№11
апрель 2019

MSK IX

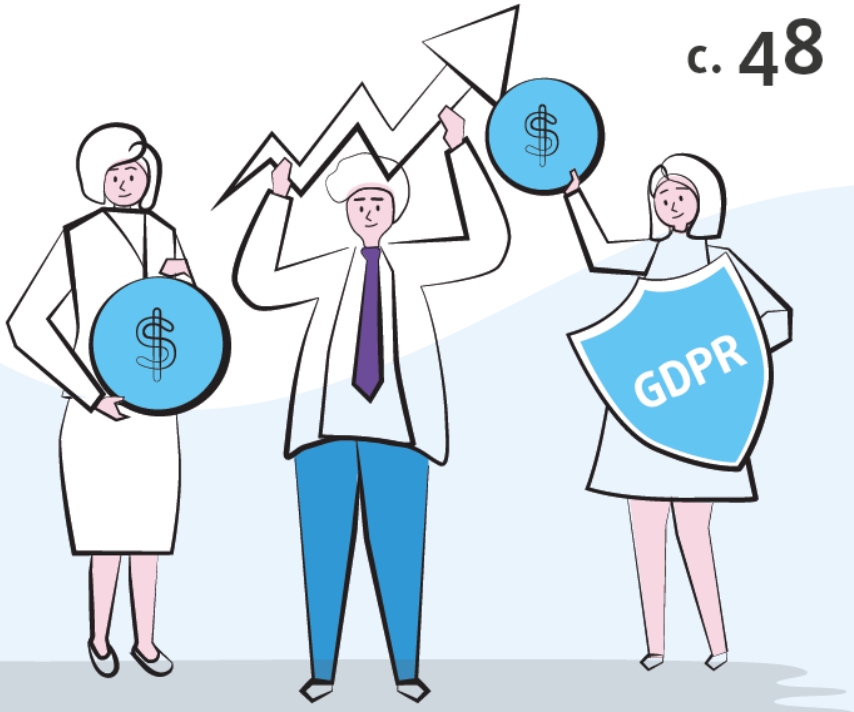
Интернет изнутри

25 лет РУНЕТУ

с. 4

с. 10

Экономика Интернета



Содержание:

Журнал «Интернет изнутри»
По всем вопросам пишите на info@internetinside.ru

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №11, дата выхода: апрель 2019 г.

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Регистрационный номер:
ПИ № ФС77-71202 от 27.09.2017

Публикуется при поддержке АНО «ЦВКС «МСК-IX»

Главный редактор:
Андрей Робачевский

Зам. главного редактора:
Новикова Татьяна

Редакционная коллегия:
Воронина Елена
Платонов Алексей

Дизайн:
Ильина Наталья

Корректор:
Рябова Наталья

Рунету 25 лет

главный редактор,
Андрей Робачевский

Дорогой читатель!

Хотя 7 апреля 1994 года принято считать днем рождения Рунета, связать конкретное событие – например, делегирование домена .ru – с появлением Интернета в России так же сложно, как связать одно из многочисленных вех развития глобального Интернета с его рождением. В этом проявляется одна из фундаментальных сущностей Интернета – взаимодействие независимых сетей при отсутствии центрального управления. А раз так – трудно найти историческое решение или декрет, или указ, постанавливающий включить Интернет.

В любом случае, **апрель 1994 года** – важная веха развития Интернета в России, так же, как январь 1983 года, когда в Интернете был внедрен стек протоколов TCP/IP, - одна из ключевых дат для Интернета в целом.

Другими словами, перед вами юбилейный номер, хотя и 11-й. И открывает его юбилейная статья Алексея Платонова **«Путевые заметки свидетеля Рунета»**, в которой он вспоминает о наиболее ключевых моментах в возникновении и развитии Рунета.

Говоря о развитии, невозможно оставить без внимания одну из основных движущих сил эволюции Интернета – экономическую. В своей статье «Экономика Интернета» Джефф Хьюстон размышляет о позитивном влиянии рыночной экономики и несостоятельности рынка на инновацию и безопасность в Интернете. Кстати, об эволюции безопасности, а точнее – «опасности» в Интернете вы сможете прочитать в статье Александра Лямина «Эволюция DDoS-атак: от первых инцидентов до терабитных атак».

Развитие Интернета стремительно – всего за несколько десятилетий он превратился из эксперимента, научно-исследовательских проектов в неотъемлемую часть социальной и экономической жизни общества. Часто государственная политика не успевает за этим процессом. Многие вопросы кибербезопасности, как на национальном, так и международном уровне остаются пока без эффективного ответа. Обзору национальной киберстратегии США посвящена статья Мадины Касеновой.

Как вы могли заметить, воспользовавшись юбилеем, мы также решили немного изменить содержательную часть журнала. Вместо сквозной тематики номера мы ограничимся передовицей на злобу дня, что позволит нам подобрать более актуальные материалы в другие разделы. Структура журнала останется неизменной, как и наши постоянные авторы – Павел Храмцов и сотрудники Координационного центра доменов .RU/.РФ.

Как всегда, нам очень интересно и важно знать ваше мнение. Что понравилось и что можно улучшить? Какие темы вы хотели бы увидеть в следующих выпусках?

Пишите нам по адресу info@internetinside.ru.

Путевые записки свидетеля Рунета

Алексей Платонов

В апреле 2019 года исполняется 25 лет со дня регистрации национального домена Российской Федерации .ru, и эта дата позиционируется как день рождения «Рунета». Термин этот – сугубо «пиаровский» и не несет в себе никакого конкретного смысла, пока не дано его четкого общепринятого определения. В рамках данного текста, посвященного нашему первому национальному домену (а есть еще и второй по хронологии, кириллический домен .рф), будем считать, что Рунет = национальный домен (точнее, все домены, заканчивающиеся на .ru) – ну просто для удобства ведения разговора. В целом, Интернет в нашей стране появился и развивался на первом этапе как частная инициатива – коммерческих организаций или научно-образовательных центров – не суть важно. Я же хотел рассказать о каких-то ключевых моментах в возникновении и развитии Рунета – в той интерпретации, о которой я сказал, с привязкой к национальной доменной зоне .ru.

В апреле 2019 года исполняется 25 лет со дня регистрации национального домена Российской Федерации .ru, и эта дата позиционируется как день рождения «Рунета». Термин этот – сугубо «пиаровский» и не несет в себе никакого конкретного смысла, пока не дано его четкого общепринятого определения. В рамках данного текста, посвященного нашему первому национальному домену (а есть еще и второй по хронологии, кириллический домен .рф), будем считать, что Рунет = национальный домен (точнее, все домены, заканчивающиеся на .ru) – ну просто для удобства ведения разговора.

Тут я сразу должен отметить (полагаю, что не все это знают), что Интернет в Россию пришел несколько раньше 1994 года (когда был зарегистрирован домен .ru), с подключением к Сети научно-образовательных организаций (Институт космических исследований, Институт органической химии, НИИЯФ МГУ) и с доменом .su – а это Курчатовский Институт и порожденные им сети «Демос» и «Релком». В целом, Интернет в нашей стране появился и развивался на первом этапе как частная инициатива – коммерческих организаций или научно-образовательных центров – не суть важно. Впрочем, история этого вопроса изложена в разных статьях и книжках, так что любопытствующие могут легко найти информацию на эту тему в Интернете и вне его. Я же хотел рассказать о каких-то ключевых моментах в возникновении и развитии Рунета – в той интерпретации, о которой я сказал, с привязкой к национальной доменной зоне .ru.

Итак, после первых подключений к Интернету разных организаций/сетей, а также после того, как пропала сама основа для домена .su – Советский Союз, возникла необходимость как-то «застолбиться» в Сети уже от имени свежеиспеченной Российской Федерации. Тут надо разъяснить, что национальный домен не является собственностью государства, как не является ею и соответствующий код ISO. Домен делегируется для использования интернет-сообществом под контролем администратора, определяемого консенсусом этого самого сообщества, освященного согласием государства. Государству нашему в 90-е годы было не до Интернета и не до доменов как составной части оного. Нестабильность, дрязги между формировавшимися олигархическими кланами, приватизация нефтяных вышек и прочих природных ресурсов – вот это и находилось в фокусе внимания госорганов. Интернет, предоставленный сам себе, также испытывал турбулентность – и из-за общего состояния экономики в стране, и вследствие сразу же возникшей конкуренции между различными группами, занимавшимися его развитием.

Известно, что домен .ru был делегирован несколько позже, чем в случае других стран xUSSR по вполне простой и естественной в той ситуации причине – организации, претендовавшие на администрирование домена («Демос», «Релком», Институт ИОХ РАН) не смогли договориться и подали три независимые заявки в IANA. Международные инстанции сети Интернет никогда не вникают во внутригосударственные разборки (тем более - «развивающихся» стран, в категорию которых мы немедленно свалились после распада СССР), и все заявки были просто-напросто заблокированы.

А в то же самое время (1992 год) Институт атомной энергии им. Курчатова, вслед за «Демосом» и «Релкомом», породил еще одну структуру (совместно с Госкомитетом по делам науки и высшей школы), которая сыграла ключевую роль в этой истории - Российский НИИ развития общественных сетей (РосНИИРОС). Институт был создан как негосударственная некоммерческая организация с задачей развития компьютерных телекоммуникаций (читай – Интернета) для научно-образовательного сообщества. С небольшим временным лагом была учреждена Ассоциация RELARN, объединившая научно-образовательные организации, которые являлись пользователями различных российских интернет-сетей (по факту это были в основном сети «Демос»

25 лет РУНЕТУ

и «Релком», имевшие наибольший охват по регионам РФ). Так возник проект RELARN, который принес огромную пользу для нашей науки и образования, обеспечив их в 90-е годы доступной электронной почтой, объединившей университеты и научные центры между собой и с международным сообществом, которое уже активно использовало возможности сети Интернет.

Связь этой истории с доменом .ru заключается в следующем. Упомянутый выше РосНИИРОС стал координатором проекта RELARN, в относительно короткое время завоевав авторитет как в научно-образовательном сообществе, так и среди интернет-операторов (а они фактически и обслуживали это сообщество на начальном этапе) в качестве нейтральной организации в некоммерческом статусе, работающей в интересах общества и государства. По существу, в лице РосНИИРОС возникла точка доверия (и это доверие для нас очень дорогого стоило), «вокруг» которой можно было договариваться по вопросам, имеющим особую важность для интернет-сообщества в целом. Так случилось и в отношении домена .ru, и чуть позже (1995 год) при создании первой в России точки обмена интернет-трафиком. В итоге всем сторонам удалось договориться, что РосНИИРОС будет выполнять функции администратора домена .ru, а также осуществлять его техническую поддержку. Государство в лице Госкомитета по делам науки и высшей школы было в курсе и не возражало. Поскольку вопросы развития Интернета в РФ никакому ведомству на этом этапе поручены не были, то мы на этом и остановились. Согласительный протокол был подписан всеми значимыми на тот момент интернет-операторами и отправлен в IANA, домен .ru был делегирован. Техническое обеспечение, включая DNS, на начальном этапе осуществлял «Релком» (в порядке спонсорской поддержки), но достаточно быстро был построен собственный технический центр, созданный с нуля исключительно российскими специалистами, принятыми на работу в РосНИИРОС.

Попутная познавательная история: очень любопытная ситуация возникла на начальной стадии развития Интернета в России – она существовала во «времена» домена .su и продолжилась (правда, на совсем короткое время) после регистрации .ru. Внутри России уже существовали IP-линки и DNS, но связность с остальным миром была очень слабая: сначала это были только почта UUCP и новости (News), да и когда появился международный цифровой канал, его пропускная способность поначалу не позволяла надежно передавать сколь-нибудь существенный объем информации. Поэтому после регистрации очередных доменов и правок зоны на «внутреннем» российском сервере файл фактически вручную дублировался на DNS-сервере в Хельсинки, где им заведовал наш коллега (и хороший друг российских сетевых администраторов) Petri Ojala. Общее сопровождение таких мероприятий (а Россия была не одинока в своем не вполне полноценном положении в сетевом мире) осуществлял Peet Beertema из Амстердама. Таким образом, «российский сегмент» обслуживался двумя авторитативными «корневыми серверами» – один из них работал внутри России, а второй был ориентирован на международную часть Сети.

История с регистратурой домена .ru показательна еще и тем, что при ее создании в полной мере удалось реализовать принципы саморегулирования: выработку правил регистрации доменных имен и контроль за их соблюдением выполняла чисто общественная структура – координационная группа домена .ru, куда входили представители всех заинтересованных организаций, прежде всего интернет-сервис-провайдеров, которые, как правило, и выполняли роль регистраторов доменов (в дальнейшем появились и профессиональные регистраторы, как правило, на базе хостинговых компаний). Фактически, это был некий прообраз современных СРО (саморегулируемых организаций), которые обеспечивают регуляцию соответствующего рынка при наличии достаточного количества субъектов («игроков»), работающих с потребителем.

Пока доменов было относительно немного, контроль процесса регистрации осуществлялся практически в ручном режиме – путем регулярного рассмотрения спорных заявок на регистрацию доменов второго уровня на заседаниях КГ. При этом список «просеивался» и на предмет наличия в нем всякого безобразия в виде, например, «ненормативной лексики». Одно время было еще такое любопытное правило: домен в виде общеупотребительного слова можно было зарегистрировать только в том случае, если название организации-заявителя совпадало с этим словом. Поэтому для получения вожделенного домена отдельные товарищи регистрировали целую организацию (хорошо известен случай, когда для получения домена sex.ru было зарегистрировано ООО «Секс»). В дальнейшем, после начала взрывообразного распространения веб-сайтов, справляться с контролем регистрации доменов стало чем дальше тем труднее, поэтому правила максимально упростились – ну разве что с матерщиной продолжали бороться в меру сил. Но при этом, благодаря максимальной открытости домена .ru, он стал и одним из наиболее успешных по скорости роста зоны второго уровня. Многие национальные домены, имеющие многочисленные ограничения на регистрации, развивались крайне медленно, выталкивая потенциальных клиентов в международные доменные зоны (.com, .org и др.), в то время как у нас подавляющее число новых регистраций шло именно в национальной зоне. Сейчас ситуация стала несколько размываться – за счет появления многочисленных новых доменов верхнего уровня, но приоритет .ru (и .рф) все-таки продолжает сохраняться.

Надо также упомянуть, что в начале 90-х наиболее популярен у нас был домен .su, который использовался, прежде всего, для сервиса электронной почты. Поскольку в перспективе .ru должен был полностью заменить «советский» домен, пришлось его продвигать, даже в некоторой степени искусственно. Способствовало росту популярности зоны .ru и то обстоятельство, что в нем сразу была разрешена регистрация доменов второго уровня, чего в .su в тот период времени не было: он был построен по географическому принципу (использовалась структура почтового адреса, то есть на втором уровне, как правило, мог быть только город).

Хочу еще на одном вопросе остановиться – на деньгах. Регистрации в домене .ru стартовали как бесплатные, но с ростом потока заявок стало понятно, что надо отходить от практики занесения доменных имен в текстовой файл на офисном компьютере и создавать нормальный реестр, да еще плюс серверное хозяйство для обработки заявок и построения собственной DNS. В зарубежных доменных зонах такой проблемы первоначально не возникло: как правило, все начиналось на базе научно-образовательных сетей (да и весь публичный Интернет «у них» стартовал как научно-образовательный проект), которые имели определенное бюджетное финансирование, из которого и можно было взять некоторые средства на общую инфраструктуру Сети. У нас такой возможности не было ввиду отсутствия сколь-нибудь значимой поддержки государства – так что пришлось коммерциализоваться ударными темпами, проще говоря, вводить оплату за регистрацию доменных имен. Оплата была довольно существенной – что-то около 50 долларов (для справки, сейчас цена составляет 120 рублей для регистраторов), но желающих получить доменное имя только прибывало – Интернет пошел в гору и быстро превратился в проект коммерческий - и у нас, и за рубежом (причем у нас даже быстрее, в отсутствие бюджетных вливаний во вновь формирующуюся отрасль). По мере роста регистраций, который опережал рост «доменной» части бюджета РосНИИРОС, цена снижалась, ну а в ответ еще больше возрастало количество доменов в зоне. У нас практически сразу появились «партнеры» из числа тех операторов, которые регистрировали домены для своих клиентов – то есть возник новоиспеченный бизнес.

Хочу отметить, что несмотря на падение цены регистрации по мере роста числа доменов в зоне, она не должна стремиться к нулю - в противном случае «условно-бесплатная» зона быстро становится «мусорной»: туда как мухи на мед слетаются разнообразные злонамеренные личности, регистрирующие домены для всяких темных дел. Ну и вообще, домен перестает быть хоть сколь-нибудь значимой ценностью, так что и отношение к нему соответствующее. Таким образом, наличие достаточно существенной прибыли у регистратуры – это закон функционирования доменной экосистемы. Учитывая, что типовая регистратура – это некоммерческая организация, возникает очевидная проблема: а как потратить деньги, которые остаются после мероприятий по развитию системы? Очевидный ответ – на какие-то понятные обществу «богоугодные дела», поскольку делить прибыль между учредителями некоммерческая организация возможности не имеет. Если говорить о международном опыте, то постепенно схема наладилась, но поначалу возникали некоторые интересные казусы: например, англичане (домен .uk) не придумали ничего лучше, как купить поле для гольфа (уж как они его дальше использовали, я понятия не имею – наверное, играли на нем в обеденный перерыв).

Но у богатых – свои причуды, что же касается нас, то особых сомнений не было. Основная задача, которую поставили перед РосНИИРОС учредители, – развитие научно-образовательных сетей, деньги на которое выделялось, в общем-то, по остаточному принципу, особенно в первой половине девяностых (не до жиру, какая уж там наука и образование). Даже когда Миннауки учредило первую межведомственную программу (она называлась «Национальная сеть компьютерных

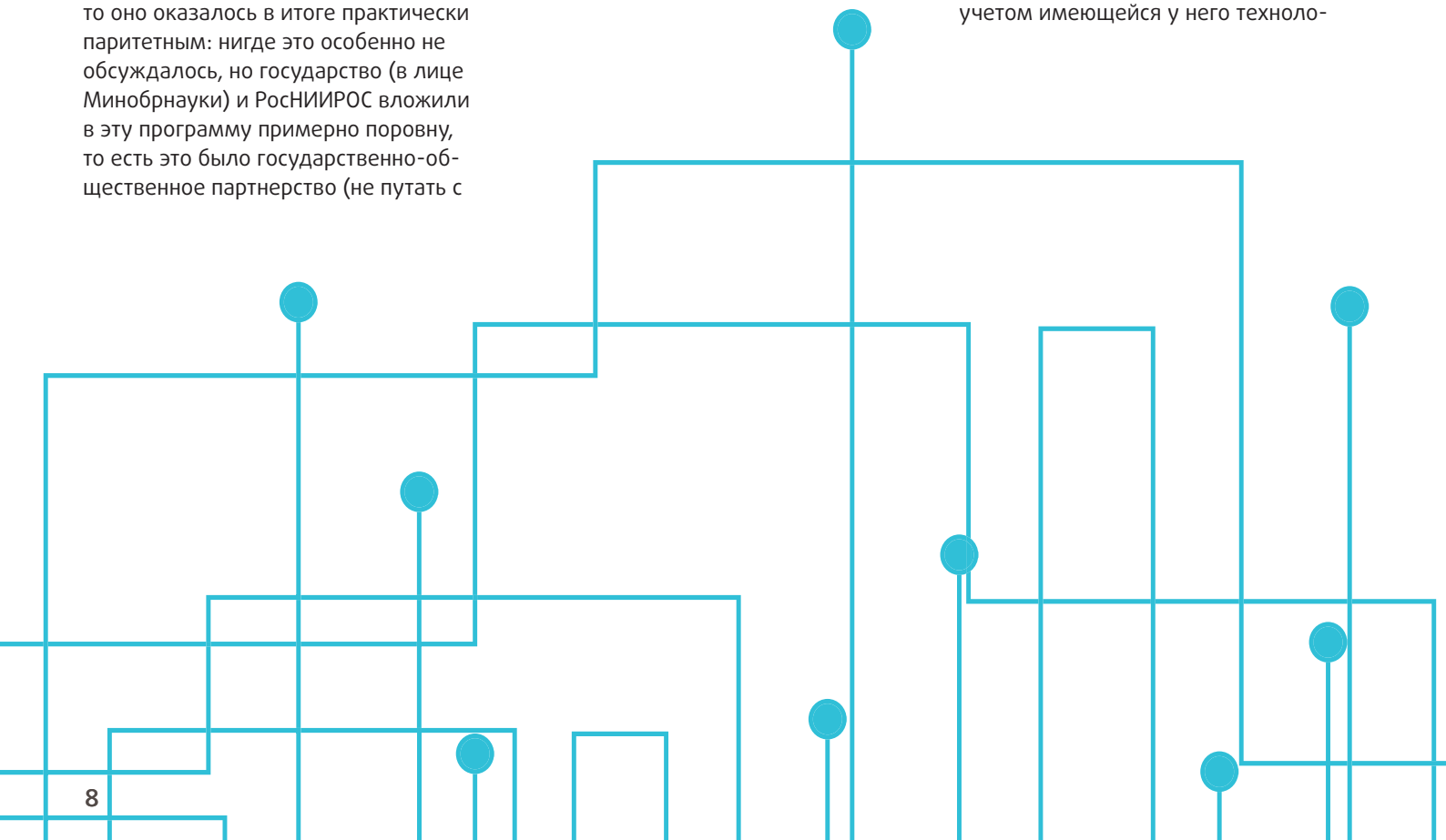
История с регистратурой домена .ru показательна еще и тем, что при ее создании в полной мере удалось реализовать принципы саморегулирования: выработку правил регистрации доменных имен и контроль за их соблюдением выполняла чисто общественная структура – координационная группа домена .ru, куда входили представители всех заинтересованных организаций, прежде всего интернет-сервис-провайдеров, которые, как правило, и выполняли роль регистраторов доменов (в дальнейшем появились и профессиональные регистраторы, как правило, на базе хостинговых компаний).

телекоммуникаций для науки и высшей школы» – НСКТ-НВШ) - и это был реальный прорыв, – средств хватало только на оплату каналов передачи данных и частично на оборудование. Догадайтесь, откуда мы брали деньги на другую «часть оборудования», зарплату весьма квалифицированных людей, да и вообще, хоть на сколько-нибудь приличное содержание организации? Правильно, из прибыли по «доменной деятельности», поскольку других доходов у нас просто не было в принципе. Кстати, когда в 1998 году произошел пресловутый дефолт, сопровождавшийся обвалом рубля, то нашу сеть удалось вытащить только за счет того, что в регистрации доменов мы перешли на цены в у.е. – ведь бюджетная подпитка считалась, естественно, в рублях, и при этом не только не выросла, но и существенно сократилась ввиду катастрофического положения в научно-образовательном хозяйстве в тот период времени. Ну и как результат, к началу века была построена одна из крупнейших в РФ на тот момент интернет-сетей, которая базировалась на наземных каналах («Ростелеком», а затем «Трансстелеком») и охватывала сотни организаций сферы науки и образования (кстати, тогда и прошла первая волна подключения российских школ – через региональные университеты). Что касается финансирования, то оно оказалось в итоге практически паритетным: нигде это особенно не обсуждалось, но государство (в лице Минобрнауки) и РосНИИРОС вложили в эту программу примерно поровну, то есть это было государственно-общественное партнерство (не путать с государственно-коммерческим – оно обеспечивает прибыль для тех, кто в нем участвует со стороны бизнеса).

Ну а что же государство? К началу 2000-х стало понятно, что Интернет – это серьезно, как с точки зрения бизнеса, так и учитывая возможности распространения информации помимо традиционных источников. В 1999 году состоялась историческая (с моей точки зрения, конечно) встреча представителей «интернет-общественности» и премьер-министра РФ В. В. Путина, на которой было решено, что все значимые государственные правовые акты, касающиеся области Интернета, должны приниматься по согласованию с основными общественными организациями, которые в этой области работают. Таковых в то время оказалось три: Ассоциация документальной электросвязи (АДЭ), Региональная общественная организация «Центр Интернет-технологий» (РОЦИТ) и Союз операторов Интернет (СОИ).

В качестве пробного камня было предложено урегулировать положение в области регистрации доменов в национальной зоне .ru, поскольку «сверху» тут все выглядело как некоторая самодеятельность. На тот момент уже имелось предложение министерства печати по созданию специализированной госструктуры, которая должна была заниматься регистрацией доменов, а одновременно предлагалось обязать все бюджетные (а может, и не только бюджетные) организации зарегистрировать домен для своего корпоративного сайта – не бесплатно, конечно. Тут, конечно, без комментариев, тем более что дело прошлое, да и обсудить, откуда взялось такое предложение, сейчас не с кем.

Решение проблемы было поручено Минсвязи, которое, в свете решения, принятого на упомянутой выше встрече, заняло весьма конструктивную позицию. В результате деятельности рабочей группы, куда вошли представители обеих сторон (государство – общественность), и было принято решение фактически институировать координационную группу, превратив ее в юридическое лицо - Координационный центр национального домена (КЦ), учредителями которого стали три присутствовавшие на встрече общественные организации плюс РосНИИРОС как администратор домена .ru, а члены координационной группы образовали первоначальный состав Совета КЦ. Функции КЦ – разработка правил регистрации и контроль их соблюдения; при этом было предложено сохранить за РосНИИРОС выполнение технических функций, с учетом имеющейся у него техноло-



гической базы и накопленного опыта. Регистрация доменов должна была осуществляться специализированными организациями – регистраторами, аккредитацию которых должен был проводить КЦ. Ну и роль государства была определена как надзорная: представитель Минсвязи вошел в Совет КЦ с правом вето на любое решение, которое могло бы нарушить интересы государства. Так и возникла та конфигурация, которая в том или ином виде сохраняется до сих пор, с учетом некоторых (надо признать, достаточно существенных) модификаций.

Какие же события произошли с момента образования Координационного центра? КЦ сразу же был включен в работу, став де-факто администратором домена .ru, но формальное переделегирование домена состоялось только в 2004 году. В 2009 году был сделан следующий шаг, без изменения общей конструкции: был создан «Технический центр Интернет», учредителями которого стали Координационный центр и «Фонд развития Интернет» (администратор исторически-территориального домена .su). Все то, что относилось к доменной тематике (люди, оборудование, технологии), переехало из РосНИИРОС в ТЦИ, так что преемственность была полностью соблюдена и в этом случае.

В дальнейшем изменился состав учредителей КЦ – помимо имеющихся участников, туда вошли «Институт развития Интернет» и собственно Минсвязи. Надо ли было государству напрямую участвовать в КЦ – прямо скажу, не знаю. На мой взгляд, это увеличило «консервативность» организации, а что касается контролирующих полномочий государства, то их вполне хватало и в предыдущей конфигурации. Но в любом случае, это мое сугубо частное мнение - в принципе, работать можно. Ну и, пожалуй, последний штрих в картине – переход ТЦИ под «крышу» (в хорошем смысле слова) «Ростелекома», что состоялось в 2018 году.

Опять же, есть в этом свои плюсы и минусы, но вот с чем поспорить нельзя, так это с тем, что стабильность конструкции возросла, равно как вырос и авторитет ТЦИ – просто за счет величия «Ростелекома» (это не ирония, я тут улыбаюсь по-доброму). Пожалуй, это все, что я хотел сказать в своих путевых записках. Разве что можно было бы еще упомянуть о кириллическом домене .рф, делегированном в 2010 году, администратором которого также стал КЦ, но поскольку тут у меня речь идет о Рунете, а не РФнете (помните определение в начале текста?), то это уже другое повествование.

Закончить эту историю я хотел бы констатацией следующего факта. Мы уже довольно давно (лет около десяти) живем в условиях кардинальных изменений условий существования сети Интернет, которые в целом можно характеризовать как переход от «техно-романтического» периода к временам жесткой бизнес-конкуренции с одной стороны и усиление контроля со стороны государства - с другой. Сеть играет все большую роль буквально во всех сторонах жизни общества – экономической, политической, социальной. Интернет является сейчас не только структурой, обеспечивающей бизнес, но и стал бизнесом сам по себе. Так называемая цифровая экономика вся насквозь пронизана глобальной Сетью, которая по существу образует для нее несущий каркас. Поэтому не удивительно, что каждое государство (и Россия в этом находится далеко не в первых рядах) проявляет к Интернету все большее внимание, поскольку от его работы зависит очень многое. Не все пока идет гладко, но очень хочется надеяться, что по мере взаимодействия государственных, общественных и профессиональных структур удастся нащупать золотую середину, которая позволит соблюсти интересы всех сторон и обеспечит активное развитие виртуального пространства, куда сейчас, хотим мы этого или нет, переходит существенная часть нашей жизни. Собственно, это и есть мое пожелание – одного из «свидетелей Рунета» с момента его возникновения 25 лет назад.

Экономика Интернета

Джефф Хьюстон (Geoff Huston)

Эйфория от безграничных возможностей, которые сулило зарождение Интернета, теперь уравновешивается опасениями и страхами. Надежна ли инфраструктура, можно ли ей доверять? Почему у нас никак не получается сделать Интернет безопасным? Кто на самом деле определяет развитие Интернета, и не попадаем ли мы в заложники узколобого эгоизма нынешних королей рынка? Очень похоже, что Интернет повторяет историю газетной индустрии, где реклама превратилась в хвост, виляющий собакой. Для Интернета таким хвостом, кажется, стал так называемый наблюдательный капитализм (surveillance capitalism)

В конце 2017 года, в телекоммуникационном секторе все разговоры очередной раз вращались вокруг пресловутой сетевой нейтральности в Соединенных Штатах. Процесс определения национальной политики в области коммуникаций как будто превратился в спортивный чемпионат – с комментаторами, восхваляющими чемпионов и втаптывающими в грязь их оппонентов. Теперь эта шумиха прошла – пусть и не принеся удовлетворительных результатов, – и ныне мы ломаем копья вокруг роли гигантских IT-компаний (таких как Facebook, Amazon, Apple, Microsoft и Alphabet – вдруг кто-то из читателей последние десять лет провел в пещере и не знает, о ком речь). Уж не разрослись ли они до таких размеров, что уже де-факто неподвластны ни одному национальному государству? Или можно все-таки создать схему госрегулирования, которая уравновесит интересы этих гигантов от технологии с национальной политикой разных стран? Это, возможно, крупнейший вопрос телекоммуникационной политики конца 2018 года, но отнюдь не единственный. Никуда не исчезли другие важные проблемы, такие как безопасность и приватность, пиринг и связность сети, рыночная эффективность и непрерывные инновации и эволюция коммуникационной отрасли, политики на основе данных, защита потребителя... и многие, многие другие.

Коммуникация, по сути, есть общение. Способ, которым мы общаемся, богатство и охват нашего общения оказывают огромное влияние на облик и функционирование нашей экономики и общества в целом. А потому рождение государственных политик в коммуникационной индустрии неслучайно становится предметом публичного обсуждения. Как мы можем повлиять на их выработку? Как можем донести информацию до тех, кто принимает решения?

Один из вариантов – собрать вместе различные аспекты того, как мы строим, поддерживаем и используем Интернет, и взглянуть на все это с точки зрения экономики и политики. Именно так поступил Центр прикладного анализа данных Интернета (Centre for Applied Internet Data Analysis, CAIDA) при Калифорнийском университете в Сан-Диего, когда учредил семинар по экономике Интернета – WIE (Workshop on Internet Economics). В декабре 2018 года этот семинар проводился в девятый раз, и я предлагаю вашему вниманию мои размышления на затронутые на нем темы. Круг участников семинара был широк и разнообразен (сетевые операторы, сервисные операторы, представители госструктур, экономисты, юристы, ученые и т.д.), дискуссии глубоки и информативны, так что подумать мне было о чем.

Что задало тон этому семинару: мы наблюдаем, как среда становится все более сегментированной и даже сектантской; плюс к тому возрождаются разнообразные торговые барьеры, которые противоречат идеалам мира открытых доступных коммуникаций, открытого для конкуренции и новаторства во всех видах. Традиционный образ публичного пространства в сфере коммуникаций как общественного достояния подвергся атаке со стороны алчных акул частного сектора, которые не покладая рук трудятся над приватизацией этого достояния, изобретая все более изощренные, коварные и извращенные способы это сделать. Даже слежкой за нами и нашими предпочтениями, даже составлением миллиардов личных досье теперь занимается частный сектор, да так, что размаху его деятельности позавидовало бы любое полицейское государство прежних времен. Какова же должна быть роль государства в такой среде? Какую часть этой роли можно (или даже нужно) делегировать частному сектору? Пока непонятно.

С исторической точки зрения те разрушительные изменения в обществе, которые привнесло с собой бурное развитие информационных технологий, по масштабу и глубине воздействия сравнимы с промышленной революцией XVIII-XIX веков; и, возможно, идеи экономиста и революционного социолога тех времен Карла Маркса сегодня стали актуальнее, чем когда-либо прежде. В наше время повальной неопределенности мы задаем себе очень простые вопросы: зачем нужно регулирование и кого следует регулировать? Как можно отличить факты от гипотез? Какими будут установки и догматы общества, рождающегося в результате нынешней цифровой революции?

Эйфория от безграничных возможностей, которые сулило зарождение Интернета, теперь уравновешивается опасениями и страхами. Надежна ли инфраструктура, можно ли ей доверять? Почему у нас никак не получается сделать Интернет безопасным? Почему мы делегируем все больше и больше ролей автоматическим системам, прекрасно понимая, что тем самым повышаем свою уязвимость к системным сбоям, которым ничего не можем противопоставить? Кто на самом деле определяет развитие Интернета, и не попадаем ли мы в заложники узколобого эгоизма нынешних королей рынка?

Очень похоже, что Интернет повторяет историю газетной индустрии, где реклама превратилась в хвост, виляющий собакой. Для Интернета таким хвостом, кажется, стал так называемый наблюдательный капитализм (surveillance capitalism): навязчивое стремление узнать все-все о каждом потребителе, его желаниях и предпочтениях, а главное – о его покупательских привычках. Каков смысл приватности в таком мире? Да и одинаков ли Интернет для всех нас?

Например, Facebook намеренно стремится кастомизировать свою платформу так, чтобы как можно лучше соответствовать желаниям и предпочтениям каждого пользователя. В результате каждый человек видит настроенную под себя социальную среду. А что, если то же самое происходит в других аспектах сети? Уж не видим ли мы лишь то, что, по мнению сетевых систем, мы хотим видеть? Операторы сетевого контента накапливают все больше и больше данных о каждом из нас; а имеем ли мы, как потребители, хоть насколько-то реалистичное представление о том, какой личной информацией расплачиваемся за доступ к цифровым сервисам? Справедлив ли этот обмен? И во что обществу в конечном счете обходится бесплатный поисковый сервис?

Вот в какой обстановке проходил декабрьский семинар.

Безопасность или же ее отсутствие

В вопросах управления безопасностью мы многому можем поучиться у авиационной индустрии. Если не учиться на ошибках в работе со сложными машинами, то эти ошибки неизбежно будут повторяться. Нужно добиться четкого понимания, что именно произошло, когда и почему. Только тогда мы можем извлечь уроки из происшедшего, только тогда можно говорить, что жить действительно стало безопаснее.

Кое-где уже внедрены элементы обязательного оповещения об инцидентах, но единообразием тут и не пахнет. Да и нормы финансовой ответственности сервисных операторов способствуют скорее тому, что инциденты стараются скрывать или сообщать минимум необходимого. А у суровых мер наказания, например закрепленных в европейской системе GDPR, есть неприятный и незапланированный побочный эффект: они осложняют выход на рынок мелким игрокам, которым не по карману платить драконовские штрафы за любое нарушение. Кроме того, карательное мышление, которым продиктованы столь жесткие меры, отнюдь не способствует созданию атмосферы открытости и честности, в которой все инциденты безопасности подвергались бы непредвзятому анализу – независимо от того, имело место формальное нарушение или нет. Поэтому возможность проанализировать ситуацию, понять ее и улучшить качество нашей цифровой инфраструктуры теряется.

Для сравнения, в медицине, например, ситуация обстоит иначе: конфиденциальность истории болезни пациента трепетно соблюдается почти всегда, но стоит вам попасть в больницу с чем-то очень опасным и очень заразным, как начинает действовать новый режим обязательного оповещения. Охрана частной жизни важна, но защита общества от смертоносных эпидемий еще важнее. Так почему не существует подобных правил оповещения об утечках данных? Какой была бы оптимальная политика, которая позволила бы нам понять масштаб угрозы и принять необходимые меры для защиты наших данных?

Говоря о защитных возможностях нашей цифровой инфраструктуры, интересно заметить, что финансовые институты в наше время подвергаются, скажем так, «нагрузочному тестированию». Системообразующие финансовые учреждения проверяются на прочность, чтобы понять: есть ли у них точка отказа и на каком уровне это может случиться. На то они и системообразующие: рухнут они, рухнет и система. А почему мы не делаем подобного в сфере данных, или они для нас не так важны, как деньги? Готовы ли мы публично проводить нагрузочное тестирование целостности и устойчивости данных для ключевых провайдеров? Ибо, как заметил один из участников, «мы вполне способны создавать системы, которыми уже не в состоянии управлять».

Перед нами стоит перспектива формирования политик на основе данных, поэтому назрел вопрос: какие конкретно данные помогут нам оценить надежность нашей цифровой инфраструктуры? Простые метрики не всегда информативны, а информативные часто бывают сложными, неочевидными и дорогостоящими. Возьмем, например, вопрос о том, улучшается или ухудшается ситуация с безопасностью. И как мы будем сравнивать угон 500 миллионов учеток из программы лояльности гостиничной сети с угоном одной-единственной кредитной карты? Может, нужно разработать какую-нибудь метрику серьезности инцидентов безопасности, которая бы принимала в расчет и тяжесть происшествия, и число пострадавших?

Дальше. Как именно нам организовать защиту? Тут уже неважно, от чего: от внутрисистемных сбоев или от злого умысла, - но как ее строить? Ведь немалая часть проблемы с обеспечением безопасности цифровых систем кроется в их сложности. Мы можем обеспечить безопасность отдельных компонентов, но даст ли это безопасность системы в целом? Ведь подобные системы часто отличаются сложным взаимодействием составных частей, что может привести к т.н. хрупкому поведению системы. А без четкого понимания уязвимостей невозможно определить, где именно следует укреплять безопасность системы. Какие активы будем защищать в первую очередь при ограниченных ресурсах? И как можно отличить адекватную защиту от паранойи? Как поймать тот

момент, когда дальнейшие усилия дадут лишь незначительное повышение безопасности?

И как организовать такую защиту? Будет ли это государственная структура, за которую платят налогоплательщики, или частная инициатива, построенная на деньги тех, кто ищет безопасности? А ведь разница между государственной политикой и частной защитной функцией колоссальна. Государственная политика по сути своей ориентирована на то, чтобы арестовать злоумышленника и не допустить нового преступления. А частная функция безопасности существует на деньги потенциальной жертвы и оберегает именно ее. Разница та же самая, что между «нельзя допустить, чтобы такое случилось снова» и «нельзя допустить, чтобы такое случилось со мной». По сути, это небо и земля.

Опыт внедрения мер безопасности

Вопрос безопасности охватывает множество аспектов – от системного обзора до индивидуальной практики, и на семинаре зашла речь, в частности, об опыте внедрения двухфакторной аутентификации (2FA) в сообществе пользователей. В наши дни она, похоже, вошла в моду, и многие сервисные провайдеры внедряют ее по принципу «все побежали - и я побежал».

Эффективность такой меры вызывает вопросы. В какой степени 2FA может противостоять вторжениям? Какова степень сокращения числа вторжений при установке 2FA в системе? Кроме того, усложнение процедуры доступа наверняка приводит к отсеву части потребителей, которые пытаются воспользоваться услугой, – и какова же степень отсева?

По словам докладчиков, в критически важной системе (такой как система учета сотрудников и оплаты труда) вторжений и утечек данных после внедрения 2FA замечено не было. Ситуация с почтовой системой чуть иная: а именно после внедрения 2FA уровень пользования системой заметно упал. Если пользование сервисом необязательно, внедрение 2FA отвадит от него часть пользователей. Все подобные системы представляют собой тот или иной уровень компромисса между простотой использования и потенциальной опасностью. Чем сложнее пользоваться системой, тем чаще ею перестают пользоваться или же находят обходные пути, сводящие на нет смысл и эффект защиты.

Есть и другой тип мер безопасности, носящий более косвенный характер и лежащий в области хорошего управления сетью с маршрутизацией и адресацией. Одним из компонентов нашей уязвимости являются т.н. распределенные атаки вида «Отказ в обслуживании» (DDoS-атаки), при которых втянутые в атаку системы начинают генерировать потоки UDP-пакетов с исходным адресом намеченной жертвы. В ряде протоколов UDP (в частности, для некоторых запросов DNS и запросов memcache) ответ значительно больше запроса. Поэтому небольшой поток триггер-пакетов, направляемых на самые обычные серверы (безопасность которых к тому же не нарушена), может вызвать настоящий потоп данных в адрес жертвы, и ее сеть просто не справится. Важнейший аспект данной конкретной разновидности DDoS-атаки – это возможность генерировать пакеты IP с фальшивым исходным адресом и передавать их по сети. Бороться с возможностью генерировать такие подложные пакеты мы уже практически бросили, поэтому теперь наше внимание обращено на сеть. Можно ли научить ее автоматически отбрасывать пакеты с подложным исходным адресом?

Первоначальная концепция была опубликована 18 лет назад в документе BCP38 (RFC 2827) и с тех пор ничуть не изменилась, как и нежелание сетевых операторов подобную систему внедрять. Проблема в том, что несистематическое внедрение мер, описанных в BCP38, само по себе неэффективно против DDoS-атак на основе подмены исходных адресов в UDP-пакетах (эта практика еще называется IP-спуфингом). Чтобы добиться результата, необходимо внедрить эти меры во всех сетях. CAIDA уже некоторое время проводит эксперимент по обнаружению сетей, пропускающих пакеты с подменой IP-адресов (http://spoofer.caida.org/). Результаты его неоднозначны. Уровень внедрения антиспуфинга в сетях уже несколько лет практически не меняется, а в то же время UDP-атаки с использованием IP-спуфинга не прекращаются, а наоборот, даже участились. Некоторого эффекта удалось добиться с помощью инструментов публичного раскрытия сетей (т.н. метод «позорного столба» – англ. «name and shame»), но, как мы поняли из опыта борьбы с деагрегированием BGP, «позорный столб» работает очень недолго, а дальше внимание к подобным спискам быстро ослабевает.

Можно считать такую ситуацию разновидностью провала рынка: многие отдельные сетевые операторы не видят достаточной выгоды в том, чтобы принять меры против IP-спуфинга, а в результате страдает все общество, поскольку самоочищающуюся от фальшивых пакетов сеть создать не удается. В результате DDoS-атаки на основе спуфинга происходят снова и снова. И что делать – непонятно. Возможно, какая-то перспектива была бы, если бы сетевые операторы несли ответственность за халатность, приведшую к возникновению предотвратимых атак, а страховщики четче прописывали условия, накладываемые на операторов при страховании их от подобных рисков. Но вряд ли это осуществимо в ближайшем будущем. Да и не стоит забывать, что хакеры – ребята очень умные. Они не повторяют раз за разом одно и то же поведение, а ищут новые лазейки. Сегодня быстрее и легче всего организовать DDoS-атаку с помощью спуфинга, но это далеко не единственная уязвимость, и если ее закрыть, то хакеры просто переключатся на другие.

Тезис о невозможности обеспечить безопасность общей системы из-за того, что никому не хочется на это тратиться, применим и к безопасности маршрутизации. Иногда застарелые проблемы остаются проблемами потому, что мало кому нужно их решать. Иногда эти застарелые проблемы трудно решить, потому что для этого требуются скоординированные действия множества сторон, а необходимый уровень координации просто недостижим. Иногда они остаются нерешенными, потому что нам не хватает понимания того, как их решать. Похоже, обеспечение безопасности междоменной системы маршрутизации попадает в одну из последних двух категорий.

Надежные данные для описания этой проблемы найти трудно. Непросто провести грань между преходящими состояниями маршрутизации, случайными ошибками в конфигурации системы маршрутизации и результатами злого умысла. Еще труднее определить масштаб воздействия маршрутизационного инцидента. Маршрутизационная атака, затронувшая популярный онлайн-сервис или же какие-либо важные сервисы, на которые мы полагаемся в жизни и работе, должна, по идее, считаться более серьезным происшествием, чем случайный инцидент, навредивший моим домашним сервисам и ничему больше. Но проблема в том, что система маршрутизации видит только пути и префиксы адресов, никак не дифференцируя их по важности.

Говоря, что перед нами застарелая проблема немалой сложности, я вовсе не утверждаю, что дело не сдвинулось с места. Мы добились подвижек в целом ряде направлений. Например, частью проблемы было отсутствие четкой и проверяемой модели полномочий, которая бы позволяла обладателю IP-адреса подтвердить, что да, сейчас этот адрес используется им, одновременно опровергнув все остальные имеющиеся претензии на обладание этим IP-адресом. Мы создали инфраструктуру открытого ключа (PKI), которая позволяет обладателям IP-адресов подписывать заявления об адресах и их разрешенном использовании, а другим инстанциям – подтверждать такие заявления. Мы разработали стандартную технологическую модель того, как включить такие цифровые подписи в работу протокола BGP и использовать их в работе систем маршрутизации.

Но несмотря на все эти достижения – и поистине титанические усилия, которые для этого потребовались, – мало надежды на то, что безопасный маршрутизационный протокол BGPSEC хоть когда-нибудь получит широкое применение. По общепринятому мнению, этот инструмент сложен до непрактичности, а его использование привносит новый набор операционных рисков, которые в глазах отдельно взятого сетевого оператора перевешивают риск подвергнуться маршрутизационной атаке. К тому же, эта мера решает только часть проблемы, т.е. не обезопасит сеть от всех видов маршрутизационных атак. Похоже, в данном конкретном случае лекарство может оказаться хуже болезни, да и непонятно, излечит оно ее вообще или нет!

И, наконец, есть проблема с ограничениями позитивных подтверждений в структуре безопасности. Позитивные подтверждения опираются на то, что добросовестные игроки могут каким-то образом отмечать свои действия или цифровые артефакты как «хорошие» – так, чтобы игрока было легко опознать, а отметку сложно оспорить. Это работает в предположении, что злоумышленник стремится избежать опознавания или не может заполучить необходимые сертификаты сам. В среде, в которой все добросовестные игроки всегда оставляют такие метки, любой материал без меток явно настораживает. Проблема в том, что в массивных распределенных системах такой поголовный охват – большая редкость. Если метки оставляет лишь часть игроков, непонятно, как расценивать непомеченный материал. О нем просто ничего нельзя сказать. К тому же, неясно, каким образом можно лишить недобросовестных игроков доступа к таким меткам. Фишинговые сайты используют TLS и часто помечаются в браузере таким же зеленым замочком, как и настоящие сайты. Видимая атрибуция и публичная отчетность тоже часто не приносят пользы. Например, прозрачность сертификатов безнадежно неэффективна против краткосрочных веб-атак типа «схватил и беги».

Общий принцип в этой сфере безопасности систем таков: навешивание дополнительных затрат на добросовестных игроков далеко не всегда устраняет возможность появления недобросовестных, а если сумма всех затрат на то, чтобы казаться добросовестным, превышает уровень потерь от краж или мошенничества, то на системном уровне получится, что мы добавили в систему новый элемент неэффективности. В такой обстановке, возможно, было бы проще и дешевле создать общий фонд компенсации за потери и примириться с риском нарушения безопасности.

Так какими же глазами нам смотреть на отсутствие безопасности в маршрутизации? Это технологическая недоработка? Если бы у нас были более совершенные устройства и инструменты, дешевые и эффективные, исчезла бы проблема? Или же это провал рынка? Сетевой оператор не видит достаточной «личной» выгоды в развертывании этих инструментов, поэтому общая выгода так и не достигается. А может, это провал госрегулирования? Если мы хотим заставить сетевых операторов обеспечить безопасность системы маршрутизации, то как нам это сделать? Нынешние примеры национального и регионального регулирования в сфере контента и шифрования просто плачевны. Отраслевые своды правил практически не имеют эффекта, так как их выполнение не проверяется, а потребители в любом случае не ощущают ценности от нововведений. И почему, спрашивается, тот же метод в другой области – в области безопасности маршрутизации – должен сработать лучше?

Изменение экономики Интернета

По различным данным, годовой доход мирового сектора телекоммуникационных услуг оценивается примерно в 1,5 триллиона долларов, что немногим больше мирового энергетического рынка и вдвое выше доходов авиационной промышленности. Сумма очень значительная, но нельзя сказать, что она непропорционально больше, чем у других секторов человеческой деятельности: в конце концов, на телекоммуникации приходится всего лишь 2% мирового ВВП.

Однако компоненты затрат в телекоммуникационной индустрии за последние два десятка лет изменились радикально. В старой формуле телефонной службы «Белла» затраты на обслуживание примерно поровну распределялись между сетью доступа, коммутационным оборудованием и средствами дальней передачи. Эта модель распределения затрат действовала для всех операторов голосовой связи с коммутацией каналов. В наши дни расходы на коммутацию и дальнюю передачу сократились до такого ничтожного уровня, что им можно просто пренебречь. Коммутация

пакетов в разы дешевле, чем старые технологии мультиплексирования с разделением времени и коммутации каналов, а оптоволоконные каналы революционизировали и капитальный, и операционный бюджеты систем связи. Благодаря такому удешевлению коммутации и передачи крупные провайдеры контента и облачных сервисов стали достраивать свои сети прямо до сетей доступа. Расходы на это по сравнению с остальными статьями очень невелики, а строительство своей сети убирает посредника между сервисом и потребителем. Побочным результатом является отток клиентов из сектора передачи, что лишь усугубляет его упадок.

Некоторые операторы связи в этой связи купили провайдеров контента, но, возможно, эта мера лишь отсрочит неизбежное, а не переломит тенденцию. Как мы уже много раз наблюдали на примере самых разных компаний, вставших перед необходимостью трансформироваться, например, грузоперевозчиков в те времена, когда водный транспорт вытеснялся железнодорожным, старая гвардия у руля редко обладает нужными для этого организаторскими способностями, профилем капитала, адекватной поддержкой инвесторов и, не в последнюю очередь, решимостью открыто признать, что нынешний способ зарабатывать деньги отжил свое, чтобы полностью освободиться от прошлого и возродить предприятие в совершенно новом облике. Реликты прошлого во времена бизнес-трансформации часто приводят к странным результатам. Операторы связи, вложившиеся в платформу доставки контента, часто в глубине души так и остаются операторами связи, которым впихнули какой-то совершенно чуждый бизнес.

Трансформация бизнеса – задача очень непростая. Например, одна из нынешних крупных транснациональных корпораций была основана в Австралии как горнодобывающее предприятие, а его владельцы и люди, которые им управляли, были по сути крестьянами. К тому времени, когда профиль руководства и инвесторов изменился, это была уже сталелитейная фирма, управляемая шахтерами. Новый виток изменения – и перед нами нефтяная корпорация под руководством сталеваров. К моменту, когда у руля оказались нефтяники, корпорация стала энергетической. И на каждом шаге развития главным источником волокиты и неадекватного принятия решений было несоответствие профиля деятельности компании профилю ее руководства и инвесторов. Так и подмывает описать нынешние попытки сетевых операторов диверсифицироваться точно так же, как в приведенном примере.

Выход провайдеров контента и облачных сервисов на доминирующие позиции в телекоммуникационной индустрии создал более сложную среду, во многом непрозрачную для внешнего наблюдателя. Потребителю важно качество обслуживания, а оно все больше и больше зависит от происходящего внутри облака распределения контента. Операторы сетей данных контента (CDN) терминируют свои частные сети распределения все ближе к границе клиента и, соответственно, сокращается роль традиционных провайдеров, которые когда-то предоставляли соединение между пользователем и сервисом. Но не стоит забывать, что именно эти провайдеры и их сети передачи исторически служили центрами мониторинга, измерения и регулирования. Чем меньше их роль, тем хуже мы видим эту среду цифровых сервисов.

Понять эту экономику контента – непростая задача. Какие сервисы используются, какие соединения предпочитаются, какой профиль контента генерируется и в какие деньги все это оценить?

Тут уместно поднять еще один старый как мир экономический вопрос: всегда ли существенное укрупнение бизнеса – это плохо? Несомненно, в цифровой экономике доминирует очень малое количество очень больших предприятий. В десятке крупнейших публичных компаний мира по рыночной капитализации – семь корпораций из мира «цифры»: это американские Apple, Alphabet, Amazon, Facebook и Microsoft, китайские Alibaba и Tencent. Да, есть и другие критерии размера, в том числе показатели дохода, прибыли, клиентской базы и так далее, но если брать именно капитализацию, то эти семь компаний из первой десятки, несомненно, большие. Но так ли они страшны? Когда предприятие становится настолько большим, что его крах может стать фатальным для стабильности общества?

Во время глобального финансового кризиса 2008 года мы под новым углом взглянули на концепцию "слишком велик для краха" в финансовой сфере. Раньше эта концепция трактовалась как «великан не падает», теперь же – как «великану нельзя дать упасть, ибо тогда он обрушит все». Вновь и вновь звучало слово «системообразующий». А как быть с поставщиками цифровых сервисов? Уж не являются ли системообразующими, по крайней мере, некоторые из этой семерки... а может, и все?

На заре двадцатого столетия судья Верховного суда США Луи Брэндайс (Louis Brandeis) утверждал, что большой бизнес слишком велик для эффективного управления. По его мнению, рост таких гигантских предприятий до уровня, на котором они становились супермонополиями, и их поведение наносят вред конкуренции, потребителям и прогрессу. Он отметил, что качество продукции таких предприятий снижалось, а цены на нее росли.

Когда крупные компании могут сами формировать под себя правовую среду, эксплуатируя недосмотр госрегуляторов для того, чтобы возложить на себя больше рисков, чем им по силам, а потери переложить на плечи налогоплательщиков, нам стоит очень сильно насторожиться. Если компания оказывается в таком положении просто по факту ее размера, то с Брэндайсом трудно поспорить; а финансовый крах 2008/2009 годов наглядно показал, что наблюдения Брэндайса распространяются и на финансовый сектор. Но говорит ли системное злоупотребление доверием общества в финансовой сфере о том, что в секторе ИКТ (информационно-коммуникационных технологий) дело обстоит так же?

Вспомним, что идеи Брэндайса разделяли не все. Ряд его современников, включая президента Теодора Рузвельта, считал, что в некоторых областях бизнес имеет полное право быть крупным и что такой крупный

Тут уместно поднять еще один старый как мир экономический вопрос: всегда ли существенное укрупнение бизнеса – это плохо? Несомненно, в цифровой экономике доминирует очень малое количество очень больших предприятий. В десятке крупнейших публичных компаний мира по рыночной капитализации – семь корпораций из мира «цифры»: это американские Apple, Alphabet, Amazon, Facebook и Microsoft, китайские Alibaba и Tencent. Да, есть и другие критерии размера, в том числе показатели дохода, прибыли, клиентской базы и так далее, но если брать именно капитализацию, то эти семь компаний из первой десятки, несомненно, большие. Но так ли они страшны? Когда предприятие становится настолько большим, что его крах может стать фатальным для стабильности общества?

бизнес может добиться большей эффективности и более низких цен на продукты и услуги чисто за счет объемов производства. Примером может служить эволюция автомобилестроения и индустрии электроприборов в первой половине XX века: автомобили, холодильники и телевизоры поначалу были дорогой экзотикой, но их производство поставили на поток – и получили продукты, доступные если не всем, то большинству, а потому буквально перевернувшие общество. В те дни администрация США установила над этими корпоративными монстрами госконтроль, но не стала лишать их монополии. *(Речь идет в первую очередь о General Motors и General Electric – прим. ред.)*

Но если других методов надзора, кроме госрегулирования, нет, то уж не позволили ли мы крупным корпорациям дорасти до нерегулируемых размеров? Любая компания, которая может сама задавать для себя правила, а затем повести себя (как нам кажется) безрассудно, может крупно навредить экономике и стабильности общества. Для иллюстрации достаточно упомянуть в одном предложении Facebook и выборы.

Снова процитирую Брэндайса: «Мы полагаем, что не существует и не может существовать таких методов госрегулирования, которые бы устранили угрозу, которая кроется в самой сути частной монополии и непреодолимой коммерческой мощи».

Но если мы все-таки не согласимся с мнением Брэндайса и попробуем создать механизмы госрегулирования, которые обеспечили бы достаточную защиту интересов общества, то имеет смысл сначала как следует изучить ту деятельность, которую мы собрались регулировать. А ее еще попробуй пойми. В мире цифровых сетей все больше и больше трафика данных уходит в тень. Операторы услуг контента используют собственные системы передачи или же вырезают себе целые диапазоны длин волны из физического кабеля. Такой уход трафика с общедоступной платформы коммуникации уже стал распространенным явлением, но этого мало: по тем обрывочным данным, которые доступны нам, можно предположить, что уже сегодня объемы трафика в частных сетях в разы превышают объемы трафика в общедоступном Интернете – при гораздо более высоких темпах роста по сравнению с последним.

Как мы можем опознать различные формы злоупотребления рыночными механизмами, такие как демпинг, намеренное воздействие на рынок или дискриминация в предоставлении услуг, если мы по-настоящему не видим этих теневых сетей? И тем не менее, они очень важны. Они являются движущими силами вложений в инфраструктуру, инноваций и – опосредованно – развития остальной, публичной части сетевых сервисов. Можем ли мы – и хотим ли – найти убедительную причину, чтобы обязать владельцев сообщать (посредством различных обязательных отчетов, измерений и т.д.) о характере использования таких частных сетей и сервисов? Есть ли у нас правовая возможность это сделать, учитывая размер фирм-владельцев? В прошлом мы уже наблюдали, как многие государства пытались перевалить эту задачу на другие юрисдикции, чтобы только не проверять себя на

прочность в плане «а сможем ли мы их заставить подчиниться». Например, антимонопольный процесс против Microsoft прошел в Европе, и все равно с малоудовлетворительным результатом. Даже если мы уверены, что предание характеристик трафика в теневых сетях гласности будет полезно для общества, вдруг окажется, что принудить операторов этих сетей к раскрытию этих данных мы просто не в силах?

Консолидация

Интернет был построен на базе нескольких четко разделенных областей активности, в каждой из которых была очень сильна конкурентная дисциплина. Не просто не было никого одного, кто мог бы доминировать во всей сетевой среде, но даже ни в одном секторе активности не было четко выраженной монополии.

Провайдеры передачи данных не предоставляли платформы, а поставщики платформ не работали с приложениями или контентом.

Процесс подключения пользователя к сервису включал в себя несколько совершенно разных действий, выполнявшихся разными поставщиками. Доменное имя выдавалось регистратором доменных имен, поиск DNS был взаимодействием между приложением-резолвером DNS и сервером DNS, IP-адрес сервиса выдавался реестром адресов, сертификаты для безопасного подключения выдавались сертификационной службой, маршрут подключения был на совести нескольких провайдеров связи, а контент хранился в сети доставки контента, с которой работал провайдер контента. И все это было построено на основе стандартных технологий, почти всегда четко определенных IETF.

По разнообразию элементов сервиса Интернет далеко не уникален: телефонная связь не менее дифференцирована. Главная разница в том, что в телефонной связи все эти элементы управляются телефонным оператором. А в Интернете нет никого, кто организовывал бы доставку сложного сервиса от начала и до конца. Подмывает заявить, что организует все пользователь, но это уже, пожалуй, чересчур. Организация осуществляется с помощью рыночных механизмов, и похоже, что функцию распределения ресурсов берет на себя рынок. Однако у пользователя тоже очень серьезная роль: именно коллективные предпочтения пользователей являются движущими силами на стороне предложения.

Но теперь эта ситуация меняется, и вряд ли к лучшему. Сервисы, предлагаемые пользователю бесплатно, оказывают гигантское влияние на его предпочтения. (О свободе тут речи уже не идет, потому что, по факту, перед нами классический двусторонний рынок, в котором сам пользователь является товаром, передаваемым рекламодателю.) А есть еще и вопрос консолидации инфраструктурных сервисов.

Например, Alphabet управляет не только платформой для интернет-рекламы, но и поисковым механизмом, почтовой платформой, хранилищем документов, общедоступным сервисом преобразования DNS, мобильной платформой, браузером и так далее, и несть им числа. Одна-единственная фирма контролирует множество отдельных видов деятельности. Вопрос с консолидацией заключается в том, остаются ли эти виды деятельности отдельными или же объединяются в один сервис.

Приведем два недавних примера для иллюстрации наших опасений.

Первый пример – это недавняя спецификация предоставления услуги DNS поверх HTTPS (DOH). Сервисом DNS не злоупотреблял только ленивый. Хакеры с помощью DNS отправляют пользователей на подложные сайты, где те становятся жертвами вирусов и мошенничества. Государственные системы контроля контента часто используют ответы DNS, чтобы сделать невозможным (а в реальности – не более чем слегка затруднить) доступ к тем или иным поименованным сервисным точкам. DNS часто применяется для сбора информации о том, что именно делает пользователь, так как любая транзакция в Интернете начинается с преобразования имени в адрес. Наблюдения за запросами DNS конкретного пользователя может оказаться достаточными, чтобы составить его профиль с высокой степенью точности.

Снова процитирую Брэндайса: «Мы полагаем, что не существует и не может существовать таких методов госрегулирования, которые бы устранили угрозу, которая кроется в самой сути частной монополии и непреодолимой коммерческой мощи».

После откровений Сноудена на IETF снизошло откровение, и началась массированная доработка протоколов Интернета, чтобы помешать невольным и в особенности вольным любителям подслушивать. DNS был центральной частью этих усилий, и появилась спецификация DNS поверх TLS – способ замаскировать содержимое запросов и ответов DNS от наблюдателя.

DOH на первый взгляд очень похож на DNS поверх TLS, так как оба протокола используют на проводе очень похожие форматы. Но, и это большое «но»: DOH считает ответы DNS веб-объектами. Их можно кэшировать. Их можно выбирать с упреждением. Быть может, даже встраивать в веб-страницы. А значит, браузер может определить собственную среду DNS, совершенно независимую от платформы, на которой работает браузер, независимую от локального провайдера и даже от DNS, каким мы его знаем. Если браузер может включить функции преобразования имен в собственную работу, то ему не нужна отдельная система преобразования имен – и даже система имен. Он может консолидировать имена и сервисы имен в своем собственном пространстве. А поскольку в наши дни на 80% пользовательских платформ используется Chrome, в руках его владельца – компании Alphabet – оказывается как-то уж очень много власти на рынке. DOH может сделать DNS непрозрачным для внешнего наблюдателя, в том числе для публики и властей, и попробуй определи, что происходит за закрытыми дверями.

Второй пример – использование протокола QUIC. Обычно приложения придерживались традиционной модели, согласно которой распространенные функции возлагались на операционную систему. У ОС есть интерфейсы для работы с локальным хранилищем данных, для различных сетевых сервисов, таких как DNS, а также для сетевых подключений и протоколов, осуществляющих соединение, таких как TCP. TCP передает свои параметры управления потоком открыто, поэтому сетевые операторы могут с помощью т.н. промежуточного ПО менять поведение сеанса TCP и навязывать собственные правила для сеанса. Это может быть очень эффективным способом, скажем так, «дискриминации по типу трафика»: сетевой оператор может практически подавлять запросы к сети от менее приоритетных сеансовых потоков, а другим сеансам предоставлять все, чего они пожелают.

Протокол QUIC, первоначально разработанный Alphabet и реализованный в браузерах Chrome, меняет всю систему. Браузер Chrome теперь содержит собственную реализацию сквозного протокола управления потоком и сам общается с другим браузером Chrome на другом конце соединения. Как он это делает: использует сервис датаграмм IP (UDP) на хост-платформе и внутреннюю инкапсуляцию для поддержки сквозного протокола точно так же, как это делается при реализации TCP в стеке IP. QUIC также защищает сам себя от наблюдения и манипулирования, шифруя свою полезную нагрузку. Таким образом, браузер консолидирует протокол сквозного управления потоком сам в себе, не давая ни операционной системе хоста, ни сети никакой информации о состоянии потока. То есть, подобно DOH, QUIC утягивает протокол сквозного контроля потока внутрь браузера и опускает над ним завесу тайны.

Оба примера описывают более глубокий и, возможно, более коварный тип консолидации в Интернете, чем корпоративные слияния и поглощения, которые мы видели до сих пор. Здесь власть не сосредоточивается в руках отдельных рыночных игроков – здесь объединяются компоненты среды. Большинство таких вещей выходят за рамки привычного госрегулирования, но результаты примерно те же, что и при слиянии корпораций. Два описанных случая консолидации приложений привели к тому, что поставщик браузера значительно укрепил свои позиции на рынке.

Измерения и политика на основе данных

В ряде стран, включая США, в последнее десятилетие предпринимались проекты по измерению потребительского широкополосного доступа в Интернет. Задача была в том, чтобы устранить неопределенность в выборе широкополосных продуктов на потребительском рынке и дать потребителю возможность сравнивать рекламные заявления о характеристиках продукта с фактически зарегистрированными его показателями. Побочным эффектом этих усилий, намеренным или нет, стало появление данных о том, имеет ли место проблема перегрузки сетей доступа и в какой степени приоритизация трафика помогает решать ее для одних типов контента и служб, совершенно не помогая другим. Эти данные помогли участникам дебатов о сетевой нейтральности хоть как-то сориентироваться.

Но стоит нам ввязаться в подобные проекты, станет легко просканировать среду и увидеть множество других возможностей, где данные помогут нам лучше понять рынок и осознать, какой вид госрегулирования (если оно вообще возможно) поможет рынку и в плане защиты потребителя, и в плане общей экономической эффективности. Сегодня мы видим различные сетевые платформы, поделенные на секторы, но с общей фундаментальной инфраструктурой и виртуальным представлением платформы в целом. Сюда относится весь спектр облачных сервисов, API, управления контентом, распределения, сброса нагрузки, шифрования трафика, а также связанные диспетчеры доступности и быстродействия для контента и сервисов. Вопросы относительно характеристик этих сервисов, уровня их использования, их фактического быстродействия, функций ценообразования и эффективности предложения на рынке – все они отражают опасения широкой публики, связанные с первоначальными опасениями касательно рынков широкополосного доступа. Чтобы определить, доросли ли эти опасения до уровня, на котором может потребоваться вмешательство регулятора, необходимо сначала определить метрики для этого сектора и затем заняться сбором данных. Разумеется, любые действия в этом направлении предполагают, что эволюция более широкой стороны предложения на этом рынке контента и цифровых сервисов достигла того уровня, когда его внутренняя структура уже не очень четко видна.

Одна из упомянутых проблем и опасений – вопрос приватности, и,

возможно, потребуется индекс приватности, включающий структурное измерение приватности в обращении с данными пользователей. Такая метрика могла бы измерять степень, в которой различные инфраструктурные сервисы консолидируются в руках небольшого числа игроков. Индексы трафика могли бы описывать объемы трафика, передаваемые по частным, гибридным или общедоступным маршрутам.

Контроль над контентом в Интернете

«Куда бы ты ни шел, от себя не убежишь», – гласит пословица. Но все-таки, как понять, куда мы идем? И как попасть куда надо, если плохо представляешь себе, где ты сейчас?

В наши дни правительства требуют от платформ социальных медиа модерировать размещаемый контент. Они заставляют операторов платформ удалять контент, который считается социально опасным, или ограничивать его распространение. Сторонники модерирования контента утверждают, что социальные медиа в целом недостаточно активно реагируют на опасный контент и вызванный им ущерб. В ответ на такие обвинения компании часто публикуют «отчеты о прозрачности», где указано число полученных жалоб, число удовлетворенных жалоб и так далее. В Германии недавно принят закон NetzDG, согласно которому компании в области социальных медиа обязаны в 24-часовой срок с момента требования удалять контент, противоречащий законодательству Германии, и публиковать отчеты с указанием числа жалоб, числа удалений, числа апелляций и числа восстановлений по итогам рассмотрения апелляций. Первый подобный отчет был опубликован в августе 2018 года. Из него четко видно, что социальные медиа отнеслись к этой мере серьезно настолько, что возникает вопрос о том, не перестарались ли они с цензурой.

Демократические процессы в нашем обществе немыслимы без публичных дебатов, а здесь необходимо понимать тонкую грань между опасным и неоднозначным, между преступным и спорным. Увы, если цензура контента возложена на оператора, он имеет тенденцию удалять все спорное без разбору, в результате чего само представление о спорном в наших глазах меняется: спорными начинают считаться уже гораздо более безобидные вещи. Здесь модель прозрачности по NetzDG ничем нам не поможет, поскольку подобных рубрик в отчетах просто нет. Попробуй разберись, какими стандартами руководствовались платформы при цензуре онлайн-контента. Вопрос этот важен потому, что опыт NetzGD, скорее всего, будет принят на вооружение другими государствами, которые вместо регулирования собственно контента возложат на оператора обязанность публично реагировать на жалобы.

Если все это делается для того, чтобы пользователи чувствовали себя в безопасности, то связь между удалениями и чувством безопасности, увы, не гарантирована. Это очень неоднозначный вопрос, тем более потому, что мы затрудняемся четко сформулировать, чего на самом деле хотим добиться – каким должен быть баланс между свободой слова и подрывным влиянием на общество.

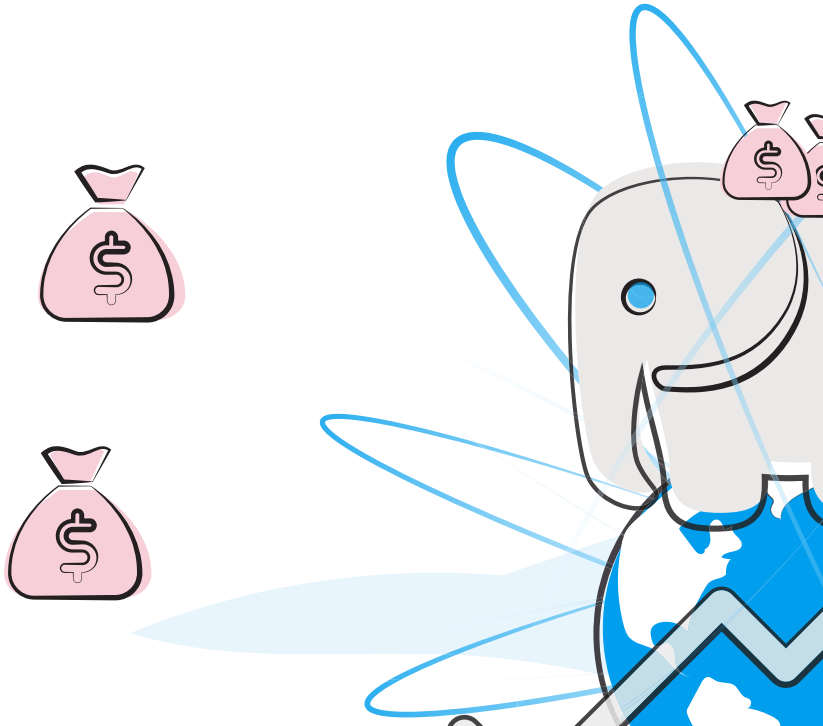
Темная материя в цифровой индустрии

Бесплатные сервисы – загадка для экономистов. Хорошими примерами тут могут служить Wikipedia и различные диалекты Unix, Github и «Яндекс», поисковик Google и сервисы Gmail. В ту же категорию попадает нелицензируемый спектр частот, используемый службами Wi-Fi. Все они активно используются в производстве товаров и услуг, все они могут реплицироваться без ограничений, но не играют роли при определении ВВП. Их не учитывают ни при расчете прибылей, ни при расчете остаточной стоимости.

Игнорируя объективную ценность таких бесплатных услуг, мы рискуем получить перекос в данных и в политиках. Например, как можно вычислить подлинную ценность государственных расходов на НИОКР в экономике, игнорируя стоимость, опосредованно возникающую в производстве технологий с открытым кодом? Насколько будет эффективна наша экономическая политика, если она разработана на основе данных, которые не учитывают объективную ценность бесплатных цифровых товаров и услуг?

Повышается ли продуктивность сектора IT и оценка его ценности в национальной экономике с ростом производства и использования таких бесплатных цифровых товаров? Или, простыми словами, почему в некоторых странах Open Source распространен гораздо больше, чем в других? И есть ли корреляция между этим показателем и эффективностью/ценностью национального сектора ИКТ?

Похоже, большая часть экономических измерений основана на производстве и движении физических товаров и платных услуг, что вполне может быть связано со структурой



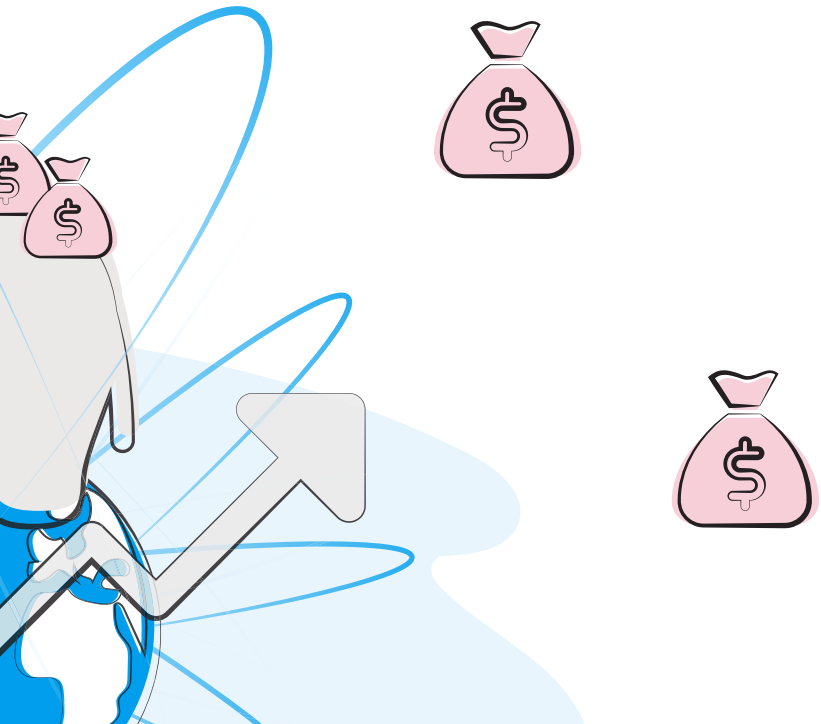
национальных экономик в постиндустриальную эпоху. Интернет привнес в мир концепцию бесплатных услуг, образцом которых являются технологии с открытым кодом, и теперь нам предстоит измерить экономическую ценность таких видов цифровых услуг и включить их в более широкий контекст измерений национальной экономики, чтобы эффективно строить экономическую политику.

Универсальное обслуживание

Одним из краеугольных камней создания телефонной сети был социальный контракт, выраженный в обязательстве оказывать универсальные услуги связи. *(Русский термин взят из ФЗ «О связи», имеется в виду доступность услуг связи каждому гражданину независимо от уровня дохода и места проживания – прим. ред.)* Частные операторы получали лицензию на оказание услуг связи потребителям, но только на определенных дополнительных условиях: их услуги должны были быть доступны каждому и финансово, и географически, включая сельские поселения и отдаленные районы, насколько позволяла техническая возможность. Операторы не могли «снимать сливки», обслуживая лишь богатейших клиентов из районов с самой низкой себестоимостью сервиса. Это повлекло за собой внутреннее субсидирование структурных расходов с тем, чтобы цена услуги оказывалась доступной даже там, где себестоимость заоблачна. Расходы на обслуживание таких районов закладывались в более-менее универсальную цену услуги для всех. Также для этого потребовалось четкое понимание того, что именно представляет собой услуга.

В телефонном мире услуга, грубо говоря, заключалась в том, чтобы передавать человеческий голос разборчиво. Но в сфере широкополосных цифровых сервисов такой основополагающей модели нет. Должны ли мы закладывать в цену услуги расходы на полный охват населения потоковым видео 4K HD? Или предоставить каждому доставку данных на скорости 10 Мбит/с? А может, даже 100? В США Федеральная комиссия по связи (FCC) определяет широкополосный сервис как скорость 25 Мбит/с вниз по течению и 3 Мбит/с вверх. Эти цифры представляют собой компромисс между тем, что можно недорого предоставлять в густонаселенных городах, где можно увидеть цифры в 1 Гбит/с и даже 10 Гбит/с, и возможностями связи в сельской и малонаселенной местности.

Даже если у нас есть цифровые показатели того, что значит "широкополосный доступ", то как нам измерять прогресс в направлении универсальности обслуживания? Подробные карты, на которых обозначаются необслуживаемые точки, крайне трудно компоновать и актуализировать для сельских и удаленных районов. Да и собрав такие данные, как мы можем координировать предоставление услуги, чтобы ни один из сервисов не имел тут зазора – в противовес концентрации на самых выгодных и дешевых в обслуживании районах?



Поддержка измерений Интернета

Все мы согласны, что в основе хорошей политики лежит хорошая информированность, но с тем, как этой хорошей информированности добиться, возникают проблемы. Объективным наблюдателям становится все труднее проводить измерения, и все громче звучат опасения о том, что для независимых измерений Интернет все больше и больше становится «черным ящиком». Если останутся только измерения силами провайдеров, то как оценить их точность, полноту и пригодность в качестве полного и объективного индикатора?

Можем ли мы как-то повлиять на провайдеров, заинтересовать их? Действительно ли наш арсенал ограничен лишь карательными мерами и взыванием к гражданскому долгу, или же есть другие механизмы для того, чтобы подвести надежный фундамент под измерительную деятельность? Неизбежно ли финансировать независимые измерительные платформы из государственного кармана, или же сектор сумеет сам выработать структуру для измерений собственными силами и за собственный счет? Мы достигли того момента, когда хорошо осознаем необходимость в надежном информационном фундаменте для выработки политики, но все еще не добрались до понимания того, как поддерживать саму деятельность по сбору такой информации.

Двусторонние рынки

Многие интернет-предприятия представляют собой двусторонние рынки, обслуживающие сразу и источники контента/приложений выше по потоку, и потребителей ниже. Здесь имеется выраженный эффект сети, когда продавцы предпочитают рынки с большим количеством покупателей, а покупатели – рынки с большим количеством продавцов. Эти предприятия эксплуатируют сетевые экстерналии вида «победитель получает все». Регуляторы признают, что подобные компании контролируют значительную долю рынка, но, как

правило, воздерживаются от санкций на том основании, что потребители получают немедленные и крупные преимущества за счет того, что операторы платформ перенаправляют часть выручки от работы на финансирование потребительских сервисов. Потребители также в плюсе, когда посредники пренебрегают сиюминутной выгодой ради увеличения доли рынка. Но вполне возможно, что терпение публики начинает истощаться, и общественное мнение оборачивается против операторов этих крупных платформ.

Более полная оценка благосостояния потребителей уравновешивает выигрыш для "нижнего" рынка – удобство, экономию, возможности бесплатного пользования, инновации – с истинной ценностью бесплатного сбора данных, их анализа и продажи вверх по течению. Без основательного анализа и верхнего, и нижнего рынков, в том числе и во взаимодействии друг с другом, крайне затруднительно оценить их полную ценность, равно как и невозможно определить, перевешивается ли ущерб от таких крупных платформ, практически искоренивших любую эффективную конкуренцию, объемом предоставляемых ими преимуществ для потребителя.

Наблюдения

Было бы безрассудно считать Интернет зрелым и устоявшимся сектором экономики, он скорее прямая противоположность этому. Его основные характеристики – скорость и усиление. Поведение игроков рынка быстро меняется, и Интернет усиливает многие из этих изменений.

Массовые злоупотребления превратили большую часть Интернета в отравленную пустошь. Любой поставщик интернет-сервисов, которому требуется гарантированная доставка, вынужден прибегать к услугам считанного количества укрепленных до зубов платформ доставки сервисов. Как будто мы снова в XIII веке, и единственное безопасное место – укрепленный замок. Допустимо ли, что в пространстве доставки служб работает лишь горстка крупных провайдеров платформ? Сам факт существования этих защищенных «замков» в качестве прагматического средства противостояния погрязшему в разбойниках Интернету уже можно считать позитивным результатом. Даже то, что строительство и эксплуатация этих замков обходится слишком дорого, чтобы их было много, само по себе не беда. А то, что Интернет работает эффективно и куда лучше, чем раньше – уж точно позитивный результат. Но что случилось с образом информационных технологий и Интернета как двигателя всеобщего социального равенства, дающего людям возможность прямого самовыражения? Этот образ ушел в прошлое, и, возможно, навсегда. И что можно сказать о горстке провайдеров крупных сервисных платформ? Правда ли, что существенное укрупнение бизнеса – это всегда плохо? Похоже, что нет или, по крайней мере, не совсем: в нынешнем Интернете для предоставления сервисов требуются усилия далеко за пределами возможностей мелкого игрока.

Но теперь на пути конкуренции возникли новые барьеры. Складывается впечатление, что для выхода на рынок новый игрок должен заручиться поддержкой одного или нескольких провайдеров крупных платформ, а критерием успеха будет покупка вашего предприятия таким гигантом. За примерами далеко ходить не надо: GitHub, Skype, WhatsApp и так далее. К декабрю 2018 года Alphabet скупила более 220 фирм. Одно из эффективных определений контроля рынка в том и заключается, чтобы диктовать новичкам условия для их выхода на рынок, а здесь практически так и есть: новые игроки могут выжить и процветать только с благословения крупных участников, а не в силу публичной политики, которая поощряла бы конкуренцию в этой сфере.

Быть может, пришло время просто принять это как данность и закрыть тему? Если Интернет – вотчина горстки гигантов, то, может, хватит тешить себя иллюзиями, что мы в конкурентной среде, и перестать строить государственную политику на основе самообмана?

С другой стороны, признание, что наш цифровой мир вращается вокруг кучки монополий, еще не означает, что так и надо, и проблемы никакой нет. Теория монополий и антимонопольное законодательство основаны на представлениях о стагнации рынка, где монополия противодействует развитию и любым изменениям, будучи заинтересованной лишь в укреплении своих позиций. Монополии вчерашнего дня были в буквальном смысле гигантами с огромным числом работников, большими капиталовложениями и зашкаливающим уровнем воздействия на общество. Сегодняшние интернет-гиганты не такие: структуры связей с заказчиками стали гораздо более плоскими, а потому относительно небольшая фирма (по числу работников и капитальных активов) может за счет развитых технологий поддерживать отношения с миллиардами заказчиков по отдельности. Конкурентное преимущество ей дает именно технологическая продвинутость, а права интеллектуальной собственности защищают ее от попыток организовать конкуренцию. Услуги и цены формируются с помощью баланса двух рынков, где массовый клиент на одном рынке приводит массового клиента на другом за счет эффекта сети. Мы достигли момента, когда эти предприятия не могут быть напрямую заменимы или подвержены давлению регуляторов без риска значительного общественного воздействия. В общем, не стоит быть так уверенными, что старые методы окажутся эффективными в новом мире.

Так что, будем рвать на голове волосы? Признаем импотенцию государственной политики в этой области? Ощутим себя во втором «позолоченном веке» *(эпоха быстрого роста экономики и населения США после гражданской войны и реконструкции Юга - прим. ред.)*, где новые гиганты пишут законы и правила для всех? Это ведь не означает, что законов и правил не будет, они просто будут писаться меньшинством для большинства.

Или все-таки не все так мрачно? Не зря же, например, Alphabet в 2017 году потратил на лоббирование американских политиков 18 миллионов долларов: настолько серьезно Alphabet относится к вопросам формирования политики. *(Чисто на всякий случай: в США лоббирование четко отличается от коррупции, поэтому потраченные на лобби суммы подлежат строгому учету и разглашению, а сами политики из них не получают ни*

Об авторе

Джефф Хьюстон (Geoff Huston), B.Sc., M.Sc. – главный исследователь APNIC, региональной интернет-регистратуры, обслуживающего Азиатско-Тихоокеанский регион.

копейки (хотя пожертвовать деньги на предвыборную кампанию нужного политика в рамках лобби – обычное дело). Институт официального лобби, кстати, и возник в попытке вывести политиков из-под негласного влияния крупных корпораций, о котором автор говорит в предыдущем абзаце – прим. ред.) Значит, игроки в индустрии еще не считают себя выше государства и общества, а это хороший знак. Проблема в том, чтобы найти точку воздействия, которая давала бы выгоду для общества в целом, укладываясь при этом в процедуры большой политики. А это отнюдь не просто. Перенос политических дебатов в Twitter, попытки «простыми словами» уложить сложные проблемы в 140-символьное прокрустово ложе толковых результатов не дадут. Сложные задачи требуют обдуманных политических решений.

Не уничтожает ли наблюдательный капитализм рыночную экономику? Она основана на том, что рынок достаточно насыщен для того, чтобы выбор был и у продавца, и у покупателя. Проблема с сегодняшней ситуаций в том, что анонимность позволяет прогибать цены и срывает нормальную работу рыночных механизмов. Рынки приняли на себя функцию распределения ресурсов в экономике всего два века назад, и Карл Маркс был одним из первых, кто изучил и описал это явление. Его энтузиазм взгляда на рынок как эффективный механизм распределения ресурсов даже больше, чем у Милтона Фридмана. Если подорвать работу рынка по распределению ресурсов, пострадает социальная справедливость. Продолжая эту мысль, можно прийти к выводу, что GDPR – это лишь небольшой шаг, и нам следует пойти дальше, принудить сборщиков информации о пользователях и их клиентов открыто раскрывать сведения о своих транзакциях и сделках. А почему бы и нет? Почему бы не постановить, что пользователь обладает правами собственности на свои личные данные, а потому для таких сделок должно требоваться его явное согласие?

Измерение консолидации – тоже непростая задача. Например, несколько лет назад два американских поставщика канцтоваров, Staples и Office Depot, решили объединиться, чтобы противостоять оттоку клиентов в Amazon. Министерство юстиции США такие горизонтальные слияния, как правило, не одобряет, поэтому разрешения не дало. Результат понятен: ни одна из компаний не может в одиночку конкурировать с Amazon по объемам, поэтому обе сейчас в очень трудном положении из-за экспансии Amazon. С другой стороны, не факт, что следовало разрешать покупку WhatsApp «Фейсбуком», так как сочетание социальной сети и мессенджера еще больше упрочивает позицию Facebook с его гигантской пользовательской базой, превращая его в еще более выгодную платформу цифровой рекламы. Аргументы за и против при разрешении или запрете слияний зависят от прогноза результата, а для точного прогнозирования нужны точные данные.

Во времена фундаментальных перемен знание того, как был устроен старый мир, не всегда может нам помочь. Цифры ВВП, не учитывающие подлинную экономическую ценность бесплатных услуг, не могут служить основой для решений. Коммерческие фирмы работают одновременно в нескольких секторах, и эффект сети создает плодотворную почву для роста доминантных игроков, способных взять свой сектор экономики под контроль. А мы прокладываем свой путь в этом мире с помощью набора политик, который стремится уравновесить интересы общества с интересами частного сектора. Но для того, чтобы выработать информированный, релевантный и эффективный процесс формирования политики, нам нужно понять, каков он, этот изменившийся мир. Мне представляется, что в нем открытые измерительные платформы и открытые наборы данных стали еще важнее, чем когда-либо. Нам необходимы общедоступные измерения, которые были бы объективны, точны, полны и, разумеется, беспристрастны – только тогда у нас есть надежда на справедливое и эффективное функционирование рынков.

От всего сердца благодарю устроителей семинара, CAIDA и Массачусетский технологический институт (MIT) за приглашение. Это были два поистине захватывающих дня!

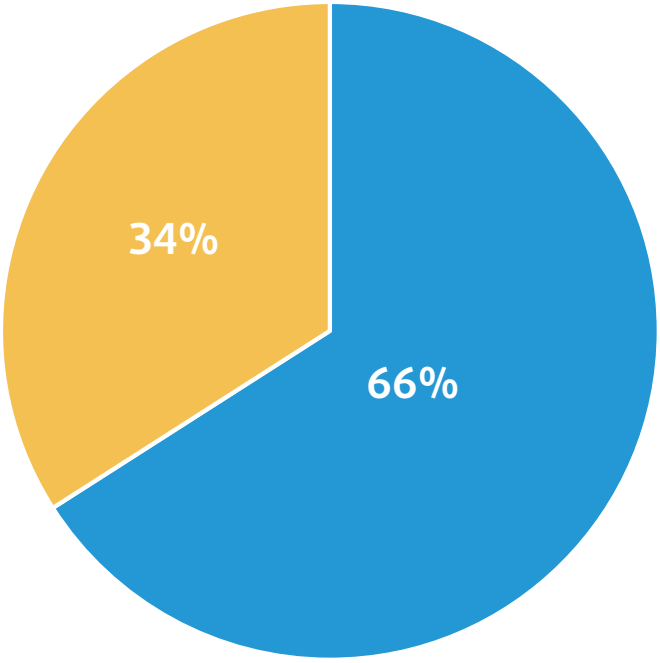
Источник: Internet Economics, http://www.potaroo.net/ispcol/2018-12/wie18.html

Оговорка

Изложенные выше воззрения могут не совпадать с позицией Asia Pacific Network Information Centre.

СТАТИСТИКА ПО ВЕБ-УЗЛАМ

66% ВСЕХ РОССИЙСКИХ СЕТЕЙ РАЗМЕЩАЮТ ВЕБ-УЗЛЫ

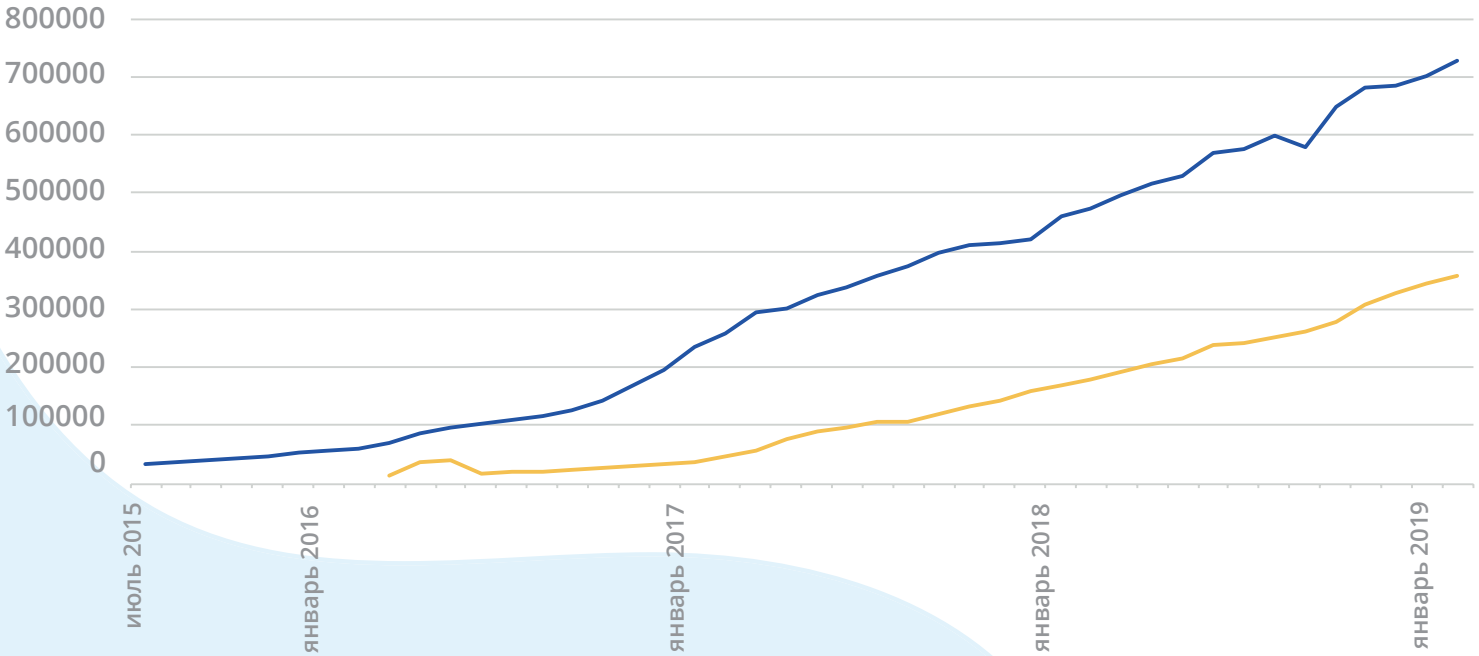


Число оконечных российских AS веб-узлов

Прочие российские AS

Источник: Ididb.ru (Фонд «ИнДата»)

ПОДДЕРЖКА ШИФРОВАНИЯ ДАННЫХ РОССИЙСКИМ ВЕБ-УЗЛАМИ



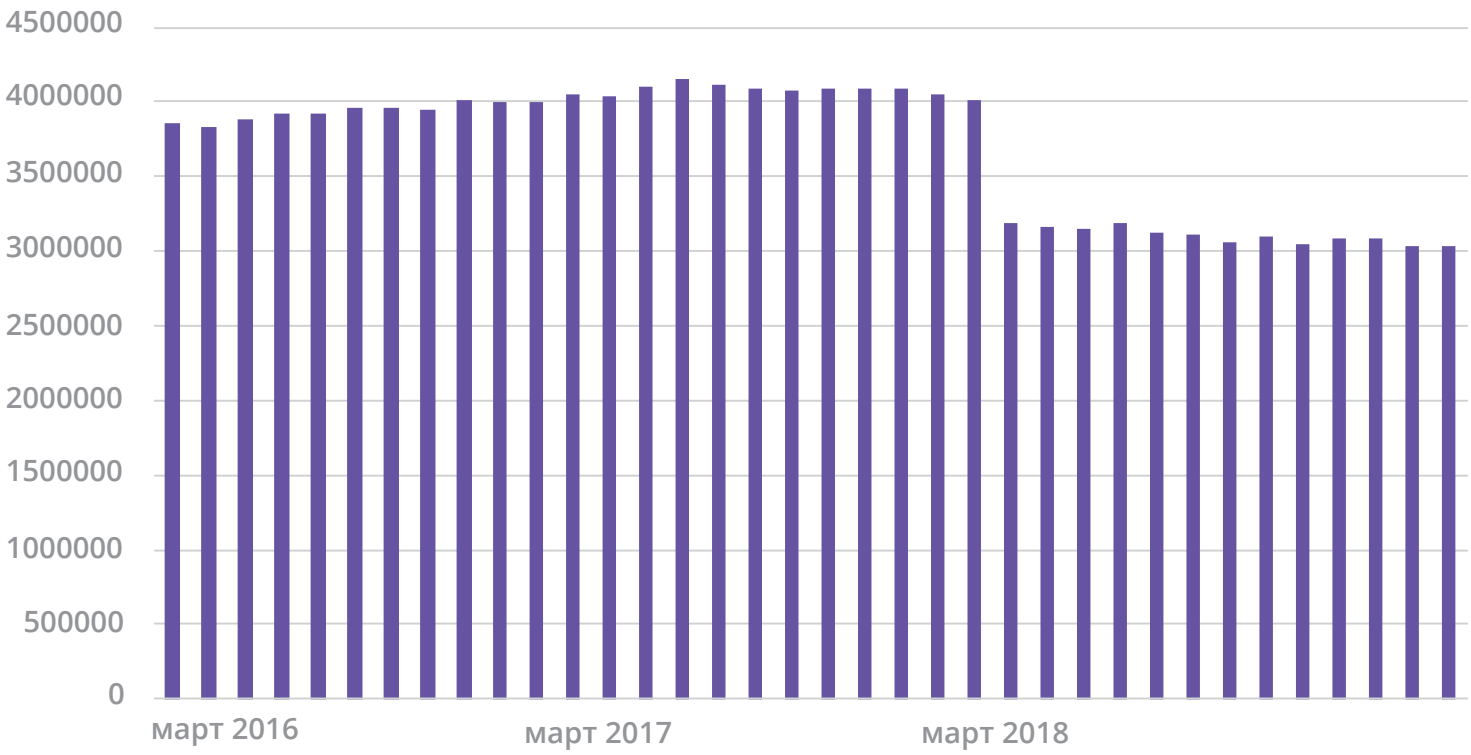
Домены, адресующие веб-узлы с редиректом HTTP -> HTTPS

Число TLS-узлов, адресуемых именем второго уровня, в .ru

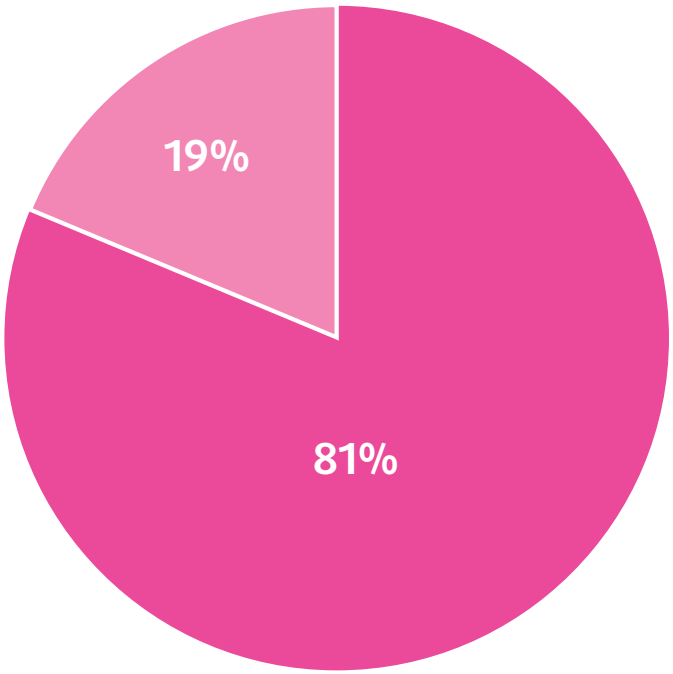
Источник: statdom.ru

ЧИСЛО ВЕБ-УЗЛОВ*

Источник: statdom.ru



ПОДДЕРЖКА IPV6 РОССИЙСКИМИ ВЕБ-УЗЛАМИ



Веб-узлы с доступом по IPv6

Общее число веб-узлов

Источник: statdom.ru

*В феврале 2018 была изменена методика подсчёта доменных парковок и HTTP-редиректов

Что происходит в IETF: устойчивость инфраструктуры и DNS

Андрей Робачевский

Давайте посмотрим, что происходит в IETF в области устойчивости интернет-инфраструктуры и DNS. Многие разработки IETF попадают в эту категорию, но здесь я хотел бы взглянуть на область маршрутизации, а именно на ее защищенность, на область передачи данных, в частности, нежелательного трафика атак распределенного отказа в обслуживании (DDoS). После откровений Эдварда Сноудена область DNS обрела вторую жизнь в IETF. Основная работа направлена на решение задачи конфиденциальности этой фундаментальной интернет-услуги.

Маршрутизация, ее устойчивость и защищенность

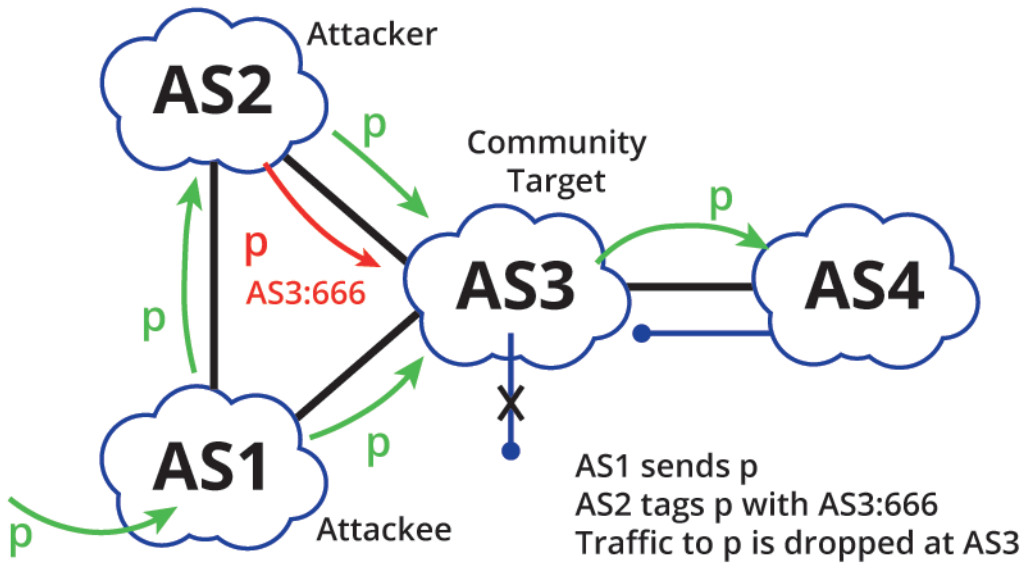
Сегодня в IETF можно увидеть много новых идей, особенно оперативного характера, направленных на повышение защищенности и устойчивости инфраструктуры Интернета, поэтому я хотел бы представить некоторые из них вам. Стандартный путь предложить решение проблемы в IETF и пригласить специалистов к его обсуждению – это направить т.н. интернет-проект, или Internet Draft (I-D). Но имейте в виду – I-D не обязательно указывает на одобрение IETF, тем более что он является стандартом, и может даже не привести к какой-либо работе в IETF.

Итак, давайте посмотрим на то, что происходит в краю BGP.

Могут ли сообщества быть вредными?

Да, если речь идет о «сообществах» BGP (BGP community). В недавней научной статье «BGP Communities: Even more Worms in the Routing Can» (https://dl.acm.org/citation.cfm?id=3278557) авторы демонстрируют, что сообщества BGP могут использоваться удаленными сторонами для влияния на маршрутизацию непреднамеренным способом. Частично из-за своей плохо определенной семантики сообщества BGP часто распространяются гораздо дальше, чем один

Рис. 1. Терминирование трафика с использованием BGP community без захвата префикса.*



*— Источник «BGP Communities: Even more Worms in the Routing Can» (https://dl.acm.org/citation.cfm?id=3278557)

маршрутный скачок, хотя их предполагаемая область действия обычно ограничена соседними автономными системами (Autonomous system, AS). Как следствие, удаленные злоумышленники могут использовать сообщества BGP для запуска удаленного терминирования (blackhole), управления трафиком и манипулирования маршрутами даже без захвата префиксов. См. рисунок 1.

...Как следствие, удаленные злоумышленники могут использовать сообщества BGP...

Проблема плохо определенной семантики усугубляется тем фактом, что текущие реализации маршрутизаторов непоследовательно манипулируют сообществами BGP и особенно «общеизвестными» сообществами (well-known communities). В нескольких популярных реализациях BGP есть различия в результатах команды set. Например, в ОС Junos производителя Juniper Networks команда «community set» удаляет все полученные сообщества, общеизвестные или нет, в то время как в IOS XR Cisco команда «set community» удаляет все полученные сообщества, кроме нескольких.

Проект I-D «Well-Known Community Policy Behavior» (https://datatracker.ietf.org/doc/draft-ietf-grow-wkc-behavior) описывает текущие поведенческие различия, чтобы помочь операторам в создании согласованной политики манипуляции сообществами в среде гетерогенного оборудования от многих производителей, а также для предотвращения введения дальнейших расхождений в реализации.

Была ли в вашей сети ситуация, когда соседняя сеть внезапно огорошила ваш пограничный маршрутизатор гораздо большим числом маршрутов, чем вы ожидали, вызывая истощение ресурсов и другие проблемы?

В документе также содержится настоятельный призыв к операторам сетей никогда не полагаться на предполагаемую политику обработки BGP-community соседней автономной системы. Например, прежде чем объявлять префиксы с NO_EXPORT или любым другим сообществом соседней сети, оператор должен подтвердить с этим соседом, как это сообщество будет обрабатываться.

BGP Large Communities в среде IXP

Некоторые сети участвуют в нескольких точках обмена траффиком (IXP), чтобы улучшить связность и оптимизировать маршрутизацию. Также распространено, что в случае использования сервера маршрутизации (Route Server, RS) для реализации многосторонних пиринговых отношений BGP Large Communities используются для инструктирования RS, как обрабатывать анонсы (например, не рекламировать определенную сеть) или предоставлять участникам дополнительную информацию, например, статус проверки RPKI.

I-D «BGP Large Communities applications for IXP Route Servers» (https://datatracker.ietf.org/doc/draft-adkp-grow-ixpcommunities) пытается документировать часто используемые BGP Large Communities, чтобы упростить согласованность их использования для множества IXP.

Создание более надежной политики маршрутизации с максимальным пределом числа анонсируемых префиксов

Была ли в вашей сети ситуация, когда соседняя сеть внезапно огорошила ваш пограничный маршрутизатор гораздо большим числом маршрутов, чем вы ожидали, вызывая истощение ресурсов и другие проблемы?

В документе «BGP Maximum Prefix Limits» (https://datatracker.ietf.org/doc/draft-sa-grow-maxprefix) описываются механизмы, позволяющие уменьшить негативное влияние неправильной конфигурации такого типа. Вместо общего ограничения, которое может быть настроено на количество префиксов, полученных от соседней сети, как определено в спецификации BGP (https://tools.ietf.org/html/rfc4271), предлагается более детальная схема с тремя контрольными точками для смягчения негативного эффекта:

- **Предел числа префиксов на входящие анонсы, до применения какой-либо политики (например, фильтрации).** Эти ограничения особенно полезны, чтобы помочь смягчить последствия утечки полной таблицы маршрутов и исчерпания памяти, когда реализация хранит отклоненные маршруты.
- **Предел числа префиксов на входящие анонсы после применения политики импорта.** Они полезны для предотвращения истощения FIB и предотвращения случайного прерывания сеанса BGP из-за префиксов, которые в любом случае не приняты политикой.
- **Предел числа префиксов на исходящие анонсы.** Достижение этого предела инициирует прекращение сеанса BGP с соседней сетью. Такие ограничения полезны, чтобы помочь смягчить негативные последствия неправильной конфигурации локальной политики. Во многих случаях было бы более желательно разорвать сеанс BGP, чем наводнять соседей неправильно настроенными анонсами.

Эти рекомендации взяты из более широкого подхода, представленного Job Snijders на конференции RIPE77 в прошлом году - https://ripe77.ripe.net/wp-content/uploads/presentations/59-RIPE77_Snijders_Routing_Policy_Architecture.pdf. См. рисунок 2.

Использование RPKI в рамках проверенной операционной практики

Общепринятым методом обеспечения того, чтобы клиенты объявляли только свои собственные сети и сети своих клиентов, является создание префиксных фильтров.

В случае, когда существуют только прямые взаимоотношения с клиентами (то есть клиенты сети являются «тупиковыми сетями»), задача относительно проста - нужно собирать префиксы, законно анонсируемые этими сетями. Чаще всего это делается с помощью выборки из регистратуры маршрутизации IRR и сбора соответствующих объектов «route». Однако внедрение RPKI может оказаться более надежной альтернативой, предоставляя криптографически проверяемый объект ROA (Route Origin Authorization), который служит аналогичной цели.

Если вы являетесь более крупной сетью и некоторые из ваших клиентов также предоставляют услуги транзита для небольших сетей, задача будет более сложной. Как определить, кто является клиентами ваших клиентов и так далее?

Чтобы помочь с этой задачей, существует специальный объект IRR - «as-set». Этот объект представляет собой список номеров AS - ASN или других объектов «as-set», - которые определяют «клиентский конус» конкретной AS.

Однако когда речь идет о RPKI, у оператора нет такой возможности ввиду отсутствия необходимой информации, предоставляемой объектом «as-set», что затрудняет создание значимых префиксных фильтров для собственного «клиентского конуса».

I-D «RPKI Autonomous Systems Cones: A Profile To Define Sets of Autonomous Systems Numbers To Facilitate BGP Filtering» (https://datatracker.ietf.org/doc/draft-ietf-grow-rpki-as-cones) пытается решить эту проблему путем введения нового объекта аттестации RPKI, называемого AS-Cone. AS-Cone - это объект с цифровой подписью, целью которого является предоставление операторам возможности определять набор непосредственных клиентов, или транзитных сетей со своими клиентами, облегчая построение префиксных фильтров для данной сети с использованием технологии RPKI.

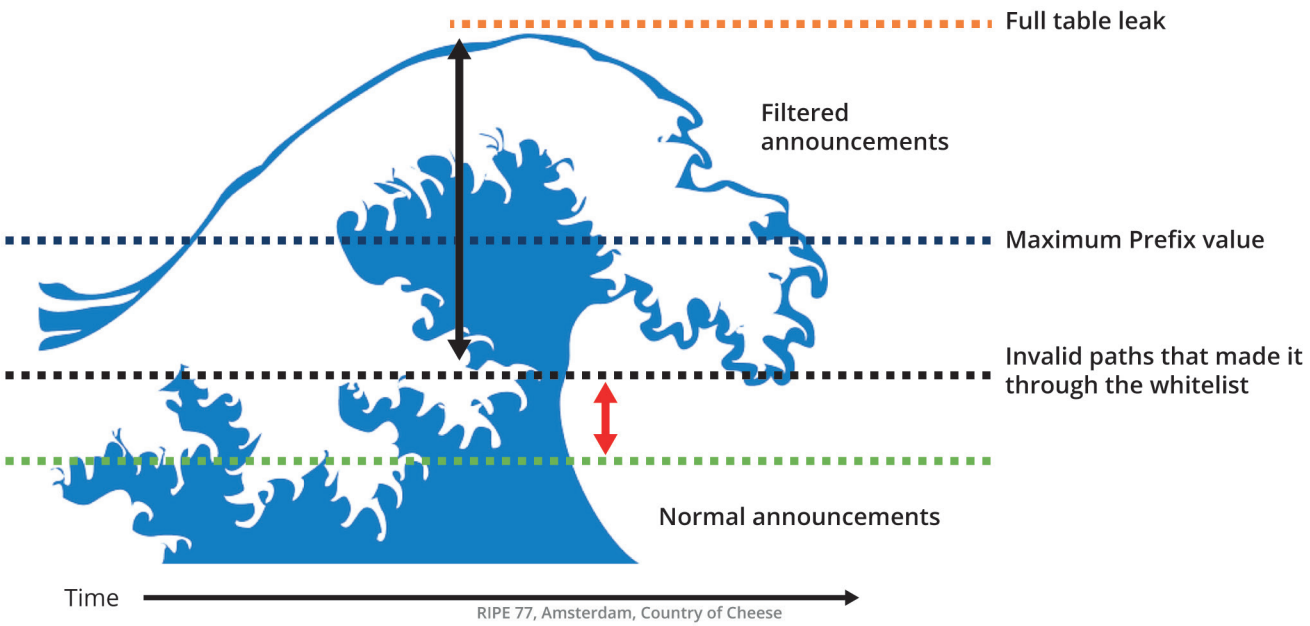
Используя RPKI, AS-Cone также решает фундаментальную проблему с традиционными объектами «as-set»: одно и то же имя объекта «as-set» может существовать в нескольких регистратурах IRR, и проверяющая сторона не обязательно знает, какой «as-set» принадлежит какой сети, и какой следует использовать.

Улучшение проверки AS-PATH

Протокол маршрутизации BGP был разработан без механизмов для проверки атрибутов BGP. Возможность манипулировать одним из них - AS_PATH - создает одну из серьезных уязвимостей системы интернет-маршрутизации. BGPsec был разработан для решения проблемы корректности AS_PATH.

Но, по словам авторов нового I-D «Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization» (https://datatracker.ietf.org/doc/draft-azimov-sidrops-aspa-

Рис. 2. Проблема использования предела после применения политики импорта.**



**— Во многих случаях число префиксов, прошедших через фильтры, все же выше предела, что вызывает прекращение сеанса. В то же время, этот подход связан с большим риском исчерпания ресурсов маршрутизатора. Источник: https://ripe77.ripe.net/wp-content/uploads/presentations/59-RIPE77_Snijders_Routing_Policy_Architecture.pdf

verification/), даже оставляя в стороне сложность BGPsec, необходимость поддержки «небезопасного» BGP позволяет злоумышленнику провести атаку с понижением уровня защищенности, чтобы свести на нет всю работу подписывания AS_PATH.

Авторы предлагают более прагматичный подход, который может помочь использовать преимущества RPKI без необходимости повсеместного развертывания BGPsec. Идея заключается в том, что любая AS может объявлять своих восходящих провайдеров и пиров - сети, которые могут распространять анонсы этой AS. Чем больше сетей это будет делать - тем больше будет шансов обнаружить неправильную конфигурацию (вредоносную или нет).

В проекте определяется семантика объектов авторизации провайдеров автономных систем (Autonomous System Provider Authorization, ASPA), которые должны стать частью RPKI. ASPA - это объекты с цифровой подписью, которые связывают ASN провайдера с номером AS клиента и подписываются владельцем AS клиента. ASPA подтверждает, что владелец AS клиента (CAS) уполномочил конкретный AS провайдера (PAS) распространять анонсы клиента далее, например, анонсируя их восходящим поставщикам или пирам провайдера.

Хотя сама информация о доменном имени является общедоступной, транзакции, выполняемые хостами... представляют собой массивные дополнительные данные, некоторые из которых имеют существенные последствия для конфиденциальности.

Смягчение DDoS-атак

Распределенные атаки отказа в обслуживании (DDoS-атаки) - это постоянная и растущая угроза в Интернете. А поскольку DDoS-атаки быстро развиваются с точки зрения объема и сложности, требуется более эффективное сотрудничество между жертвами и сторонами, которые могут помочь в смягчении таких атак. Способность быстро и точно реагировать на начинающуюся атаку, передавая точную информацию поставщикам услуг по снижению риска, имеет решающее значение.

Решение этой проблемы – в этом состоит задача рабочей группы DOTS (DDoS Open Threat Signaling, http://datatracker.ietf.org/wg/dots/). Целью DOTS является разработка основанного на стандартах подхода для сигнализации в реальном времени связанных с DDoS телеметрии, а также запросов обработки угроз и данных между элементами, связанными с обнаружением, классификацией, отслеживанием и смягчением атак DDoS. Этот протокол должен поддерживать запросы на услуги по смягчению последствий DDoS и обновления статуса через межведомственные административные границы.

Другим интересным случаем, приобретающим все большую важность, особенно с появлением потребительских устройств Интернета вещей (IoT), является снижение DDoS-атак, исходящих из домашней сети. I-D «Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Call Home» (https://datatracker.ietf.org/doc/draft-reddy-dots-home-network) предлагает решение для этих случаев. Это расширение протокола сигнального канала DOTS позволит серверу DOTS инициировать безопасное соединение с клиентом DOTS, который в свою очередь сможет передать информацию о трафике атаки на сервер DOTS.

В типичном сценарии развертывания сервер DOTS является частью клиентского оконечного оборудования (CPE), а клиент DOTS находится в сети ISP. В этом случае сервер DOTS в домашней сети инициирует запрос в мирное время, а затем впоследствии клиент DOTS в среде ISP может инициировать запрос на смягчение, когда провайдер обнаруживает, что в домене сервера DOTS есть атака от скомпрометированного устройства. Впоследствии сервер DOTS будет использовать информацию о трафике DDoS-атаки для идентификации скомпрометированного устройства в своем домене, запускающего DDoS-атаку, может уведомить администратора сети и предпринять соответствующие действия по смягчению последствий (например, для помещения в карантин скомпрометированного устройства или блокировки его трафика для атаки цели, пока запрос на смягчение не будет отозван).

Конфиденциальность в DNS и ее последствия

Будь то посещение веб-сайта, обмен почтовыми сообщениями или общение в социальной сети, для определения фактического нахождения ресурса, а именно его IP адреса, необходима система DNS. Эта система обеспечивает трансляцию имени ресурса (например, facebook.com) в его IP-адрес (например, 2a03:2880:f129:83:face:book::25de), необходимый для установления связи. Таким образом, транзакции DNS могут быть связаны с приложениями, которые мы используем, с сайтами, которые мы посещаем, а иногда даже с людьми, с которыми мы общаемся.

Хотя сама информация о доменном имени является общедоступной, транзакции, выполняемые хостами - запросы, которые они выполняют, и имена, которые они пытаются транслировать, - представляют собой массивные дополнительные данные, некоторые из которых имеют

существенные последствия для конфиденциальности. То, что ищет пользователь или группа, может многое сказать об этом пользователе или группе.

К сожалению, DNS не использует никаких механизмов для обеспечения конфиденциальности этих транзакций, и поэтому соответствующая информация может легко регистрироваться операторами резолверов DNS и серверов имен, а также может быть перехвачена другими. Дискуссия о последствиях DNS для конфиденциальности тесно связана с тем, в какой степени такая информация может быть легко доступна другим, возможно, мошенническим организациям.

Вообще говоря, в DNS существует два типа взаимодействий: а) между пользовательским компьютером (через системное приложение, называемое резолвером-заглушкой, stub resolver) и рекурсивным резолвером, и б) между рекурсивным резолвером, который обычно находится в сети сервис-провайдера пользователя и выполняет рекурсивные запросы DNS от имени пользователя, и авторитетным сервером, содержащим информацию, относящуюся к запросу. Во избежание перехвата DNS-транзакции должны быть зашифрованы и аутентифицированы, но масштаб двух типов взаимодействий (stub resolver с рекурсивным резолвером и рекурсивный резолвер с авторитетными серверами) сильно отличается.

Защита транзакций DNS между резолвером-заглушкой и рекурсивным резолвером требует только одного доверительного отношения между двумя системами, и, таким образом, процедура начальной загрузки (например, настройка секретных ключей или сертификатов в преобразователе-заглушке) проста. Однако для обеспечения безопасности транзакций между рекурсивным резолвером и всеми авторитетными серверами имен требуется большое количество доверительных отношений (по одному между каждым рекурсивным резолвером и каждым авторитетным сервером имен) и, таким образом, требуются более сложные решения и более скоординированные усилия для развертывания решения (например, инфраструктуры открытого ключа).

Это и вопросы производительности являются основными причинами, по которым основная работа в области конфиденциальности DNS направлена на защиту транзакций между резолвером-заглушкой и рекурсивным резолвером. Однако рабочая группа DPRIVE была недавно реорганизована для рассмотрения этого аспекта.

IETF использует два основных подхода для повышения конфиденциальности транзакций DNS:

- минимизация имени запроса (Query Name Minimisation) для уменьшения количества (частных) данных, которые несет запрос, и
- шифрование транзакций между резолверами-заглушками и рекурсивными резолверами, чтобы предотвратить прослушивание этих данных третьими лицами.

Работа над этими двумя областями не сильно пересекается, поскольку минимизация имени запроса направлена на уменьшение утечки информации, которая происходят, когда рекурсивный резолвер повторно отправляет исходный запрос несколько раз в процессе рекурсивной трансляции имени DNS. С другой стороны, ряд альтернативных попыток направлен на повышение конфиденциальности транзакций DNS между резолверами-заглушками и рекурсивными резолверами.

Минимизация информации

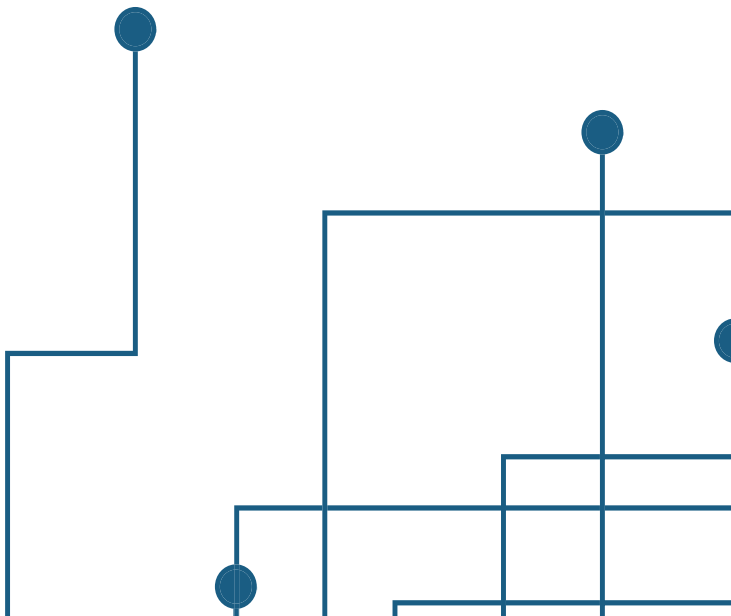
Минимизация QNAME - это экспериментальное предложение, документированное в RFC7816 «DNS Query Name Minimisation to Improve Privacy» (https://datatracker.ietf.org/doc/rfc7816/), которое направлено на минимизацию объема информации, отправляемой в запросах DNS. Вместо повторной отправки одного и того же DNS-запроса на каждый авторитетный сервер имен, минимизация QNAME требует, чтобы рекурсивный резолвер учитывал иерархию DNS, запрашивая необходимые данные (обычно - записи авторитетных серверов дочернего домена) только для имени соответствующего уровня, начиная с домена верхнего уровня, и увеличивая один уровень в глубину домена для каждого последующего запроса. Например, для трансляции имени www.example.ru резолвер обратится к корневому серверу с запросом для имени «ru», и так далее.

В области шифрования IETF фокусируется на двух основных технологиях:

DNS через TLS (DoT)

RFC7858 «Specification for DNS over Transport Layer Security (TLS)» (https://datatracker.ietf.org/doc/rfc7858/) определяет, как установить связь с рекурсивным резолвером по защищенному соединению TLS. Однако этот подход также может быть применен для улучшения свойств конфиденциальности транзакций между рекурсивными резолверами и официальными серверами.

Протокол DoT использует отдельный номер порта, порт TCP 853, а не существующий порт службы DNS (53). Рекурсивные резолверы могут быть аутентифицированы с помощью ключа SPKI (подробности см. в разделе 3.2 и разделе 4 RFC7858).



DNS через HTTPS (DoH)

RFC8484 «DNS Queries over HTTPS (DoH)» (https://datatracker.ietf.org/doc/rfc8484/) определяет, как отправлять и получать DNS-запросы по HTTPS. Настройка сервера выполняется отдельно, а соединение с резолвером защищено, как и любой другой HTTPS-трафик. DoH в основном нацелен на веб-браузеры и вряд ли сможет быть применен для улучшения свойств конфиденциальности транзакций между рекурсивными резолверами и авторитетными серверами имен. Вот где начинается некоторое противоречие.

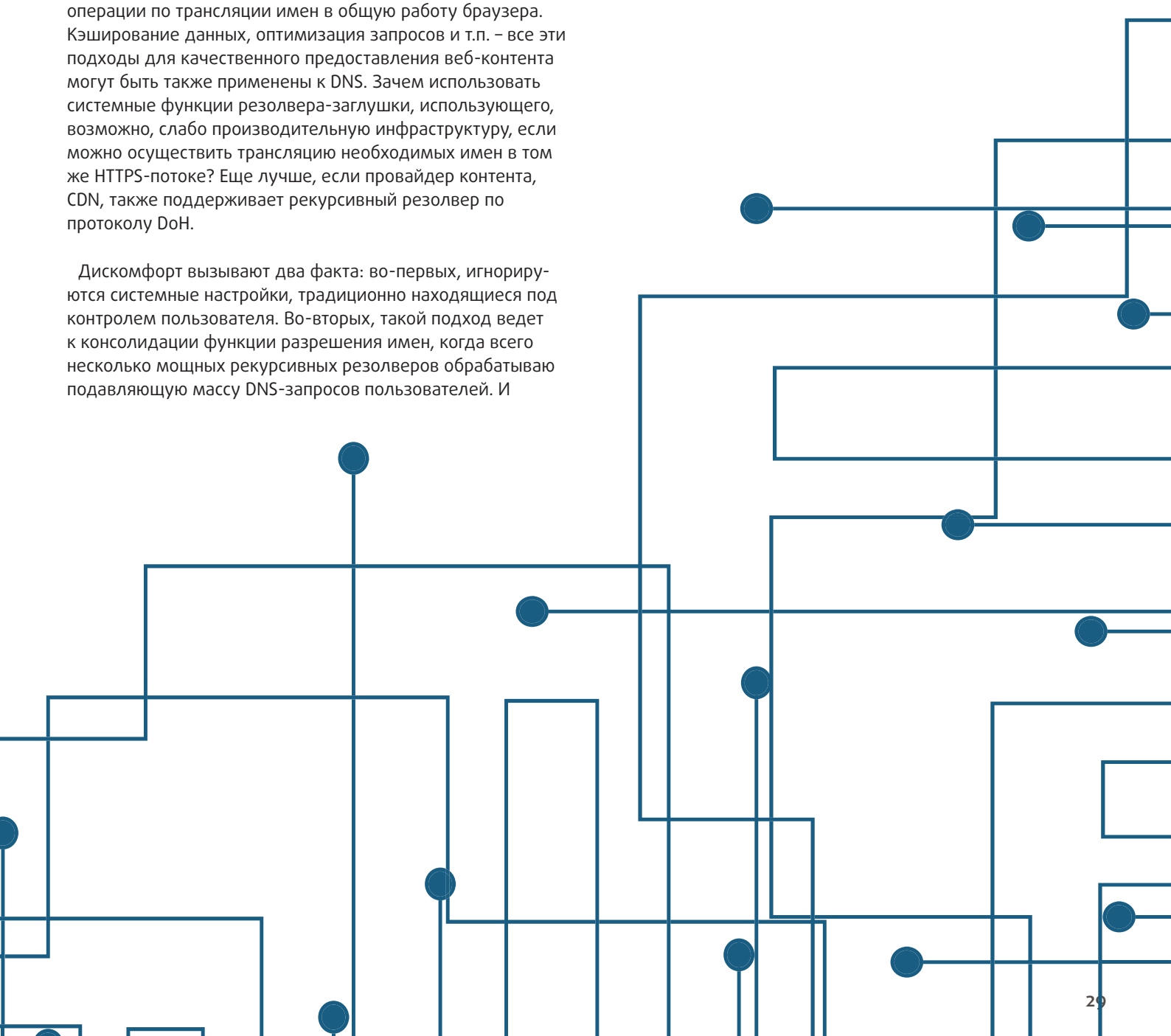
Поскольку HTTPS используется для передачи DNS-запросов, он делает DNS необнаружимым и не блокируемым. Это может быть проблематичным, поскольку DNS широко используется для обеспечения соблюдения политик различного рода - от операционных целей интернет-провайдера до блокирования контента на национальном уровне.

DoH имеет и другие спорные моменты. Использование протокола HTTPS позволяет идеально интегрировать операции по трансляции имен в общую работу браузера. Кэширование данных, оптимизация запросов и т.п. – все эти подходы для качественного предоставления веб-контента могут быть также применены к DNS. Зачем использовать системные функции резолвера-заглушки, использующего, возможно, слабо производительную инфраструктуру, если можно осуществить трансляцию необходимых имен в том же HTTPS-потоке? Еще лучше, если провайдер контента, CDN, также поддерживает рекурсивный резолвер по протоколу DoH.

Дискомфорт вызывают два факта: во-первых, игнорируются системные настройки, традиционно находящиеся под контролем пользователя. Во-вторых, такой подход ведет к консолидации функции разрешения имен, когда всего несколько мощных рекурсивных резолверов обрабатываю подавляющую массу DNS-запросов пользователей. И хотя DNS-транзакции обретают сильную защиту конфиденциальности от возможных попыток транзитных сетей манипулировать или просматривать эти данные, консолидация запросов в DoH-резолвере работает в противоположном направлении.

Хотя сухой остаток зависит от конкретной модели угроз, кому вы больше доверяете – своему сервис-провайдеру или, скажем, CloudFlare? В конце концов, и тот и другой могут наблюдать значительную часть реальных запросов контента.

Инфраструктура маршрутизации и передачи данных и глобальная система трансляции имен DNS являются фундаментом сегодняшнего Интернета. От их устойчивости и защищенности зависит устойчивость и защищенность Интернета в целом, его услуг и пользователей. Приятно видеть, что работа в IETF вносит существенный вклад в решение этой задачи.



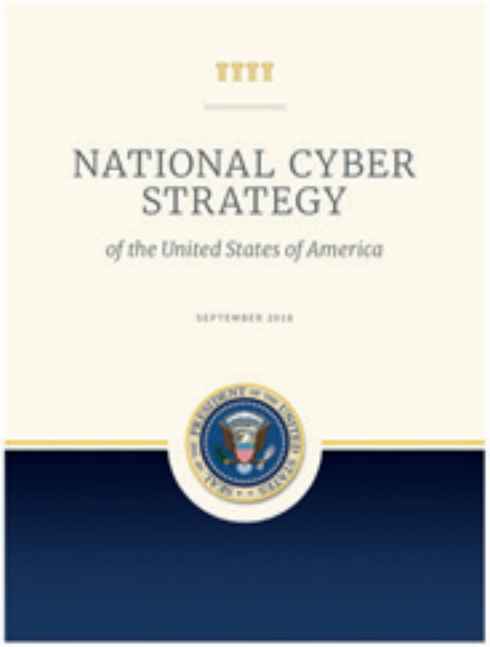
Усиливая национальную безопасность: обзор Национальной киберстратегии США 2018 года

Мадина Касенова

Интернет формирует и диверсифицирует процессы социальной регуляции и современная логика регулирования отношений, так или иначе, связывается с Интернетом. Правительством США в сентябре 2018 года была принята Национальная киберстратегия Соединенных Штатов Америки (*National Cyber Strategy of the United States of America*). Содержательный анализ этого документа со всей очевидностью свидетельствует о том, что киберпространство рассматривается как критически важный объект национальных интересов США, а его безопасное использование объективно сопрягается с международно-правовым сотрудничеством.

Интернет, в силу своей уникальной технологической архитектуры, выступает критически важным элементом информационно-коммуникационных технологий, приобретая существенное (если не ключевое) значение в современной жизни человека, общества, государства. Интернет радикально и в трансграничном масштабе изменил взаимодействие государств и лиц, расширив их коммуникативные возможности и сферы их «цифрового присутствия». Вряд ли оспоримым является тот факт, что за последний четвертьвековой период интенсивное расширение социальных сфер применения Интернета диверсифицировало правовую регламентацию целого ряда отношений. Киберпространство, данные (в их «широком» значении, охватывающие данные личного характера/персональные данные), информация и т.д. стали самостоятельными объектами правового регулирования[1]. Более того, в нынешних условиях выбор стратегического вектора социально-экономического развития современных государств ориентирован на «цифровую экономику», реализация которой без применения Интернета – не достижима[2].

Безусловно, становится очевидным, что те трансграничные коммуникативные возможности, которые возникли в связи с применением Интернета, стали определяющими в обусловленности сопряжения, в частности, национально-правовых и международно-правовых интересов государств при формировании их подходов правового регулирования использования Интернета в целом.



Оглядываясь назад: международная стратегия США в отношении киберпространства

В сентябре 2018 года Соединенные Штаты Америки приняли важный документ – Национальную киберстратегию США (*National Cyber Strategy of the United States of America*)[3]. Содержательный анализ этого документа со всей очевидностью свидетельствует о том, что киберпространство рассматривается как критически важный объект национальных интересов США, а его безопасное использование объективно предопределяет необходимость международно-правового сотрудничества. Предваряя обращение к содержанию названного документа (далее – «Киберстратегия США»), рассмотреть следующее.

При рассмотрении Киберстратегии США нельзя не вспомнить, что в 2011 году правительство США приняло «Международную стратегию США в отношении киберпространства. Процветание, безопасность и открытость сетевого мира» (*International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World*)[4]. Названный документ (далее – «Международная стратегия киберпространства США») закрепил

подход понимания правительством США, что технологические, правовые, политические и прочие вызовы так или иначе будут сопровождать функционирование, а также перспективы развития сетевых технологий и, прежде всего, Интернета как их центрального звена. Именно такой подход обусловил формулирование в Международной стратегии киберпространства США семи стратегических направлений регулирования киберпространства, требующих совместных усилий государств, при сотрудничестве с технологическим, гражданским, научным сообществом, в содействии построения и поддержания открытых, функционально совместимых (интероперабельных), безопасных и надежных сетей внутри США и за их пределами.

Стратегическими и взаимосвязанными направлениями в Международной стратегии киберпространства США были обозначены: «Экономика: укрепление международных стандартов и инноваций, открытые рынки»; «Защита наших сетей: усиление безопасности, надежности и отказоустойчивости»; «Правопорядок: расширение сотрудничества и правовое регулирование»; «Военная сила: подготовка к вызовам безопасности XXI века»; «Управление использованием Интернета: содействие эффективным и всеобъемлющим структурам»; «Международное сотрудничество: потенциал, безопасность и процветание»; «Свобода Интернета: защита основных свобод и частной жизни».

Обозначенные семь направлений Международной стратегии киберпространства США, помимо их взаимосвязанности, с одной стороны, представляли не конкретные инструкции, но, скорее, широкие принципы, обрисовывающие приоритеты правительства США в сфере киберпространства; с другой стороны, определяли сферы, в каждой из которых правительство США предполагало необходимость сотрудничества на международном, региональном и двустороннем уровнях. Будучи политико-стратегическим документом, Международная стратегия киберпространства США *de facto* и *de jure* была призвана продемонстрировать «национальный и международный» вектор действий правительства США в сфере киберпространства.

Примечательно, что принятие Международной стратегии киберпространства США (в т.ч. ее содержательный анализ) позволяло констатировать значительное изменение отношения США к необходимости расширения международного сотрудничества на различных уровнях, широкого использования инструментария международного права и т.д. Этот фактор носил принципиальный характер, поскольку ретроспективный взгляд на подходы США, сложившиеся к моменту принятия Международной стратегии США в международно-правовом плане, позволял говорить о том, что именно международное право было той сферой, к которой в США зачастую относились «скептически»[5].

Американские юристы консервативного толка нередко игнорировали «авторитет международного права»[6], несмотря на Статью VI Конституции Соединенных Штатов[7], которая наделяет акты международного права той же силой и теми же приоритетами, что и федеральные законы; «американский подход» к роли международного права достаточно долгое время отражал «крайне правые» доктринальные взгляды. По мнению ряда американских юристов-международников негативное отношение к международному праву и международным институтам коренится в традиционных для США ценностях. Например, Майкл Гленнон (*Michael J. Glennon*) отмечал, что поскольку международное право не смогло выполнить своей основной задачи, а именно предотвратить использование силы в отношениях между странами, – дальнейшее соблюдение США ограничений, накладываемых международным правом, было бы пагубным для США[8].

Такой тезис разделялся целым рядом юристов-консерваторов в области международного права. К примеру, Джек Голдсмит (*Jack L. Goldsmith*) и Эрик Познер (*Eric A. Posner*) утверждали, что национальные государства не «интернационализировали» международное право и не придерживаются его, а «действуют, исходя из собственных интересов», соответственно, международное право – это набор правил, которые можно использовать, когда удобно, и проигнорировать или даже преобразовать, когда они мешают[9]. Джек Голдсмит (*Jack Goldsmith*) и Тим Ву (*Tim Wu*) в своей работе «Кто контролирует Интернет?: иллюзии безграничного мира»[10] отмечали, что недостаточность международных соглашений в сфере управления Интернетом отражает слабость международного права и его неспособность предложить эффективные решения по этому вопросу[11].

В контексте сказанного сам факт принятия Международной стратегии киберпространства США, а также закрепление в этом документе правительством США необходимости международного сотрудничества в киберпространстве и его развития – стал важным фактором понимания США того, что Интернет не является «территорией вне права», в т.ч. международного права.

Безусловно, с «позиций» 2019 года Международную стратегию киберпространства США важно воспринимать с учетом временных параметров ее принятия, включая внутринациональную политико-экономическую ситуацию в США, а также международно-правовой, геополитический и т.д. контексты, существовавшие в 2011 году, которые по сути и определили ее содержательный формат. Вместе с тем, оценивая Киберстратегию США, целесообразно отметить, что в новых, значительно изменившихся за последние восемь лет социально-политических экономических, международно-правовых и т.д. условиях, Международная стратегия киберпространства США сохраняет свое значение.

Источники и составные части

Нынешняя Киберстратегия США 2018 года основывается, во-первых, на Стратегии национальной безопасности США (*National Security Strategy of the United States of America*), которая была принята через 11 месяцев после начала работы новой администрации президента США, т.е. в декабре 2017 года[12]; во-вторых, на Административном распоряжении президента США 13800 «Об усилении кибербезопасности федеральных сетей и критической инфраструктуры» (*Executive Order*, «*Strengthening of Federal Networks and Critical Infrastructure*»)[13].

Киберпространство, так же, как и в рассмотренной ранее

Международной стратегии киберпространства США, продолжает позиционироваться правительством США как критически важный объект, требующий сохранения его природы, совместных международных усилий по снижению возникающих угроз и вызовов, связанных с опасностью его фрагментации, подрывом открытого, функционально совместимого (интероперабельного), безопасного, транспарентного применения Интернета как основы киберпространства.

Несмотря на то, что Киберстратегия США формально не ссылается на рассмотренную ранее Международную стратегию киберпространства США, однако и в предметном, и в содержательном плане ключевые подходы, в т.ч. понятийно-терминологический ряд (кибербезопасность, процветание, интероперабельность, транспарентность и т.д.), стратегические направления и т.д. – остаются неизменными, равно как неизменной остается и приверженность целям и задачам, которые сопрягаются с необходимостью и неизбежностью поддержания совместных усилий государств, технического, гражданского, академического сообщества и т.д. в деле поддержания функционирования и использования киберпространства. (Сопоставительная таблица, которая завершает настоящую статью, как представляется, наглядно подтверждает высказанный тезис.)

Целый ряд государств, включая Российскую Федерацию, достаточно скептически относятся к необходимости международного сотрудничества в киберпространстве по «широкому кругу вопросов», и вектор правового регулирования переносится исключительно в сферу национального права.

Киберстратегию США предваряет обращение президента США, в котором обозначены следующие ключевые направления укрепления потенциала кибербезопасности и обеспечения защиты США от киберугроз и вызовов: защита США посредством сохранения сетей, систем, функциональных элементов и данных; содействие американскому благоденствию посредством содействия безопасной, процветающей цифровой экономике и стимулирования сильных внутристрановых инноваций; сохранение мира и безопасности посредством укрепления способности США сдерживать и, в случае необходимости, принимать меры воздействия на тех, кто использует киберинструменты в злонамеренных целях, при этом такие способности осуществляются во взаимодействии с союзниками и партнерами; усиление американского влияния за рубежом с тем, чтобы расширить основополагающие принципы открытого, функционально совместимого, интероперабельного, надежного и безопасного Интернета.

Киберстратегия США логически продолжает концептуальные подходы Стратегии национальной безопасности США 2017 года, структурно коррелирует ей (о чем свидетельствует даже рубрикация обоих документов и названия разделов). Киберстратегия США, как и Стратегия национальной безопасности США 2017 года, структурно содержит четыре исходных столпа (*Pillars*) или основополагающих элемента, формулировки которых идентичны. При этом, в отличие от соответствующих основополагающих направлений Международной стратегии киберпространства США и Стратегии национальной безопасности США 2017 года, в каждом из четырех столпов Киберстратегии США сформулирована конкретная цель, а также соответствующие приоритетные действия. Целесообразно в общем плане обозначить четыре столпа Киберстратегии США, цели, а также содержательные разделы, определяющие приоритетные направления и действия.

Столп I: *Защитить американский народ, Отечество и американский образ жизни:* формулирует ключевую цель – управлять рисками кибербезопасности для повышения защиты и устойчивости информации граждан США и информационных систем. Этот основополагающий элемент охватывает три раздела.

Раздел первый – обеспечение безопасности федеральных сетей и информации - предполагает приоритетные действия: дальнейшую централизацию управления и надзора за федеральной гражданской безопасностью; согласование управления рисками и деятельностью в сфере информационных технологий; совершенствование управления рисками федеральной системы снабженческих цепочек; усиление кибербезопасности федеральных подрядчиков; обеспечение лидирующих позиций правительства США по лучшим и инновационным практикам.

Раздел второй – защита критической инфраструктуры - охватывает следующие приоритетные действия: совершенствование распределения функций и сфер ответственности; определение приоритетов действий в зависимости от характера идентифицированных национальных рисков; привлечение провайдеров информационно-коммуникационных технологий как посредников кибербезопасности; защита американской демократии; создание благоприятных условий для инвестиций в кибербезопасность; определение приоритетов национальных исследований и содействие развитию инвестиций; улучшение транспортной, морской и космической кибербезопасности.

Раздел третий – борьба с киберпреступностью и улучшение отчётности об инцидентах - предусматривает такие приоритетные действия: меры по улучшению отчетности и реагирования на инциденты; улучшение электронного надзора, а также совершенствование права о компьютерных преступлениях; снижение угроз от транснациональных преступных организаций в киберпространстве; улучшение задержания преступников, находящихся за рубежом; укрепление потенциала правоохранительных органов стран-партнеров в борьбе с преступной кибердеятельностью.

Столп II: *Содействие американскому процветанию:* в качестве ключевой цели определяет сохранение влияния США в технологической экосистеме, а также развитие киберпространства в качестве открытого двигателя экономического роста, инноваций и эффективности. В этот основополагающий элемент включены три раздела.

Раздел первый – содействие развитию жизнеспособной и устойчивой цифровой экономики - направлен на такие приоритетные действия: стимулирование гибкой и защищенной технологической торговли; определение приоритета инноваций; инвестирование в инфраструктуру следующего поколения; содействие свободному трансграничному потоку данных; поддержание лидерства США в передовых технологиях; содействие полному жизненному циклу кибербезопасности.

Раздел второй – поощрение и обеспечение изобретательности США - предполагает, что приоритетные действия – это обновление механизмов обзора иностранных инвестиций и деятельности в США; поддержание сильной и сбалансированной системы защиты интеллектуальной собственности; защита конфиденциальности и целостности американских идей.

Раздел третий – создание высококлассного кадрового штата сотрудников кибербезопасности - подразумевает следующие приоритетные действия: создание и поддержание кадрового резерва; расширение возможности для переподготовки и образования для американских служащих и рабочих; увеличение кадрового персонала кибербезопасности федерального уровня; использование исполнительных органов для выявления и поощрения талантливых кадров.

Столп III: *Сохранение мира посредством силы:* в качестве ключевой цели формулирует выявление, противодействие, пресечение, ослабление интенсивности, а также сдерживание действий в киберпространстве, которые дестабилизируют и противоречат национальным интересам США, с сохранением превосходства США в киберпространстве и посредством киберпространства. Данный основополагающий элемент охватывает два раздела.

Раздел первый – повышение киберстабильности посредством норм ответственного поведения государств в качестве приоритетных действий - предполагает поощрение всеобщей приверженности к нормам, действующим в киберпространстве.

Раздел второй – атрибуты и сдерживание неприемлемого поведения в киберпространстве - направлен на необходимость таких приоритетных действий, как руководство заявленными целями, а также взаимодействие с разведывательными органами; введение соответствующих мер воздействия за негативные последствия в киберпространстве; создание киберсдерживающих инициатив; противодействие вредоносному кибервлиянию и информационным операциям.

Столп IV: *Усиление американского влияния:* как ключевую цель формулирует сохранение долгосрочной открытости, функциональной совместимости, безопасности и надежности Интернета, который поддерживается и усиливается интересами США. Этот основополагающий элемент включает два раздела.

Раздел первый – содействие открытому, функционально совместимому надежному и безопасному Интернету - в качестве приоритетных действий определяет следующее: защита и содействие свободе Интернета; сотрудничество со странами-единомышленниками, промышленностью, академическим и гражданским сообществом; содействие многосторонней модели управления использования Интернета; содействие многосторонней функциональной совместной надежной коммуникационной инфраструктуре и подключения к Интернету; поддержание рынков в отношении изобретательности США по всему миру.

Раздел второй – создание международного киберпотенциала - связывается с приоритетными действиями, направленными на: улучшение кибермобилизующих мер.

Краткий анализ

Автор отдает себе отчет, что в формате статьи даже такой «описательный» содержательный контекст Киберстратегии США, как представляется, достаточен, поскольку дает общее представление относительно предметной направленности документа. Вместе с тем, можно обратить внимание на следующее.

Во введении Киберстратегии США дважды упоминается Россия, однако такое упоминание осуществлено в ряду таких стран как Китай, Иран и Северная Корея. При этом Китай во введении также упомянут дважды, однако Китай один раз назван в контексте обозначенных стран (Россия, Иран и Северная Корея) и один раз отдельно от этих стран, в качестве страны, которая занималась «киберподдержкой экономического шпионажа и кражей триллиондолларовой интеллектуальной собственности».

В настоящее время, когда выбор стратегического вектора социально-экономического развития современных государств ориентирован на «цифровую экономику», и Россия не является в этом плане исключением[14], «усиливается конфликт» между национально-правовыми подходами регулирования применения Интернета и достаточно различающимися, а нередко и противоположными интересами государств с учетом трансграничных коммуникативных возможностей Интернета. Несомненно, средства, методы национально-правовые подходы «разрешения этого конфликта», а также меры правовой защиты и т.д. будут претерпевать радикальные изменения и варьироваться в зависимости от специфики национальных правопорядков государств. Вместе с тем, сложно положительно ответить на вопрос о том, можно ли достичь целей и решать задачи реализации «цифровой экономики» в рамках «суверенного технологического развития», «суверенного Интернета», отсутствия конкурентной среды и т.д.

С этой точки зрения в Киберстратегии США в самостоятельный раздел выделено содействие развитию жизнеспособной и устойчивой цифровой экономики.

Примечательно, что в этом же разделе отмечается, что государства «все чаще предусматривают ограничительные положения о локализации данных ... в качестве оправдания для цифрового протекционизма, подводя это под категорию национальной безопасности».

В конце прошлого века, в эпоху «интернет-эйфории» был популярен доктринальный тезис о том, что регулирование отношений в сфере Интернета настолько многообразно, что «способно породить такие синергетические» связи, которые могут трансформировать роль суверенных государств как субъектов международного права[15]. Существующая реальность опровергла этот тезис. Более того, роль государства в регулировании Интернета расширяется. Государства *ergo omnes* субъекты международного права, а положительный ответ на вопрос о применимости международного права к киберпространству, регулированию применения Интернета и т.д. не вызывает сомнений. Однако остаются открытыми вопросы относительно того, каковы формы и методы такого применения, как они соотносятся с национальными интересами государств[16].

Целый ряд государств, включая Российскую Федерацию, достаточно скептически относятся к необходимости международного сотрудничества в киберпространстве по «широкому кругу вопросов», и вектор правового регулирования переносится исключительно в сферу национального права. Применительно к рассматриваемой в настоящей статье проблематике Киберстратегии США противоположность подходов США и России в этом плане достаточно очевидна.

В связи с Российской Федерацией все же следует сказать, что определенные «надежды» связываются с тем фактом, что она принимала активное участие в обсуждении новой редакции Конвенции №108 Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*). Соответствующий протокол о новой редакции названной Конвенции №108 был принят министрами иностранных дел государств-членов Совета Европы 18 мая 2018 года (г. Эльсинор, Дания). Россия не только принимала активное участие в разработке и обсуждении этого протокола, но и согласно распоряжению №294-рп президента РФ от 10 октября 2018 г. названный протокол был подписан от имени Российской Федерации . В редакции принятого протокола Конвенция №108 Совета Европы о защите физических лиц при автоматизированной обработке персональных данных в момент подготовки настоящей статьи ратифицирована не была.

Сопоставительная таблица

«Международная стратегия США в отношении киберпространства» 2011 г. **Стратегические направления**	«Стратегия национальной безопасности США» 2017 г. **Столпы (основополагающие элементы)**	«Национальная киберстратегия США» 2018 г. **Столпы (основополагающие элементы)**
1. Экономика: укрепление международных стандартов и инноваций, открытые рынки	**Столп I:** Защитить американский народ, Отечество и американский образа жизни	**Столп I:** Защитить американский народ, Отечество и американский образа жизни
2. Защита наших сетей: усиление безопасности, надежности и отказоустойчивости	**Столп II:** Содействовать американскому процветанию	**Столп II:** Содействовать американскому процветанию
3. Правопорядок: расширение сотрудничества и правовое регулирование	**Столп III:** Сохранить мир посредством силы	**Столп III:** Сохранить мир посредством силы
4. Военная сила: подготовка к вызовам безопасности XXI века	**Столп IV:** Усилить американское влияние	**Столп IV:** Усилить американское влияние
5. Управление использованием Интернета: содействие эффективным и всеобъемлющим структурам		
6. Международное сотрудничество: потенциал, безопасность и процветание		
7. Свобода Интернета: защита основных свобод и частной жизни		

Ссылки

1. К примеру, в отношении личных данных см.: Архипов В. В. Проблема квалификации персональных данных как нематериальных благ в условиях цифровой экономики, или Нет ничего более практичного, чем хорошая теория // Закон. 2018. № 2.

2. Достаточно назвать: Стратегию Единого цифрового рынка Евросоюза (*EU Digital Single Market strategy*). *6 May 2015*. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 (Дата обращения: 09.09.2018); Указ президента РФ от 07.05.2018 № 204 (в ред. от 19.07.2018) «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 г.». СПС «Консультант Плюс».

3. *National Cyber Strategy of the United States of America* (September 2018). URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Дата обращения: 09.09.2018)

4. *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World.* URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Дата обращения: 09.09.2018)

5. В частности, в историко-правовом плане США зачастую пренебрегали международным правом и своими международными обязательствами, когда таковые «мешали» достижению их политических целей. Достаточно вспомнить, что правительство США заявило о выходе из Договора о противоракетной обороне, проигнорировало Киотский договор, отозвало подпись США под Соглашением о создании постоянно действующего Международного уголовного суда; весной 2003 года были введены войска в Ирак, даже после того, как не был получен соответствующий мандат Совета Безопасности ООН, что было оценено как нарушение Устава ООН. См. об этом подробнее, например, URL: http://www.stlr.org/html/volume8/schoenbergerintro.php (Дата обращения: 15.09.2018)

6. См. *Viktor Mayer-Schenberger & Malte Ziewitz*. Jefferson Rebuffed: The United States and the Future of Internet Governance. The Columbia Science and Technology Law Review. 8 Colum. 188 (2007), http://www.stlr.org/html/volume8/schoenbergerintro.php (Дата обращения: 09.09.2018)

7. «Настоящая Конституция и законы Соединенных Штатов, которые должны быть приняты в соответствии с ней; и все договоры, заключенные или которые должны быть заключены в соответствии с полномочиями Соединенных Штатов, являются высшим законом страны...» (Конституция США, Статья VI) *The Constitution of the United States*. URL: http://constitutionus.com (Дата обращения: 09.09.2018); также см. *Curtis A. Bradley*. Customary International Law and the Continuing Relevance of Erie. 120 Harvard Law Review. 869, 891-92 (2007).

8. См., например, *Michael J. Glennon*. The UN Security Council in a Unipolar World, 44 Va. J. Int'l L. 91, 94-100 (2003); также Michael J. Glennon. Limits of Law, Prerogatives of Power: Interventionism After Kosovo (2001); Michael J. Glennon. How International Rules Die, 93 Geo. L.J. 939 (2005).

9. См. *Jack L. Goldsmith & Eric A. Posner*. The Limits of International Law 225-26 (2005). Анализ работы *Jack L. Goldsmith & Eric A. Posner*. The Limits of International Law (2005) – см. Paul Schiff Berman «Seeing Beyond the Limits of International Law». URL: http://www.papers.ssrn.com/sol3 (Дата обращения: 09.09.2018); *David Sloss*, Do International Norms Influence State Behavior? 38 Geo. Wash. Int'l Law Review. 159 (2006).

10. *Jack Goldsmith and Tim Wu*. Who Controls the Internet?: Illusions of a Borderless World. New York: Oxford University Press, 2006. pp i-xii, 1-219 (2006).

11. См. *Jack Goldsmith and Tim Wu*, указ раб. URL: http://ijoc.org/ois/index.php/ijoc/aecticle/viewFile/76/66 (Дата обращения: 09.09.2018)

12. *National Cyber Strategy of the United States of America* (December 2017). URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (Дата обращения: 09.09.2018)

13. President Executive Order 13800 «*Strengthening of Federal Networks and Critical Infrastructure*. URL: https://www.dhs.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure (Дата обращения: 09.09.2018); *Executive Order* – Административное распоряжение президента США является нормативно-правовым актом.

14. Указ президента РФ от 07.05.2018 № 204 (в ред. от 19.07.2018) «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 г.». СПС «Консультант Плюс».

15. Об этом см., например: *Kurbalija J.* Internet Governance and International Law. URL: http://www.wgig.org/docs/book/Jovan_Kurbalija%20.pdf (Дата обращения: 15.08.2018); *Mathiason J.* A Framework Convention: An Institutional Option for Internet Governance. Concept Paper for the Internet Governance Project. December, 2004. URL: http://dcc.syr.edu/miscarticles/igpFC.pdf (Дата обращения: 15.08.2018); *Land M.* Toward an International Law of the Internet. University of Connecticut School of Law. November 19, 2012 // Harvard International Law Journal. 2013. Vol. 54. P. 43–98, и др.

16. *Mayer F.C.* Review The Internet and Public International Law – Worlds Apart? URL: http://www.ejil.org/pdfs/12/3/1536.pdf (Дата обращения: 09.09.2018)

Эволюция DDoS-атак: от первых инцидентов до терабитных атак

Александр Лямин

В 2019–2020 годах DDoS-атаки имеют все шансы выйти на уровень более 10 Тбит/с. Этому будут способствовать экспоненциальный рост количества подключенных к сети устройств (развитие IoT) и линейный рост числа уязвимостей, к чему приводят отсутствие общепринятых практик безопасности при разработке, а также по-прежнему низкая грамотность пользователей. Такие необходимые действия, как обновление прошивок и изоляция сетевых устройств от внешнего доступа, выполняются не везде.

Основные вехи в развитии DDoS-атак с указанием силы и использовавшегося вектора атаки

Первая в мире DDoS-атака — SYN flood — была зафиксирована в 1994 году. А рекомендации по противодействию атакам такого рода были опубликованы лишь в 1996. Эти материалы подготовил Координационный центр CERT (Computer Emergency Response Team) Университета Карнеги — Меллона, официально признав таким образом наличие проблемы. Поводом для подготовки рекомендаций стало первое масштабное нападение — на крупнейшего интернет-провайдера Нью-Йорка Panix Networks. Это была коммерческая атака, организованная спамерами, которые решили отомстить компании за то, что она не позволила им рассылать рекламные сообщения пользователям.

В том же 1996 году впервые был опубликован (http://phrack.org/issues/48/13.html%22%20%5Cl%20%22article) набор публичных инструментов с исходным кодом для осуществления DDoS-нападений. Спустя два года этот инструментарий был задействован против Мичиганского университета — состоялась вторая крупная DDoS-атака.

В 2000 году были проведены атаки RiverHead & MafiaBoy (последнюю провел 15-летний канадец, из-за действий которого почти неделю лежали такие ресурсы, как Yahoo!, Fifa.com, Amazon.com, eBay, CNN, Dell и др.).

Здесь заканчивается эра blackhole/sinkhole — то есть полного сброса трафика, этот метод уже не может нейтрализовать наиболее крупные атаки. Наступает следующий этап — применение Customer Premises Equipment от поставщиков оборудования для защиты от DDoS на стороне заказчика.

- В 2001 году появляются атаки HTTP flood (в этот момент оформляется индустрия кибербезопасности).
- В 2003 DDoS докатился и до России: был атакован MasterHost — самый крупный хостинг нашей страны на тот момент.
- В 2004 Cisco Systems поглотила израильского разработчика средств предотвращения атак Riverhead Networks. Благодаря этой покупке ей удалось создать первый успешный коммерческий продукт для борьбы с DDoS — Cisco Guard.
- В 2005 Arbor Networks на ежегодном мероприятии World-Wide Infrastructure Security Survey сообщила о мощной атаке 8 Гбит/с.
- В 2007 серьезным распределенным атакам на отказ в обслуживании подверглась Эстония. Впервые всю силу DDoS-атак ощутило на себе государство, до этого считалось, что такими инструментами пользуются пранкеры/вымогатели.
- В 2008 появляется хакерская группа Anonymous, которая занимается дефейсами сайтов и DDoS-атаками.
- В 2011 реализована DDoS-атака на компанию Sony, комбинированная с проникновением. Результатом стала компрометация данных учетных записей Playstation Network.

Начинается эра глобальных облачных сервисов защиты от DDoS.

- В 2013 году из мести атакована организация Spamhaus, 300 Гбит/с — новый рекорд мощности атаки.
- В 2014 хакерская группировка Lizard Squad на рождественские каникулы устраивает атаку на Xbox Live и Playstation Network.
- В августе 2016 — во время Олимпийских игр — происходят атаки мощностью до 500 Гбит/с.
- В сентябре 2016 реализована атака ботнета Mirai в 620 Гбит/с на сайт журналиста-расследователя Брайана Кребса (Brian Krebs). Провайдер Akamai отключает сайт Кребса от защиты (которую предоставлял pro bono).

По состоянию на 2016 год защита с помощью оборудования уже была катастрофически недостаточной для нейтрализации входящих атак многочисленных ботнетов. Требовались другие возможности. И они появились. Крупнейшие компании, занимающиеся сетевой безопасностью, завершают построение распределенных сетей фильтрации.

- В 2016 году с использованием ботнета Mirai проводятся мощные атаки 620 Гбит/с — 1,2 Тбит/с на провайдера DNS-сервиса Dyn, в США наблюдаются перебои с доступом к сайтам.

- В 2018 реализуются атаки на GitHub с использованием найденной в популярной библиотеке memcached уязвимости (500 Гбит/с — 1,7 Тбит/с).

Настоящее время: терабитные атаки с амплификацией и рост количества атак прикладного уровня

В начале 2018 года было установлено сразу несколько рекордов. В конце февраля компания Qrator Labs, специализирующаяся на противодействии DDoS-атакам и обеспечении доступности интернет-ресурсов, зафиксировала атаку полосой 500 Гбит/с на платежную систему Qiwi. Всего за несколько дней пиковая скорость атаки выросла до глобальных масштабов — 1,7 Тбит/с, о чем рапортовал Arbor Netscout, нейтрализовавший данную атаку, направленную на самый популярный репозиторий кода — GitHub.

На сегодняшний день, на пороге 2019 года, ландшафт DDoS-атак представлен частыми атаками в первую очередь прикладного уровня (L7 по модели OSI). После истории с ботнетом Mirai, создатель которого по приговору суда получил два года тюрьмы и штраф 8 миллионов долларов, очень немногие случайные люди атакуют крупные цели. И дело не в страхе наказания, а в увеличившемся «входном пороге» для осуществления серьезных атак, способных нанести повреждения достаточно масштабным интернет-ресурсам так, чтобы это стало заметно.

Наиболее болезненные DDoS-атаки — уже давно сугубо профессиональный бизнес, оборот которого сложно оценить. Две наиболее частые причины для проведения атаки на отказ в обслуживании — это: а) сопровождение попыток проникновения — так сложнее вернуть нормальное состояние системе и остановить злоумышленника; б) конкурентная борьба. Напомним, что до сих пор в качестве источника заработка владельцы крупных скомпрометированных и зараженных сетей устройств в основном используют либо продажи в дарк-вебе атакующей полосы, либо вымогательство.

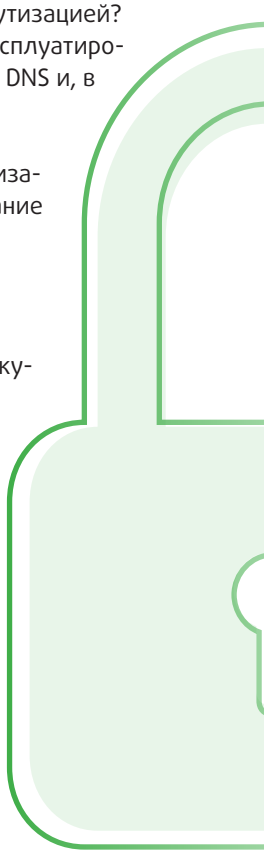
В 2019–2020 годах DDoS-атаки имеют все шансы выйти на уровень более 10 Тбит/с. Этому будут способствовать экспоненциальный рост количества подключенных к сети устройств (развитие IoT) и линейный рост числа уязвимостей, к чему приводят отсутствие общепринятых практик безопасности при разработке, а также по-прежнему низкая грамотность пользователей. Такие необходимые действия, как обновление прошивок и изоляция сетевых устройств от внешнего доступа, выполняются не везде. Мощные атаки опасны в первую очередь тем, что такой объем трафика способен исчерпать доступную полосу среднего регионального провайдера. Невозможность фильтровать трафик на уровне ключевых узлов сети — это очень опасный фактор. Поэтому появление волны недоступности интернет-ресурсов, потенциально влияющей на несколько крупных стран и регионов, — это лишь вопрос времени.

Сочетание сложности и объема трафика уже приводит к тому, что наиболее целенаправленные атаки на специфические болевые точки приложения очень сложно нейтрализовать эффективно и быстро — без простоя.

Но растет не только количество устройств. Ключевой единицей взаимодействия в сети является не отдельное устройство, а сущность — автономная система (AS). На сегодняшний день в мире зарегистрировано более 60 тысяч автономных систем. Вот здесь и начинается будущее безопасности объединенных сетей. Насколько успешно удастся противодействовать манипуляциям с маршрутизацией? Ведь злоумышленники обязательно будут эксплуатировать уязвимости протоколов ядра интернета: DNS и, в первую очередь, BGP.

- 2019 год и далее — манипуляции маршрутизацией, атаки на шифрование, масштабирование сетей и экспоненциальный рост трафика.

Прежде чем мы перейдем к рассмотрению проблематики злонамеренных манипуляций трафиком, необходимо проанализировать текущие тенденции в развитии Интернета.



1. Все больше трафика в Интернете шифруется. По данным Let's Encrypt к моменту написания данной статьи в браузере Firefox 76,5% страниц загружалось с использованием защищенного соединения. Это не значит, что три четверти Интернета «зашифровано», но динамика данного показателя, составлявшего 25% в начале 2014 года, однозначно свидетельствует об успешном принятии SSL-сертификатов в вебе. Зашифрованный трафик, казалось бы, бессмысленно перехватывать.

2. Человечество начало подключать к сети абсолютно всё. И то, что в свое время произошло с электричеством, мы наблюдаем в настоящее время с Интернетом в еще больших масштабах. Каждая камера, трекер, мобильный телефон и бесчисленное множество других мелких и крупных гаджетов сегодня отправляют стабильный поток информации в лучшем случае на сервер производителя.

3. Сеть построена фактически на основе одного протокола — BGP. Border Gateway Protocol, или протокол граничного шлюза, — это краеугольный камень архитектуры современного Интернета. Как бы странно это ни звучало, но протокол слабо защищен от атак злоумышленников, так как представляет собой протокол «доверия». При этом операторы AS не сдают

Сценарии получения сертификата безопасности злоумышленником

Процедура получения TLS-сертификата для домена от сертификационного центра TLS (CA — Certificate Authority) обычно проходит в следующей последовательности:

1. Создается аккаунт на веб-сайте центра сертификации.
2. CSR (certificate signing request — запрос подписи сертификата) создается и загружается на сайт центра сертификации.
3. Центр сертификации предлагает опции подтверждения владения доменом: WHOIS-запись — загрузка специальной HTML-странички по требуемому URL — создание уникального токена в записи DNS TXT (а также иногда другие способы).

После подтверждения владения требуется оплатить (некоторые сертификаты бесплатные) услуги центра сертификации — и всё: вы получаете TLS-сертификат!

Такой сертификат действителен в течение месяцев или даже лет и может быть использован для подтверждения владения сайтом во Всемирной сети.

Злоумышленник может легко мимикрировать под владельца сайта, совершая атаки перехвата трафика.

никаких экзаменов, не получают сертификаты и т.д., находясь в равных возможностях со всеми другими AS.

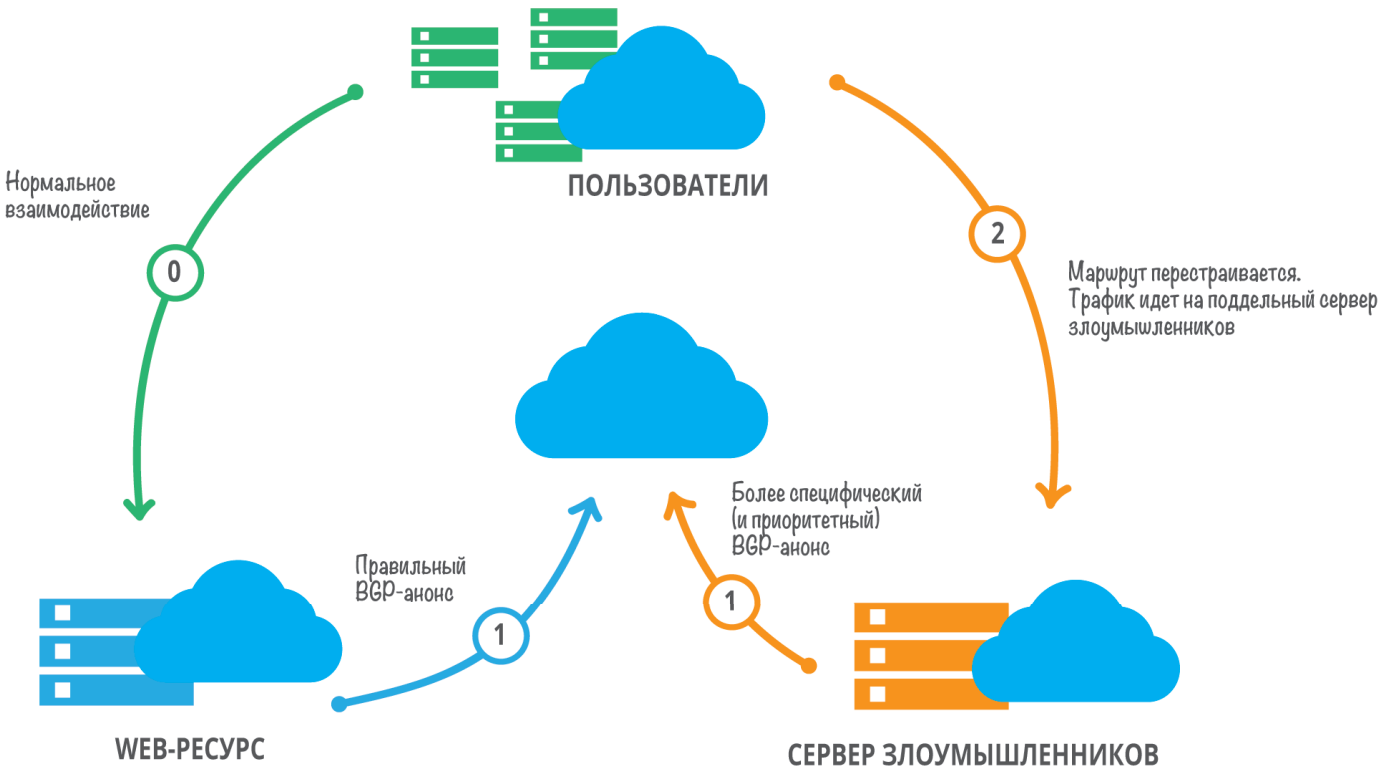
К чему же всех нас приводит эта архитектурная диспозиция?

Во-первых, мы уже видели, как некорректная конфигурация автономных систем и анонсов сетевых префиксов наносит урон, несовместимый с нормальной работой сетевых ресурсов, поскольку единовременное перенаправление трафика крупного ресурса может вывести из строя неподготовленную транзитную точку — то есть потенциально любую AS. В этом году в результате подобной «утечки маршрута» ресурсы Google были недоступны в Японии.

Киберпреступник также может совершить подобное действие, и чем дольше оно будет оставаться незамеченным, тем тяжелее окажутся последствия. Если ресурс, подвергшийся подобной атаке, не использует SSL-сертификат для шифрования клиентского трафика, то его можно перехватить и записать целиком. Вместе со всеми данными, которые пользователь вводил на такой странице.

Злонамеренность или случайность подобных сетевых инцидентов оценить тяжело, но общее число ликов/хайд-

Рис. 1. Схема типичного BGP Hijack.



жеков — достаточно легко. По методологии Qrator.Radar, «хайджек» (hijack, или перехват трафика) отличается от «рут лика» (route leak, или утечка маршрута) отсутствием корректных регистрационных данных при создании маршрута. См. рисунки 1 и 2.

На момент написания публикации:

а) утекших префиксов — 92 585 от 544 операторов, из них хорошо распространившихся — 2195 префиксов от 322 операторов;

б) хайджеков/перехватов — 102 602 префикса от 8589 операторов, из них хорошо распространившихся — 54 564 от 7665.

Как видите, цифры впечатляют. На сегодняшний день операторы AS обязаны пристально следить за состоянием собственных систем, иначе те могут очень быстро стать жертвами атак киберпреступников.

Теперь давайте рассмотрим потенциальные проблемы, которые может устроить достаточно подготовленный злоумышленник. Есть случаи, когда даже пресловутое шифрование не способно оградить вас от последствий.

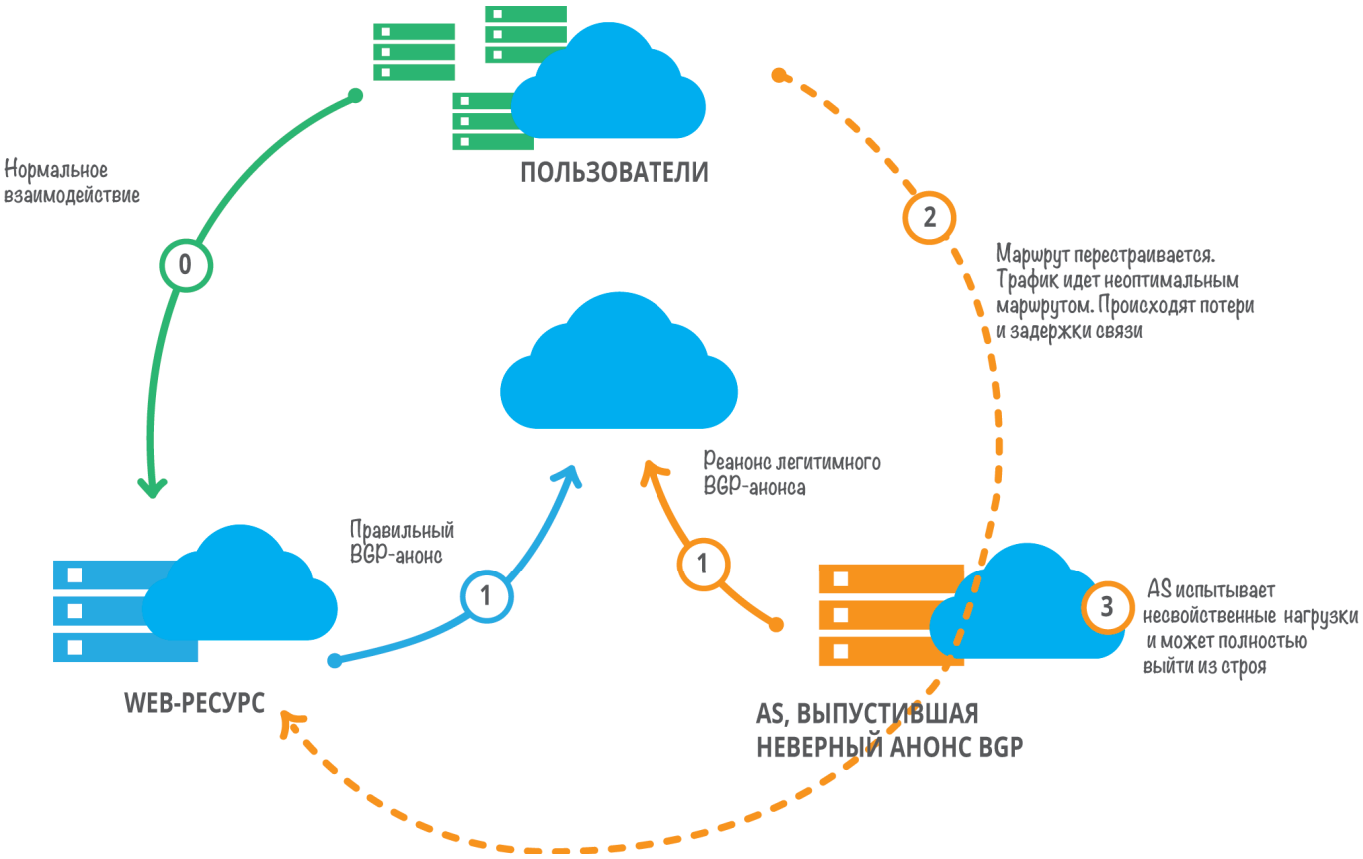
Негативные сценарии

Мы уже знаем, что перехваты трафика происходят каждый день и в достаточно большом количестве. Утечка персональных данных пользователя — далеко не самый худший сценарий, хотя и неприятный. Наиболее серьезная проблема в современном Интернете — это утеря банковских реквизитов и контроля над счетом. Причем преступникам совершенно не обязательно проводить сложные и рассчитанные на психологические уязвимости фишинговые атаки — в 2018 году с пользователями уже можно не взаимодействовать ради достижения желаемого результата.

Ведь если можно перехватить и перенаправить для обработки запросы пользователей на заранее выбранные поддельные серверы, то ни пользователь, ни владелец ресурса сразу же не идентифицирует подмену. Как мы уже упоминали, даже установленный сертификат не гарантирует безопасности пользователей или вашего бизнеса, ведь злоумышленники могут выпустить вполне легальный сертификат, легитимный для браузера пользователя, при помощи все того же перехвата. Или подписать самостоятельно фальшивый сайт, на который пользователи попадут в результате перехвата трафика. Итогом такой атаки могут стать колоссальные убытки для бизнеса, при том что пользователь ничего не заподозрит. Подобная атака была проведена в недавнем прошлом на одно из крупнейших облаков в мире — Amazon EC2, когда на фишинговом сайте использовался самоподписанный сертификат. По идее, у пользователей должны были возникнуть подозрения, но так как далеко не все смотрят на значки «замка», означающего корректный сертификат для запрашиваемой страницы, то за два часа атаки из одного популярного криптокошелька было выведено активов на сумму около 150 тысяч долларов. Издание The Register, специализирующееся на инфобезопасности, подробно описало (https://www.theregister.co.uk/2018/04/24/myetherwallet_dns_hijack/) инцидент в конце апреля 2018 года.

Добавим лишь, что этой возможности эксплуатации

Рис. 2. Схема типичного BGP Route Leak.



протокола BGP уже более десяти лет.

Но ведь наша компания не занимается онлайн-продажами, возразите вы. И даже не обрабатывает транзакции. Так чего же нам бояться, если мы, допустим, информационный ресурс? По идее, у наших пользователей даже нечего украсть. Значит, у нас всё в порядке?

> **Бритва Хэнлона идеально работает в мире современных сетей, ежедневно подтверждая известную фразу: «Никогда не приписывайте злому умыслу то, что вполне возможно объяснить глупостью»**

Нет. В мире перехватов трафика удар может быть нанесен (и будет нанесен!) в первую очередь по вашей репутации, и есть проверенный способ сделать это — дефейс (deface). Именно так называется изменение внешнего вида страницы, отображаемой через браузер пользователя. И хорошо еще, если это будет «безобидная» детская проделка с кучей рекламы, угроз или прочего непотребства на главной странице вашего ресурса. Но подумайте о том, к каким последствиям может привести спланированная атака. Пользователи в течение дня или нескольких часов будут видеть фальшивую резонансную новость, опровергать которую впоследствии вы будете долго и мучительно (и с финансовыми потерями). Не будем забывать и о том, что в каждой стране есть законы, за нарушение которых любой информационный ресурс закроют в два счета из-за угрозы национальной безопасности.

Любой бизнес, даже не оказывающий напрямую услуги связи и не продающий электронные продукты, но имеющий хотя бы малейшее представительство в глобальной сети, уязвим для атак на BGP.

Наша компания на практике часто сталкивается с достаточно небрежным отношением пользователей к такой угрозе, а главное — к тем последствиям, которые могут наступить.

И, как это ни прискорбно, все чаще мы видим такое отношение у наших же коллег — занимающихся созданием, разработкой и развитием услуг и продуктов интернет-связности.

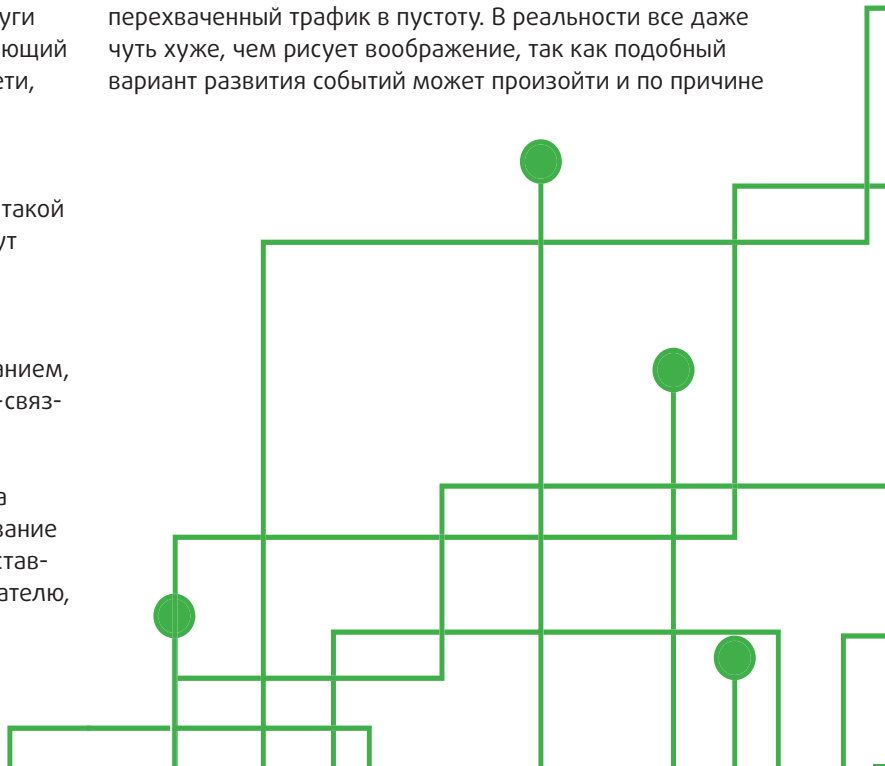
Возьмем для примера любую сеть доставки контента (CDN). Сегодня без таких сетей невозможно существование крупных, глобально распределенных ресурсов, предоставляющих контент в точке, наиболее близкой к пользователю, его запрашивающему.

На первый взгляд, выполнить дефейс такой компании нельзя: у нее может не быть посещаемого сайта. И перехватывать тяжелые ответы сервера с медиаконтентом, отправляемым пользователю, казалось бы, тоже бессмысленно — не фильмы же смотреть злоумышленникам одновременно с жертвой. Однако у CDN есть другая ключевая характеристика, на которую можно влиять, — скорость доставки контента. Ведь именно в эффективном и быстром выполнении данной задачи и кроется смысл существования подобных сетей.

В результате перехвата трафик такой сети может начать двигаться по произвольному маршруту — например, через другой континент. Как вам задержка в 100–200 миллисекунд для каждого из пакетов по направлению к CDN? Подобный рост сетевой задержки сильно повлияет на скорость реакции сервера на запросы.

И это проблема не столько сетей доставки контента, сколько классических операторов связи — в первую очередь предоставляющих широкополосное подключение к сети. Вы гарантируете своим клиентам набор параметров в виде SLA? А что будет, если ваш бизнес не сможет выполнить обещания? Мы все знаем, что происходит на конкурентном рынке: потребитель выбирает альтернативного поставщика. Гонка за временем в процессе майнинга криптовалют (вознаграждение достанется только той группе майнеров, которая первой нашла «правильный» хэш для нового блока) — еще один интересный пример того, как сетевая задержка может перевернуть парадигму сервиса или процесса, в котором задействовано множество людей.

Основное, что нужно запомнить из всего рассказанного нами о вероятных последствиях утечки или перехвата трафика, — это то, что атакующему не требуется слишком много «телодвижений» для достижения своей цели. Помимо вышеупомянутых способов нанести вред, злоумышленник всегда имеет абсолютно реальную возможность вывести ваш ресурс из строя, просто направив перехваченный трафик в пустоту. В реальности все даже чуть хуже, чем рисует воображение, так как подобный вариант развития событий может произойти и по причине



чужой ошибки. Бритва Хэнлона идеально работает в мире современных сетей, ежедневно подтверждая известную фразу: «Никогда не приписывайте злому умыслу то, что вполне возможно объяснить глупостью». Такой постулат постоянно доказывают разнообразные инциденты маршрутизации, часть из которых мы освещаем в блоге сервиса Radar (https://blog.qrator.net/ru/). Крупные компании, впервые сталкивающиеся с подобной проблемой, обычно тратят больше часа только на установление причин, а для применения контрмер могут потребоваться дни. И все это время бизнес простаивает, терпя соответствующие убытки.

Как оценить ущерб от подобного инцидента? Как установить, был ли инцидент локальным? Насколько серьезными могут быть последствия? Для этого необходимо получить ответ на ключевой вопрос: чей трафик был перехвачен?

Чем более крупные операторы были задеты и чем больше было их число, тем большее количество именно ваших потенциальных пользователей и потребителей будет задето. И тем более серьезным станет и сам инцидент. В зависимости от потребительского портфеля компании, критически важно знать не только общее количество пострадавших, но и их поименный список.

Можно ли защититься от атак на маршрутизацию? К сожалению, нельзя. Существуют определенные способы противодействия, так как приоритет на пути движения трафика всегда отдается более специфичным (more specific в терминологии BGP) путям. Но для того чтобы начать анонсировать такие пути от вашей автономной системы, как минимум нужно вовремя узнать о том, что произошло что-то плохое. Как?

Мониторинг и только мониторинг

И именно созданием такого продукта занимается команда Radar внутри Qrator Labs. По состоянию на конец 2018 года Radar — это один из крупнейших в мире коллекторов путей, собирающий данные от более 500 сессий по всему миру и имеющий возможность отслеживать даже локальные изменения. Открытыми данными сервиса Radar уже сегодня пользуются более 3500 уникальных автономных систем. Более того, на сегодняшний день эта услуга бесплатна при условии обновления данных раз в 24 часа.

Для людей, знакомых с процессом создания и внедрения обновлений протоколов ядра Интернета, уточним: сетевые инженеры Qrator Labs совместно с зарубежными специалистами, в рамках Инженерного совета интернета (IETF), разрабатывают расширение протокола BGP под названием AS Provider Authorization, направленное именно на борьбу с утечками маршрутов и перехватом трафика (черновик расширения доступен в IETF Datatracker по адресу https://datatracker.ietf.org/doc/draft-azimov-sidrops-aspa-profile/).

Безопасность и современные тренды

Павел Храмцов

Если подходить к вопросу формально, то можно просто ограничиться цитатой с сайта недавно прошедшего мероприятия: «Нынешний DNS излишне медленен и неэффективен из-за попыток поддержки систем DNS, которые не соответствуют стандартам DNS, установленным два десятилетия назад. Чтобы обеспечить дальнейшую устойчивость системы, пришло время положить конец этой ситуации и исправить несоответствующие системы. Это изменение сделает большинство операций DNS немного более эффективными, а также позволит операторам развертывать новые функции, в том числе новые механизмы защиты от DDoS-атак.»

Начало 2019 года ознаменовалось несколькими событиями, которые заставляют задуматься над вопросом: будет ли Интернет прежним, т.е. будет ли это единая открытая среда информационного обмена или мы скатимся к децентрализации по национальным и корпоративным квартирам?

Обзор этих событий хотелось бы начать не с соображений о «суверенном Рунете», а с события сугубо технического. Речь идет о DNS Flag Day[1]

DNS Flag Day – что это было?

Если подходить к вопросу формально, то можно просто ограничиться цитатой с сайта данного мероприятия: «Нынешний DNS излишне медленен и неэффективен из-за попыток поддержки систем DNS, которые не соответствуют стандартам DNS, установленным два десятилетия назад.

Чтобы обеспечить дальнейшую устойчивость системы, пришло время положить конец этой ситуации и исправить несоответствующие системы. Это изменение сделает большинство операций DNS немного более эффективными, а также позволит операторам развертывать новые функции, в том числе новые механизмы защиты от DDoS-атак.

Поставщики программного обеспечения и услуг DNS, перечисленные на этом сайте, согласились скоординировать удаление поддержки несовместимых реализаций в районе 1 февраля 2019. Это изменение коснется только сайтов, использующих несовместимое программное обеспечение».

Прежде чем начать разбираться в том, чем же плох текущий глобальный сервис DNS и что за революционные улучшения предлагаются, обратим внимание на сам принцип внедрения улучшений инициаторами DNS Flag Day.

Кратко его можно сформулировать следующим образом: корпорации, разработчики софта и технические гуру лучше всех знают, что нужно конечному пользователю и компаниям, которые этого конечного пользователя обслуживают. Поэтому не нужно ни с кем ничего обсуждать, не нужно втягиваться в дебаты по принципу мультистейкхолдеризма, не нужно обеспечивать совместимость по принципу «снизу-вверх», а следует просто всех поставить перед фактом изменений. Достаточно всех уведомить об этом факте за неполный год до наступления часа «ч», по принципу «кто не спрятался, я не виноват!»

Вообще говоря, это нечто новое в практике внедрения технологий DNS. Можно, конечно, вспомнить браузерные войны начала века, но там все-таки были формально нестандартизованные протоколы и технологии. В случае с DNS мы имеем технологию, которая является базовой для множества интернет-сервисов, и ей пользуются десятки лет.

Теперь разберемся в сути вопроса. Речь идёт о согласованном прекращении поддержки резолверами «обходных механизмов», позволяющих сейчас работать с DNS-серверами, которые не отвечают на запросы с EDNS[2]. Инициаторы акции (провайдеры DNS-резолвинга и разработчики резолверов) договорились отключить поддержку «обходных механизмов».

Любопытно, что организаторы DNS Flag Day на странице акции обращают внимание на то, что «It is important to note that EDNS is still not mandatory. If you decide not to support EDNS it is okay as long as your software replies according to EDNS standard section 7». Это означает, что речь не идет об обязательной поддержке EDNS, а только о корректной работе DNS в соответствии с текущими спецификациями, например, RFC-1035.

Следует также обратить внимание на тот факт, что ряд популярных общеупотребимых механизмов парирования DDoS с использованием DNS, например, атак типа DNS-amplification (дроп пакетов), прямо противоречат выбранному способу проверки готовности DNS к переходу на EDNS. Никто от этих механизмов отказываться не собирается. Отказ привел бы к частичной деградации DNS-сервиса в случае атаки.

Что же такое EDNS? EDNS - набор расширений для оригинального протокола DNS, позволяющий дополнить его рядом полезных функций. Среди ключевых моментов - DNS-cookie. Поддержка EDNS необходима также для работы DNSSEC.

Как изменилось поведение резолверов-участников акции с 1 февраля 2019? Они перестали использовать «костыли» в случае отсутствия каких либо ответов на запросы с EDNS.

Отсутствие ответов возможно в следующих случаях:

а) авторитативный сервер игнорирует запросы, не укладывающиеся в «классический» формат (встречается весьма редко, обычно в «самодельных» системах, так как все распространённые программные пакеты DNS-серверов EDNS поддерживают). В этом случае считается, что авторитативный сервер настроен некорректно, так как он должен прислать тот или иной ответ, например, сообщение об ошибке;

б) запросы или ответы фильтруются промежуточными узлами. Обычно это разнообразные межсетевые экраны. Фильтроваться могут либо запросы/ответы, превышающие определённую длину (типовые для UDP 512 байтов), либо запросы/ответы, которые содержат дополнительные флаги. Первый вариант, с ограничением по длине, исторический и напрямую к EDNS не относится, но, тем не менее, работе протокола препятствует. Второй вариант непосредственно связан с EDNS, так как работает «по DNS-заголовкам», однако на практике этот вариант встречается редко. Фильтрация DNS-пакетов может использоваться в составе мер противодействия DDoS-атакам. Основная особенность здесь в том, что корректно работающий резолвер и корректно работающий авторитативный сервер всё равно не могут провести обмен данными в рамках протокола, так как им мешает промежуточный фильтр.

Ранее резолверы просто повторяли запросы без EDNS. Теперь резолверы участников акции считают авторитативный сервер, от которого не был получен ответ на запрос с EDNS, нерабочим, соответственно, перестают к нему обращаться. В этом и состоял «переломный момент» DNS Flag Day.

Такое поведение подразумевает, что каждый авторитативный сервер должен быть доступен для корректных DNS-запросов, отправляемых с EDNS, и сервер должен отвечать на такие запросы. Из этого не следует, что сервер должен полностью поддерживать EDNS: если сервер отвечает корректным пакетом с кодом DNS-ошибки («Ошибка формата»), то в этом случае резолвер всё же попробует повторить запрос без EDNS. В частности, такое поведение заявлено для Unbound и BIND.

С практической точки зрения, ситуация эквивалентна повсеместному внедрению EDNS, так как устранение «особенностей» обработки EDNS-пакетов там, где эти «особенности» внедрены преднамеренно, проще всего

Нынешний DNS излишне медленен и неэффективен из-за попыток поддержки систем DNS, которые не соответствуют стандартам DNS, установленным два десятилетия назад. Чтобы обеспечить дальнейшую устойчивость системы, пришло время положить конец этой ситуации и исправить несоответствующие системы. Это изменение сделает большинство операций DNS немного более эффективными, а также позволит операторам развертывать новые функции, в том числе новые механизмы защиты от DDoS-атак.

реализовать, внедрив данную технологию в полной мере.

Есть, правда, один момент, о котором уже упоминалось, связанный с парированием DDoS. В этом случае применяется RRL (Response Rate Limit). При установленных RRL часть запросов просто не обрабатывается.

Не стоит думать, что с 1 февраля наступил «конец света» в DNS. Нововведение не является критическим в масштабах Интернета. Во-первых, проблемы с потерями и блокированием EDNS довольно редки. Во-вторых, на проблемных направлениях ещё должны обновиться резолверы. Что касается авторитативных серверов, то большинство (по числу зон) уже так или иначе поддерживает работу с EDNS-пакетами, поэтому здесь массовой недоступности узлов для конечных пользователей ожидать не следует. Если где-то и остались несовместимые "самодельные" решения либо старые версии типового ПО, то им следует доработать программный код или обновить пакеты.

Особенность данной ситуации в том, что существенную роль играет сетевой транспорт и его настройка. То есть факторы, которые к DNS относятся косвенно, и исправить их обновлением ПО DNS нельзя. Здесь, в теории, возможна ситуация, когда крупный провайдер доступа обновил резолверы, но не поменял настройки прохождения пакетов, соответственно, его конечные клиенты останутся без службы DNS (ситуация теоретическая, потому что такой провайдер уже должен был бы отмечать дефекты в работе DNS на своих сетях). Поэтому для исключения возможных аварий требуется участие провайдеров доступа, служб NOC, обеспечивающих прохождение пакетов DNS «в обе стороны» - и на стороне клиентов (рекурсивных резолверов), и на стороне авторитативных серверов. Такое участие состоит в проверке правил межсетевых экранов и подобного программно-аппаратного обеспечения: пакеты EDNS, при штатной работе сети, не должны блокироваться (если тотальное блокирование всё же необходимо, то следует отправлять на адрес источника пакета сообщение DNS о неверном запросе).

Таким образом, принудительное внедрение EDNS в том виде, в каком оно было проведено, больше похоже на PR-акцию, чем на полезное во всех смыслах мероприятие.

В общем-то, тот факт, что разработчики лучше всех знают, как осчастливить конечного пользователя, общеизвестен, а DNS Flag Day – это лишнее тому подтверждение.

Зашифруем всё, или DoT & DoH & ESNI

Не EDNS единым живут гуру DNS. Наиболее популярная тема дискуссий этой зимы - внедрение протоколов DNS over TLS и DNS over HTTP(S). Этим вопросам были посвящены целиком секция на ME DNS Forum[3] и половина секции Emerging Identifiers Technology на ICANN64[4].

Назначение и особенности реализации DoT и DoH прекрасно разобраны в статье Джеффа Хьюстона[5] (на русском ее можно прочитать на сайте «Интернет изнутри»[6]), поэтому здесь мы не будем углубляться в технические детали этих протоколов.

Собственно, обсуждение последствий внедрения DoH и DoT идут не по поводу инструментария реализации, а по поводу последствий таковой.

Основной вопрос дискуссии – приведет ли внедрение DoH и DoT к фрагментации/децентрализации Интернета или эти опасения надуманы? Останется ли мантра ICANN «One World, One Internet, One Namespace» верной?

Основная идея протоколов DoH и DoT заключается в защите от прослушивания DNS-трафика, который ходит между конечным пользователем (точнее, stub resolver-ом конечного пользователя) и кэширующим резолвером.

До тех пор, пока конечный пользователь при обращении к системе DNS использовал кэширующий резолвер своего провайдера, никаких «подводных» камней, принципиально влияющих на работу всей системы DNS, замечено не было.

Рис. 1. Популярность публичного резолвера Google в различных частях света.

Code	Region	DNSSEC Validates	Uses Google PDNS	Samples	Weight	Weighted Samples
XA	World	17.34%	15.11%	103,800,272	1	103,800,272
XF	Oceania	30.22%	10.32%	524,275	1.59	831,060
XE	Europe	22.74%	10.72%	20,139,269	0.84	16,924,634
XC	Americas	21.53%	12.69%	29,661,408	0.69	20,319,733
XB	Africa	16.19%	27.68%	4,775,044	1.91	9,117,193
XD	Asia	14.19%	15.12%	48,700,230	1.16	56,607,582
XG	Unclassified	0.00%	100.00%	720	0	0

Вся информация о запросах пользователя и ответах на них попадала на резолвер провайдера.

Ситуация меняется, когда в качестве кэширующего резолвера используют публичные резолверы, например, Google (8.8.8.8) или CloudFlare (1.1.1.1). Учитывая топологию размещения сервисов Google - Google Cache, - часто указанные публичные резолверы отвечают быстрее резолверов провайдера. Многие провайдеры включают публичные резолверы в настройки DHCP для своих конечных пользователей, чтобы не заморачиваться с поддержкой своих собственных резолверов.

Согласно статистике лаборатории APNIC[7] значительная часть DNS-трафика обрабатывается публичными резолверами Google (рис. 1).

В ряде стран, например, в Монголии, доля использования резолвера Google превышает 50%, т.е. информационные предпочтения граждан этой страны – открытая книга для Google.

Здесь следует заметить еще один момент. Достоверность информации в современной системе DNS обеспечивается технологией DNSSEC[8]. Но все проверки кончаются на уровне кэширующего резолвера, т.е. в дискутируемом случае они заканчиваются на уровне публичного кэширующего резолвера Google или CloudFlare.

В этой связи интересны замечания Пола Хофмана, которые он сделал в своем выступлении на секции Emerging Identifiers Technology на ICANN64. Суть этих замечаний сводится к тому, что, во-первых, в рамках построения замкнутых корпоративных систем одно и то же пространство имен можно резолвить в разные пространства адресов и использовать для этого открытую публичную сеть, а во-вторых, DNS-резолвингом можно управлять через JavaScript.

В настоящий момент можно свободно получить корневую зону и в соответствии с RFC-7706[9] разместить ее на резолвере и включить prefetching[10] (предварительное кэширование соответствий между доменными адресами и IP-адресами) непосредственно на резолвере. Следует также принять во внимание тот факт, что в DNSSEC не подписывается дополнительная секция ответов авторитетных серверов.

Все это позволяет предположить, что при использовании DoH и DoT возможно построение полностью или частично совершенно разных «интернетов» на одном и том же пространстве имен. Все зависит исключительно от позиции провайдера резолвинга и реакции конечных пользователей на факт выявления «аномалий».

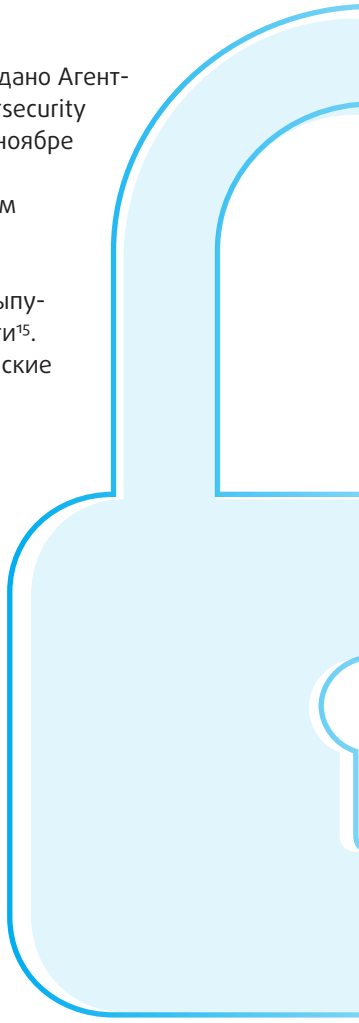
А пока высказываются такие опасения, в браузере FireFox уже реализована поддержка DoH[11] - и в качестве сервера умолчания используется сервер CloudFlare[12].

Справедливости ради, следует заметить, что стандартный протокол HTTPS даже версии 1.3 не обеспечивает полной защиты DNS-информации. В рамках обмена между браузером и сервером в незашифрованном виде передается SNI (Server Name Indication).

Однако здесь тоже есть прогресс. В октябре 2018 FireFox стал первым браузером, в котором была реализована поддержка Encrypted SNI[13].

Подведем итог: вследствие последних изысканий в области безопасного DNS мы можем получить в качестве транспорта DNS-запросов протокол HTTP, встроенные в приложения, например, в браузеры, резолверы и «плоскую» систему резолвинга на основе технологических решений «корпораций добра».

CISA предупреждает



В ноябре 2018 года в США было создано Агентство кибербезопасности (CISA - Cybersecurity and Infrastructure Security Agency). В ноябре 2019 оно подготовило первый отчет, который оказался посвящен вопросам безопасности DNS[14].

В связи с этим корпорация ICANN выпустила свой обзор предметной области[15]. На что обратили внимание американские специалисты?

Во-первых, это атаки на систему регистрации доменных имен, а если говорить более конкретно, на информационные системы регистраторов с целью завладеть «паролями и явками» администраторов доменных имен.

Во-вторых, это атака с целью перехвата DNS-трафика и перенаправления его на DNS-серверы атакующего.

Вообще говоря, первая уязвимость известна давно. Причина в том, что вся «чувствительная» информация в системе регистрации передается до сих пор по электронной почте. На практике никаких других дополнительных средств аутентификации клиенты регистраторов не используют.

Домены регистрируются на год и более. Следовательно, в течение этого срока клиент на сайт регистратора не заходит и информацию своего аккаунта не проверяет. Довольно часто используются публичные почтовые сервисы, а они в случае неиспользования аккаунта могут передавать его новым пользователям.

В этой ситуации получить пароль и идентификатор не так уж и сложно. Имея на руках эту информацию, редко можно «увести домен», как правило, для этого одной электронной почты недостаточно. А вот изменить записи DNS или поменять TLS-сертификаты можно.

На эту брешь в системе регистрации доменов верхнего уровня указывали давно. Подмены адресов случались довольно часто. Но ICANN отреагировала только сейчас, когда появился подробный разбор такого рода атак[16].

По сути, рассматриваются несколько вариантов «редактирования»: замена адресных записей, замена NS-записей, а также возможность подмены легитимных ответов.

В связи с этой атакой также была рассмотрена возможность перехвата DNS-трафика и перенаправление его на DNS-инфраструктуру атакующего. В этом случае не нужно получать «пароли и явки», нужно просто отвечать на полученные запросы.

Если в случае подмены записей необходимо совершенствовать систему аутентификации регистраторов, то в случае утечек и перехватов трафика должен помочь DNSSEC.

О хорошем

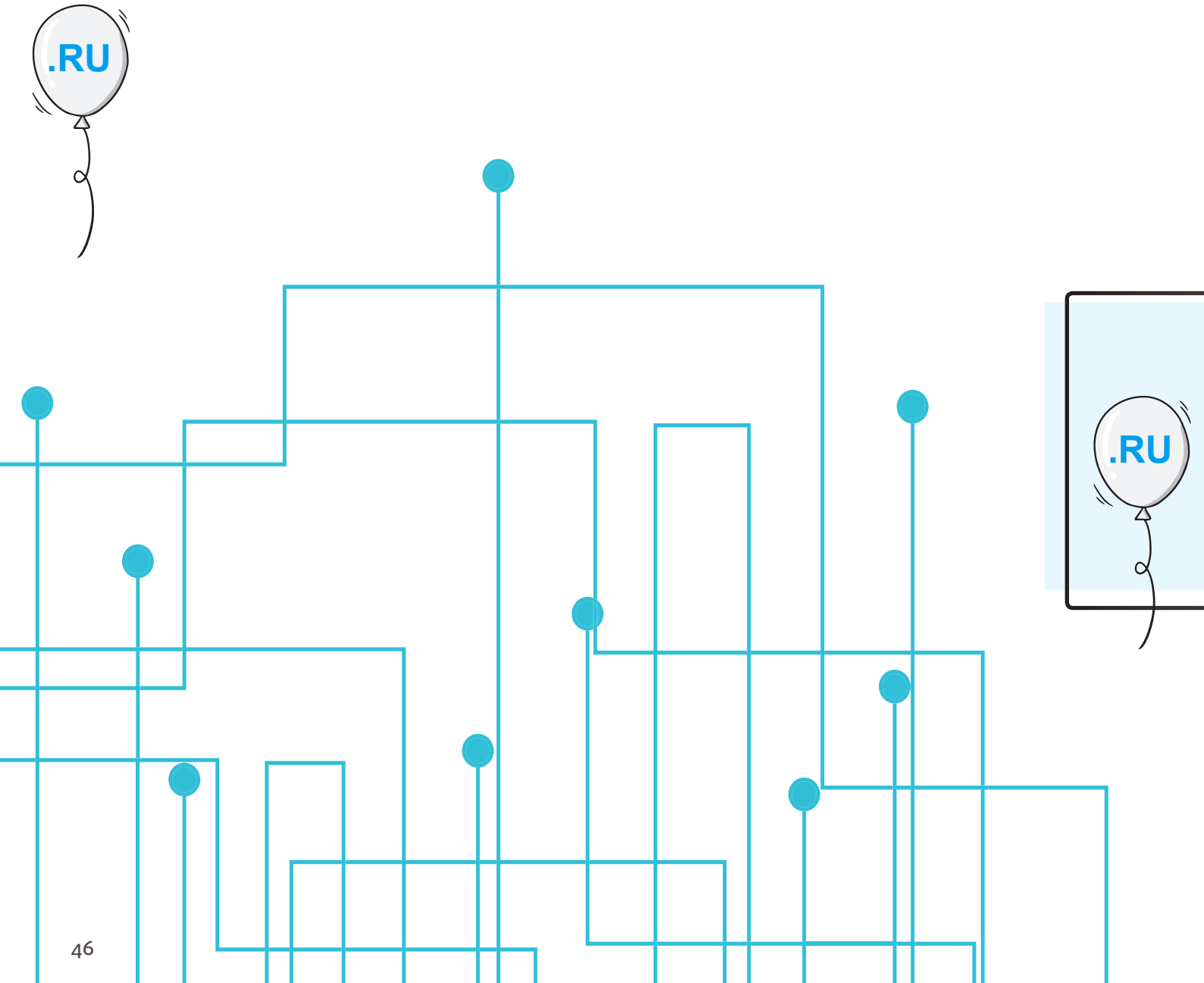
Здесь можно просто процитировать Координационный центр национального домена сети Интернет: «7 апреля 1994 года Российская Федерация получила национальный домен .ru, зарегистрированный международным сетевым центром InterNIC».

Это значит, что 7 апреля 2019 года домену .ru исполнится 25 лет.

Сейчас в «точке ru» зарегистрировано более пяти миллионов доменных имен – это шестое место среди доменов, выделенных странам.

В среднем серверы DNS национального домена в день обслуживают около семи миллиардов запросов. И это количество постоянно увеличивается год от года.

Доменное пространство имен в .ru принято называть Рунетом. С 25-летием, Рунет!



Ссылки

1. https://dnsflagday.net/index-ru.html

2. https://tools.ietf.org/html/rfc6891

3. https://www.mednsf.org/program/

4. https://static.ptbl.co/static/attachments/200822/1552364329.pdf?1552364329

5. http://www.potaroo.net/ispcol/2016-06/dprive.html

6. http://internetinside.ru/privatnost-dns/

7. https://stats.labs.apnic.net/dnssec?s=Uses+Google+Public+DNS&d=Auto&w=30&t=green

8. http://internetinside.ru/bezopasnost-i-privatnost-dns-dlya-konech/

9. https://tools.ietf.org/html/rfc7706

10. https://tools.ietf.org/html/draft-pchowdaiah-prefetch-dns-query-over-http-00

11. https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/

12. https://mozilla.cloudflare-dns.com/dns-query

13. https://tools.ietf.org/html/draft-ietf-tls-esni-03

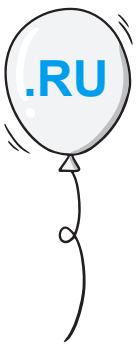
14. https://cyber.dhs.gov/ed/19-01/

15. https://www.icann.org/news/announcement-2019-02-25-ru

16. https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

**Доменное пространство имен в .ru принято называть Рунетом.
С 25-летием, Рунет!**

Сейчас в «точке ru» зарегистрировано более пяти миллионов доменных имен – это шестое место среди доменов, выделенных странам.



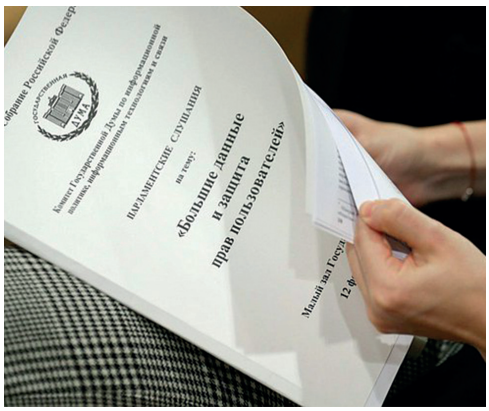
Новости Доменной индустрии

Важные события 2019

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ ПРЕДСТАВИЛ ИТОГИ 2018 ГОДА ДЛЯ ДОМЕННОЙ ИНДУСТРИИ

На 12-й ежегодной конференции «Рунет 2018: итоги года» директор Координационного центра доменов .RU/.РФ Андрей Воробьев представил итоги года для доменной индустрии. В крупнейшем национальном домене .ru насчитывается более 5 миллионов доменных имен, в .рф – более 800 тысяч. С начала 2018 года в двух российских доменах зарегистрировано более 1,4 миллиона доменных имен, этим занимаются 46 аккредитованных регистраторов. Интересно, что за 2018 год существенно сократилась доля зарегистрированных россиянами доменных имен в новых доменах верхнего уровня. Если в 2017 году таких доменных имен было 5,7% от всех, зарегистрированных в России, то в 2018 году их доля составляет всего 0,4%. Доля национальных доменов среди всех имен, которые используются в России, за год увеличилась с 78,3% до 80,9%. Выросла доля регистраций россиянами имен в национальных доменах .ru и .рф: в 2018 году она составляет 80,9%, что на 2,6 процентных пункта выше, чем было в конце 2017 года. Также Андрей Воробьев представил результаты работы проекта «Нетоскоп» в 2018 году, отметив, что в базе проекта находится более 4 миллионов доменных имен (второго, третьего и ниже уровней), которые были замечены или заподозрены в нежелательной активности, а с начала года в базу было добавлено 760 054 доменных имени. Больше всего в базе доменов, на которых размещен вредоносный код – так называемых зловредов. Это 95,8% «плохих» доменных имен третьего уровня и 83,8% «плохих» доменных имен второго уровня.



ОСНОВНАЯ ПРОБЛЕМА В РЕГУЛИРОВАНИИ БОЛЬШИХ ДАННЫХ – ТЕРМИНОЛОГИЧЕСКАЯ

12 февраля в Государственной Думе РФ прошли парламентские слушания «Большие данные и защита прав пользователей», организованные комитетом ГД по информационной политике, информационным технологиям и связи. На парламентских слушаниях обсуждались проблемы определения больших данных, разделения понятий больших и персональных данных, их доступности и конфиденциальности, а также возможности коммерческого использования информационных массивов. В парламентских слушаниях принял участие директор Координационного центра доменов .RU/.РФ Андрей Воробьев. Он познакомил участников с большой работой, которую провела рабочая группа по большим данным, действовавшая при Координационном центре доменов .ru/.рф в 2016-2017 годах. Рабочая группа объединила более 70 участников, представлявших крупнейшие российские интернет-компании – операторов связи, провайдеров контента и облачных услуг, операторов банковских, логистических и других сервисов. Перед рабочей группой была поставлена задача подготовить отраслевые рекомендации для законодателей, разрабатывающих правовые нормы в области больших данных. В ходе работы было выявлено, что основная проблема в регулировании больших данных – терминологическая: большие данные очень часто путают с персональными данными, что приводит к неоправданному ужесточению нормативных требований к операторам данных. Рабочей группой был предложен иной подход, позволяющий отделить ПД от остальных данных о пользователе.

ОБМЕН ОПЫТОМ С ЗАРУБЕЖНЫМИ КОЛЛЕГАМИ – КЛЮЧ К РАЗВИТИЮ НАЦИОНАЛЬНЫХ ДОМЕНОВ

20-21 февраля в Дубае (ОАЭ) прошли два крупных международных отраслевых мероприятия – 75-я конференция Азиатско-Тихоокеанской ассоциации доменов верхнего уровня (APTLD75) и 6-й Ближневосточный DNS-форум (ME DNS Forum). Эксперты Координационного центра доменов .RU/.РФ рассказали о российском опыте и наработках в области развития национальных доменов и формирования устойчивой интернет-инфраструктуры. 20 февраля на секции, посвященной возможным направлениям развития системы корневых серверов, выступил заместитель руководителя отдела внешних коммуникаций Михаил Анисимов, который рассказал о последних российских законодательных инициативах по созданию устойчивой интернет-инфраструктуры и успокоил слушателей, подробно объяснив, что же такое на самом деле «автономный российский Интернет». Во второй день работы APTLD75 и ME DNS Forum эксперты Координационного центра приняли участие в секции, где обсуждались вопросы маркетинга национальных доменов, и в юридической секции. Руководитель отдела внешних коммуникаций Мария Колесникова представила результаты проведенного в 2018 году Координационным центром доменов .ru/.рф исследования особенностей поведения российских пользователей при выборе и покупке доменных имен. На юридической секции Михаил Анисимов рассказал о том, как Координационный центр взаимодействует с представителями государства, и как правила регистрации доменных имен в доменах .RU и .РФ и национальное законодательство дополняют друг друга и помогают обеспечить прозрачную работу в правовом поле как методами государственного регулирования, так и элементами самоуправления.

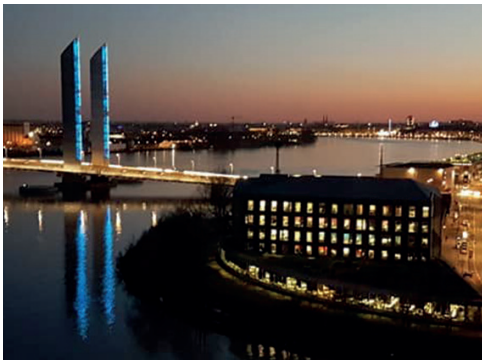
ВОПРОСЫ UNIVERSAL ACCEPTANCE – В ЦЕНТРЕ ВНИМАНИЯ ICANN

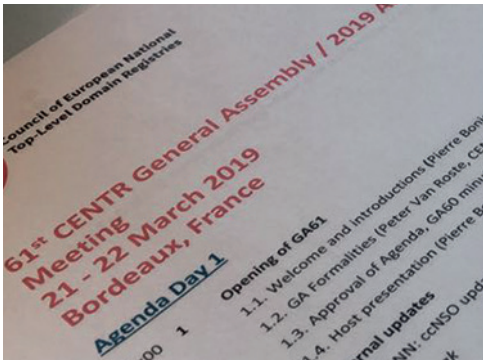
В марте в японском городе Кобе прошла 64-я конференция ICANN, собравшая более 2000 участников из разных стран мира. Одной из главных тем конференции стала проблема всеобщего принятия интернационализированных доменов верхнего уровня (IDN), новых доменов верхнего уровня и адресов электронной почты на нелатинских языках – Universal Acceptance. Этот вопрос стал одним из важнейших на Публичном форуме – одной из главных секций ICANN 64, где любой из участников конференции может задать вопрос совету директоров корпорации. Все выступавшие сходились во мнении, что сегодня необходима еще более активная просветительская работа, а также четкая координация между всеми стейкхолдерами, участвующими в процессах всеобщего принятия. В ходе ICANN 64 состоялась встреча делегации Координационного центра доменов .RU./.РФ, а также представителей российских регистратур IDN-доменов верхнего уровня .москва и .дети с членами UASG. Во время встречи участники договорились плотно сотрудничать над разработкой информационных материалов для продвижения идей Universal Acceptance в регионе. Также во время конференции прошла совместная секция с участием поддерживающих организаций и консультативных комитетов ICANN, посвященная вопросам развития IDN и Universal Acceptance. На секции выступила руководитель отдела внешних коммуникаций Координационного центра доменов .RU/.РФ Мария Колесникова. Она рассказала о том, какие усилия в этой области прилагает российская регистратура, и каким образом должна вестись работа с конечными пользователями.

СОЦИАЛЬНЫЕ ПРОЕКТЫ ДЛЯ ШКОЛЬНИКОВ И ИХ РОДИТЕЛЕЙ

11-12 февраля в Общественной палате РФ прошел IV Съезд Национальной родительской ассоциации. Участникам съезда были представлены информационно-методические материалы по родительскому просвещению, на съезде обсуждались программные документы, описывающие участие родителей в реализации государственной семейной и образовательной политики. Важным событием съезда стало открытое заседание Экспертного совета НРА, на котором выступил директор Координационного центра доменов .RU/.РФ Андрей Воробьев. В докладе «Роль социально ориентированных НКО в реализации социальных проектов Координационного центра, направленных на популяризацию доменов RU/РФ и приуроченных к 25-летию Рунета» директор КЦ подробно остановился на том, как Координационный центр вместе с партнерскими организациями формирует в Рунете пространство, безопасное для детей и подростков, и организует социальные и просветительские программы, в которых участвуют тысячи российских школьников. Отдельно было рассказано о проектах, которые Координационный центр реализует вместе с известными НКО – телеканалом «Карусель», Школой новых технологий, Фондом социального кино и другими. Например, в год 25-летия домена .ru КЦ совместно с Фондом социального кино планирует выпустить цикл фильмов про то, как Интернет помогает в жизни людям из социально незащищенных категорий.

25 февраля в РАНХиГС открылась Всероссийская ежегодная научно-практическая конференция «Информационная безопасность и дети». Конференция направлена на обсуждение самых актуальных вопросов обеспечения информационной безопасности в образовательных организациях через механизм государственно-общественного управления. На открытии конференции выступил директор Координационного центра доменов .RU/.РФ Андрей Воробьев. В докладе «Роль саморегулирования в борьбе с противоправным контентом» Андрей Воробьев подчеркнул важность использования педагогическим сообществом наработок интернет-компаний, а также представил социальные проекты Координационного центра доменов .RU/.РФ: игру «Изучи интернет – управляй им!» и другие познавательные и просветительские проекты для детей и юношества. В заключение своего выступления Андрей Воробьев дал старт регистрации на Всероссийский семейный IT-марафон 2019, который уже в третий раз проводится Координационным центром вместе с Национальной родительской ассоциацией, Академией инновационного образования и фондом «Разумный Интернет».





АНДРЕЙ ВОРОБЬЕВ: «НАХОДИТЬ РЕШЕНИЯ ДЛЯ БОРЬБЫ С ПРОТИВОПРАВНЫМ ИСПОЛЬЗОВАНИЕМ ДОМЕНОВ МЫ МОЖЕМ ТОЛЬКО ВМЕСТЕ»

21-22 марта в Бордо (Франция) состоялась 61 Генеральная ассамблея Совета европейских регистратур национальных доменов (61st CENTR General Assembly). В ее работе приняли участие более 60 делегатов, в том числе представители Координационного центра доменов .RU/.РФ. Делегаты ассамблеи CENTR обсудили возможное влияние на отрасль функции обращения к DNS поверх HTTPS (DoH, DNS over HTTPS). Представитель ICANN Рой Арендс (Roy Arends) рассказал, чем технология DoH отличается от традиционной DNS, и почему развитие технологии, изначально придуманной для того чтобы увеличить приватность пользователя, становится поводом для большого количества новых вопросов и сомнений. Эти же вопросы обсуждались и в последующей панельной дискуссии, в которой участвовали сотрудники национальных регистратур и приглашенные эксперты. Другим вопросом ассамблеи CENTR стало обсуждение роли регистратур национальных доменов в борьбе с противоправным контентом.

На ассамблее с докладом выступила заместитель директора Координационного центра доменов .RU/.РФ, член Совета директоров CENTR Ирина Данелия. Она рассказала о последних законодательных инициативах в Российской Федерации, в том числе про ставший известным не только в России, но и за ее пределами т.н. закон об автономизации Рунета.

ФОНД РАЗВИТИЯ ИНТЕРНЕТ

Безопасность

«ФОНД РАЗВИТИЯ ИНТЕРНЕТ» ПРИСОЕДИНИЛСЯ К МЕМОРАНДУМУ О СОТРУДНИЧЕСТВЕ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

28 марта 2019 года Координационный центр доменов .RU/.РФ и «Фонд развития Интернет» (регистратура домена .su) подписали меморандум о сотрудничестве. Этот меморандум направлен на то, чтобы скоординировать усилия регистратур российских доменов верхнего уровня для противодействия использованию доменов в противоправных целях и укрепления кибербезопасности. Таким образом, регистратура домена .su присоединилась к усилиям других регистратур российских доменов в области обеспечения информационной безопасности. В ноябре 2018 года свои подписи под меморандумом поставили руководители Координационного центра доменов .RU/.РФ и «Фонда содействия развитию инфраструктуры Интернет» (FAITID) – регистратуры доменов верхнего уровня .moscow и .москва.

Календарь событий: 2019 год

Международные события

20-24 мая
RIPE 78,
Рейкьявик, Исландия

Встречи RIPE проводятся два раза в год и собирают более 700 участников для обсуждения вопросов политики распределения номерных ресурсов (IP-адресов и номеров автономных систем) в зоне обслуживания RIPE NCC, сотрудничества, а также технических вопросов, связанных с маршрутизацией, DNS, связностью, измерениями и инструментарием. Прием пленарных докладов заканчивается 9 апреля, но блиц-доклады принимаются до и в течение встречи. https://ripe78.ripe.net/

3-4 июня
ENOG 16/Региональная встреча RIPE NCC,
Тбилиси, Грузия

ENOG (Евро-азиатская группа сетевых операторов) представляет собой региональный форум интернет-специалистов, занимающихся важнейшими аспектами работы Интернета. В рамках форума они имеют возможность обмениваться опытом и знаниями по вопросам, присущим Российской Федерации, странам СНГ и Восточной Европы. Прием пленарных докладов заканчивается 19 апреля 2019.
https://www.enog.org/enog-16/

10-12 июня
NANOG 76,
Вашингтон, США

Североамериканская группа сетевых операторов (The North American Network Operators Group, NANOG) является одной из самых активных профессиональных ассоциаций в области сетевой архитектуры, конфигурации и технического администрирования сетей в Интернете. Основной фокус NANOG - на технологиях и системах, обеспечивающих работу Интернета: система глобальной маршрутизации, DNS, пиринг и связность. NANOG имеет активный список рассылки и проводит конференции три раза в год. Поскольку инженерные вопросы NANOG имеют глобальный характер, участие в списке рассылки и конференциях может быть полезно широкому кругу технических специалистов в области сетевых технологий Интернета. Прием пленарных докладов заканчивается 6 мая 2019.
https://www.nanog.org/

18-20 июня
EuroDIG,
Гаага, Нидерланды

Европейский диалог по управлению Интернетом (EuroDIG) является открытой многосторонней платформой для обмена мнениями об Интернете и его управлении. Созданная в 2008 году несколькими организациями, представителями правительства и экспертами, она способствует диалогу и сотрудничеству с интернет-сообществом по вопросам государственной политики в отношении Интернета.
https://www.eurodig.org/index.php?id=76

17-21 июня
AIS/AfNOG/AfriNIC,
Кампала, Уганда

Ежегодная встреча AIS представляет собой региональную многостороннюю конференцию по ИКТ, которая объединяет бизнес и техническое сообщество в области ИКТ в Африке для обсуждения региональных и глобальных проблем и проблем ИКТ. AIS организуется совместно AFRINIC и AfNOG.
Встречи AFRINIC предоставляют уникальную возможность для лиц и организаций, связанных с Интернетом, собираться для обсуждения политик, регулирующих распределение номерных интернет-ресурсов в африканском регионе, для обмена техническими знаниями и участия в семинарах и учебниках.

AfNOG - это форум для сотрудничества и обмена технической информацией между операторами сетей в Африке. https://www.afnog.org/

24-27 июня
ICANN 65,
Марракеш, Марокко

Встречи ICANN проводятся три раза в год в различных регионах земного шара для того, чтобы предоставить возможность активным членам сообщества ICANN лично поучаствовать в обсуждении насущных проблем. Общей темой, конечно, является DNS - глобальная система трансляции имен. Здесь обсуждаются как технические вопросы обслуживания услуг DNS, так и юридические и бизнес-аспекты предоставления регистрационных услуг. Участие во встречах ICANN бесплатно.
https://meetings.icann.org/en/marrakech65

21-26 июля
IETF 105,
Монреаль, Канада

IETF (Internet Engineering Task Force) является одной из основных организаций по разработке стандартов Интернета. В основном работа в IETF проходит в многочисленных списках рассылки, соответствующих различным рабочим группам (этих групп более 100). Совещания IETF - это хорошая возможность познакомиться с новейшими тенденциями в области сетевых технологий и принять участие в их разработке. В выходные перед началом совещаний пройдет IETF Hackathon, посвященный практическому воплощению стандартов IETF, и IETF Codesprint по доработке приложения datatracker - важного инструментария IETF.
https://www.ietf.org/how/meetings/105/

В России

22-25 мая
Сочи, Красная поляна

КРОС-2019

Конференция российских операторов связи КРОС проводится ежегодно с 2006 года. Организатор мероприятия - компания НАГ. Аудитория мероприятия - специалисты и руководители компаний телекоммуникационной отрасли. Для многих из них конференция давно стала крупнейшим отраслевым событием года, традицией, навсегда связанной с историей развития телекоммуникаций в России.
https://cros.nag.ru/

29-31 мая
Казань, «Корстон»

IT&Security Forum 2019

ITSF – это площадка для выступлений, дискуссий и демонстраций цифровых технологий. Она была создана 12 лет назад, и развивалась, формируя сообщество представителей IT-индустрии и различных других отраслей экономики чья эффективность и развитие зависят от цифровых технологий. Более 1000 участников в 2018 году, компании из 80 городов, 660+ м^2 выставочных площадей, более 70 выступлений экспертов.
https://itsecurityforum.ru/

В Москве

24-25 апреля
Лесные дали

Форум MULTISERVICE (MUSE)

Ежегодный форум операторов связи и вещателей MULTISERVICE (MUSE) это крупнейшее мероприятие отрасли, которое содержит не только формальную программу, но и славится своей неформальной стороной. Доклады и круглые столы, контент-шоу с бизнес-кейсами, технические и правовые секции, диалог с властью и регулятором, все с максимальным акцентом на полезность и актуальность.
http://muse-forum.ru/

10-11 мая
Flacon

Data Fest6

Международная серия бесплатных конференций, объединяющих всех связанных с Data Science исследователей, инженеров и разработчиков. 10 мая: индустриальный день с глубоким погружением в реальные Data Science и Machine Learning приложения в разных областях; 11 мая: научный день, все самые горячие исследовательские и инженерные темы, воркшопы.
https://datafest.ru/

10-11 июня
Математический
институт
им. В.А. Стеклова РАН

OS Day 2019. Инструменты, их разработка и опыт применения

Шестая научно-практическая конференция OS DAY посвящена инструментам разработки операционных платформ и системного программного обеспечения. Главная тема – проблемы и достижения в сфере создания инструментов, которые обеспечивают высокий уровень кибербезопасности в следующих процессах: отладка и анализ поведения операционных систем, верификация и инструментация системного и прикладного кода, управление требованиями и тестированием.
https://osday.ru/index.html

25-27 июня
Сколково

Бизнес-фестиваль инноваций и цифровизации

«Дойче Мессе РУС» и Технопарк «Сколково» совместно представляют самую крупную в мире выставку в области информационных технологий и телекоммуникаций. Проект имеет перспективы стать одним из лидирующих IT-мероприятий и достойным преемником ганноверского проекта, сделать решения и продукцию более ощутимыми, объединить технологию и бизнес в новом, увлекательном формате.
https://cebit-russia.ru/

MSK IX

10 ГОРОДОВ

500+ УЧАСТНИКОВ

42 ПЛОЩАДКИ

21 УЗЛЕЛ DNS-СЕТИ

ПОДКЛЮЧЕНИЯ ДО **100G**

ТРАФИК **3,3Тбит/с**

MSK-IX ускоряет коммуникации между интернет-компаниями, предоставляя нейтральную платформу Internet eXchange для обмена IP-трафиком между сетями и глобальную распределенную сеть DNS-серверов для поддержки корневых доменных зон.

Более 500 организаций используют сервисы MSK-IX для развития сетевого присутствия в 10 городах. К MSK-IX подключены операторы связи, социальные сети, поисковые системы, видеопорталы, провайдеры облачных сервисов, корпоративные и научно-образовательные сети.

127083, г. Москва, ул. 8 Марта, д. 1, стр. 12
тел.: +7 495 737-92-95
www.msk-ix.ru


+7 495 737-92-95
WWW.MSK-IX.RU

Интернет изнутри

2019