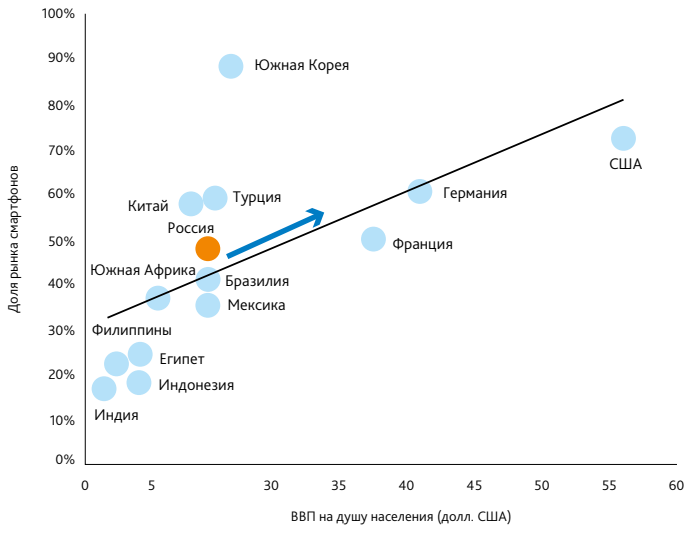
Среднее: 241

НАЛИЧИЕ ДОСТУПНОГО ОБОРУДОВАНИЯ

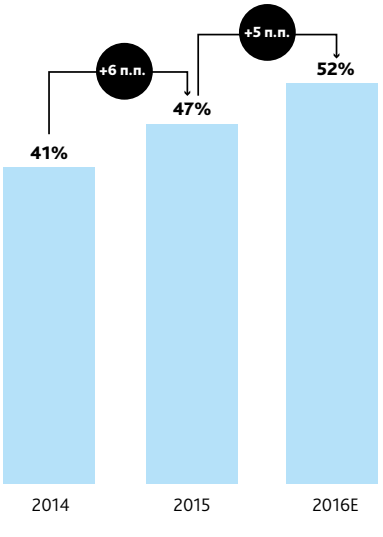
По сравнению с большинством стран, российские потребители склонны к более дешевым смартфонам. Доля рынка смартфонов только что достигла 50% и демонстрирует потенциал дальнейшего роста.

Android сделал планшеты и смартфоны одинаково доступными всем, благодаря открытому исходному коду. Компании различных размеров могут теперь потратить средства на изготовление смартфонов и планшетов, поскольку им не нужно разрабатывать свою собственную операционную систему и инвестировать в это миллионы.

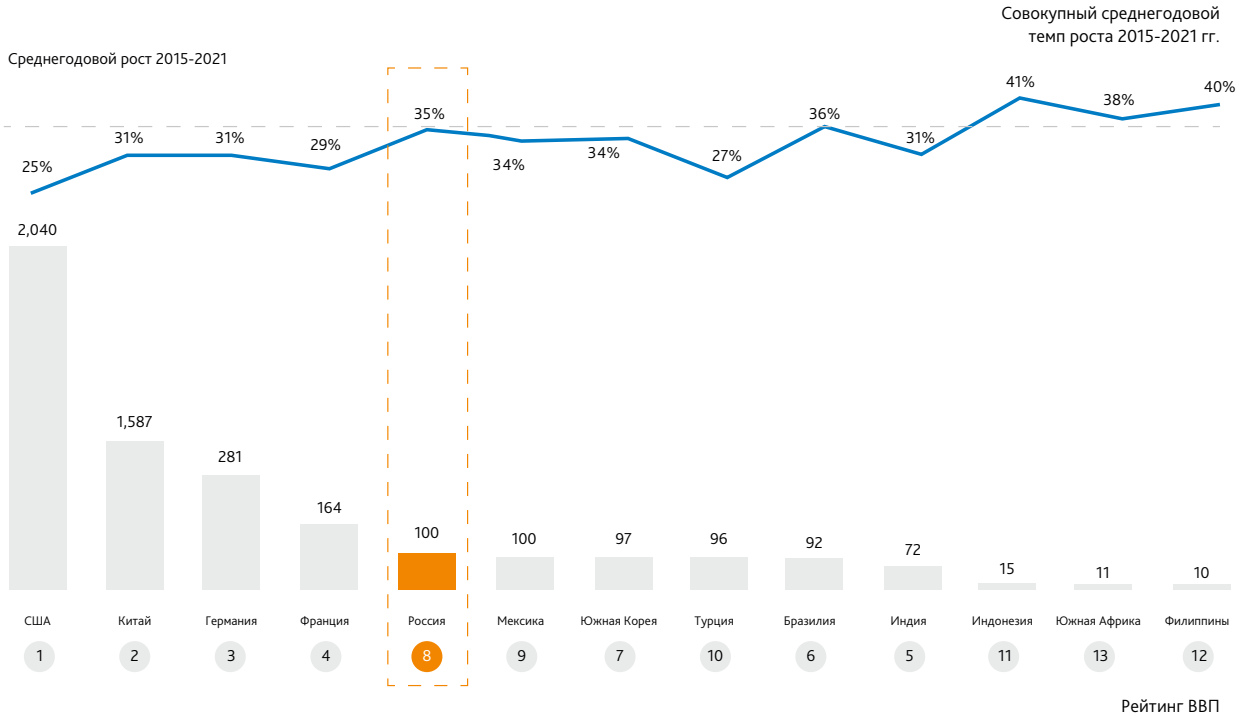
Доля рынка смартфонов по странам, 2015 г.
% от населения старше 18 лет



Доля рынка смартфонов, Россия, 2014-2016 гг. (предварительные данные) *% от населения старше 18 лет*



Непрямой вклад мобильной интернет-экономики (Слой 3), 2016 г.
Проиндексировано к России = 100 / Источник: Euromonitor, Statista, вторичные исследования, анализ ОС&С



В России доля рынка дорогих телефонов с ОС Android очень низка — даже по сравнению с iOS. Поэтому Android больше ассоциируется с более низким доходом, редкой частотой замены устройств и использованием их для совершения небольших сделок. Однако разработчики приложений говорят, что пользователи Android более активны, чем пользователи iOS (что касается электронной коммерции и электронных платежей, пользователи iOS совершают сделки на большие суммы, но не очень часто, а пользователи Android, наоборот, совершают много мелких сделок на небольшие суммы через короткие промежутки времени).

III. ВЫСОКИЙ УРОВЕНЬ РАЗВИТИЯ

ПЕРСПЕКТИВА С ТОЧКИ ЗРЕНИЯ БИЗНЕСА

Мобильная интернет-экономика поддерживает развитую экосистему технологических стартапов, а также местных и международных технологических гигантов.

Развитая экосистема стартапов, а также присутствие местных технологических успешных компаний может быть связана с непрекращающимися инвестициями правительства в ИТ и цифровую грамотность (например, включение в школьную программу уроков информатики уже в 1985 г.)

Это также объясняет, почему в России косвенный вклад мобильной интернет-экономики один из самых больших — т.е. увеличение доходов от повышения эффективности и продаж в других отраслях/немобильном бизнесе (топливная эффективность логистических компаний, повышение продаж малого и среднего бизнеса, занимающегося реализацией одежды и обуви, посредством постов в Инстаграм/рекламе, улучшение в деятельности по продажам фармацевтических компаний/компаний, реализующих товары повседневного спроса) и доходов от продаж компаний, занимающихся исключительно поддержкой цифровых технологий (умные счетчики, умные дома, умные автомобили, мобильные билеты, мобильные платежи и пр.), при этом уровень роста — самый высокий среди ряда сравниваемых стран (ожидаемый рост в 2015–2021 гг.— 35%, в США — 25%, в Китае — 31%).

Мы полагаем, что такой большой объем и ожидаемый дальнейший рост вызваны следующим:

а) высокая цифровая/мобильная грамотность российских пользователей;

б) использование многими компаниями (как местными, так и международными) инновационных устойчивых решений (например, мобильные терминалы/мобильные устройства, платежная инфраструктура, разработка программного обеспечения/приложений, целевой мобильный/цифровой маркетинг) как для мобильного, так и для немобильного бизнеса, реализации которых способствует высокая доступность и широкие возможности разработчиков.

Скачивания через магазины приложений
Источник: App Annie

Наше исследование и интервью в компаниях показали, что многие из них позиционируют свои команды разработчиков Android как разработчиков совершенно новой продукции/услуг, поскольку Android дает возможность осуществлять разработку и тестирование при меньших затратах, чем при альтернативных ОС, и сокращает время до выхода продукции на рынок. Хотя изначально такая позиция была характерна для разработчиков игр, она распространилась и на другие сегменты. В настоящее время ведущие российские банки задействуют продвинутые команды разработчиков Android, которые руководят общей работой по развитию мобильных приложений и поддерживают онлайн-банкинг своими инновациями.

Высокий девелоперский уровень в России также нашел отражение в разработке игр. По данным App Annie, некоторые российские разработчики игр во многих странах вошли в десятку лучших по общей выручке от App Store и Google Play в 2016 г.— Playrix занял 8-е место в России и Испании, 9-е в Германии, 10-е в Италии и Великобритании.

ПЕРСПЕКТИВА С ТОЧКИ ЗРЕНИЯ ПОТРЕБИТЕЛЯ

Живая девелоперская среда в России позволяет внедрять инновации, особенно в мобильных технологиях.

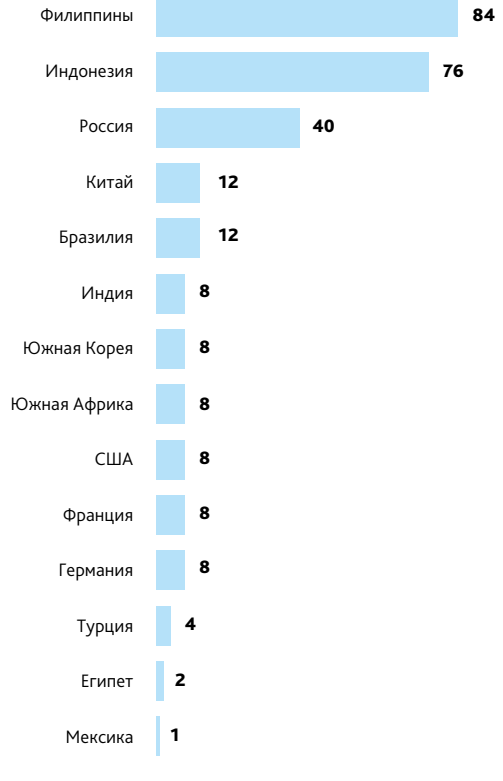
Таким образом, контент для мобильных потребителей очень разнообразен, владельцы российских смартфонов — одни из самых вовлеченных в мире потребителей, и Россия занимает 5-е место по объему скачивания приложений как в Google Play, так и в App Store.

Количество российских приложений в…	App Store	Google Play Store
Топ 10	5	6
Топ 20	42%	5
Топ 50	34%	22

Топ самых скачиваемых приложений в российских магазинах демонстрирует, что российские потребители предпочитают приложения, разработанные российскими разработчиками. В списке 25 ведущих издателей входят такие страны, как Россия, США и Китай (слева — App Store, справа — Google Play)

Россия также занимает одно из ведущих мест с точки зрения количества скачиваний на душу населения, при этом среднее количество скачиваний составляет 40 скачанных приложений в год. Возможно, это происходит по следующим причинам:

1. Большой выбор приложений: как приложений, так и игр; постоянное снабжение как с точки зрения разнообразия, так и с точки зрения российского контента.
2. Более высокий социально-экономический статус владельцев смартфонов: владельцами смартфонов, несмотря на рост, все равно пока выступают потребители со средним и высоким уровнем дохода; такие люди сразу пробуют все новое, в том числе новые приложения.



Скачивания на душу населения, 1 половина 2015 г. *Включая все платформы, только владельцы смартфонов* **/** *Источник: Inmobi, Statista, анализ ОС&С*

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

1994 год
7 апреля

**ДЕЛЕГИРОВАН
ДОМЕН .RU**

2010 год
12 мая

**ДЕЛЕГИРОВАН
ДОМЕН .РФ**

cctld.ru | кц.рф

ПРОШЛОЕ И НАСТОЯЩЕЕ ВТОРИЧНОГО РЫНКА ДОМЕНОВ .RU И .РФ

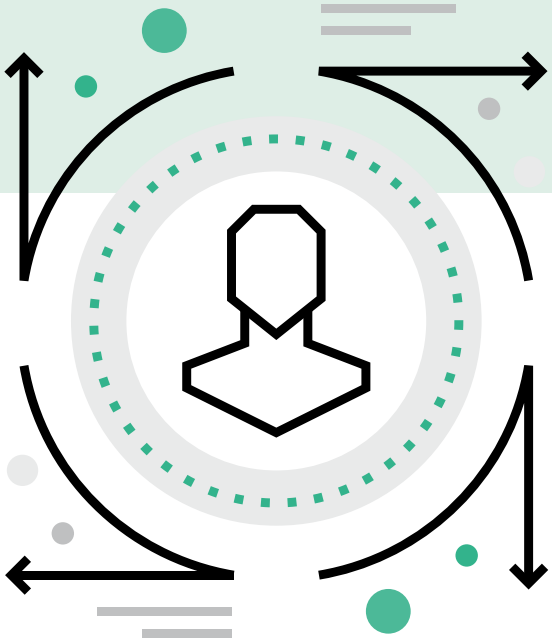
.TXT
ДМИТРИЙ ДЕНИСКИН
Директор по развивающимся рынкам REG.RU

КАЖДЫЙ ДЕНЬ ТОЛЬКО В РОССИИ СОВЕРШАЮТ ТЫСЯЧИ СДЕЛОК С ДОМЕННЫМИ ИМЕНАМИ. ИХ РЕГИСТРИРУЮТ, ПЕРЕПРОДАЮТ, НАСЛЕДУЮТ, ДАРЯТ. ЗА ДОМЕНЫ ВЕДУТСЯ СУДЕБНЫЕ СПОРЫ И КОРПОРАТИВНЫЕ ВОЙНЫ. ОСОБЫЙ ИНТЕРЕС ВЫЗЫВАЕТ ИМЕННО ВТОРИЧНЫЙ РЫНОК, ОБЪЕМ КОТОРОГО СОСТАВЛЯЕТ МИЛЛИОНЫ РУБЛЕЙ. ПРЕДЛАГАЕМ ПОЗНАКОМИТЬСЯ С ИСТОРИЕЙ ФОРМИРОВАНИЯ ВТОРИЧНОГО РЫНКА ДОМЕНОВ В РОССИИ И С ПЕРСПЕКТИВАМИ ЕГО РАЗВИТИЯ.

ПЕРВОНАЧАЛЬНЫЕ ПРАВИЛА РЕГИСТРАЦИИ ДОМЕНОВ В ЗОНЕ .RU СОДЕРЖАЛИ ПРЯМОЙ ЗАПРЕТ НА ПЕРЕПРОДАЖУ ДОМЕННЫХ ИМЕН, ХОТЯ ФАКТИЧЕСКИ НЕОФИЦИАЛЬНЫЕ СДЕЛКИ НА ВТОРИЧНОМ РЫНКЕ ПРОХОДИЛИ.

.RU БЕЗ ПРЕДОПЛАТЫ. DOMAIN KITING

С 1990-х и вплоть до февраля 2002 года домен .RU можно было зарегистрировать без предоплаты, по сути — бесплатно. В течение двух месяцев домен работал, затем снимался с делегирования и через месяц удалялся реестром, если оплата не поступала. Это привело к возникновению практики, получившей в западной доменной индустрии название domain kiting («прокатывание домена»), когда доменом фактически можно было пользоваться бесплатно.



1999 Г. ПЕРВАЯ МАССОВАЯ РЕГИСТРАЦИЯ

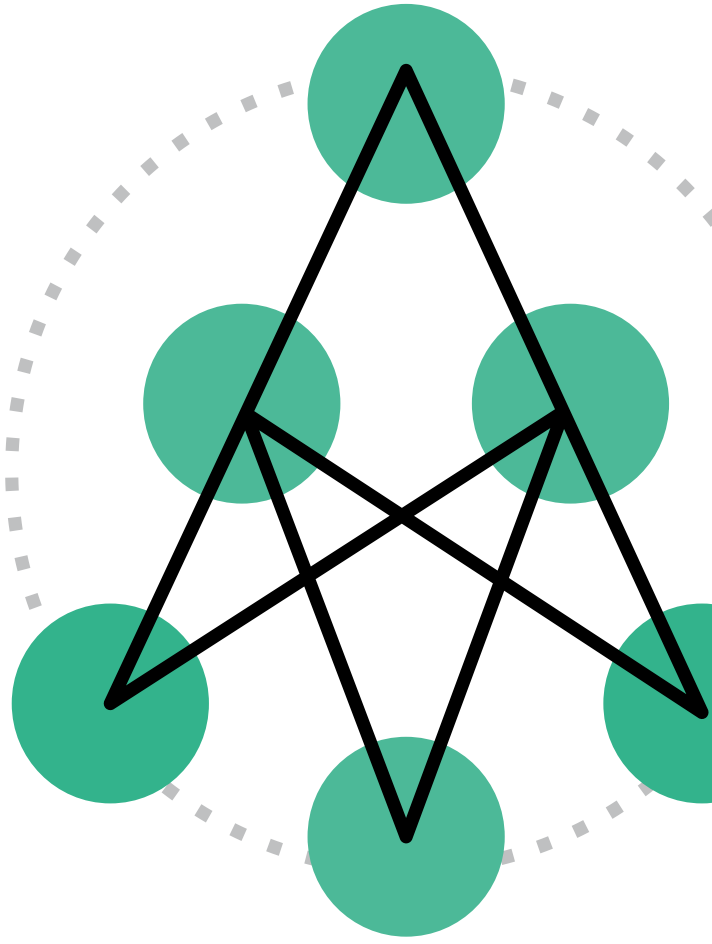
Адвокатское бюро «Арбитражсудправо» подало заявки на регистрацию ~ 1300 доменов .RU. В основном это были траслитерированные ключевые слова, например, britva.ru, chemodan.ru, chulki.ru и kolgotki.ru, krysha.ru, unitaz.ru, kipr.ru, но встречались и домены типа rentv.ru, vremechko.ru. Оплачены тогда были далеко не все домены, но поступок вызвал живое обсуждение в профессиональной среде.

2000 Г. ВТОРАЯ МАССОВАЯ РЕГИСТРАЦИЯ

20-летний житель Дубны Денис Гледенов зарегистрировал на своё имя более 1670 доменных имён в российском сегменте Интернета. В интервью 2002 года газете «Коммерсант» Денис признался: «Сейчас я ежемесячно продаю от трёх до шести доменов на $10–15 тыс.».

2003 Г.

Хорошие освобождающиеся домены, как правило, регистрируются одними и теми же профессиональными игроками, которые вкладываются в технологии. В это время ещё встречаются те, кто передаёт домены не с помощью отправки официальных писем, а в формате «домен удалится, и ты его зарегистрируешь».



ЦЕНА РЕГИСТРАЦИИ ДОМЕНА .RU ДЛЯ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ

Наибольшее влияние на развитие вторичного рынка оказали реселлерские программы регистраторов. При розничной цене в 600 рублей оптом домены можно было регистрировать по 90–100 рублей.

ДО 2000 ГОДА / $120, по курсу 27

3240 РУБ.

С 01.02.2000 / $36, ПО КУРСУ 30,67

1104 РУБ.

С 13.02.2001 / $24, ПО КУРСУ 28,68

688 РУБ.

С 01.01.2004 / $23,6 (СНИЖЕНИЕ СТАВКИ НДС), ПО КУРСУ 29,45

695 РУБ.

2007–2016 ГГ. / в среднем

600 РУБ.

2017 Г. / в среднем

950 РУБ.

2004 Г. ЛЕГАЛИЗАЦИЯ ВТОРИЧНОГО РЫНКА

Из новых Правил регистрации доменов в зоне .RU были исключены два пункта:

1.8. Домен и право на администрирование домена не являются объектами купли-продажи.

4.16. Администратор зоны .RU имеет право прекратить делегирование всех доменов, по отношению к которым не выполняются условия, изложенные в п.1.8. настоящего Регламента.

Старые правила — www.cctld.ru/ru/docs/archive/detail.php?ELEMENT_ID=428

МАЙ 2006 Г. ЗАПУСК ПЕРВОГО АУКЦИОНА ОСВОБОЖДАЮЩИХСЯ ДОМЕНОВ

К этому времени нагрузка на серверы регистратора RU-CENTER в момент освобождения становится так велика, что является по сути DDOS-атакой.

КОРОТКИЕ ДОМЕНЫ

26.06.2006

ЗАРЕГИСТРИРОВАНЫ ВСЕ ТРЁХЦИФЕРНЫЕ ДОМЕНЫ

09.09.2006

ЗАРЕГИСТРИРОВАНЫ ВСЕ ТРЁХБУКВЕННЫЕ ДОМЕНЫ

14.04.2008

ЗАРЕГИСТРИРОВАНЫ ВСЕ ТРЁХСИМВОЛЬНЫЕ ДОМЕНЫ

НОЯБРЬ 2006 Г. VODKA.RU

Артемий Лебедев продал зарегистрированный в 1997 году домен VODKA.RU за 50 000 долларов компании «Русский Стандарт».

2007 Г. ДОМЕЙНЕРЫ

Пресса впервые начинает употреблять термин «домейнер», отличая его от кибersквоттера.

2007 Г. 50% ОСВОБОЖДАЮЩИХСЯ ДОМЕНОВ РЕГИСТРИРУЮТСЯ ПОВТОРНО

Весной 2005 года повторно регистрировалось менее 10% освобождающихся доменов. К концу 2007 года этот показатель превышает 50%.

Кибersквоттер — лицо, регистрирующее доменные имена брендов (торговых марок) с целью их дальнейшей перепродажи или недобросовестного использования.

Домейнер — лицо, занимающееся регистрацией доменных имён и их покупкой на вторичном рынке с целью монетизации или дальнейшей перепродажи.

2007 Г. ПРОДАЖА KOLESO.RU ЗА $36 000

2008 Г. ЗАРАБОТОК НА ОПЕЧАТКАХ — 600 ОДНОКЛАССНИКОВ

С появлением систем pay per click стало возможным монетизировать трафик доменных имён. В результате возрос процент регистрации освобождающихся доменов, стали регистрировать доменные имена с опечатками. Так, для домена odnoklassniki.ru на тот момент можно было насчитать 600 доменов с опечатками (odnaklasneke.ru, ondoklasniki.ru, adnaklasniki.ru, obnoklasniki.ru, odnuklassniki.ru и т. п.).

ВЕСНА 2008 Г. АУКЦИОНЫ ОСВОБОЖДАЮЩИХСЯ ДОМЕНОВ ВВОДЯТ ЕЩЁ 3 РЕГИСТРАТОРА

19.03.2008 — Mastername;

25.04.2008 — Regtime;

29.04.2008 — R01.

ЯНВАРЬ 2010 Г. ДОМЕН HI.RU ПРОДАН ЗА $80 600

АПРЕЛЬ 2013 Г. ПРОДАЖА FL.RU ЗА $64 500

ДЕКАБРЬ 2013 Г. ДОМЕННЫЙ БРОКЕР

Регистратор REG.RU запускает услугу «Доменный брокер». Желающий приобрести домен на вторичном рынке может делегировать компании ведение всего цикла переговоров и сделки.

ФЕВРАЛЬ 2016 Г. AU.RU ПРОДАН ЗА 1,5 МЛН РУБЛЕЙ

2016 Г. 12 НОВЫХ РЕГИСТРАТОРОВ

2011 Г.
3 НОВЫХ РЕГИСТРАТОРА

2012 Г.
2 НОВЫХ РЕГИСТРАТОРА

2013 Г.
2 НОВЫХ РЕГИСТРАТОРА

2014 Г.
3 НОВЫХ РЕГИСТРАТОРА

2015 Г.
5 НОВЫХ РЕГИСТРАТОРОВ

2016 Г.
12 НОВЫХ РЕГИСТРАТОРОВ

В 2016 году резко возросло количество новых аккредитаций регистраторов. Новые регистраторы создаются существующими участниками рынка для повышения вероятности регистрации освобождающихся доменов.

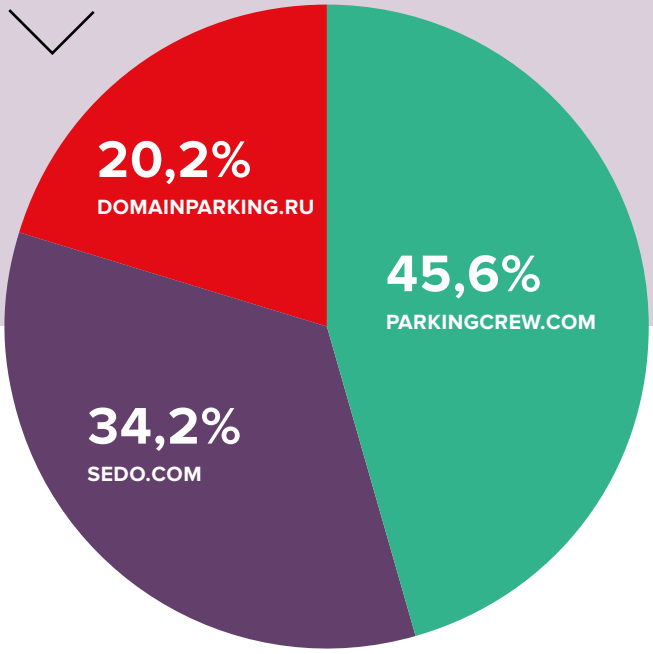
НАСТОЯЩЕЕ И БУДУЩЕЕ ВТОРИЧНОГО РЫНКА

2017 Г.
КРУПНЕЙШАЯ ПРОДАЖА. NEWS.RU ЗА $100 000

2017 Г.
ПАРКИНГИ ДОМЕНОВ

РАЗМЕЩЕНО НА СЕРВИСАХ ПАРКИНГА

РАСПРЕДЕЛЕНИЕ ПО ПЛАТФОРМАМ



.RU / 10%

563 460 ДОМЕНОВ

.РФ / 5%

45 130 ДОМЕНОВ

РАСПРЕДЕЛЕНИЕ ДОМЕНОВ .RU И .РФ ПО СЕРВИСАМ ПАРКИНГА

SALENAMES.RU
219 049
приватный,
на базе ParkingCrew

PRIVATEPERSON.RU
77 828
приватный, на базе SEDO

SEDO.COM
41 459
публичный, на базе SEDO

PARKINGCREW.COM
18 851
публичный,
на базе ParkingCrew

DOMAINPARKING.RU
113 971
публичный,
собственные шаблоны

POISHI.COM
60 270
приватный, на базе SEDO

SNPARKING.RU
19 128
публичный,
на базе ParkingCrew

PARKING.NIC.RU
12 907
публичный, на базе SEDO

DOMAINPARKING.RU — САМЫЙ ПОПУЛЯРНЫЙ ПУБЛИЧНЫЙ ПАРКИНГ В РОССИИ

8 400 000
уникальных посетителей на всех доменах в месяц

114 000
доменов .RU

25 000
доменов .РФ

1 100
доменов .SU

5 400
предложений о продаже пользователи получают ежемесячно

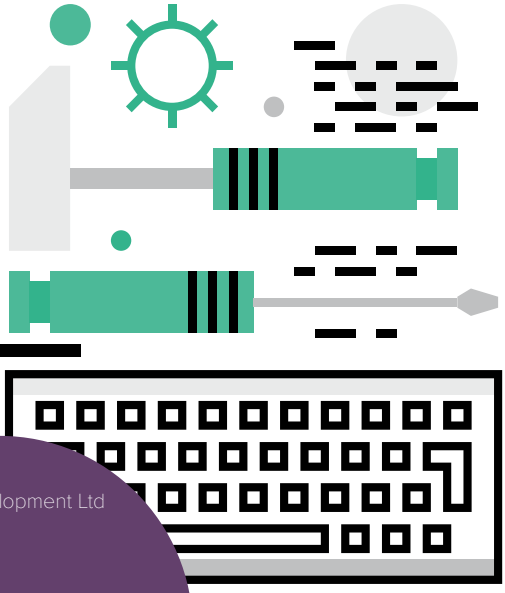
7 200
активных пользователей

200
доменов в месяц продается через сервис

Источник: domainparking.ru

2017 Г. КРУПНЕЙШИЕ ВЛАДЕЛЬЦЫ ДОМЕНОВ

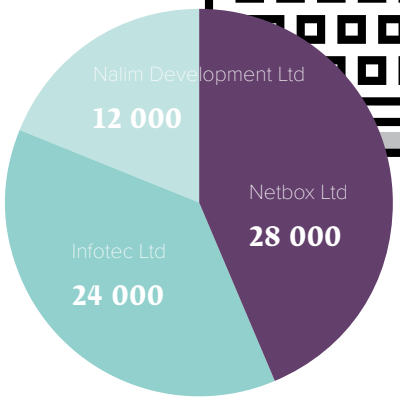
Большим количеством доменов владеют как физические, так и юридические лица.



ТОР3 КРУПНЕЙШИХ ВЛАДЕЛЬЦЕВ-ФИЗИЧЕСКИХ ЛИЦ

Данные о владельцах-физических лицах не являются общедоступными в соответствии с законодательством РФ.

Источник: statdom.ru



ТОР3 КРУПНЕЙШИХ ВЛАДЕЛЬЦЕВ-ЮРИДИЧЕСКИХ ЛИЦ

Источник: statonline.ru

2017 Г. ОСВОБОЖДАЮЩИЕСЯ ДОМЕНЫ

Рынок освобождающихся доменов — это часть вторичного рынка. Его объём составляет от 5 до 8 миллионов рублей в месяц. От момента освобождения топовых доменов до их повторной регистрации проходит в среднем всего 0,08 секунд.

ДИНАМИКА РЕГИСТРАЦИИ ОСВОБОЖДАЮЩИХСЯ ДОМЕНОВ

10% ДОМЕНОВ
РЕГИСТРИРУЮТСЯ В МОМЕНТ ОСВОБОЖДЕНИЯ

3,5% ДОМЕНОВ
РЕГИСТРИРУЮТСЯ В ТЕЧЕНИЕ 1,5 ЧАСОВ

1% ДОМЕНОВ
РЕГИСТРИРУЮТСЯ В ТЕЧЕНИЕ НЕДЕЛИ

**Ежемесячно в REG.RU на освобождающиеся домены в зоне .RU делается свыше 10 000 ставок.
Заметно меньше в .РФ — всего 700–1000 ставок и 40–60 ставок на домены .SU.
Размер самой популярной ставки — около 1000 рублей.**

2017 Г. ПРИВАТНЫЕ ПРОДАЖИ

GAME.RU, СТРАХОВКА.РФ, SOVEST.RU, 1000.RU

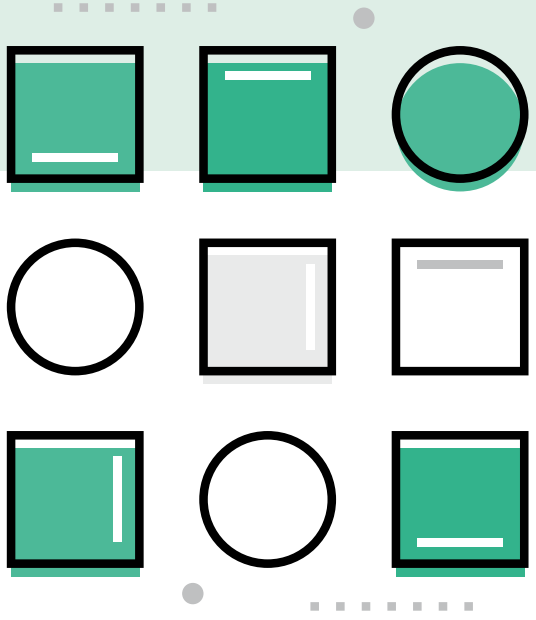
По оценкам экспертов рынка, эти домены были проданы по цене более 1 млн рублей.

Лишь небольшое число продаж доменов на вторичном рынке проходит публично. О таких продажах можно косвенно судить по данным о смене администратора домена.

ЧИСЛО ПЕРЕДАЧ ДОМЕНОВ У РЕГИСТРАТОРА REG.RU В МЕСЯЦ:

.RU — 90 (только ручная передача, без учёта онлайн);

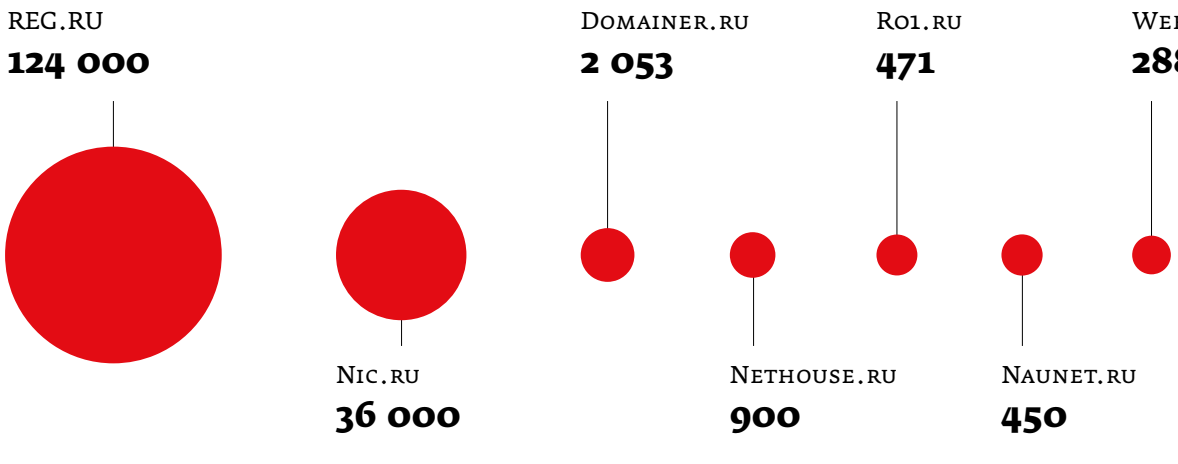
.РФ — 20 (только ручная передача без учёта онлайн).



2017 Г. МАГАЗИНЫ ДОМЕНОВ

Магазин доменов — это витрина на сайте регистратора, где клиенты могут выставить свой домен на продажу. Сегодня 7 российских регистраторов предоставляют автоматизированный сервис продажи доменов для своих клиентов.

ЧИСЛО ДОМЕНОВ .RU В МАГАЗИНАХ РЕГИСТРАТОРОВ



В МАГАЗИНЕ ДОМЕНОВ REG.RU

Для передачи доменов .RU/.РФ требуется лично поданное заявление либо нотариально заверенное письмо с указанием получателя домена. Но у REG.RU есть услуга оформления поручения, которая позволяет продать домен онлайн любому лицу.

123 000

ДОМЕНОВ .RU /

ИЗ НИХ 67% МОЖНО КУПИТЬ ОНЛАЙН

35 000

ДОМЕНОВ .РФ /

ИЗ НИХ 38% МОЖНО КУПИТЬ ОНЛАЙН

120

заявок на смену владельца ежемесячно обрабатывает регистратор REG.RU (только ручная передача, без учёта онлайн)

600 000

рублей — крупнейшая продажа клиента через магазин REG.RU

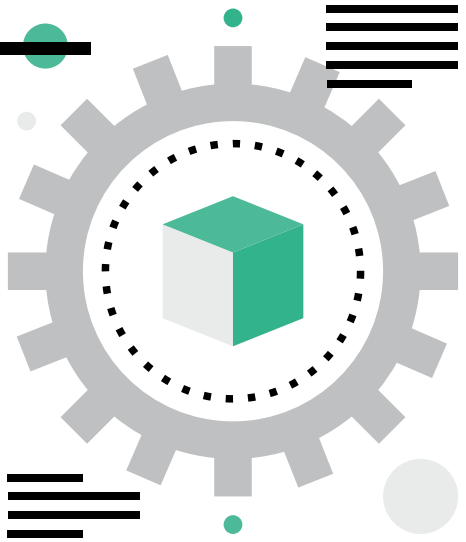
5 036

рублей — средняя цена продажи домена клиентами REG.RU

1 050

доменов ежемесячно продают клиенты REG.RU через магазин

ТРЕНДЫ



300 000 ДОМЕНОВ

по оценкам экспертов, могут не продлить держатели крупных портфолио доменов .RU после планируемого Координационным центром повышения цены для регистраторов (на 71% или 59 рублей в абсолютном выражении).

www.cctld.ru/ru/press_center/news/news_detail.php?ID=11381

12 НОВЫХ РЕГИСТРАТОРОВ

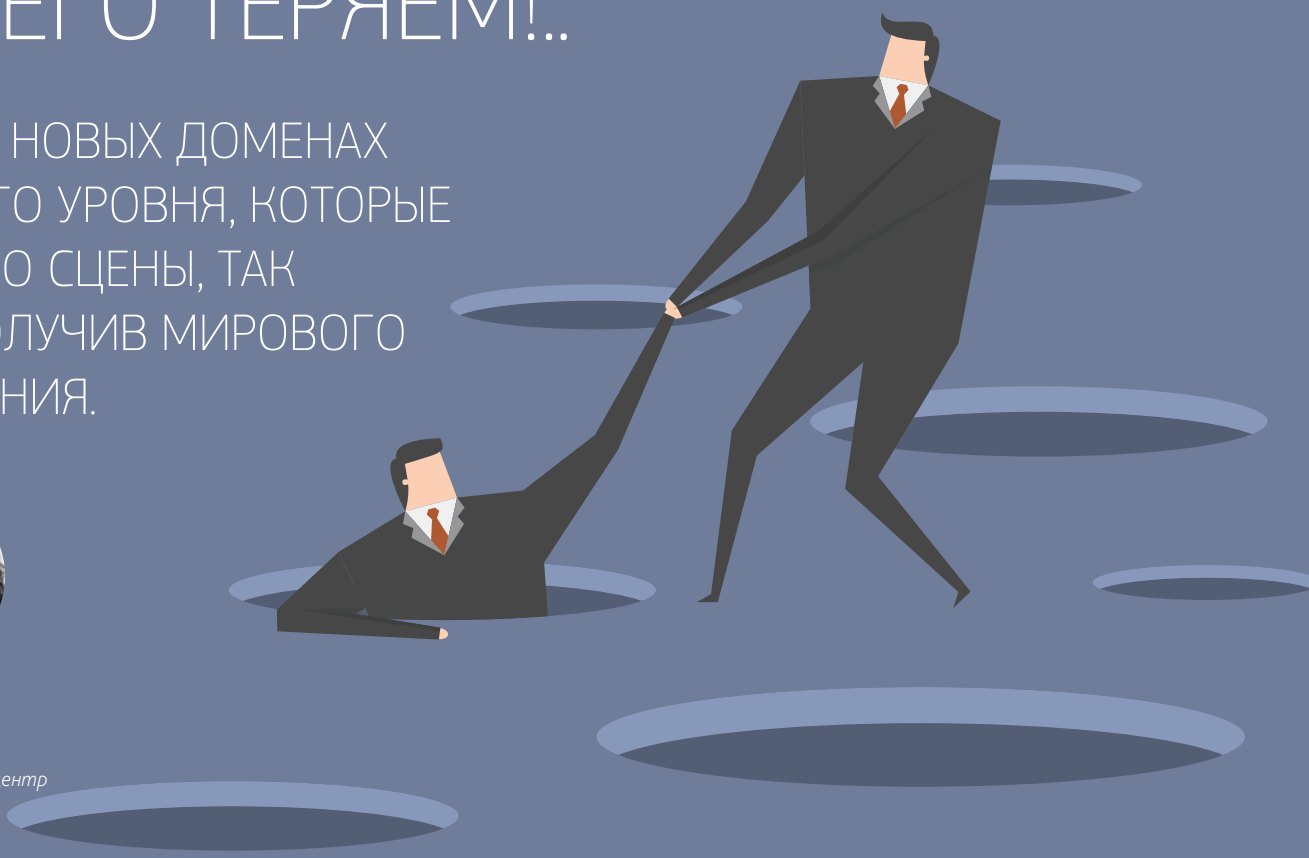
аккредитовано в 2016 году. Новые регистраторы создаются существующими участниками рынка для повышения вероятности регистрации освобождающихся доменов.

10 000 ДОМЕНОВ .RU

удаляются по рабочим дням с начала 2017 года. Реально число удаляемых доменов могло быть больше, но правилами Координационного Центра введено ограничение. Из-за этого домены попадают в очередь и освобождаются спустя несколько дней от запланированной даты. Координационный центр рассматривает возможность увеличить предел доменов, удаляемых в конкретный день. Изменение status quo приведёт к перераспределению рынка освобождающихся доменов между регистраторами.

МЫ ЕГО ТЕРЯЕМ!..

...ИЛИ О НОВЫХ ДОМЕНАХ ВЕРХНЕГО УРОВНЯ, КОТОРЫЕ УШЛИ СО СЦЕНЫ, ТАК И НЕ ПОЛУЧИВ МИРОВОГО ПРИЗНАНИЯ.



.TXT
ВИКТОРИЯ БУНЧУК
Координационный центр доменов .RU/.РФ

Система доменных имен (DNS) неприступна только с виду — на самом деле она не раз доказывала, что консерватизм не в ее стиле. Самая грандиозная из ее «акций» из разряда «свобода и равноправие» началась в 2012 году, когда заработала программа Международной интернет-корпорации ICANN по созданию новых доменов верхнего уровня (New gTLD program). Она дала возможность буквально каждому (конечно, с оговоркой, что этот «каждый» обладает N-ной суммой денег и серьезными техническими возможностями) завести собственное пространство в интернете, холить и лелеять его, а также зарабатывать на пользователях, желающих ощутить радость обладания адресом в доселе невиданном .BLOG, .AUTO или, скажем, .ОНЛАЙН.

К слову, благодаря упомянутой программе ICANN, DNS всего за 4 года увеличилась на 2 тысячи доменов верхнего уровня. Верхнего, Карл! И это не предел: корпорация пообещала, что вновь откроет границы к 2020-му, а, значит, нас ждет очередной наплыв доменов, и в глазах не перестанет рябить…

Среди тысяч новичков наметились не только лидеры, но и плетущиеся в хвосте. В первых рядах числятся, например, .XYZ (больше 6 млн регистраций), .TOP (4 млн адресов), .CLUB (950 тысяч) и проч. В последних — .WHOSWHO, .MOTORCYCLES, .WED и многие другие «счастливчики», так и не набравшие даже сотню «престижа». А между тем, поддержка домена верхнего уровня не дешевое удовольствие. И некоторые доменовладельцы уже решили от него отказаться. Но об этом чуть позже, пока заглянем в историю и найдем еще несколько примеров, когда DNS избавлялась от лишнего, чем еще раз доказала подвижность своей структуры.

***

Один из самых ярких примеров — национальный домен Югославии .YU, прекративший свое существование по причине распада страны. И хотя это событие случилось в 1990-х, домен продержался до весны 2010 года. Похожая история приключилась и с доменом Чехословакии.CS (стоит отметить, что этим буквосочетанием успело попользоваться и союзное государство Сербии и Черногории, однако союз оказался непрочным, а .CS вновь оказался не у дел).

Был удален из корня DNS и домен .BU. Это произошло в 1997 году, когда страна, для которой он предназначался, была переименована: Бирма стала Мьянмой, а .BU заменили на .MM. По той же причине из обращения был выведен и домен .ZR, принадлежавший Заиру; ныне государство зовется Демократической Республикой Конго, для которой был выделен домен .CD, некогда привлекавший внимание не только местных жителей, но и всех любителей «раскачать толпу» в клубе.

Ну и совсем уже положительная история связана с удалением домена .DD, который был зарезервирован для ГДР. После падения Берлинской стены Восточная Германия фактически перестала существовать — .DD стал не нужен, а Германия объединилась под доменом .DE. Кстати, в связи с ненужностью был ликвидирован и домен .UM, предназначавшийся Малым Отдаленным островам США: на территории, состоявшей из 5 островов, 2 атоллов и 1 рифа, просто некому было интересоваться доменной индустрией.

И если продолжать рассказ о национальных доменах, плавно переходя к новым (New gTLD), позволим себе аккуратный прогноз.

В апреле 2017-го глава Казахстана Нурсултан Назарбаев распорядился перевести казахский алфавит, основанный на кириллической письменности, на латиницу: переход планируется завершить в 2025 году — к этому моменту латинский алфавит будет использоваться в деловой документации, книгах и периодических изданиях. А ведь у Казахстана, кроме «классического» двухбуквенника .KZ, есть и кириллический домен .ҚАЗ, заработавший в 2012 году по процедуре Fast Track. Думается, в связи с новой политикой государства, к 2025-му будет отказано и в работе .ҚАЗ, тем более, что кириллический домен значительно уступает по популярности «старшему брату» .KZ (1008 регистраций против 130 тысяч).

***

Как мы уже говорили, есть «отказники» и среди New gTLD. Например, .DOOSAN. Домен создавался для одноименной южнокорейской корпорации, занимающей 7 место в мире по выпуску землеройной и дорожно-строительной техники.

Удален из корня DNS и .FLSMIDTH, также являющийся доменом-брендом, заявителем на который выступила датская компания FLSmidth — крупный поставщик оборудования и услуг для предприятий цементной и горно-перерабатывающей промышленности.

Освободился и домен .IINET, который создавался в интересах австралийской группы компаний iiNet, предоставляющий широкий спектр услуг в области интернета и телекоммуникаций на национальном уровне.

Оказались в несчастливом ряду домен .MUTUELLE для французской федерации, объединяющий около 600 региональных организаций взаимопомощи, и домен .ORIENTEXPRESS для компании Orient Express Hotels, Ltd (OEH), владеющей 40 отелями класса «Люкс», ресторанами, туристическими поездами и круизными лайнерами в 24 странах мира.

Причин для закрытия этих доменов может быть несколько, но, очевидно, все они сводятся к тому, что владельцы просто не сдюжили: сложность технической поддержки целой зоны, ежегодные внушительные взносы в ICANN и общая дороговизна «предприятия», низкая заинтересованность пользователей и, как следствие, мизерное количество регистраций (хотя, в данном случае стоит говорить об осознанном отказе от конечных пользователей: «брендовые» домены верхнего уровня обычно закрыты для регистраций извне; от чего, в первую очередь, страдает окупаемость или рентабельность). Наконец, просто неоправданные надежды — дорогая игрушка оказалась бесполезной…

***

Согласно отчетам ICANN, в рамках программы New gTLD были введены порядка двух сотен доменов-брендов. И вероятно, каждый из них испытывает похожие трудности (в большей или меньшей степени). Не исключено, что коснутся эти проблемы и более открытых доменов. Другими словами, доменопад наверняка продолжится.

Ведь чтобы оказаться на гребне дот-волны, недостаточно только желания, материальных и технических ресурсов: для полноценного существования необходимы пользователи, бизнес, государственные и общественные организации, действительно заинтересованные в интернет-адресах с «нестандартным» окончанием,— а иначе выжить в условиях жесткой конкуренции, которая только усилится с началом второго тура New gTLD, невероятно сложно.

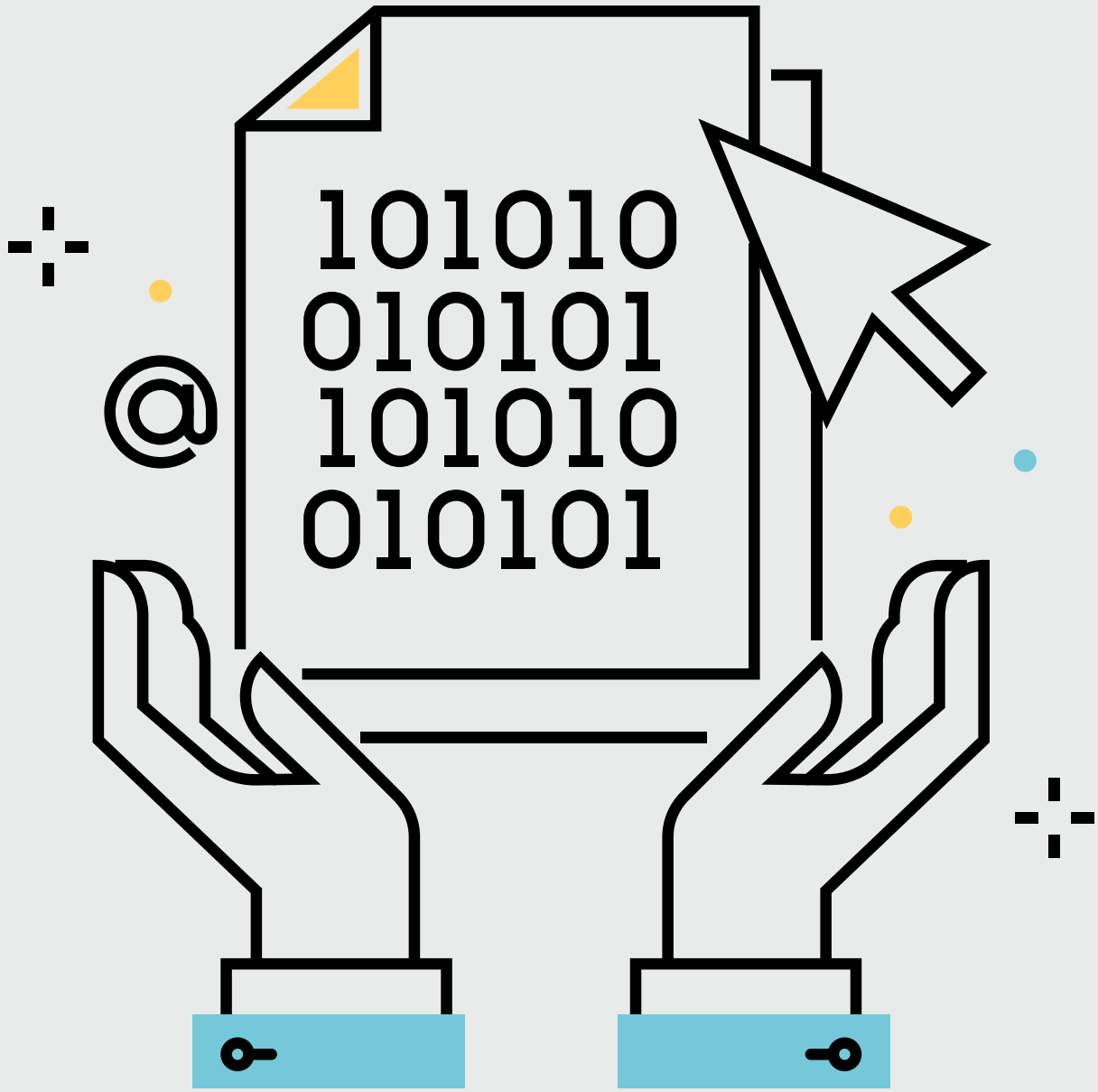
ДОМЕНЫ И ПРАВО

.TXT

М.А. РОЖКОВА
Доктор юридических наук,
эксперт Российской Академии наук

.TXT

Д.В. АФАНАСЬЕВ
Эксперт Экспертного комитета
Государственной Думы по информационной политике,
информационным технологиям и связи



ФУНКЦИЯ ПЕРЕАДРЕСАЦИИ

В п. 15 ст. 2 Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации) содержится определение **доменного имени** — под ним понимается *обозначение символами, предназначенное для адресации сайтов в сети Интернет в целях обеспечения доступа к информации, размещенной в сети Интернет.* С помощью доменного имени пользовательское сетевое устройство (компьютер, смартфон и проч.) переадресуется на конкретный информационный ресурс.

Доменное имя принципиально отличается от IP-адреса (сокр. от англ. *Internet Protocol Address*), который присваивается каждому работающему в сети Интернет устройству (серверу, компьютеру, смартфону и проч.), позволяя идентифицировать его среди иных работающих в Интернете устройств. В п. 16 ст. 2 Закона об информации под **сетевым адресом** (IP-адресом) понимается *идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему.*

Таким образом, на одном сервере (сетевое устройство), имеющем соответствующий IP-адрес, могут размещаться одновременно тысячи разных информационных ресурсов (сайтов, порталов, домашних страниц и т.д.), имеющих разные доменные имена. В то же время сайт (информационный ресурс), имеющий одно доменное имя, может быть размещен сразу на нескольких серверах и соответствовать одновременно нескольким IP-адресам — например, для распределения нагрузки на серверы.

Неразграничение понятий «доменное имя» и «сетевой адрес» (IP-адрес) нередко становится препятствием в защите прав заинтересованных лиц.

Так, в Конституционный Суд РФ была подана жалоба, в которой оспаривалась конституционность п. 2 ч. 2 ст. 15.1 Закона об информации. Статья 15.1 Закона посвящена «Единому реестру доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено» (далее — Единый реестр), созданного в целях ограничения доступа к сайтам, содержащим запрещенную к распространению информацию. В оспариваемом п. 2 ч. 2 ст. 15.1 предусмотрено, что в Единый реестр включаются не только доменные имена и (или) указатели страниц сайтов[1] в сети Интернет, но и сетевые адреса (IP-адреса) без уточнения применения этой нормы в различных ситуациях. Таким образом, оспариваемая норма не исключает возможность блокирования сетевого адреса (IP-адреса), на котором расположен информационный ресурс, содержащий запрещенную к распространению информацию, что в итоге может повлечь блокировку не одного сайта, содержащего запрещенную информацию, а целого сервера, на котором, как отмечалось, могут располагаться тысячи сайтов, причем сайтов «добросовестных».

Об аналогичной ситуации и шла речь в деле заявителя упомянутой жалобы: информационный ресурс заявителя (*digital-books.ru*) находился на одном сервере, т.е. по одному IP-адресу с другим сайтом, на котором была размещена информация, запрещенная к распространению (*rastamantales.ru*). В результате ограничения доступа ко всему IP-адресу был заблокирован на три месяца и информационный ресурс заявителя, не содержащий никакой запрещенной информации. По мнению заявителя жалобы, в подобных случаях «владельцы сайтов, не содержащих запрещенной информации, лишаются права распространять незапрещенную информацию законным способом и фактически подвергаются мерам юридической ответственности при отсутствии правонарушения».

Конституционный Суд РФ не нашел оснований для принятия данной жалобы к рассмотрению, отметив при этом следующее: «Что же касается владельцев сайтов, не содержащих запрещенной к распространению в Российской Федерации информации, но доступ к которым оказался ограничен в связи с включением в реестр сетевого адреса, то их права на распространение информации, по существу, оказываются затронуты не решением о включении сетевого адреса в Единый реестр и принятыми в связи с этим мерами, а ненадлежащими действиями (бездействием) обслуживающего их провайдера хостинга. Соответственно, защита их права на

[1] *Речь идет о едином указателе ресурса — URL (сокр. от англ. Uniform Resource Locator – единый указатель местонахождения ресурса)*

распространение информации должна осуществляться, прежде всего, в рамках правоотношений с обслуживающим их провайдером хостинга»[2].

Таким образом, Конституционный Суд РФ, по сути, уклонился от оценки нарушения прав владельцев информационных ресурсов, не содержащих запрещенной информации, доступ к которым был заблокирован при применении мер ответственности к владельцам других информационных ресурсов.

Между тем Европейский Суд по правам человека (далее — ЕСПЧ) в схожей ситуации признавал права владельцев информационных ресурсов нарушенными.

Так, при рассмотрении дела «Ахмет Йилдырым против Турции»[3] ЕСПЧ было установлено, что заявитель являлся владельцем информационного ресурса (созданного с помощью сервиса *Google Sites (sites.google.com))*, на котором им публиковались собственные научные труды и материалы, отражающие его взгляды по различным вопросам. В июне 2009 г. национальный суд в рамках борьбы с преступлениями в Интернете принял решение о применении предварительной меры в виде блокирования сайта, принадлежащего другому владельцу (далее — сайт нарушителя), но затем решение было изменено и принято решение о блокировании доступа ко всем сайтам, созданным на *Google Sites*. Вследствие этого заявитель был лишен доступа к собственному сайту. Ходатайство об отмене распоряжения в отношении сайта заявителя было отклонено национальным судом. По состоянию на апрель 2012 г. заявитель по-прежнему не мог пользоваться своим сайтом, хотя уголовное дело в отношении владельца другого сайта (сайта нарушителя с незаконным содержанием) было прекращено в марте 2011 г.

ЕСПЧ признал подобное блокирование ограничением права заявителя на свободу выражения мнения (ст. 10 Конвенции по правам человека). Это объяснялось тем, что сервис *Google Sites* предназначен для облегчения создания и совместного использования сайтов в сети Интернет, вследствие чего он является средством осуществления свободы слова. Кроме того, ЕСПЧ сослался на то, что блокирование доступа ко всем сайтам на *Google Sites* представляет собой ограничение права пользователей сети Интернет на получение информации, поскольку Интернет в настоящее время стал одним из главных средств, с помощью которых люди реализуют право на выражение мнения, а также получение и распространение информации, гарантированное ст. 10 Конвенции. Причем в постановлении ЕСПЧ отмечалось, что *Google Sites* содержит столь значительное количество данных и информации, что он по своему объему сопоставим с онлайн-архивами крупных газет или традиционных библиотек. В то же время национальный суд из-за единственного сайта нарушителя вынес решение о блокировании доступа ко всем ресурсам Google Sites, закрыв доступ к такому большому количеству информации на неопределенный срок.

ЕСПЧ указал, что, вынося решение о блокировании Google Sites в качестве предварительной меры, национальный суд исходил из того, что это единственно возможный способ блокирования сайта нарушителя. Между тем названная мера в данном случае не может рассматриваться в качестве единственно возможной — блокирование доступа ко всем сайтам на *Google Sites* из-за единственного сайта нарушителя представляет собой ограничение свобод, гарантированных ст. 10 Конвенции по правам человека.

ФУНКЦИЯ ИДЕНТИФИКАЦИИ БИЗНЕСА И ЧАСТНЫХ ЛИЦ

Система доменных имен, упрощающая и ускоряющая переадресацию в сети Интернет, начала создаваться в 80-е годы прошлого столетия. Но к пользователям Интернета довольно быстро пришло понимание того, что, помимо чисто технической функции адресации, доменные имена из-за их простой для запоминания формы могут использоваться и в иных целях.

В связи с этим в п. 10 доклада Всемирной организации интеллектуальной собственности (далее — ВОИС) по доменным именам уже в 1999 г. отмечалось: «Доменные имена были предназначены для выполнения технической функции способом, удобным для пользователей Интернета. Они предназначались для предоставления компьютерам легко запоминающейся и идентифицирующей адресации без необходимости прибегать к идентифицирующему цифровому IP-адресу.

[2] *Определение КС РФ от 17.07.2014 № 1759-О.*

[3] *Постановление ЕСПЧ от 18.12.2012 по делу «Ахмет Йилдырым против Турции» (Ahmet Yildirim v. Turkey; жалоба № 3111/10)*

Именно потому, что они легко запоминаются и идентифицируются, доменные имена, кроме того, приобрели дополнительное предназначение в качестве идентификаторов бизнеса или частных лиц. В то время как телефонные и факсимильные номера состоят из анонимного набора цифр, не несущих какого-либо дополнительного смысла, доменные имена, вследствие своего предназначения быть легко запоминаемыми и идентифицирующими, часто несут в себе дополнительное значение, связанное с наименованием или обозначением бизнеса, либо его продуктами или услугами»[4]. С учетом этого в Отчете ВОИС 2002 года подчеркивалось: «Большинство организаций, вне зависимости от того, относятся ли они к электронной коммерции или нет, рекламируют свои доменные имена для обозначения своего присутствия в Интернете. Таким образом, хотя они, как таковые, и не являются объектом интеллектуальной собственности, доменные имена в настоящее время выполняют функцию идентификации, подобную той, что несут в себе товарные знаки»[5].

Таким образом, доменные имена с определенного момента, помимо *технической функции переадресации в сети* Интернет, стали использоваться для *выделения (идентификации) товаров, работ, услуг* одних производителей, продавцов и исполнителей среди аналогичных товаров, работ, услуг. Иными словами, функция доменного имени, на которую обращается внимание в большинстве работ зарубежных исследователей, — это *функция идентификации бизнеса или частных лиц*.

ДОМЕНЫ КАК ИМУЩЕСТВО

Доменное имя, рассматриваемое в контексте его функции как средства адресации в сети Интернет, не может признаваться самостоятельным объектом гражданских прав. Но если рассматривать доменное имя в качестве упомянутого выше «идентификатора бизнеса или частных лиц», то здесь ситуация меняется на прямо противоположную. Подтверждение этому утверждению можно найти в практике ЕСПЧ.

Так, в деле «Паеффген против Германии»[6] ЕСПЧ прямо указал на то, что права на использование доменов имеют экономическую ценность и сделал вывод о том, что эти права подпадают под действие ст. 1 Протокола № 1 к Конвенции по правам человека. Иными словами, ЕСПЧ рассматривает права на использование домена в качестве нематериального актива, обладающего бесспорной имущественной значимостью. То есть *права на доменное имя отнесены ЕСПЧ к имущественным правам*, которые российским законодательством прямо **признаются разновидностью имущества**.

Статья 128 ГК РФ признает имущественные права разновидностью имущества. При этом надо иметь в виду, что доменное имя представляет собой нематериальный объект, поэтому *сам домен — вследствие естественных свойств (п. 4 ст. 129 ГК РФ) — не допускает его передачу*; переход (передача) от одного лица к другому возможно только в отношении (имущественных) прав на доменное имя. То же можно сказать относительно возможности, например, обращения взыскания — взыскание может быть обращено лишь на права на доменное имя, относящиеся к имущественным правам (что предусматривает ст. 75 ФЗ «Об исполнительном производстве»), но никак не на само доменное имя.

Сказанное подтверждает недопустимость заключения в отношении доменных имен таких договоров, как, например, «договор купли-продажи доменного имени» или «договор аренды доменного имени» (что обусловлено нематериальной природой объекта, исключающего возможность владения и пользования) — договоры об отчуждении или о передаче в использование допустимы только в отношении лишь прав на доменное имя.

---

[4] *Final Report of the WIPO Internet Domain Name Process «The Management of Internet Names and Addresses» 30.04.1999 (www.wipo.int/amc/en/processes/process1/report/index.html)*

[5] *Интеллектуальная собственность в Интернет: обзор проблем. — Женева: ВОИС, 2002. С. 24.*

[6] *Постановление ЕСПЧ от 18.09.2007 по делу Паеффген против Германии (Paeffgen GMBH v. Germany; жалоба № 25379/04, 21688/05, 21722/05 и 21770/5).*

.TXT
ДЕНИС ЖИЛИН
Координационный центр доменов .RU/.РФ

РОЛЬ КООРДИНИРУЮЩИХ ОРГАНИЗАЦИЙ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ИНТЕРНЕТА

ОДИН ИЗ СПОСОБОВ ПРЕДОТВРАЩЕНИЯ ВРЕДОНОСНОЙ АКТИВНОСТИ В СЕТИ — МЕХАНИЗМЫ САМОРЕГУЛИРОВАНИЯ, КОТОРЫЕ ЯВЛЯЮТСЯ, С ОДНОЙ СТОРОНЫ, МЕРОЙ ПРЕДУПРЕЖДЕНИЯ, А С ДРУГОЙ — ДИСЦИПЛИНИРУЮЩИМ КОДЕКСОМ ПОВЕДЕНИЯ ДЛЯ ОРГАНИЗАЦИЙ, ЗАНЯТЫХ В ИНТЕРНЕТ-ОТРАСЛИ.

ВЕЧНАЯ БОРЬБА ДОБРА СО ЗЛОМ ВЕДЕТСЯ И В ИНТЕРНЕТ-ПРОСТРАНСТВЕ. СЛУЧАЕТСЯ, ЧТО «ТЁМНЫЕ» ВДРУГ ОКАЗЫВАЮТСЯ НА ШАГ ВПЕРЕДИ, И «СВЕТЛЫМ» ПРИХОДИТСЯ ЗАНИМАТЬ ПОЗИЦИЮ ОБОРОНЫ. ЧТОБЫ ПОВЛИЯТЬ НА ЭТУ СИТУАЦИЮ, ОТРАСЛЬ КРАЙНЕ ЗАИНТЕРЕСОВАНА В РЕАЛИЗАЦИИ ПРОЕКТОВ, КОТОРЫЕ ОСНОВАНЫ НА ПРИНЦИПАХ САМОРЕГУЛИРОВАНИЯ, ЧТО СВОДИТ К МИНИМУМУ БЮРОКРАТИЧЕСКИЕ И ВРЕМЕННЫЕ ПРОВОЛОЧКИ.

Одним из примеров подобных инициатив является проект **«Нетоскоп»**, созданный Координационным центром национального домена сети Интернет.

Координационный центр занимается разработкой правил регистрации доменных имен в российских доменных зонах, аккредитацией регистраторов и исследованием перспективных проектов, связанных с развитием российского интернета, а также выполняет функции регистратора национальных доменов .RU и .РФ. Главной задачей Координационного центра является обеспечение надежного и стабильного функционирования DNS-инфраструктуры Рунета. Именно поэтому в 2012 году появился «Нетоскоп», работа которого направлена на обеспечение безопасности в доменном пространстве. К участию в проекте были приглашены крупнейшие российские компании с целью организовать научно-техническое сотрудничество (НТС) в этой области.

Совместные усилия участников проекта позволили создать и развить уникальную по своей сути исследовательскую платформу для агрегации информации о вредоносных ресурсах в сети Интернет, позволяющую проводить анализ источников «зловредов» и в оперативном режиме обмениваться данными. Сегодня в состав участников НТС входят такие компании и организации как Роскомнадзор, Ростелеком, Group-IB, Лаборатория Касперского, Технический центр интернет, RU-CERT, BI.ZONE, Яндекс, Mail.ru, а также голландский исследовательский центр SURFnet/University of Twente.

За время работы проекта накоплены данные, содержащие более 2 млн записей о доменах, когда-либо замеченных во вредоносной активности в зонах .RU, .РФ и .SU; 42% из них — это доменные имена второго уровня, остальные — третьего и ниже. Самую большую долю в .RU и .SU (85%) занимает распространение вредоносного ПО (maleware), а в зоне .РФ — инциденты, связанные с фишингом (47%).

Нельзя не отметить, что «Нетоскоп» обладает большим аналитическим потенциалом. Так, в рамках проекта создан первый в России информационный ресурс http://нетоскоп.рф/, посвященный безопасности в доменном пространстве. На сайте доступны публикуемые на регулярной основе новости, справочные и аналитические материалы о тенденциях распространения всех типов вредоносной активности.

Также посетителям ресурса доступен онлайн-сервис по проверке доменных имен на предмет их использования в «зловредной» активности. Если вы обнаружили мошеннический сайт и ваши опасения подтвердились, то вы можете сообщить об инциденте, и меры будут приняты незамедлительно.

Обращения о ресурсах с противоправным контентом, сообщения о случаях фишинга, несанкционированного доступа к информационным системам, а также о фактах размещения и распространения вредоносных программ с доменных имен в зонах .RU, .РФ и .SU попадают на рассмотрение к компетентным организациям и затем к регистраторам. Далее, на основании правил регистрации, регистратор вправе прекратить делегирование доменных имен для ресурсов, замеченных в том или ином противоправном действии. Конечно, если владелец ресурса готов сотрудничать, то есть «перевоспитать» свой сайт, устранив с его страниц зловред, работа домена будет восстановлена.

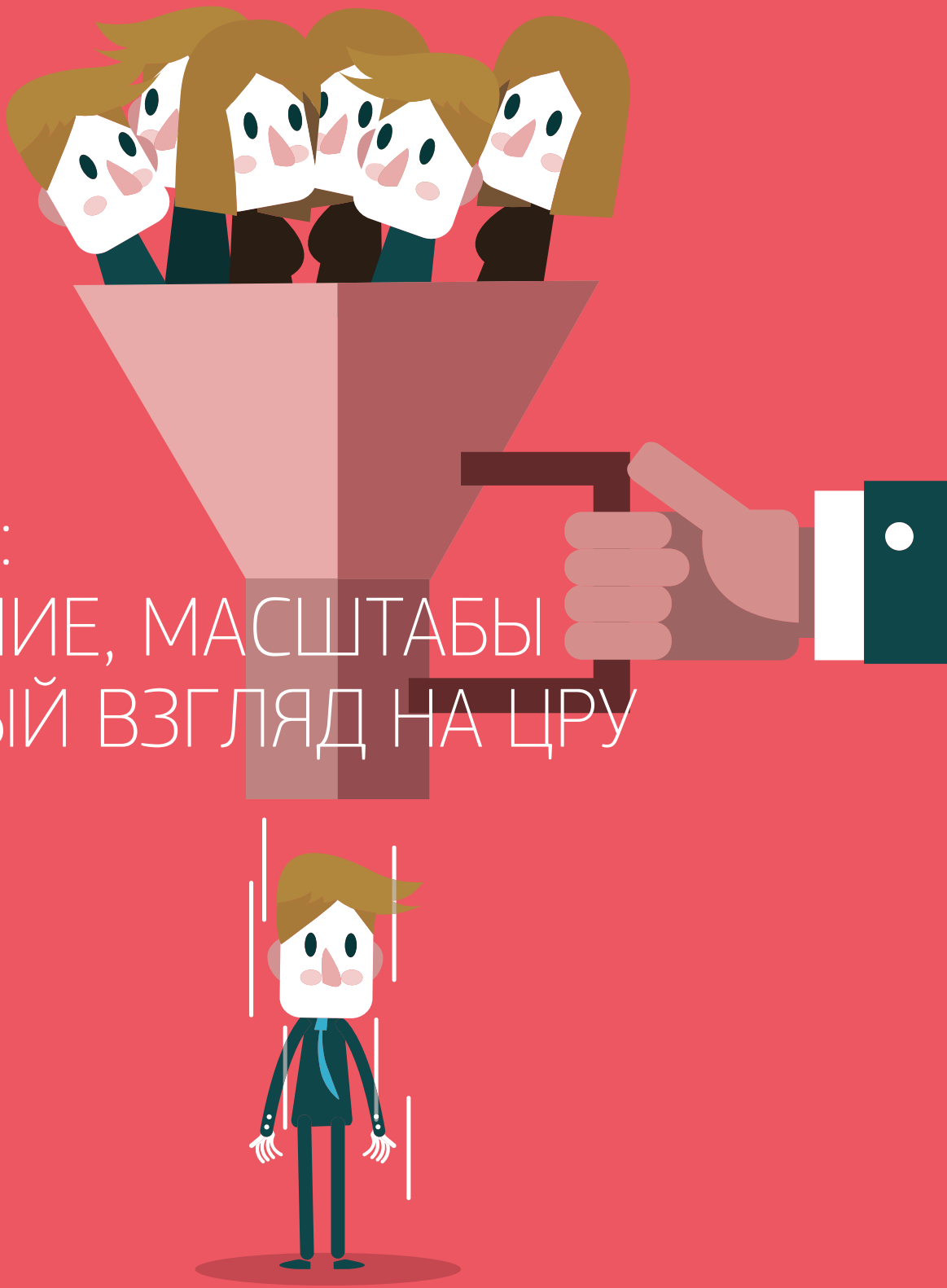
Подобная работа представляется очень важной, поскольку это и механизм саморегулирования на уровне отрасли и одновременно возможность противодействовать злоумышленникам без привлечения правоохранительных органов.

Другой пример, когда при участии отрасли создаются условия для комфортного и безопасного размещения сайтов — **кириллическая доменная зона .ДЕТИ**. Это адресное пространство предназначено исключительно для размещения сайтов детской тематики. Чтобы обеспечить безопасное использование ресурсов этой доменной зоны, в ней реализована **система мониторинга**.

Ее главная задача — выявлять нарушения по всем типам вредоносной активности, а также факты, связанные с распространением запрещенной для детей информации. Работа системы обеспечивается службой реагирования, которая функционирует в двух режимах — автоматическом и ручном; ежедневный мониторинг производится автоматически с использованием программного комплекса, а вот проверкой информации, которая определяется роботом как негативная, занимаются специалисты.

Таким образом, это является еще одним примером саморегулирования на уровне одного из участников интернет-индустрии.

АВТОР: ДЕНИС ЖИЛИН, КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ



УТЕЧКА: ЗНАЧЕНИЕ, МАСШТАБЫ И НОВЫЙ ВЗГЛЯД НА ЦРУ

.TXT
ОЛЕГ ДЕМИДОВ

7 МАРТА НА САЙТЕ ПРОЕКТА WIKILEAKS БЫЛ ОПУБЛИКОВАН МАССИВ ДАННЫХ ПОД НАЗВАНИЕМ YEAR ZERO, КОТОРЫЙ, ПО СЛОВАМ АДМИНИСТРАТОРОВ ПРОЕКТА, ЯВЛЯЕТСЯ ЛИШЬ ПЕРВОЙ ЧАСТЬЮ БОЛЕЕ ОБШИРНОГО МАССИВА, НАЗВАННОГО ИМИ VAULT 7 («УБЕЖИЩЕ 7»). УТВЕРЖДАЕТСЯ, ЧТО ВСЯ ЭТА ДОКУМЕНТАЦИЯ ИЗНАЧАЛЬНО БЫЛА СОЗДАНА ЦРУ И ПРЕДСТАВЛЯЕТ СОБОЙ «БАЗУ ЗНАНИЙ» ВЕДОМСТВА О ЕГО ПРОГРАММАХ ПО ВЗЛОМУ ЭЛЕКТРОННЫХ ПЛАТФОРМ И УСТРОЙСТВ, ИНТЕРНЕТ-СЕРВИСОВ, ПЕРЕХВАТУ СОДЕРЖИМОГО ОНЛАЙН-КОММУНИКАЦИЙ И ОСУЩЕСТВЛЕНИЮ ЦЕЛЕВЫХ ОПЕРАЦИЙ В КИБЕРПРОСТРАНСТВЕ.

Эта утечка является одной из крупнейших в истории ЦРУ и спецслужб вообще, и по объему раскрытых документов сразу же превзошла серию публикаций программ тайной электронной слежки и создания киберарсенала АНБ, начатую Эдвардом Сноуденом летом 2013 г. До этого достоянием общественности становились лишь отдельные кибероперации ЦРУ. В их числе разработка средств кибершпионажа и саботажа для замедления ядерной программы Ирана с 2005 по начало 2010-х гг. (включая печально известный компьютерный червь Stuxnet, внедрение которого в автоматизированные системы управления технологическим процессом (АСУ ТП) на производственном комплексе в г. Натанз в 2009–2010 гг. привело к выводу из строя каскада центрифуг для обогащения урана). Кроме того, в феврале 2017 г. Wikileaks опубликовали документы, согласно которым в 2012 г. ЦРУ вело агентурную и электронную слежку за лидерами президентской избирательной кампании во Франции. То есть в принципе наличие у ЦРУ собственных киберсредств для целевых операций и программ их применения — не новость, однако масштаб таких программ до публикаций Vault 7 никто не представлял.

При этом перед нами до сих пор лишь вершина айсберга — Wikileaks заявили, что опубликовали лишь первую часть утекшего архива (Year Zero), охватывающего документы за 2013–2016 г. Общий объем массива самих средств вредоносного ПО ЦРУ оценивается в несколько сотен млн строк кода, для сравнения, код поискового движка Google, одного из крупнейших проектов в истории программирования, насчитывает порядка 2 млрд строк. Wikileaks приняли решение не публиковать файлы и документы, содержащие сам компьютерный код разработанного ЦРУ вредоносного ПО. Это разумно, так как публикация таких средств в открытом доступе мгновенно позволит пополнить ими свои арсеналы зарубежным спецслужбам и компьютерным преступникам по всему миру. В этом смысле как перед ЦРУ, так и перед Wikileaks сейчас стоит единственная общая задача — предотвратить расползание средств из киберарсенала ЦРУ по международному рынку компьютерной преступности.

Впрочем, значительная часть «базы знаний» содержит не готовые образцы вредоносного ПО или детальное описание уязвимостей, а скорее концепции, черновые наброски подходов к преодолению защиты и построению векторов атаки на те или иные ИТ-продукты и решения. Вообще, модель организации данных о киберарсенале спецслужбы достаточно любопытна: она представляет собой вики-массив электронных документов и файловых приложений, которые могут пополнять, редактировать и комментировать зарегистрированные пользователи системы. Сообщество пользователей превышает 5 тыс. чел. и включает в себя штатных сотрудников ЦРУ и представителей компаний-подрядчиков (по некоторым оценкам, 10–12 структур), работающих со спецслужбой в рамках проектов по развитию киберсредств. Движок базы знаний также основан на ПО Confluence, разработанном частной компанией Atlassian. По мере обновления данных по тем или иным проектам формируются разные версии соответствующих вики-страниц — в общей сложности массив включает 1136 предыдущих версий отдельных страниц.

В итоге, все это выглядит более похожим на базу знаний какой-нибудь ИТ-корпорации, чем на архив документов спецслужбы в стереотипном представлении с нечитаемыми машинно сканами документов, грифами «секретно» и десятками подписей ответственных сотрудников. Разведка как бюрократическая машина тоже модернизируется, причем не

только по формату, но и по стилю коммуникаций, который тоже напоминает общение в хакерском сообществе и частных компаниях. Страницы с описаниями средств эксплуатации уязвимостей насыщены интернет-мемами, комментаторы зачастую позволяют себе весьма неформальную лексику, описывая грубые ошибки в коде систем, которые удалось взломать, и так далее. Для обмена идеями перспективных разработок с 2009 г. организован внутренний формат «Симпозиума по сетевым технологиям, инжинирингу, исследованиям и развитию» с иронической аббревиатурой NERDS. Названия ряда техник атак и проектов по разработке вредоносного ПО несут отсылки к популярным персонажам компьютерных игр и кинематографа.

КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ЦРУ

АТАКИ НА МОБИЛЬНЫЕ УСТРОЙСТВА

Одним из наиболее масштабных и опасных проектов ЦРУ, судя по Vault 7, является разработка средств обхода защиты, удаленного контроля и тайного сбора данных с мобильных устройств пользователей (планшеты, смартфоны).

Среди разработок под Android — 8 эксплойтов (средств эксплуатации уязвимостей), позволяющих осуществлять удаленный доступ к устройству после заражения; два из них нацелены на продукцию Samsung (смартфоны Samsung Galaxy, Nexus и планшеты Samsung Tab). Большинство разработок (15) основаны на технике атаки с повышением привилегий в системе: после изначальной доставки вредоносного кода в систему контролирующий его через Сеть злоумышленник может преодолевать различные слои защиты устройства и в конечном счете получить почти неограниченный контроль над ним (root access). При этом становятся доступны возможности удаленного управления камерой устройства, микрофоном, файлами и данными, хранящимися в системе, записи действий пользователя с клавиатурой (кейлоггинг), съема данных геолокации, записи переписки и разговоров, блокировки обновлений системы, самостоятельной установки и удаления приложений и проч. Три эксплойта адаптированы под заражение системы через уязвимости в мобильных браузерах (Chrome, Opera, мобильный браузер Samsung). Для реализации такой атаки пользователь должен перейти на скомпрометированный либо фишинговый сайт, с которого эксплойт незаметно загружается в систему и заражает ее. Сходные возможности предлагают эксплойты для устройств на iOS (iPhone). Однако полностью скомпрометировать защиту устройств iPhone позволяет лишь один эксплойт. Остальные эксплойты ЦРУ представляют собой техники атаки для преодоления отдельных средств и уровней защиты в программной платформе iOS. Так, некоторые вредоносные программы позволяют обходить «песочницу» (sandbox) — программную функцию в iOS, которая блокирует прямой доступ приложения к самой операционной системе.

По оценкам экспертов, в сумме применение таких эксплойтов позволяет практически полностью взломать защиту тех версий мобильных ОС, под которые они разработаны. Однако из архива данных Vault 7 складывается впечатление, что ЦРУ несколько отстает в написании средств эксплуатации уязвимостей от развития и обновления самих ОС.

Вообще положение с уязвимостями достаточно интересно. С одной стороны, только в разработках для компрометации мобильных устройств использовано до нескольких десятков так называемых уязвимостей нулевого дня (zero-days) в мобильных ОС. Особая опасность таких уязвимостей в том, что они неизвестны вендору (производителю) соответствующего продукта и отраслевому сообществу — а значит, они еще не закрыты, для них не разработаны исправления (патчи), которые устраняют угрозу атаки. Отсюда и понятие «нулевого дня». Однако в то же время быстрое обновление версий мобильных ОС на рынке во многом сводит на нет успехи ЦРУ в выявлении уязвимостей нулевого дня и разработке использующих их средств для версий ОС прошлого поколения. Так, сразу после публикации Vault 7 представитель Apple сообщил СМИ, что все ключевые уязвимости, выявленные ЦРУ в iOS, уже устранены компанией. Отсюда может следовать двоякий вывод — либо ЦРУ и вправду пока не успевает за рынком, либо в Vault 7 просто не отражены последние наработки спецслужбы: по оценкам экспертов, база знаний отражает ситуацию с развитием проектов «мобильного» отдела полтора-два года назад.

Особую тревогу у пользователей вызвали сообщения том, что эксплойты ЦРУ позволяют взламывать защиту приложений на мобильных устройствах и свободно перехватывать переписку из защищенных мессенджеров. Это не совсем так. Инструменты ЦРУ действительно позволяют

собирать данные переписки, которую пользователь ведет в защищенных мессенджерах, но их криптографическая защита при этом остается нетронутой. Вместо этого в тех случаях, когда внедрение эксплойта дает злоумышленнику удаленный доступ к устройству, для чтения переписки используются возможности других его приложений. Например, активируется функция снимков экрана устройства (скриншотов) в тот момент, когда пользователь запускает приложение-мессенджер и ведет в нем переписку. Сохраненные скриншоты со снимками текста переписки отсылаются на сервер, который контролируют агенты ЦРУ. При этом ЦРУ не создало инструментов, которые бы позволяли преодолевать криптографическую защиту самих мессенджеров и расшифровывать данные из них напрямую. Скомпрометированы в данном случае операционные системы самих устройств, а не сторонние защищенные приложения.

АТАКИ НА ДЕСКТОПНЫЕ УСТРОЙСТВА И СЕТЕВОЕ ОБОРУДОВАНИЕ

По аналогии с разработкой средств атак на мобильные ОС, ЦРУ создало отдельную подборку уязвимостей и линейку эксплойтов для взлома операционных систем и других программных платформ десктопных (настольных) устройств. Часть из таких эксплойтов может быть внедрена в систему удаленно — через содержащий вредоносный код файл, направленный фишинговым электронным письмом, или при входе на скомпрометированный сайт в Интернете. Однако существенная часть средств предполагает локальное внедрение в систему — через внешний носитель. Это важный для ЦРУ функционал, так как целевые операции ведомства зачастую требуют доступа к системам и инфраструктуре, которая находятся на защищенных объектах и надежно изолированы от сети. Так, в линейку средств ЦРУ входят вирусы для передачи информации с компьютеров под управлением Windows, физически изолированных от сети (air-gapped systems). Одним из таких инструментов является HammerDrill v2.0: средство, которое внедряется в Nero — популярное ПО для записи информации на оптические диски (CD и DVD) и затем передается с компьютера на компьютер вместе с диском, на котором записано. Попадая на компьютер под управлением Windows, HammerDrill заражает его вредоносной программой-трояном и может собирать с системы необходимые данные. Другие направления разработки включают средства для заражения программой-трояном внешних USB-носителей (флэшек), которые также при попадании в систему под Windows запускают вредоносный код и собирают из системы необходимые данные. Для настольной продукции Apple (MacBook) был разработан руткит (вредоносное ПО, позволяющее злоумышленнику дистанционно контролировать систему на уровне программного ядра) под названием QuarkMatter. После внедрения в систему с помощью эксплойта это ПО переписывает низкоуровневую программную прошивку EFI на устройствах MacBook, давая автору атаки контроль над системой. Поскольку прошивка EFI находится ниже по уровню, чем сама ОС MAC, такое вредоносное ПО крайне трудно обнаружить и самостоятельно удалить из системы.

Эксплуатация уязвимостей в ОС различных устройств (ПК и сетевого оборудования) осуществлялась и в рамках другого проекта инженерно-технической группы — HIVE. Проект реализован в виде вики-каталога вредоносного ПО, который содержит специализированные и при необходимости обновляемые программные закладки (implants) для различных ОС и программных платформ, в том числе Windows, OS X, Solaris, MikroTik (используется в маршрутизаторах) и Linux. Закладки в данном случае представляют собой скрытно внедряемые в систему программы, либо преобразованные фрагменты кода исходной программы, которые позволяют осуществлять несанкционированный доступ к ресурсам системы, изменяя свойства ее защиты. То есть, внедряя программные закладки за счет эксплуатации найденных в перечисленных ОС уязвимостей, ЦРУ в дальнейшем могло осуществлять удаленный контроль через сеть над устройствами.

АТАКИ НА «УМНЫЕ» ТЕЛЕВИЗОРЫ

Много шума в СМИ наделал и проект Отдела встраиваемых систем (EDB) ЦРУ Weeping Angel («Плачущий ангел») по взлому с целью скрытого сбора данных «умных» телевизоров Samsung серии F8000, подключаемых к Интернету. После того как разработанные ЦРУ средства внедрялись в систему, при выключении устройства владельцем активировался режим, имитирующий отключение системы. Отключался экран и светодиодные индикаторы на передней панели устройства, что создавало у пользователя впечатление, что его телевизор

действительно выключен. При этом микрофон, которым оснащены LED-телевизоры Samsung F8000, напротив, включался и записывал аудиоданные — а именно, используя встроенную систему распознания голоса, разговоры людей рядом с устройством. Записанные данные затем сохранялись (в объеме до 700 мегабайт) и отправлялись на сервер, контролируемый спецслужбой. Таким образом, «умные ТВ» Samsung фактически исполняли функцию устройств для тайной прослушки собственных пользователей.

Однако в действительности ЦРУ и их британским коллегам удалось достичь лишь частичного успеха в его реализации. По сути, единственным способом получить контроль над тем или иным конкретным устройством было внедрение в него программной нагрузки через внешний съемный носитель — например, USB-флэшку. Кроме того, в режиме имитации отключения устройства блокировалось подключение к сетям Wi-Fi, не отключались светодиодные индикаторы на задней панели телевизора — в итоге пользователь мог заподозрить, что устройство работает ненормально. Наконец, разработанное для удаленного исполнения команд ПО не работало с программными прошивками F8000 после версии 1116,— соответственно, обновление прошивки телевизора сводило на нет всю проделанную работу.

ЦРУ отнюдь не является пионером идеи взломать устройства «умного телевидения». Уже к 2013 г. проблемы с безопасностью и уязвимости «умных» телевизоров были уже достаточно широко известны как ИТ-отрасли, так, видимо, и спецслужбам.

РАЗРАБОТКА КОНЦЕПЦИИ АТАК НА «УМНЫЙ» ТРАНСПОРТ

В массиве данных ЦРУ присутствует документ 2014 г., в котором приводится список «перспективных направлений работы» подразделения. В перечне среди прочего фигурирует разработка средств для эксплуатации устройств Интернета Вещей, а также систем транспорта и операционной системы QNX. QNX — это коммерческая распределенная ОС для рынка встраиваемых систем, разработанная канадской компанией Quantum Software Systems, в 2010 г. приобретенная разработчиком защищенных средств коммуникации BlackBerry. В настоящее время она используется в ряде отраслей, включая 3D-навигацию и развлекательные мультимедийные системы. Но в последнее время BlackBerry продвигает QNX прежде всего в нише управления различными системами «умного» автотранспорта. В настоящее время основанные на QNX мультимедийные системы используются примерно в 60 млн автомобилей производства Ford, Fiat и Maserati. В октябре 2016 г. Blackberry расширила сотрудничество с Ford, подписав соглашение, согласно которому разработка Ford SYNC — информационно-развлекательной системы нового поколения в автомобилях Ford будет вестись на базе QNX.

Таким образом, ЦРУ действительно рассматривало возможности эксплуатации систем умного автотранспорта, ориентируясь на поиск уязвимостей в ключевых программных платформах в этой нише. Потенциальные возможности в этой сфере огромны, т.к. современные автомобили до предела насыщены информационными технологиями и системами обмена данными на различных уровнях от тех же систем развлечения и предоставления информации водителю до систем, передающих телематические данные и непосредственно контролирующих работу ключевых узлов автомобиля, включая фары, тормоза, рулевое управления и сам двигатель. Даже если не говорить о нише беспилотных авто и наиболее прорывных проектов с точки зрения компьютеризации систем управления (Tesla), достаточно упомянуть, что ПО легковых авто последнего поколения по данным того же Ford составляет до 150 млн строк кода — больше, чем в магистральных авиалайнерах. В столь сложных системах неизбежно находятся уязвимости, позволяющие построить вектор атаки, особенно если их неотъемлемой функцией является беспроводная передача данных через Wi-Fi и Bluetooth. Как и в случае с «умными телевизорами», ЦРУ не первым обратило внимание на возможности взлома «умных авто». В последние два-три года взлом различных компонентов «умных авто» стал одним из популярных упражнений для специалистов по информационной безопасности. Одним из наиболее ярких примеров можно назвать взлом систем управления 2014 Jeep Cherokee, который успешно провели в 2015 г. ИБ-исследователи Чарли Миллер и Крис Валасек. За счет эксплуатации уязвимости в информационно-развлекательной и навигационной системе Uconnect экспертам в конечном счете удалось получить контроль над управляющими системами автомобиля, что позволило удаленно поворачивать руль, кратковременно блокировать тормоза и заглушать двигатель. По итогам тестового взлома производитель (Fiat Chrysler) вынужден был отозвать 1,4 млн

авто для устранения уязвимостей. Вопиющим случай оказался еще и потому, что за счет уязвимости в системе Uconnect исследователи получили возможность удаленного доступа к тысячам других использующих ее транспортных средств.

Однако и в этом случае огромные потенциальные возможности не были реализованы ЦРУ, если судить по опубликованной части массива Vault 7. В нем отсутствуют списки конкретных уязвимостей в ПО «умных авто», для которых предлагается разработать средства эксплуатации. Тем более не упоминаются сами такие средства и какие-либо проработанные векторы атак. Даже сама постановка задачи с «невидимыми покушениями» является домыслом Wikileaks, в чем те честно признаются. Вместе с тем, это никак не устраняет проблему на будущее — разведслужба несомненно создаст действующие инструменты для кибероперациий с «умным транспортом», это лишь вопрос времени. В этом смысле угроза эксплуатации ИТ-инфраструктуры «умного транспорта» в кибероперациях спецслужб пока явно недооценена его производителями и пользователями.

ОБХОД СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

Отдельным направлением работы спецслужбы стало создание целой линейки средств вредоносного ПО для компрометации и обхода самых распространенных антивирусных решений для конечных пользователей и корпоративных клиентов. Каталог с описанием таких средств для 21 антивирусного продукта включает таких отраслевых лидеров как Comodo, Avast, Kaspersky, AVG, ESET, Symantec, Microsoft Security Essentials (встроенный антивирус для Windows). Используемые техники и средства эксплуатации уязвимостей в антивирусном ПО достаточно разнообразны и продвинуты, но не во всех случаях гарантируют их авторам гарантированный обход всех средств антивирусной защиты от того или иного производителя. Например, для обхода защиты продуктов Лаборатории Касперского эксплуатируется ошибка в обработке обращений самого антивируса к одной из динамически подключаемых библиотек (DLL) в ОС Windows. В результате злоумышленник может подменить исходную библиотеку собственной, к которой и будет обращаться рабочий процесс антивируса — таким образом, антивирусная защита будет преодолена и открыта возможность для атаки на систему. Однако такая уязвимость присутствует только в предыдущих версиях антивирусного ПО Лаборатории Касперского, которые адаптированы для работы с OS Windows XP и Windows 7. Для обхода защиты других антивирусных средств (F-Secure, Avira) используются две уязвимости в функционировании их эвристических алгоритмов обнаружения и классификации потенциальных вредоносных программ.

Главный вывод по этому направлению работы формулируют сами сотрудники ЦРУ в своих примечаниях к техническому описанию средств эксплуатации уязвимостей: дело не в блестящем уровне созданных спецслужбой эксплойтов, а в обилии грубых и местами курьезных ошибок в коде самих антивирусных средств. И даже с учетом этого в ряде случаев ведомству удалось выявить уязвимости и разработать средства их эксплуатации лишь для старых и уже в основном неактуальных версий антивирусного ПО.

ПРОТИВОДЕЙСТВИЕ РАССЛЕДОВАНИЮ КОМПЬЮТЕРНЫХ АТАК

Помимо разработки средств обхода и эксплуатации антивирусной защиты устройств пользователей, сотрудники ЦРУ уделили серьезное внимание мерам противодействия расследованию совершаемых ими атак и иных операций. В базе данных ведомства содержится блок детальных инструкций по техникам написания кода вредоносного ПО и осуществления компьютерных атак таким образом, чтобы не оставлять «цифровых отпечатков», которые бы компрометировали саму спецслужбу, а также правительство США и «организаций-партнеров» при расследовании инцидентов. Одним из источников рекомендаций по написанию вредоносного ПО служит документ-мануал «Правильные и неправильные методы проведения специальных мероприятий». Весьма интересный документ «Требования к криптографии Управления сетевых операций» содержит подробные инструкции по применению сотрудниками ЦРУ средств криптографической защиты информации при организации сетевых атак, удаленном управлении вредоносным ПО на зараженных системах.

НАКОПЛЕНИЕ И ИСПОЛЬЗОВАНИЕ ЧУЖИХ РАЗРАБОТОК ВРЕДОНОСНОГО ПО

В дополнение к разработке собственного вредоносного ПО ЦРУ активно изучало чужие

разработки и стремилась заимствовать и адаптировать их для решения своих задач. Согласно краткому описанию в шапке самого документа, поддержание такой базы данных с точки зрения спецслужбы могло нести двойную пользу. Во-первых, «полуфабрикатные» образцы чужого вредоносного кода могут быть быстро и с небольшими ресурсозатратами доработаны для решения ЦРУ точечных задач вместо разработки с нуля многофункциональных собственных инструментов. Во-вторых, применение заимствованных у киберпреступников и, возможно, зарубежных хакерских группировок паттернов вредоносного ПО и техник компьютерных атак опять же помогает решить задачу запутывания расследования инцидентов и уничтожения своих «цифровых отпечатков».

Стоит также отметить, что объектом внимания спецслужбы стали кибероперации отдельных группировок, предположительно связанных с их военными коллегами из АНБ. Так, отдельный файл посвящен анализу ошибок, которые привели к раскрытию деятельности Equation Group — группировке-источнику повышенной угрозы (APT), которая в течение 14 лет с 2001 по 2015 гг. атаковала при помощи крайне передовых средств вредоносного ПО правительственные и корпоративные цели как минимум в 42 странах, оставаясь незамеченной. В конечном счете деятельность Equation Group была раскрыта Лабораторией Касперского благодаря ряду допущенных членами группировки ошибок в техниках атак и «заметании следов» — и теперь ЦРУ пытается предусмотреть эти ошибки.

МАСКИРОВКА АГЕНТУРНЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ВРЕДОНОСНОГО ПО

Наконец, важный для понимания методов целевых операций ЦРУ проект — Fine Dining, еще один инструментарий техник атак. Примечателен он тем, что содержит 24 «обманные» программы, которые позволяют агенту ЦРУ внедрять в систему вредоносное ПО прямо при свидетелях. Эти приложения визуально маскируют процесс работы агента с устройством, в результате у непосвященного наблюдателя эта деятельность не вызовет подозрений: средства Fine Dining позволяют маскировать процесс внедрения вредоносного ПО под запуск агентом видеоплеера, работу с презентацией в PowerPoint, компьютерную игру и даже запуск антивирусного сканера (Антивирус Касперского, McAfee, Sophos). Разработка столь изощренного инструментария показывает, насколько большую роль в программах киберразведки ЦРУ играет агентурная работа, и в то же время — насколько возможности спецслужбы ограничены необходимостью внедрять в системы вредоносное ПО не удаленно, через сеть, а через прямой физический доступ. Для сравнения, ничего подобного в киберарсенале АНБ за 4 года разоблачений не нашлось — и это логично, т.к. военные работают в рамках концепции радиоэлектронной разведки (signals intelligence, SIGINT) и развивают технологии удаленных атак на системы. Для ЦРУ же основным форматом исторически являлась именно агентурная разведка (human intelligence, HUMINT). В этом смысле весь гигантский киберарсенал ведомства, включая ПО и инфраструктуру для удаленных операций в Сети, по большому счету остается продвинутым технологическим приложением к полевой работе агентов — хотя документы Vault 7 и позволяют говорить о технологически обусловленном синтезе SIGINT и HUMINT.

НЕКОТОРЫЕ ВЫВОДЫ И НАБЛЮДЕНИЯ

Любые обобщения в отношении нынешней утечки и программ развития киберсредств ЦРУ следует считать промежуточными и неполными, пока не опубликованы остальные имеющиеся в распоряжении Wikileaks данные. С этой оговоркой уместно обозначить несколько моментов.

1. Систематическая и развернутая в индустриальном масштабе деятельность ЦРУ по развитию собственного арсенала киберсредств для целевых разведопераций создает достаточно серьезную постоянную угрозу как для пользователей, так и для вендоров продукции и решений в широком диапазоне ниш ИТ-рынка. Сложившаяся ситуация ставит перед крупнейшими вендорами ОС, а также самих мобильных и десктопных устройств (Apple, Google, Microsoft, Samsung и др.) задачу по выработке консолидированной стратегии повышения уровня защиты ОС и разработки новых архитектурных решений и стандартов для нейтрализации системной угрозы со стороны государственных программ электронной разведки.
2. ИТ-отрасль США, за исключением узкого круга специализированных подрядчиков

спецслужб, не выглядит вовлеченной в те или иные формы сотрудничества с ЦРУ. В массиве данных Vault 7 нет данных о взаимодействии ИТ-вендоров и разработчиков с разведслужбой. Речь идет лишь о том, что ЦРУ методично и целенаправленно собирало информацию об уязвимостях в продукции различных компаний и разрабатывало разнообразные средства эксплуатации этих уязвимостей — самостоятельно и при содействии других спецслужб и подрядчиков. В этом смысле нынешний сюжет несколько отличается от истории программ АНБ.

3. Несмотря на весь свой масштаб и технологическую изощренность, созданный ЦРУ киберарсенал не является инструментом массового неизбирательного перехвата и сбора данных (bulk data interception). Формула, которая отражает назначение раскрытых программ ЦРУ: «глобальный инструментарий для точечных целевых операций».
4. Наличие арсенала средств для кибероперации и тайного сбора данных в Сети становится не только приоритетной задачей государственного уровня, но и ключевым активом в смысле удержания и расширения аппаратных полномочий и борьбы за бюджет на уровне отдельных силовых ведомств, подчас конкурирующих друг с другом. В более широком смысле раскрытие утечки ЦРУ подводит черту под очевидным фактом состоявшейся вепонизации киберпространства. Государства по всему миру применяют проактивные киберсредства в постоянном и необходимом режиме, зачастую не делая принципиальных различий между целями на своей территории и за рубежом. В этих условиях наивно полагать, что гражданские и военные спецслужбы России, Китая, Израиля, государств ЕС и вообще любой другой страны не развивают собственные средства тайного сбора данных и программы кибероперации или готовы от них отказаться.
5. Теоретически самая страшная угроза, которую могли бы нести раскрытые проекты ЦРУ — разработка средств, позволяющих гарантированно взламывать криптографическую защиту в реализациях ключевых протоколов и стандартов (AES, RSA, TLS/SSL) и таким образом разрушать существующие экосистемы безопасности как крупнейших ИТ-вендоров, так и Интернета в целом. Но, исходя из уже раскрытой Wikileaks части данных, ЦРУ даже не ставило перед собой в явном виде такую задачу. Для пользователя, чье устройство стало целью атаки, а данные похищены, разница в том, была ли при этом взломана криптографическая защита используемых им сервисов, или нет, может быть неочевидна. На самом деле она принципиальна: даже самые отработанные и передовые методы атак с эксплуатацией уязвимостей в архитектуре ПО конкретных моделей и продуктов ИТ-рынка требуют доставки вредоносного ПО на устройство. Для этого приходится выстраивать некую более-менее специфическую, а во многих случаях и индивидуальную схему, вектор атаки, чтобы обеспечить применение эксплойта на том или ином конкретном устройстве.
6. На основе уже раскрытых данных можно сказать, что ЦРУ уступает АНБ по степени «продвинутости» и технологическому уровню своих разработок. Несмотря на обилие выявленных уязвимостей в мобильных и десктопных ОС, антивирусных продуктах и иных системах, разработку большого количества достаточно серьезных эксплойтов, закладок и других средств, раскрытый арсенал ЦРУ не содержит ни принципиально новых техник атак, ни по-настоящему прорывных образцов вредоносного кода. Кроме того, в документах утечки нет описания инструментов, которые бы в полной мере подпадали под условное понятие «кибероружия»: например, средств эксплуатации уязвимостей в АСУ ТП критически важных объектов и стратегических оборонных инфраструктур. Впрочем, с учетом наличия у ЦРУ солидного прошлого опыта таких разработок, это скорее говорит о неполноте данных в опубликованном массиве документов, чем о том, что подобные проекты были свернуты.
7. Нынешние утечки могут стать катализатором давно необходимых подвижек и изменений по крайней мере в двух областях. Одна из них — согласование и внедрение стандартов

и механизмов безопасности в тех нишах, где они по различным причинам отсутствуют. Например, речь идет об Интернете Вещей, устройства которого сегодня массово эксплуатируются для организации беспрецедентно масштабных сетевых атак, которые уже угрожают устойчивости ключевых сервисов Интернета, включая глобальную DNS. Еще одна область, где стандартизация безопасности серьезно отстает от развития самой технологии — «умный транспорт», который как раз попал в прицел ЦРУ. Наконец, подвижки необходимы и в таких областях, как внедрение обязательного шифрования данных на нижних уровнях сетей производственных объектов (уровень обмена данными между АСУ ТП). Угроза со стороны государственных спецслужб может стать для заинтересованных сторон в каждой из этих ниш (вендоры, операторы, интеграторы, национальные регуляторы и пользователи) необходимым стимулом к ускоренной разработке и внедрению углубленных стандартов и архитектурных принципов безопасности.

Вторая область, в которой остро необходим прогресс — выработка международного режима ответственного поведения в киберпространстве, в том числе в части разумного ограничения государственных кибероперация. С учетом последних событий, надежд на то, что этот вопрос решат между собой сами государства, откровенно мало. Принимаемые на международных площадках доклады и меры доверия пока по большей части остаются декларациями о намерениях, а бюджеты программ спецслужб на создание военизированного киберпотенциала на много порядков превышают расходы на продвижение дипломатических инициатив по регулированию поведения в киберпространстве. Ситуацию может изменить альянс глобальных ИТ-вендоров и инженерного сообщества, чьим бизнес-интересам и принципам деятельности напрямую угрожают государственные программы кибероперация. В этом смысле, российские, китайские и американские вендоры, разработчики и сетевые инженеры могут оказаться в одной лодке, даже пока их правительства скованы взаимным недоверием и гонкой цифровых вооружений. Частных игроков между собой объединяют интересы бизнеса, а с сетевыми инженерами их сближает необходимость поддержания единства и открытости Интернета, без которой невозможно существование глобального трансграничного ИТ-рынка.

УТЕЧКИ МАРШРУТОВ BGP

.TXT

АЛЕКСАНДР ЛЯМИН
Qrator Labs

МНОГИМ КАЖЕТСЯ, ЧТО ОНИ ДЕТАЛЬНО ПРЕДСТАВЛЯЮТ СЕБЕ, КАК РАБОТАЕТ ИНТЕРНЕТ. ВОТКНУЛ КАБЕЛЬ, ПОДОЖДАЛ НЕМНОГО, ВБИЛ ТРЕБУЕМЫЙ АДРЕС — И ВОТ ОН, ВО ВСЕЙ КРАСЕ. КАК ВЫ УЖЕ ПОНЯЛИ — ЭТО НЕ ДО КОНЦА ВЕРНО.

Ликвидацию безграмотности стоит начинать с основ. Так и здесь, в случае с интернетом, важно не обманывать себя и хорошо понимать значение данного понятия, образованного путем слияния двух слов: interconnected (объединенные) и networks (сети).

Не существует единого интернета, как единой сети или единого физического пространства — он представляет собой сеть, узлы в которой объединены разными отношениями: пирингом (соседством), в рамках которого соседние «сети», а на деле — автономные системы, обмениваются трафиком, а также отношения вида «провайдер-клиент».

А происходит это как раз с помощью динамического протокола, называемого BGP (Border Gateway Protocol), или «протокола пограничной маршрутизации», который позволяет владельцам автономных систем обмениваться информацией о маршрутах движения трафика. То есть недостаточно соединить собственные автономные системы физическим кабелем, необходимо заключить договоренности и соглашения, которые сделают такой обмен трафиком возможным. И договариваются об этом поставщики электронных услуг — в первую очередь провайдеры связи, поставщики соединения для индивидуальных пользователей и бизнеса. Чем выше качество услуги, тем выше спрос, тем лучше конкурентное положение, тем большую цену можно просить за такую услугу — вот почему корректные маршруты движения трафика так важны. Наличие некорректных путей увеличивает временные и финансовые издержки, предоставляемый сервис деградирует, а трафик концентрируется в потенциально узких местах.

BGP протокол технически не обязывает операторов взаимодействовать, что используется операторами связи в случае пиринговой войны. В большинстве случаев пиринговые войны приводят к отсутствию прямой связности между операторами связи — в этом случае трафик идет не напрямую, а через сети третьих операторов связи, значительно увеличивая сетевые задержки. Однако, при отсутствии желающих пропускать через себя трафик, данные сети оказываются полностью недоступны друг для друга. Например, в настоящее время, крупнейшие операторы IPv6 Cogent Communications и Hurricane Electric не имеют ни прямых, ни альтернативных маршрутов. Это может приводить к проблемам доступа для пользователей не только внутри этих двух сетей, но и для их клиентов.

BGP — уникальный протокол, наряду с DNS представляющий собой основу функционирования интернета. Его современная версия, используемая с 1996 года, требует доработки и улучшения, но об этом чуть позже. Здесь же важно отметить следующее: текущий уровень финансирования, вложения человеческих и временных ресурсов в развитие тех стандартов и механизмов, благодаря которым интернет стал таким всеобъемлющим, каким мы его знаем сегодня, катастрофически низок.

BGP создавали с допущением, что сетевые инженеры понимают, что делают. Как и многие другие элементы глобальной сети, этот протокол создавался, когда общее количество автономных систем исчислялось десятками — сейчас же их уже более 50 тысяч. Понятно, что число технически грамотных инженеров не может расти теми же темпами.

Куда интереснее процесс, в котором протоколы, стандарты и системы, создаваемые на базе доверия людей и организаций друг к другу, сохранили собственную работоспособность даже тогда, когда интернет стал «наполняться» деньгами — в начале девяностых годов прошлого столетия. Однако избежать проблем, возникающих вследствие интенсивного роста количества конечных пользователей, не удалось. Поэтому сегодня мы часто говорим о legacy — «наследии», но не в хорошем смысле данного слова, а о проблемном наследии, сегодня становящемся опасным. Опасным, потому что право на пользование интернетом начинает входить в базовые права гражданина развитого и современного государства, без доступа к сети многие люди уже сегодня получают куда меньше возможностей для самореализации.

Сегодня владельцы автономных систем — это коммерческие организации, операторы связи, продающие услуги конечным клиентам: интернет-бизнесу и интернет-пользователям, поэтому и работа протокола BGP в большинстве случаев выражает взаимодействие между операторами. Отсюда первая проблема — маршруты BGP отражают существующие бизнес-отношения, но если маршруты контролируются инженерами, то бизнес — управляющими и владельцами компаний. Это принципиально разные роли, с разными целями и способами достижения желаемого.

Устройство протокола BGP позволяет маршрутизаторам принимать объявленные маршруты (пути трафика от источника к цели), от других BGP-маршрутизаторов, что делает возможным не только автоматическое и децентрализованное вычисление маршрута, но также позволяет обнаруживать инциденты, возникающие вследствие некорректной настройки или простой злонамеренной активности.

«УТЕЧКА МАРШРУТА»

Это появление на пути движения трафика к цели промежуточной точки, которой там быть не должно, но она есть, так как «объявила» свое наличие где-то в пути движения трафика. Внедрившийся в этот путь оператор связи некорректно объявляет путь движения трафика от источника к цели — и маршрут «утекает» в неверном направлении, перестает быть оптимальным, самым дешевым и быстрым. Следствием такой утечки может быть не просто увеличенная задержка, но и частичная или полная недоступность целевого ресурса.

Мы в Qrator Labs, имея опыт решения подобных проблем, считаем, что в большинстве подобных случаев виноваты технические специалисты, не до конца понимающие принципы работы протокола BGP.

Такие «особенности» протокола могут быть использованы для перехвата стороннего трафика, что упрощает «атаку посредника» (man in the middle). Этим (некорректной настройкой протокола) грешат и некоторые транзитные операторы, в том числе и национального уровня. Ключевая проблема здесь — это опциональность любых настроек BGP, включая настройку фильтрации входящих и исходящих маршрутов, которая «сама по себе», или «из коробки», не работает. Между «правильной настройкой BGP» и «хоть какой-нибудь настройкой BGP» лежит огромная пропасть. В первом случае требуются глубокие знания, во втором — умение пользоваться поиском в интернете. А потому уже не кажется невероятным тот факт, что практика копирования и вставки примеров кода так сильно распространена и при настройке BGP.

Отказ в обслуживании (DoS) — крайнее следствие возможных проблем BGP. В большинстве ситуаций неоптимальные маршруты ведут, в первую очередь, к увеличенным задержкам в получении клиентом доступа к файлам, страницам и любым другим данным. Наличие задержек более 300 миллисекунд (3/10 секунды)является заметным для среднестатистическоого человека — оно раздражает. Раздражающие услуги продаются гораздо хуже удовлетворяющих.

Подобное может приводить к достаточно плачевным последствиям, что уже не раз происходило. Так, например, в 2008 году YouTube,

ТИПИЧНЫЙ ПРИМЕР:

Провайдер, который обслуживает ваш канал, использует список сетей клиентов, как единственный механизм фильтрации исходящих анонсов. Как результат, вне зависимости от источника анонсов, клиентские сети всегда будут анонсироваться по всем доступным направлениям. Пока существуют анонсы напрямую, данная проблема остается трудно обнаруживаемой. Но, однажды, сеть этого поставщика начинает деградировать, а его клиенты пытаются увести анонсы и отключают BGP сессию с проблемным провайдером. Что происходит в дальнейшем? Клиенты ожидают, что проблема будет нивелирована, но данный оператор продолжает анонсировать клиентские сети во всех направлениях, создавая тем самым утечки маршрутов, и стягивая на свою и так проблемную сеть значительную часть клиентского трафика, делая его в итоге недоступным.

третий по посещаемости сайт в глобальной сети в настоящий момент, на полтора часа стал недоступен для абсолютно всех пользователей интернета. Причина — попытка заблокировать видеохостинг для пакистанских пользователей, рубанув с плеча и проанонсировав соседям и далее предпочтительную сеть, но с недоступным видеохостингом. Значительное количество операторов связи в течение трех минут приняли данную инструкцию как руководство к действию и YouTube потерял доступность. Это уже «угон» или hijack — злонамеренное воздействие на маршруты трафика. Хотя, скорее всего, власти Пакистана и не предсказывали подобные последствия, вероятнее всего, имела место спешка и некорректная настройка. Корень данной проблемы жив до сих пор, и лекарство работает лишь локально. Подобные глобальные проблемы могут случаться и по сей день.

Этапроблема BGP называется MOAS (multiple origin autonomous system), что примерно расшифровывается как **«разные автономные системы, имеющие перекрывающиеся анонсируемые сети»**. MOAS помогают решать архитектурные задачи в интернете (так, для примера, Amazon анонсирует собственные адресные блоки из разных автономных систем в разных регионах — и это нормально), но в то же время, механизм MOAS может быть использован и злоумышленниками — они «угоняют» заданное адресное пространство для последующего анализа перенаправленных данных различными методами. В 2016 году Qrator Labs детектировала 155000 подобных конфликтов.

Сегодня, чаще всего, типичным сценарием «угона» является захват злоумышленниками небольшого и, внешне, неиспользуемого участка адресного пула провайдера, что малозаметно по своей природе. Впоследствии это пространство используется для организации кибератак, распространения спама и проведении других противозаконных активностей. Когда эту деятельность обнаруживают те, кого «обокрали», преступники просто переключаются на адресное пространство другого оператора и все продолжается. Проблема MOAS оставалась незамеченной вплоть до 2016 года, когда многие провайдеры, поняв репутационные риски, наконец отнеслись к ней всерьез и начали предпринимать активные действия и вводить жесткие правила. Spamhaus — известная некоммерческая организация, занятая поиском и идентификацией спама и спамеров, не задавая вопросов добавит IP-адреса нарушителей (с точки зрения Spamhaus) в публично доступный список спамеров, после чего доказать собственную невиновность и непричастность будет сложно и поздно.

Некоторые провайдеры, в целях экономии ресурсов или времени, вместо корректной и самостоятельной настройки оборудования и ПО запрашивают «содействие» у вышестоящего провайдера, который в рамках «услуги» делает «легитимный угон» (потому что владелец угоняемой сущности просил это сделать) заданного адресного пространства и анонсирует фильтруемый набор IP-адресов далее своему клиенту. Даже такая, на первый взгляд, безобидная шалость может привести к следующим проблемам:

- Провайдер, предоставляющий подобную «услугу» по запросу, забывает добавить настройку No-Export Community, что приводит к потенциально неконтролируемому распространению подобных похищенных префиксов. В результате, запрещенный в одной стране сервис может оказаться недоступен по всему миру.
- Зачастую мы наблюдаем захват не одного IP-адреса (сетевой префикс /32), а куда более крупного блока /24 (256 IP-адресов в сети). Эта ошибка настолько серьезна, что теоретически она может привести к глобальной недоступности. Вся сеть, которая размещает запрещенный ресурс (чаще всего крупный хостинг-провайдер или CDN), может «слечь» на несколько часов или дней, пока ошибку не исправят.

В текущей версии протокола BGP при неправильной настройке анонсов или нарушении рекомендуемых практик конфигурации всегда есть вероятность, что некорректный анонс распространится глобально. Такие проблемы выявляются с большим трудом, если пытаться искать источник проблемы исходя только из данных об изменении трафика на уровне своей автономной системы. Использование встроенного инструмента «сообществ» (BGP- communities) при настройке BGP-маршрутизации является наиболее тонким способом добиться необходимой работоспособности и корректной маршрутизации на месте, в рамках автономной системы, за которую вы отвечаете.

Глобально решить данную проблему быстро невозможно, ведь как мы уже поняли — единого интернета просто не существует, существует множество отдельных кусочков, в каждом из которых присутствуют собственные настройки BGP-маршрутизации. А единственный путь сделать мечту реальностью в рамках всей Земли долог и мучителен, и лежит через «Инженерный совет интернета» (IETF), рассматривающий и утверждающий все изменения универсальных стандартов и протоколов.

В Qrator Labs решили пойти именно этим путем, так как если вы хотите добиться глобальных улучшений, связанных с инфраструктурой интернета, то иного выхода просто не существует. Для нас BGP-инциденты представляют если не опасность, то серьезные риски для качества предоставляемой услуги клиенту, поэтому мы пытаемся найти техническое решение проблемы.

Поскольку причиной большинства утечек, над решением проблемы которой мы сейчас работаем, оказалась неправильная настройка, стало ясно, что единственный способ решить проблему — устранить условия, при которых ошибки инженеров способны влиять на других операторов связи. Опциональные механизмы фильтрации в BGP нужно встроить в сам протокол, тем самым снизив сложность его настройки.

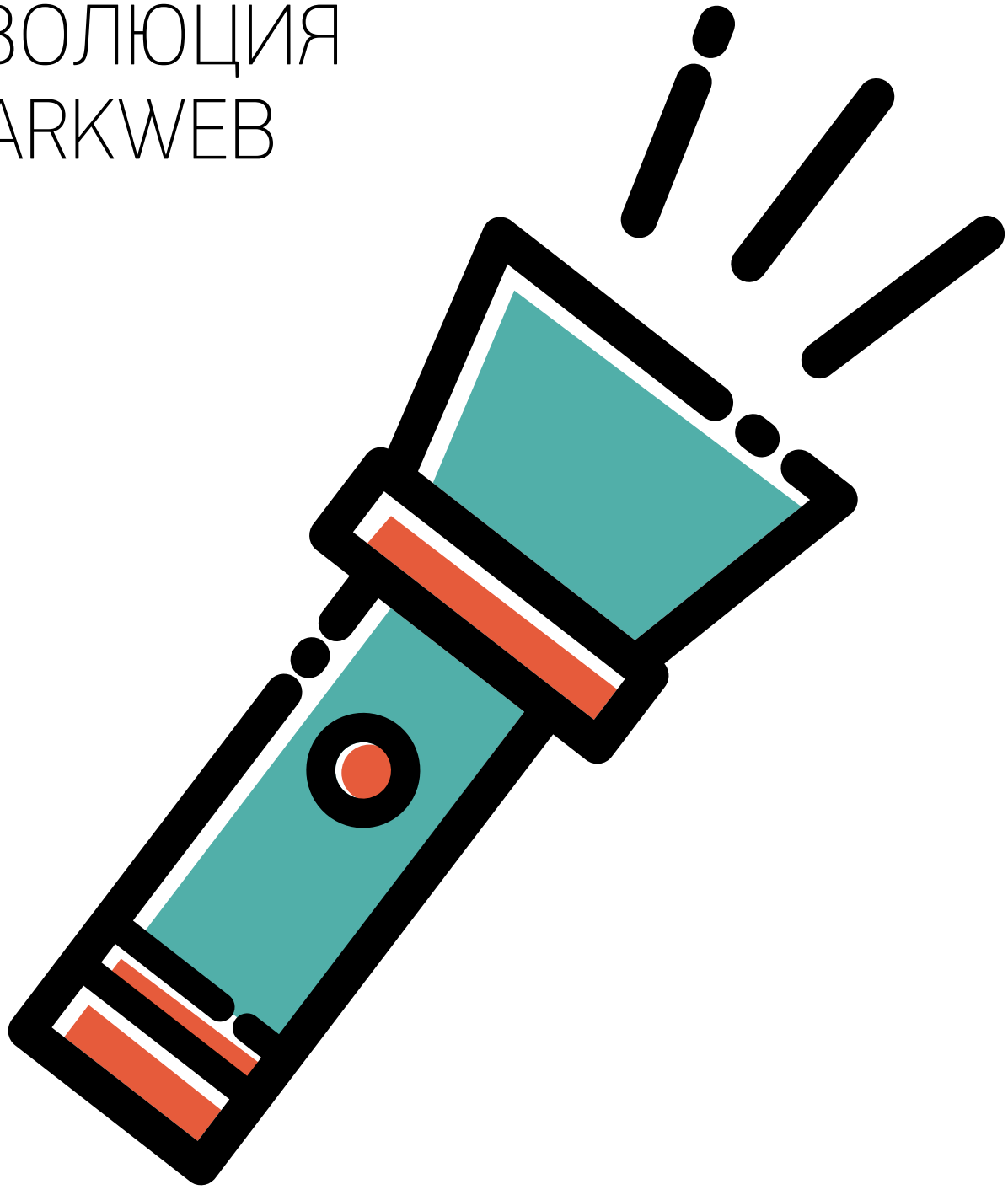
Подробнее про работу инженерного совета можно узнать из Википедии, от себя мы добавим лишь, что IETF не является юридическим лицом, и существует в виде сообщества. Это позволяет быть независимым от любых правовых вопросов и регулятивных требований какой-либо страны, что, в общем-то, правильно. То, что не

существует в физической форме, нельзя взломать, атаковать или засудить. IETF не платит зарплаты, из чего следует, что все участники организации работают в этом совете добровольно. Из этого также следует, что такая деятельность едва ли выходит на приоритет выше, чем «неприбыльная». Поэтому работа по разработке новых стандартов зачастую идет медленно, за исключением конференций IETF, являющихся эпицентрами активности.

Внедрение нашей инициативы по модификации протокола BGP, конечно, займет годы. Но, мы пытаемся сделать «новый BGP» безопасным, не только исключив саму возможность появления утечки маршрутов в результате ошибки. Наше расширение BGP, находящееся в стадии только частичного развертывания, предоставляет механизм для автоматического обнаружения утечек и предотвращения их распространения. Все это — благодаря возможности отразить напрямую в настройке протокола бизнес отношения между операторами связи. Авторами данной модификации стала интернациональная группа, состоящая из Александра Азимова и Евгения Богомазова из Qrator Labs, Ренди Буша из «Интернет Инициатив Японии», Кейра Патела из компании Arccus и Котикалапуди Шрирама из Национального Института Стандартов и Технологий США.

В конце концов, кому-то придется улучшить интернет — лучше, если это будут профессионалы, а не регуляторы.

ЭВОЛЮЦИЯ DARKWEB



.TXT

БЕНЖАМИН БРАУН
Akamai

2016 ГОД БЫЛ ГОДОМ АКТИВНОЙ ДЕЯТЕЛЬНОСТИ ДЛЯ ТЕМНОГО ИНТЕРНЕТА. ПОЯВИЛИСЬ НОВЫЕ КРИПТОВАЛЮТЫ ПОМИМО БИТКОЙНА, СУЩЕСТВЕННО РАСШИРИЛОСЬ ПРЕДЛОЖЕНИЕ НА РЫНКАХ ТЕМНОЙ СЕТИ. НЕСКОЛЬКО ВЕДУЩИХ ХАКЕРСКИХ ФОРУМОВ И ПОДПОЛЬНЫХ РЫНКОВ ИСЧЕЗЛИ, И ИХ МЕСТО СТРЕМЯТСЯ ЗАНЯТЬ НОВЫЕ. БЫЛИ АНОНСИРОВАНЫ НОВЫЕ ИНТЕРЕСНЫЕ, БАЗИРУЮЩИЕСЯ В ДАРКНЕТ, УСЛУГИ КОНФИДЕНЦИАЛЬНОСТИ В ВИДЕ ПРЕДЛОЖЕНИЙ ISP И VPN.

Вдобавок к этому, в 2016 году активность темного интернета и его пользователей определялась действенной политикой и правоприменительными мероприятиями. Эти меры, принимаемые при поддержке Штатов, продолжают оставаться главной темой обсуждения на форумах пользователей и рынков темного интернета. Они заставляют пользователей делиться анализом блокировок, потенциальных последствий новой политики, советами и руководствами в области операционной безопасности (OPSEC), рассказами о взаимодействии с правоохранительными органами и предположениями о том, как наилучшим образом обезопасить сервисы темного интернета и его пользователей от дальнейших усилий правоохранительных органов США.

ГЛУБОКАЯ СЕТЬ VS. ТЕМНАЯ СЕТЬ VS. ДАРКНЕТ

Глубокая Сеть, Темная Сеть, Даркнет — несмотря на то, что в медиа эти термины часто используются как взаимозаменяемые, они представляют различные, хотя и связанные, сегменты интернета. Глубокая сеть обозначает страницы и сервисы на серверах, которые доступны посредством стандартных интернет-браузеров и способов связи, но не индексируются основными поисковыми системами. Темная сеть — сравнительно небольшая часть Глубокой Сети, имеет отношение к веб-сервисам и страницам, которые намеренно скрыты. Эти страницы и сервисы недоступны через стандартные браузеры, они базируются на использовании оверлейной сети, которая требует особых прав доступа, прокси-конфигураций или специализированного ПО. Даркнет объединяет структуры, в которых доступ заблокирован на уровне сети, например, Tor или I2P. Под эту категорию часто попадают также частные VPN и mesh-сети.

РАЗЛИЧНЫЕ ДАРКНЕТЫ

Tor — далеко не единственная даркнет-структура. Несмотря на то, что Tor наиболее популярен, существует несколько «сетей анонимности», популярность которых растет. Примерно столько же по времени, как и Tor, существует Invisible Internet Project (I2P). Как и Tor, I2P — это сеть, которая располагается поверх интернета и предоставляет определенную маскировку личности пользователя, не предоставляя при этом полной анонимности. В настоящий момент открытый I2P-протокол поддерживает веб-серфинг, общение в сети, ведение блогов и обмен файлами.

Выпущенный в 2000 году Freenet — это, возможно, третий по популярности Даркнет после Tor и I2P. Freenet — P2P-платформа, которая предполагает защиту и слежки и цензуры,— имеет ограничения из-за сравнительно небольшого числа узлов, что делает разоблачение выделенных пользователей потенциально более легким, особенно в случае, если действующее лицо имеет стремление и ресурсы, чтобы запустить значительное число собственных узлов, что, предположительно, произошло с «Black Ice Project». В настоящее время разработчики и пользователи Freenet работают над тем, чтобы сделать ее более устойчивой.

ПЕРЕСТАНОВКИ В ПРОЕКТЕ TOR

В декабре 2015 года новым руководителем проекта был назначен бывший исполнительный директор и президент Electronic Frontier Foundation (EFF) Шари Стил. В мае 2016 из проекта ушел Якоб Апплебаум, после чего был утвержден новый совет директоров. Штаб-квартира группы была перенесена из Кембриджа в Сиэтл. Вследствие этих

перестановок один их старейших и крупнейших участников проекта, Лаки Грин, также покинул Tor.

В статье «Конфиденциальность в пост-Сноуденской Америке» агентства Pew Research Center, вышедшей в июне 2016 г., авторы утверждают, что, по результатам их исследования, «около 86% пользователей интернета предпринимали шаги для того, чтобы скрыть или удалить следы своего онлайн-присутствия, но многие из них говорят о том, что они хотели бы большего или они не знают, какие средства можно для этого использовать». В дальнейшем в статье говорится, что «около 74% утверждают, что для них «крайне важно» контролировать, кто получает о них информацию, и 65% — что для них «крайне важно», какую информацию о них получают». С преобладанием подобных настроений можно ожидать, что популярность сервисов, ориентированных на конфиденциальность, таких, как Tor, будет только расти.

ИЗМЕНЕНИЯ НА РЫНКЕ TOR

13 апреля 2016 года исчезла Nucleus — одна из самых крупных торговых площадок Темного Интернета. Многие подозревают, что это было мошеннический выход. Мошеннический выход имеет место, когда владельцы торговой площадки ждут, пока на нее будет переведено большое количество биткойнов, а затем закрывают сайт, чтобы заблокировать исходящие транзакции и исчезают вместе с биткойнами. С этого момента список веб-маркетов был перетрясен.

ТОП-5 торговых площадок по размеру и количеству транзакций:

- AlphaBay
- Dream Market
- Hansa Market
- Valhalla (бывш. Silkkitie)
- Outlaw Market

ЭКОНОМИЧЕСКИЕ ТРЕНДЫ НА TOR-РЫНКАХ

2015 и особенно 2016 годы ознаменовались глобальным сдвигом предложения на рынке Темной Сети: фокус сместился с запрещенных наркотических средств на финансовое мошенничество. Предложение включает в себя вредоносные программы, взломанные базы учетных данных, персональные данные, медицинские записи, финансовые счета, руководства по взлому, номера кредитных карт. На пяти ведущих торговых площадках можно купить логины от взломанных аккаунтов, и цена на них постоянно снижается. Аккаунты Yahoo, Dropbox, Walmart, Gamestop, Uber, Amazon, Ebay, Netflix и многих других продаются в среднем по доллару за аккаунт.

«УДАРЬ КРОТА» ХАКЕРСКИХ ФОРУМОВ

В январе 2016 года с новым главным админом на сцену вернулся хакерский форум Даркнета «Hell». «Hell» привлек к себе внимание после утечки данных об уязвимости сайта Adult Friend Finder (Поиск взрослых друзей), и закрытия сайта в июле 2015 года. В декабре 2016 года был восстановлен печально известный форум Darkode. Новая версия Darkode была запущена в открытом интернете после провалившейся попытки восстановления в сети Tor. Эти форумы, наряду с недавно взломанным форумом Nulled, традиционно являлись рассадниками для неопытных хакеров, где они обменивались пособиями, инструментами, разработками, украденными данными, и где можно было взять в аренду сервисы для взлома и DDoS-атак. После восстановления пользователи форумов значительно перемешались. Интересно посмотреть, где пользователи форумов продолжат обустраивать свои норы. Традиционно хакерские форумы были мишенью для гигантской игры «Ударь крота», как со стороны правоохранительных органов, так и со стороны конкурирующих форумов.

НОВЫЕ ISP И VPN ТЕМНОЙ СЕТИ

В июле 2016 года на конференции Хакеры Планеты Земля (HOPE) Гарет Левелин анонсировал запуск Brass Horn Communications, нового провайдера, который использует систему OnionDSL чтобы «Tor-рифицировать» весь клиентский трафик роутера, пропустить его через контролируемый провайдером канал и провести несколько Tor-манипуляций, прежде чем приступить к интернет-навигации. Система предположительно не дает провайдерам регистрировать относящийся к идентификации трафик клиента. Пока система существует в бета-версии, однако, если рынок на нее отреагирует, система может оказаться

интересной для сервисов, которые основываются на блэклистинге и геоблокинге.

В том же русле действует новый VPN-сервис TGVPN (бывш. I2VPN). Сервис призван усилить технологии Tor (или, как опция, I2P) и BTC с целью увеличения анонимности и приватности. BTC-адрес и подпись используются для аутентификации, в то время как пользовательский трафик пропускается через 3 уровня шифрования (OpenVPN, WrapVPN, TLS).

КРИПТОВАЛЮТЫ

Биткойн. 2016 год был успешным для биткойна (BTC), который, обогнав бразильский реал, стал лучшей по динамике валютой года. BTC увеличился в стоимости более чем вдвое и за год вырос на 126%. Факторами роста стали относительная волатильность и девальвация ряда бумажных валют и деятельность на китайском рынке. Во второй половине 2016 года юань составлял 98% от общего объема торговли BTC. В промежутке с 2011 по 2017 год стабильность BTC неизменно нарастает. Для Темного Интернета это означает, что BTC с большой степенью вероятности останется основной валютой для киберпреступников, защитников неприкосновенности личных данных и всех, кого интересует концепция альтернативных и криптовалют.

Monero. В августе 2016 года торговые площадки темной сети AlphaBay и Oasis анонсировали начало поддержки Monero как платежного средства. В течение нескольких месяцев после этого рост стоимости Monero составил 669%. Капитализация рынка Monero в 2016 году выросла с 5 млн USD до 185 млн USD. Также Monero была интегрирована в экономику масштабной ролевой онлайн-игры CryptoKingdom.

В отличие от биткойна, Monero не использует открытые книги учета операций и, как утверждается, поддерживает полностью анонимные транзакции. Учитывая этот факт, можно ожидать, что платежную структуру Monero начнут использовать для всего, начиная от украденных данных до схем DDoS-атак и вымогательства данных.

Zcash. Еще одна ориентированная на конфиденциальность криптовалюта, дебютировавшая в 2016 году. В октябре она оценивалась в шокирующие 2 млн USD, но в последующие месяцы последовало падение. К концу ноября стоимость опустилась ниже 100 USD. В отличие от BTC и Monero, Zcash не вызвала большого интереса у инвесторов.

ИСПОЛЬЗОВАНИЕ ТЕМНОЙ СЕТИ ДЛЯ АТАК

В течение 2016 года сеть Tor по-прежнему использовалась для сокрытия вредоносных механизмов, использующих трафик, таких, как SQLmap, Tor's Hammer, UFONet, HIVE, и обновленные версии LOIC (Low-Orbit Ion Cannon). Важно отметить, что вредоносный трафик, проходящий через Tor, нельзя назвать значительным по объему. Из-за ограниченности пропускной способности, DDos-атаки через Tor вызывают меньше беспокойства, нежели такие типы атак, как SQL Injection (SQLi) или Remote Code Execution (RCE). Для защиты от подобных типов атак гораздо эффективнее использовать грамотно настроенный Web Application Firewall (WAF), который позволяет отфильтровывать легитимный трафик, блокируя при этом вредоносный трафик.

СУДЕБНЫЕ И ПРАВООХРАНИТЕЛЬНЫЕ ДЕЙСТВИЯ

Джордж Котрелл являлся советником Найджела Фаража, видного члена Партии Независимости Великобритании. Джордж был арестован ФБР по обвинению в 21 преступлениях, касающихся отмывания денег в Темной Сети, фрода, шантажа и вымогательства. Серия арестов продавцов на рынках Темной Сети продолжилась с захватом брюссельской группировки итальянской мафии, которая специализировалась на торговле MDMA. IcyEagle был пойман на продаже фрод-сервисов, включая похищенные банковские счета и пакеты персональных данных.

В ответ на теракты в Мюнхене, где исполнитель приобрел оружие на рынке Темной Сети, глава немецкой федеральной полиции (BKA) Хольгер Мюнх объявил о фокусировании внимания правоохранительных органов на деятельности темного интернета. Кульминацией этой деятельности стала совместная операция Федеральной таможенной службы и Центрального отделения кибербезопасности Германии 11 августа, в ходе которой было обыскано 6 частных владений в Баварии. В результате было арестовано 4 подозреваемых, изъято 11 кг амфетамина, 150 гр. кокаина, 250 гр. героина, 175 гр. MDMA, 1425 таблеток экстази, 645 гр. марихуаны. Обнаружена комнатная плантация марихуаны с 72 растениями и биткойн-кошелек, с содержимым, эквивалентном 400 тыс. USD.

Австрия выразила обеспокоенность, аналогичную Германии, и выпустила поправку к национальному Закону об использовании оружия. Поправка дает правоохранительным органам право носить оружие в частном порядке, не будучи на службе. Также поправка существенно увеличивает размер наказания за несанкционированное использование или передачу огнестрельного оружия. Министр внутренних дел Австрии считает данные меры эффективными для борьбы с незаконной торговлей оружием в Темной Сети.

Прибыльная организация фальшивомонетчиков была захвачена в ходе крупной операции, возглавленной Европолом. Криминальная группа, состоявшая из 8 человек и известная как NapoliGroup, участвовала в инвестировании мошеннических схем, распространив фальшивых купюр на более чем 7,6 млн евро. В своей деятельности NapoliGroup использовала как Темную Сеть, так и биткойны.

Дополнительно к вышеприведённым мерам, на выявление подозреваемых по всему миру направлены действия ФБР США. Согласно доступным материалам судебных слушаний, по меньшей мере 8 тыс. компьютеров в 120 странах были использованы в рамках одного ордера. Это была часть операции PlayPen, в ходе которой ФБР взяла под контроль сайт темного интернета, распространяющий детскую порнографию, использовав при этом различные техники эксплуатации сети и браузера, чтобы раскрыть конечных пользователей.

ПРОГНОЗЫ НА 2017 И ПОСЛЕДУЮЩИЕ ГОДЫ

Глобальный сдвиг ожидается в 2017–2018 гг. с переходом рынков Темной Сети на ориентированные на конфиденциальность платформы «все в одном». Сообщается, что разработчики криптовалюты ShadowCash строят свою собственную платформу, которую они назвали UMBRA. UMBRA предоставляет функцию сквозного шифрования чата, управление кошельками криптовалют, безопасные платежи и механизмы перевода остатков по счету, а также торговую площадку P2P. Разработчики также работают над интеграцией Tor и I2P в целях повышения защиты приватности пользователей.

Аналогичная платформа, которая разрабатывается в настоящее время — это Komodo platform. Платформа нацелена на защиту анонимности пользователя посредством технологии доказательства с нулевым разглашением (zero knowledge proof) уже упомянутой криптовалюты Zcash, а также блокчейна, который использует отложенный механизм доказательства выполнения работы (dPoW). Платформа также включает в себя мультикошелек под названием Iguana для хранения средств в различных криптовалютах.

Подобные платформы нацелены на усложнение наиболее часто встречающихся способов нарушения цифровой конфиденциальности, которые в настоящее время переживают биржи торговых площадок Темной Сети. Эти платформы не решают проблем, связанных с транспортировкой и доставкой материальных товаров, однако они предоставляют позитивные стимулы для подпольных торговых площадок будущего. Эти стимулы привлекают вендоров и потребителей, которые ищут простоты использования и большего чувства безопасности.

НЕВИДИМАЯ СЕТЬ

Видимая часть Сети

4%

сетевого контента (около 8 млрд страниц) индексируется поисковыми сервисами

Глубокий веб

- Научные исследования и базы данных
- Медицинские базы
- Финансовая информация
- Юридические документы
- Репозитории компаний

7,9

зеттабайт

96%

всего контента интернета

Дарквеб

- TOR
- Диссиденты
- Торговля запрещенными субстанциями и товарами

ЭКОСИСТЕМА
ЦИФРОВОЙ ЭКОНОМИКИ РОССИИ

СЕГМЕНТЫ РЫНКА, ГДЕ ДОБАВЛЕННАЯ СТОИМОСТЬ СОЗДАЕТСЯ С ПОМОЩЬЮ ЦИФРОВЫХ (ИНФОРМАЦИОННЫХ) ТЕХНОЛОГИЙ

УРОВНИ ЦИФРОВОЙ ЭКОНОМИКИ

- Технологические компании
- Поставщики для технологических компаний
- Снижение издержек / повышение эффективности за счет цифровых технологий для компаний других секторов экономики
- Снижение издержек / повышение качества жизни для граждан

ХАБЫ ЭКОСИСТЕМ

- Финансы и торговля
- Маркетинг и реклама
- Инфраструктура и связь
- Государство и общество
- Образование и Кадры
- Медиа и развлечения
- Стартапы
- Кибербезопасность

СРЕЗЫ ДЛЯ ХАБОВ

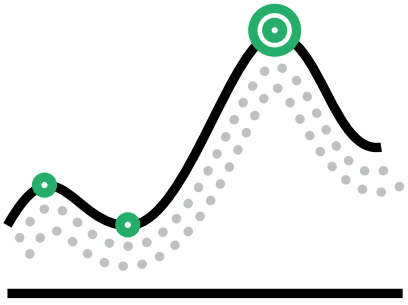
- Разработка и дизайн
- Аналитика и данные
- AI и BigData
- Бизнес-модели
- Hardware
- Интернет вещей
- Mobile
- Регулирование
- Платформы

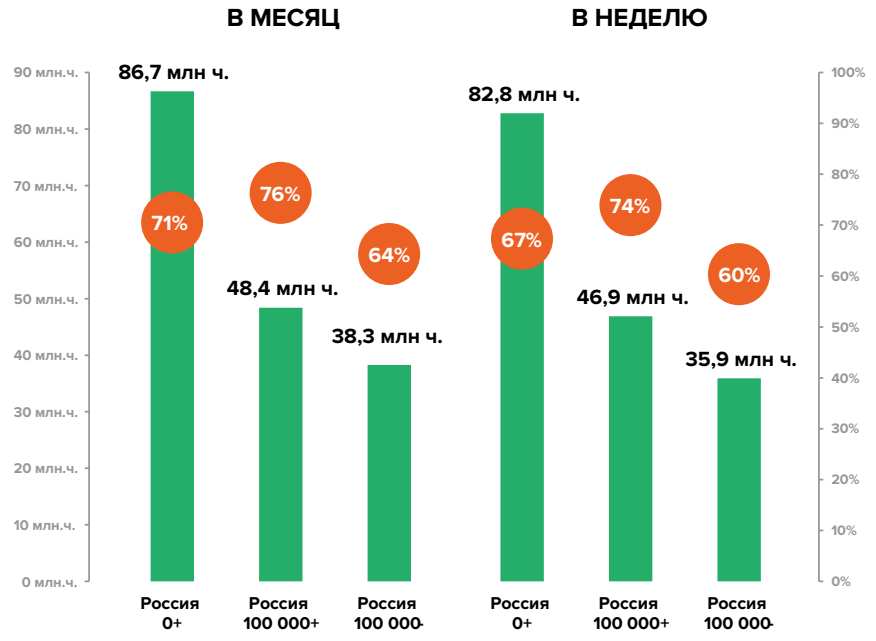
АУДИТОРИЯ

Количество Интернет-пользователей

Сентябрь 2016 г. — Февраль 2017 г., в млн чел. и в % от населения 12+ лет

Пользуются интернетом хотя бы один раз...





РЫНКИ

Топ-10 холдингов

Февраль 2017, Россия 0+, 12-64 лет

в среднем за день		в среднем за неделю		за месяц	
Mail.Ru Group	32 354 т.ч.	Mail.Ru Group	47 214 т.ч.	Mail.Ru Group	53 918 т.ч.
Яндекс	28 049 т.ч.	Яндекс	44 278 т.ч.	Яндекс	52 417 т.ч.
Google Sites	21 096 т.ч.	Google Sites	39 937 т.ч.	Google Sites	50 736 т.ч.
Facebook	6 093 т.ч.	Facebook	16 290 т.ч.	Rambler&Co	28 305 т.ч.
Rambler&Co	5 769 т.ч.	Rambler&Co	16 090 т.ч.	Facebook	27 753 т.ч.
Alibaba Group	4 348 т.ч.	Wikimedia foundation	13 614 т.ч.	Wikimedia foundation	26 398 т.ч.
Avito	3 677 т.ч.	Alibaba Group	12 995 т.ч.	Alibaba Group	23 248 т.ч.
Wikimedia foundation	3 543 т.ч.	Avito	11 710 т.ч.	Avito	22 034 т.ч.
Gismeteo	2 259 т.ч.	Газпром медиа	8 416 т.ч.	Газпром медиа	18 090 т.ч.
Газпром медиа	2 201 т.ч.	ИД Hearst Shkulev Media	7 509 т.ч.	ИД Hearst Shkulev Media	15 997 т.ч.

ВЛИЯНИЕ РУНЕТА НА ЭКОНОМИКУ

2,4%
ОТ ВВП (ИНТЕРНЕТ-РЫНКИ)

3,8%%
ОТ ВВП (Мобильная экономика)

КАДРЫ
2,5
млн работников

ИНФРАСТРУКТУРА И ПО
2000
млрд рублей

МАРКЕТИНГ И РЕКЛАМА
171
млрд рублей

ЦИФРОВОЙ КОНТЕНТ
63
млрд рублей

ЭЛЕКТРОННАЯ КОММЕРЦИЯ
1238
млрд рублей

СОВЕТЫ ПО ЦИФРОВОЙ ЭКОНОМИКЕ

1. Рабочая группа Экономического совета при Президенте Российской Федерации по направлению «Цифровая экономика».
2. Совет по законодательному обеспечению развития цифровой экономики при Председателе Государственной Думы РФ.
3. Рабочие группы по проработке Поручения Президента по итогам послания Федеральному Собранию при Минэкономразвития РФ и Минкомсвязи РФ.
4. Рабочая группа «Связь и ИТ» Экспертного совета при Правительстве РФ.

5 Компании и НКО: РАЭК, Центр стратегических разработок, Агентство стратегических инициатив, фрии, Ростех, Ростелеком, Сбербанк, Яндекс

ВЫЗОВЫ ЦИФРОВОЙ ЭКОНОМИКИ

- Безопасность данных, инфраструктуры, граждан
- Конфиденциальность
- Загрязнение информационного пространства
- Прозрачность принятия решений алгоритмами
- Необходимость пересмотра законодательства и международных отношений

РЕГУЛИРОВАНИЕ

1 Трансграничный характер цифровой экономики

2 Особое внимание к вопросам кибербезопасности

3 Стимулирование и поддержка направлений:

- **Импортозамещение**
- **Обеспечение равных условий ведения деятельности интернет-компаниями в РФ**
- **Реформа налогообложения отрасли цифровых технологий**
- **Экспорт информационных технологий**
- **Развитие инфраструктуры доступа и хранения данных**
- **Стимулирование безналичных платежей и всех видов массовых цифровых коммуникаций и сервисов**

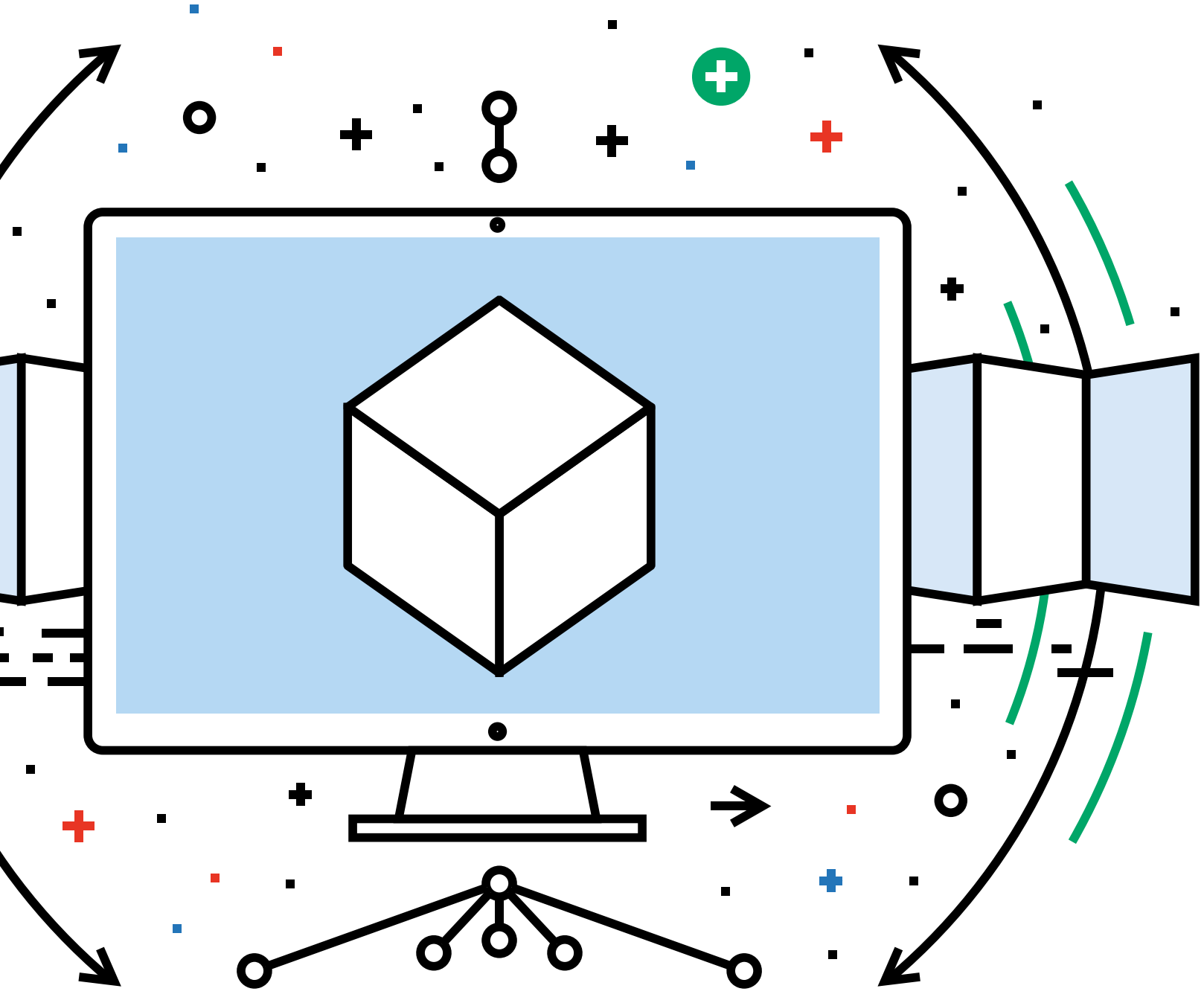
4 Законотворчество на упреждение

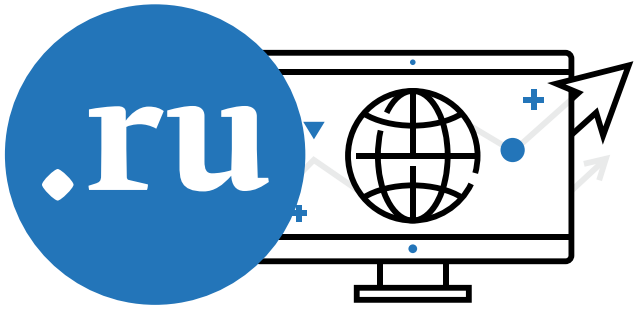
- **Большие данные и искусств. интеллект**
- **Робототехника**
- **Автономные платформы и Интернет вещей**
- **Блокчейн**

5 ОРВ должна учитывать долгосрочные планы и прогнозы развития — на 10-20 лет

Домены России

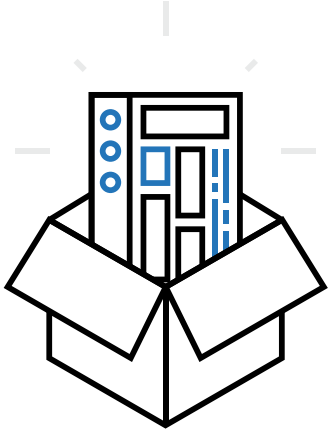
ПО ДАННЫМ STATDOM.RU / СВОДНЫЕ ДАННЫЕ НА АПРЕЛЬ 2017





Общее число доменов

5 528 092



Делегировано доменов 5 259 608

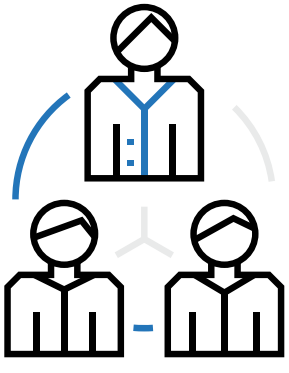
Общее число администраторов **2 004 898**

Число веб-узлов

4 161 617

Число зон с MX-записями, для которых есть IP-адрес

2 869 647

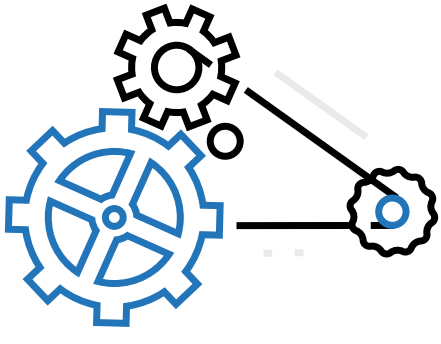


Число администраторов физических лиц

1 617 479

Узлы TLS (HTTPS), с корректным сертификатом

300 167

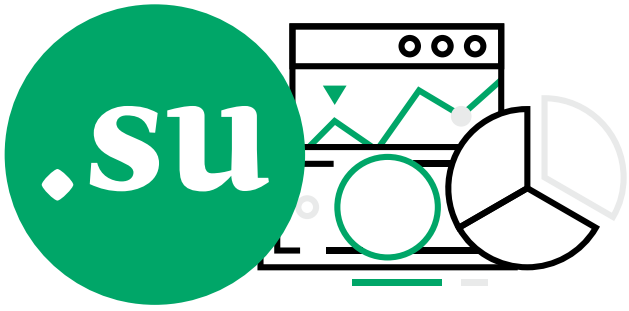


Веб-узлы с Google AdSense

283 633

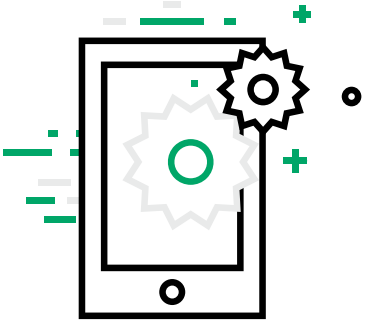
Веб-узлы с «Яндекс.Директ»

14 143



Общее число доменов

119 185



Делегировано доменов 105 580

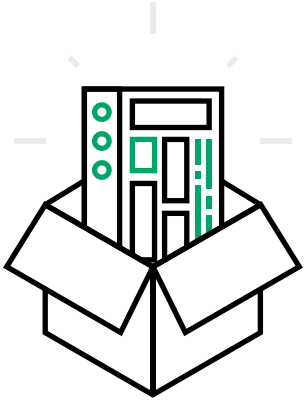
Общее число администраторов 74 875

Число веб-узлов

77 794

Число зон с MX-записями, для которых есть IP-адрес

61 731

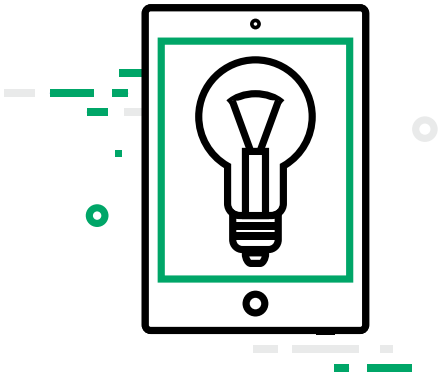


Число администраторов физических лиц

58 703

Узлы TLS (HTTPS), с корректным сертификатом

5 564

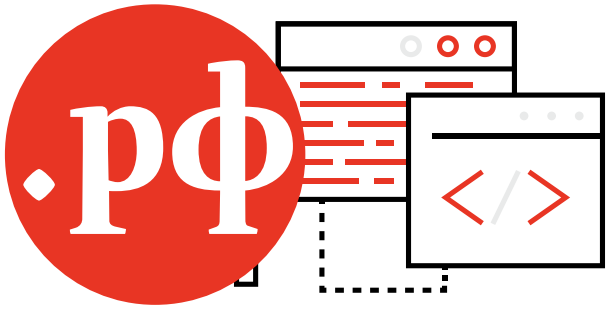


Веб-узлы с Google AdSense

2 980

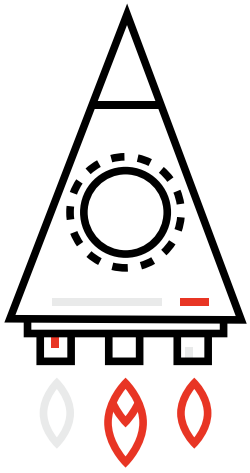
Веб-узлы с «Яндекс.Директ»

245



Общее число доменов

902 820



Делегировано доменов 793 386

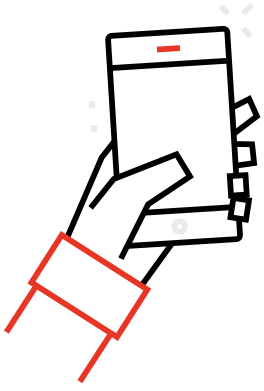
Общее число администраторов **378 088**

Число веб-узлов

563 722

Число зон с MX-записями, для которых есть IP-адрес

346 161

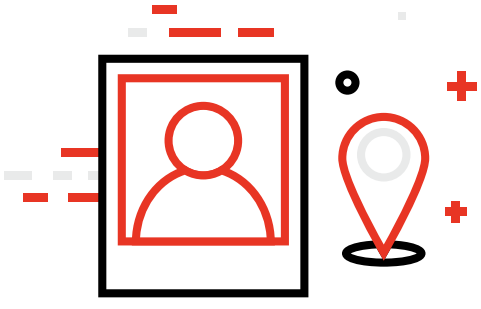


Число администраторов физических лиц

301 918

Узлы TLS (HTTPS), с корректным сертификатом

16 713



Веб-узлы с Google AdSense

13 738

Веб-узлы с «Яндекс.Директ»

637

СОСТОЯНИЕ КИБЕРБЕЗОПАНОСТИ

IV КВАРТАЛ 2016

КРУПНЕЙШАЯ DDOS-АТАКА

517 ГБИТ/С

ИНТЕРНЕТ ВЕЩЕЙ — «ТОПЛИВО» ДЛЯ АТАК

ПОСТОЯННЫЕ АТАКИ СТАНОВЯТСЯ ОБЫДЕННОСТЬЮ

30 АТАК

ПРОТИВ ОДНОЙ КОМПАНИИ В СРЕДНЕМ

140%

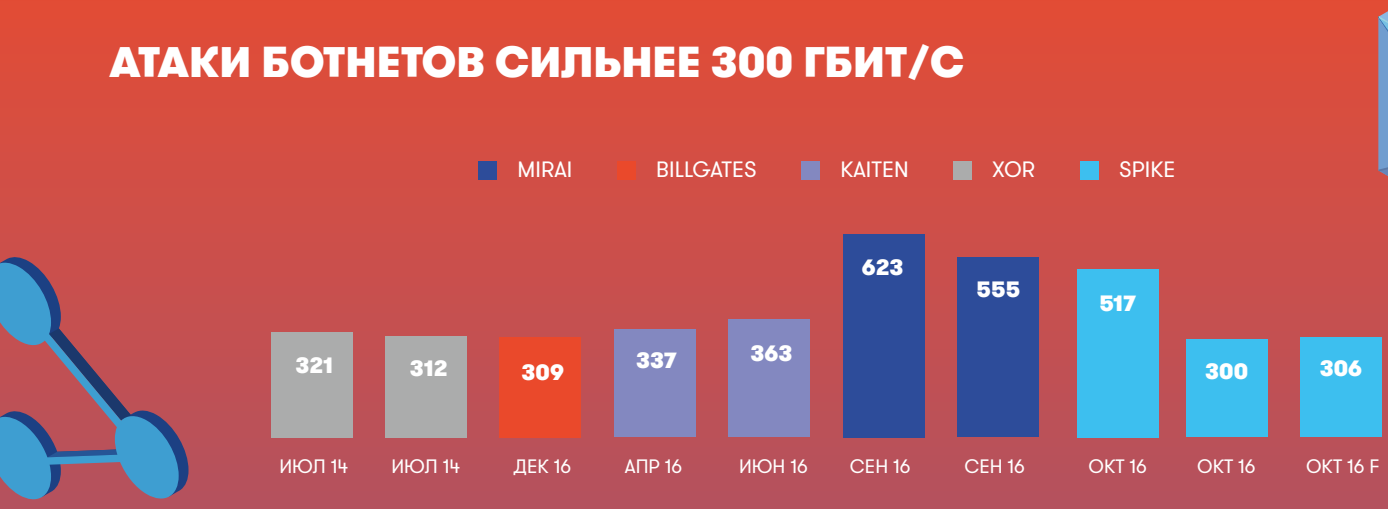
РОСТ ПО СРАВНЕНИЮ С 2015

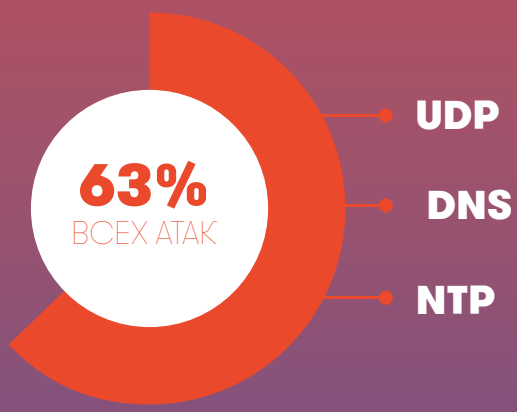
12 МЕГА-АТАК

СИЛЬНЕЕ

100 ГБИТ/С

АТАКИ БОТНЕТОВ СИЛЬНЕЕ 300 ГБИТ/С





ТРИ АТАКИ СИЛЬНЕЕ

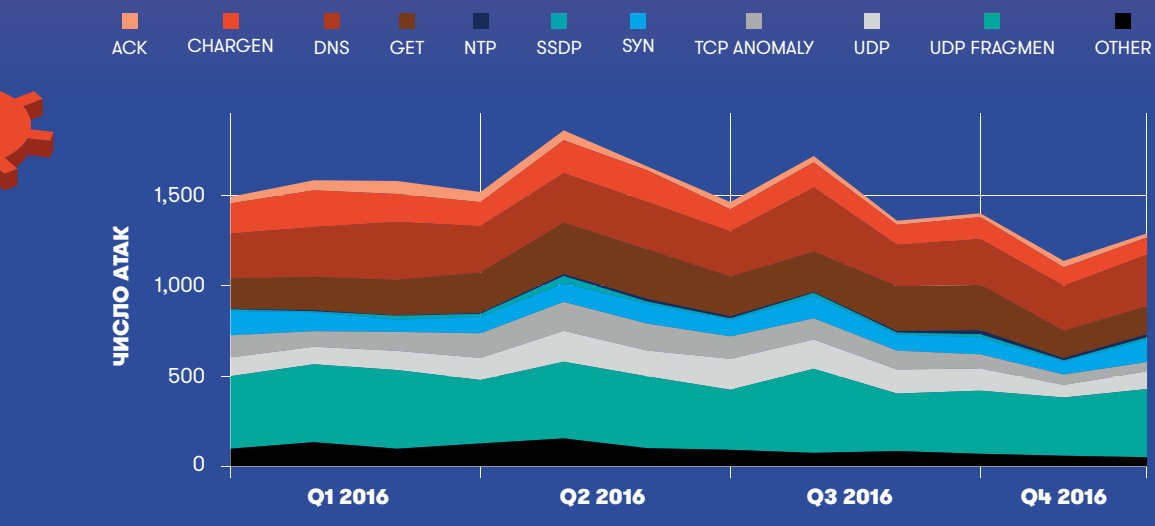
300 ГБИТ/С
ЗА 4 КВАРТАЛ

ИСТОЧНИКИ АТАК

США **24%**

- ВЕЛИКОБРИТАНИЯ **9.7%**
- ГЕРМАНИЯ **6.6%**
- КИТАЙ **6.2%**
- РОССИЯ **4.4%**
- ИТАЛИЯ **3.1%**
- ИСПАНИЯ **3.0%**
- БРАЗИЛИЯ **3.0%**
- ФРАНЦИЯ **2.8%**
- НИДЕРЛАНДЫ **2.8%**

ВЕКТОРЫ DDOS АТАК



5 000 000 000 ЗАПРОСОВ В СУТКИ

О ТОМ, КАК РАБОТАЕТ РОССИЙСКАЯ DNS-ИНФРАСТРУКТУРА, РАССКАЗАЛА ГЕНЕРАЛЬНЫЙ ДИРЕКТОР MSK-IX **ЕЛЕНА ВОРОНИНА**

ЕЛЕНА ПАВЛОВНА, НА ТЕРРИТОРИИ РОССИИ ФУНКЦИОНИРУЮТ УЖЕ НЕСКОЛЬКО КОРНЕВЫХ DNS-СЕРВЕРОВ. А НУЖНЫ ЛИ ОНИ НА ТЕРРИТОРИИ СТРАНЫ НА САМОМ ДЕЛЕ ИЛИ ЖЕ ЭТО БОЛЬШЕ ВОПРОС ПРЕСТИЖА? НУЖНО ЛИ ИХ СТРОИТЬ И ОТКРЫВАТЬ? СКОЛЬКО ЭТО СТОИТ?

Основные критерии работы системы DNS — это скорость отклика, доступность сервиса и достоверность информации. Всякий раз, когда пользователь сети набирает имя веб-сайта или отправляет электронную почту, сетевое приложение, которое он использует, обращается к DNS. Чем ближе к потребителю расположен искомый сервер DNS (с сетевой точки зрения), чем у него выше производительность, тем меньше времени потребуется на обмен DNS-информацией между сетевыми устройствами, и тем быстрее запрос пользователя будет перенаправлен на искомый ресурс.

Второй, очень важный аспект получения быстрого отклика — это доступность сервиса. Она определяется многими факторами: доступностью сети, производительностью серверов, их загрузкой и пр. Для повышения доступности сервиса строят распределенные DNS-сети с множеством дублирующих серверов. Построение распределенных сетей является также элементом повышения безопасности сервиса.

Размещение зеркал корневых серверов в непосредственной близости к потребителю призвано решить первые две задачи — скорость отклика и доступность сервиса. Этим фактором объясняется широкое международное сотрудничество между операторами корневых серверов и точками обмена трафиком (IXP), так как такой подход дает возможность широкому кругу провайдеров получить доступ к информации DNS наиболее коротким и быстрым путем. Таким образом, размещение зеркал корневых серверов определяется технологической целесообразностью.

Технология построения распределенных DNS-сетей появилась в начале 2000-х и в то время являлась технической новацией. Сегодня в мире размещено более 700 узлов зеркал корневых серверов, и создание новых узлов — это будни эксплуатации телекоммуникационной инфраструктуры. Условия размещения серверов определяются операторами корневых серверов. Финансовая политика у всех операторов разная.

КАК РАБОТАЕТ РОССИЙСКАЯ DNS-ИНФРАСТРУКТУРА? ГДЕ ЗАКАНЧИВАЕТСЯ РОССИЙСКАЯ ЗОНА ОТВЕТСТВЕННОСТИ?

Суть интернета — глобальная сеть. Если требуется определить какую-либо локальную часть этой сети, необходимо сформулировать уникальный признак.

Понятие «российская DNS-инфраструктура» столь же неопределённое с технической точки зрения, как и понятие «российский сегмент сети Интернет». Для формирования этого понятия требуется сформулировать ответы на множество специфичных вопросов. Например, на такой: относится ли DNS домена, администрируемого зарубежным юридическим лицом (например, в домене .TV), но зарегистрированного российским юридическим лицом, к российской DNS-инфраструктуре?

Поэтому давайте сузим вопрос до инфраструктуры доменов .RU и .РФ. Мы, как оператор сети DNS для доменов .RU и .РФ, делаем все возможное для того, чтобы DNS cloud (распределенная сеть DNS-серверов) работал надежно, эффективно, с минимальными задержками. Кстати, в контракте с Техническим центром Интернет на предоставление услуг DNS сформулировано следующее: «Требование по уровню услуг: доступность сервиса DNS 0 минут простоя = 100% доступность». Это означает, что сбоев в работе нашего сервиса DNS не должно быть в принципе.

Зона нашей ответственности — это DNS cloud, состоящий из серверов, телекоммуникационного оборудования, каналов связи, систем управления, мониторинга, безопасности и прочих средств, необходимых для стабильной работы системы.

DNS-СЕТЬ MSK-IX НАСЧИТЫВАЕТ 18 УЗЛОВ В ЕВРОПЕ, АЗИИ, СЕВЕРНОЙ И ЮЖНОЙ АМЕРИКЕ, В ТОМ ЧИСЛЕ 9 В РОССИИ — А ВСЕ ЛИ ЭТИ УЗЛЫ ПОЛНОСТЬЮ ЗАГРУЖЕНЫ? ЗАЧЕМ ИХ СТОЛЬКО?

Технологии и мотивы построения распределенной DNS-сети для корневых доменов и доменов верхнего уровня сходны.

Сеть строится, исходя из требований по скорости отклика, доступности сервиса и достоверности данных. Узлы, входящие в состав сети, имеют разную конфигурацию, коннективность, решения по безопасности и прочие параметры. В состав всех узлов входит техническое решение, позволяющее собирать и обрабатывать статистические данные работы узла, в том числе статистику обращений. Построена сеть внешних пробников самоконтроля, позволяющая оценить скорость ответа и доступность сервиса из внешних сетей. Эти данные позволяют нам принимать решения о целесообразности размещения узла

в той или иной локации, необходимой производительности и коннективности конкретного узла.

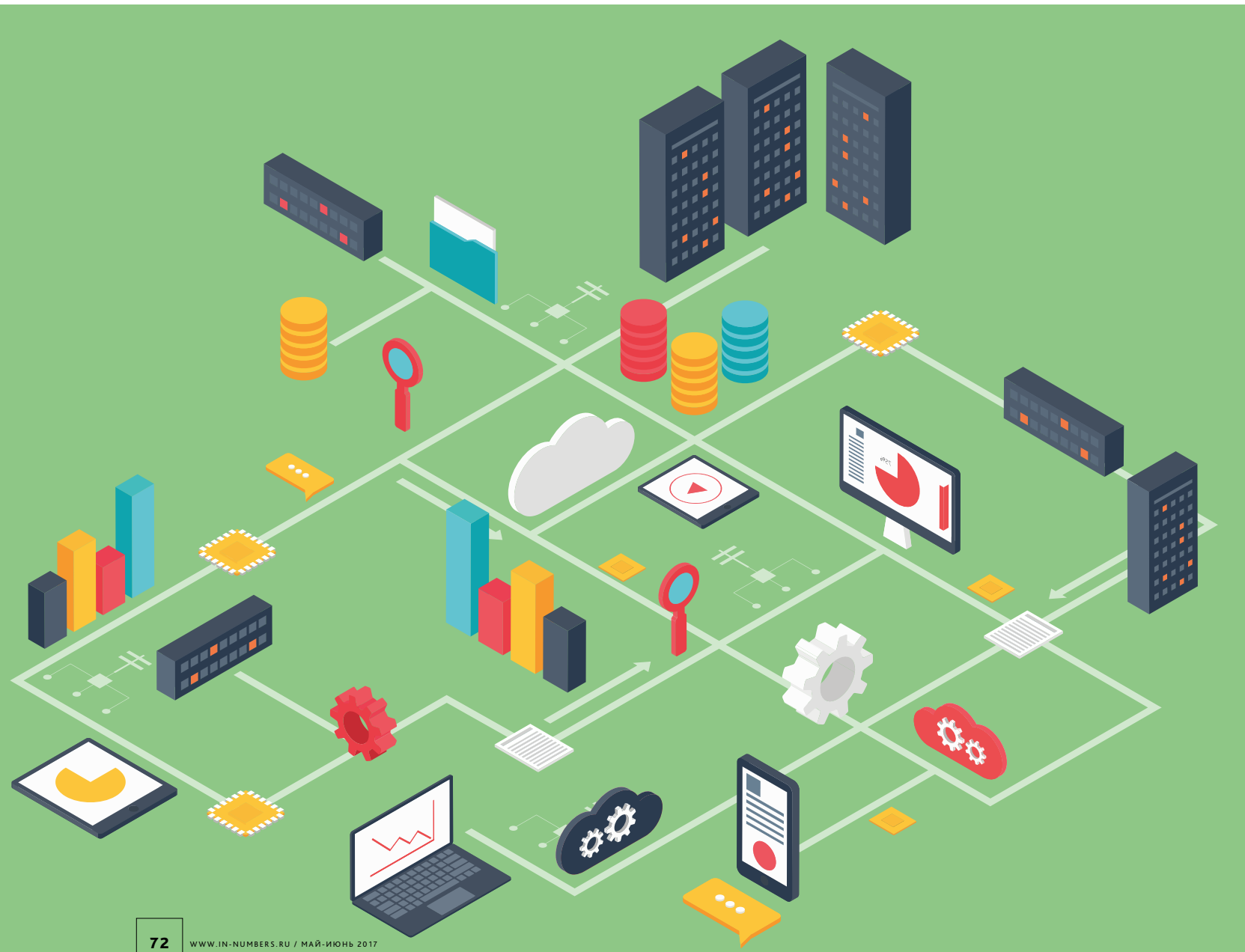
В среднем наш DNS cloud обрабатывает около 5 000 000 000 запросов в сутки. Состав узла определяется, в том числе, и нагрузочными характеристиками. Например, в Москве сервис испытывает наибольшую нагрузку. Поэтому в Москве организована сеть из нескольких узлов, размещенных на географически разнесенных площадках.

Технологии DNS cloud позволяют более эффективно решать вопросы безопасности, такие как противодействие DDoS-атакам. Кроме того, приближая серверы к потребителю услуг, мы создаем предпосылки для повышения скорости отклика интернет-ресурсов, размещенных в российских доменных зонах.

ПЛАНИРУЕТСЯ ЛИ СТРОИТЕЛЬСТВО НОВЫХ DNS-УЗЛОВ?

Мы планируем сеть, исходя как из технических потребностей, так и из запросов и потребностей пользователей наших услуг. Хочу заметить, что эти потребности постоянно меняются вместе с изменением технологий и интересов общества.

Например, очень интересен проект размещения новых DNS-узлов в местах локализации русскоязычного контента за рубежом — в первую очередь в странах СНГ, где проживает большое количество русскоязычного населения и русскоязычный интернет-контент пользуется большой популярностью. Потребность есть, и проект может быть реализован при наличии финансирования.



ВСЕРОССИЙСКИЙ КОНКУРС

«Позитивный контент»

Конкурс лучших интернет-проектов для детей и молодежи

Прием заявок на участие
с 1 июня 2017
www.positivecontent.ru

ОРГАНИЗАТОРЫ

РОЦИТ

ДЕТИ детский интернет

ФОНД РАЗВИТИЯ ИНТЕРНЕТ

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

«РОССИЙСКИЙ СЕГМЕНТ» ИНТЕРНЕТА — ЭТО СОВЕРШЕННО НЕОПРЕДЕЛЕННОЕ ПОНЯТИЕ

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР ТЕХНИЧЕСКОГО ЦЕНТРА ИНТЕРНЕТ **АЛЕКСЕЙ ПЛАТОНОВ** — О БЕЗОПАСНОСТИ, НОВЫХ ДОМЕНАХ И КАЧЕСТВЕ ЗАКОНОПРОЕКТОВ ОБ ИНТЕРНЕТЕ

ЧТО ТАКОЕ, С ВАШЕЙ ТОЧКИ ЗРЕНИЯ, «БЕЗОПАСНОСТЬ ДОМЕННОГО ПРОСТРАНСТВА»? СУЩЕСТВУЕТ ЛИ ВООБЩЕ ТАКОЕ ПОНЯТИЕ, ИЛИ ЖЕ ПРАВИЛЬНЕЕ ГОВОРИТЬ О БЕЗОПАСНОСТИ ВСЕГО ИНТЕРНЕТА?

Конечно, правильнее говорить о безопасности всего интернета в целом, поскольку в технологическом плане (замечу, что под интернетом сейчас многие понимают совершенно разные объекты) это единая система, построенная на основе многоуровневой (7 или 5 уровней– не имеет значения) сетевой модели. Но при этом вполне имеет право на существование вопрос о безопасности каждой составной части этой системы. Другое дело, что термин «доменное пространство» не соответствует никакому технологическому объекту — это просто обозначение совокупности доменных имен, использующихся для адресации в сети. Поэтому в этой теме следует говорить о таких вещах, как безопасность системы DNS (Domain Name System) или о безопасности реестров, в которых регистрируются и хранятся доменные имена. В каждом случае это достаточно специфический вопрос, имеющий, прежде всего, техническую направленность.

ТЦИ ФАКТИЧЕСКИ ОТВЕЧАЕТ ЗА ТО, ЧТОБЫ В РОССИЙСКОМ ИНТЕРНЕТЕ ВСЕ РАБОТАЛО КАК ЧАСЫ: НАБРАЛ ДОМЕН В БРАУЗЕРЕ — ПОПАЛ НА САЙТ. А НАСКОЛЬКО СЛОЖНО ТЕХНИЧЕСКИ ОБЕСПЕЧИТЬ ФУНКЦИОНИРОВАНИЕ РОССИЙСКИХ ДОМЕНОВ, КОТОРЫХ НА ПОДДЕРЖКЕ У ТЦИ, ПО ПОСЛЕДНИМ ДАННЫМ, ПОЧТИ 6,6 МИЛЛИОНА?

Вы говорите об адресации в сети интернет — и этот вопрос необходимо уточнить. Дело в том, что словосочетание «российский интернет» или «российский сегмент» сети интернет — это совершенно неопределенное понятие. Точнее, его можно определить различными способами (например, если обратиться все к той же пресловутой сетевой модели — на физическом, сетевом и прикладном уровнях), и в каждом случае это будет правильно. Суть состоит в том, что сеть интернет, в существующей реализации, является единой и сугубо международной (или трансграничной) — естественно, я опять говорю о технологической системе. Поэтому можно говорить только о том, что ТЦИ вместе со своими партнерами обеспечивает адресацию в пространстве национальных доменов .RU, .РФ, территориального домена .SU, а также «глобальных» доменов (так называемых gTLD) — .ДЕТИ и .TATAR, администраторами которых являются российские юридические лица. При любом раскладе «российский интернет» этими доменами не исчерпывается.

Что же касается обеспечения функционирования упомянутых выше доменов, то задача, конечно же, достаточно сложная. Наш коллектив занимается этим страшно давно — аж с 1994 года, когда домен .RU был делегирован Российскому НИИ развития общественных сетей (РосНИИРОС — в то время оператор научно-образовательных сетей RELARN-IP и RBNet), «наследником» которого в этой области деятельности, собственно, и является ТЦИ. Технический центр национального домена .RU как отдельное юридическое лицо — АО «Технический центр Интернет» — был образован в 2009 году, и уже в нем система была переработана и доведена до, не побоюсь этого слова, мирового уровня — причем на основе собственных разработок. Я могу это утверждать, потому что наш технический центр постоянно тестируется со стороны международной корпорации ICANN, которая контролирует работоспособность gTLD-доменов (в нашем случае — .ДЕТИ и .TATAR) — соответственно, мы должны удовлетворять всем весьма жестким требованиям, которые эта корпорация предъявляет.

ГЛАВНЫЙ РЕЕСТР И СИСТЕМА РЕГИСТРАЦИИ ДОМЕНОВ, Т.Е. ТО, ЧТО НАХОДИТСЯ В ВЕДЕНИИ ТЦИ — ЭТО КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА? ЧТО ВООБЩЕ, ПО ВАШЕМУ МНЕНИЮ, ОТНОСИТСЯ К КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЕ?

Для начала хочу отметить, что интернет создавался как сеть военного назначения, то есть в эту конструкцию изначально была заложена высокая отказоустойчивость и многократное резервирование различных систем и технологических процессов — таких как адресация, маршрутизация, передача данных и т.д. Сейчас за рубежом помимо термина «критический» часто используется понятие «essential» — «существенный», применяемое к компонентам, жизненно важным для системы, но не приводящих к ее немедленному краху в случае отказа. Другими словами, за счет резервирования и дублирования этих компонентов у нас достаточно времени для того, чтобы починить все, что нужно, и вернуться к штатной работе. Так что главный реестр, систему регистрации и DNS как раз можно охарактеризовать как существенные компоненты «российского интернета», но никак не критические. Что же касается второй части

вопроса — что можно отнести к критической инфраструктуре, то для того, чтобы на него ответить, необходимо определить предмет обсуждения, то есть говорить не об абстрактной критичности, а о конкретных объектах, работа которых сильно завязана на сеть Интернет, а также об ущербе, который возникает в случае нарушения функционирования этих объектов. Кстати, эти вопросы достаточно хорошо сейчас проработаны в законодательстве Европейского союза, и лучше будет не изобретать велосипед, а воспользоваться уже полученными результатами.

ТЦИ ЯВЛЯЕТСЯ УЧАСТНИКОМ ПРОЕКТА КООРДИНАЦИОННОГО ЦЕНТРА ДОМЕНОВ .RU/.РФ «НЕТОСКОП», И ДАЖЕ НЕ ПРОСТО УЧАСТНИКОМ, А КОМПАНИЕЙ, КОТОРАЯ ОБЕСПЕЧИВАЕТ ТЕХНОЛОГИЧЕСКУЮ ПЛАТФОРМУ ДЛЯ ИССЛЕДОВАНИЙ. ЧЕМ «НЕТОСКОП» ПОЛЕЗЕН ДЛЯ ТЦИ? МОГУТ ЛИ СПЕЦИАЛИСТЫ ТЦИ, КОТОРЫЕ УЧАСТВУЮТ В ЭТОМ ПРОЕКТЕ, НА ОСНОВАНИИ НАКОПЛЕННЫХ ДАННЫХ СДЕЛАТЬ КАКИЕ-ТО ВЫВОДЫ ОБ УРОВНЕ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ РОССИИ?

Напомню, что цель проекта «Нетоскоп» — проводить постоянный мониторинг вредоносной активности и вести единую базу данных классификации доменных имен в национальных доменных зонах .RU/.РФ. При этом основную роль в сборе информации о «зловредах» играют профессиональные игроки рынка информационной безопасности — как российские, так и зарубежные. Задача ТЦИ, помимо обеспечения платформы и рабочих инструментов работы — предоставление возможности использования реестров .RU/.РФ для агрегирования и систематизации данных по администраторам доменов, в которых наблюдается вредоносная активность. Таким образом, «Нетоскоп» является инструментом, с помощью которого КЦ осуществляет с регистраторами, уполномоченными организациями и администраторами доменов координирующие действия, направленные на борьбу с вредоносной активностью в национальных зонах. Что касается аналитических исследований по общему состоянию безопасности в соответствующих доменных зонах, то это вопрос КЦ. Хочу здесь подчеркнуть, что данные по доменам .RU/.РФ отнюдь не являются исчерпывающими для понимания ситуации с безопасностью в киберпространстве России — это только некоторая часть информации, относящаяся к использованию конкретных доменных имен для вредоносной деятельности.

За 5 лет существования проекта «Нетоскоп» удалось кардинально снизить количество претензий к национальным зонам со стороны зарубежных коллег. Образно выражаясь, мы перестали быть главными злодеями глобального рынка доменных имен, каковыми нас представляли в различных международных отчетах — и надо сказать, небезосновательно.

А КАК ОБСТОЯТ ДЕЛА У ТЦИ С ВНЕДРЕНИЕМ НОВЫХ ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ: TLS, DNSSEC, ЧТО-ТО ЕЩЕ? НАСКОЛЬКО ОХОТНО РОССИЙСКИЕ АДМИНИСТРАТОРЫ ДОМЕННЫХ ИМЕН ПОЛЬЗУЮТСЯ ЭТИМИ ТЕХНОЛОГИЯМИ?

ТЦИ придает большое значение защите информационных ресурсов, связанных с доменными зонами .RU/.РФ. В частности, с этой целью у нас применяется система управления информационной безопасностью в соответствии с принципами и требованиями международного стандарта ISO/IEC27001:2013 (Information technology — Security techniques — Information security management systems — Requirements). Для реализации криптографических алгоритмов, применяемых в системе DNSSEC ТЦИ при подписи клиентских доменов, используются 8 различных стандартов, включая отечественный — ECC-GOST (RFC5933). Подписание файла зоны ключами DNSSEC выполняется на двух географически разнесенных (в Москве и Санкт-Петербурге) серверах подписей. Процедура управления ключевой информацией DNSSEC выполняется персоналом ТЦИ с привлечением лицензиата ФСБ на операции по шифрованию данных и управление ключевой информацией — ООО «Удостоверяющий Центр Интернет».

Что касается протокола TLS, то он используется в нашей системе для защиты взаимодействия с регистраторами. На всех серверах реестра ограничено использование устаревших версий SSL, в апреле 2017 года в реестре была внедрена поддержка новейшего протокола TLS v1.2, использующего систему шифрования, работающую на эллиптических кривых — сейчас это считается наиболее надежным вариантом.

В отношении использования технологии DNSSEC российскими администраторами доменных имен могу констатировать, что их активность невысока — например, в зоне .RU подписано менее 1% общего количества доменов (в домене .РФ ситуация не лучше). Объяснить это довольно просто: инцидентов, связанных со специфическими атаками на DNS,

практически нет, а пользователь начинает что-то делать только в условиях прямой и явной угрозы. «Обязаловки» тут быть не может: мы просто даем соответствующую возможность, а использовать ее или нет — дело самого администратора. Хочу отметить, что в мировой практике ситуация с внедрением DNSSEC находится примерно на том же уровне (кроме тех доменов, где предпринимаются специальные усилия), и причина ровно та же.

КАК ВЫ СЧИТАЕТЕ, ЯВЛЯЮТСЯ ЛИ УГРОЗОЙ ДЛЯ БЕЗОПАСНОСТИ СЕТИ НОВЫЕ ДОМЕНЫ, КОТОРЫХ ПОЯВИЛОСЬ УЖЕ БОЛЕЕ 1200?

В глобальном смысле — нет. Все эти домены живут не сами по себе, а в рамках определенных достаточно жестких требований, сформулированных международной корпорацией ICANN, которая и является инициатором проекта new-gTLD. В качестве примера могу привести мониторинг угроз безопасности доменам верхнего уровня, осуществляемый через обязательный (в перспективе) сервис регистратуры — DRSP (Domain Reputation Service Providers). Конечно, существуют некие «местечковые» опасения: как же так, наши российские пользователи работают с доменами, которые мы не контролируем — возникает чувство незащищенности. Ответ тут очень простой — сеть Интернет глобальна, и у нас нет другого выхода, как более активно работать с международными организациями, координирующими вопросы безопасности — тогда все будет хорошо.

ПОЯВЛЕНИЕ НОВЫХ ДОМЕНОВ ПОВЛЕКЛО ЗА СОБОЙ И ПОЯВЛЕНИЕ СОТЕН НОВЫХ РЕГИСТРАТУР. А ЧТО С ТЕХНИЧЕСКИМИ ЦЕНТРАМИ? ПОЯВИЛИСЬ ЛИ НА РЫНКЕ НОВЫЕ ИГРОКИ? И КАК У НИХ ОБСТОИТ ДЕЛО С КИБЕРБЕЗОПАСНОСТЬЮ?

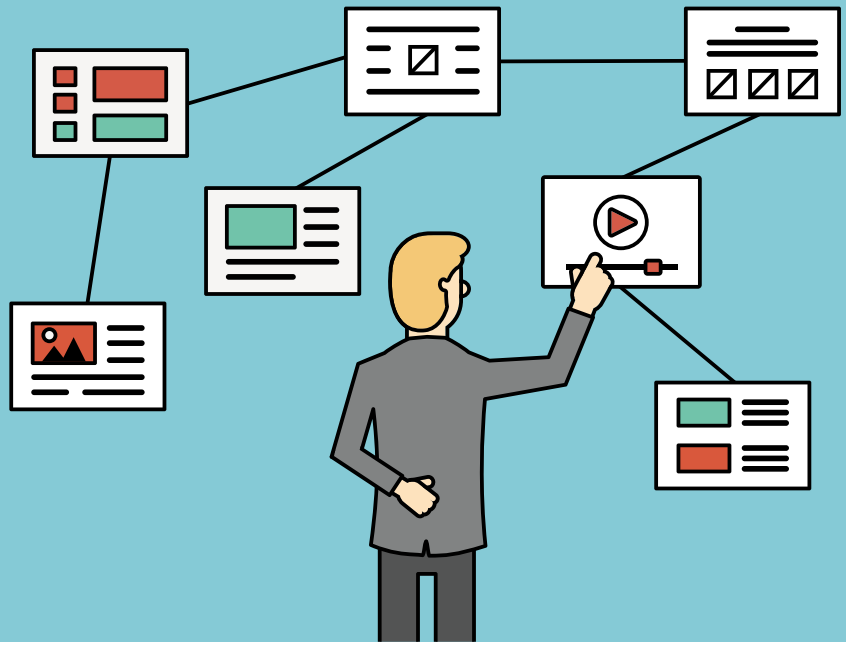
Общий объем рынка new-gTLD пока относительно невелик по сравнению с общим количеством доменов в традиционных gTLD и национальных ccTLD, поэтому активного роста числа технических центров не наблюдается. Их общее количество (для new-gTLD) сейчас — 43. Среди них есть традиционные техцентры типа Verisign, Afilias, Neustar — у них, по большому счету, даже масштабирования бизнеса не произошло. Есть участники, которые выросли из техцентров доменов второго уровня: например, CentralNic (сейчас занимает первое место по числу новых доменов на поддержке — 8 млн штук, что составляет почти 1/3 общего количества) или FlexIReg. Имеется группа техцентров национальных доменов — кроме ТЦИ, в ней представлены, например, бразильцы, новозеландцы, австралийцы, японцы. Совсем новых немного — могу отметить Google и Delloite. Кстати, в этом случае имеет место очень знаменательный процесс — приход в доменный бизнес лидеров своих сегментов рынка — информационных технологий и юридических услуг.

ПОЛТОРА ГОДА НАЗАД ВЫ ГОВОРИЛИ О ТОМ, ЧТО ЗАКОНОПРОЕКТЫ, ЗАТРАГИВАЮЩИЕ ИНТЕРНЕТ-ОТРАСЛЬ, ДОЛЖНЫ ПРОХОДИТЬ ТЕХНИЧЕСКУЮ И ТЕХНОЛОГИЧЕСКУЮ ЭКСПЕРТИЗУ. ИЗМЕНИЛАСЬ ЛИ СИТУАЦИЯ ЗА ПРОШЕДШИЕ МЕСЯЦЫ? СТАЛИ ЛИ ЗАКОНОПРОЕКТЫ, КАСАЮЩИЕСЯ ИНТЕРНЕТА, БОЛЕЕ ГРАМОТНЫМИ В ТЕХНИЧЕСКОМ ОТНОШЕНИИ?

Мне трудно прокомментировать эту тему, поскольку я не занимался отслеживанием и изучением законопроектов, возникших за последние месяцы. Единственное, что могу сказать — системы для профессионального обсуждения и формирования таких законопроектов не появилось, а, следовательно, ничего измениться не могло. Могут быть документы более грамотные, менее грамотные — но качество их может кардинально повышено только за счет системы, которая должна быть основана на каких-то публичных рабочих группах при Минкомсвязи, на профильных комитетах АДЭ, общественных организациях типа КЦ и т.д. Я, как наблюдатель «со стороны», вижу сейчас ситуацию, при которой законопроекты готовятся кулуарно, часто в интересах каких-то вполне конкретных выгодополучателей, а не в интересах отрасли, затем в них вносятся несущественные поправки по итогам «общественных обсуждений», после чего происходит проталкивание документа через Госдуму. Я не знаю, как обстоят дела в других отраслях народного хозяйства, но в отношении интернета дело выглядит именно так. Совершенно типичный пример — пресловутый «закон Яровой», который в принятом виде абсолютно бессмысленный и невыполнимый в технологическом плане, но зато интересен поставщикам систем хранения данных и строителям дата-центров. Теперь его надо как-то доводить до ума за счет подзаконных актов, правительственных распоряжений и т.д. Может, все же имеет смысл попробовать как-то по-другому делать такие вещи?

ДОМЕН — ЭТО НЕ САЙТ

.TXT
АЛЕКСАНДР ВЕНЕДЮХИН
Ведущий аналитик АО «Технический Центр Интернет»



Веб, как технология, возник в 1991 году, а действительно широкое распространение получил к 1995 году. Нет никаких сомнений, что именно веб стал той движущей силой, которая превратила современный Интернет в одно из ключевых достижений цивилизации. И тем не менее, технологически веб — всего лишь один из сервисов, работающих в Интернете. При этом далеко не самый древний сервис.

Так, система доменных имен (DNS) спроектирована в 1983 году, а внедрена в глобальной Сети в 1985, то есть за несколько лет до появления www-сервисов. Уже из этого можно сделать вывод, что и DNS, и доменные имена, как частный аспект системы, не являются чем-то похожим на «адресное» дополнение веба. Да, пользователи Сети привыкли, что для того, чтобы попасть на сайт, можно ввести его имя в адресной строке браузера. При этом чуть менее подготовленные пользователи вообще предпочитают вводить доменное имя не в адресной строке браузера, а в поисковой строке привычной поисковой машины, будь то Google или Яндекс. Однако способность направить браузер на нужный сервер по символьному имени — лишь одна из способностей доменной системы имен.

DNS представляет собой распределенную базу данных, которая хранит пары «ключ-значение». Существенной особенностью этой базы данных является то, что логические разделы образуют здесь иерархию, которая определяет права внесения новых записей и изменения существующих. Система также предоставляет сервис по поиску в базе данных. Когда пользователь вводит в адресную строку браузера имя домена, адресующего сайт, и браузер соединяется с соответствующим сервером, как раз работает иерархический сервис поиска, который позволяет найти в глобальной системе по имени домена соответствующую пару «имя-значение IP-адреса». Именно IP-адрес из этой пары обозначает сервер, с которым соединяется браузер, то есть тот сервер, на котором работает (публикуется) веб-сайт.

В DNS хранятся не только и не столько адреса серверов, на которых размещаются веб-сайты. Есть большое число других типов записей (структуры данных, размещаемые в DNS, называют «записями»), среди них: имена почтовых серверов; индексы и идентификаторы, используемые для обнаружения спама; имена серверов, поставленные в соответствие их адресам (так называемые «обратные зоны»); отпечатки криптографических ключей и так далее, и тому подобное. Другими словами: веб не влияет на работу DNS и напрямую не связан с этой системой, которая лежит в основе современной инфраструктуры Интернета, наряду с протоколами TCP/IP. Но, конечно, без DNS современный веб работать перестанет. Несмотря на то, что, если специально постараться и настроить сервер, на сайты можно будет заходить непосредственно по IP-адресам: соединение в таком случае установить удастся,

но вот огромный пласт современных сопутствующих веб-технологий работать не будет. Так, например, невозможной окажется проверка TLS-сертификатов, необходимых для защищенного соединения по HTTPS — сертификаты выпускаются только для имен доменов, а это часть DNS.

Пусть test.ru — это имя домена. Под ним можно разместить веб-сайт, настроив DNS таким образом, что test.ru будет указывать на IP-адрес сервера с веб-сайтом. Доменое имя test.ru — это имя второго уровня в зоне .ru. С давних времен, когда другие сервисы были не менее распространены, чем www, для последнего традиционно выделялось специальное имя www.test.ru — это имя третьего уровня, где www соответствует записи в зоне test.ru. При этом под именами www.test.ru и test.ru могут находиться разные веб-сайты, или, например, test.ru вообще может не обозначать никакого сайта (или другого ресурса), но оставаться полноценным именем в DNS. Еще раз обратите внимание — на уровне DNS никаких сайтов не существует, в этой системе лишь содержится запись, которая ставит в соответствие имени www.test.ru некоторый IP-адрес. Подстрока www при этом тоже никак не определяет того, что по данному адресу доступен веб-сервер — это всего лишь символы имени, они не задают тип протокола. Использование www — это только традиция, ничуть не хуже сработают web.test.ru, site.test.ru или abrakadabra.test.ru. Кстати, правило именования сайтов с www уходит в прошлое: сейчас веб является сервисом по умолчанию, поэтому должен быть доступен под именем без www.

DNS — распределенная и иерархическая система. Домен, а точнее доменная зона, которые обозначаются сочетанием строк символов, разделяемых точками, представляют собой идентификатор некоторого пространства имен. Разберем обозначение server.test.ru: оно относится к пространству внутри зоны server, которая находится внутри зоны test, последняя размещается внутри зоны ru, а все они вместе — внутри так называемого корневого домена, обозначение которого часто опускают, однако в полной записи корневой домен может быть обозначен завершающей точкой справа (server.test.ru.). Имени server.test.ru (так называемая «вершина» зоны) может быть сопоставлен, например, IP-адрес, который соответствует некоторому узлу Сети. Эта ситуация полностью аналогична описанной в предыдущем абзаце.

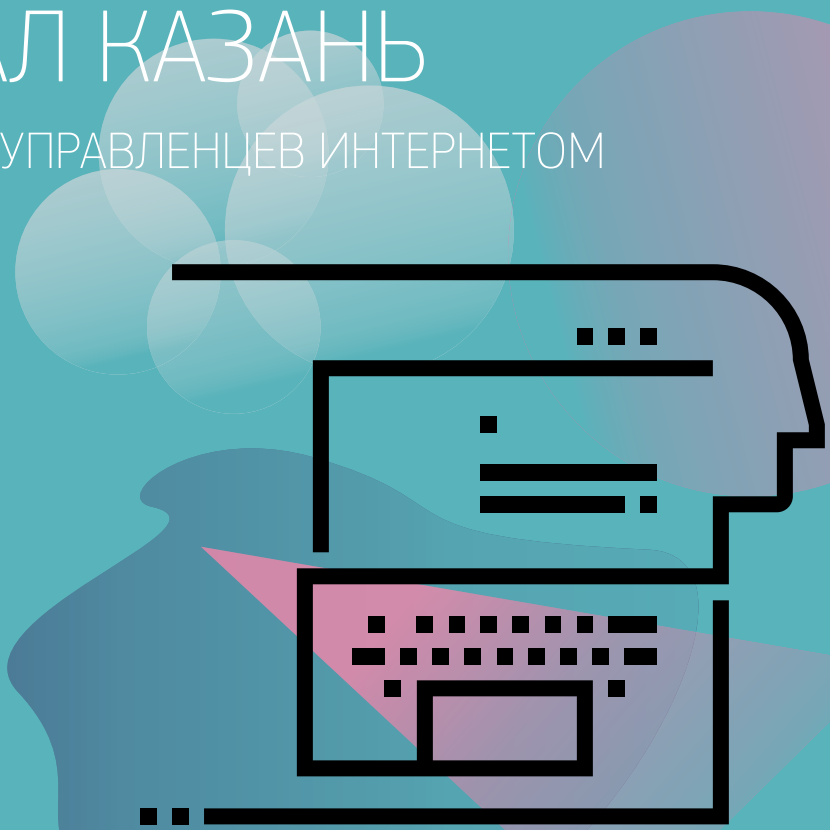
Но это вовсе не означает, что server.test.ru «схлопнулось» до одной точки, одного узла. Напротив, этому же имени в DNS могут соответствовать и многие другие записи: о почтовых серверах, о списке IP-адресов, которые могут отправлять почту от адресов в данной доменной зоне и так далее. Скажем, если полностью удалить из DNS зону с именем server.test.ru, то перестанет работать не только веб-сайт, но и электронная почта для адресов в этой зоне. То есть, понятие доменного имени существенно шире одного из вариантов использования, которым является размещение веб-сайта.

В иерархию выстроены и права управления доменными зонами. Право внесения изменений, добавления новых имен и записей (это разные вещи: одному имени могут соответствовать несколько записей) делегируется администратором зоны, которая находится уровнем выше (то есть, «правее»). Так, администратор зоны .ru делегирует права по управлению пространством имен зоны второго уровня test.ru администратору этой зоны. Администратор также может делегировать кому-то права по управлению servers.test.ru, но может и самостоятельно создавать записи и новые зоны внутри test.ru. Административная иерархия может быть довольно сложной. В техническом смысле она проецируется в иерархию серверов имен (NS), которые поддерживают ту или иную доменную зону. Именно назначение «ответственных» (авторитативных) серверов имен, которые указываются в зоне уровнем выше, и является технической операцией, делегирующей доменные имена в DNS на практике. Заметьте, что делегирование не связано напрямую с регистрацией доменного имени. Зарегистрированный домен (доменная зона) может быть не делегирован, это означает, что он будет отсутствовать в DNS. Также возможно делегирование без всякой процедуры регистрации, обычно оно наблюдается на уровнях ниже второго: например, администратор зоны test.ru делегирует зоны shop.test.ru, device.test.ru и передает кому-то права управления этими зонами без какой бы то ни было процедуры регистрации домена.

Итак, доменное имя — часть системы адресации Интернета, эта часть позволяет пользователям запоминать вместо числовых адресов символьные имена, которые помогают им отличать один сайт от другого. Но к самим веб-технологиям доменное имя имеет не больше отношения, чем дорога — к автомобилю.

КАК Я БРАЛ КАЗАНЬ

ПУТЕВЫЕ ЗАМЕТКИ УПРАВЛЕНЦЕВ ИНТЕРНЕТОМ



.TXT

МИХАИЛ АНИСИМОВ
Координационный центр доменов .RU/.РФ

ВЕСНА 2017 ГОДА ВЫДАЛАСЬ ХОЛОДНОЙ ПО ПОГОДЕ, НО ОЧЕНЬ ЖАРКОЙ ПО МЕРОПРИЯТИЯМ. ТАКОЙ ПЛОТНОСТИ СОБЫТИЙ, КОМАНДИРОВОК, ВСТРЕЧ И ДРУГИХ АКТИВНОСТЕЙ НА ЕДИНИЦУ ВРЕМЕНИ Я НЕ ПОМНЮ ДАВНО. ГЛАВНЫМ, КОНЕЧНО, БЫЛ ВОСЬМОЙ РОССИЙСКИЙ ФОРУМ ПО УПРАВЛЕНИЮ ИНТЕРНЕТОМ, ПРОШЕДШИЙ В ИННОПОЛИСЕ, В РЕСПУБЛИКЕ ТАТАРСТАН. ПОД ЗНАКОМ ПОДГОТОВКИ К НЕМУ ПРОШЕЛ КУСОК ОСЕНИ, НОВОГОДНИЕ ПРАЗДНИКИ И ВСЯ ВЕСНА.

Начать надо с того, что это был первый форум, который проходил не в Москве. Координационный центр доменов .RU и .РФ проводил его совместно с Министерством информатизации и связи Татарстана и мэрией Иннополиса. Выездные мероприятия — то еще приключение. Спикеры, оборудование, декорации, пресса — все это надо не просто собрать, но и доставить в место проведения мероприятия, найти местных подрядчиков, учесть все местные транспортные и остальные реалии. В таких случаях мне на память всегда приходит старый-старый анекдот с шикарной фразой в конце «а сейчас со всем этим мы попробуем взлететь».

Надо отдать должное, даже несмотря на все трудности с приглашением гостей в регионы, форум в этом году был очень представительный. В различных секциях получилось собрать гостей из различных европейских стран, США, Китая, Вьетнама, ЮАР, представителей различных международных организаций вроде ООН или Совета Европы, наших давних партнеров и друзей из ICANN, ISOC, APTLD и RIPE NCC.

Хотя приглашение спикеров — это, конечно, была отдельная история. По своему драматизму она вполне сошла бы за хорошую детективную историю. Там было все — утерянные письма и отказы в визах, внезапные родственники, которых надо откуда-то спасать, переводы на другие должности и другие интриги. Если бы эту историю экранизировали, я бы хотел, чтобы меня сыграл Киану Ривз.

К счастью, в конце концов все закончилось хорошо, и собрали действительно достойную конференцию. В этот раз говорили о разных вопросах: кибербезопасности, электронном правительстве, международном сотрудничестве и инновациях в интернете.

Начался форум с того, что исполнительный директор Ассоциации Азиатско-Тихоокеанских регистратур доменов верхнего уровня Леонид Тодоров прочитал лекцию о принципах управления интернетом для начинающих. В качестве начинающих выступили и студенты, специально прогулявшие свои лекции в Университете Иннополиса, и гости форума, и даже некоторые спикеры. Леонид, явно ведущий свою уже сто пятидесятую лекцию, хорошо поставленным голосом и свойственным только ему особым чувством юмора рассказал о том, как менялись подходы к управлению глобальной сетью на протяжении всей ее истории, от прокладки первого трансатлантического кабеля и до недавнего завершения процесса IANA Transition.

Вообще в этом году форум носил ярко выраженный молодежный характер. На всех секциях говорили о том, что надо привлекать новых участников ко всем процессам, в особенности молодежь — им предстоит формировать облик интернета будущего и представлять интересы своих стран и своих сообществ на глобальной арене. За день до самого форума некоторые наши спикеры специально ездили в ВУЗы Казани, чтобы рассказать студентам о последних трендах и новых вызовах, с которыми они же и столкнутся.

На секции по кибербезопасности говорили о такой насущной проблеме, как атрибуция атак и поиск ответственных за совершение киберпреступлений. Пожалуй, самая горячая тема прошлого года, когда во всех новостях мы только и слышали о русских хакерах на американских выборах, китайских киберсолдатах и электронных шпионах США. Ничто не вызывало споров больше, чем попытка одних экспертов обвинить в различных инцидентах конкретные страны, и других — откреститься от этих обвинений. На секции спикеры попробовали договориться между собой, а возможно ли вообще установить, кто стоит за происшествием. Главным итогом было предложение более полно обмениваться информацией между различными ответственными организациями из разных стран и более плотно работать техническим специалистам и экспертам по законодательному регулированию.

Об электронном правительстве говорили с участием Министерства связи Татарстана, а также представителей министерств Вьетнама, ЮАР, секретариата глобального форума IGF. Участники делились своим опытом внедрения электронных услуг и налаживания обратной связи между государством и гражданским обществом.

Очень интересную задачу поставили себе спикеры секции по международному сотрудничеству — они попытались определить, существует ли общая для евразийского континента повестка в вопросах управления интернетом. Можно ли выявить что-то общее в том, как интернетом управляет Китай, Европа, страны СНГ? Как выяснилось, есть несколько принципов, которые разделяют все присутствующие, например, про роль межгосударственного диалога или про необходимость образования в сфере IT. То, что панелисты смогли так легко договориться, кажется, стало сюрпризом даже для них самих.

Интернету вещей посулили блестящее будущее на секции про инновации и новые рубежи развития глобальной сети. По словам участников, он уже сейчас незаметно, невидимо проник в смежные отрасли, а буквально через несколько лет полностью изменит их облик. Сельскохозяйственные дроны, станки, управляемые через Wi-Fi, грузы с радиометками и огромные массивы информации, которые все это сопровождают — примерно так будет выглядеть промышленность в скором времени. Спикеры особо отметили, что уже после 2020 года количество устройств, подключенных к глобальной сети, вполне может сравниться с количеством людей, имеющих доступ к интернету, и даже превысить их. Будущее интернета действительно за предметами, а не живыми пользователями.

Вечером после завершения конференции традиционно праздновался день рождения домена .RU. Проходило все в Казани, в ресторане Пашмир, куда мы отправились на автобусах. Иннополис находится на открытой местности, сам город небольшой и открытый всем ветрам, так что некоторые гости в шутку называли его «Инно-поле-с». Непривыкшие к такой погоде гости из южных стран добирались до автобуса короткими перебежками.

Как правило, неформальная или праздничная часть всех выездных мероприятий оформляется обязательно с местным колоритом. Вот и сейчас по совету коллег выбрали ресторан с местной кухней, пригласили артистов, которые исполняли татарские песни и танцы, рассказывали о национальных инструментах и даже знакомили гостей с татарским языком. Кульминацией вечера стал вынос большого барана, зажаренного на вертеле — с ним сфотографировались, кажется, все.

Вообще Казань в этот раз встретила невероятно гостеприимно — погода, так долго капризничавшая перед форумом, вдруг подарила несколько солнечных дней, пробки вдруг каким-то волшебным образом рассосались и позволили добираться везде вовремя. На следующий день мы нашей довольной, но уставшей командой выбрались в местный кремль и за обязательным татарским сувениром — чак-чаком. Учитывая мои национальные корни, мне заказали привезти его в каких-то промышленных количествах.

Гостеприимство города оказалось настолько большим и бескомпромиссным, что самолет, на котором в Москву улетала практически вся команда и часть спикеров, вначале задержали на пять часов, а потом и вовсе отменили. Тут же нашелся другой рейс, который вылетал буквально через полчаса, и на который еще надо было купить билеты, зарегистрироваться и сдать багаж. Эти толпы людей, бегающих по терминалу с чак-чаком наперевес, я буду помнить еще очень долго. Но надо отдать должное нашим девушкам-ивентщикам: они быстро взяли ситуацию в свои руки, организованно поменяли всем билеты (кажется, даже нескольким сторонним пассажирам, чему те были очень рады) и проследили, чтобы все нашли свой самолет.

Возвращались домой мы уже глубокой ночью. Москва встретила привычными пробками и весенней слякотью. Прошедшее мероприятие превратилось в воспоминание — ты уже не чувствуешь его так остро, на кончиках пальцев, и не переживаешь выход каждого спикера как собственный выпускной в школе. Оглядываясь назад, ты не веришь, что всего три дня вместили в себя столько событий. В груди появляется то самое щемящее чувство — удовлетворение от проделанной работы и легкая грусть, что все закончилось. И еще более острое осознание того, как же это круто, быть причастным к таким удивительным вещам.

.TXT
СЕРГЕЙ АЛИМБЕКОВ
Заместитель директора по техническому развитию ФРИИ

НА ПУТИ К ЦИФРОВОЙ ЭКОНОМИКЕ

ИЗ ГОДА В ГОД ПОЧТИ НА ЛЮБОЙ КОНФЕРЕНЦИИ, ПОСВЯЩЕННОЙ РАЗВИТИЮ РОССИЙСКОЙ ИНТЕРНЕТ-ОТРАСЛИ, МЕЛЬКАЮТ С ЗАВИДНЫМ ПОСТОЯНСТВОМ ОДНИ И ТЕ ЖЕ ИНДИКАТОРЫ: КОЛИЧЕСТВО ПОЛЬЗОВАТЕЛЕЙ СЕТИ, КИЛОМЕТРАЖ ПРОЛОЖЕННЫХ КАБЕЛЕЙ, ЧИСЛО СМАРТФОНОВ НА РУКАХ НАСЕЛЕНИЯ, САЙТОВ В ЗОНЕ .RU. ПОЛЕЗНЫЕ ЦИФРЫ — СПОРУ НЕТ. ДОСТАТОЧНО ЛИ ИХ, ЧТОБЫ СНОВА И СНОВА ОТМЕЧАТЬ ТРИУМФ ИНТЕРНЕТ-ИНДУСТРИИ В РОССИИ? УВЫ, НЕТ.

Гипотеза лингвистической относительности, сформулированная когда-то Эдвардом Сепиром и Бенджамином Уорфом, гласит: язык определяет сознание. Измеряя российский интернет в числе пользователей, километрах оптики и терабайтах переданных данных, мы сами загоняем себя в устаревшую парадигму прошлых десятилетий, когда только закладывалась основа современной цифровой экономики. Загонять себя в эти рамки — обречь себя на постоянное технологическое отставание.

Действительно, интернет прошлого легко описывался пропускной способностью, числом сайтов и построенных ЦОДов. Точно так же, как в индустриальном обществе, основой инфраструктуры, помимо дорог и мостов, также стали физические объекты — станки и заводы, а в постиндустриальном — телеграфные и телефонные кабели. Но времена «железной» инфраструктуры ушли в прошлое больше десятка лет назад, когда инвесторы всего мира были опьянены сладким будущим телекомов. Интернет,

которым нужно грезить сегодня,— это триумвират стандартов, платформ и протоколов. И чем быстрее наша отрасль перестроит не только свой лексикон, но и способ мышления, тем более конкурентоспособной окажется российская экономика в цифровой эпохе.

В цифровой экономике ядром новой инфраструктуры выступает код, то есть софт, который ложится поверх сетей, гаджетов и датчиков, уже развернутых, но зачастую не утилизированных в полной мере. Тысячи и миллионы строчек сложного кода, объединенные мощной глобальной идеей и бизнес-моделью, способны менять целые рынки. Uber уже не только транспортная платформа, он выходит на рынок логистики и доставки. WeChat — состоявшаяся финансовая и торговая платформа, угрожающая банкам и игрокам электронной коммерции. Свои платформы для интернета вещей продвигают и Google, и Huawei. Платформой «больших данных» собирается стать Facebook — и это будущее еще не определено, потому что для данных и больших данных у нас до сих пор нет понятийного аппарата.

Одна из историй из нашего опыта: для одного из наших проектов по обработке больших данных нам понадобились данные геопозиционирования пользователей от мобильного оператора. И хотя партнер был готов нам эти обезличенные данные предоставить, все остановилось в процессе согласования договора. Почему? Все дело в отсутствии нормативов: нет никаких формально обозначенных понятий, что такое данные, кому их можно и нельзя передавать, как именно это делать и так далее. Нет ни закрепленного нормативами языка, предназначенного для описания работы цифровой экономики, ни стандартов его использования.

Хоть мы во ФРИИ часто говорим, что данные — это новая нефть, есть один важный нюанс: ценность нефти не снижается в зависимости от времени, которое ушло на её хранение. В отношении данных это не совсем верно. Данные без движения, без обмена между компаниями легко обесцениваются. Просто накопить много данных, а затем продавать их куда-то на сторону — то же самое, что топить печку ассигнациями. Ценность каждой порции данных несоизмеримо возрастает, если уметь ее правильно извлекать, структурировать и обмениваться с другими игроками рынка. Разумеется, с помощью накопленного массива данных можно решить какие-то внутренние проблемы компании. Но синергетический эффект в цифровой экономике возрастает только при свободном обмене данными. А для этого надо создать правила и условия обмена, соответствующие технологии, API — в общем, ту самую инфраструктуру. А на базе этой инфраструктуры уже появится масса дополнительных сервисов и стартапов. Например, всего десять лет назад, чтобы купить билет на самолет, нужно было стоять в очереди в кассу авиакомпании, а отель бронировать по телефону. Появление в отрасли цифровой инфраструктуры дало предпринимателям возможность открыть десятки конкурирующих сервисов, некоторые из них выросли в настоящих гигантов интернет-отрасли. А сама индустрия авиаперевозок получила приток новых клиентов и прозрачность, о которой можно было раньше только мечтать.

Разумеется, на пути к становлению цифровой экономики предстоит решить целый ряд проблем. Например, проблему так называемого «цифрового феодализма», когда каждый уважающий себя IT-специалист разрабатывает собственную информационную систему — как для бизнеса, так и для государства. Но создание объединенной информационной системы или реестра таких систем — тупиковый путь: как только ты написал ТЗ на такую систему, оно в тот же момент становится устаревшим. Но преодолеть проблему цифрового феодализма можно с помощью агентов по обмену данными, которые будут обеспечивать передачу информации между всеми этими системами. Над одним из таких механизмов работает и ФРИИ — это IDX, механизм для обмена данными в инфраструктуре новой цифровой экономики.

IDX — лишь один из примеров распределенной сервисной платформы будущего, которая может стать точкой роста цифровой экономики. Системы обеспечения целостности и систематизации больших данных, фиксации событий на базе умных контрактов и технологии blockchain, ИИ и виртуальной реальности — вот сквозные проекты, которые будут создавать новые рынки и источники дохода в цифровой экономике. А пользователями всех этих платформ будем все мы — как уже пользуемся множеством открытых платформ вроде финтех-сервисов, Uber и мессенджеров, которые обеспечивают уже сегодня не только коммуникации между людьми, но и между людьми и «машинами» и «машин» между собой. Это только начало.

ИЗУЧИ ИНТЕРНЕТ — УПРАВЛЯЙ ИМ

игра-интернет.рф

Онлайн-портал для школьников, который поможет узнать
как устроен интернет и работают главные IT-сервисы

ОБРАЗОВАТЕЛЬНЫЙ МОДУЛЬ

- ЗНАНИЯ И ФАКТЫ ПОДАЮТСЯ В ФОРМЕ УВЛЕКАТЕЛЬНЫХ ЗАДАЧ, АРКАДНЫХ ИГР, ПАЗЛОВ, ГОЛОВОЛОМОК, МУЛЬТИМЕДИА ВОПРОСОВ

ТРЕНИРОВОЧНОЕ ПРИЛОЖЕНИЕ

- ДЛЯ ЗАКРЕПЛЕНИЯ ПОЛУЧЕННЫХ ЗНАНИЙ
- ДОСТУПНО ДЛЯ ANDROID, IOS, WINDOWS

ВСЕРОССИЙСКИЙ ОНЛАЙН-ЧЕМПИОНАТ

- ВОЗМОЖНОСТЬ ПРОВЕРИТЬ СИЛЫ И ПРОДЕМОНСТРИРОВАТЬ ЗНАНИЯ, УСТАНОВИТЬ НОВЫЕ РЕКОРДЫ, ПОЛУЧИТЬ ЗВАНИЕ ЧЕМПИОНА И ЦЕННЫЕ ПРИЗЫ
- ПРОВОДИТСЯ ЕЖЕГОДНО

Цель проекта — повышение уровня цифровой грамотности начинающих
пользователей интернета в современной интерактивной форме

ОРГАНИЗАТОР

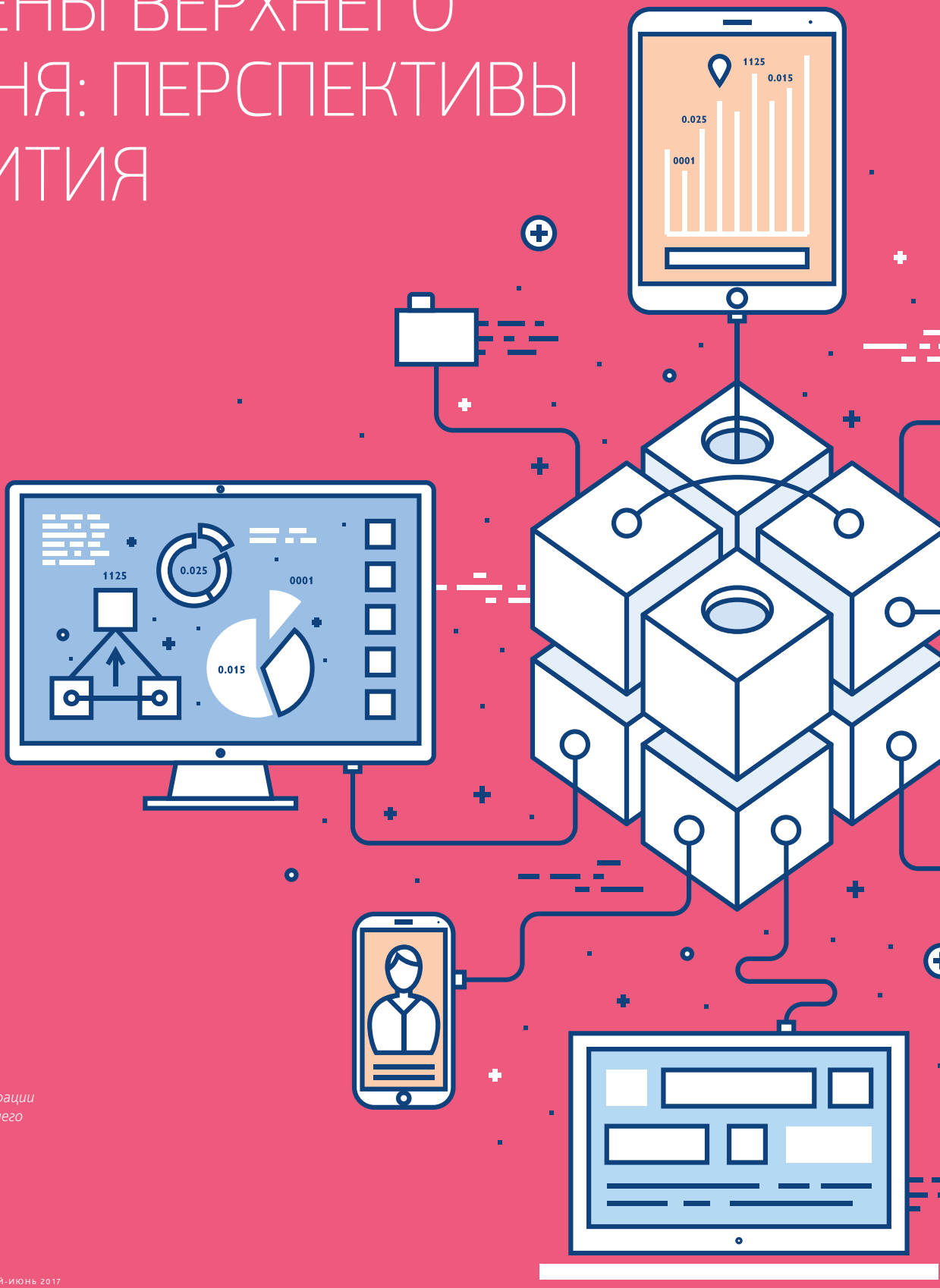
КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

ГЕНЕРАЛЬНЫЙ ПАРТНЕР

Ростелеком

игра-интернет.рф

КОРПОРАТИВНЫЕ ДОМЕНЫ ВЕРХНЕГО УРОВНЯ: ПЕРСПЕКТИВЫ РАЗВИТИЯ



.TXT
СЕРГЕЙ ГОРБУНОВ
Руководитель направления развития сервисов регистрации имен в новых доменах верхнего уровня, RU-CENTER Group

ТРЕТЬ ИЗ БОЛЕЕ ЧЕМ ВОСЬМИСТА РАБОТАЮЩИХ К НАСТОЯЩЕМУ МОМЕНТУ NEW GTLD — ДОМЕНЫ БРЕНДОВ. BMW, IBM, HERMES, PHILIPS — ВОТ ДАЛЕКО НЕ ПОЛНЫЙ СПИСОК КОМПАНИЙ С МИРОВЫМ ИМЕНЕМ, ПОДАВШИХ ЗАЯВКИ НА СОЗДАНИЕ ДОМЕННЫХ ИМЕН, СОВПАДАЮЩИХ С НАЗВАНИЕМ ИХ ПРОДУКТОВ И УСЛУГ.

ПРИ ЭТОМ ПОЛНОЦЕННОЕ ИСПОЛЬЗОВАНИЕ КОРПОРАТИВНЫХ ДОМЕННЫХ ЗОН — ПОКА СКОРЕЕ ЭКЗОТИКА. В БОЛЬШИНСТВЕ ИЗ НИХ СЕГОДНЯ ДОСТУПНО ТОЛЬКО ОДНО ИМЯ ВИДА NIC.DOMAIN (НАПРИМЕР, NIC.TOSHIBA) И ТО СКОРЕЕ ПОТОМУ, ЧТО ЭТО НЕОБХОДИМО ДЛЯ ФОРМАЛЬНОГО СООТВЕТСТВИЯ ТРЕБОВАНИЯМ КОРПОРАЦИИ ICANN, КООРДИНИРУЮЩЕЙ СОЗДАНИЕ НОВЫХ ДОМЕНОВ, В ТОМ ЧИСЛЕ ДЛЯ БРЕНДОВ.

ПРИЧИН, ПО КОТОРЫМ КОРПОРАТИВНЫЕ ЗОНЫ ОСТАЮТСЯ НЕВОСТРЕБОВАННЫМИ У ИХ ОБЛАДАТЕЛЕЙ, НЕСКОЛЬКО.

Во-первых, многие компании участвовали в New gTLD исключительно в целях защиты коммерческих названий своих продуктов, опасаясь, что совпадающие с ними домены верхнего уровня могут быть зарегистрированы третьими лицами и впоследствии использованы в целях, противоречащих репутации брендов-заявителей. В таких случаях получение собственного домена верхнего уровня стало скорее юридическим проектом, успешно завершенным по итогам прохождения необходимых процедур ICANN.

В некоторых компаниях юристы, отвечающие за обеспечение прав интеллектуальной собственности и изначально инициировавшие внедрение корпоративного домена, после его получения пытаются передать доменную зону в маркетинговые подразделения для дальнейшего коммерческого использования, однако зачастую это не имеет успеха.

Маркетологи, как правило, опасаются размещать какие-то проекты в новом домене ввиду риска его слабой узнаваемости у целевой аудитории в сравнении с привычными именами второго уровня. Коммерческие отделы зачастую действуют по принципу «не навреди»: при не всегда очевидных преимуществах «переезда» на собственный домен верхнего уровня возможная потеря части трафика на сайтах (и, как следствие, клиентов) остается весомым аргументом против перемен.

Однако даже если инициатива создания корпоративной доменной зоны в свое время исходила, например, от департамента маркетинга или первого лица компании, ситуация, в которой ее домен так пока и не используется, остается распространенной.

Дело в том что внедрение New gTLD растянулось на несколько лет и за этот период произошла естественная ротация кадров: в результате в ряде компаний сторонники брендированного доменного пространства сменились на тех, кто относится к этой идее без энтузиазма.

На это накладывается бюрократия больших корпораций — в результате процесс размещения контента в доменах брендов зачастую продвигается крайне медленно или вовсе стоит на месте.

Тем не менее примеры успешного использования New gTLD компаниями есть — так, уже больше года глобальный сайт Canon доступен по адресу global.canon, а немецкие дилеры Audi получили по доменному имени в одноименной зоне, сделав ее лидером по количеству регистраций в «закрытых» доменах (более 500 имен на сегодняшний день).

Очевидно, что этот тренд будет набирать обороты вместе с дальнейшим ростом распространенности и узнаваемости новых доменов. Сегодня бизнес все чаще делает выбор в пользу ярких имен New gTLD, а пользователи постепенно привыкают к тому, что кроме традиционных адресов .com, .net, .ru существуют сотни тематических.

В конечном итоге это будет стимулировать бренды к более активному использованию принадлежащих им доменных зон — его преимущества очевидны.

Анонсировав перенос сайтов в отдельный домен верхнего уровня, компания в дальнейшем исключит ситуации, когда какое-то интересующее ее имя, например, для промо-акции, окажется занято под сторонний проект. Все зарегистрированные доменные имена будут однозначно ассоциироваться

с брендом, также значительно снизится риск успешного создания связанных с ним мошеннических ресурсов — клиенты компании будут знать, что контент, размещенный за пределами ее корпоративной зоны, не является официальным. При этом привычные адреса сайтов бренда могут оставаться активными — достаточно настроить для них перенаправление на имена в новом домене, сделав, таким образом, переход к его использованию постепенным и безболезненным для пользователей.

Значительный потенциал развития корпоративных доменов отмечают и эксперты доменного рынка. По их прогнозам, основное число заявок в рамках следующего этапа New gTLD (ожидается в 2020 году) придется именно на зоны для брендов.

Они будут интересны, в первую очередь, компаниям с разветвленной филиальной или дилерской сетью, широкой продуктовой линейкой или несколькими направлениями деятельности под единым брендом.

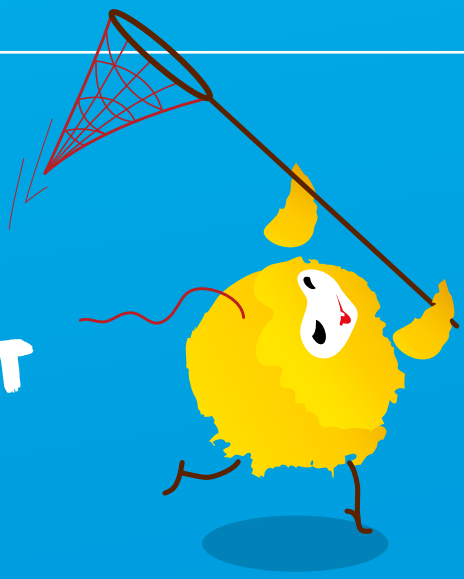
Домены верхнего уровня могут быть востребованы в том числе и у российского корпоративного сектора: оказывая комплексные услуги по сопровождению внедрения New gTLD, мы в RU-CENTER регулярно получаем соответствующие запросы от отечественных производителей и поставщиков товаров и услуг. Окончательный уровень спроса определят обновленные правила и стоимость подачи заявок на домены — эти аспекты в настоящий момент прорабатывает ICANN.

Отраслевая активность в новых зонах *(Источник: РБК)*

Компании	Зарегистрированные домены
АВТОПРОИЗВОДИТЕЛИ	
Fiat	.alfaromeo, .ferrari, .fiat, .lancia, .maserati
BMW	.bmw, .mini
Chrysler	.chrysler, .dodge, .jeep
Ford	.ford, .lincoln
Nissan	.infiniti, .nissan
Toyota	.lexus, .toyota
Другие	.audi, .bentley, .honda, .hyundai, .jaguar, .kia, .lamborghini, .landrover, .volkswagen, .volvo, .seat, .suzuki
РИТЕЙЛЕРЫ	
Alibaba Group	.alibaba, .alipay, .taobao
Wal-Mart	.asda, .george, .samsclub, .walmart
The Gap	.athleta, .bananarepublic, .gap, .oldnavy, .piperlime
Macys	.bloomingdales, .macys
Другие	.bestbuy, .boots, .mango, .next, .obi, .zara
ФИНАНСОВЫЙ СЕКТОР	
American Express	.americanexpress, .amex
Citigroup	.banamex, .citi
Barclays Bank	.barclaysbank, .barclays
JP Morgan	.chase, .jpmorgan, .jpmorganchase
Другие	.bbva, .bnpparibas, .forex, .hsbc, .lacaixa, .ubs, .visa
МЕДИА	
	.bbc, .bloomberg, .canalplus, .eurovision, .cbs, .guardian, .hbo, .observer, .showtime, .spiegel, .theguardian

.ДЕТИ

ДОМЕН ДЛЯ САЙТОВ О ДЕТЯХ И ДЛЯ ДЕТЕЙ



ТАКОЙ ИНТЕРНЕТ, ГДЕ ОПАСНОСТИ НЕТ

- Объединяет сайты для детей и подростков
- Защищает пользователей от негативной и опасной информации, круглосуточный мониторинг сайтов
- Содержит только качественные познавательные, образовательные и развлекательные ресурсы, которым можно доверять

интернет.дети

Домен .ДЕТИ необходим компаниям, СМИ, детским садам, школам, досуговым учреждениям, фондам и всем, кто работает в интересах детей и подростков

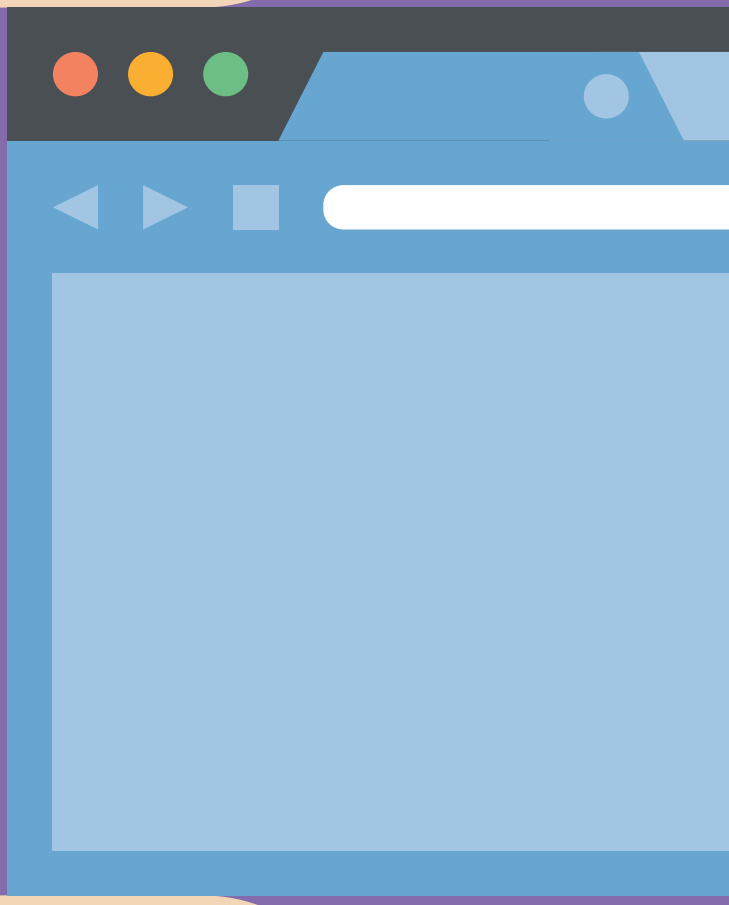
Аккредитованные регистраторы:

RU center

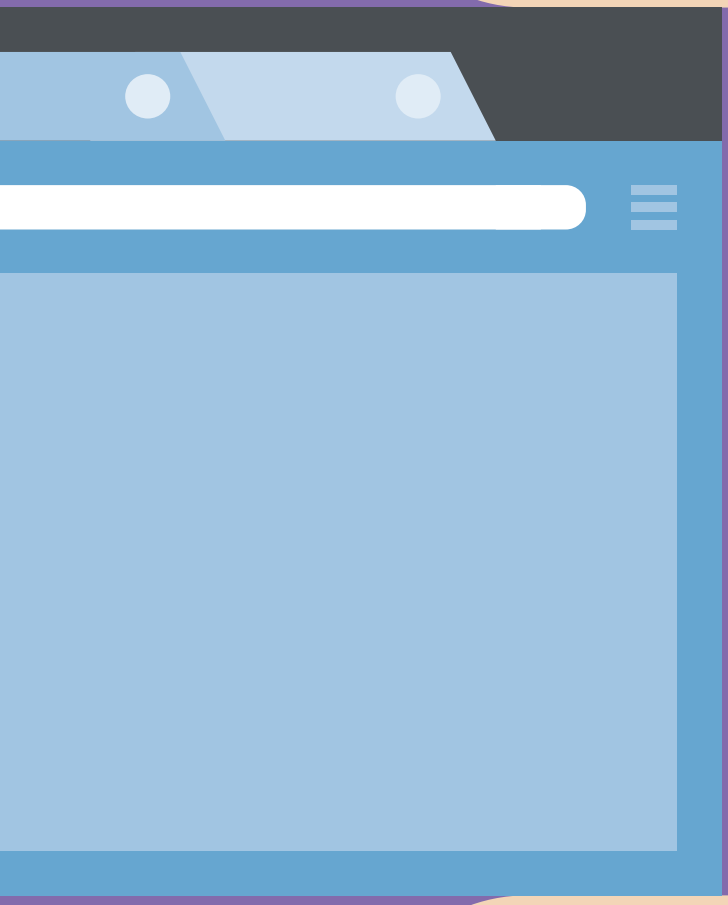
REG.RU

webnames.ru

TLS КАК ДВАЖДЫ ДВА



ВЫ НАВЕРНЯКА ИСПОЛЬЗУЕТЕ TLS ПОСТОЯННО. НАПРИМЕР, ЕСЛИ ВЫ ЗАХОДИЛИ В СИСТЕМУ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ (ИНТЕРНЕТ-БАНК), ТО ИСПОЛЬЗОВАЛИ ЗАЩИЩЁННУЮ ВЕРСИЮ ПРОТОКОЛА HTTP — HTTPS, А ОНА РАБОТАЕТ ПОВЕРХ TLS. В ВАШЕМ СМАРТФОНЕ ИСПОЛНЯЕТСЯ НЕСКОЛЬКО ПРИЛОЖЕНИЙ-МЕССЕНДЖЕРОВ, ОНИ ТАКЖЕ ИСПОЛЬЗУЮТ TLS ДЛЯ ОРГАНИЗАЦИИ ЗАЩИЩЁННОГО КАНАЛА СВЯЗИ С СЕРВЕРОМ. ЕСЛИ ВЫ ПОЛУЧИЛИ СООБЩЕНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ, ТО, С ОЧЕНЬ БОЛЬШОЙ ВЕРОЯТНОСТЬЮ, ОНО ПРОШЛО СРАЗУ ЧЕРЕЗ НЕСКОЛЬКО СЕРВЕРОВ, КАНАЛЫ ПЕРЕДАЧИ ДАННЫХ МЕЖДУ КОТОРЫМИ ЗАЩИЩЕНЫ TLS.



.TXT

АЛЕКСАНДР ВЕНЕДЮХИН
Ведущий аналитик
АО «Технический Центр Интернет»

TLS ИСПОЛЬЗУЕТСЯ В РАЗЛИЧНЫХ ТЕХНОЛОГИЯХ VPN, ПОЗВОЛЯЮЩИХ СОЗДАВАТЬ ЗАЩИЩЁННЫЕ ТУННЕЛИ ДЛЯ ИНТЕРНЕТ-СОЕДИНЕНИЙ. ИЗ ЭТОГО, КСТАТИ, СЛЕДУЕТ ПОЛЕЗНОЕ НАБЛЮДЕНИЕ: TLS ЗАЩИЩАЕТ НЕ ТОЛЬКО ВЕБ, НО И МНОГИЕ ДРУГИЕ ПРИЛОЖЕНИЯ. TLS — ОСНОВНОЙ БЕЗОПАСНЫЙ ТРАНСПОРТ СОВРЕМЕННОЙ СЕТИ: ЕСЛИ РАНЖИРОВАТЬ ПРОТОКОЛЫ ПО ОБЪЁМУ ПЕРЕДАВАЕМОГО ТРАФИКА, ТО TLS ОКАЖЕТСЯ В САМОЙ ВЕРХУШКЕ РЕЙТИНГА.

ИМЕНА И НАЗВАНИЯ

Знакомство с TLS нередко начинается с путаницы в названиях. Первоначально технология называлась SSL, и была реализована в веб-браузере фирмы Netscape в 1994–1995 годах (Netscape Navigator — один из первых веб-браузеров). До сих пор название SSL можно очень часто услышать, возможно, даже чаще, чем каноническое TLS. В самом общем виде, SSL и TLS, действительно, являются синонимами. Однако в процессе стандартизации технологию переименовали: современное название — TLS (Transport Layer Security), сейчас следует использовать только его как каноническое обозначение, это позволяет избежать возможных разночтений с версиями, так как все современные версии носят название TLS, а все версии SSL устарели, являются небезопасными и не должны использоваться.

Самая современная из стандартизованных в RFC версий TLS — 1.2. Следующая версия протокола находится в разработке, под текущим обозначением TLS1.3. Если использовать в качестве примера веб, то современный веб-сервер должен поддерживать TLS версий 1.1 и 1.2, отдавая предпочтение последней. SSL ни в каких версиях поддерживаться не должен (это касается не только веба; исключение относится лишь к почтовым серверам, которые вынуждены сохранять совместимость со старыми клиентами, и к некоторым встроенным программным продуктам). То же относится и к сертификатам, которые широко известны под именем SSL-сертификаты, но лучше называть их TLS-сертификатами. Да, отличий в сертификатах между TLS и SSL нет никаких, но так как используются они именно для TLS, обозначение «TLS-сертификат» будет гораздо более точным.

ЗАЧЕМ TLS

Предназначение TLS — создать защищённый канал между клиентом и сервером. В случае веба клиентом будет веб-браузер, а сервер — это узел, обслуживающий сайт, с которым устанавливается соединение. TLS позволяет убедиться, что браузер соединяется именно с тем узлом, с которым планировалось. Для идентификации служит доменное имя, адресующее веб-сайт. Процедура установления подлинности идентификатора (имени) и сопоставления ему узла (веб-сервера) называется аутентификацией. Главную роль в этой процедуре играет TLS-сертификат, сопоставляющий доменному имени некоторый криптографический параметр — в подавляющем большинстве случаев это открытый ключ сервера.

Полагать, что TLS целиком предназначен для шифрования, неправильно. Шифрование лишь один из аспектов, который во многих случаях оказывается бесполезен, если не обеспечиваются аутентификация и целостность. Сохранение целостности означает, что клиент (программа, работающая на компьютере пользователя), может убедиться в неизменности полученных данных, в том, что по пути их никто не отредактировал и не подменил. В итоге это даст гарантии, что пользователь видит на экране именно то, что задумал автор сайта. Однако про необходимость обеспечения целостности часто забывают.

Не так важно, содержит ваш сайт какую-то конфиденциальную информацию или только общедоступные тексты (например, описания товаров или услуг). Если данные передаются без защиты, злоумышленики могут подменить их на одном из транзитных узлов, преследуя самые разные цели. Подходящий транзитный узел найдётся практически всегда: так устроена глобальная Сеть — данные здесь передаются через большое количество промежуточных серверов, коммутаторов/маршрутизаторов и прочих вычислительных устройств. Отсутствие защиты целостности приводит к тому, что оператор публичного (открытого) сегмента WiFi с помощью нехитрых операций проводит инъекцию дополнительного программного кода в страницы, которые ваш посетитель загружает с вашего сайта. Этот программный код, в лучшем случае, может показывать какую-то дополнительную рекламу (либо подменять рекламные места, предусмотренные веб-мастером на вашем сайте). А в худшем случае — пользователь может увидеть полностью заменённую страницу (другие товары, другие условия доставки, другие цены), либо окажется перенаправленным на другой сайт с небезопасным сомнительным содержанием. При этом на стороне веб-сервера изменений, произошедших со страницей на лету, никак не будет видно. Получается, что потенциальному клиенту на страницах сайта показывается невесть что, а владелец сайта даже не догадывается об этом.

TLS позволяет решить данную проблему: попытка как-то заменить данные, передаваемые по защищённому каналу, приведёт лишь к тому, что посетитель сайта увидит сообщение об ошибке соединения — никакой нежелательной, «подменной» информации его браузер не отобразит. Иными словами:

вашему сайту может не требоваться шифрование, но обеспечить целостность информации необходимо, только так вы, как владелец или администратор сайта, сможете быть уверены, что ваш посетитель видит именно те страницы, которые вы опубликовали. Очевидно, то же самое относится к сообщениям электронной почты или сообщениям в мессенджерах.

Аутентификация не менее важна: ведь если подлинность сервера не проверяется, то можно подменить сайт целиком, перехватив запрос на уровне DNS или заменив сессию и узел на уровне IP. В таком случае посетителю опять можно показывать любую информацию, вплоть до сайта-конкурента, выступая от имени подлинного узла. Заметьте, что TLS может обеспечивать аутентификацию обеих сторон, устанавливающих соединение: и сервера, и клиента. Клиентская аутентификация сейчас используется крайне редко, но она позволяет усилить различные схемы авторизации: здесь используется такой же (по структуре) TLS-сертификат, как и для сервера, однако он подтверждает подлинность запросов клиента. Например, аутентификация клиента с использованием TLS-сертификата может быть использована для предоставления доступа к закрытым разделам веб-сайта, в дополнение к паролю или вместо пароля.

ТЕХМИНИМУМ

Рассмотрим работу TLS на примере веба — здесь поверх TLS используется протокол HTTPS, а клиентом обычно выступает веб-браузер (слово «обычно» вполне оправдано — нередко в роли клиента оказывается не браузер, а та или иная утилита «скачивания веб-ресурсов» или поисковый робот). Для того чтобы TLS заработал, веб-сервер должен быть настроен соответствующим образом: должна быть включена поддержка данного протокола, установлен TLS-сертификат и соответствующий ему секретный ключ. Секретный ключ сервера входит в пару ключей, открытая часть которой опубликована в составе серверного сертификата. Пара ключей используется обычным образом: секретный ключ позволяет сгенерировать значение электронной подписи, а открытый — эту подпись проверить. TLS-сертификат — это всего лишь «электронный документ» стандартного вида, который не содержит ничего секретного и передаётся в открытом виде. Серверный TLS-сертификат в большинстве случаев нужно подписать в том или ином удостоверяющем центре. Удостоверяющий центр служит третьей стороной, которая подтверждает подлинность узла, удостоверяя своей электронной подписью соответствие между именем и ключом, указанными в сертификате. Браузеры используют встроенный список сертификатов удостоверяющих центров (УЦ), которые позволяют проверить валидность подписи из сертификата, предъявленного сервером. Нужно отличать подписи, которые предоставляет УЦ, от подписей, генерируемых сервером при установлении соединения.

Новое TLS-соединение устанавливается в несколько этапов, по довольно сложной схеме. Впрочем, основные принципы можно описать в нескольких словах. Получив серверный TLS-сертификат, браузер проверяет его валидность (то есть устанавливает подлинность подписей, сверяет время действия сертификата). Ключевых моментов в такой проверке два: во-первых, сертификат должен содержать действующую подпись удостоверяющего центра, который входит в список доверенных узлов браузера; во-вторых, должны совпадать сетевые имена (доменные имена), а указанное в сертификате имя — с именем узла, с которым устанавливается соединение.

Если аутентификация сервера прошла успешно, то браузер может договориться с сервером о так называемом сессионном симметричном ключе шифрования. Этот ключ необходим по той причине, что для шифрования передаваемых данных используется быстрый симметричный шифр. Симметричный шифр подразумевает, что клиент и сервер используют одинаковый (симметричный) набор ключей, каждый из которых является секретным. Не следует путать эту схему с асимметричными криптосистемами, где используется пара связанных ключей, состоящая из секретной и открытой части. Асимметричные криптосистемы не подходят для шифрования потоков данных по многим причинам, и в TLS они сейчас используются для генерирования и проверки электронных подписей.

Стороны, устанавливающие TLS-соединение, вырабатывают общий секретный ключ согласно схеме Диффи-Хеллмана, которая позволяет договориться об общем секрете через открытый канал связи, не раскрывая секрета. Ключ из сертификата используется для того, чтобы сервер мог удостоверить с помощью электронной

подписи переданные в сторону клиента параметры Диффи-Хеллмана, а клиент — проверить эту подпись (это и есть основное отличие использования подписей УЦ и сервером). Если бы параметры не удостоверялись подобным образом, то соединение оказалось бы подверженным атаке типа «человек посередине» (атака посредника), в которой перехватывающий узел вмешивается в протокол Диффи-Хеллмана и подменяет параметры на собственные, выдавая себя каждой из сторон за другую.

Всё это, тем не менее, может показаться сложным. К счастью, для получения самого общего понимания работы TLS в рамках шифрования так же достаточно уяснить всего два момента: во-первых, данные шифруются симметричным шифром, он работает быстро, но использует только секретные ключи, которые должны быть известны обеим сторонам; во-вторых, ключ из сертификата сервера ничего не шифрует, а служит для проверки электронной подписи, которая подтверждает, что о симметричном ключе клиент договорился именно с тем сервером, с которым планировал. Интересно, что существует историческая схема установления соединения TLS, в которой общий секрет не генерируется по протоколу Диффи-Хеллмана, а действительно шифруется при помощи открытого ключа криптосистемы RSA, после чего передаётся клиентом в сторону сервера. Такую схему до сих пор используют некоторые узлы, в том числе интерфейсы интернет-банков, но, согласно современным представлениям, данная схема не обладает требуемой стойкостью.

Помимо согласования параметров симметричного шифрования, узлы договариваются о некоторых других криптографических параметрах соединения. В частности, о настройках алгоритма вычисления/проверки кода аутентификации сообщения (имитовставки). Именно код аутентификации позволяет проверять целостность передаваемых данных.

В теории, можно создать TLS-соединение, которое будет передавать данные в открытом виде, но защищая их от изменения — то есть канал будет обеспечивать только целостность и аутентификацию. Более того, можно отказаться и от аутентификации узлов, создав соединение в так называемом «анонимном» режиме. Однако такие режимы практически не используются: выбранное наугад современное TLS-соединение скорее всего окажется зашифрованным.

ПОЛОЖЕНИЕ ДЕЛ

По состоянию на апрель 2017 года в домене .RU — а это флагманский домен Рунета — насчитывалось чуть более 300 тыс. узлов, корректно поддерживающих TLS для HTTPS (данные проекта statdom.ru). Многие из них — это веб-узлы с большим трафиком. Поэтому если считать по объёмам пользовательских запросов, то можно сказать, что основная часть веб-трафика в Рунете уже зашифрована и защищена TLS. При этом проникновение технологии растёт очень быстро: в апреле 2016 года защищённых узлов было всего лишь 87 тыс.

Браузеры активно продвигают защищённый протокол. Так, Google Chrome уже помечает как небезопасные страницы, передаваемые по протоколу HTTP, если на них присутствуют формы для ввода паролей или данных банковских карт. Это одна из новых и довольно распространённых проблем: многие веб-мастеры удивляются, почему браузер стал отмечать их страницы как небезопасные — причина же обычно в том, что на странице находится форма ввода логина в «личный кабинет» или в «список покупок», которая содержит поле ввода с атрибутом password.

Ожидается, что в ближайшее время (год-два) принципы маркирования протоколов веба браузерами ещё ужесточат: открытый протокол HTTP будет во всех случаях отмечаться специальным значком как небезопасный. То есть, HTTPS (и, соответственно, TLS) станет необходимым протоколом по умолчанию, а ситуация окажется обратной к сложившейся сейчас, когда HTTPS отмечается как безопасный, а HTTP пока считается нейтральным. В других, отличных от веба, применениях, поддержка TLS уже стала строгим требованием: приложения просто отказываются работать, если не удаётся установить защищённое и аутентифицированное TLS-соединение с сервером.

Ситуация в глобальной Сети стремительно движется в сторону усиления защиты информации. В самом ближайшем будущем основная часть передаваемого между клиентами и серверами трафика окажется зашифрована и защищена от подмены, а TLS послужит фундаментом для этого радикального инфраструктурного изменения.

ПОЛЕЗНЫЙ ИНТЕРНЕТ

.TXT
ВИКТОРИЯ БУНЧУК
Координационный центр доменов .RU/.РФ

ИНТЕРНЕТ — ВЕЩЬ МНОГОГРАННАЯ. ОН СТАЛ НЕ ТОЛЬКО ЧАСТЬЮ ЧЕЛОВЕЧЕСКОГО ДОСУГА, НО ТАКЖЕ ПЛАТФОРМОЙ ДЛЯ ОБЩЕНИЯ И ОБМЕНА МНЕНИЯМИ, УДОБНЫМ И ДОСТУПНЫМ ИНСТРУМЕНТОМ ДЛЯ РАБОТЫ И ОБРАЗОВАНИЯ. ОДНАКО, КАК В КАЖДОЙ СКАЗКЕ ЕСТЬ ЗЛОДЕЙ, КОТОРЫЙ ПОРТИТ ЖИЗНЬ ПОЛОЖИТЕЛЬНЫМ ПЕРСОНАЖАМ, ТАК И В ИНТЕРНЕТ-ПРОСТРАНСТВЕ, КРОМЕ БОЛЬШИХ ВОЗМОЖНОСТЕЙ, ПОДЖИДАЮТ РАЗНОГО РОДА ОПАСНОСТИ. ТЕ, ЧТО ПОМЕЛЬЧЕ — НАНОСЯТ ВРЕД «ЖЕЛЕЗУ», ПОКРУПНЕЕ — КРАДУТ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ТРОЛЛЯТ И ДАЖЕ ЗАСТАВЛЯЮТ СОВЕРШАТЬ НЕПОПРАВИМОЕ.

Самое интересное, что с большинством из этих проблем можно и вовсе не столкнуться, приняв превентивные меры. Но среднестатистический российский пользователь продолжает надеяться на авось, начинающий — кидается в омут с головой, просто не задумываясь о возможных последствиях, а родители этого начинающего пользователя с технологиями скорее на «вы», поэтому не всегда могут предостеречь. Так, по данным исследований, индекс цифровой грамотности взрослых пользователей Рунета оценивается в 5,42 пт. из 10, компетентность детей — как треть от максимально возможного. При этом и у детей, и у родителей наблюдается низкая мотивация к «прокачке» собственных навыков.

Как встряхнуть пользователя, донести до него, что интернет — объект повышенной опасности, однако будет хорошим другом, если соблюдать элементарные правила общения? Ответ — запустить пару онлайн-проектов, которые научат играючи.

Один из таких — **«Изучи интернет — управляй им!» (http://игра-интернет.рф/)**. Это совместный проект Координационного центра национальных доменов .RU/.РФ и ПАО «Ростелеком», созданный в 2012 году специально для школьников, да и вообще всех начинающих пользователей Рунета (ведь сегодня в сеть активно входят и люди возраста 65+ — чем не начинающий юзер?).

Проект объединяет:

- *портал*, где в интерактивной форме (игры, задачки, пазлы, мультимедиавопросы) представлена информация об устройстве интернета, его составных «элементах», иерархии, истории, работе главных IT-сервисов, а также о сетевой безопасности и персональных данных;
- *мобильное приложение*, с помощью которого можно «отрабатывать» полученные на портале знания в любое удобное время;
- *Всероссийский онлайн-чемпионат среди школьных команд*, в рамках которого участники проекта демонстрируют свои ИТ-знания. Кстати, в 2016 году все вопросы и задания Чемпионата были посвящены теме безопасности в интернете — защите от сетевых угроз, конфиденциальности данных, безопасности в социальных сетях и работе антивирусов.

Еще один проект, связанный с киберликбезом начинающих пользователей и запущенный при активной поддержке Координационного центра, — **персональныеданные.дети**. Идеологом и главным разработчиком, как несложно догадаться, стала Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Это интерактивный портал, который, опять же языком игр, «бродилок» и раскрасок, раскрывает понятие персональных данных, учит, в первую очередь детей, безопасному использованию личных данных в интернете и соблюдению конфиденциальности своей жизни при использовании цифровых технологий.

Кстати, о домене **.ДЕТИ**. Это воплощенная в жизнь идея о создании обособленного сегмента интернета для юных пользователей сети, свободного от всяческих интернет-угроз: технических, коммуникационных, контентных. Реализацией проекта на стадии запуска в 2014 году и активной ресурсной поддержкой сегодня занимается Координационный центр.

Кириллический домен .ДЕТИ создан для адресации сайтов о детях и для детей, а также ресурсов, адаптированных под подростковые интересы, их особенности восприятия информации. Таким образом, миссия домена .ДЕТИ

заключается в создании интернет-пространства доверия, повышении цифровой грамотности детей и подростков, а также в объединении качественного интернет-контента на одной площадке.

Другая важная задача .ДЕТИ — сделать пребывание детей в интернете комфортным и безопасным. Противодействие «зловредам» и уязвимостям на сайтах, работающих в домене, осуществляется с помощью программного комплекса мониторинга вредоносной активности и нежелательного контента, которая работает круглосуточно 365 дней в году. С помощью этой системы, развернутой на всю доменную зону (что само по себе уникально, подобной практики в других доменах просто нет), оператор реестра оперативно устраняет всю зловредную активность в зоне и негативный контент с детских сайтов. Работа программного комплекса проверяется и обеспечивается живыми людьми — специалистами собственной службы реагирования.

Эта «фишка» домена .ДЕТИ стала особенно актуальной сегодня, когда исследования говорят о 95% детей (то есть людей в возрасте до 14 лет) в интернете, треть из которых проводят в сети до 8 часов в день, причем бесконтрольно!

Кроме персональныеданные.дети, в зоне работают сотни полезных и безопасных ресурсов, которые тем или иным образом приобщают детей к миру информационных технологий. Например, библиотека.дети — здесь расположился сайт Российской государственной детской библиотеки (РГДБ); карусель.дети — сайт одноименного федерального канала, ориентированного на детей 3–14 лет; профессии.дети — мультимедийный онлайн-сервис для профориентации детей и подростков; математика-просто.дети — информационный сайт, который помогает школьникам разных возрастов найти решение задач по алгебре и геометрии; где.дети — мобильное приложение, которое поможет родителям быть в курсе местоположения и действий их ребенка; и множество других. Каталог ресурсов в .ДЕТИ доступен на сайте **http://интернет.дети/**.

Для поддержки подобных ресурсов, созданных не только в .ДЕТИ, но и в любом другом доменном пространстве России, Координационный центр совместно с Фондом Развития Интернет, РАЭК и РОЦИТ с 2009 года проводит **конкурс интернет-проектов, ориентированных на детей, подростков и молодежь,— «Позитивный контент» (www.positivecontent.ru)**. Это один из самых известных и престижных конкурсов Рунета, **главные задачи** которого — способствовать наполнению российского сегмента сети Интернет качественными познавательными, образовательными, информационными и развлекательными digital-продуктами, отвечающими современным требованиям информационной безопасности; а также содействовать повышению уровня цифровой грамотности населения России через популяризацию качественных интернет-проектов с позитивным контентом.

***

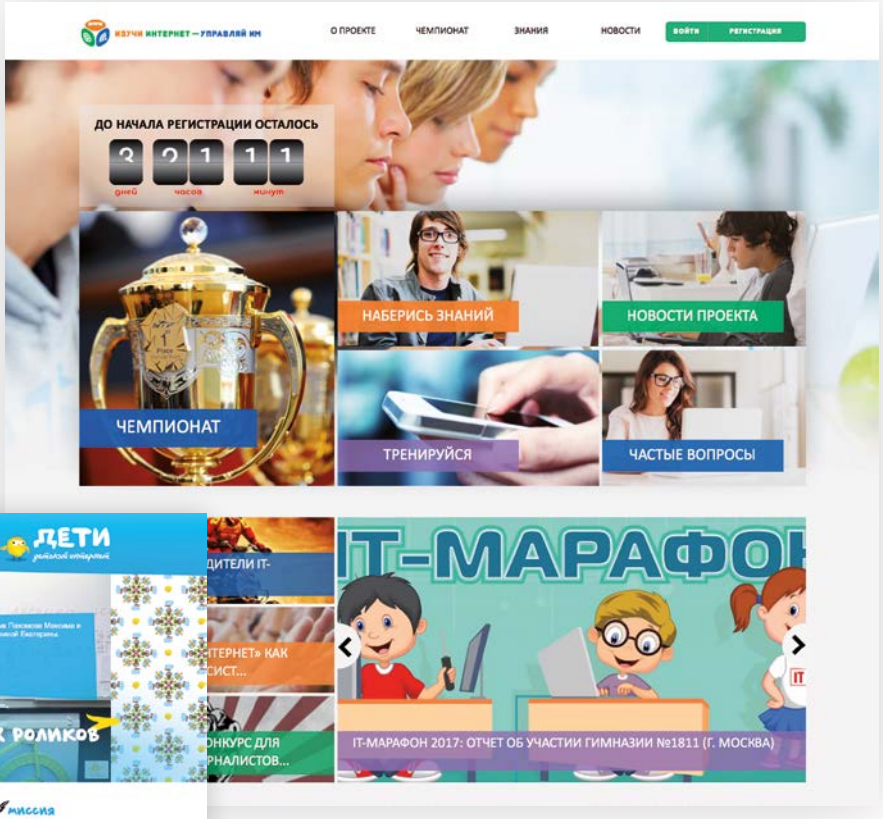
Стоит отметить, что попутно с решением проблемы цифровой грамотности, перечисленные проекты стараются воспитать в детях интерес к информационным технологиям в целом, а также пробудить в них желание осваивать ИТ-инструменты дальше, все глубже вникая в тему, постепенно вырастая в настоящего айтишника. Это тоже важно. Ведь не секрет, что на отечественном рынке труда наблюдается дефицит квалифицированных IT-кадров, и голод только растет: на последнем форуме РИФ+КИБ 2017 было озвучено, что спрос на специалистов в сфере информационных технологий всего за год вырос на 70%! И уже сейчас совершенно очевидно, что развитие технологий, их применимость в ранее нетипичных направлениях (тот самый Интернет вещей), а также автоматизация процессов сохранят IT-специалистов как одних из самых востребованных на рынке труда.

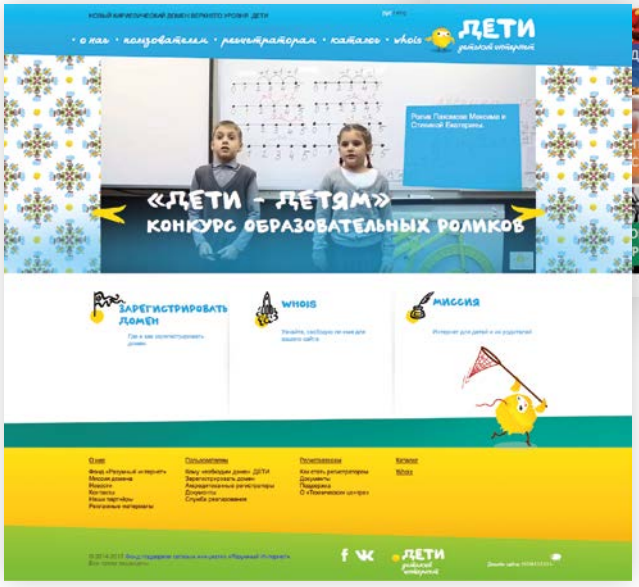
Так, к работе над проектом **«Изучи интернет — управляй им!»** привлекаются ученики старших классов, участвующие в программе Департамента образования города Москвы «Школа реальных дел»: они разрабатывают новые темы и сценарии познавательных игр для портала проекта, а также вопросы для мобильного приложения; в последнем случае школьники могут побывать и в роли программистов, выполнив ряд элементарных действий по наполнению шаблона приложения контентом.

Другой проект Координационного центра, который воспитывает в детях интерес ко всему, что внутри и вокруг интернета — **«DOT-журналистика. Юнкоры» (http://дот-журналистика.рф/)**. Это конкурс для начинающих журналистов, которые хотят и любят писать об интернет-технологиях. В рамках проекта проводятся творческие встречи в школьных пресс-центрах, где, кроме всего прочего, обсуждается роль журналистов в освещении событий, связанных с IT-индустрией.

И еще один проект Координационного центра, направленный на будущих айтишников с гуманитарным уклоном — **молодежный конкурс работ по праву информационных технологий и интеллектуальной собственности «IP&IT LAW»**. Конкурс проводится совместно с Московским государственным юридическим университетом им. О. Е. Кутафина (МГЮА) и организацией IP CLUB. К участию в нем приглашаются абитуриенты, студенты вузов, аспиранты и молодые специалисты из России и других стран, имеющие необходимые знания в области права. На конкурс необходимо представить актуальное и ранее не публиковавшееся исследование, в котором с опорой на законодательство, доктрину, отечественную и зарубежную судебную практику рассматриваются проблемные правовые вопросы, а также даются новые варианты их решения.

Кроме этих, масштабных, проектов, которые успешно работают в течение многих лет, Координационный центр предпринимает и «одиночные вылазки». Так, организация участвует в Едином уроке безопасного интернета, проводит лекции по безопасности и истории интернета, выпускает методические пособия и просветительские брошюры.

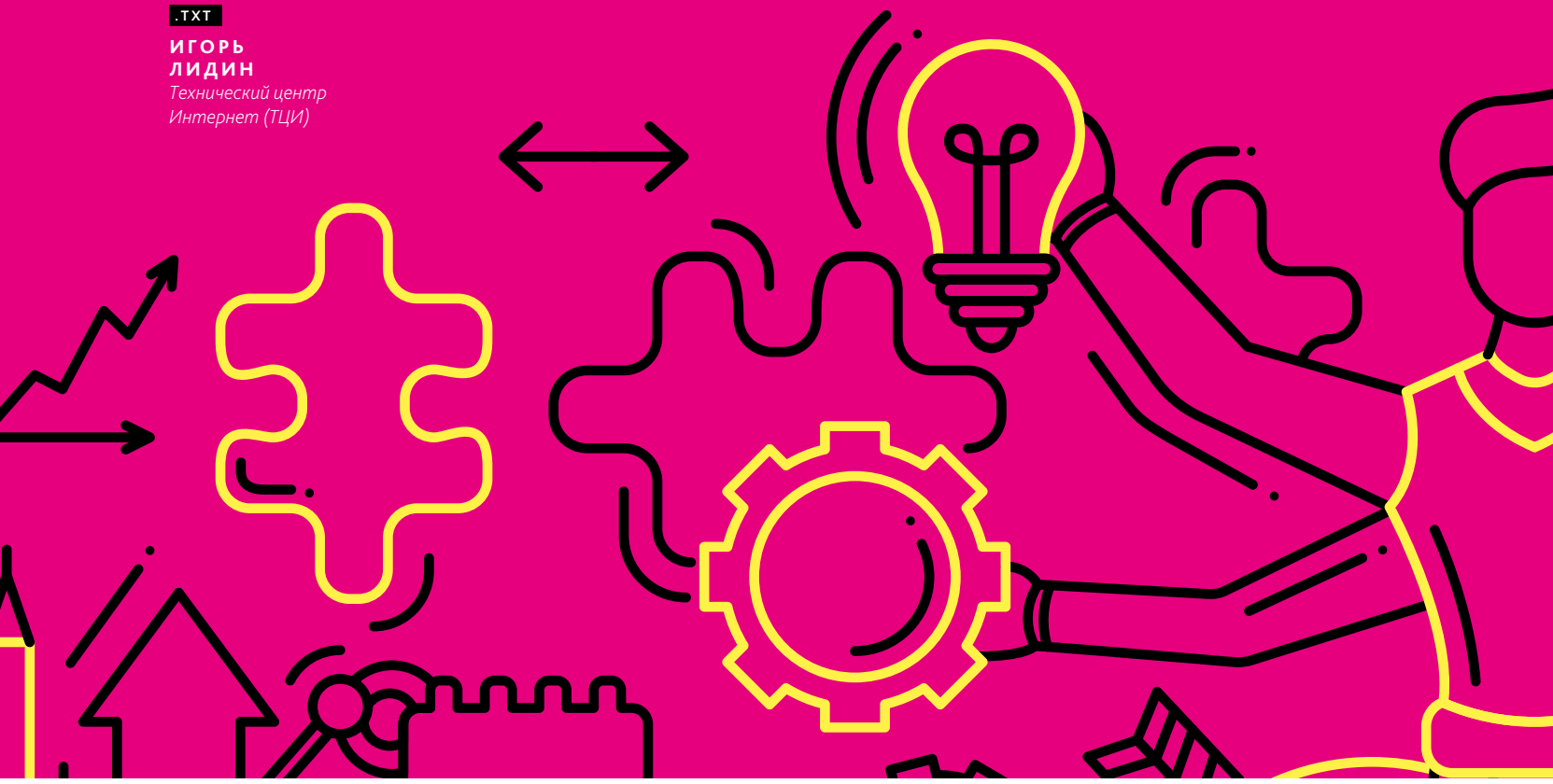




DNS ВОКРУГ НАС

.TXT

ИГОРЬ ЛИДИН
Технический центр Интернет (ТЦИ)



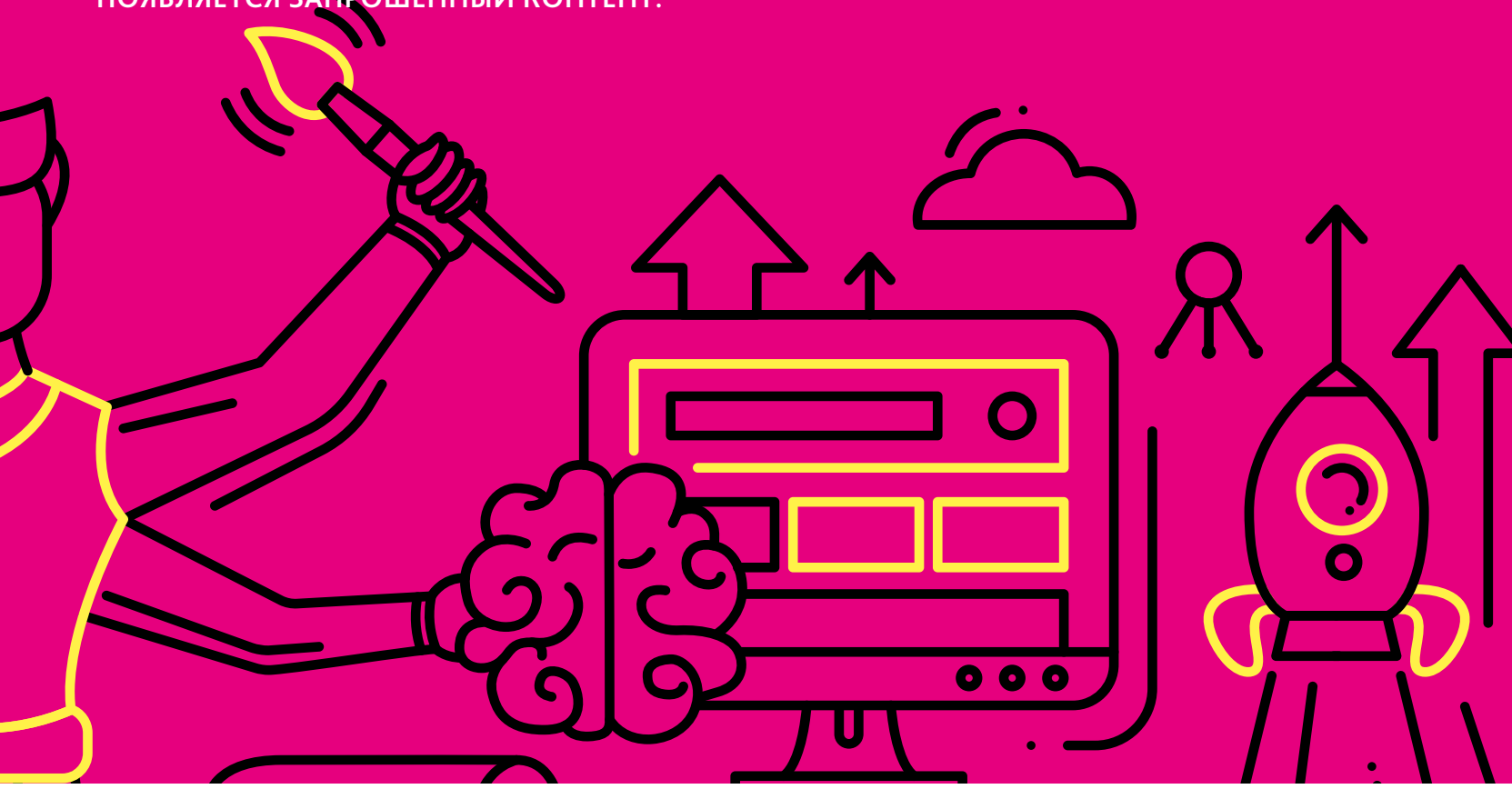
Мало кто задумывается в этот момент, что там происходит в деталях, как система находит нужные серверы, как решает, откуда взять какие картинки или строчки текста. Однако все знают, что у сайта есть адрес, его надо задать — вбить в браузер, «достать» из закладок, перейти по ссылке. Если адрес правильный — мы получим нужный ресурс.

Символьные имена узлов в интернете, или доменные имена, придумали в далеком 1983 году, и с тех пор система DNS, которая и обеспечивает их существование, неразлучна с сетью, какой мы ее знаем сегодня. Процесс преобразования символьных доменных имен в цифровые IP-адреса, которые «понятны» компьютерам — «разрешение имен» через DNS — происходит множество раз на каждом подключенном к сети устройстве незаметно для его владельца, избавляя его от необходимости что-либо знать о низкоуровневых особенностях адресации узлов в интернете.

Чтобы система DNS работала, поддерживается сложная распределенная инфраструктура, «размазанная» по всей сети, включающая в себя сотни тысяч специальных серверов, сотни управляющих и координирующих организаций, таких как координатор мирового уровня ICANN, держатели реестров доменов первого уровня, регистраторы доменов и так далее.

Наличие уровня абстракции в виде доменных имен позволяет администраторам ресурсов интернета гибко управлять своей инфраструктурой без негативного влияния на пользователей — перемещать и заменять серверные мощности, балансировать нагрузку. Отредактировали информацию в базе данных DNS — и вот уже сайт открывается из центра обработки данных в Германии, хотя еще вчера его сервер был расположен в Москве. Пользователям, обращающимся к ресурсу по символьному имени,

ЛЮБОЙ ПОЛЬЗОВАТЕЛЬ ИНТЕРНЕТА, ОТКРЫВАЯ УТРОМ В БРАУЗЕРЕ ЗАКЛАДКУ С ЛЮБИМЫМ САЙТОМ НОВОСТЕЙ ИЛИ СОЦИАЛЬНОЙ СЕТЬЮ, ЗАПУСКАЕТ СЛОЖНЫЙ, СОСТОЯЩИЙ ИЗ МНОЖЕСТВА ЭТАПОВ ТЕХНИЧЕСКИЙ ПРОЦЕСС. ИНТЕРНЕТ РАБОТАЕТ, ШЕСТЕРЕНКИ ВЕРТЯТСЯ. В ОКНЕ БРАУЗЕРА В РЕЗУЛЬТАТЕ ПОЯВЛЯЕТСЯ ЗАПРОШЕННЫЙ КОНТЕНТ.



можно предоставлять обслуживание с наиболее близких к ним серверов, что широко используется в системах доставки и дистрибуции содержимого (CDN).

Понятно, что, когда открывается сайт, его символьное имя с помощью обращения к распределенной базе данных на серверах DNS по всему миру преобразуется в цифровой IP-адрес, указатель на нужный сервер в интернете, и дальше к нему происходит обращение через сеть. Это наиболее очевидное для большинства интернет-пользователей применение DNS. Но далеко не единственное.

Во-первых, содержимое современного сайта, как правило, состоит из множества различных компонентов. Картинки, аудио- и видеоролики, загружаемые шрифты, кусочки выполняемого кода («скрипты») могут собираться в одно целое из разных мест. У каждого места — свой адрес. В каждом адресе — свое доменное имя. Чтобы собрать содержимое сайта, иногда надо сделать сотню DNS-запросов.

Во-вторых, интернет — это не только сайты. Каждый раз, отправляя сообщение электронной почты, мы ожидаем, что оно будет доставлено по указанному адресу. Адрес email состоит из двух частей — уникальной.левой@и.доменной.правой. Чтобы выяснить, на какой сервер передать сообщение, почтовый сервер делает специальный запрос в DNS, запрашивая имя почтового сервера получателя по доменной части адреса email — MX-запись.

Анализируя полученный email на предмет спама, почтовый сервер получателя письма снова сделает несколько запросов в DNS, выясняя, имеет ли исходный узел право отправлять сообщения с данного адреса. Для этого используется технология SPF, которая подразумевает публикацию в DNS

специальных записей, содержащих закодированные политики, определяющие соответствующие разрешения.

Возможно, в сообщении также будет проверена автоматическая электронная подпись DKIM — это технология, позволяющая подтвердить принадлежность отправителя к домену в интернете. Ключ для проверки электронной подписи будет взят, опять же, из DNS, где для него предусмотрен специальный формат хранения.

Приложения для смартфонов или планшетов, реализующие какие-либо интернет-сервисы, мессенджеры или социальные сети, на первый взгляд, не требуют ввода никаких адресов — все просто открывается и работает. Но «под капотом» все равно то же самое — чтобы добраться до своих данных в «облаке», используются символьные доменные имена. Трудно «зашить» в приложение непосредственно IP-адрес сервера — любое изменение в инфраструктуре, затрагивающее адреса, приведёт к тому, что все перестанет работать.

Множество обращений к DNS происходит, даже если мы оставим устройство в покое. Операционные системы выполняют целый ряд действий в фоновом режиме: получение push-сообщений, синхронизация времени с серверами NTP, проверка наличия обновлений для системы или магазина приложений. В той или иной форме все эти действия подразумевают использование сервиса DNS.

Именно символьные имена являются идентификаторами узлов в TLS-сертификатах — элементах одной из важнейших технологий обеспечения безопасности коммуникаций в интернете. Каждое установление соединения по защищенным протоколам HTTPS или IMAPS может вызвать ряд обращений к DNS как со стороны инициатора подключения, так и со стороны сервера. База данных DNS может

также использоваться для публикации разрешений и запретов на выпуск TLS-сертификатов для данного домена в рамках технологии Certificate Authority Authorization (CAA): при выпуске сертификата удостоверяющий центр может справляться о наличии соответствующих закодированных в DNS инструкций.

В классической DNS данные в распределенной системе не защищены от подмены или сокрытия путем манипуляций над ними в канале между пользователем и серверами DNS. Для защиты разработана технология DNSSEC, которая с помощью криптографии и иерархии электронных подписей обеспечивает неизменность опубликованных в DNS данных.

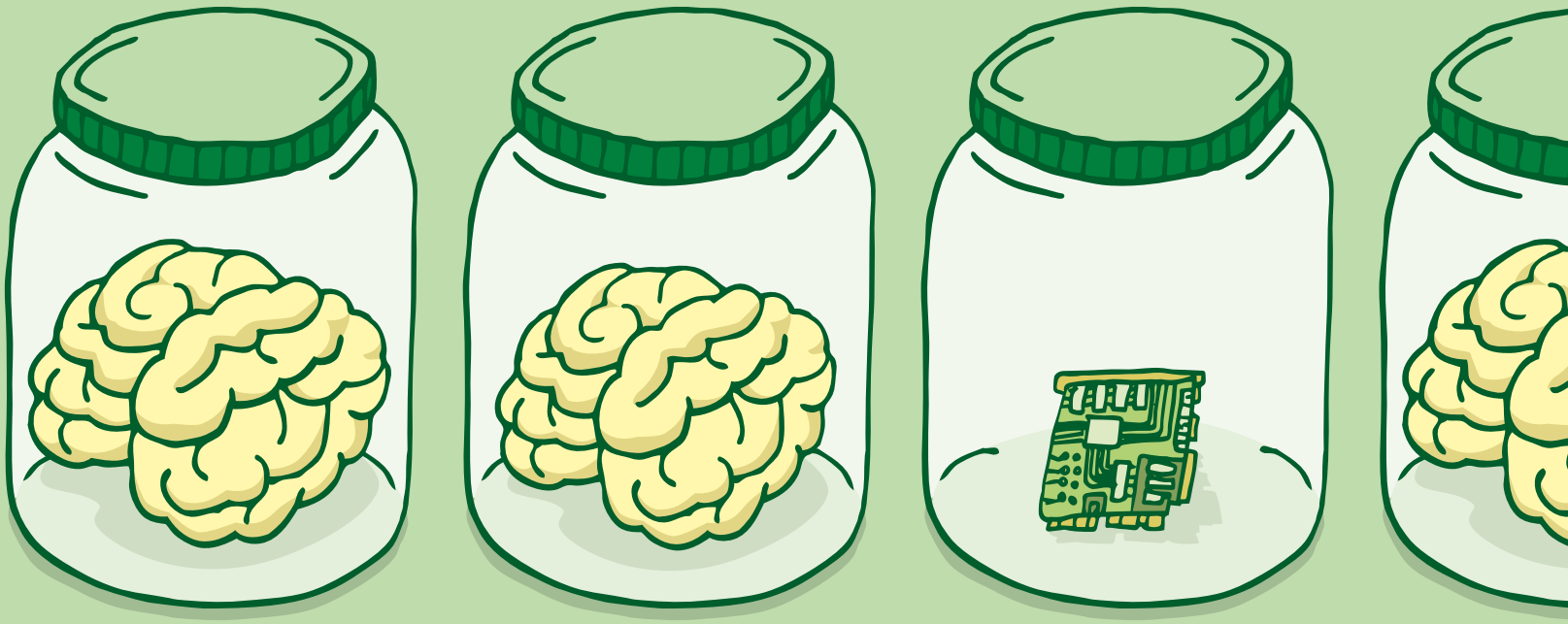
Таким образом, обращениями к данным DNS сопровождается почти любое действие пользователя в интернете или даже просто фоновая активность подключенного к сети устройства.

Анализируя обращения к DNS, например, на стороне провайдера, можно получить много информации о поведении пользователя в сети. Помимо возможности наблюдения, такая информация в больших масштабах представляет серьезный коммерческий интерес. Для противодействия утечке этих данных существует, например, пока еще экзотическая технология DNSCrypt, позволяющая скрыть их с помощью шифрования канала между системой пользователя и доверенным DNS-сервером.

Большинство пользователей замечает существование DNS только тогда, когда что-нибудь идет не так и перестает работать. Однако DNS — неотъемлемая часть интернета, без которой глобальная Сеть перестала бы быть доступной и удобной средой.

КАК ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ МЕНЯЕТ ЛИЦО ОНЛАЙН-РЕКЛАМЫ

.TXT
АНТОН МЕЛЕХОВ
RTB House



ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ (ИИ) НАВСЕГДА ИЗМЕНИЛ МИР ЦИФРОВОЙ РЕКЛАМЫ. КАК МАРКЕТОЛОГ, ИИ ПРЕДОСТАВЛЯЕТ НАМ НЕДОСТУПНОЕ РАНЕЕ РЕШЕНИЕ С ЛУЧШИМИ ВАРИАНТАМИ ПРИВЛЕЧЕНИЯ ПОТЕНЦИАЛЬНЫХ ПОКУПАТЕЛЕЙ И РЫНКОВ СБЫТА. НО ВСЕ ЖЕ НАМ ЕСТЬ КУДА СТРЕМИТЬСЯ. ИНСТРУМЕНТЫ ГЛУБОКОГО ОБУЧЕНИЯ — ЭТО СЛЕДУЮЩАЯ ВАЖНАЯ СФЕРА ИССЛЕДОВАНИЙ В ОБЛАСТИ ИИ, ЧТО ДАЕТ НАМ ПОСЫЛ К БУДУЩИМ ИННОВАЦИЯМ В КАЖДОЙ ОТРАСЛИ ЭКОНОМИКИ, НАЧИНАЯ НОВУЮ ЭПОХУ МАРКЕТИНГА КАК ДЛЯ РЕКЛАМОДАТЕЛЕЙ, ТАК И ДЛЯ КОНЕЧНЫХ ПОТРЕБИТЕЛЕЙ.

Современные интерфейсы уже адаптированы под интересы пользователя на индивидуальном уровне в соответствии трендам, поведению и другим параметрам в виде дисплейной рекламы либо персонализированной. Но применение алгоритмов глубокого обучения может достичь большего.

Глубокое обучение меняет само наше представление об эффективности. DeepMInd от Google читает речь в видео по губам лучше профессионала (опытный переводчик может транслировать только 12,4% слов без ошибок, в то время как ИИ — все 46,8%). ИИ даже способен создать фильм — как показанный совсем недавно агентством Saatchi & Saatchi на фестивале «Каннские Львы».

Безусловно, рекламная отрасль будет продолжать использовать методы глубокого обучения. Последнее заявление Coca-Cola о планах компании использовать ботов ИИ в создании музыки для рекламных роликов, написания текстов, постов в социальных сетях и даже покупки медиа — дает нам понять, что революция в рекламе с участием глубокого обучения становится ближе, чем мы ожидали.

ВЗГЛЯД РЕКЛАМОДАТЕЛЯ: САМООБУЧАЮЩИЕСЯ АЛГОРИТМЫ РАЗУМНО РЕАГИРУЮТ НА НЕШТАТНЫЕ СИТУАЦИИ

По сведениям от Adlucent, потребители жаждут персонализированных рекламных сообщений, а 71% респондентов предпочитают рекламу, ориентированную на их интересы и покупательские привычки. Исследование также показало, что люди почти в два раза чаще переходят по объявлению с неизвестным брендом, если объявление было адаптировано к их предпочтениям.

С ростом доступа к данным и стремительной конкуренцией, маркетологам сейчас крайне важно разобраться в массе окружающих пользователей, но это очень нелегко сделать. Типичная модель персонализации может быть реализована и без сверхпродвинутых алгоритмов, но мы знаем, что предел здесь уже достигнут. Новые алгоритмы глубокого обучения могут обнаруживать неожиданные ситуации и скрытый в них потенциал.

Представьте, что вы забыли день рождения своего друга. Осталось всего два дня, и у вас нет времени в запасе, чтобы искать товар, но вместе с тем его достаточно для того, чтобы присмотреть нечто интересное. В таком случае высокоточная персонализация проявит себя, и модель глубокого обучения поймет, что вы с энтузиазмом что-то ищете. Независимо от того, происходит ли внезапное изменение в поведении или кажущаяся срочной вечеринка, типичная модель не заметит этих пунктов в данных, но глубокое обучение сможет их связать.

Широкое понимание покупательского поведения потребителей еще не стало таким доступным для игроков рынка электронной коммерции, но этот факт является критичным для маркетологов. Например, довольно легко найти закономерности в принятии решений для типичных, известных пиков продаж, таких как «Черная Пятница» или «Международный Женский День». Однако, довольно сложно определить действия, когда дело доходит до идентификации отдельных событий с очень конкретным контекстом (например, день рождения близкого друга или внезапное событие).

Именно здесь глубокое обучение берет верх над традиционными методами. Действуя по примеру биологических нейронов в нашем мозге, глубокое обучение вступает в игру, позволяя получить более надежные и полные машинные интерпретации описания пользователей и покупательского потенциала клиента без каких-либо вмешательств человека.

В отличие от традиционного подхода в машинном обучении, глубокое обучение способно найти одного пользователя в онлайн-аудитории — человека, который изначально выглядел как хаотически

действующий пользователь, но на самом деле обладает наибольшим потенциалом для завершения покупки.

Это становится возможным благодаря самообучающимся алгоритмам, которые определяют каждого потенциального клиента, ищущего продукт, и отличающегося в этом от других пользователей. Алгоритмы обращаются к истории и видят, что человек динамично менял свое поведение. Затем они обеспечивают чрезвычайно точную вероятность конверсии, получая данные не только именно от этого пользователя, но и от других пользователей в сети.

Например, если подарком на день рождения должны стать новые наушники, то ретаргетинг на основе глубокого обучения позволил бы пользователю быстро найти еще 10 различных моделей, проверить спецификации, сузить диапазон цен. Глубокое обучение определит ситуацию как необычную и срочную, в то время как традиционные алгоритмы квалифицируют ее как нерешительное и неустойчивое поведение или не видят совсем. Зная, что человеку срочно нужно что-то купить, электронный магазин может автоматически подтолкнуть пользователя к завершению покупки в своем магазине.

ВЗГЛЯД ПОТРЕБИТЕЛЯ: АЛГОРИТМЫ ГЛУБОКОГО ОБУЧЕНИЯ ПРЕДУГАДЫВАЮТ МОИ ЖЕЛАНИЯ

Когда ИИ применяется к любому коммерческому продукту или распределению услуг, он становится уникальным расширением наших знаний о себе. Это феноменально работает на примере системы рекомендаций Netflix. Многие фильмы, просмотренные на Netflix, исходят от пожеланий алгоритмов глубокого обучения, которыми пользуется компания. Amazon также доверяет самообучающимся алгоритмам. Запатентованная компанией система «опережающей доставки» (anticipatory shipping), основанная на алгоритмах, может очень точно определять шаблоны в покупательском поведении посетителей сайта и прогнозировать марку, ценовой диапазон и товар, который будет покупаться. Исходя из этого, предложения могут направлены в центры распределения товаров еще до того, как заказ размещен, что по сути является революцией в электронной коммерции.

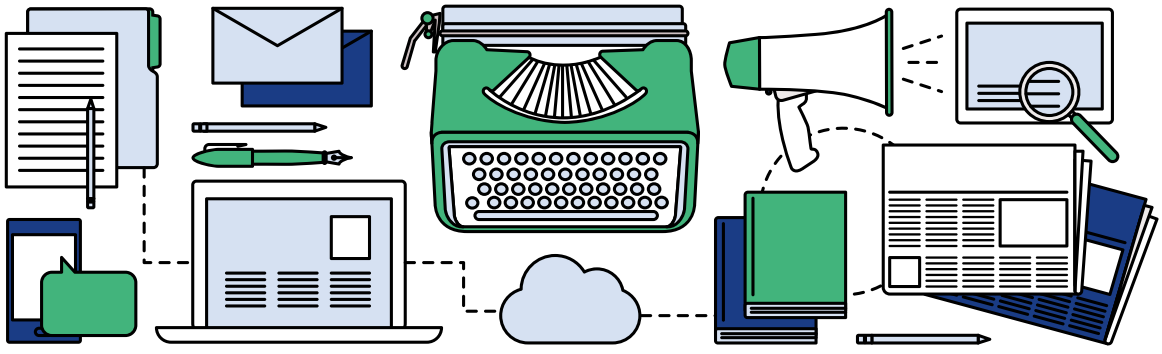
ИИ, а особенно глубокое обучение, являются идеальными инструментами для прогнозирования желаний пользователя в рекламной отрасли. Эта технология упрощает повседневную рутинную работу пользователей над поиском, предоставляя четко таргетированные объявления, которые содержат не только товары, которые мы с большей вероятностью покупаем, но и те, которых мы не видели, или товары, о которых мы даже не задумывались.

Представьте, что вы только что купили новую камеру. Алгоритмы глубокого обучения будут анализировать каждую часть того, что вы делали: дата выбора и покупки, характеристики камеры, история, поведение и так далее. Алгоритмы смогут изучать рекомендации товара в соответствии с вашими личными потребностями, выходящими за рамки обычных предложений. Совместимые объективы или дополнительные карты памяти, штатив камеры могут быть хорошими рекомендациями, в то время как предлагаемое видеообъявление с камерой-дроном может показать вам то, о чем вы даже не думали, а теперь хотите подсознательно.

Суть глубокого изучения впечатляющая — процесс обучения проходит так же, как и у людей, только много, много быстрее. Глубокое обучение рассматривает пожелания каждого человека по принципу «один на один», а также учитывает данные от миллионов других пользователей и выдает результаты в режиме реального времени. Это выдающиеся навыки, которыми человек никогда не сможет овладеть.

Инструменты глубокого обучения приведут рекламодателей к изменениям в способах выдачи рекомендаций товаров, тщательно соизмеряя ценность потенциального покупателя, прогнозируя вероятность конверсии, а самое главное — предугадывая свои желания. По мнению RTB House, международной компании, предоставляющей современную технологию ретаргетинга, самообучающиеся алгоритмы помогают добиться сверхточного анализа пользователей и, как следствие, делают рекламу на 40% более эффективной.

В ближайшем будущем рекламодатели и пользователи будут наблюдать эволюцию в рекламе. Хотя сперва это кажется фантастикой, но на самом деле это естественный прогресс в сторону совершения более эффективных онлайн-операций, чем когда-либо прежде.



ДОТ

конкурс для начинающих журналистов, которые хотят и любят писать об интернете

ЖУРНАЛИСТИКА
ЮНКОРЫ

УЧАСТНИКИ:

ЮНЫЕ КОРРЕСПОНДЕНТЫ ДО 18 ЛЕТ

НА КОНКУРС ПРИНИМАЮТСЯ:

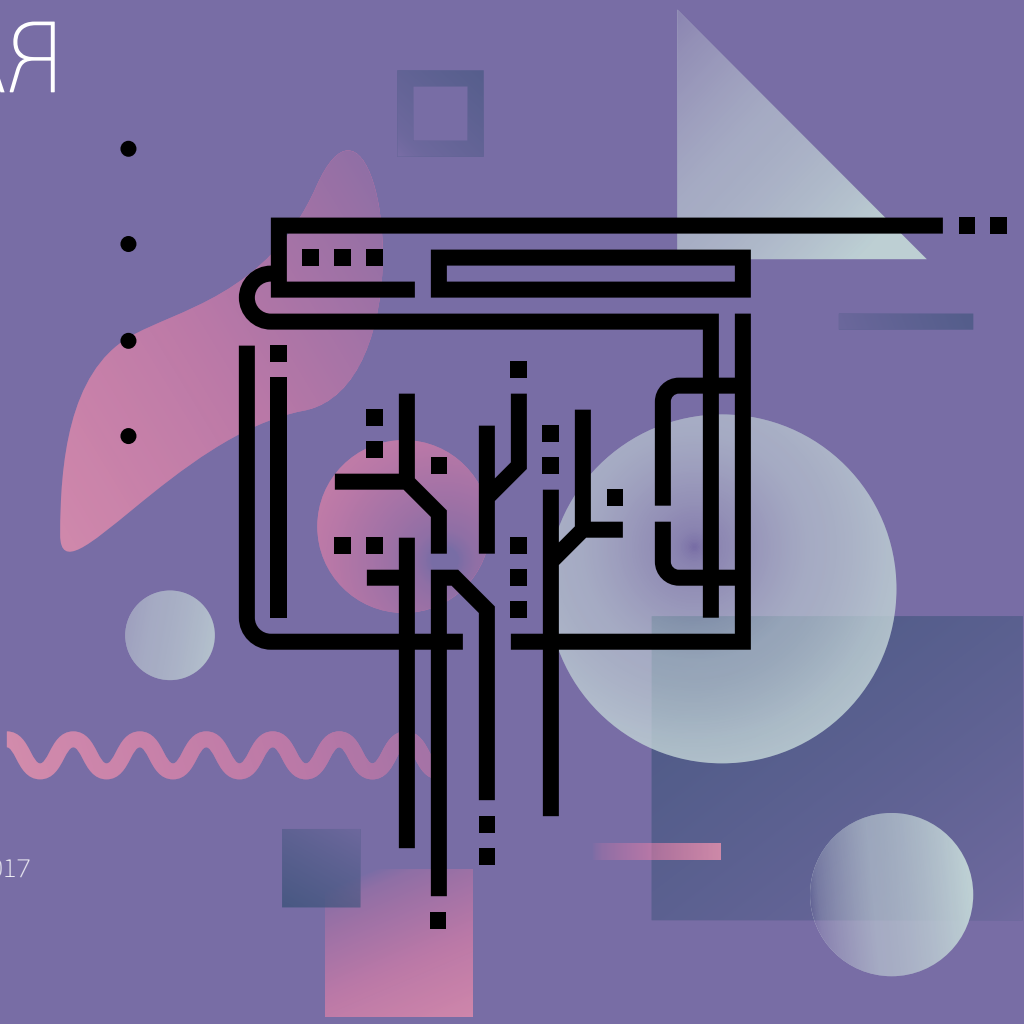
- статьи, аналитические материалы, видео- и радиорепортажи, интервью, обзоры
- созданные одним автором или авторским коллективом
- посвященные теме, связанной с интернет-технологиями

Работа должна быть создана в рамках конкурса: с 31 января по 1 октября ‘17

работы на конкурс принимаются до 1 октября ‘17

ОФИЦИАЛЬНЫЙ САЙТ: ДОТ-ЖУРНАЛИСТИКА.РФ

ЦИФРОВАЯ ДЕРЖАВА



.TXT

СЕРГЕЙ ПЛУГОТАРЕНКО
Директор РАЭК

ИЗ ВЫСТУПЛЕНИЯ НА ФОРУМЕ RIGF-2017

ИСТОРИЯ СТАНОВЛЕНИЯ И САМОРЕГУЛИРОВАНИЯ ОНЛАЙН-ЭКОНОМИКИ

Онлайн-экономика создавалась постепенно, приковывая к себе внимание крупнейших отраслевых организаций, бизнес-структур, позже — государства.

В далеком 1996 году был создан РОЦИТ, тогда же был впервые организован Российский Интернет Форум (РИФ+КИБ). Позже, в 2006 году, начала свою деятельность Ассоциация Электронных Коммуникаций (РАЭК). РАЭК начала проводить отраслевые исследования, производить аналитические продукты, лоббировать интересы интернет-бизнеса, способствовать саморегулированию отрасли. В 2010 году стали появляться новые ассоциации и объединения в области медиа- и интернет-сервисов, стартовали институты развития, инвестфонды в ИТ-области. Все эти годы профильные мероприятия собирали все большую аудиторию — общественность, бизнес и государство стали видеть потенциал в таком, казалось бы, иллюзорном термине, как «Цифровая экономика».

ИНТЕРНЕТ-ОТРАСЛЬ СЕГОДНЯ — ЭТО ЗРЕЛАЯ И САМОДОСТАТОЧНАЯ ИНФРАСТРУКТУРА

Мы видим основные показатели интернет-зависимых рынков и умеем оценивать их — исследования «Мобильная экономика» и «Экономика Рунета» ежегодно дают наиболее полный аналитический отчет о состоянии Цифровой экономики. Мы умеем выявлять консолидированную позицию и единое мнение отрасли, выстраивать межотраслевой договор, работать с пользователями. Мы хотим и умеем работать с молодыми специалистами, понимаем важность развития стартапов. Мы производим системный анализ законодательных инициатив и умеем отстаивать интересы интернет-бизнеса. Вот так, на наших глазах, интернет-отрасль становится одним из наиболее развивающихся сегментов экономики страны.

ОТРАСЛЬ И ГОСУДАРСТВО: ОПЫТ ВЗАИМОДЕЙСТВИЯ

Хотелось бы особенно отметить RIW 2014, в открытии которого принял участие В. Володин. Тогда, в рамках пленарной сессии, было решено создать Дом интернета, а также впервые была представлена концепция Института Развития Интернета. В следующем году, в декабре, состоялся форум «Интернет+экономика», в котором принял участие Президент Российской Федерации Владимир Путин. В 2016 году Владимир Путин в «Послании Президента России Федеральному Собранию» четко определил приоритеты развития Цифровой экономики России.

ЦИФРОВАЯ ЭКОНОМИКА РОССИИ: ОСНОВНЫЕ ПОКАЗАТЕЛИ

Рунет остается самым активным и самым растущим сегментом экономики страны, который все больше влияет на другие отрасли.

Вклад экономики Рунета в ВВП страны в 2015 году составил 2,4%. На мобильный интернет приходится около 25–30% от общего объема рынка. Мобильность остается доминирующим трендом, который вместе с цифровыми сервисами все больше влияет на самые разные сферы деятельности.

Ближайшее будущее — это повсеместное применение интернета и IT в парадигме интернета вещей. К 2020 году количество подключенных к Сети устройств превысит 50 млрд. Проекты с их использованием конвертируются в «умные» города, транспорт или здравоохранение, новое качество жизни, уровень безопасности и др. На наших глазах экономика Рунета трансформируется во всеобъемлющую Цифровую экономику, строительством которой будет заниматься интеллектуальная нация. Цифровая экономика для нас — это та реальность, в которой мы живем. Нас окружает огромное количество веб-сервисов, основная задача которых состоит в повышении доступности различных услуг и упрощении процессов их получения.

Мобильный интернет является одним из главных драйверов развития Цифровой экономики — на сегодняшний день мобильный интернет составляет 3,7% ВВП России, а 62 млн россиян являются пользователями мобильного интернета. Что касается аудитории мобильного интернета, то основными потребителями мобильного контента являются молодые люди в возрастном промежутке 12–24 года. Кроме того, Россия является пятым в мире рынком по числу скачиваний мобильных приложений.

Последние два года аудитория Рунета растет исключительно за счет мобильной составляющей. Пройдет еще немного времени, и мобильные устройства станут основными устройствами потребления контента: пользователи будут проводить за ними гораздо больше времени, чем теперь, несмотря на то, что даже сейчас средний пользователь не расстается с гаджетами по несколько часов в день. Мобильная экономика не совсем окрепла. Пользователи лишь изучают товары на мобильных устройствах, но не слишком часто покупают их таким путем. Форматы мобильной рекламы в мобильных версиях сайтов и приложений не устоялись, а стоимость клика или показа там еще очень низкая. Большую часть доходов получают единицы компаний-разработчиков. Предстоит многое сделать, чтобы мобильные платформы стали приносить такие же деньги, как десктоп.

РЕГУЛИРОВАНИЕ ОНЛАЙН-ЭКОНОМИКИ СЕГОДНЯ

В декабре прошлого года важность Цифровой экономики впервые была продемонстрирована на столь высоком уровне — в своем послании Федеральному Собранию Президент России Владимир Путин сделал особый акцент на этом сегменте.

Президент подчеркнул, что это — вопрос национальной безопасности и технологической независимости России, в полном смысле этого слова — нашего будущего. Далее он предложил провести инвентаризацию и снять все административные, правовые, любые другие барьеры, которые мешают бизнесу выходить как на существующие, так и на формирующиеся высокотехнологичные рынки. То, каким образом Цифровая экономика будет регулироваться на законодательном уровне — приоритетный вопрос для созданного Совета и сегодняшнего заседания.

Для оценки отношения отрасли к новым и существующим законам, регулирующим онлайн-экономику, у РАЭК есть специальный проект «Законодательный барометр РАЭК» — раз в полгода аналитики Ассоциации опрашивают большое количество отраслевых экспертов и публикуют результаты мониторинга законопроектной деятельности, касающейся регулирования интернет-индустрии.

Все мы понимаем: сегодня необходим «фазовый переход» и смена парадигмы регулирования Цифровой экономики на Инновационно-стимулирующий режим. При этом отрасль сегодня готова к сотрудничеству: из пассивного наблюдателя законодательных инициатив в её отношении пора превращаться в проактивного создателя / модификатора нормативной базы и сильного партнера государства в этом направлении.

В декабре 2016 года РАЭК представила данные «Законодательного барометра РАЭК». Так, по количеству резонансных законодательных инициатив в области регулирования Рунета 2016 год может конкурировать только с 2013 годом. Однако общее количество проектов в 2016 году заметно выросло. Очевидна также некоторая стабилизация отношения к регуляторным инициативам. Это говорит о достаточно конструктивном настрое интернет-индустрии, понимании механизмов принятия и реализации законодательных нововведений, которые не всегда так страшны,

как читаются. Многие законопроекты эксперты не смогли оценить однозначно положительно или отрицательно, поэтому они получили оценку «неоднозначно» (более трети законопроектов, внесённых в 2016 году).

Эксперты РАЭК отмечают следующие существенные барьеры на пути консолидации отрасли и инициаторов законопроектов:

- Отсутствие обязательных процедур ОРВ и технической экспертизы для законопроектов;
- Зачастую бессистемный характер взаимоотношений с экспертным сообществом при их привлечении к оценке законопроектов;
- Нередки случаи игнорирования отрицательных экспертных заключений;
- Отсутствие осознания до последнего времени на всех уровнях того, что цифровые технологии и Цифровая экономика в России должны получить статус «национального достояния» и вопросы стимулирования их развития должны войти во все стратегические программы и приоритетные направления развития страны.

Мы считаем, что построение Цифровой экономики требует радикального пересмотра подходов к регулированию. Необходимо помнить и о трансграничном характере интернета, и о международных концепциях, и о том, как отечественное законодательство будет вписываться в мировую картину; мы должны понимать, что отгородиться от мира не получится. Особое внимание в связи с этим требуется к вопросам кибербезопасности.

ЦИФРОВОЕ БУДУЩЕЕ

На сегодняшний день существуют несколько драйверов Цифровой экономики — это мобильная экономика, интернет вещей, «умные» города, транспорт и здравоохранение.

Да, Цифровая экономика для нас — это та реальность, в которой мы уже живем. На наших глазах экономика Рунета трансформируется во всеобъемлющую Цифровую экономику, строительством которой будет заниматься интеллектуальная нация. С одной стороны, мы надеемся, что новый созыв Госдумы продолжит развитие положительного тренда в сотрудничестве с отраслевыми экспертами, наметившийся в 2015–2016 годах.

Кто такие менеджеры по продукту?

BUDU GURU
Гид по карьере в IT

Менеджер по продукту в IT отвечает за создание новых продуктов и развитие существующих. Именно он определяет конечное назначение продукта и стремится сделать его максимально удобным и полезным для потребителя.

Как еще называют

- Product Owner
- Менеджер интернет-проектов
- Продакт-менеджер

Места работы

- Технологические компании
- Дизайн-бюро
- FMCG-компании
- Digital-агентства

Профессия на стыке специальностей

Маркетинг: создавать востребованный продукт и развивать каналы продаж

Tech: управлять веб-разработкой продукта

Дизайн: проектировать удобные и красивые интерфейсы

Основные задачи

- Работать с дизайнерами, программистами и маркетологами
- Изучать потребности аудитории
- Формулировать задачи для команды
- Утверждать концепцию конечного продукта
- Следить за соблюдением концепции на всех этапах создания продукта

При реализации проекта используются средства государственной поддержки, выделенные в качестве гранта в соответствии с распоряжением Президента Российской Федерации от 05.04.2016 No68-рп и на основании конкурса, проведенного Общероссийской общественной организацией «Российский Союз Молодежи»

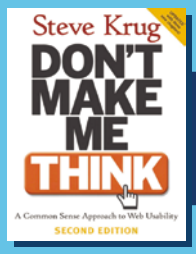
Что делает менеджер продукта?

Ключевые навыки

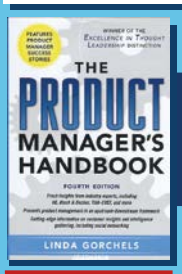
- **Маркетинг**
  (каналы привлечения траффика, создание инфоповодов, продвижение продукта)
- **Управление веб-разработкой**
  (управление командой, составление требований, гибкие методики разработки (Agile/Lean))
- **Стратегия**
  (стратегия вывода продукта на рынок, привлечение инвестиций, разработка дорожной карты продукта, анализ конкурентов)
- **Основы анализа и интернет-аналитики**
- **Разработка системы KPI, анализ в Google Analytics, Яндекс-метрика**
- **Дизайн**
  (основы дизайна и UX, проектирование интерфейсов)

С чего начать

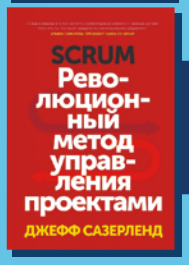
Книги по теме



«Don't Make Me Think Usability»



«The Product Managers Handbook»



«Scrum. Революционный метод управления проектами»

Курсы

нетология

«Руководитель Digial-продукта»
netology.ru

udemy

Курс для руководителя продуктов (на английском)
www.udemy.com

#tceh_edu

«Профессия продакт-менеджер в IT
tceh.com

Сайты

- vc.ru
- mediaskunk.ru
- themedia.center

Источники:

ABC Technology and Games - NBN stats: Australia's broadband future and why the Coalition's alternative «won't work»

Битрикс 24 - Карта российского рынка дистанционной работы 2015

При реализации проекта используются средства государственной поддержки, выделенные в качестве гранта в соответствии с распоряжением Президента Российской Федерации от 05.04.2016 No68-рп и на основании конкурса, проведенного Общероссийской общественной организацией «Российский Союз Молодежи»

О РАБОТЕ ФРОНТЕНД-РАЗРАБОТЧИКА

АНАТОЛИЙ ОСТРОВСКИЙ
СТАРШИЙ РАЗРАБОТЧИК ИНТЕРФЕЙСОВ В ЯНДЕКСЕ

КТО ТАКОЙ ФРОНТЕНД-РАЗРАБОТЧИК?

Разработчик интерфейсов (также этого специалиста называют фронтенд-разработчик от английского front-end developer) занимается созданием клиентской части сайтов, а также программной части. Фронтенд-разработчик отвечает за то, что пользователь видит на сайте, и то, как он с ним взаимодействует.

Кроме того, фронтенд, так же как и бэкенд (от англ. back-end — «оборотная сторона» — программно-аппаратная часть — прим. сайта), включает в себя разработку серверного кода. Постараюсь объяснить разницу между фронтендом и бэкендом в классическом понимании. Например, бэкенд-сервер может отвечать за то, чтобы данные попали в базу данных, а затем повлияли на какие-либо показатели. Например, лайк определенного твита (сообщения в социальной сети Twitter — прим. сайта) влияет на общие тренды. А фронтенд-сервер выступает приемником информации от пользователя. Такое разделение сделано для удобства разработки.

ЧЕМ ФРОНТЕНД-РАЗРАБОТЧИК ОТЛИЧАЕТСЯ ОТ ДИЗАЙНЕРА, КОТОРЫЙ ТОЖЕ РАБОТАЕТ НАД ТЕМ, КАК ВЫГЛЯДИТ САЙТ?

Дизайнер придумывает внешний вид интерфейса, а фронтенд пишет код и воплощает в жизнь макет. Однако разработчик и сам должен разбираться в дизайне. Художник может в чем-то ошибиться, пожертвовать удобством в пользу красоты. Дизайнер не обязан следить за каждым шагом разработчика. Его задача в первую очередь нарисовать идею. То, как это реально будет работать, остается за фронтендом. Поэтому разработчику интерфейсов нужно уметь исправить недочеты и выпустить хороший продукт.

КАК ВЫ СТАЛИ ФРОНТЕНД-РАЗРАБОТЧИКОМ?

Мое образование не слишком связано с программированием. Я окончил Российский экономический университет имени Г. В. Плеханова по специальности «прикладная информатика в экономике». Еще во время учебы я решил, что хочу стать дизайнером сайтов. Планировал поступить на курсы в Британскую высшую школу дизайна, но, к сожалению, они совпали с моей сессией.

Тогда я начал самостоятельно изучать литературу — читал книги и статьи по веб-дизайну. Позже решил опробовать теоретические знания на практике. Создал свою домашнюю страницу, позже дополнил ее форумом. На третьем или четвертом курсе я устроился стажером в небольшую веб-студию.

После полугода работы в студии я приобрел неплохой опыт и поступил в Школу разработки интерфейсов Яндекса. А после ее успешного окончания пошел работать в сам Яндекс.

ПОЛУЧАЕТСЯ, ФРОНТЕНД-РАЗРАБОТЧИКУ НЕ ОБЯЗАТЕЛЬНО ИМЕТЬ СПЕЦИАЛЬНОЕ ВЫСШЕЕ ОБРАЗОВАНИЕ? А ГДЕ ОН МОЖЕТ ПРИОБРЕСТИ НЕОБХОДИМЫЕ ДЛЯ РАБОТЫ НАВЫКИ?

Например, на курсах. Могу порекомендовать Школу разработки Яндекса, в которой учился я сам. Насколько мне известно, такие Школы проводят не только в Москве, но и в Санкт-Петербурге, Минске, Екатеринбурге. Но обучают там не с нуля. Абитуриенты должны уметь создавать простенькие сайты, верстать, писать на языке программирования JavaScript. При поступлении нужно решить тестовые задания, решение которых в большинстве случаев можно найти в интернете, если постараться. Поступить непросто, но учеба дает очень многое.

Также я наслышан о курсах от портала javascript.ru, но сам на них не ходил.

КАК СТАРШЕКЛАССНИКУ, ИНТЕРЕСУЮЩЕМУСЯ РАЗРАБОТКОЙ, ПОНЯТЬ, С ЧЕМ ЕМУ БУДЕТ ИНТЕРЕСНЕЕ РАБОТАТЬ: ИНТЕРФЕЙСАМИ ИЛИ СЕРВЕРНОЙ ЧАСТЬЮ?

Обычно люди, которые решают заняться разработкой, не испытывают сомнений, кем именно они хотят стать. Человек просто понимает, что ему больше нравится: работать с базой данных, писать код бэкенда, или отвечать за скорость и правильность отображения сайта. Как правило, осознание своих интересов происходит еще на этапе знакомства с этими специальностями. Мне известна всего пара примеров, когда человек решил сменить специализацию и ушел из фронтенд-разработки в бэкенд.

При выборе будущего занятия стоит учитывать, что работа фронтенд-разработчика может показаться менее увлекательной, чем работа бэкенда, ведь все сайты с точки зрения структуры

более-менее понятно устроены. Зато технологии в разработке интерфейсов развиваются куда стремительнее, чем в бэкенд-разработке. Почти каждый день появляются новые решения для создания сайтов. Например, два года назад Facebook презентовал свою библиотеку для разработки фронтенда React. Сегодня у нее уже почти 1000 контрибьютеров (то есть 1000 человек поучаствовали в написании ее кода). Это огромные масштабы. В том же бэкенде такого практически не бывает, все решения закрытые и делаются определенной группой людей.

Через год после запуска эта библиотека эволюционировала, и с её помощью можно делать приложения для iOS и Android. То есть, умея делать сайты на React, человек автоматически может быть и мобильным разработчиком. По-моему, это очень здорово. И, думаю, это только начало.

КАКОЙ КАРЬЕРНЫЙ РОСТ МОЖЕТ БЫТЬ У ФРОНТЕНД-РАЗРАБОТЧИКА?

У него есть два пути. Он может стать руководителем. Вначале — группы, затем — нескольких групп, и наконец получить позицию технического директора. Если же человеку неинтересно управлять людьми, можно стать экспертом, ведущим разработчиком, выступать на конференциях и быть гуру для менее опытных коллег.

КАКИЕ КОМПЕТЕНЦИИ ДОЛЖНЫ БЫТЬ У ФРОНТЕНД-РАЗРАБОТЧИКА?

Мне кажется, по сравнению с бэкенд-разработчиками, «фронты» более общительны. Им нужно много общаться с менеджерами и дизайнерами, чтобы понимать, как должен работать конечный продукт.

Также фронтенд-разработчик должен быть ответственным и дотошным. Бывает, что один из бэкендов (а их бывает много) перестает отвечать. В таком случае пользователю все равно нужно дать максимально возможный набор информации, который сейчас доступен. Например, если отказали в рекомендации новостей, то, возможно, доступна хотя бы остальная статья. Но если на странице статьи недоступна статья, то проще показать пользователю страницу ошибки (например, сервис временно недоступен). Такие моменты решает и программирует именно фронтенд-разработчик. Ни один дизайнер и менеджер такое предусмотреть не сможет. А фронтендер должен.

ОТ ЧЕГО МОЖЕТ УСТАТЬ ФРОНТЕНД-РАЗРАБОТЧИК?

Может утомить однотипность задач. Как я уже говорил, сайты имеют примерно одинаковую структуру, у них есть шапка, меню, лента новостей и т.п. Редко попадаются заказчики, которые хотят нечто новое, над чем придется поломать голову и придумать нестандартное решение.

СКОЛЬКО ПОЛУЧАЕТ ФРОНТЕНД-РАЗРАБОТЧИК?

Зависит от знаний и умений специалиста. Я не очень хорошо знаю рынок сейчас, но, думаю, стажер или младший разработчик получает от 60 тысяч в месяц. Конечно, если под фронтендом понимается только верстка страничек без JavaScript, оплата будет меньше.

Верхней же зарплатной границы нет — все зависит от способностей специалиста.

БУДУТ ЛИ ФРОНТЕНД-РАЗРАБОТЧИКИ ВОСТРЕБОВАНЫ В БЛИЖАЙШИЕ 10–15 ЛЕТ?

Уверен, что будут. Уже сегодня фронтенд-разработчик может создавать не только сайты и веб-приложения, но и приложения для мобильных устройств. Приложения для телевизоров и некоторые операционные системы, например, Firefox OS, тоже сделаны на технологиях фронтенда. Я думаю, что в будущем возможности использования технологий, которыми пользуются фронтенд-разработчики, будут только расти.

ЧЕМ МОЖЕТ ЗАНЯТЬСЯ ФРОНТЕНД-РАЗРАБОТЧИК, РЕШИВШИЙ ПОПРОБОВАТЬ СЕБЯ В ЧЕМ-ТО НОВОМ?

Он может заняться разработкой мобильных приложений. Многие решения в мобильной разработке и разработке интерфейсов весьма похожи.

Если же человек больше не хочет заниматься разработкой, он может попробовать себя в роли менеджера проектов. Это подойдет специалисту, который умеет общаться с людьми, способен ставить задачи и следить за их исполнением. Можно податься в тестировщики, хотя обычно люди движутся как раз в обратном направлении: из тестирования в разработку.

КТО ДЛЯ ВАС ЯВЛЯЕТСЯ РОЛЕВОЙ МОДЕЛЬЮ В ПРОФЕССИИ?

Думаю, каждый находит своих «гуру» в определенных сферах. Например, в мире CSS (верстки) для меня это Роман Комаров. У него есть много хороших докладов и замечательный сайт с настоящей «магией» верстки.

Кроме того, для себя я выделил Пола Айриша и Дэна Абрамова. Полезно посмотреть презентации этих известных фронтенд-разработчиков (например, здесь Пол Айриш очень доступно рассказывает о разработке приложений на JavaScript — прим. сайта), а также послушать их доклады. Опыт, которым они делятся со зрителями, помогает мне работать продуктивнее.

СУЩЕСТВУЕТ ЛИ КАКАЯ-ЛИБО ВОЗМОЖНОСТЬ ЕЩЕ В ШКОЛЕ ПОЛУЧИТЬ ОПЫТ, КОТОРЫЙ В БУДУЩЕМ ПОМОЖЕТ СТАТЬ РАЗРАБОТЧИКОМ ИНТЕРФЕЙСОВ?

Нужно как можно раньше научиться ставить себе задачи, в противном случае человек просто не будет знать, с чего начать. Например, можно поступить как я и поставить задачу создать сайт-резюме. Потом этот сайт можно будет усовершенствовать: добавить возможность комментирования страницы.

И, конечно, нужно учить английский язык, чтобы иметь возможность знакомиться с самими современными курсами и пособиями и не ждать, когда их переведут на русский язык.

ЧТО ВЫ МОГЛИ БЫ ПОСОВЕТОВАТЬ ПОЧИТАТЬ И ПОСМОТРЕТЬ ПОДРОСТКАМ, КОТОРЫЕ ХОТЯТ БОЛЬШЕ УЗНАТЬ О ФРОНТЕНД-РАЗРАБОТКЕ?

Для старта я бы порекомендовал платформу Codecademy. Там можно изучить популярные языки программирования, пройти уроки по фронтенд-разработке, а потом попробовать что-нибудь сделать самому. Обязательно нужно много раз перечитать курс по JavaScript. Еще один полезный сайт — HTMLBook. На нем есть много примеров верстки. И вообще это большая энциклопедия для разработчика интерфейсов. Сам я периодически пересматриваю лекции на youtube-канале «Фронтенд», где выступают ребята из Яндекса.

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

Нетоскоп

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
В ДОМЕННОМ ПРОСТРАНСТВЕ

netoscope.ru | нетоскоп.рф

16+

РОССИЙСКАЯ НЕДЕЛЯ
ВЫСОКИХ ТЕХНОЛОГИЙ

СВЯЗЬ

Информационные и коммуникационные технологии

24—27 апреля 2018

30-я юбилейная международная выставка

Организатор:

ЭКСПОЦЕНТР МОСКВА

При поддержке:
- Министерства промышленности и торговли РФ
- Федерального агентства связи (РОССВЯЗЬ)
- Российской ассоциации электронных коммуникаций (РАЭК)

Под патронатом ТПП РФ

Россия, Москва, ЦВК «Экспоцентр»

www.sviaz-expo.ru

12+ Реклама

RIW.MOSCOW

1/2/3
НОЯБРЯ

ЭКСПОЦЕНТР