№14
Декабрь 2020

MSK IX

Интернет изнутри

Инфраструктура передачи данных

Содержание:

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

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №14, дата выхода: Декабрь 2020 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

Продакшн:
Гончаров А.В.

Дизайн и вёрстка:
artnovikovaolga.ru

Арт-директор:
Новикова Ольга

Дизайнер:
Сдобнова Юлия

Корректор:
Рябова Наталья

Обложка разработана с использованием ресурсов сайта Freepik.com

С юбилеем, MSK-IX!

главный редактор,
Андрей Робачевский

Дорогой читатель!

В этом году крупнейшая точка обмена трафиком страны и одна из крупнейших в мире, MSK-IX, празднует свой **25-летний юбилей**. Возраст солидный, сравнимый с возрастом самого Интернета! Но у многого, связанного с Интернетом, с возрастом происходит омолаживание – технологии становятся все более продуктивными, приложения все более удивляющими, а число пользователей только растет. Так и MSK-IX, рожденная с одним коммутатором, связавшим семь провайдеров, сегодня обеспечивает связность более 500 участников, передавая более 4 Гб данных в секунду.

О том, как это начиналось и во что превратилось, рассказывают две статьи – «IXP - перекресток Интернета» от Елены Ворониной и «Эволюция обмена трафиком» Александра Ильина.

Мы также пригласили «ветеранов отрасли» поделиться своими воспоминаниями и взглядами на сегодняшний и завтрашний Интернет. Здесь вы встретите тех, чьи идеи, труд и энтузиазм заложили основы Рунета и стали залогом его успешного развития.

Юбилей заставляет не только оглянуться назад, но и поразмышлять о настоящем, а также заглянуть в будущее. Джон Левин познакомит читателей с новыми разработками в IETF по усилению защищенности электронной почты – кстати, первого непредвиденного «приложения-убийцы» молодого Интернета. Я же попробую взглянуть на историю борьбы за качество и ее будущую траекторию.

Этот год, к сожалению, не только год юбилея. Кризисная ситуация, связанная с вирусом **COVID-19**, еще раз доказала работоспособность Интернета и организаций, обеспечивающих его функционирование. Но не обошлось и без «черных лебедей», о которых расскажет Мадина Касенова в соавторстве с Еленой Ворониной.

Не оставили мы без внимания и нашу стандартную тему «Новости науки и техники». Павел Храмцов приглашает вас в свою рубрику.

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.

IXP - перекресток Интернета

Елена Воронина

Перекресток – место **пересечения**, примыкания или разветвления дорог на одном уровне.

Правила дорожного движения

MSK-IX – 25 лет! Кажется, еще вчера проект был просто идеей. Четверть века – и... можно обернуться назад и увидеть, какой длинный путь пройден, какая огромная работа проделана, какой результат достигнут.

25 лет назад, с разбросом в 1-3 года, в мире появилось множество IXP (Internet eXchange Point, Точка обмена трафиком), большинство которых успешно ведет деятельность до сих пор и широко известно профессионалам телекоммуникационной отрасли, а в последнее время и более широкому кругу предприятий интернет-бизнеса.

В чем причина устойчивости такого узкоспециализированного и довольно трудного для понимания широкой публикой проекта, как IXP? Пробуем разобраться.

В 1995 году Интернет уже перестал быть инструментом только ученых и военных. В Москве появилось более одного провайдера, а именно семь, трафик между сетями которых проходил через зарубежные сети. Это было дорого и долго. Естественно, провайдеры были заинтересованы в быстром обмене трафиком. Быстрый обмен трафиком с использованием нейтральной инфраструктуры - именно то, что мог предложить Internet exchange провайдерам.

Это справедливо и сегодня, 25 лет спустя, базовая идея пиринга не изменилась: быстрое соединение с соседними сетями, организация оптимальных, самых быстрых маршрутов трафика, особенно на региональном уровне. Если не акцентироваться только на технологической составляющей, идея локальных IXP мне представляется очень патриотичной!

Соглашение семи провайдеров об обмене интернет-трафиком положило начало российской сети Интернет, сети провайдеров получили общую точку Internet eXchange Point: Перекресток семи дорог...

И действительно, ассоциация с дорожным перекрестком как нельзя лучше иллюстрирует роль IXP в транспортной инфраструктуре Интернета. Перекресток – необходимая инфраструктурная составляющая транспортной сети, и появляться он должен там, где необходимо, чтобы **организовать** движение так, чтобы ездить было быстро и удобно, а разобраться в этом было бы просто.

Поэтому важной составляющей успеха IXP является место размещения: точки обмена трафиком размещаются в местах концентрации кабельной сетевой инфраструктуры, которую имеют возможность использовать более чем три провайдера. Нужно заметить, что зачастую IXP являются катализатором роста ЦОД: провайдеры стремятся разместить сетевые узлы в тех ЦОД, где есть возможность быстрой организации соединений сетей, как мультипиринговых, так и приватных.

Говоря кратко, важно оказаться в нужном месте и в нужное время.

Несмотря на то, что основная идея IXP в целом остается прежней, технологически точки обмена трафиком кардинально изменились: это касается и производительности оборудования, и емкости каналов связи, и концепции «логической точки пиринга», и разнообразных сопутствующих пирингу «бантиков».

На одной из рабочих групп IXPs в рамках конференции RIPE после нескольких презентаций европейских точек обмена трафиком Роб Блокзайл (Rob Blokzijl, сооснователь и почетный председатель RIPE) заметил, что появилось логическое противоречие: точки обмена трафиком рассказывают о распределенных пиринговых сетях. Почему? Они же точки (IXP – internet exchange point)!

Менялись коммуникационные технологии, новые формы доступа в Интернет потребовали развития инфраструктуры для предоставления услуг нового поколения меняющемуся миру. Предложение услуг для все более мобильных конечных пользователей означало, что сети должны были стать ближе к пользователю. Это также означало, что сети должны быть соединены с большим количеством центров обработки данных, а центры обработки данных должны быть соединены друг с другом – и это должно быть сделано как в глобальном, так и в локальном масштабе.

Соглашение семи провайдеров об обмене интернет-трафиком положило начало российской сети Интернет, сети провайдеров получили общую точку Internet eXchange Point: Перекресток семи дорог...

Новые сетевые реалии привели к изменению топологии канальной инфраструктуры пиринговых сетей, но логически, на транспортном уровне, IXP так и осталась точкой, логической точкой. Перекресток сохранил свою функцию!

В мире цифровой глобализации обмен трафиком данных в IXP позволяет одним подключением осуществить связность с сотнями сетей. Это обеспечивает гибкость маршрута, надежную и устойчивую связь, избыточность и повышенное качество сети, контроль, а также выход на стратегические рынки и экосистемы из удобного места, которое может быть монетизировано и оптимизировано.

Идея IXP популярна во всем мире. В ноябре 2020 в Peering DB (база данных пиринговых отношений сетей с использованием точек обмена трафиком) насчитывалось более 800 IXPs. IXP есть во всех странах, в которых есть собственные интернет-ресурсы и интернет-провайдеры. История их появления и развития разнообразна. Первые IXP создавались по инициативе интернет-провайдеров или профессиональных ассоциаций, но затем к этой идее стал проявлять интерес сетевой бизнес: контент-провайдеры, операторы центров обработки данных выступали инициаторами организации региональных IXP. ЦОДы открывают возможность для всех сетевых операторов работать в «одноранговом» режиме, а для контента важен быстрый доступ к широкой аудитории пользователей. Кстати, операторы такого важного сетевого сервиса, как DNS, традиционно организуют к нему доступ через подключение к точкам обмена трафиком. Операторы авторитетных DNS-серверов, являясь профессионалами в области сетевых технологий, быстро оценили преимущества быстрого доступа к широкой аудитории пользователей, а также снижение возможности масштабных атак на отказ в обслуживании в условиях локальной связности.

Важной составляющей успеха IXP является место размещения: точки обмена трафиком размещаются в местах концентрации кабельной сетевой инфраструктуры, которую имеют возможность использовать более чем три провайдера. Нужно заметить, что зачастую IXP являются катализатором роста ЦОД: провайдеры стремятся разместить сетевые узлы в тех ЦОД, где есть возможность быстрой организации соединений сетей, как мультипиринговых, так и приватных.

Признавая IXP важным сетеобразующим (по аналогии с градообразующим) элементом интернет-инфраструктуры, возникли международные программы по созданию IXP в развивающихся странах, странах Африки и пр. Точки обмена трафиком должны помочь снизить затраты на создание сетевой инфраструктуры (региональный трафик не должен утилизировать межрегиональные каналы) и создать условия для оптимального доступа к региональному контенту.

Многие государства и региональные правительства оказывают поддержку точкам обмена трафиком, оценивая возможности локализации регионального трафика и доступности региональных информационных ресурсов. В самом деле, странно и нетехнологично, если житель удаленного региона получает сетевые государственные услуги в столице или по каналам связи с использованием сети иностранного государства.

В условиях новой реальности, к которой мы привыкаем начиная с 2020 года, многие компании перешли на режим удаленной работы. В этом случае IXP также обеспечивают более безопасную среду для тех компаний, которые поддерживают работу сотрудников из дома. IXP гарантирует, что конфиденциальный трафик остается локальным, а не путешествует через Франкфурт, Стокгольм или Амстердам. Кроме того, сетевая задержка регионального маршрута минимальна.

Подумайте об этом так: когда вы не контролируете свою сетевую маршрутизацию, вы не знаете, куда идет трафик. Он может идти сначала на запад, а потом на восток, к своей конечной точке. Неоптимальная связность может подорвать успех корпоративных приложений или стратегий облачных вычислений, сдерживая бизнес на высококонкурентном рынке. Подобно «петлям», которые являются наихудшим случаем неоптимальной маршрутизации, зигзагообразная или вообще плохая маршрутизация добавляет задержку, jitter и лишние промежуточные устройства и точно так же снижает производительность сети. А что вы знаете о маршрутной и пиринговой политике своего вышестоящего провайдера? Вот то-то и оно.

Высокопроизводительные приложения, как, например, высококачественные видеостриминг, виртуальная реальность или периферийные вычисления, требуют более тесных точек агрегации и доступа к конечным пользователям. Позволяя сетям сегодняшнего дня более эффективно маршрутизировать трафик, достигать более низкой задержки, снижать затраты и увеличивать охват, IXPs обеспечивают основу для более эффективной экосистемы сетей и приложений.

Тренд последнего времени – Интернет вещей, умные сообщества.

Представьте себе будущее, полное самоуправляемых автомобилей, которые должны подключаться к системам управления - своим маршрутам движения, светофорам и т.д. Все устройства Интернета вещей, которые должны взаимодействовать друг с другом, должны делать это напрямую. Данные, которые они посылают, не должны проходить через третью сторону, за много километров, а затем возвращаться обратно, чтобы добраться до

места назначения. Светофор должен послать свой сигнал автомобилю наиболее коротким путем! Представьте ситуацию, если возникнет сетевая задержка!

Другой пример - игровая индустрия. Для производства одной игры часто задействовано несколько компаний, работающих над различными компонентами. Компании обмениваются большими объемами данных. А когда игра готова, она должна быть максимально приближена к своему конечному пользователю, иначе будет страдать качество и кошелек игрока. То же самое справедливо и для медиаиндустрии.

И совсем бытовой пример. Многочисленные владельцы дачных участков все чаще следят за своими системами (безопасность или газовый котел) с помощью Интернета. Не все поддержат идею доступа к любимым устройствам через соседние регионы!

Имея IXP, город создает городскую сетевую экосистему, которая может привлечь и удержать эти типы контента и сервисов.

В связи с продолжающейся трансформацией цифровых предприятий, переносом данных и вычислительных процессов в облако, потоковой передачей с увеличивающимся разрешением и новыми областями технологий, такими как 5G, искусственный интеллект или Интернет вещей, трафик данных в настоящее время растет с поразительной скоростью. Без хорошей связанности такие технологии, как Интернет вещей, не могут быть реализованы. Инфраструктура IXP позволяет распределять нагрузки при пиках трафика, минимизировать риск простоев, сокращать задержки и помогать клиентам масштабировать свои бизнес-модели. Минимальные задержки особенно важны для будущих технологий. Дело не столько в объеме, сколько в качестве. Чем ближе ресурс физически находится к клиенту, тем короче время доставки пакета данных. Чем более развиты цифровые бизнесы, чем больше появляется специализированных технологических сетей, тем важнее становится функция организации связанности этих сетей.

Интернет изнутри
IXP - перекресток Интернета 25 лет MSK-IX

Доступ к качественному, надежному и быстрому Интернету важен как никогда. От геймеров до компаний, внедряющих «умные решения», от производственных конвейеров, городов до транспортной системы люди, компании и сами сети продолжают расширять потребность в высокоскоростном Интернете. Одним из ключевых элементов этой эволюции является использование точек обмена трафиком. IXP являются мощным решением оптимизации производительности и масштабируемости сети, обеспечивая готовность сегодняшнего Интернета к задачам и приложениям будущего.

25 лет MSK-IX

«Ты помнишь, как всё начиналось?
Всё было впервые и вновь...»
(А. Макаревич)

В этом году MSK-IX празднует свой 25-летний юбилей. Повод оглянуться назад и поразмышлять, как это начиналось и какой огромный путь был пройден. Мы попросили ветеранов отрасли поговорить об истории развития MSK-IX и Интернета в России в целом, поделиться своими воспоминаниями о ключевых событиях прошлого и взглядами на будущее.

Юные годы видеоконференций в Интернете

Юрий Гугель, РосНИИРОС, инженер

Сейчас, когда MSK-IX уже 25 лет, при онлайн-видео или аудиотехнологиях взаимодействия территориально распределенных коллективов или отдельных пользователей Интернета возникает только один вопрос - как подобрать удобную программу для проведения видеоконференции. А вот когда MSK-IX был один год, стояли другие вопросы.

Да, было понимание того, что Интернет можно использовать для общения ученых, телемедицины, дистанционного обучения, проведения конференций, совещаний и т.д. Но был вопрос, как это сделать на каналах передачи данных с полосой пропускания 64 кбит/с, да к тому же загруженными под 100% интернет-трафиком пользователей. И тут на помощь приходила технология Multicast, позволяя рационально использовать пропускную способность сети и вычислительные ресурсы устройств, участвующих в обработке данных.

Это сейчас надо включить программу видеоконференции и ввести имя сервера. 25 лет назад перед включением программы на компьютере необходимо было подготовить всю транспортную сеть между участниками для проведения видеоконференции. Вся сеть между участниками видеоконференции должна была поддерживать Multicast-трафик. Это накладывало серьезное ограничение на размещение участников видеоконференции - они находились в одной сети.

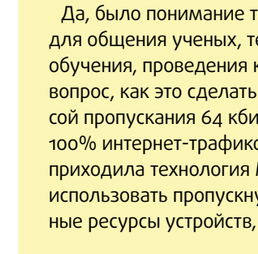
В далеком 1995 году на базе федеральной университетской компьютерной сети RUNNet, используя в качестве транспортной инфраструктуры спутниковые каналы с полосой пропускания 64 кбит/с, проходили видеоконференции, в которых принимали участие до 15 университетов одновременно. Это были Мероприятия с большой буквы.

В подготовке к проведению видеоконференции принимали участие все админы университетов, где планировалось проведение. Выбор самой программы видеоконференции не вызывал вопросов. Такие программные средства, как VAT (Visual Audio Tool), VIC (Video Conference) от LBNL's Network Research Group (https://ee.lbl.gov), заложили основу и определили стандарты для текущих звуковых чатов через IP (VoIP) и мультимедийных интернет-приложений. Специально подготавливалась магистральная сеть и сети университетов для прохождения Multicast-трафика. Оптимизировался трафик на сети, обеспечивая, сколько возможно, доступную полосу пропускания на каналах между университетами.

При проведении самой видеоконференции были своеобразные рекомендации участникам. Не шевелиться и не вращать головой. Видеоконференция являлась, по сути своей, мероприятием, которое позволяло передавать видеоизображение и звук. При ограниченной полосе пропускания звук более критичен к потерям данных на промежуточной транспортной сети, ему обеспечивался приоритет перед видео. А потери на видео не так заметны, если участники не шевелятся.

Для передачи многоадресного IP-трафика между различными сетями уже во всем Интернете была развернута виртуальная сеть Mbone (сокращение от «multicast backbone»). Mbone использовалась для совместных распределенных коммуникаций, таких как видеоконференции или общие рабочие места для совместной работы, и, конечно, для видеотрансляций (какой-то аналог современных вебинаров). На её основе работала система виртуальных комнат для видеоконференций. Mbone получила развитие в научно-исследовательских и образовательных международных сетях и исследовательских центрах. Коммерческие сервис-провайдеры не жаловали Mbone из-за того, что приложения, использующие Mbone, создавали большие потоки данных.

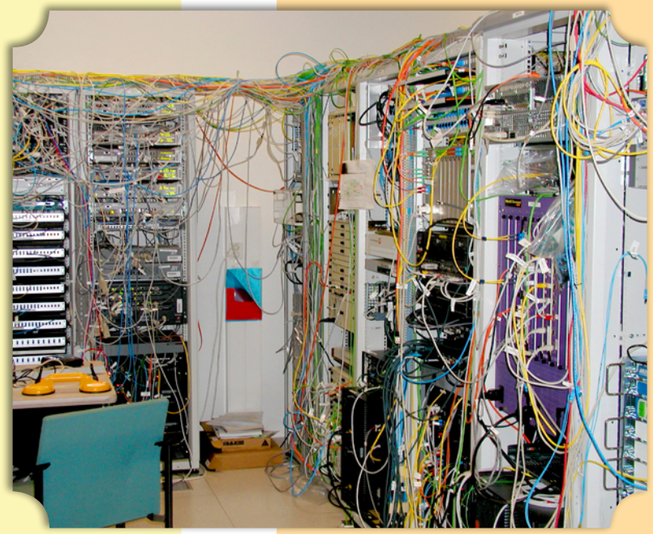
Для внутрироссийского обмена мультимедийным трафиком между сетями MSK-IX в 2000 году запустил отдельный выделенный Multicast-IX. А когда сеть RBnet (один из многих проектов Российского НИИ Развития общественных сетей, РосНИИРОС) сделала подключение в Чикаго к широко известной специализированной точке обмена трафиком научных сетей STARTAP/StarLight, связность с Mbone получили и все российские сети, имеющие подключение к MSK-IX. Это подключение RBnet к Mbone сделало возможным организацию видеоконференций на международном уровне участников московской точки обмена трафиком MSK-IX.



Оглядываясь назад

Аркадий Кремер, президент АДЭ (Ассоциация документальной электросвязи)

Создание Московской точки обмена интернет-трафиком по инициативе РосНИИРОС и образование АО «Центр взаимодействия компьютерных сетей MSK-IX» безусловно относятся к ключевым событиям, происходившим на заре развития российского Интернета. В 1990-е годы маршрутизация трафика российских пользователей осуществлялась через зарубежные сети, объем российского контента был минимален и пользователи обращались прежде всего к зарубежным интернет-ресурсам. В стране отсутствовала развитая IP-инфраструктура, обеспечивающая эффективное взаимодействие российских сетей, предоставляющих доступ в Интернет. Количество пользователей Интернета в стране было невелико, объем потребляемого ими трафика незначителен - и доминирующей технологией доступа являлась Dial up.



За прошедшие с тех пор 25 лет ситуация в российском сегменте Интернета изменилась радикально. Драматически выросло количество пользователей и Россия стала одним из крупнейших интернет-рынков Европы. При этом российская аудитория, в массе своей, не англоязычная и потребляет, прежде всего, русскоязычный контент, генерируемый и располагающийся внутри страны.

Изменились технологии доступа. Dial up ушел в прошлое, и абоненты потребляют широкополосный доступ по фиксированным и мобильным сетям на мегабитных скоростях. В стране созданы разветвленные операторские IP-сети, конкурирующие между собой и покрывающие практически всю населенную территорию. Можно констатировать, что сегодня в России сформирована одна из наиболее самоподдерживающихся и самодостаточных интернет-экосистем в Европе.

Говоря об истории успеха, хотел бы выделить три фактора: профессионализм, сотрудничество, образовательно-просветительская деятельность.

Первый фактор – это заинтересованность профессионального научно-технического сообщества. Подлинное развитие Интернета в средство повышения эффективности государственного управления, ведения бизнеса и улучшения жизни людей происходило по мере повышения заинтересованности в его использовании со стороны крупных операторских компаний и разработчиков технических средств. Профессиональный бизнес в полной мере сумел реализовать основное свойство и предназначение Интернета – объединять для совместной работы многочисленные и разнообразные устройства и информационные ресурсы, подсоединяемые к различным сетям. Интернет – это не сети, не устройства и не информационные ресурсы, а то, что их объединяет.

Второй фактор – сотрудничество на национальном и международном уровне. Важным проявлением такого сотрудничества явилось образование Координационного центра развития национальных доменов. Сегодня этот центр является национальным техническим общественно-государственным регулятором развития доменной инфраструктуры в нашей стране. Российские эксперты принимают участие в деятельности различных международных организаций, занимающихся вопросами развития Интернета.

Третий фактор – образовательно-просветительская деятельность. Это подготовка кадров, способных развивать интернет-технологии, обеспечивая технологическую независимость и информационную безопасность, и готовых представлять интересы страны в международных организациях, создание и внедрение механизмов обеспечения доверия и безопасности при использовании Интернета, формирование информационной культуры цифровой трансформации.

В заключение хотел бы отметить, что вклад MSK-IX в то, что достигнуто, и роль в том, что еще предстоит сделать, трудно переоценить!

История про первые блокировки нежелательного контента

Андрей Колесников, директор Ассоциации интернета вещей

Дело было в 1999 году, когда мне, будучи начальником сервиса «Россия-Он-Лайн», приходилось решать не только технологические, но и административные вопросы.

К нам в столовую в обед на Красноказарменной, 12 пришел целый полковник милиции Иванов (назовем его так) и потребовал выключить сайт compromat.ru, ссылаясь на вышестоящее начальство. А начальство было не простое, уже не вспомнить: ФСБ или целый Министр МВД. Страшновато, короче. Естественной моей реакцией было приглашение отобедать, чем «Совам Телепорт» богат, и одновременно отправка секретного сигнала Борису Пирожихину (жалко его, умер) срочно прибыть на разбор полетов. Первое, что сказал Борис, - хостинг не наш, знать не знаю ничего. Не по адресу пришел, начальник.

Однако накануне мы приобрели провайдера «Гласнет», и мало кто знал, что в наследство нам достался чистый и незамутненный рупор компрометирующей либеральной прессы. Полковник ушел в расстроенных чувствах (от обеда отказался). Но о приданном «Гласнета» узнали в бухгалтерии «Совам Телепорта» и решили сделать аудит: кто там, что там, и платят ли. Оказалось, что compromat.ru не платил уже шесть месяцев и был такой не один. В качестве меры было избрано решение погасить хосты неплательщиков - и Марина Никерова привела приговор в исполнение. Таким образом, я стал первым палачом онлайн-свободы в Рунете. Полковник тоже остался доволен. Правда, через несколько дней «Компромат.ру» пришлось включить, после того, как оплатили долги. Казалось бы, при чем тут юбилей MSK-IX? Ну так «Совам Телепорт» был в ряду его самых первых пользователей.

Краткая история Интернета бедных и маленьких

Дмитрий Бурков, председатель президиума Фонда содействия развитию технологий и инфраструктуры Интернет (FAITID)

Три тысячи символов (лимит заметки, включая пробелы) – это очень мало для истории, но очень много для современного восприятия... Тогда только анекдоты пунктиром...

Доисторические времена

Раскулачивание AT&T в 1984 (дерегулирование дальней связи) и возникновение CSNET тогда же не было совпадением и привело к первому межсетевому соединению с ARPANET и далее - к NSFNET/ANS с их AUP.

1991/1992 – CIX позволил решить проблему легализации связи с ними – но он был один и слишком далеко... Основным же стимулом к развитию соединений был email.

Самым же сильным толчком для нас стала либерализация рынка связи в Европе (1993) – официальное создание Eunet и создание AMS-IX в 1994. Это был существенный шаг в локализации трафика.

Стало очевидным, куда идти.

При этом ставка телекомов на ISO/OSI, X.../ISDN/BISDN при поддержке на уровне правительств задержало их, создало нишу, которая была быстро заполнена и в конце концов перевернула всё.

Немного про лихие 90-е

Для меня всё слилось в один длительный миг – как использовать РосНИИРОС в мирных целях, РЕЛАРН, Московский бэкбон.

Цифровые каналы – без них мы бы ничего не сделали. От освоения наследия, начиная с остатков проекта «Союз»-«Аполлон», несозданной системы радиовещания... Наконец – первые PDH-системы «Ростелекома» и оптика «Ленэнерго»/«Лейво».

Нам повезло – у нас не было цифровых сетей передачи данных (и, соответственно, поминутных и попакетных платежей), и это ускорило наше развитие. Sender keeps all (доходы) – основная интернет-модель быстро стала основной.

Итак, в начале цифра на T1, затем E1 и оптика, от самоделок до конца COCOM и первых кисок. В параллельной жизни – становление Eunet, борьба с Соросом в сети. Отсюда его вытеснили – но легче от этого не стало...

В параллель - осознание необходимости ухода от первых сетевых (по сути, пиринговых) войн и – как результат – перевод в РосНИИРОС домена .su, создание регистратуры .ru под его крышей. MSK-IX - логичное завершение этого перехода. Эта модель просуществовала в таком виде 5-6 лет (миг), после чего трения в регистрации доменов привели к реструктуризации деятельности того, что напихали в РосНИИРОС (и он чуть не лопнул от этого), и поэтапной миграции/эволюции в текущее состояние. Где-то были витки по спирали – но мы там, где есть...

Вот и вся история...

Где мы и куда всё идёт?

Вольница приходит к концу.

Входные билеты на рынок подорожали. Мобильный рынок стал закрытым клубом. Телекомы опять доминируют на транспортном и не только рынке.

Мы опять идем к крупным сетям, соединенным между собой. Это теперь начинает предопределяться и технологически (например, 5G). С 5G будут острова, опять как в начале, соединенные по другим принципам. Почему-то напоминает домашние сети в глобальном масштабе.

Так что же с IX-ами? Изначально мейнстрим - теперь резервация, или просто естественный лонгтейл? Будущее покажет.

P.S. *Простите за упрощения и за то, что кого то не упомянул явно – не в этом формате.*

Делюсь воспоминаниями

Михаил Медриш, ООО «Актор информационные системы», технический директор

Вопрос редколлегии журнала поделиться воспоминаниями заставил задуматься. За более чем 25 лет, на протяжении которых слово «Интернет» обозначает предмет моей профессиональной деятельности, накопилось столько воспоминаний, что впору книгу толстую писать. Книга тут не поместится, поэтому несколько слов об одном сюжете из конца 90-х и начала 00-х, который был частью важных изменений в российском Интернете, сделавшим его таким, какой он есть сегодня.

Во второй половине 90-х стало ясно, что развитие Интернета дошло до такого уровня, когда проявилась необходимость установления правовых рамок. Тогда основной площадкой для обсуждений проблем развития Интернета и разработок проектов документов была «Ассоциация документальной электросвязи», на ежегодных конференциях которой присутствовали практически все значимые персоны Интернета, регулятора и спецслужб. В конце 1997 года АДЭ приняла план работ в области стандартизации на 1998–1999 годы. Этим планом предусматривались разработки руководящих документов «Сети и службы передачи данных» и «Телематические службы». В начале июня 1998 года Госкомсвязи формально определил АДЭ в качестве базовой организации по стандартизации в области документальной электросвязи и утвердил принятый ранее план АДЭ. Для написания соответствующих документов были созданы рабочие группы, куда вошли представители регулятора, бизнеса, науки и ФСБ. Параллельно с этим - также под эгидой АДЭ - велась разработка документа, посвящённого ОРМ на сети Интернет (СОРМ 2).

Я участвовал в работе всех этих групп. Казалось, что наиболее проблемным будет документ по СОРМ, но участники рабочей группы как со стороны операторов, так и со стороны ФСБ показали не только профессионализм, но и способность на разумный компромисс. Я это могу с уверенностью говорить, так как в той рабочей группе выполнял функции techwriter. Сложнее оказалась задача написания руководящих документов (РД).

РД «Сети и службы передачи данных» был отнюдь не greenfield, а вторая редакция. К технологиям передачи данных ISDN, X.25, X.36 (про сети, построенные на технологии ATM, в 1999 году вышел отдельный РД) добавили технологию на базе протокола IP. Сегодня читать это РД без улыбки вряд ли получится. Однако в то время появление протокола IP, в том числе и IPv6 в нормативном документе создало формальные предпосылки для его широкого применения и развития Интернета в России.

Больше всего проблем проявилось при написании РД «Телематические службы». Важный момент – название. Оно взято из рекомендации МСЭ-Т, определявшей телематические службы как «службы электросвязи (кроме телефонной, телеграфной и служб передачи данных), которые организуются с целью обмена информацией через сети электросвязи». К телематическим службам отнесли факсимильные службы, службы электронных сообщений, службы голосовых сообщений, службы телеконференции, информационные службы. Придумывание содержания всех этих служб, а также соответствующих требований заняло много времени и попортило немало нервов всем участникам процесса. Прошло 20 лет - и практически все телематические службы растворились во мраке. Факсимильная почта и почта X.400 прекратили существование, службы телеконференций и электронная почта не стали услугами операторов связи, служба голосовых сообщений так и не стала полноценной услугой, и упоминание о телематических службах исчезло из нормативного поля. Но не всех. Одна осталась – доступ к информационным ресурсам, которая сейчас называется телематическая услуга связи.

С этим «доступом к информационным ресурсам» у меня личные счёты, так как раздел «Услуги доступа к информационным ресурсам» в РД писал я. С самого начала ситуация была бредовой. Такой услуги, конечно, в реальной жизни не существовало, так как доступ к информационным ресурсам пользователь организует сам, обращаясь через сеть к сайту (сервису). Но оказалось, что к моменту написания документа было выдано и действовало несколько сотен лицензий с такой формулировкой. И поставить услугу вне закона было невозможно. Мы с Юрием Владимировичем Златкисом, который от Госкомсвязи руководил процессом, договорились, что я опишу услугу как услугу оператора связи поставщику информационного сервиса (сейчас такие называются ОРИ), который, подключившись к сети, предоставляет информацию из своего сервиса любому, кто её запросит через сеть. И тогда те, кто имеют такую лицензию, скорее всего, не будут её продлять, так как услуги передачи данных достаточно. После завершения действия всех этих странных лицензий новые выдаваться не будут. Но в первой половине 2000-го из Госкомсвязи ушёл Юрий Владимирович, а также его руководители Рокотян и Мардер. Дело заканчивал уже через год Миков. В процессе окончательных согласований в текст соответствующего раздела РД были внесены небольшие текстуальные изменения, которые полностью перевернули логику. В получателях услуги оказался конечный пользователь, имеющий доступ в Интернет. И РД был утверждён в 2001 году совсем не в таком виде, как мы со Златкисом планировали.

Через некоторое время эта услуга стала называться телематической услугой связи. В ней остался тот самый дурацкий состав услуги для конечных пользователей – «доступа к информационным системам информационно-телекоммуникационных сетей, в том числе к сети Интернет». Мало того, ещё добавилась функция «приема и передачи телематических электронных сообщений». Понятно, что оператор связи ни то, ни другое не делает, так как он «труба», которая IP-пакеты в сеть передаёт и из сети принимает. А «телематических электронных сообщений» в природе не существует.

Правильным было бы убрать телематическую услугу связи из перечня услуг связи. Но нет, вместо этого в недавнем, авторства Минцифры, проекте нового постановления правительства по поводу лицензирования в области связи телематическая услуга связи присутствует как ни в чём не бывало.

Но даже учитывая все недостатки и проблемы, появление и введение в действие 20 лет назад нормативных документов, описывающих Интернет и услуги, с ним связанные, стали важным позитивным событием, давшим толчок к развитию Интернета в России. А случившийся в 2002 году отказ крупных российских операторов от бесплатного пиринга и появление в 2003 году нового закона «О связи», где услуга по присоединению и взаимодействию сетей была законодательно закреплена, создали условия для развития устойчивой инфраструктуры российского Интернета и, в частности, определили сегодняшнее место точек обмена трафиком.

Сеть FREEnet как зеркало развития Интернета в России

Мендкович А. С., Институт органической химии им. Н. Д. Зелинского РАН, заведующий лаборатории, д.х.н.; Русаков А. И., Ярославский государственный университет им. П. Г. Демидова

Одной из семи IP-сетей, операторы которых в 1995 году заключили соглашение о создании первого в стране узла обмена IP-трафиком (Internet eXchange), была сеть FREEnet. А уже в октябре 1996 было осуществлено подключение узла FREEnet на ММТС-9 к московскому узлу обмена интернет-трафиком MSK-IX. Это позволило заключить пиринговые соглашения с большинством сетей, подключенных к MSK-IX, и обеспечить скоростной обмен трафиком с этими сетями.

История развития сети FREEnet как в капле воды отразила в себе, пожалуй, все основные достижения, промахи и противоречия постперестроечной эпохи в нашей стране.

Сеть FREEnet (The network For Research, Education and Engineering), созданная на базе лаборатории Компьютерного обеспечения химических исследований (ЛКОХИ) Института органической химии АН СССР начала функционировать 20 июля 1991 года. Основные направления работ по созданию и дальнейшему развитию сети возглавляли сотрудники ЛКОХИ Е. Миронов, Д. Сидельников и А. Галицкий.

Поскольку в 1991 году непосредственное подключение по протоколу IP к зарубежным сетям не допускалось ограничениями КОКОМ, первоначально связь с зарубежными сетями осуществлялась через шлюзы сети SUEARN, которая в это время уже функционировала в ЛКОХИ. В 1992, сразу после отмены вышеупомянутых ограничений, было организовано международное IP-соединение FREEnet с датской научно-образовательной сетью UNI-C. К исходу 1993 года внешняя коннективность осуществлялась уже по двум выделенным международным каналам, соединяющим FREEnet с NSFnet (США) и с NASK (Польша).

С самого начала сеть создавалась по принципу «снизу вверх», как ответ на потребности академического сообщества в современных средствах коммуникации. В 1995-1998 годах развитие сети происходило особенно динамично: к примеру, за один 1996 год почти вдвое увеличилось количество региональных сегментов сети FREEnet. К 1998 году к опорной сети FREEnet были подключены 17 российских региональных сегментов. Через FREEnet осуществлялся доступ в глобальный Интернет национальных научно-образовательных сетей Республики Беларусь, Украины и Азербайджана.

К концу 1998 года экстенсивный характер развития сменился интенсивным: на фоне замедления темпов количественного роста сети рост пропускной способности сетевой инфраструктуры продолжался нарастающими темпами и сопровождался внедрением новых технологий.

Если на начальном этапе развития сети основное внимание уделялось формированию и обеспечению доступа к информационным и вычислительным ресурсам для науки и образования, в том числе и национального масштаба, то впоследствии стало активно осуществляться внедрение технологий многоадресного вещания и видеоконференций. Была освоена принципиально новая для российских научных сетей технология IP over ATM и впервые в России был инсталлирован и использован международный ATM-канал. В 1999 в сети FREEnet был внедрен протокол IPv6.

В последующие годы сеть FREEnet продолжала развиваться: выросли скорости каналов связи и объём трафика, реализована дифференцированная обработка различных классов трафика в масштабах всей сети, повысилась отказоустойчивость ядра сети. Критически важные элементы сети дублируются неоднократно, позволяя сохранить работоспособность сети даже в случае нескольких одновременных аварий. Большинство пользователей FREEnet по-прежнему принадлежат к научному и образовательному сообществам.

Интернет, КоКом и «Техно»

Андрей Романов, заместитель директора Координационного центра доменов .RU/.РФ

Празднование очередного юбилея, причем неважно, какого, мысленно отправляет нас в то время, в котором случилось отмечаемое. Юбилей MSK-IX - в начало 90-х, когда начиналась история российского Интернета.

Мы начали работать в компании «Техно» (это был кооператив, модная в то время организационная форма для развития инноваций) с операционными системами типа Unix в 1989 году в рамках проекта, совместного с НИИ Авиационного оборудования, по построению различных систем для использования в авиации. Работали на импортном оборудовании, произведенном австралийской компанией Labtam. На этой почве начали сотрудничать с «Релкомом» и «Демосом» в процессе строительства российского Интернета.

Во время путча в 91 году «Демос» подключил к сети «Релком» огромное количество серверов по всей стране. Буквально за три дня у сети появился более серьезный статус. Сеть базировалась исключительно на технологии электронной почты. Была установлена точка доступа непосредственно в Белом доме. Понимая важность обмена информацией с защитниками Белого дома, мы с коллегами из «Техно» параллельно тоже сделали там точку доступа. Правда, это произошло уже непосредственно перед окончанием путча. В Белый дом тогда снаружи попасть было достаточно сложно.

В 1991 году Билл Джолиц, один из исследователей, работавших в Калифорнийском университете в Беркли, в котором на средства DARPA велись работы по развитию системы Unix, перенёс версию BSD системы Unix на IBM-PC-совместимый компьютер с процессором Intel 80386. Такие компьютеры к тому моменту уже появились в России. И это дало возможность строить на их основе достаточно мощные сетевые серверы. В это время значительная часть высокопроизводительного телекоммуникационного оборудования попадала под ограничения Координационного комитета по экспортному контролю, более известного как КоКом или КОКОМ (англ. Coordinating Committee for Multilateral Export Controls, CoCom) — международная организация, созданная для многостороннего контроля над экспортом в СССР и другие социалистические страны. В эпоху холодной войны КоКом составлял перечни «стратегических» товаров и технологий, не подлежащих экспорту в страны «восточного блока», а также устанавливал ограничения по использованию товаров и технологий, разрешённых для поставки в виде исключения. Это касалось также и оборудования для построения интернет-сетей, а именно серверов и сетевых маршрутизаторов. Появление версии Unix для IBM-PC-совместимых компьютеров частично решало эту проблему. Компания «Техно» стала дистрибутором ОС BSDI в России.

Примерно в то же время, в конце 1993 - начале 1994 года, РосНИИРОС развивал проект создания Московской опорной сети (МОС) для научных и учебных организаций. В частности, при построении южного участка московской опорной сети (ЮМОС) специалисты компании «Техно» представили оригинальное решение для высокоскоростного (на тот момент) соединения 64 Kbps на базе обычных модемов и маршрутизаторов на основе персональных компьютеров с ОС BSDI (коммерческая версия ОС). Наличие такого решения и его демонстрация партнерам способствовали достаточно быстрому частичному снятию ограничений CoCom, и в Россию начались поставки маршрутизаторов компании Cisco Systems, что привело к бурному развитию IP-сетей в России, а также к построению сетей доступа пользователей к услугам сети Интернет.

В 1994 и 1995 годах компания «Техно» реализовала на базе этой же технологии достаточно крупный проект создания IP-сети для банка Столичный (узлов на 20-25, точно не помню). Это была практически первая подобная банковская сеть в России.

В общем, многие актуальные идеи быстро подхватывались и опробовались в «Техно», в результате к 93-94 году не менее трети узлов UUCP и около половины узлов On Line TCP/IP, входивших в сеть «Релком», работало через серверы «Техно». А еще в «Техно» имелся учебный центр, через который прошло много региональных и не только региональных специалистов по Internet и Unix'y. Это был период пика сетевой деятельности «Техно», на тот момент это уже было акционерное общество.

MCK-IX – Время, вперед!

Кирилл Аношин, директор национальной гильдии фрилансеров

Время в современном мире не просто течет, оно летит с околокосмической скоростью. Я много думал, с чем же можно провести аналогию? Ответ на этот мой вопрос оказался на поверхности. Это процесс развития интернет-технологий и сервисов! Этот процесс окружает меня, я участвую сам в этом процессе и, удивительно даже для самого себя, принимал участие в становлении или развитии многих интернет-сервисов.

Время. Время. Время. Вроде, совсем недавно, в начале 90-х годов прошлого века, мне очень сильно повезло в жизни попасть в развивающийся российский телеком. Компьютеры. Каналы связи. Модемы. Сети передачи данных X.25 - ИАС, «Роснет», «Роспак», «Спринт» и другие. Электронная почта. Специализированные информационные системы.

1400, 2400, 9600, 14000, «Ремарт», X.400, UUCP – и опять крупно повезло. В моей жизни появился тот Интернет (именно с большой буквы). «Релком», «Демос-Интернет», РосНИИРОС, домены... и люди, которые всем этим занимались и готовы были делиться своими знаниями и пониманием будущего.

Первый интернет-канал к российском оператору 64К и появление Московский точки обмена трафиком – MCK-IX.

Первый наш канал Т1 на запад. Подключение к MCK-IX и новые возможности. Возможность выбирать скорость порта, возможность бесплатно обмениваться клиентским трафиком с коллегами по рынку, возможность за небольшие деньги улучшать связность внутренних сетей и не гонять трафик через западные каналы и порты.

Все это было буквально «вчера», а сегодня MCK-IX отмечает свой юбилей – 25 лет!

Те «наивные» 1 или 10 Мбит/с-порты, на которых можно было стыковаться тогда, остались в прошлом. Сейчас это крупнейшая российская точка обмена интернет-трафиком с портами до 10 Гбит/с, площадка, предоставляющая огромные возможности для масштабирования сетей и сервисов в Интернете.

Тогда это просто «девятка» в Москве и несколько провайдеров, а сейчас это «десяток» объединённых в единый организм городов с наибольшим потреблением интернет-трафика и вхождение в топ мировых лидеров по объему передаваемого трафика и подключений.

За это время было много интересных событий, можно вспомнить и кривые анонсы от некоторых провайдеров, и те же «пиринговые войны», к которым MCK-IX не имеет прямого отношения, но и ей досталось. Но лучше, конечно, вспоминать хорошее. Развитие внутри Москвы, выход в другие города, регионы и страны!

Зная и понимая, какой это колоссальный труд, хочется от всей души поблагодарить людей, которые стояли у истоков, которые занимались и занимаются развитием, и пожелать им только успехов, только «прямого» оборудования, самой качественной оптики, еще большего масштабирования и выхода на дальние регионы мира!

«Радио МГУ» - последний советский телекоммуникационный проект

Бережнев Сергей Филиппович, НИИЯФ МГУ, ведущий конструктор (руководитель проекта «Радио МГУ»)

«Радио МГУ» - один из крупнейших телекоммуникационных проектов конца советской и начала российской эпохи. Начался он с того, что НИИЯФ МГУ предложили создать центральный узел будущей телекоммуникационной сети для УНК ИФВЭ. УНК – это проект ускорителя на встречных пучках с энергией в системе центра масс порядка 6 ТЭВ. Планировалось строить сеть на базе стандартных модемов со скоростями 4,8 кбит/с. Понятно, модемная сеть не могла бы справиться с потоками информации, порождаемыми УНК. Нужна была сеть со скоростями на порядки более высокими. Был создан эскизный проект такой сети. Он был одобрен НТС войск связи, советом по автоматизации ОЯФ АН СССР и включен как составная часть в проект УНК ИФВЭ. А потом проект УНК был приостановлен. Мы остались с проектом сети на базе радиорелейных линий, с разрешением на частоты (что нам потом очень пригодится) и стали развивать кампусную сеть МГУ на базе протоколов Интернета с центральным узлом в НИИЯФ.

После распада Советского Союза на Западе появилась мода на оказание помощи бывшим советским республикам в реализации различных проектов по организации компьютерных коммуникаций с Западом.

В 1992 году в Москву прилетела делегация из двух сотрудников немецкой научной сети DFN (Адлера и Раушенбаха) и одного сотрудника немецкого ускорительного центра в Гамбурге DESY (Ханса Фрезе). Министерство науки Германии поручило им выяснить, как можно обеспечить доступ в Интернет для российских ученых, есть ли в Москве научные группы, на которые можно опереться.

Учитывая тесные связи между DESY и советскими институтами, шлюз в Германии должен был располагаться в DESY. Делегация быстро выяснила, что в НИИЯФ МГУ уже существует готовый проект сети на базе радиорелейных линий с пропускной способностью 2 Мбит/с. Было заключено соглашение между DESY и НИИЯФ МГУ о совместной деятельности по организации доступа российских научных институтов в Интернет через немецкую научную сеть и узел в DESY.

Спутниковый канал емкостью 256 кбит/с был запущен в конце 1993 года. По своей пропускной способности он существенно превосходил любой из существующих тогда российских интернет-каналов. В1994-1995 годах была увеличена емкость основного канала Москва-Гамбург и были организованы еще семь спутниковых узлов, десятки институтов подключились к точкам доступа «Радио МГУ» в Москве.

Существенно, что все узлы системы, в том числе и в Гамбурге, находились под контролем «Радио МГУ». Емкость каналов системы позволила обеспечить временный транзит значительной части трафика и других научных сетей. На М9 был создан центральный узел, через который обменивались трафиком и выходили во внешний мир практически все (за исключением КИАЭ) ядерные научные институты и ряд других крупных институтов (сейчас их число значительно сократилось). После создания в 2010 НИЦ КИАЭ входящие в эту структуру институты перевели свои основные каналы на обслуживание в НИЦ КИАЭ, сохранив backup-каналы в «Радио МГУ». Таким образом, сеть «Радио МГУ» сосредоточена сейчас на обеспечении доступа в Интернет для НИИЯФ МГУ и нескольких других подразделений МГУ. Кроме того, сеть обеспечивает резервирование каналов для ряда других организаций.

Следующим этапом развития «Радио МГУ» стала единая спутниковая сеть для стран Кавказа, Средней Азии и Афганистана. К 2000 году существовала довольно хаотичная система доступа научных организаций этих стран к Интернету. Линии связи обеспечивали доступ в Интернет только конкретной организации, речи о создании единой научной сети для данной страны пока не шло. Сами каналы финансировались различными научными фондами. Было принято решение объединить все эти мелкие проекты в один большой в рамках научной программы НАТО «Наука ради мира и безопасности».

Проект был реализован в 2001-2010 годах. В рамках проекта были организованы национальные научно-исследовательские сети в тех странах, где они до того не существовали. Были организованы каналы связи, обеспечившие для стран-участниц доступ в мировой Интернет. Большую поддержку проекту оказало министерство образования России. Для участников сети из стран СНГ был открыт бесплатный доступ до многих электронных баз данных организаций Минобра. Это привело к тому, что участники сети активно работали с Россией. Трафик с Россией для большинства стран-участников проекта составлял 40%. Исключение составляли Азербайджан и Грузия, где трафик с Россией составлял ~ 20%. В настоящее время проект в старом виде завершен, но старые связи между NOC остались и могут быть использованы для организации новых совместных проектов.

Описанные выше проекты не могли быть реализованы без поддержки очень многих людей: ректора МГУ В. А. Садовничего, академика-секретаря ОЯФ А. С. Скринского, директора НИИЯФ МГУ М. И. Понасюка, П. Ф. Ермолова, В. И. Саврина, Ганса Фрезе из DESY. Я благодарен за поддержку всему нашему коллективу: Д. Авдееву, Н. Гришину, Г. Ермакову, С. Болотину, С. Никифорову, Андрею Линкевичу и многим другим.

А давайте вспомним такое место, как М9, на карте Интернета!

Михаил Коротаев, ФГУП ТТЦ «Останкино», главный специалист

Мы знаем, где начался интернет-взрыв в нашей вселенной Земля (кстати, а где?), но вот интернет-взрыв в нашей галактике .ru начался с этой точки, хотя началось все еще в галактике **.su.**

- **Первый IP-канал – запущен на М9 (кстати, а кто помнит, куда был первый междугородный IP-канал?).**
- **Первый DNS – на М9 (а какое имя было у того сервера?).**
- **Первый междугородний маршрутизатор – на М9 (а что он собой представлял?).**
- **Первый модемный пул – на М9 (конечно, один из первых, но как звучит!).**
- MCK-IX часто путали с М9 (посмотрите, а ведь и вправду близки, и ведь не только по названию);
- все ЦОД в РФ всегда сравнивали себя с М9, хотя М9 долго не вносили в рейтинги ЦОДов, видимо, считали его вне конкуренции (несколько лет в рейтингах АРС М9 не было, хотя это был самый большой в то время в РФ коммерческий ЦОД и Телехаус).

Ответы на вопросы в тексте:

- Интернет зародился в одном из проектов DARPA (это было еще до меня).
- Первый IP-канал – это был ТЧ канал Москва (М9) – Барнаул, канал в СПб, увы, был только вторым.
- Первый DNS-сервер имел имя kremlsun.su (иногда пишут cremlun, но это неверно. Кстати, история этого SUN-сервера сама по себе интересна, эта «тумбочка» была подарена корпорацией SUN организации SUUG, которая занималась поддержкой первой доменной зоны .su в нашей галактике).
- Первый маршрутизатор – это обычный настольный аналог IBM PC (сейчас этот формат называется desktop) с операционной системой XENIX (поправленной И. Чечиком под задачи IP-маршрутизатора) с платой на несколько RS-232-портов. Я тогда был админом этой точки, другого компьютера не было, поэтому я иногда поверх XENIX запускал MS DOS и играл в игрушки. (Только вдумайтесь – на главном маршрутизаторе РФ админ играет в «Диггеров» и в «Тетрис». Вот какой был гаджет в то время.)

> **«М9 - это точка пересечения Интернета в РФ.»**

М9 - это точка пересечения Интернета в РФ.

Вот примеры этого:

- один из первых вопросов любого заказчика в телекоммуникациях - «есть ли канал до М9» (конечно, первый всегда про цены, а вот второй - про канал до М9);

Правовые аспекты становления Интернета в России

Сергей Мальянов, советник вице-президента по взаимодействию с органами государственной власти ПАО «Вымпелком»

История Рунета будет неполной, если не вспомнить о становлении системы государственного надзора в этой сфере. Развитие сети Интернет в стране объективно потянуло за собой и вопросы контроля нового направления со стороны государства.

Стартовой точкой эры контроля современного Рунета и всего, что с ним связано, можно считать весну 2000 года, когда в положении о новом министерстве Российской Федерации по связи и информатизации появилась задача «государственный надзор за деятельностью в сфере связи и информатизации» (постановление правительства РФ № 265 от 28.03.2000) и была создана Система государственного надзора за связью и информатизацией в Российской Федерации (постановление правительства РФ № 380 от 2803.2000).

Основой создания новой Системы надзора стал департамент по надзору за связью и информатизацией министерства (ДНСИ). Его руководителем был назначен Николай Андреевич Логинов, ранее возглавлявший Главное управление государственного надзора за связью в Российской Федерации. Заместителем руководителя ДНСИ стал перешедший из Совета безопасности РФ Валерий Николаевич Бугаенко. Он и предложил мне в октябре 2000 года возглавить отдел по надзору за информатизацией.

Если вопросы надзора в сфере связи уже были понятны и был накоплен большой опыт (Главгоссвязьнадзор был создан ещё в ноябре 1993 года), то тема надзора за деятельностью в сфере информатизации была абсолютно новой, не отработанной как по содержанию, так и методологически.

Положением о государственном надзоре за связью и информатизацией сфера контроля была описана очень лаконично: «надзор за соответствием предоставляемых услуг в области информатизации установленным нормам». Да и действующие в тот период нормативные правовые акты (НПА) не давали ответа на вопрос, что же такое государственный надзор за деятельностью в сфере информатизации.

Требовалось выявить и описать эти услуги (предмет, объект, субъект, содержание), найти в НПА уже существующие требования и нормы и разработать новые (закрепив их в соответствующих НПА), разработать методическую основу проведения контрольных мероприятий, обучить сотрудников и спланировать проверки.

Было принято решение провести научно-исследовательскую работу, в которой и проработать все эти вопросы, определить направления надзора в этой сфере, на их базе подготовить проект Концепции государственного надзора в сфере информатизации и необходимые методические рекомендации.

Возглавил эту работу Валерий Николаевич Бугаенко. Под его началом была собрана группа руководителей ведущих отраслевых научных организаций, работавших в сфере информатизации: ГУП НТЦ «Информрегистр», ФГУП ВНИИПВТИ, ФГУП НТЦ «Информсистема», ФГУП МНИИ «Интеграл». Методологическую поддержку оказывало ФГУП ЦНИИС.

За основу было принято целеполагание, установленное федеральным законом от 20 февраля 1995 г. N 24-ФЗ «Об информации, информатизации и защите информации»: создание оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Работа продолжалась почти весь 2001 год. Обсуждение результатов работы всегда было бурным. Каждый старался доказать, что его направление особенное. Тем не менее, в результате были определены следующие возможные направления контроля:

- формирование и использование в соответствии с законодательством Российской Федерации электронных информационных ресурсов, включая электронные издания, базы и банки данных;
- предоставление информационных услуг (услуг по обработке информации);
- распространение и использование пользователями (потребителями) информации программ для электронных вычислительных машин;
- состояние автоматизированных информационных систем независимо от формы собственности и ведомственной принадлежности;
- обеспечение защиты информации, не связанной со сведениями, составляющими государственную тайну, в информационных системах (автоматизированных информационных системах) независимо от формы собственности и ведомственной принадлежности. Позже это направление расширилось за счет получения Роскомнадзором полномочий Уполномоченного органа по защите прав субъектов персональных данных.

Одновременно шел поиск механизмов практической реализации этих направлений. Например, была проведена большая работа по отработке возможности участия органов государственного надзора за связью и информатизацией в мероприятиях по защите программ для ЭВМ и баз данных как объектов интеллектуальной собственности. На встречах, проведенных с руководством фирмы «1С» (Борис Нуралиев), «Майкрософт-Россия» (Ольга Дергунова) и юридической фирмой Latham & Watkins (юридический партнер «Майкрософт-Россия»), определились различные позиции и понимание субъектов и способов контроля нелегального использования программ для ЭВМ. Предложения и ожидания коллег не вписывались в систему государственного института надзора. Проведение нескольких тестовых проверок подтвердили наши сомнения.

Важным результатом работы стало определение предметной области государственного надзора в сфере информатизации как контроля соблюдения единых обязательных требований по формированию (созданию, хранению, обработке, распространению, передаче, обмену) информационных ресурсов, доступа к ним, созданию и применению обеспечивающих информационных и коммуникационных систем и технологий. Этот подход и был положен в основу деятельности Россвязьнадзора.

Другим важным результатом этой работы стало понимание нами, что во главе угла государственного надзора и в сфере информатизации (информационных технологий), и в сфере связи должны стоять четко сформулированные и понятные всем участникам рынка «обязательные требования». Задача по продвижению и реализации на практике этого принципа была поставлена мне, когда Валерий Николаевич возглавил в конце 2002 года ДНСИ, а я стал его заместителем.

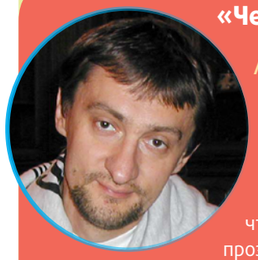
Эта логика легла в основу разработанных административных регламентов Роскомнадзора. Кстати, самым первым в стране административным регламентом был регламент Роскомнадзора по лицензированию деятельности в области связи. Кроме того, наше системное понимание сущности «обязательных требований», порядка их формирования и установления четко легло в нормы федерального закона от 31.07.2020 № 247-ФЗ «Об обязательных требованиях в Российской Федерации». Но это уже другая история.

С высоты сегодняшнего дня отдельные подходы 2001 года кажутся наивными. И это справедливо. Но, в целом, многие идеи и принципы контроля, выработанные в 2001-2002 годах, воплощены в жизнь и работают. Но и они меняются. Новое время диктует новые условия и ставит новые задачи.

В заключение хочу сказать, что содержание понятия «услуги в области информатизации» так и не было закреплено в НПА. В ходе работы над этой темой термин «услуги в области информатизации» был декомпозирован и объективно был сделан плавный переход к устоявшимся в дальнейшем понятиям «информационные услуги», «услуги по обработке информации», «предоставление информации», «распространение информации» и т.д., которые и были закреплены в федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации». Сегодня требования этого закона и составляют основной предмет контроля в сфере информационных технологий.

Ни на момент становления самой идеи этого законодательства, ни на сегодняшний день стопроцентной кодификации сферы информационных технологий не возникло и, скорее всего, и не произойдет, т.к. сама предметная область по сути своей крайне разнообразна, а в силу этого разнообразия и единообразное регулирование вряд ли возможно.

А Рунет с того времени не остается без постоянного и пристального контроля со стороны государства...



«Черное зеркало» для Рунета

Александр Зайцев, «Билайн», руководитель проекта строительства ЦОД

Увы, но зеркало треснуло, и то, что раньше казалось светлым и прозрачным, превратилось в темное и очевидно недоброе: ясно, что мы все под колпаком - и каждый шаг, каждое слово может отозваться так, что последствия придется разгребать очень долго – это, конечно же, да.

Однако, когда - уже более 25 лет назад - устанавливали на пятом этаже легендарной «девятки» (ММТС-9) свои первые маршрутизаторы и коммутаторы, признаюсь, никаких особых опасений не было. Более того, присутствовала определенная гордость за причастность к такому большому и важному делу - да-да, социальная значимость проекта имела существенный вес в тогдашней системе ценностей.

Потом, уже в начале двухтысячных, когда общественная ситуация в стране стала весьма стремительно меняться, какое-то время было даже удивительно, что государство остается настолько либеральным в отношении Интернета. Пожалуй, только АДЭ попыталась как-то «взять под контроль и возглавить», ожидаемо безуспешно.

Но что же тут поделаешь, телеком-инфраструктура всегда была «в зоне особого внимания», вожделенной целью, лакомым кусочком для государственных спецслужб, тем паче Internet Exchange – узел, подключившись к которому, получаешь доступ к практически всем ручейкам и рекам трафика, по крайней мере, малых и средних провайдеров. Поэтому, имея в виду участие «Ростелекома» в MSK-IX (51%), есть риск превращения IX'а в настоящий государственный «объект критической инфраструктуры» со всеми сопутствующими атрибутами, такими как «учения по изоляции Рунета» и прочая.

Ожидаемым ответом на приход государства в Интернет стало стремительное развитие технологий, позволяющих если не «примирить» эти казалось бы непримиримые миры, то хоть как-то сосуществовать в одной вселенной: одноранговые сети с размазыванием контента по всей Сети в связке с лицензиями Copyleft, плюс Tor, что, однако, ни в коем случае не умаляет важности MSK-IX как стратегического узла Рунета, настоящего остова Сети, ибо сказано, что всякое ПО хорошо работает только поверх должной инфраструктуры.

Анализ больших данных Рунета на MSK-IX – по большому счету, это куда круче анализа предпочтений покупателей любого ТЦ на Тверской - здесь несомненно велика роль фонда «Индата», чьи технологические отчеты составляют яркую и, IMHO, самую интересную тему ежегодных конференций, которые MSK-IX продолжает проводить теперь уже под эгидой «Ростелекома».

НСН, MSK-IX и президентские выборы

Алексей Соколов, «Яндекс», директор по развитию сетевой инфраструктуры

В 1994 году на территории Института космических исследований Российской академии наук (ИКИ РАН) был запущен один из первых информационных проектов в российском сегменте сети Интернет под названием «Национальная служба новостей» (НСН, www.nns.ru). Площадка была выбрана не случайно: ИКИ РАН был одним из первых, имевшим связанность с международными компьютерными сетями (в конце 80-х — с европейской сетью Bitnet, а немного позднее - с сетью Интернет по прямому каналу в Вашингтон). Подключения в советское время были осуществлены, благодаря сотрудничеству с Европейским космическим агентством и NASA, а также мудрой технической политике Равиля Равильевича Назирова, отвечавшего тогда за компьютерное обеспечение научной работы, проводимой в ИКИ РАН. Вторым аргументом за выбор именно этой площадки было ее территориальное расположение – вблизи телефонной станции ММТС-9, на базе которой тогда еще существовала сеть цифровых каналов «Искра-2» и поэтому эта станция являлась «точкой притяжения» всех тогдашних российских интернет-провайдеров.

Вдохновителем проекта был Валерий Бардин, ранее принимавший активное участие в «Релкоме» и «Демосе» (одни из первых интернет-провайдеров в России). Коммерческий блок возглавляла Мария Степанова, за серверную часть отвечали Сергей Аншуков и Николай Саух, за PR и GR - Кирилл Чащин, а за внешние технические коммуникации на тот момент — Алексей Соколов.

Идея проекта была простой: собирать в одну полнотекстовую базу данных все газетные источники со всей России, включая региональную прессу, и предоставлять на коммерческой основе доступ к этой информации через Интернет, учитывая необходимость авторских отчислений правообладателям информации. Поскольку в то время не существовало веб-версий изданий СМИ, кроме центральных, то поначалу всю информацию приходилось сканировать вручную. Для этого был создан целый цех, оборудованный десятками сканеров, и организована доставка более, чем 100 центральных и региональных изданий для оперативной обработки. На базе всей получаемой информации готовилась новостная лента, аналогично ленте информационных агентств, с наиболее важными событиями (за это отвечал Михаил Лукин). Также делались дайджесты по интересующей заказчиков тематике - для крупных корпораций и отдельных лиц, которые в основном готовил Рустам Амиров.

Поскольку в то время большинство представителей российской политики и бизнеса не осознавали до конца, какую пользу можно извлечь из такого объединенного массива данных, возможности анализа такой всеобъемлющей и разноплановой информации, то коммерческий успех у всего этого предприятия был весьма скромным. При этом, в силу относительной малочисленности в то время пользователей сети Интернет в России, рекламная модель получения дохода также не могла быть использована.

Проект оставался малоизвестным широкой публике, хотя многие значимые деятели Интернета бывали там частыми гостями. Однако в 1996 году произошло событие, которое дало толчок к более широкой известности НСН. Это были выборы президента Российской Федерации. Каким-то образом команде НСН удалось договориться получать данные по результатам голосования в онлайн-режиме напрямую из Центральной избирательной комиссии и тут же публиковать их в Интернете. Это было настолько важное событие для России и всего мира, что в этот день практически все внимание пользователей глобальной сети (и в России, и за рубежом) было приковано к этому сервису!

Надо сказать, что интернет-каналы этого проекта были по тем временам очень неплохими: доступ в Интернет был организован со скоростью 2 Мбит/с (потоком E1) через одного из существовавших тогда провайдеров «Макомнет», сетевое оборудование которого располагалось рядом с офисом, в метрополитене. При этом такая канальная инфраструктура, естественно, не могла бы обеспечить той потребности в трафике, которая была необходима в период публикации на сайте непрерывно обновляемых результатов выборов.

Но, к счастью для проекта, незадолго до этого на ММТС-9 была организована московская точка обмена трафиком (MSK-IX), куда подключились все значимые в тот период провайдеры Интернета в России, а команда НСН протянула туда свое оптоволокно и организовала резервированные каналы 10 Мбит/с по мало тогда еще используемой в России технологии Ethernet поверх оптики, благодаря чему удалось обеспечить бесперебойную доставку информации в период этого события.

Таким образом, MSK-IX сыграла важнейшую роль в реализации принципа открытости при проведении первых, действительно значимых выборов президента современной России.

С ЮБИЛЕЕМ, MSK-IX!

Валерий Бардин

Три года из жизни Интернета

Василий Прокин, ООО «Эквант», директор технической эксплуатации

1991 год.
Интернету восемь лет.

В Москве только один провайдер передачи данных – Центральный телеграф. Предлагаемые услуги – телеграфные сообщения и телекс. Скорость передачи данных - 50 бод! Гаджеты размещены на площадях почтовых отделений и называются телетайпами. Функцию последней мили осуществляют курьеры, которых называют почтальонами.

В СССР один контент-провайдер - информационное агентство ТАСС.

Шла перестройка, появились представительства зарубежных компаний и организаций. Им требовался доступ к современной сети данных X25 и электронной почте X-400. Правительство СССР принимает решение о создании на базе Центрального телеграфа (ЦТ) совместного предприятия с американской корпорацией SPRINT для операторской деятельности в сетях передачи данных X25. Руководителем компании стал энергичный менеджер Виктор Ратников.

Центральный узел «РоСпринт» располагался на ЦТ (Тверская, 7) и по аналоговому каналу 9600 кбит/с был подключён к узлу SPRINT в Вашингтоне.

Пользователи имели доступ к сервису по выделенным линиям и через модемный пул на 16 линий.

1993 год.
Интернету десять лет.

Появились первые заказы на подключения по протоколу TCP/IP. Приобрели, по рекомендации американских коллег, оборудование у малоизвестной компании Cisco. Сформировали дополнительный международный канал до Хельсинки со скоростью 9600 килобит в секунду. Для доступа к Интернету через телефонную сеть ввели в эксплуатацию отдельный модемный пул на 16 линий. Пользователи X25 использовали телефонную линию для передачи данных не более нескольких минут в день. Интернет-пользователи зависали в сеансах связи часами. Модемные линии для Интернета были заняты на сто процентов. Увеличение количества линий доступа не спасало. Вновь вводимые линии загружались мгновенно. Учитывая возможности МГТС, апргрейд пула всегда был головной болью.

Происходила реорганизация отрасли связи. Из единого комплекса предприятий связи на основе приватизации возникали отдельные компании. Возникла ЗАО «ММТС-9» (Международная междугородняя телефонная станция – 9) по адресу улица Бутлерова, 7. Через нее проходили все аналоговые, а затем цифровые каналы связи. Как по России, так и зарубежные. Генеральный директор Ярославский Александр Владимирович и главный инженер Громов Владимир Александрович выделили технологические ресурсы для размещения оборудования телекоммуникационных коммерческих компаний, которые стали появляться в то время. Де факто это стало первым телехаусом в России подобно телехаусу на Хадсон Стрит, 60 в Нью-Йорке.

1995 год.
Интернету 12 лет.

«РоСпринт» построил свои региональные узлы в Хабаровске, Иркутске, Новосибирске, Ростове, Самаре и Санкт Петербурге. Все они были соединены звездой с Москвой. Каналы были аналоговые и арендованные у «Ростелекома». Развитие Интернета привело к хронической нехватке мощностей каналов. При этом обмен трафика между российскими провайдерами проходил за рубежом, загружая самые дорогие и переполненные международные каналы. Необходимость создания точки обмена российского Интернета в Росиии, Internet eXchange (IX), была очевидна. Подобные пиринговые точки обмена уже в то время существовали во Франкурте-на-Майне, в Лондоне и Нью-Йорке.

ММТС-9 была выбрана из-за демократических условий размещения оборудования на своих площадях. Точку обмена решили назвать M9-IX.

«С Юбилеем, MSK-IX!»

Неюбилейные размышления на юбилейную тему

Михаил Якушев, заместитель директора Института права цифровой среды НИУ ВШЭ

Приближение юбилейных дат всегда «подталкивает» к воспоминаниям о том, как ты был участником или свидетелем событий, которые предполагается отпраздновать. Но четвертьвековой юбилей MSK-IX – всё же нечто большее, чем просто история возникновения и развития одной из айтишных организаций. Повспоминать, конечно, можно и многим, и о многом, но такие воспоминания неизбежно влекут за собой некоторые размышления и, не побоюсь этого слова, определённые обобщения. Итак, повспоминаем, поразмышляем и пообобщаем.

Первое, о чём мне, как начинающему мемуаристу, хочется сказать, – это о проблеме смены поколений. Я «вошёл» в интернет-сообщество именно в первые годы существования MSK-IX и «расцвета» РосНИИРОСа как ключевых компонентов инфраструктуры российского Интернета. Мне было непривычно ощущать себя «молодым новичком» в компании тех очень уважаемых людей, которые «поднимали» первые сети, организовывали обмен трафиком, заключали соглашения о создании российской доменной зоны. Среди них были и «патриархи» (можно сказать, «дедушки» российского Интернета), которые раньше всех увидели и поняли, ЧЕМ может стать Интернет для мировой цивилизации. Были и мои ровесники, уже зарекомендовавшие себя не только как грамотные эксперты, но и успешные бизнесмены в том странном и необычном бизнесе, который был так не похож ни на что известное в сфере «традиционной» электросвязи. Для представителей этих двух поколений российских интернетчиков, конечно, я был «молодой кадр», к тому же, разбиравшийся лучше всего в немного неожиданной для них области – интернет-праве. Тем не менее, всем нам удалось достаточно быстро найти общий язык и успешно работать вместе.

Сейчас, когда можно говорить уже о седьмом или восьмом поколениях российских интернетчиков, профессионально и психологически не похожих на «нас четвертьвековой давности», важно напомнить им, насколько всё же нас объединяло тогда и взаимное доверие, и взаимное уважение. И это во многом определило успех работы MSK-IX и всех «причастных» организаций на все последующие годы.

А кстати, можно ли считать такую работу успешной? Да! На фоне того, как подобного рода задачи решали коллеги за рубежом. Еще раз – да! – если сравним с другими проектами национального масштаба, которые развивались в нашей стране в последние 25 лет. Третий раз – да! – поскольку за все эти годы не было НИ ОДНОГО сбоя в функционировании технической системы российского Интернета. По крайней мере, какого-то такого сбоя, о котором по прошествии стольких лет кто-то мог бы вспомнить и поставить кому-то это в упрёк.

Второе. Всё, что делалось двадцать пять лет назад, было шагом в неизвестное. Надо было не только просчитывать всё и вся с точки зрения техники и финансов, но и предусматривать развитие и умощнение с перспективой на ближайшие годы. И при этом еще принимать решения, полностью выверенные с юридической стороны. Что такое «трафик», «Интернет», «сетевой адрес», «автономная система», «DNS» и т.д. и т.п., в 1995-м году вряд ли отчётливо понимало больше сотни человек на всю Россию. А кто вправе распределять эти ресурсы, на каких принципах двусстороннего и многостороннего взаимодействия (явно противоречащих стандартным для конца 1980-х годов правилам присоединения телефонных сетей) строить договорную работу, как и в каких пределах допускать вмешательство государства... На эти – и тысячи других вопросов – не было однозначных ответов. Причём и у зарубежных коллег тоже.

Справились. Принятые решения оказались верными. В немалой степени те технические и организационные решения, которые «запустили» MSK-IX в середине 1990-х, обусловили взрывной рост российского Интернета к началу XXI века и его стабильное развитие в последующие десятилетия. Появление десятков, сотен, тысяч новых интернет-компаний, от узкоспециализированных до многофункциональных; создание десятков тысяч новых рабочих мест, причём достаточно хорошо оплачиваемых и престижных для молодёжи; обеспечение едва ли не лучшей в мире устойчивой связности российского Интернета; принятие очень сложного и казавшегося очень несвоевременным решения о передаче полномочий по управлению национальным доменом от РосНИИРОСа новой организации – Координационному центру; появление впоследствии «Технического центра интернет» – всё это так или иначе явилось следствием не только высокого профессионализма и технологического предвидения, но и в значительной степени личного мужества и гражданской позиции нескольких скромных и спокойных людей, стоявших во главе начинавшихся тогда процессов и проектов.

Третье. Ну а поскольку «или хорошо, или никак» принято говорить только о покойниках, а наш юбиляр и молод, и полон сил, и, надеюсь, планов на будущее, хотелось бы поменьше писать чего-то хвалебного и побольше - чего-то объективного.

Оптимальным ли был процесс развития MSK-IX, и шире, инфраструктуры российского Интернета в целом, за истекшие четверть века? Скорее всего - да. Были ли допущены ошибки, которые потребовали тех радикальных изменений в системе управления российским Интернетом в последние годы? Похоже, что всё-таки нет. Следовательно, причины таких изменений и перспективы возможного развития еще ждут своего объективного анализа.

Чего так и не удалось всем нам – так это упорядочить взаимодействие всех участников «экосистемы Интернета» в соответствии с законодательством. Точнее – описать это взаимодействие в терминах законах и, таким образом, его легализовать. Прекратить споры о том, нужно ли выдумывать правила построения и присоединения сетей передачи данных. О том, существуют ли «телематические услуги связи». О том, как соотносить требования о связности интернет-сетей с требованиями о «локализации» их узлов (и «точек обмена трафиком») внутри территории страны. О «стоимости» сетевых адресов. О «владении» автономными системами – и так далее. Российское законодательство в области Интернета «застряло» на рубеже веков, отстав от зарубежных правовых систем минимум на десятилетие – и часть вины за это лежит на тех, кто неизбежно лучше других понимал, что и как в Интернете работает, но предпочитал «не отвлекаться» на скучные юридические вопросы. Так что многое, что в теоретическом плане было непонятно тогда, не до конца понятно и сейчас.

Тем не менее, несмотря на все юридические и законодательные «сложности», техническая инфраструктура российского Интернета реально и успешно работает. Все, кто был причастен к созданию MSK-IX, доказали своё умение руководить сложными и масштабными техническими проектами.

Сейчас, когда можно говорить уже о седьмом или восьмом поколениях российских интернетчиков, профессионально и психологически не похожих на «нас четвертьвековой давности», важно напомнить им, насколько всё же нас объединяло тогда и взаимное доверие, и взаимное уважение. И это во многом определило успех работы MSK-IX и всех «причастных» организаций на все последующие годы.

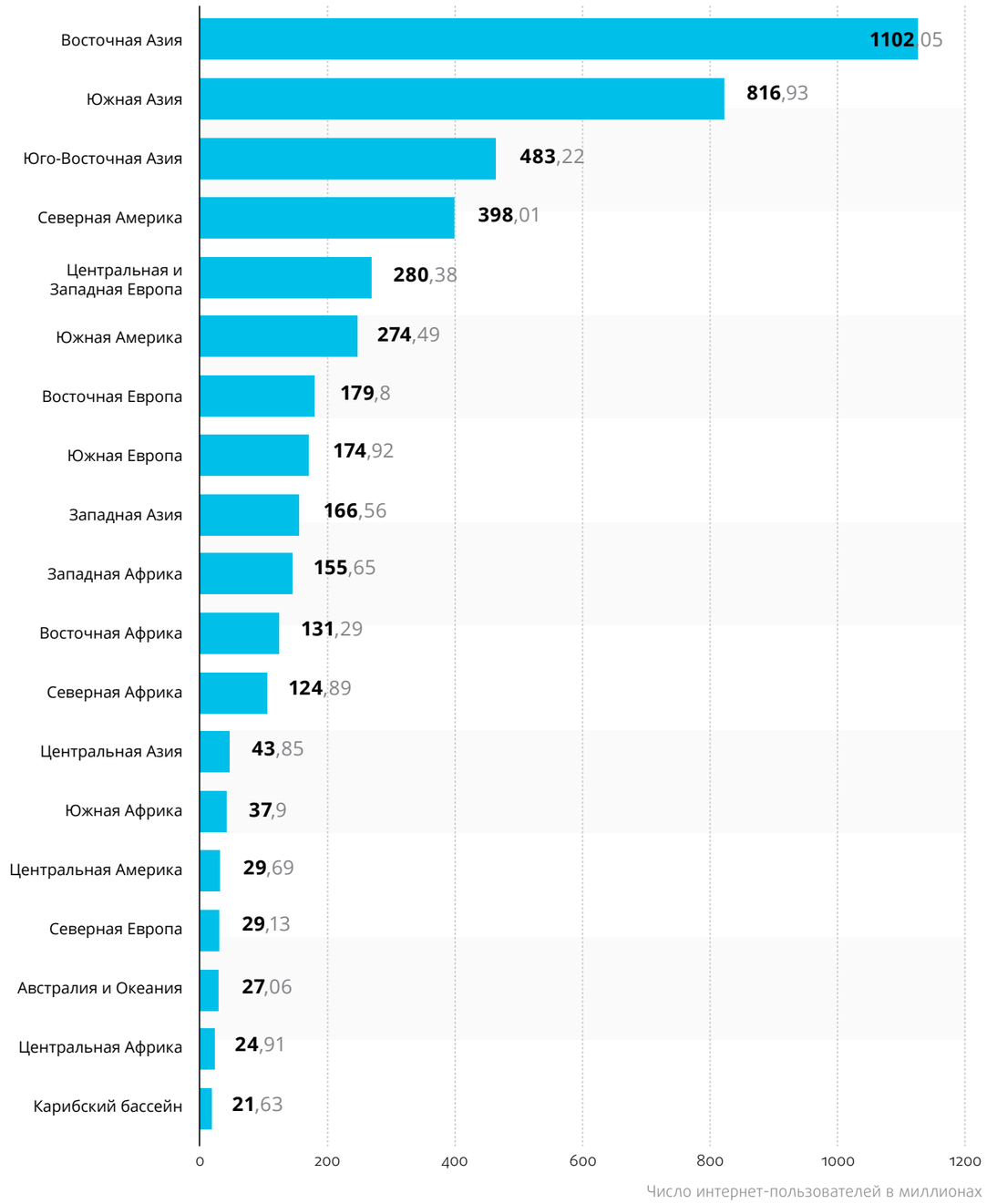
Как ни парадоксально, подтверждением этих слов может служить следующий факт. Многие ли из российских пользователей Интернета знают о существовании MSK-IX (и подобных предприятий), о том, чем эта организация занимается и какое значение имела и имеет в развитии Интернета в нашей стране? Думаю, что очень и очень немного. Но это и нормально! Если об организации начинают говорить только в случае масштабных технических сбоев – значит, всё остальное время она работает эффективно, и эта эффективность незаметна как раз обеспечением бесперебойности и качества работы интернет-компаний в Москве и по всей стране. В конечном итоге, часто ли мы задумываемся о существовании организаций под названием «Водоканал», когда включаем воду в раковине? Льётся то, что надо, надлежащей температуры и без ненужных примесей – вот и доказательство качественной работы тех, кто отвечает за эту услугу.

Пройдут еще годы, будут новые юбилеи и поводы вспомнить, как появился и развился в России Интернет. Но я уверен, что имена тех, кто участвовал в этом казавшемся «несерьёзным» проекте, рано или поздно будут так же вписаны в историю страны, как имена Попова, Курчатова, Королёва.

Пожелаем же создателям MSK-IX здоровья и долгих лет творчества!

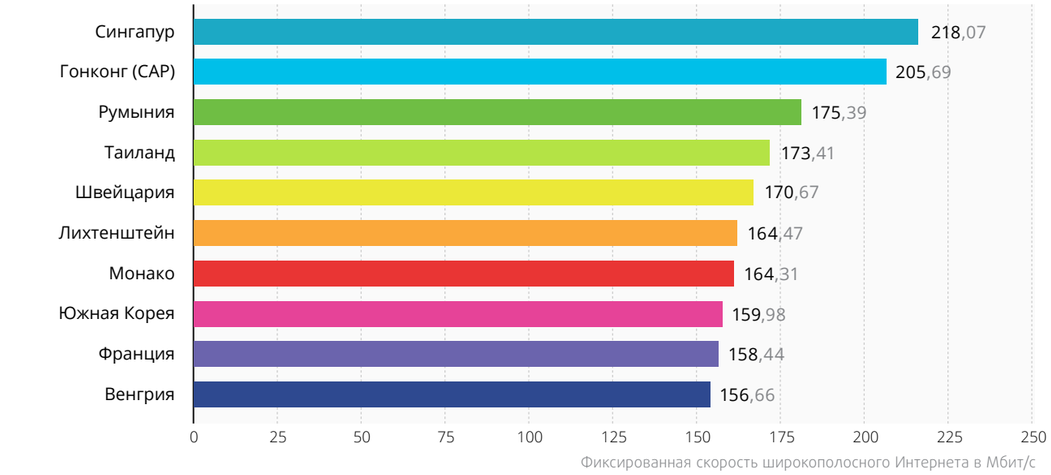
ЧИСЛО ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЕЙ В 2020 ГОДУ, ПО РЕГИОНАМ (В МЛН).

Источник: Statista, https://www.statista.com/statistics



СТРАНЫ С НАИБОЛЬШЕЙ СРЕДНЕЙ ПРОПУСКНОЙ СПОСОБНОСТЬЮ ФИКСИРОВАННЫХ ШИРОКОПОЛОСНЫХ СЕТЕЙ ДОСТУПА (В МБ/С)

Источник: Statista, https://www.statista.com/statistics



СТРАНЫ С НАИБОЛЬШЕЙ СРЕДНЕЙ ПРОПУСКНОЙ СПОСОБНОСТЬЮ МОБИЛЬНЫХ СЕТЕЙ (В МБ/С)

Источник: Statista https://www.statista.com/statistics

КАБЕЛИ, КОТОРЫЕ НАС СОЕДИНЯЮТ.
ПРОТЯЖЕННОСТЬ НОВЫХ ПОДВОДНЫХ КОММУНИКАЦИОННЫХ СИСТЕМ (В КМ) ПО ГОДАМ.

Источник: Tableau https://public.tableau.com/profile/varunvarma87#!/vizhome/Cablesthat-connectus/SubmarineCables

Эволюция обмена трафиком

Александр Ильин

Одновременно с развитием интернет-технологий перед операторами стояла, стоит и будет стоять достаточно непростая задача – как обеспечить максимально качественный обмен данными между участниками рынка. Мировые центры обмена трафиком находятся тут на гребне новых технологий, поскольку крайне важно обеспечить не только высокоскоростной обмен данными, но и иметь необходимые запасы прочности инфраструктуры с учетом дальнейшего роста объема передаваемых данных. Именно о технологиях развития точек обмена трафиком мы и поговорим сегодня.

У истоков

В России в 1995 году (в этом году исполняется 25 лет с того знаменательного момента) была создана первая точка обмена трафиком. Обслуживание этой сети передали в руки компании РосНИИРОС. Оборудование для «первой» точки долго искать не стали. В те годы у РосНИИРОС активно развивалась сеть FDDI, поэтому решили применить один из таких коммутаторов для начала проекта. Это была Cisco Catalyst 1200. Сеть решили запустить по технологии Ethernet, а FDDI использовать не стали. Всего восемь портов Ethernet было достаточным для начала проекта. Уникальное оборудование по качеству и надежности исполнения. До сих пор такое оборудование функционирует исправно и стоит сейчас в музее MSK-IX.

Итак, начало положено – казалось бы, чего проще: поставили коммутатор, включили туда операторов связи - и точка обмена трафиком готова. Так и было какое-то время. Площадка росла и развивалась, появлялось все больше новых игроков рынка, и она прирастала все новыми участниками.

Однако с первых же дней стало понятно, что за этой кажущейся простотой лежит немалая техническая работа. Участники включались разные, с разным оборудованием, политиками маршрутизации и правилами работы своих сетей. В то время инженеров, обладающих глубокими знаниями протоколов, специфики работы оборудования, было довольно мало - и были велики риски ошибок. И практически с первых дней эти ошибки стали влиять на инфраструктуру обмена трафиком. Стало понятно, что просто коммутатор с объявленными правилами игры мало спасает от ошибок участников. Стали появляться первые технические правила, выстраданные болью и возможными проблемами во взаимодействии операторов. Появилось и новое оборудование. Сеть плавно перешла на Cisco Catalyst 3000, а затем и на Cisco 5505. Росло и количество участников. В 1997 году уже 25 провайдеров было подключено к MSK-IX.

Технологическое развитие

Интересно, что в то время технологии развивались семимильными шагами и кругом было много новых идей. Было неочевидно, что среди прочих выиграет именно Ethernet. Однако наш рынок в то время уберегало некоторое отставание от технологий Запада. Одной из таких технологий была ATM (Asynchronous Transfer Mode — асинхронный способ передачи данных). Она лишь успела появиться на российском рынке - и практически тут же уже устарела. Это позволило сэкономить достаточно много ресурсов и помогло нам впоследствии развиваться на шаг впереди. Эта же ситуация была и с сетями ADSL. В то время как во всей Европе активно строили ADSL, у нас традиционные операторы связи не были готовы к этому – это позволило внутри страны построить сети Ethernet с использованием волоконно-оптических линий связи, и сейчас почти в каждом доме есть оптика, в то время как европейские потребители довольствуются ADSL-технологиями, потому что они оказались построены раньше, на этапе новых технологий уже были и до сих пор работают и всех устраивают.

Интересен тот факт, что именно в те годы, когда вокруг появились сети ATM, на нашей инфраструктуре появились ATM LANE-модули, что позволило нам смешать две технологии (Ethernet и ATM). Это было новаторское решение, у которого на тот момент не было аналогичных применений на пиринговых платформах, но нам быстро стало понятно, что технология Ethernet это обмен «каждый со всеми», в то время как ATM требует отдельного установления стыков «каждый с каждым».

Прогресс не стоял на месте, количество участников продолжало расти. Развивалась и инфраструктура обмена трафиком – вместо одного коммутатора, расположенного на одной площадке, сеть стала распределенной. Это повышало надежность и резервируемость - появилось три коммутатора на MMTC-9 в Москве. Интересно, что в России того времени появлялось множество операторов и главное наше отличие от крупнейших европейских центров обмена трафиком было в том, что у нас было в десятки раз больше уникальных автономных систем. Мы одни из первых задумались над созданием удобного для всех участников механизма обмена маршрутами. Сначала для этой цели были выбраны маршрутизаторы Cisco. К сожалению, они добавляли номер автономной системы IX в маршруты, но других решений на тот момент не было. Шли постоянные доработки этой системы как со стороны производителей, так и со стороны нашей технической службы. Cisco реализовала даже специальную версию операционной системы IOS для нужд точек обмена трафиком (с прозрачной работой Route Server). Однако в результате длинных и

сложных тестов нами был выбран программный подход к решению этой задачи, и мы ушли от зависимости производителей сетевого оборудования.

В Москве продолжали строиться новые дата-центры, и одна площадка на MMTC-9 уже не могла вмещать всех операторов. В 2000 году M9-IX расширилась и появилась MSK-IX, было построено оптоволоконное кольцо, объединяющее сразу четыре точки в разных частях города, пропускная способность была рекордной по тем временам – 1 Гб/с.

Для технической службы построение распределенной топологии было вызовом - стало понятно, что не обойтись без протокола резервирования кольцевой топологии. В то время выбор был невелик, и было принято решение остановиться на STP (Spanning Tree Protocol). Он вполне отвечал запросам того времени, но имел существенный недостаток - кольцо всегда было разорвано - и одна линия связи была пустой, в то время как другие испытывали повышенную нагрузку. Применение этого протокола стало накладывать также дополнительные требования к участникам. Пришлось выстраивать фильтры на границах сети, чтобы избежать регулярного перестроения Spanning-Tree при смене оборудования участников. Сколько было копий сломано, чтобы выстроить конфигурацию правильным образом и защитить сеть MSK-IX.

Интерес к нашей инфраструктуре рос с каждым днем. Нам стали предъявлять все более высокие требования к качеству и надежности. Мы особо уделяли внимание модернизации самой платформы, но не могли оставлять в стороне и надежность стыков участников.

Многие задумались о резервировании своих подключений к IX. Стали появляться резервные стыки с MSK-IX. Не у всех участников была возможность резервировать свою собственную сеть, но стык с IX все хотели иметь зарезервированный. Мы столкнулись с архитектурной проблемой - нельзя задать IP-адреса из одной подсети MSK-IX на разных интерфейсах одного устройства. В результате была запущена вторая IP-сеть с другим блоком адресов на MSK-IX и мы попросили участников поднять дополнительные адреса на их оборудовании. Мы постоянно работали над повышением качества сети и уже в 2001 году применили новые технические подходы и установили Cisco 6506 в качестве основного коммутатора системы. Cisco была обеспечена двойным супервизором и двойными блоками питания, что повышало надежность в случае отказа какого-либо элемента устройства.

Интересен тот факт, что именно в те годы, когда вокруг появились сети ATM, на нашей инфраструктуре появились ATM LANE-модули, что позволило нам смешать две технологии (Ethernet и ATM). Это было новаторское решение, у которого на тот момент не было аналогичных применений на пиринговых платформах, но нам быстро стало понятно, что технология Ethernet это обмен «каждый со всеми», в то время как ATM требует отдельного установления стыков «каждый с каждым».

Все эти решения накладывали еще больше требований к производителям оборудования, и мы активно участвовали в создании общего для всех платформ обмена трафиком документа IXP-Wishlist. По сути, был создан ключевой европейский документ для взаимодействия платформ обмена трафиком с производителями оборудования, где описывались методики, подходы и требования для реализации обмена трафиком. Требования складывались весьма специфичные, учитывая разнообразие подходов операторов к построению сетей и применению решений, способных нарушить работоспособность пиринговой экосистемы. Особенно много усилий было направлено на блокировку всевозможных «петель» и предупреждение их на самых ранних стадиях. Бриджевые петли крайне негативно влияли на работу сети и могли в мгновение остановить работу участников.

В то же время рынок специализированных устройств стал активно расширяться и на рынок стали выходить новые игроки, заинтересованные создавать все более мощные и функциональные устройства.

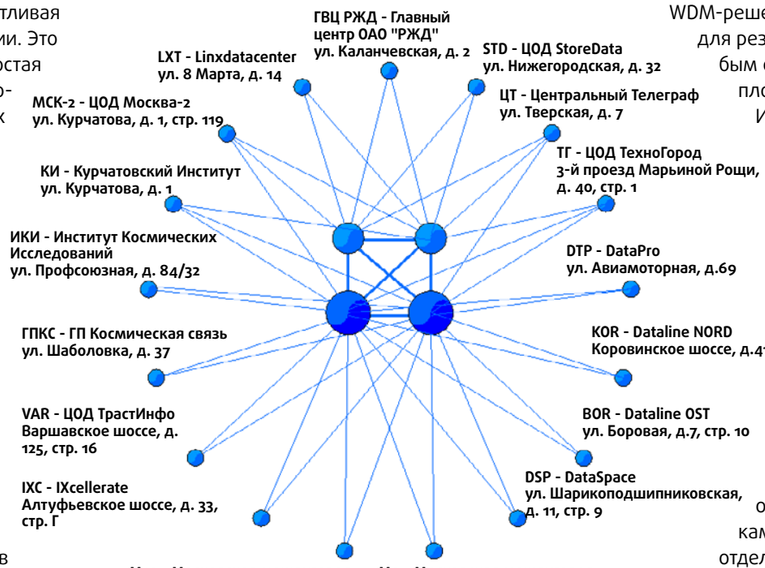
Появилось сообщество Euro-IX (ассоциация европейских точек обмена интернет-трафиком), членом которой стала MSK-IX. Деятельность ассоциации строилась, исходя из следующих целей: объединение усилий точек обмена трафиком в поиске оптимальных технических и административных решений, отстаивание единой позиции в диалоге с производителями оборудования и обмен опытом между специалистами по построению пиринговых платформ. MSK-IX вошла в пятёрку крупнейших точек обмена трафиком.

Бизнес-требования продолжали расти. Резервирование маршрутов, инфраструктуры, наращивание портовой емкости, возникли задачи по качеству передачи данных. Оборудования Cisco 6500 уже явно было недостаточно, архитектура имела ряд аппаратных ограничений и не была застрахована от потерь трафика в случае перегрузки внутренней шины данных. В технической службе MSK-IX продолжался активный процесс по поиску новых решений. Были проведены испытания нескольких платформ и по совокупности факторов выбран производитель оборудования Force10 (сейчас DellForce10). Поскольку одновременно заменять все оборудование не предоставлялось возможным, то был разработан поэтапный план миграции - с тем, чтобы минимально затронуть работоспособность сети. Таким образом, сеть стала многовендорной и это добавило еще правил в общую копилку требований к участникам и их оборудованию. Этот процесс продолжался и продолжается до сих пор. Force10 сменила компания Extreme Networks, а затем и оборудование Huawei. Каждый раз техническая служба руководствовалась в первую очередь техническими аспектами выбора. Исторически, каждые 3-4 года ситуация

на рынке меняется, выходят на арену все новые игроки, в то время как старые не всегда выживают, либо теряют интерес к этому сегменту рынка. Именно поэтому выбор платформы - это постоянная задача технической службы. Одним из направлений рутинной деятельности развития пиринговой платформы является поиск решений, подбор платформ и поиск новых производителей оборудования, продолжительные и сложные тесты в лаборатории, прежде чем решение дойдет до применения в производственном процессе. Это нелегкая и интересная задача.

С ростом сложности применяемых решений мы стали понимать, что невозможно запускать сервисы, используя исключительно описание документации. Требуется длительная и кропотливая работа в лаборатории. Это ежедневная и непростая задача по моделированию необходимых данных с целью проверки, обкатки решений и четкой диагностики во взаимодействии с производителями. На рынке мало решений, пригодных к использованию в пиринговых сетях без дополнительных доработок, и от того, насколько оперативно производитель готов сотрудничать, внедрять специальные решения, зависит надежность и стабильность нашей сети. Для принятия решений о внедрении новых технологий применяются высокопроизводительные устройства для нагрузочного тестирования. Преимущество этого подхода не только в том, что такое оборудование способно генерировать большие потоки данных, но и в том, что оно также способно имитировать работу участников и контролировать целостность и качество передаваемых через нашу платформу данных.

Рис. 1. Сегодняшняя топология MSK-IX



Новые услуги, новая архитектура

Новым вызовом для технической службы явилось внедрение и развитие нового проекта MSK-IX - «Медиалогистика», - который позволил транслировать телевизионные и радиосигналы с применением инфраструктуры MSK-IX. Трансляция ТВ-сигналов потребовала еще более критичного отношения к качеству передаваемого трафика. Даже микропотери трафика, которые могли пройти незаметно при использовании TCP, стали фиксироваться при передаче ТВ-сигналов. Внутри платформы нами было реализовано обеспечение качества передачи (QoS) и дополнительно был реализован мониторинг микропотерь на всей сетевой инфраструктуре. Накопленный опыт, по сути, уникален, поскольку ни в одной крупнейшей точке обмена трафиком не передается внутри ядра такое количество мультикаст-данных с гарантированными характеристиками доставки. По сути, мы получили в распоряжение сервис, удовлетворяющий высоким требованиям качества, которые нами и были реализованы в рамках платформы.

На текущий момент топология сети построена по принципу двойного «ядра», в центре которого установлены коммутаторы Huawei с применением технологии MLAG. Ядра расположены в географически разнесенных частях города в независимых энергозонах (рис. 1). Остальные площадки стыкуются либо с применением оптики, либо с применением WDM-решений с двумя ядрами для резервирования. Особым случаем выглядит площадка на MMTC-9. Исторически на этой площадке высокая концентрация интернет-провайдеров и наиболее нагруженное оборудование, эта площадка критична для текущей инфраструктуры. MSK-IX имеет три точки присутствия на MMTC-9, которые выглядят отдельными площадками. Стыковать их все отдельно с ядрами - не самая оптимальная идея (так как увеличит задержки между этажами M9 и понизит надежность), и поэтому для этой площадки нами была выработана отдельная схема мини-ядер. Все оборудование на MMTC-9 стыкуется с этими двумя независимыми мини-ядрами, которые в свою очередь стыкуются с основными ядрами платформы обмена трафиком. Такая схема обеспечивает простоту диагностики и помогает проводить работы на каждом плече (ядре) сети, не затрагивая функциональность общей инфраструктуры. Применяемые нами подходы позволяют избегать каких-либо простоев сети, успешно масштабировать решения с опережением развития скоростей подключений участников. Наши решения обеспечивают высокий уровень надежности на данном этапе развития технологий.

Зарубежный опыт

А что же происходит на международной арене с оборудованием для точек обмена трафиком?

По сути, сейчас рынок разделился и практически сети крупнейших точек обмена трафиком построены с использованием разных вендоров и применяют разные подходы

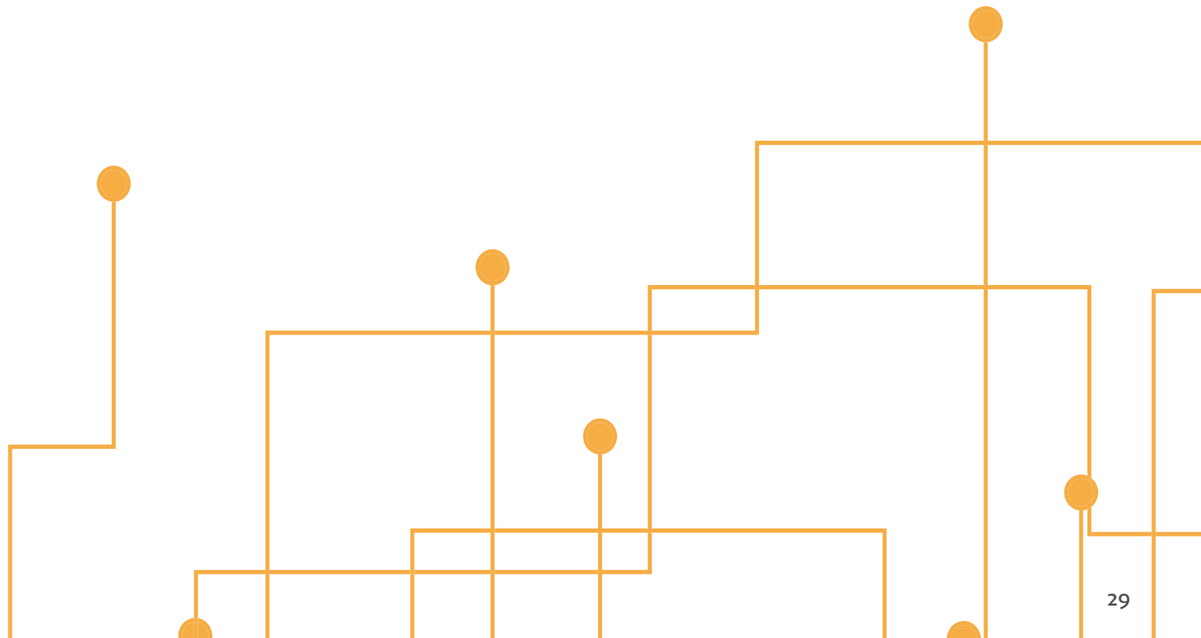
и решения. AMS-IX применяет вот уже много лет оборудование Brocade (сейчас Extreme Networks). У них внедрено достаточно интересное решение по резервированию клиентских подключений. Оптические подключения резервируются с помощью оптических переключателей. Хотя и стоимость такого решения весьма высока (многопортовые оптические переключатели - недешевое удовольствие), она еще и подвержена дополнительным рискам. Часто при проведении работ коллегам из AMS-IX приходится переключать сразу группу портов на другое устройство, причём делать это одномоментно, чтобы исключить потери трафика. Плюс оптические переключатели сами вносят дополнительную точку отказа. Однако за много лет коллегам удалось выстроить надежную сеть, и она тоже показала свою эффективность.

Немецкие коллеги из DE-CIX построили свою основную сеть на платформе Alcatel Lucent (сейчас Nokia). Их сеть активно масштабируется на другие платформы под их управлением и развивается по всему миру. Интересно также выглядит подход компании LINX (Лондон). Несколько лет назад ими было принято решение о строительстве сразу двух параллельных точек обмена трафиком на разном оборудовании. Для этой цели сейчас применяется Juniper Networks и EdgeCore. Такой подход позволил не только зарезервировать инфраструктуру, но и проводить плановые работы по отдельности на той или другой линейке оборудования, а также тестировать и внедрять новые решения. В частности, они реализовали новый технологический подход на оборудовании Edgecore, где оборудование выступает в роли «whitebox» (простейших «коробок» с коммутацией пакетов), а внешняя компания IP Infusion реализовала функционал обмена трафиком на этой платформе.

Интересно, что технология Ethernet показала свою эффективность не только в рамках городского обмена, но и при построении распределенных сетей. Один из крупнейших центров обмена создан в Бразилии. Коллегам удалось объединить в единую сеть по всей стране свыше 30 центров обмена трафиком, крупнейшие из которых находятся в Сан-Паоло и Рио-де-Жанейро. Азиатские центры обмена трафиком имеют свою специфику в применении технологий. Например, коллеги в JPIX обслуживают сразу две сети в разных городах. Топология этих сетей сделана по образу звезды, где центр расположен в Токио и Осаке. В целом, решений на рынке платформ обмена трафиком достаточно много и они постоянно дорабатываются, и в крупнейших центрах применяются нестандартные подходы к управлению и обслуживанию подобных сетей.

Если же заглянуть на кухню точек обмена трафиком, то несложно заметить, что многие базируются на традиционной топологии Layer 2. При доступности современных протоколов и решений этот подход выглядит некоторым атавизмом. Однако это далеко не так. Многие крупнейшие точки обмена трафиком (в том числе и наша) регулярно ищут новые способы решения задач и проводят испытания таких технологий, как OpenFlow, VXLAN, VPLS и других, но важно отметить, что основу всех решений составляет надежность, управляемость и масштабируемость, и немаловажным фактором выступает простота «траблшутинга» (troubleshooting). И тут, как ни странно, на настоящий момент побеждает именно простота Layer 2-топологии, применяемой на нашей платформе обмена, хотя, безусловно, будущее нам еще покажет.

За 25 лет своего существования MSK-IX из единственного коммутатора превратилась в распределенную надежную высокоскоростную инфраструктуру обмена трафиком. Это развитие шло в ногу с развитием самого Интернета – менялись скорости, технологии и оборудование, появлялись новые приложения. Неизменным остался дух сотрудничества, позволивший нам вместе с операторами-участниками вывести MSK-IX на мировой уровень. Несмотря на солидный по Интернет-меркам возраст, MSK-IX по-прежнему молода и готова к будущему.



В поисках качества

Андрей Робачевский

В повседневном использовании Интернета мы не очень задумываемся о параметрах качества Сети. Для большинства приложений Интернет просто работает, а если работает плохо, то трудно сказать, в чем проблема – то ли домашняя сеть тормозит, то ли провайдер, то ли сам веб-сайт. И никого не удивляет, что, например, качество видеоконференции Zoom или Skype вчера было отличным, а сегодня видео замирает, а речь участников прерывается. И тем не менее, сегодня также никого не удивляет, что телефония через Интернет по качеству мало отличается от традиционной (а если и отличается, то винить в первую очередь стоит плохую настройку домашней сети), что мы можем смотреть стриминг-видео высокого разрешения, и что облачное хранилище подчас превосходит по производительности локальный диск. А как насчет удаленной хирургии и автономных автомобилей?

Мы знаем, что Интернет – это технология «best effort», а это значит, что сеть будет пытаться обеспечить передачу до последнего, пока пользователь сам не оставит свои попытки. Но сегодня «best effort» уже не ассоциируется с мучительными замираниями передачи, а то и вовсе прерыванием связи. Интернет пережил колоссальную трансформацию, которая сделала возможным видеостриминг высокого разрешения, облачные вычисления и сетевые компьютерные игры с погружением в виртуальную реальность. Так все-таки, может Интернет обеспечивать качество или нет?

Попробуем в этом разобраться.

Начну с того, что задачи обеспечения параметров качества передачи, или QoS (Quality of Service), органично вписываются в сети коммутации каналов, такие как традиционные телефонные сети. В традиционной телефонии каждая сеть, через которую проходит вызов, должна сначала зарезервировать ресурсы, а затем предоставить канальную емкость для соединения или разговора, если вызываемый абонент снял трубку. В результате соединение между двумя говорящими имеет гарантированные пропускную способность и другие параметры качества, как, например, задержку. Но если хотя бы одна из сетей перегружена и не может обеспечить канальную емкость, все предыдущие резервирования должны быть отыграны назад, и сеанс передачи не состоится.

Другой особенностью является то, что сети коммутации каналов являются синхронными, по существу, не использующими буферизации. Это означает, что задержка при передаче между пользователями определяется в основном скоростью распространения сигнала или, другими словами, расстоянием между абонентами.

Интернет же коренным образом отличается от телефонных сетей. Топология и связность сетей, как правило, весьма разветвленная и нерегулярная. «Стандартной услуги» как таковой нет - различные приложения имеют различные требования к пропускной способности и качеству сети. Также Интернет является сетью пакетной передачи, где IP-дейтаграммы асинхронно передаются узлами-маршрутизаторами по каналам со значительной вариацией пропускной способности. Это, в свою очередь, выражается в нерегулярности трафика и требует использования буферов для сглаживания «всплесков». Как мы увидим дальше, буферизация и управление очередями пакетов является важным фактором качества связи.

Но пакетная передача – это полбеды. Основная проблема обеспечения качества заключается в обеспечении связности между сетями и соответствующих взаимоотношений между операторами. Подавляющее большинство этих взаимоотношений берут в расчет только усредненные параметры пропускной способности и только в целом по каналу, не различая отдельные приложения и типы трафика.

Таким образом, для обеспечения заданных параметров качества в Интернете или хотя бы приоритизации отдельных приложений необходимо **а)** создать возможность для сетей договариваться не только о «связности», но и о более детальных параметрах передачи, включая динамическое резервирование пропускной полосы; и **б)** внедрить механизмы обеспечения заданных параметров качества в рамках одной сети, или точнее, в рамках одного административного домена.

Начнем с межсетевого вопроса.

IntServ или интеграция служб

В середине 90-х годов прошлого века в IETF (www.ietf.org) была разработана концепция, получившая название Integrated Services, или IntServ (Интегрированные службы). Как указано в документе RFC1633[1], описывавшем архитектуру IntServ, «это расширение [архитектуры Интернета] необходимо для удовлетворения растущих потребностей в услуге реального времени для широкого диапазона приложений, включая телеконференции, удаленные семинары и распределенное моделирование». Также IntServ должен был обеспечить возможность мультиплексирования различных классов трафика в сети, что позволило бы операторам предоставлять различные изолированные друг от друга услуги, используя общую сетевую инфраструктуру.

IntServ определяет два основных класса приложений: приложения реального времени, чувствительные к задержке, и «эластичные» приложения, для которых не так важно, когда именно будут получены данные, а точнее, дейтаграммы.

Чувствительность к задержке приложений реального времени также различается. Например, для передачи голосового или видеопотока приложению необходимо знать максимально возможную задержку для обеспечения адекватной буферизации. В противном случае поток будет прерываться и его качество деградирует. Для таких приложений IntServ предлагает т.н. гарантированную услугу, при которой задержка не может превысить заданную величину.

Менее чувствительные приложения смогут удовольствоваться т.н. предсказуемыми услугами, гарантирующими среднестатистическую задержку. Соответственно, предполагается, что стоимость таких услуг будет значительно дешевле, так как этот подход позволяет достичь гораздо большей утилизации сети. Наконец, «эластичные» приложения могут продолжать пользоваться «обычным» Интернетом с его услугой best effort.

Хотя сам подход казался привлекательным, он требовал двух существенных изменений в архитектуре и функционировании Интернета. А именно, обеспечения требования контроля доступа и резервирования.

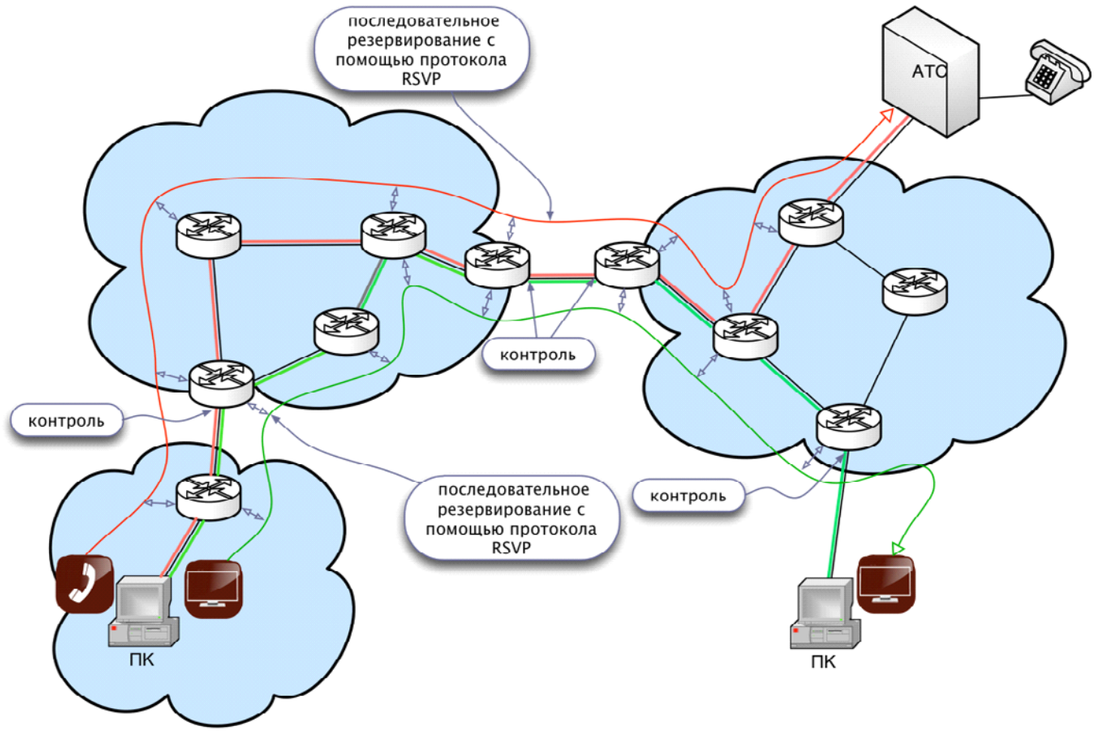
Действительно, для возможности предоставления гарантий по задержке и пропускной способности сетевые ресурсы должны быть первоначально зарезервированы по всему пути передачи данных от источника к получателю (и обратно, поскольку большинство потоков являются дуплексными). Этот процесс очень напоминает резервирование канала в телефонии, только вариация параметров этих каналов значительно больше. Это, в свою очередь, потребовало внедрения дополнительного сигнального протокола резервирования (такой протокол был разработан - RSVP[2]) и модификации протоколов внутри- и межсетевой маршрутизации.

Далее, прежде чем сеанс связи сможет состояться, приложение должно «заключить контракт» с сетью, в соответствии с которым сеть будет обеспечивать передачу данных. Этот «контракт» предусматривает, что приложение не выйдет за рамки установленных параметров, а сеть обеспечит входной контроль. Более того, этот «контракт» должен быть заключен со всеми независимыми сетями на пути от отправителя к получателю.

Схематично архитектура IntServ показана на рис. 1.

Даже не вдаваясь в подробности, можно заметить, что уже на техническом уровне внедрение IntServ означало существенное усложнение архитектуры Сети. В экономическом смысле это означало существенное удорожание инфраструктуры для поддержки новой функциональности. Бизнес-отношения и систему взаиморасчетов между сетевыми операторами необходимо было коренным образом пересмотреть.

Рис. 1. Архитектура IntServ. На схеме представлено резервирование двух каналов с различными параметрами качества: для видеоконференции (зеленый цвет) и голосовой связи (красный цвет).



Наконец, технологии IntServ должны были быть внедрены и поддерживаться глобально, во всем Интернете. В чем ценность островков качества в океане услуг «best effort»?! Как и в случае многих других глобальных технологий, преимущества от их внедрения становятся ощутимыми, только когда они получают значительное распространение – своего рода замкнутый круг, который нелегко разорвать.

Другими словами, даже одной из перечисленных проблем было достаточно, чтобы поставить под сомнение будущее предлагаемого решения. В случае с IntServ решение осталось в основном на бумаге.

DiffServ – почувствуйте разницу

Однако идея поддержки качества в глобальной инфраструктуре Интернета была слишком заманчивой - и IETF сделал вторую попытку и взялся за разработку другого подхода, целью которого было обеспечение относительного, а не абсолютного, как в случае с IntServ, качества передачи. Другими словами, приложениям реального времени гарантируется определенная емкость, в рамках которой различные потоки конкурируют между собой. Эта архитектура была названа Differentiated Services, или DiffServ.

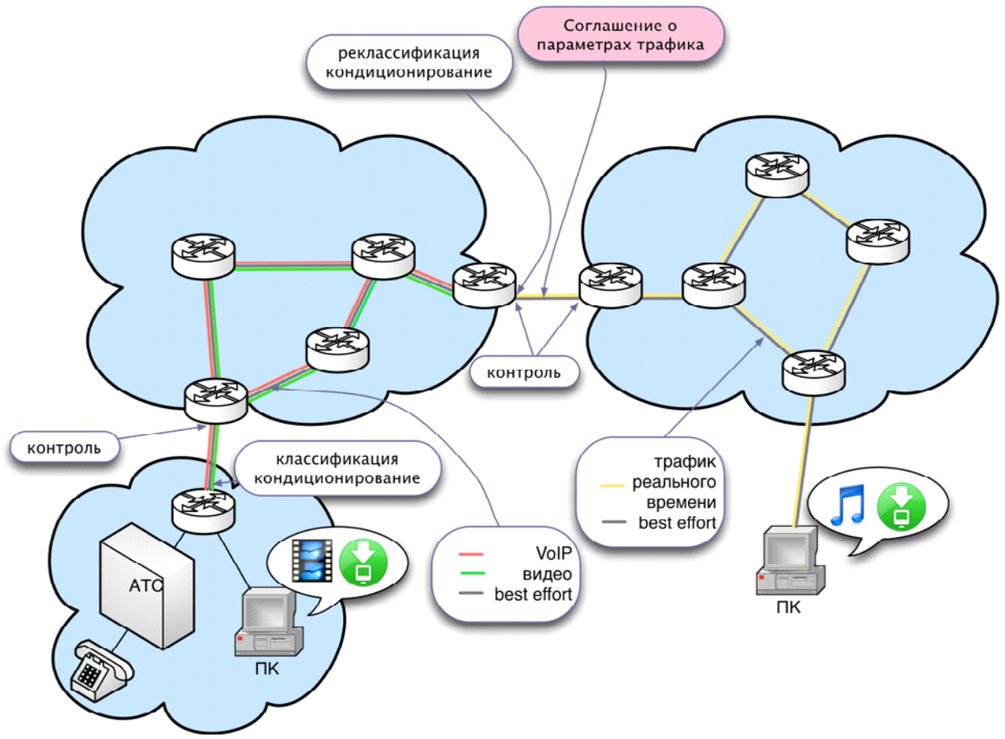
Вместо резервирования на уровне потока/приложения, в DiffServ контроль производится на уровне достаточно статичных агрегированных «профилей» трафика. Классификация пакетов и принадлежность их к тому или иному профилю определяется по полю IP Type of Service (TOS), исторически оставшемуся в заголовке IP-пакета. Соответственно, соглашение между различными сетями должно включать договоренность о параметрах ограниченного числа профилей. При этом на входе в сеть производится контроль и возможное кондиционирование трафика для каждого профиля, которое включает буферизацию или даже отброс пакетов, если агрегированный поток превышает договоренные параметры.

Масштабируемость данного подхода, безусловно, лучше по сравнению с IntServ. Еще важнее, что DiffServ не требует динамического резервирования и сохранения состояния для каждого узла сети и каждого потока, проходящего через нее. Однако неразрешимым вопросом остается проблема предоставления определенного качества индивидуальному приложению, включая сигнализацию и гарантии. Трудно представить, что динамические требования многообразных приложений Интернета можно уложить в прокрустово ложе статической конфигурации нескольких профилей.

Другими словами, и это решение не вызвало большого энтузиазма среди операторов. Ресурсы и инвестиции, требуемые для внедрения «качественных» решений, нашли лучшее применение в увеличении канальной емкости, благо и стоимость этих каналов к концу 90-х значительно упала.

Замечу, что концепции DiffServ используются для оптимизации трафика во внутренней инфраструктуре сети оператора, и здесь производители оборудования всегда рады помочь с широким набором возможностей, однако задача обеспечения сквозного качества в Интернете остается иллюзией. О полезных применениях DiffServ мы поговорим чуть позже.

Рис. 2. Система DiffServ, позволяющая управлять качеством ограниченного числа «профилей» трафика. На схеме: голосовой трафик, видео и обычный трафик «best effort».



DetNet – сетевой детерминизм

Но если обеспечение качества передачи в Интернете, а точнее, в интердоменном пространстве, представляется сложным, «качественная» передача данных в отдельно взятой сети является вполне достойной и реальной задачей. Ведь, в конце концов, проблема глобального качества не в технологии, а в отсутствии экономических мотивов усложнённых межсетевых отношений.

Над решением этой задачи работает созданная в рамках IETF рабочая группа DetNet (Deeterministic Networking, https://datatracker.ietf.org/wg/detnet/about/). Основная цель DetNet - обеспечить конвергенцию чувствительных не-IP-сетей в общую сетевую инфраструктуру. Это требует точной эмуляции развернутых в настоящее время специализированных сетей, которые, например, используют аналоговые (например, с модуляцией 4-20 мА) и последовательные цифровые соединения точка-точка для обеспечения связи с высокой надежностью, синхронизацией и отсутствием джиттера. Хотя задержка аналоговой передачи - это, по существу, скорость света, традиционные последовательные каналы обычно медленные (порядка кбит/с) по сравнению, скажем, с Gigabit Ethernet, и некоторая задержка обычно приемлема. Что неприемлемо, так это введение чрезмерного джиттера, который может, например, повлиять на стабильность систем управления.

Особенностью DetNet является то, что она занимается исключительно значениями наихудшего случая для сквозной задержки, джиттера и неупорядоченности пакетов. Средние или типичные значения не представляют особого интереса, поскольку они не влияют на способность системы реального времени выполнять свои задачи. В общем случае тривиальная схема организации очередей на основе приоритетов даст лучшую среднюю задержку для потока данных, чем DetNet, однако это может быть неподходящим вариантом для DetNet из-за показателей задержки в наихудшем случае.

DetNet обеспечивает выполнение таких строгих требований по передаче данных с помощью трех основных методов: размещение и резервирование ресурсов, защита сервиса и использование статических предопределенных маршрутов.

Конечно, существуют более простые методы, доступные (и используемые сегодня) для достижения уровней задержки и потери пакетов, приемлемых для многих приложений. Приоритизация и избыточное выделение ресурсов - один из таких методов. Однако эти методы обычно работают лучше всего в отсутствие какого-либо значительного объема некритического трафика в сети (если такой трафик поддерживается). Они также могут работать только в том случае, если критический трафик составляет лишь небольшую часть теоретической емкости сети, если все системы работают должным образом или если действия конечных систем, нарушающие работу сети, отсутствуют.

DetNet использует три метода для обеспечения такого качества обслуживания:

- Распределение ресурсов

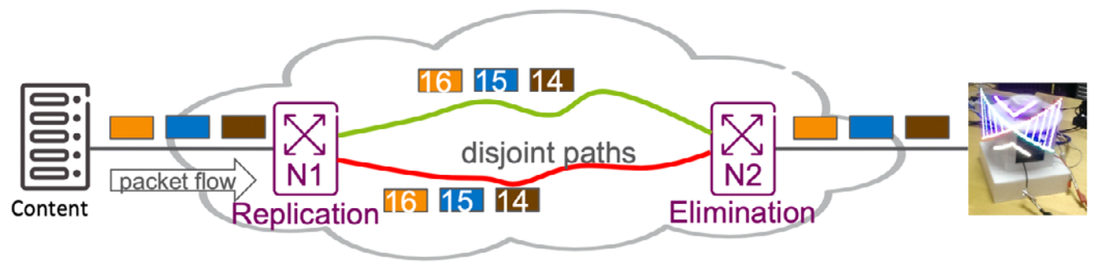
  Обеспечение гарантий QoS DetNet осуществляется за счет устранении потери пакетов из-за конкуренции потоков. Это может быть достигнуто только путем предоставления достаточного буферного пространства на каждом узле по сети, чтобы гарантировать, что никакие пакеты не будут отброшены из-за нехватки буферов. При этом каждый из узлов DetNet должен внимательно следить за соблюдением зарезервированных параметров передачи, например, предотвращая отправку пакета раньше времени. Дело в том, что такой пакет потребует дополнительного буферного пространства на следующем узле и может таким образом превысить зарезервированные параметры.

  DetNet обеспечивает ограниченную задержку передачи за счет резервирования полосы пропускания и ресурсов буфера на каждом узле DetNet на пути потока DetNet. В настоящее время рассматриваются три возможных класса архитектур плоскости управления DetNet[3]: полностью распределенная система управления, использующая протоколы динамической сигнализации, как, например RSVP-TE; полностью централизованная система управления, подобная SDN; и система управления, объединяющая эти два класса.

- Защита сервиса

  Защита сервиса направлена на устранение потери пакетов из-за отказов оборудования, включая случайные сбои носителей и/или памяти. Эти типы потерь пакетов могут быть значительно уменьшены за счет репликации потока данных и последующего их распределения по нескольким непересекающимся путям пересылки. Функции защиты сервиса также следят за упорядоченным получением пакетов. Принцип работы этих функций представлен на рис. 3.

Рис. 3. Репликация, устранение и упорядочение пакетов в DetNet.[4]



- Явные маршруты

Чтобы получить преимущества небольшого количества переходов и при этом обеспечить защиту даже от очень кратковременных потерь связи, DetNet использует явные маршруты, где путь, выбранный данным потоком DetNet, не изменяется, по крайней мере, не сразу и, вероятно, вообще не изменяется в ответ событиям сетевой топологии. Защита услуг (см. разделы 3.2.2 и 3.2.2.3) по явным маршрутам обеспечивает высокую вероятность непрерывного соединения. Явные маршруты могут быть установлены различными способами, например, с помощью RSVP-TE [RFC3209], с помощью сегментной маршрутизации (SR) [RFC8402], с помощью подхода SDN [RFC8453], с помощью IS-IS [RFC7813] и т.д. обычно используется в путях коммутации меток (LSP) MPLS TE (Traffic Engineering).

Основная цель DetNet - обеспечить конвергенцию чувствительных не-IP-сетей в общую сетевую инфраструктуру. Это требует точной эмуляции развернутых в настоящее время специализированных сетей, которые, например, используют аналоговые (например, с модуляцией 4-20 мА) и последовательные цифровые соединения точка-точка для обеспечения связи с высокой надежностью, синхронизацией и отсутствием джиттера.

Архитектура DetNet

Функциональность DetNet реализована на двух смежных подуровнях в стеке протоколов: подуровне сервиса DetNet и подуровне передачи. Подуровень сервиса DetNet обеспечивает защиту сервиса для более высоких уровней стека протоколов и приложений. Подуровень передачи обеспечивает функциональность DetNet в базовой сети, например, путем предоставления явных маршрутов и распределения ресурсов для потоков DetNet. Упрощенная схема сети DetNet представлена на рис. 4.

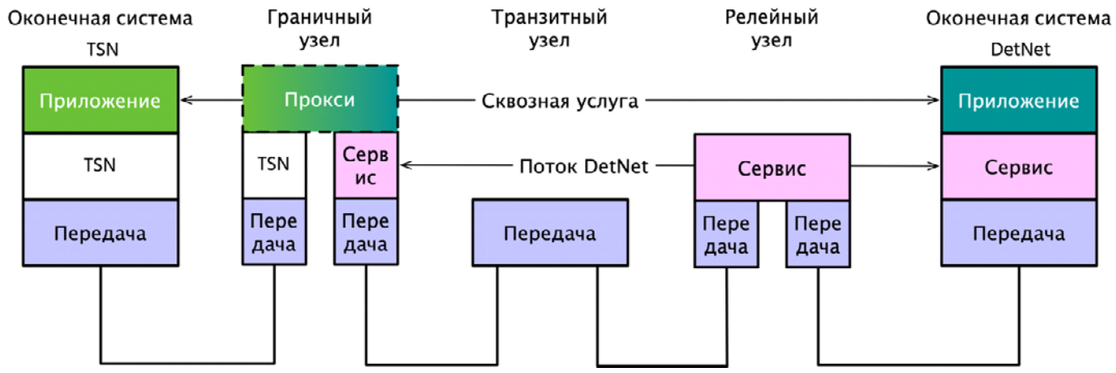
Оконечные системы с поддержкой DetNet и узлы DetNet могут быть связаны между собой подсетями, то есть технологиями «уровня 2». Для поддержки трафика DetNet эти подсети должны предоставлять совместимые услуги. Примеры сетевых технологий «уровня 2» включают MPLS TE, TSN (Time Sensitive Networking, IEEE, Time-Sensitive Networking (TSN) Task Group, https://1.ieee802.org/tsn/) и каналы OTN (Optical Transport Network) точка-точка. Конечно, возможны и многоуровневые системы DetNet, где одна DetNet выступает в качестве подсети и предоставляет услуги более высокоуровневой системе DetNet.

DetNet может также использоваться для предоставления услуг «уровня 2», например, для приложений TSN. В случае использования DetNet как сети «уровня 3» сквозной услугой является соединение IP. Концептуально это напоминает услуги типа L3VPN или IP поверх MPLS.

Важным вопросом для успешного применения этой технологии является вопрос масштабирования. Для резервирования отдельных потоков DetNet требуется значительная информация о состоянии в каждом узле сети, особенно когда требуется адекватное устранение неисправностей. Для возможности эффективной поддержки большого количества потоков необходима их агрегация. Такие агрегированные потоки могут рассматриваться узлами DetNet в основном как отдельные потоки DetNet.

Технология DetNet находится в процессе разработки. Одноименная рабочая группа в IETF[5] стандартизовала основные архитектурные аспекты технологии, но многое еще предстоит сделать.

Рис. 4. Схема сети DetNet со шлюзом в сеть TSN (Time Sensitive Networking)



Несколько лет назад Джефф Хьюстон проанализировал[6] проблемы внедрения «качества обслуживания» в Интернете и пришел к выводу, что под этой маркой производители оборудования продают не что иное, как «новое платье короля».

Но задачи перевода существующих приложений на унифицированную технологию и приложения будущего - индустриальные приложения автоматизации и контроля, телемедицины - ставят вопросы QoS на повестку дня острее, чем когда либо. И хотя QoS как гарантия точных параметров качества – пропускной способности, максимальной задержки, джиттера – в глобальном Интернете вряд ли будет внедрена по причинам, которые Джефф точно описал, обеспечение заданных параметров в рамках единого административного домена «специализированных» сетей вполне реально. Причем с использованием протоколов и архитектуры Интернета.

Ссылки

1. http://datatracker.ietf.org/doc/rfc1633

2. http://datatracker.ietf.org/doc/rfc2205

3. https://tools.ietf.org/id/draft-malis-detnet-controller-plane-framework-04.html

4. Источник: https://www.ietf.org/proceedings/101/slides/slides-101-rtgarea-deterministic-networking-detnet-00

5. https://datatracker.ietf.org/group/detnet

6. Geoff Huston, «The QoS Emperor's Wardrobe», https://www.potaroo.net/ispcol/2012-06/noqos.html

Защита электронной почты с помощью DMARC и ARC

Джон Левин (John Levine)

Спецификация DMARC начиналась как относительно простой метод предотвращения фишинга, который взяли на вооружение известные коммерческие домены. Затем этот метод был переориентирован на борьбу со спамом. Хотя такое перепрофилирование в основном и решило проблему спамового подлога для многих систем, оно также нанесло значительный сопутствующий ущерб спискам рассылки электронной почты. Для того, чтобы справиться с недостатками DMARC, группа крупных провайдеров электронной почты разработала механизм аутентификации ARC, который позволяет в каком-то смысле изучить историю сообщения и узнать, каким образом не согласованное в рамках DMARC сообщение приобрело такой статус.

В современном Интернете электронная почта превратилась в один из самых полезных сервисов, но одновременно стала и наиболее разочаровывающим. Лучшим её свойством стало то, что любой человек может отправить сообщение кому угодно без предварительной договорённости, а худшим недостатком стало то же самое – возможность отправить сообщение кому угодно без предварительной договорённости. По мере того, как в 90-е годы прошлого века и в нулевые нынешнего электронная почта становилась всё более вездесущей, росла и доля сообщений, которые адресаты не хотели бы получать. В 2005 году появились статьи о спаме за авторством Дейва Крокера (Dave Crocker)[1] и Джона Кленсина (John Klensin)[2]. С той поры получили широкое распространение несколько описанных в статье Крокера методов борьбы со спамом, а сама проблема спама стала ещё острее.

Важно проводить различие между *спамом* – незапрашиваемыми сообщениями, которые распространяются с помощью массовой рассылки, и *фишингом (phishing)* – письмами, которые отправляются с целью введения получателя в заблуждение с последующей попыткой получить от него данные учётных записей/счетов или другой частной информации. (Некоторые фишинговые письма являются массовыми, а другие отправляются конкретным жертвам; последний метод получил название *адресный фишинг (Spear phishing)*.) Начиная с 2007 года компания PayPal, ставшая одним из самых частых целей фишинга, начала сотрудничать с некоторыми крупными почтовыми системами, стремясь не допустить попадания фишинговых сообщений в почтовые ящики получателей. В основе лежала идея о том, что системы получателя смогут идентифицировать настоящее электронное письмо от PayPal и отбрасывать любые другие сообщения, «притворяющиеся» письмами PayPal. Для того, чтобы обобщить этот метод и способствовать его распространению, в 2012 году отраслевая группа инициировала проект DMARC. В 2015 году спецификация *Domain-based Message Authentication, Reporting & Conformance* (DMARC) была опубликована в качестве информационного RFC[3], и в настоящее время эта технология наиболее широко применяется в крупных почтовых системах.

Принцип работы DMARC заключается в привязывании адреса в заголовке «**From:**» RFC 5322[4] сообщения к почтовой аутентификации и в предоставлении возможности оператору домена предлагать получателям почты рекомендации по используемым политикам. Если сообщение проходит успешную валидацию методами *Sender Policy Framework* (SPF) или *DomainKeys Identified Mail* (DKIM), а домен при валидации совпадает с доменом в заголовке **From:**, то сообщение считается «согласованным» с DMARC. Почтовая система-отправитель может публиковать записи политик DMARC в DNS, «требуя», чтобы системы-получатели отправляли на карантин (помещали в папку спама) или отбраковывали несогласованные сообщения. Весь этот механизм очень хорошо работает в изначальной области применения DMARC – почте между бизнесом и потребителем (B2C), в рамках которой отправляющая сторона обычно полностью контролирует все сообщения, отправленные из своего домена. Особенно успешно этот механизм зарекомендовал себя для PayPal. В этой системе вся почта представляет собой вариации на тему «зайдите в свою учётную запись, чтобы узнать, что нового», поэтому случайная потеря некоторых сообщений по причине их неправильной обработки сервисом DMARC не является большой проблемой.

Основополагающие и предыдущие работы в этой области

DMARC полагается на два уже существующих метода аутентификации почты – SPF[5] и DKIM[6]. SPF осуществляет валидацию домена в адресе **MAIL FROM:** RFC 5321[7]. Домен может опубликовать использующую сложный синтаксис запись SPF, чтобы задать набор IP-адресов.

Если сообщение было отправлено с одного из этих адресов, то SPF-валидация объявляется успешной. (Это очень упрощённое описание; полную информацию см. в [5].) К достоинствам SPF относится простота реализации этого расширения, поскольку для этого не требуется вносить изменения в исходящие сообщения и достаточно лишь единственной записи DNS. Однако с помощью этого метода можно описать лишь ограниченное подмножество способов доставки почты. В большинстве случаев так можно обрабатывать только почту, которую отправитель напрямую посылает получателю без использования переадресации или пересылки; кроме того, это плохо подходит для почты, посланной третьей стороной по поручению отправителя. Хотя SPF и предоставляет код **-all**, - который рекомендует получателям отбраковывать поступившие из домена сообщения при неудачном результате валидации SPF, большинство почтовых систем не прислушиваются к этому совету из-за слишком высокого процента ложных срабатываний.

DKIM осуществляет валидацию контента сообщений при помощи добавления в сообщение заголовков криптографической подписи, которые получатель может проверить, используя ключ в DNS. Каждая подпись хранится в поле заголовка **DKIM-Signature**, содержащем несколько субполей, в том числе для имени домена, добавившего подпись. Успешная валидация подписи DKIM означает, что, во-первых, в сообщение не вносились изменения с момента его подписания, и, во-вторых, домен в подписи берёт на себя ответственность за сообщение. Поскольку DKIM осуществляет валидацию контента сообщения, а не пути, на него не влияет переадресация.

DKIM значительно труднее реализовать, чем SPF, поскольку для него следует так модифицировать программное обеспечение почтовых систем, чтобы оно могло добавлять в каждое исходящее сообщение заголовки для подписи. Кроме того, необходимо, чтобы подписывающая система создавала пары ключей открытый/секретный, публиковала открытый ключ в DNS и вписывала секретный ключ в настройки подписывающего ПО. Валидация DKIM считается неудачной, если в процессе передачи сообщение было изменено - например, когда список рассылки добавляет метку темы или примечание к сообщению, а иногда просто потому, что агент *Message Transfer Agent* (MTA) изначально не был настроен на добавление подписи. (В крупных компаниях бывает очень трудно отслеживать все компьютеры, отправляющие электронную почту. Как это будет понятно позднее, DMARC помогает решить эту проблему.)

К DKIM имеется опциональное дополнение под названием *Author Domain Signing Practices* (ADSP)[8], которое как бы представляет собой прототип DMARC. Домен может опубликовать в DNS запись ADSP, которая предупреждает, что если сообщение с этим доменом в поле **From:** не имеет действительной подписи DKIM из того же домена, то получатели должны игнорировать такое сообщение. Правила ADSP никогда не применялись за пределами экспериментов, и со временем группа IETF превратила их в историческую (утратившую актуальность) спецификацию.

Развёртывание DMARC

Одна из причин того, почему предыдущие подходы к реализации политик отправителя (такие, как SPF **-all** и ADSP) потерпели неудачу, заключается в том, что нет никаких способов их протестировать - за исключением включения и последующего наблюдения за результатами. Это выполнимо для небольшого домена с парой почтовых серверов, однако для крупных компаний риск оказался чрезмерно высоким, поскольку они не всегда полностью осведомлены обо всех своих системах, отправляющих электронную почту, а также о настройках таких систем.

В состав DMARC входит целый ряд функций для проверки согласования почты домена перед публикацией рекомендаций по политикам. Там имеются мощные средства для создания отчётов, которые просят другие системы прислать отчёты о почте, претендующей на отправление от имени домена. Перед публикацией любых политик домены неизменно просят о направлении отчётов - с тем, чтобы «увидеть», какие отправляемые ими сообщения согласованы, а какие нет. Это позволяет им исправить проблемы с согласованием до публикации политик.

Валидация DMARC

После поступления сообщения первым шагом валидации DMARC является поиск записи политики DMARC для домена заголовка **From:**, после чего проводится валидация подписи(ей) DKIM и SPF сообщения и затем возможны операции с самим сообщением. Первый шаг заключается в поиске записи политики для домена **From:** сообщения – записи DNS TXT. Если этим доменом является **marketing.mybiz.example**, то сначала проводится поиск в **_dmarc.marketing.mybiz.example**. Если там обнаруживается запись типа TXT (текстовая запись) с использованием синтаксиса DMARC (например, она начинается с **v=DMARC1;**), то это и есть искомая запись политики. Если ничего не найдено, то выполняется поиск записи политики в «организационном домене».

Спецификация DMARC содержит умышленно нечёткое определение относительно того, каким образом следует искать организационный домен, однако на практике всегда используется список *Mozilla Public Suffix List* (PSL)[9], в котором организационный домен представляет собой наддомен непосредственно под опубликованным суффиксом (суффиксом опубликованного DNS-узла). В данном случае, если домен является типичным доменом верхнего уровня (TLD, Top-Level Domain), который принимает регистрацию на втором уровне, организационным доменом будет **mybiz.example**. Поэтому будет выполнен поиск записи типа TXT в домене **_dmarc.mybiz.example**. Если там будет обнаружена такая запись с синтаксисом DMARC, то это и есть запись политики; в противном случае для этого домена отсутствует запись политики.

Запись DMARC представляет собой список пар «ключ=значение» с правилами для проверки согласования того, что следует делать с несогласованной почтой и куда отправлять агрегированные отчеты и отчеты об ошибках. Типичная запись может выглядеть следующим образом:

```
v=DMARC1; p=none; rua=mailto:dmarc-a@example.net;
ri=3600; ruf=mailto:dmarc-f@example.net
```

В данном случае политика отсутствует (**none**), отчеты о злоупотреблениях и ошибках отправляются по указанным адресам (**rua** и **ruf**), а интервал между запрошенными отчётами составляет один час (**ri** равен 3600 секундам). У второй проверки на наличие организационного домена двойная цель. Во-первых, вторая проверка облегчает раз-

вертывание DMARC в рамках крупных компаний, поскольку одна организационная запись DMARC может отхватывать все субдомены организации. Во-вторых, она охватывает несуществующие субдомены организационного домена в случаях, когда враждебные или ошибочные отправители посылают сообщения, притворяющиеся отправленными из такого субдомена.

Следующим шагом валидации является проверка, согласован ли домен заголовка From: с SPF-идентификатором сообщения. Результатом валидации SPF может быть одно из следующих значений: *None, Neutral, Pass, Fail, Softfail, Temperror* или *Permerror*. Для согласования в рамках DMARC допустим только результат *Pass*.

Запись политики DMARC может требовать строгого согласования SPF. Это означает, что домен **From:** и SPF-идентификатор должны быть одинаковыми. Или она может требовать нестрогого согласования SPF - в таком случае они лишь должны быть в одном организационном домене. В рамках предыдущего примера, если доменом **From:** является **marketing.mybiz.example**, то для нестрогого согласования SPF достаточно SPF-идентификатора **mail.mybiz.example** или просто **mybiz.example**. По умолчанию используется нестрогое согласование.

Затем механизм валидации проверяет согласование DKIM. Для каждой действительной подписи DKIM сообщения он сравнивает домен **From:** с доменом **d=** подписи. Запись политики может задавать строгое или нестрогое согласование DKIM, которое требует точного совпадения доменов или существования в одном и том же организационном домене соответственно. Если согласована хотя бы одна действительная подпись DKIM, то сообщение считается DKIM-согласованным. Если сообщение согласовано либо в рамках процедуры SPF, либо DKIM, то оно считается согласованным в рамках DMARC.

Если сообщение согласовано, то на этом всё и заканчивается, за исключением, возможно, сохранения некоторых статистических данных для последующих отчётов. Если же оно не согласовано, то ситуация потенциально является гораздо более сложной, если система получателя решит следовать рекомендации политики, что в настоящее время и делает большинство почтовых систем (по крайней мере, по объему обрабатываемой почты).

Запись политики может содержать следующие рекомендации: **none**, **quarantine** или **reject**. Кроме того, она может задавать опциональное процентное значение, определяющее, как часто следует применять политику. Рекомендация **none** означает, что получатель вправе делать с сообщением всё, что угодно. Рекомендация **quarantine** означает, что с сообщением следует обращаться с повышенным скептицизмом, возможно, поместив его в папку спама или пометив как подозрительное. Рекомендация **reject** означает, что получателя просят отклонить сообщение в конце сеанса SMTP и не обрабатывать его дальше. Если процентная доля задана меньше, чем 100, то рекомендация заключается в том, чтобы поступить с указанным процентом несогласованной почты из домена согласно значению рекомендации, а с остальной частью обращаться на один шаг менее сурово. Например, если была рекомендация reject, а процент указан как 25, то четверть несогласованной почты будет отклонена, а оставшиеся три четверти помещены в карантин. (Процент не имеет никакого значения, если политика не задана.)

Как уже отмечалось выше, процентная доля указывается для того, чтобы позволить владельцам доменов постепенно реализовывать политики, посмотреть на результаты и ограничить ущерб от неправильного конфигурирования.

Отчёты DMARC

DMARC включает в себя два мощных средства для создания отчётов. Домен может запросить ежедневные агрегированные отчеты о том, какие IP-адреса отправляли почту с этим доменом в заголовке **From:** с подробными данными о согласовании DMARC, а также о валидации DKIM и SPF. Агрегированные отчеты отправляют многие крупные почтовые системы, включая Google, Yahoo/AOL, Comcast и Fastmail.

Кроме того, существует возможность запросить копии сообщений, которые не прошли валидацию DMARC, однако по причинам, связанным с защитой личных данных, лишь немногие системы это делают. LinkedIn является единственной крупной почтовой системой США, которая отправляет отчеты об ошибках.

Эти отчеты очень полезны и интересны даже для сайтов, которые не планируют публиковать политику DMARC. С их помощью можно узнать, куда на самом деле идёт ваша почта и кто ещё отправляет сообщения, заявляя, что они от вас.

Для того, чтобы можно было запрашивать каждый тип отчета, запись политики домена включает в себя метку со списком URI mailto (URI - унифицированный идентификатор ресурса), каждый с опциональным лимитом для максимального размера отчёта, который способна обработать система. По умолчанию интервал отправки агрегированных отчетов равен одному дню.

Агрегированные отчеты представляют собой XML-файл, сжатый с помощью gzip или ZIP, который прикреплён к сообщению электронной почты. Этот XML-файл включает в себя раздел («запись») для каждого отправляющего IP-адреса с подразделами («строка») для каждой комбинации результатов аутентификации. Например, ниже приводится раздел отчёта, описывающий полученную от двух IP-адресов почту, который Google отправил в мою систему *Smail*:

```
<record> <row>
<source_ip>2001:470:1f07:1126:0:43:6f73:7461</source_ip>
<count>1</count>
<policy_evaluated> <disposition>none</disposition>
<dkim>pass</dkim> <spf>pass</spf>
</policy_evaluated> </row>
<identifiers> <header_from>taugh.com</header_from>
</identifiers> <auth_results>
<dkim> <domain>iecc.com</domain> <result>pass</result>
<selector>k1912</selector>
```



```
</dkim> <dkim>
<domain>taugh.com</domain> <result>pass</result>
<selector>k1912</selector>
</dkim> <spf>
<domain>taugh.com</domain> <result>pass</result>
</spf> </auth_results>
</record>
<record> <row>
<source_ip>209.85.220.55</source_ip> <count>4</count>
<policy_evaluated> <disposition>none</disposition>
<dkim>fail</dkim> <spf>fail</spf>
</policy_evaluated> </row>
<identifiers> <header_from>taugh.com</header_from>
</identifiers> <auth_results>
<dkim> <domain>googlegroups.com</domain>
<result>pass</result> <selector>20161025</selector>
</dkim> <spf>
<domain>googlegroups.com</domain> <result>pass</result>
</spf> </auth_results>
</record>
```

Первая запись для адреса IPv6 сообщает об отправленном с моего почтового сервера сообщении. У этого сообщения одна действительная подпись SPF и две действительные подписи DKIM: одна с доменом заголовка **From:** и одна для домена сервера. Это значит, что сообщение согласовано согласно DMARC. Вторая запись описывает четыре сообщения с действительными подписями SPF и DKIM, однако домены SPF и DKIM не совпадают с заголовком **From:**, поэтому они не считаются согласованными согласно DMARC. Поскольку у второй группы сообщений в качестве идентификаторов аутентификации используется **googlegroups.com**, они, скорее всего, представляют собой то же самое, упомянутое выше сообщение, которое было изменено и заново отправлено в список рассылки Google Groups. [Поскольку я знаю, что в этот день отправлял только одно сообщение в данный список, это позволяет мне узнать количество подписчиков Gmail в списке. Мне приходилось видеть аналогичные утечки и более крупных списков, например, список, ведущийся группой NANOG (*North American Network Operators' Group*).]

Более крупные почтовые системы получают отчёты с большим количеством сообщений и разделов. Эти отчёты предназначены для автоматической обработки. В настоящее время доступны программы с открытым исходным кодом, которые анализируют такие отчёты и записывают сводную информацию в базу данных[10]. Однако чаще эти отчёты напрямую отправляют в такие специализированные службы, как *Dmarcian*[11] или *Agari*[12], которые предлагают условно-бесплатные сервисы по анализу отчетов: бесплатный простой анализ, а также более сложный анализ и рекомендации по исправлению ситуации за плату.

Ещё одним типом отчётов является отчёт об ошибках. В случае, если поступает сообщение с адресом домена в заголовке **From:** и оно не проходит валидацию DMARC, система-получатель может (но обычно она так не делает) отправить обратно отчёт об ошибках. Такой отчёт представляет собой многосекционное сообщение электронной почты, содержащее раздел со структурированным отчётом и полную или частичную копию неисправного сообщения.

Ниже приводится типичный раздел такого отчёта:

```
Feedback-Type: auth-failure User-Agent: Lua/1.0 Version: 1.0
Original-Mail-From: nanog-bounces@nanog.org Original-
Rcpt-To: xxx@linkedin.com
Arrival-Date: Thu, 26 Dec 2019 19:22:54 +0000 Message-ID:
<20191226191849.6BBF111BA67D@ary.qy>
Authentication-Results: dmarc=fail (p=none; dis=none)
header.from=iecc.com
Source-IP: 50.31.151.76
Delivery-Result: delivered
Auth-Failure: dmarc
Reported-Domain: iecc.com
```

Сообщение в отчёте об ошибках могло быть легитимным, но оно либо было несогласованным на момент отправки, либо было изменено в процессе доставки и, таким образом, стало несогласованным. Либо оно могло оказаться мошенническим – попытка фишинга или просто случайный спам, для которого спамовое ПО выбрало ваш домен с целью подделки обратного адреса. Что касается этого конкретного отчёта, то очевидно, что реальное сообщение ретранслировалось через список рассылки NANOG.

Исходный отчёт об ошибках включал полный адрес получателя. Это означает, что просмотрев отчёты об ошибках, любой пользователь, размещающий сообщения на NANOG, может увидеть тех, кто подписан на LinkedIn. Возможность такой утечки данных объясняет, почему большинство сайтов вообще не отправляют отчёты об ошибках, а большая часть из тех, которые это делают, ограничивают отправляемую информацию, обычно включая только заголовки недоставленных сообщений и удаляя адресные данные получателей.

Использование отчётов DMARC для публикации политик

Перед тем, как публиковать политику DMARC с использованием **quarantine** или **reject**, операторы доменов должны убедиться в том, что почти вся отправляемая ими почта (максимально близкая к 100% доля) согласована в рамках DMARC. Если SPF-записи домена не охватывают все IP-адреса, посылающие легитимную почту, то это может привести к отправке несогласованных сообщений, которые не смогут пройти валидацию SPF. У некоторых исходящих почтовых агентов MTA (*Mail Transfer Agent*) могут быть некорректно настроены параметры DKIM (или совсем не настроены), что приведёт к отсутствию согласованной подписи DKIM. В крупных компаниях часто могут возникать ситуации, когда агенты MTA отправляют почту, о которой не знали диспетчеры сети - например, если подразделение настроило собственный локальный сервер или заключило контракт со сторонней системой отправки почты.

Данные, полученные из отчётов DMARC, показывают оператору IP-адреса, которые отправляют несогласованную

почту, и, как правило, позволяют легко определить причину такого несогласования. Меры по исправлению ситуации могут включать обновление SPF-записей домена для добавления отсутствующих агентов MTA, исправление конфигурации подписания DKIM в агентах MTA либо принудительную реализацию правил в отношении несанкционированных почтовых серверов или сторонних отправителей почты. (Многие сторонние исполнители могут осуществлять подписание DKIM с использованием домена клиента, однако для этого нужно обеспечить либо совместное использование секретных ключей подписи, либо делегирование субдерева DNS, которым этот исполнитель сможет управлять.)

После того, как оператор установит достаточно эффективный контроль за своей почтой, он может постепенно включать политики отправки почты. В качестве промежуточного шага между отсутствием политики и политикой отклонения (сообщений) DMARC предлагает политику карантина, которая даёт получателям шанс восстановить ошибочно отнесённую к неправильной категории почту. Кроме того, в записи политики можно использовать параметр процентной доли, который позволяет постепенно реализовывать политики и ограничить ущерб при возникновении ошибок.

DMARC против списков рассылки

Первоначально DMARC предназначался для доменов в таких компаниях/организациях как банки, которые в основном отправляют почту в рамках отношений B2B и B2C, и почти не использовался в обычной электронной почте «от человека человеку». В тех случаях, когда компания обдумывает, когда публиковать политику DMARC и какую именно политику публиковать, необходимо учитывать, что часть легитимной почты поступит в несогласованном состоянии из-за промежуточной обработки, которую нельзя описать с помощью DMARC. Поскольку, как предполагается, компания знает, какую почту отправляет, она может сопоставить преимущества снижения угрозы фишинга со стоимостью потерянной почты и принять разумное для себя решение.

В 2014 году AOL и Yahoo – две крупные почтовые системы, обслуживающие индивидуальных потребителей, – были взломаны в ходе несвязанных между собой инцидентов, которые привели к тому, что злоумышленники украли данные миллионов пользователей из их адресных книг. Украденные данные были очень быстро проданы спамерам, которые использовали их для отправки спама пользователям AOL и Yahoo как будто бы от имени друзей. Всё это создало огромную проблему для служб поддержки AOL и Yahoo, так как пользователи жаловались на спам и спрашивали, почему друзья заваливают их спамом. Сначала AOL, а затем и Yahoo «решили» эту проблему, стремительно опубликовав политики DMARC **p=reject**, которые инструктировали каждую почтовую систему, реализующую DMARC, отклонять любые сообщения электронной почты AOL или Yahoo, не поступающие непосредственно от AOL или Yahoo. Это решение сильно отличалось от описанных ранее действий других компаний. В данном случае целью политики было снижение ущерба от эксплуатационного сбоя; это не приносило почти никаких выгод большинству пользователей и одновременно создавало большие проблемы для пользователей дискуссионных списков.

В любой почтовой системе, предназначенной для индивидуальных потребителей, существует небольшая, но важная часть пользовательской почты, которая является несогласованной, но в то же время легитимной и востребованной получателями. Это часто происходит из-за того, что маршрутизация почты осуществляется не напрямую от отправителя конечным получателям. Особым камнем преткновения остаются дискуссионные списки электронной почты, обычные действия диспетчеров которых превращают большую часть почты в несогласованные сообщения. Такая ситуация может привести к неполучению почты, отправленной подписчикам почтовых систем, которые распространяют политики DMARC на входящие сообщения. Кроме того, это может привести к удалению подписчиков из списков из-за ошибок отправки, вызванных отказами DMARC. (Согласно сведениям, полученным от одного из инсайдеров, Yahoo знала о проблемах со списками рассылки, но всё равно решила опубликовать политику **p=reject**.) Ещё одним источником несогласованной почты являются сторонние почтовые сервисы. Небольшая организация, например, спортивный клуб или отряд скаутов, часто использует список извещений, где обратным адресом для уведомления является персональный адрес секретаря организации, который, возможно, зарегистрирован в почтовых системах AOL или Yahoo.

Для того, чтобы решить проблемы, которые DMARC создаёт для списков рассылки, был предложен целый ряд обходных путей. Но ни один из них не оказался вполне успешным. Первоначально самый простой подход заключался в том, чтобы попросить пользователей, отправляющих почту с адресов, подпадающих под действие политик DMARC, подписаться на списки с других адресов. Этот подход перестал приносить пользу, когда AOL и Yahoo щёлкнули переключателем.

С тех пор программное обеспечение, управляющее списками рассылки, применяло самые разные подходы для того, чтобы обеспечить согласование сообщений, отправляемых такими списками. В некоторых случаях списки пробовали выключать все функции, которые изменяют сообщения способами, делающими недействительными подписи DKIM, надеясь, что в результате подписи DKIM останутся действительными при переадресации из списка. Этот метод показал не очень хорошие результаты – в том числе потому, что переадресованные сообщения не были согласованы в рамках SPF (список использует собственный адрес «конверта» для управления возвратами), а пользователям нужны вносимые списками изменения, например, добавление меток строки темы для идентификации списка.

Списки рассылки остановились на двух общих подходах противодействия DMARC[13]. Наиболее распространённый заключается в том, чтобы вставлять адрес списка в заголовок **From:**. Это позволяет списку добавлять подпись DKIM со своим собственным доменом и обеспечивать DMARC-согласование сообщения. Например, если входящее сообщение включало:

From: Steve C <steve@aol.com>
To: nodule@lists.example.com

Список может переписать это как:

From: Steve C via the nodule list <nodule@lists.example.com>
To: somelist@lists.example.com
Reply-To: Steve <steve@aol.com>

Переписанный заголовок **From:** обычно включает комментарий к адресу автора и имя списка. Фактический адрес автора добавляется в заголовок **Reply-To:** либо иногда в заголовок **Cc:**. Такой подход позволяет реализовать согласование DMARC, поскольку список может добавить DKIM-подпись **lists.example.com**, но затрудняет обработку отправляемой почты из списка. Почтовые агенты пользователя обрабатывают заголовок **Reply-To:** по-разному, что приводит к путанице относительно того, отвечает ли кто-то автору сообщения, списку или обоим. Добавляя ещё больше беспорядка к этой путанице, некоторые списки переписывают заголовки для сообщений только в тех доменах автора, которые публикуют политику DMARC. А это приводит к тому, что сообщения из одного и того же списка имеют разные заголовки.

Другой подход заключается в том, чтобы переписать заголовок **From:** с заменой проблемного адреса автора на другой адрес, который согласован в рамках DMARC, но, тем не менее, представляет автора. Например, мои списки рассылки переписали бы заголовки предыдущего примера так, чтобы изменить адрес автора лишь посредством добавления суффикса локального домена:

From: Steve C <steve@aol.com.dmarc.fail>
To: nodule@lists.example.com

dmarc.fail представляет собой реальный домен, зарегистрированный мною. (Он был доступен.) Я публикую запись MX record для ***.dmarc.fail** для того, чтобы получать любую почту, отправленную на переписанные адреса. Переписанное сообщение, как и письма, отправленные списками рассылки, имеет DKIM-подпись **dmarc.fail** и поэтому оно корректно согласовано в рамках DMARC. При переписывании адреса программой управления списком она создаёт для переписанного адреса переадресовочную запись, которая перенаправляет на исходный адрес. Через несколько дней переадресовочные записи удаляются - для того, чтобы ответы, отправленные вскоре после исходного письма, поступили автору, однако переадресация весьма ограничена и поэтому не очень полезна для передачи стороннего спама.

Этот метод работает относительно хорошо. Поскольку меняется только заголовок **From:**, это не оказывает никакого воздействия на **Reply-To:** или другое поведение почты, но при этом легко распознаётся идентификатор автора. Прочие системы реализовали ту же идею - возможно, в менее пассивно-агрессивной манере. Рабочие списки рассылки IETF переписывают адрес в локальную часть (адреса электронной почты), например:

From: Steve C <steve=40aol.com@lists.ietf.org>

Коммерческий сервис списков рассылки LISTSERV переписывает адрес в непрозрачный локальный адрес, а настоящий адрес помещает в заголовок **Reply-To:**

From: Steve C <ooooooo6b01fa96f-dmarc-request@lists.example.com>
Reply-To: Steve C <steve@aol.com>, Nodule list <nodule@lists.example.com>

Основной недостаток переписывания адресов заключается в том, что для управления набором временных пересыльных адресов требуется доступ к локальной почтовой системе списка. Весь этот процесс невозможно реализовать только внутри ПО для управления списками.

Ещё один подход к преодолению недостатков DMARC, используемый некоторыми списками, состоит в «обёртывании» сообщения путём вкладывания его в виде MIME-элемента внутрь внешнего сообщения от списка. В большинстве списков рассылки имеется опция MIME-сжатия, позволяющая отправлять однодневные сообщения в виде набора MIME-элементов внутри отдельного ежедневного сообщения. Фактически этот процесс превращает каждое письмо в состоящий из одного сообщения дайджест. Обычно адрес списка помещается в заголовок **From:** внешнего сообщения, при этом внутреннее письмо остаётся неизменным.

Чисто технически этот подход должен работать хорошо, поскольку в нём используется существующие, давно унифицированные функции электронной почты согласно RFC 5322. Для того, чтобы это проверить, я провёл несколько экспериментов, но результаты оказались очень плохими, так как почтовые агенты пользователя обрабатывают прикреплённые MIME-сообщения как нечто второстепенное. И хотя внутреннее письмо обычно отображается разборчиво, во многих случаях на него невозможно ответить без выполнения дополнительных громоздких шагов, а иногда это не удаётся вовсе. При этом обработка составных сообщений или писем с вложениями не отличалась последовательностью. Группа IETF провела эксперименты с несколькими типами MIME-оболочек и решила, что переписывание заголовка **From:** является лучшим выбором из всех плохих вариантов.

Хотя все эти методы и позволяют спискам рассылки отправлять согласованные с DMARC письма, ни один из них не работает настолько хорошо, чтобы списки могли вернуться в ситуацию до внедрения DMARC.

ARC

Несмотря на то, что объём почты, который крупные провайдеры получают через списки рассылки, весьма невелик – где-то около 1-2% от количества не относящихся к спаму сообщений, пользователи сильно заинтересованы в её получении. После ряда лет, в течение которых они получали многочисленные жалобы, несколько крупных провайдеров услуг электронной почты разработали механизм аутентификации *Authenticated Received Chain* (ARC), который помогает им обрабатывать желаемую, но не согласованную пользовательскую почту.

Очевидным способом обращения с несогласованной почтой из списков рассылки является внесение её в белый список. Крупные почтовые системы очень хорошо знают, где находятся такие списки (во всем мире количество хостов списков рассылки скорее всего составляет примерно 10 000), поэтому они могут просто, без всяких условий принимать почту из таких списков, зная, что она нужна их пользователям. Однако при таком подходе возникает другая проблема – списки рассылки не очень хорошо отсортировывают спам, что приводит к постоянным «протечкам» спама через них.

В частности, перед переадресацией сообщения большинство таких списков проверяет только то, что адрес в заголовке **From:** подписан на список. Если аккаунт подписчика окажется взломан и начнёт отправлять спам, любое отправленное в список сообщение, как правило, будет переадресовано. Даже если аккаунт не будет взломан, но в украденной адресной книге окажется ваш адрес и адрес списка, на который вы подписаны, то спамовое ПО способно подделать письмо от вас в список, и это опять приведёт к тому, что список выполнит переадресацию. Я наблюдал такую ситуацию много раз. При этом возникает чувство сильной фрустрации, поскольку пользователь, чей адрес подделан, не может ничего предпринять.

Целью механизма ARC является добавление к сообщению «цепи опеки», которая показывает, что с ним происходило при каждой переадресации. Этот метод позволяет конечной принимающей системе задним числом принимать решения по фильтрации спама на основе того, что случилось с сообщением в переадресующих системах.

ARC работает на базе существующей технологии электронной почты. Он адаптирует заголовок *Authentication-Results* (A-R)[14], который многие почтовые системы вставляют во входящее письмо для записи статуса аутентификации сообщения на момент его получения агентом MTA. Ниже приводится типичный заголовок A-R, который мой почтовый агент MTA вставил во входящее сообщение, поступившее от принадлежащего Apple сайта **me.com**:

Authentication-Results: iecc.com; spf=pass spf.mailfrom=xxx@me.com spf.helo=mr85pooim-hyfv06011401.me.com smtp.remote-ip="17.58.23.191"; dkim=pass header.d=me.com header.s=1a1hai header.a=rsa-sha256; dmarc=pass header.from=me.com (p=quarantine, pct=100)

В первом поле записано имя системы, добавившей заголовок, после чего следуют группы результатов аутентификации - в данном примере для SPF, DKIM и DMARC. Каждая группа включает результат и релевантные пункты, например, конверт **MAIL FROM** и отправляющий IP-адрес для SPF. Все поля являются опциональными, за исключением имени системы; они добавляются только для тех типов аутентификации, которые проверила система. ARC объединяет модифицированный заголовок A-R и два заголовка DKIM-подобных подписей в «*пломбу*» ARC, которая предназначена для описания прохождения сообщения через такую систему, как, например, диспетчер списков рассылки. У отдельного сообщения может быть несколько пломб ARC, если оно прошло через ряд переадресующих систем.

Каждой пломбе присваивается номер, начиная с 1 для той, которая добавлена первой. Каждый заголовок в пломбе ARC имеет пункт **i=**, который указывает, частью какой пломбы он является.

Ниже приводится пример заголовков в пломбе ARC:

ARC-Message-Signature: i=1; a=rsa-sha256; d=microsoft.com; s=abcd; h=From:Date:... ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=pass ...; dkim=pass ...

ARC-Seal: i=1; a=rsa-sha256; s=abcd; d=microsoft.com; cv=none; b=j7M/jt9eVP...

Подпись *ARC-Message-Signature* (AMS) почти идентична подписи DKIM, но с добавлением поля **i=**. Она предназначена для покрытия обычных заголовков и тела сообщения на момент его отправки из подписывающей системы. Если система внесла изменения в сообщение, то AMS применяется после таких изменений. При получении сообщения будет действительной самая последняя подпись AMS - за исключением ситуации, когда промежуточная система модифицировала сообщение после применения пломбы ARC, но не добавила собственную пломбу.

Заголовок *ARC-Authentication-Results* (AAR) сообщает статус аутентификации на момент получения сообщения «пломбирующей» системой, т.е. до того, как любые изменения были отражены в AMS.

Заголовок ARC-Seal представляет собой DKIM-подобную подпись, которая охватывает только три заголовка пломбы ARC, обеспечивая валидацию самой пломбы. Кроме того, она показывает, оставалась ли нетронутой цепочка пломб ARC при пломбировании сообщения, используя для этого поле **cv=** (значение цепочки). Если пломба является самой первой, то значение цепочки равно «none», поскольку предыдущая пломба отсутствует. Для любой последующей пломбы значение цепочки равно «pass», если предыдущая пломбы была действительной (успешная валидация DKIM-подобных подписей), а у предыдущей пломбы было **cv=none** или **cv=pass**. В противном случае значение цепочки равно «fail».

Если почтовая система получает сообщение с действительной цепочкой ARC от заслуживающего доверия источника, она может использовать информацию пломб ARC для внесения исключений в свою политику DMARC. В качестве простого примера давайте представим, что поступает сообщение, несогласованное в рамках DMARC, но имеющее действительную цепочку пломб ARC. В одной из пломб заголовок AAR показывает, что сообщение было согласовано в рамках DMARC (**dmarc=pass**), а домен **header.from** был тем же, что имеется в настоящее время в сообщении. Это означает, что рассогласование произошло из-за изменений, внесённых переадресующей системой. Если эта переадресующая система считается заслуживающей доверия (например, это хост дискуссионных списков), то получающая система может принять решение о доставке сообщения. При этом возможен более сложный анализ, однако я ожидаю, что подобный тип анализа с поиском типичных операций списка рассылки будет наиболее распространённым. Поскольку вредоносные системы способны добавлять поддельные пломбы ARC, этот анализ имеет смысл только для почты, поступающей из заслуживающих доверия источников. Для почтовых систем, которые слишком малы для сбора надёжных данных об отправляющих им почту хостах, идентификация достаточно достоверных источников, к которым можно применить исключения ARC, вероятно станет проблемой. В настоящее время предпринимаются усилия по созданию разделяемых списков заслуживающих доверия хостов (для списков рассылки), которые, возможно, окажутся достаточно плодотворными, поскольку количество активных хостов списков невелико и изменяется довольно медленно.

К настоящему времени внедрение ARC уже началось, но этот механизм ещё не является достаточно распространённым, чтобы списки рассылки прекратили направленную против DMARC «порчу» заголовков. Библиотеки *Python* и *Perl* для DKIM уже добавили поддержку ARC[15]. Диспетчер списков рассылки Sympa 6.2 поддерживает ARC, как и GNU Mailman 3.1 (но не версии Mailman 2.x).

Крупные почтовые системы, включая *Gmail* от Google и **outlook.com** от Microsoft, обеспечивают некоторую поддержку ARC. Как *Gmail*, так и **outlook.com** ставят пломбы ARC на пересылаемую почту и почту от списков рассылки, но еще не используют их для фильтрации сообщений, за исключением экспериментальных целей. Лишь несколько списков рассылки уже добавили пломбы ARC, частично по причине отсутствия поддержки ARC в ПО управления списками, которым они в настоящее время пользуются, и частично из-за того, что диспетчеры списков не знают об ARC.

Выводы

Спецификация DMARC начиналась как относительно простой метод предотвращения фишинга, который взяли на вооружение известные коммерческие домены - например, домены банков и поставщиков платёжных услуг. Затем потребительские почтовые системы AOL и Yahoo переориентировали этот метод на борьбу со спамом, который подделывал адреса их пользователей. Хотя такое перепрофилирование в основном и решило проблему спамового подлога для этих систем, оно также нанесло значительный сопутствующий ущерб спискам рассылки электронной почты. Несмотря на то, что многие списки пытались найти пути для обхода проблем DMARC, все эти методы имели изъяны, которые в конечном итоге приводили к неудовлетворительному результату. Для того, чтобы справиться с недостатками DMARC, группа крупных провайдеров электронной почты изобрела механизм аутентификации ARC, который позволяет в каком-то смысле изучить историю сообщения и узнать, каким образом не согласованное в рамках DMARC сообщение приобрело такой статус.

Продолжающееся развитие DMARC, списков рассылки и ARC представляет собой очередной раунд эволюции мер защиты с порой неожиданными последствиями. Если повезёт, то ARC окажется конечным пунктом этой последовательности, состоящей из результата, побочного эффекта и нейтрализующего эффекта, но мы этого не узнаем до тех пор, пока ARC не получит более широкое распространение. Возможно, это произойдёт в течение ближайших нескольких лет.

Список источников и дополнительная литература

1. *Dave Crocker, «Challenges in Anti-Spam Efforts», The Internet Protocol Journal, Volume 8, No. 4, December 2005.*

2. *John Klensin, «Another Look at Spam», The Internet Protocol Journal, Volume 8, No. 4, December 2005.*

3. *Murray Kucherawy and Elizabeth Zwicky, Eds., «Domain-based Message Authentication, Reporting, and Conformance (DMARC)», RFC 7489, March 2015.*

4. *Peter W. Resnick, «Internet Message Format», RFC 5322, October 2008.*

5. *Scott Kitterman, «Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1», RFC 7208, April 2014.*

6. *Murray Kucherawy, David Crocker, and Tony Hansen, «DomainKeys Identified Mail (DKIM) Signatures», RFC 6376, September 2011.*

7. *John C. Klensin, «Simple Mail Transfer Protocol», RFC 5321, October 2008.*

8. *John Levine, Mark Delany, Eric Allman, and Jim Fenton, «DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)», RFC 5617, August 2009.*

9. *See* https://publicsuffix.org/for the PSL, and https:// wiki.mozilla.org/Public_Suffix_Listfor *a description of its use and history.*

10. *See* https://www.taugh.com/rddmarc/

11. *Dmarcian:* www.dmarcian.com

12. *Agari:* www.agari.com

13. *Mailman and DMARC,* https://wiki.list.org/DEV/DMARC

14. *Murray Kucherawy, «Message Header Field for Indicating Message Authentication Status», RFC 8601, May 2019.*

15. *See* https://pypi.org/project/dkimpy/ *for the Python library, and* https://metacpan.org/release/Mail-DKIM *for the Perl library.*

Источник: Internet Protocol Journal, Vol. 23, N 1, https://ipj.dreamhosters.com/wp-content/uploads/2020/07/231-ipj.pdf

Аллюзии 2020 к теории «чёрных лебедей» телекома

Елена Воронина, Мадина Касенова

В ряду событий не только текущего 2020 года, но и последних десятилетий XXI века отнюдь не будет преувеличением выделить беспрецедентную ситуацию пандемии COVID-19, которая, в том числе, привела к существенному ограничению возможностей перемещения значительного числа лиц на внутригосударственном и межгосударственном уровнях, потребовала фиксации установления местонахождения лиц, включая их социальные контакты и т.д. Ситуация пандемии COVID-19 объективировала масштабный рост использования интернет-технологий, предъявила новые требования к скорости и качеству связи при передаче данных, бесперебойности работы интернет-приложений. Технологическая инфраструктура Интернета выдержала такого рода «испытание», одновременно высветив необходимость принятия комплекса дальнейших мер, с одной стороны, в плане эффективности поддержания ее устойчивости и безопасности, с другой стороны, оптимизации сетевой инфраструктуры, принципов маршрутизации, пиринговой политики, а также активизации развертывания и развития широкополосных сетей поколения 5G. Нынешний этап сдерживания каскадного распространения COVID-19 лишь актуализирует потребности реализации повестки обозначенных мер.

В рамках настоящей статьи представляется важным обратить внимание на два фактора, рельефно обозначившихся в 2020 году, катализатором которых во многом стала пандемия COVID-19. Первый имеет отношение к обеспечению функциональности сетей связи, их устойчивости и безопасности, когда при масштабном росте интернет-трафика возникла необходимость решения проблем предельных показателей загрузки их емкости. Второй связан с политико-правовыми изменениями подходов США, обусловленными диверсификацией защиты телекоммуникационной и технологической инфраструктуры. Игнорировать эти факторы едва ли стоит, поскольку они во многом определят акценты развития технологической инфраструктуры передачи данных, включая трансграничный формат их передачи.

I. Целый ряд аналитических показателей свидетельствует, что более полутора миллиардов человек в мире работают и учатся в режиме онлайн, множество бизнес-процессов реализуются в этом же режиме, равно как и осуществляются важнейшие международные контакты государств, международных организаций. Так, по данным Организации экономического сотрудничества и развития (Организация OECD)[1] онлайн-формат охватывает около 1,3 миллиарда граждан государств, входящих в эту организацию[2]. Обобщенные аналитические выкладки Организации OECD представляют несомненный интерес и основные из них целесообразно привести.

Значительный всплеск интернет-трафика и увеличение нагрузки на телекоммуникационные сети до 60% с начала пандемии COVID-19 отмечаются операторами фиксированной и мобильной широкополосной связи, а также поставщиками контента и облачных сервисов по всей коммуникационной цепочке Интернета, взаимодействие сетей которых обеспечивается посредством точек обмена трафиком Интернета (IXP).

Множество показателей свидетельствуют об изменении тенденций предыдущих периодов в зоне западноевропейских стран и, к примеру, британская транснациональная телекоммуникационная холдинговая компания BT Group plc[3], охватывающая более 150 стран и регионов, являющаяся крупнейшим поставщиком услуг фиксированной, широкополосной и мобильной связи в Великобритании, сообщает об увеличении использования фиксированной широкополосной связи в дневное время в будние дни с 35% до 60%. Испанская Telefónica отмечает увеличение нагрузки на сети почти на 40%, при росте мобильного трафика на 50% и голосового - на 25%. Итальянская компания Telecom Italia сообщает об увеличении трафика фиксированных сетей на 63%, а мобильной сети - на 36%. Французской Orange зафиксирован рост трафика ее международной инфраструктуры, значительная часть контента которой, генерируемая пользователями Франции, на 80% сосредоточена в США. Транснациональные телекоммуникационные компании США – Verizon и AT&T – сообщают как о масштабном увеличении трафика, так и о нагрузках на точки обмена трафиком. Показатели компании Verizon фиксируют увеличение интернет-трафика сетей VPN (Virtual Private Network) на 52% и трафика инструментов совместной работы - на 47%. Компания AT&T сообщает, что трафик ее базовой сети вырос на 23%, количество минут звонков через мобильную голосовую связь выросло на 33%, а по Wi-Fi - на 75%, при этом количество минут для абонентской телефонной связи выросло на 64% по фиксированным линиям. Увеличение интернет-трафика

фиксируют операторы, поставщики контента и облачных сервисов Азиатско-тихоокеанского региона, в частности, это демонстрируют показатели в 30-40% японской компании NTT Communications.

Точки обмена трафиком как один из ключевых элементов базовой инфраструктуры Интернета испытывают беспрецедентные нагрузки во всех регионах мира, начиная с начала второго квартала 2020 года, когда обострилась ситуация пандемии COVID-19. Организации, обеспечивающие работу точек обмена трафиком Интернета ведущих стран, отмечают устойчивую нагрузку интернет-трафика и увеличение до 60% общей пропускной способности, при том, что отдельные точки обмена трафиком достигали рекордов пикового трафика по сравнению с их базовыми уровнями до вспышки COVID-19. В Нидерландах пропускная способность увеличилась на 22,3% к началу второго квартала 2020 года. AMS-IX (Амстердам), LINX (Лондон) к апрелю 2020 года достигали максимального пика трафика. В Германии зафиксирован рост пропускной способности в 16,5% и в текущий период немецкая DE-CIX (Франкфурт), одна из крупнейших точек обмена трафиком в мире, обеспечивает пропуск данных со скоростью более 9 терабит в секунду (Тб/с). Трафик российской компании MSK-IX на начало марта 2020 составлял 3,5 Тб/с, а к середине марта – 4,39 Тб/с, что подтверждало его рост на 25% всего лишь за двухнедельный период. В связи с нагрузкой трафика INEX (Дублин) увеличил пропускную способность межкоммутаторных соединений на 100 Гбт/с, а доступную пропускную способность портов – до 4,2 Тб/с. Сравнительный анализ предыдущих показателей в точках обмена трафиком в Интернете и другие актуальные статистические данные и тенденции, существующие в настоящее время на рынке IXP, представили организации-IXP Японии, Чили, США, ЮАР, Бразилии и других стран[4], данные подтверждают общий тренд.

Из-за повышенного спроса несколько контент-провайдеров, такие как Netflix, Akamai и YouTube, изменили по умолчанию настройки потокового видео в пиковые часы в зоне Европы с высокой четкости на стандартную в целях обеспечения связанности в период пиковых нагрузок трафика. Компании Cisco, Webex, Facebook, Google, Zoom и др. отмечали наибольшее распространение применения облачных приложений для видеоконференцсвязи; с начала периода пандемии COVID-19 трафик видеоконференцсвязи увеличивался на 120%.

Архитектура национальных коммуникационных сетей различается не только в связи с разным временным периодом их создания, но также разным масштабом охвата сетей (городская густонаселенная инфраструктура, малонаселенные сельские местности, труднодоступные горные районы) и т.д. Несмотря на эти факторы, национальные коммуникационные сети развитых стран в целом приспосабливаются к изменениям, вызванным увеличением нагрузок на их пропускную способность, принимают меры для того, чтобы избегать перегрузок в пиковые периоды, своевременно реагируют на общий повышенный спрос передачи данных и одновременно поддерживают критически важные услуги, такие как телемедицина и экстренное реагирование. Ключевой инфраструктурный компонент интернета – система доменных имен (DNS) - имеет решающее значение для беспрепятственного доступа к различным службам Интернета, соответственно, операторы авторитетных серверов DNS, операторы национальных доменов верхнего уровня (ccTLD) не только учитывают увеличение нагрузки трафика, но и в приоритетном порядке обеспечивают доступность веб-сайтов служб экстренной помощи.

Справляться со значительным увеличением интернет-трафика, а также с тем, чтобы услуги подключения и связи работали надежно, стабильно и безопасно, помогает не только оптимизация работы самих сетевых операторов (операторов фиксированной и мобильной связи, поставщиков контента и проч.), не только расширение IXP (количество подключенных сторон, осуществляющих пиринговые соединения, обусловленные ростом объема базового пропуска передаваемого трафика), но также ответственные действия и помощь со стороны регулирующих органов и правительств государств в плане поддержки функционирования коммуникационных сетей, обеспечения их мощности в целях удовлетворения повышенного спроса, схем их использования и устранения сбоев при передаче данных. Например, в Швеции операторы сектора связи поддерживают активный диалог и предпринимают совместные меры со шведским регулирующим органом – Post and Telecom Authority (PTS)[5] – для выполнения своих критически важных операций при решении вопросов доступа к центрам обработки данных, кабельным соединениям, сотовым станциям и другим критически важным объектам инфраструктуры, несмотря на то, что принятие соответствующих законодательных оснований еще формально не закреплено и пока находится в процессе рассмотрения соответствующими органами власти.

Мониторинг производительности ключевых служб интернет-инфраструктуры подтверждает возрастание нагрузки на сети операторов мобильной связи и связывается с увеличением использования приложений по мобильным сетям, зачастую использующимся в качестве замены фиксированной широкополосной связи, что вызывает перегрузку полос пропуска, например, при потоковой передаче видеоконференций. В условиях масштабной и возрастающей нагрузки на сети операторов мобильной связи правительства и регулирующие органы ряда развитых государств, во-первых, высвобождают для операторов мобильной связи на временной основе дополнительный радиочастотный спектр для увеличения пропускной способности эфирного интерфейса в целях уменьшения перегрузки сетей подвижной связи, во-вторых, предоставляют неиспользуемый радиочастотный спектр посредством одобрения коммерческих сделок по использованию спектра между поставщиками, которые вводят такой неиспользуемый спектр в эксплуатацию. К примеру, в США AT&T, Version и T-Mobile получили одобрение регулирующего органа – Федеральной комиссии по связи (FCC)[6] - на заключение коммерческого соглашения с поставщиком спутникового телевидения Dish об эксплуатации неиспользуемого беспроводного спектра компании для увеличения пропускной способности для решения проблемы перегрузок, возникших в связи с ситуацией COVID-19. Кроме того, FCC предоставила интернет-операторам временный доступ к спектру в диапазоне 5,9 ГГц для удовлетворения растущего спроса на широкополосную связь в сельской местности и

предоставила использование спектра в течение 60 дней в диапазонах AWS-4 и AWS-3.

Крупные сетевые операторы, для минимизации перегрузок своих сетей и увеличения пропускной способности их трафика подключаются к нескольким точкам обмена трафиком, добавляя дополнительные порты либо увеличивая пропускную способность портов. (Хотя отдельные порты могут быть перегружены, точки обмена трафиком обычно используют лишь долю пропускной способности сети от теоретической емкости своей портовой емкости и межсетевых соединений). С учетом того, что Италия оказалась в числе стран, значительно пострадавших от пандемии COVID-19, Telecom Italia начиная с 6 апреля 2020 года предприняла меры по обеспечению пирингового соединения в нескольких точках обмена трафиком для улучшения работы сети.

Существует зависимость некоторых крупных сетевых операторов от частных межсетевых соединений, которые представляют собой волоконно-оптические перекрестные соединения в центрах обработки данных, между маршрутизаторами крупнейших сетей доступа и крупнейшими или наиболее важными сетями, предоставляющими услуги веб-сайтов, видеоконференции и т.д. Отсутствие прямых межсетевых соединений между крупными сетевыми операторами или перегрузка межсетевого соединения могут негативно влиять на сети. Иногда крупные операторы связи в некоторых странах идут по пути отказа от локального межсетевого соединения с другими сетями, вынуждая небольшие сети отправлять региональный трафик на большие расстояния в точки обмена трафиком в других странах и обратно, хотя это приводит к более высоким затратам и снижает качество и стабильность связи. К примеру, два крупных оператора в Канаде взаимодействуют друг с другом в точках обмена трафиком, находящихся в США, в результате чего 64% внутреннего трафика Канады проходит через границу США. При этом, несмотря на отсутствие прямого подключения, прямо и косвенно влияющего на общую доступность интернет-ресурсов для канадских пользователей, операторам Канады удается поддерживать стабильность интернет-трафика при передаче данных.

Обобщая изложенное и, воспользовавшись журналистским клише «вызовы и угрозы», можно констатировать, что технологическая основа Интернета, совместно эксплуатируемая поставщиками услуг и платформами, в условиях масштабного увеличения объема трафика и нагрузок на технологические сети по всей коммуникационной цепочке Интернета, взаимодействие сетей которых обеспечивается посредством точек обмена трафиком (IXP), с ними справилась и продемонстрировала функциональную устойчивость. Реальность кризиса пандемии COVID-19 и его текущее каскадное развитие, с одной стороны, лишний раз подтверждает критически важное значение Интернета как «сети сетей», обеспечивающей коммуникационное взаимодействие миллионов лиц; с другой стороны, с очевидностью высвечивает необходимость поддержки телекоммуникационных компаний со стороны регулирующих органов и правительств стран как в плане совместного решения проблем масштабного роста интернет-трафика и предельных показателей загрузки емкости сетей, вызванных кризисными явлениями, так и в плане необходимости их поддержки в развитии и совершенствовании сетей.

II.

Ситуация с COVID-19 во многом стала катализатором целого ряда процессов политико-правового характера, поскольку государства по-разному решали возникшие проблемы необходимости поддержания устойчивого функционирования и безопасности критически важной телекоммуникационной и технологической инфраструктуры, а также обеспечения защиты данных (персональных данных, данных геолокации лиц и объектов, неличных данных и т.д.), когда акселерация агрегирования данных приобрела значительный объем и масштаб. В этом плане нельзя не обратить внимание на меры, предпринятые правительством США, начиная с конца первого полугодия 2020 года, которые так или иначе повлияют на диверсификацию телекоммуникационной сферы и регулирование защиты данных. В частности, речь идет об инициативе «Чистый путь развития 5G» (*5G Clean Path Initiative*), объявленной администрацией президента США (29 апреля 2020), которая направлена на защиту критической телекоммуникационной и технологической инфраструктуры США. В начале августа 2020 это программа была расширена, получив название «Чистая Сеть» (*Clean Network*)[7]. В русле этой программы и для защиты конфиденциальности данных физических и юридических лиц США, включая американские органы и структуры государственной власти, от агрессивных действий правительства КНР и китайских компаний, президент США (6 августа 2020) издал два исполнительных приказа (*Executive Orders*): «О противодействии угрозе, возникающей в связи с TikTok» (исполнительный приказ о TikTok)[8] и «О противодействии угрозе, возникающей в связи с WeChat» (исполнительный приказ о WeChat)[9]. Представление о значении всех обозначенных документов даст их краткое содержание.

Clean Network представляет собой многоцелевую и комплексную программу, интегрирующую технологические решения инфраструктуры данных и интернет-приложений, и предусматривает пять сквозных сетевых компонентов: чистый оператор передачи данных (*clean carrier*), чистый магазин приложений (*clean store*), чистые приложения (*clean apps*), чистое облако (clean cloud), чистый кабель (*clean cable*). При этом Clean Network основана на технологически нейтральных стандартах цифрового доверия, разработанных и признанных на международном уровне, а конкретно, документе Центра стратегических и международных исследований (*Center for Strategic and International Studies, CSIS*)[10], Инструментальных средствах объективной оценки рисков кибербезопасности и соразмерных мерах по их минимизации, связанных с развертыванием мобильных сетей поколения 5G Европейского Союза (*European Union's 5G Toolbox*)[11] и Пражских предложениях, рекомендованных для 5G (*Prague Proposals 5G Recommendations*)[12]. На сегодняшний день более 30 ведущих операторов мобильной связи нескольких десятков государств поддержали 5G Clean Path, исключив использование компонентов китайских производителей и поставщиков оборудования для сетей 5G, что покрывает 52% мировой экономики[13].

В связи с тем, что диверсификация цепочек поставок должна защищать свободу, конфиденциальность и безопасность данных лиц, права человека и надежное сотрудничество в коммуникационных сетях, 5G Clean Path нацелена на то, чтобы все данные сетей 5G, входящие или исходящие из американских дипломатических систем и объектов, передавались только посредством надежного оборудования и средств, заслуживающих доверия, а не через оборудование сомнительных и ненадежных поставщиков, таких как Huawei и ZTE. Ограничение допуска ненадежных IT-поставщиков к американским дипломатическим и ведомственным системам, в частности, предполагает введение новых строгих требований к инновационным сетям, обеспечивающим связь между государственными учреждениями и органами США (как на территории США, так и за ее пределами), включая мобильный трафик сетей беспроводного Интернета поколения 5G, передающий данные таких американских систем[14]. США призвали заинтересованные страны и телекоммуникационные корпорации присоединиться к реализации механизмов 5G Clean Path и Clean Network, поскольку инфраструктура сетей, которые разворачиваются и управляются китайскими технологическими компаниями, а значит, контролируются китайским правительством, несет значительные риски для безопасности сетей и пользователей. Участие государств и корпораций в создании устойчивой международной коалиционной стратегии в отношении мер и механизмов, предусмотренных Clean Network, позволит ограничить деятельность китайских технологических компаний, вовлеченных в развертывание телекоммуникационных сетей поколения 5G, и исключить применение технических компонентов китайского производства в сетях 5G.

Clean Network представляет собой многоцелевую и комплексную программу, интегрирующую технологические решения инфраструктуры данных и интернет-приложений, и предусматривает пять сквозных сетевых компонентов: чистый оператор передачи данных (clean carrier), чистый магазин приложений (clean store), чистые приложения (clean apps), чистое облако (clean cloud), чистый кабель (clean cable).

Логическим развитием и поддержкой механизмов, предусмотренных Clean Network, стало принятие президентом США двух исполнительных приказов, упомянутых выше (исполнительный приказ о TikTok и исполнительный приказ о WeChat). Предварительно нельзя не сказать несколько слов о правовом значении самих исполнительных приказов президента США.

Во-первых, исполнительный приказ президента США – это письменный документ, изданный президентом, обладающий всей силой закона и устанавливающий обязательные к исполнению нормативные предписания и действия, которым руководствуются все ветви исполнительной власти (исполнительные органы, государственные должностные лица и лица, определяющие политику государства). Исполнительный приказ равен по своей силе законодательному акту, принятому Конгрессом США, но направлен на решение ключевых стратегических задач политико-правового характера в *конкретной сфере* отношений. В формально-юридическом плане исполнительный приказ подписывается президентом США, утверждается Административно-бюджетным управлением (*Office of Management and Budget*) и Генеральным прокурором (*US Attorney General*), официально публикуется и регистрируется в федеральном реестре.

Во-вторых, исполнительные приказы издаются президентом США в рамках его функциональной компетенции как главы исполнительной ветви власти, являются способом осуществления его официальных полномочий в обеспечении соблюдения законов США. Президент США издает исполнительные приказы без прохождения законодательных процедур. Вместе с тем, хотя исполнительный приказ обладает силой федерального закона, он обладает ограниченной правовой силой. Такого рода ограничения связаны с соответствующими полномочиями президента США, установленными Конституцией США[15], действующими законодательными актами; также исполнительный приказ может ограничиваться определенными законодательными актами Конгресса США. По общему правилу исполнительные приказы могут отменяться президентом США, принявшим такой приказ, следующим президентом, Конгрессом США и судом США. К примеру, Конгресс США вправе отменить действие исполнительного приказа, исключив его из финансирования, необходимого для его реализации. Между тем, отмена действия исполнительного приказа президента США является редкостью и, кроме того, существует возможность для президента, издавшего тот или иной приказ, наложить вето на соответствующее решение Конгресса. В реальных условиях деятельности Конгресса США получить большинство в две трети голосов, необходимое для преодоления президентского вето, достаточно сложно. Полномочия по отмене исполнительного приказа президента США принадлежат также судебной власти, однако такие полномочия преимущественно реализуются, когда существует прямое противоречие действующему федеральному законодательству или нарушаются гражданские права отдельных лиц или группы лиц.

Осуществляя свои исполнительные полномочия, президент США в августе 2020 года издал два исполнительных приказа в отношении мобильного приложения TikTok, принадлежащего китайской компании ByteDance Ltd, а также мобильного приложения WeChat, предназначенного для обмена сообщениями, социальных сетей и электронных платежей, которое принадлежит китайской компании Tencent Holdings Ltd. Президент США тем самым определил ключевые стратегические подходы политико-правового характера в *конкретной сфере* отношений, а именно в сфере безопасного использования интернет-услуг, защиты информационной инфраструктуры и коммуникационных технологий.

Оба рассматриваемых исполнительных приказа приняты в рамках предоставленной президенту США компетенции, согласно Конституции США, законов США, включая Акт о

международных чрезвычайных экономических полномочиях[16], Акт о национальных чрезвычайных ситуациях[17] и Свод законов США (раздел 301, Главы 3)[18], а также с изданным ранее президентом США исполнительным приказом № 13873 от 15 мая 2019 года «Защита безопасности цепочек поставок информационных и коммуникационных технологий и услуг»[19].

В рассматриваемых исполнительных приказах отмечается, что китайские мобильные приложения TikTok и WeChat автоматически собирают огромные массивы информации пользователей, предоставляя китайским компаниям и правительству КНР доступ к персональным данным лиц, конфиденциальной информации личного и служебного свойства, позволяя правительству КНР использовать механизмы слежки за пользователями, давая возможность подвергать цензуре чувствительный контент и осуществлять дезинформационную деятельность в интересах КНР. Например, сопоставительные исследования свидетельствуют, что наряду с данными и сообщениями китайских пользователей, мобильные приложения WeChat и TikTok содержат миллиарды данных и досье сообщений, отправленных пользователями США, Тайваня, Южной Кореи, Австралии, Индии и других стран, кроме того, посредством этих приложений китайские компании распространяют неподтвержденные теории о происхождении COVID-19, собирают данные о сетевой активности пользователей, включая информацию о местоположении лиц, их истории онлайн-просмотров и поиска.

В связи с очевидными рисками в плане защиты личной и служебной информации, персональных данных и, в целом, для поддержания своей национальной безопасности, ряд государств предпринимают меры, ограничивающие или запрещающие использование китайских приложений. Меры, установленные в исполнительных приказах, относящиеся к китайским мобильным приложениям TikTok и WeChat, непосредственно предназначены для противодействия реальным угрозам, возникающим для национальной безопасности, внешней политики и экономики США. Исполнительные приказы президента США о TikTok и WeChat имеют обязательную силу на федеральном уровне и предполагают к середине ноября 2020 года принятие соответствующих правил и положений, требующихся для их реализации.

Исполнительный приказ о TikTok предусматривает мероприятия, направленные против владельцев китайского мобильного приложения TikTok. В исполнительном приказе отмечается, что использование мобильного приложения TikTok (для обмена видео, проведения видеоконференций) несет угрозу национальной безопасности, поскольку позволяет осуществлять несанкционированный сбор личной и конфиденциальной информации американских пользователей и передавать данные на серверы, расположенные в КНР, что потенциально дает возможность Китаю отслеживать данные местонахождения федеральных служащих и подрядчиков, создавать досье лиц для шантажа и осуществления корпоративного шпионажа.

Исполнительный приказ предписывает, что американские компании и организации должны исключить применение и распространение в США мобильного приложения TikTok на своих устройствах. Для любых лиц США (как физических, так и юридических, относящихся как к частному сектору, так и государственному), а также в отношении любых лиц или имущества, подпадающего под юрисдикцию США, устанавливается запрет на осуществление всех сделок и трансакций с китайской компанией ByteDance Ltd (известной также как компания Zìjié Tiàodòng), включая ее дочерние компании и любые организации, в которых эта китайская компания имеет какой-либо интерес.

Исполнительный приказ о WeChat, равно как и в отношении приложения TikTok, предусматривает запрет на использование WeChat в США. Запрет использования мобильного приложения WeChat (принадлежит китайской компании Tencent Holdings Ltd, известной также как Téngxùn Kònggǔ Yǒuxiàn Gōngsī) относится ко всем трансакциям с китайской компанией Tencent Holdings Ltd, ее дочерним компаниям и любым организациям, связанных с ней, и касается любого лица США, а также лица или имущества, находящегося под юрисдикцией США. В связи с тем, что мобильное приложение WeChat предназначено не только для обмена сообщениями в социальных сетях, но и для электронных платежей, из-за возможности мгновенного перевода средств или других активов исполнительный приказ о WeChat не предусматривает предварительного уведомления соответствующих лиц о принятии мер запретительного характера в отношении лиц, нарушающих запреты, установленные в этом приказе.

Кратко рассмотренные документы правительства США (5G Clean Path и Clean Network, исполнительные приказы президента США о TikTok и WeChat), как представляется, дают основания для обобщенного тезиса о том, что триггер развития инфраструктуры сетей поколения 5G и передача данных контента смещается в направлении исключения технологических компонентов китайского производства, ограничения связности между сетями и облачными инфраструктурами «китайской принадлежности», что, в свою очередь, окажет влияние на диверсификацию регулирования телекоммуникационной инфраструктуры, формата использования интернет-приложений и защиты данных пользователей. Одновременно нельзя не заметить, в частности, неоднозначную оценку 5G Clean Path и Clean Network целым рядом стран, поскольку воплощение в жизнь такого рода решений может отразиться на перекраивании топологии связности, потерям производительности сетей, их стабильности и, в целом, повлиять на фрагментацию Интернета.

Ссылки

1. *Organization for Economic Co-operation and Development (OECD).* http://www.oecd.org/

2 *OECD Report* https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/, а также информация о докладе Организации OECD. https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/

3. *BT Group plc (ранее – British Telecom) в настоящее время действует под этим коммерческим обозначением (штаб-квартира – Лондон, Великобритания).*

4. В настоящее время European Association IX (Euro-IX, основанная в 2001 г. и объединяющая 71 точку обмена трафиком со всего мира) готовит свой ежегодный отчет 2019-2020. https://www. euro-ix.net/

5. *Swedish Post and Telecom Authority.* https://www.pts.se/en/about-pts/

6. Федеральная комиссия по связи (Federal Communication Commission, FCC) является федеральным органом правительства США, регулирующим сферу государственной и международной радиосвязи, телевидения, проводной, спутниковой и кабельной связи на территории США (во всех 50 штатах и Округе Колумбия), и отвечает за обеспечение реализации права США в области связи. https://www.fcc.gov/about/overview

7. *Clean Network Initiative.* https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/

8. *Executive Order on Addressing the Threat Posed by TikTok.* https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

9. *Executive Order on Addressing the Threat Posed by WeChat.* https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/

10. *Center for Strategic and International Studies, CSIS. Criteria for Security and Trust in Telecommunications Networks and Services CSIS Working Group on Trust and Security in 5G Networks.* https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200511_Lewis_5G_v3.pdf; *The Clean Network program.* https://www.state.gov/the-clean-network/

11. *European Union's 5G Toolbox.* https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

12. *Prague Proposals 5G recommendations.* https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf;

13. Речь идет, к примеру, о японских компаниях мобильных технологий (NTT, NEC, KDDI, SoftBank и Rakuten), французской компании Orange, индийской Jio, австралийской Telstra, южнокорейских SK и KT, компании Великобритании O2, хорватской Hrvatski Telekom, эстонской Tele2, ирландской Three, латвийской LMT, нидерландской Vodafone Ziggo, польской Plus, сингапурской Singtel, датской TDC, испанской Telefónica и др. Крупные канадские телекоммуникационные компании Bell, Telus и Rogers объявили об отказе от оборудования Huawei при строительстве канадских телекоммуникационные компании Канады решили сотрудничать с Ericsson, Nokia, Samsung, а не с китайской Huawei при строительстве канадских сетей 5G, равно как и Греция будет использовать Ericsson (вместо Huawei) для развития своей инфраструктуры сетей 5G. О таком же подходе объявили ряд компаний Испании, Бразилии, Германии и др. стран. https://www.forbes.com/sites/roslynlayton/2020/09/04/state-departments-5g-clean-network-club-gains-members-quickly/#6e61cb457536

14. В начале 2020 г. Федеральная комиссия по связи (FCC) отозвала лицензии у четырех китайских компаний и отклонила заявку China Mobile. Кроме того, инициирован запрет для американских операторов облачных сервисов 5G относительно предоставления данных таким китайским компаниям, как Alibaba, Baidu, Tencent. https://www.forbes.com/sites/roslynlayton/2020/09/04/state-departments-5g-clean-network-club-gains-members-quickly/#6e61cb457536

15. Статья II Конституции США наделяет президента исполнительной властью, дающей ему право контроля за различными аспектами осуществления исполнительной власти, возлагает на него ответственность за добросовестное исполнение законов США, что не позволяет ему действовать вне рамок закона; соответственно, противоречащие действующему закону решения президента признаются недействительными. Конституции зарубежных государств: Великобритания, Франция, Германия, Италия, Европейский Союз, Соединенные Штаты Америки, Япония. (8-е изд.) - М.: Инфотропик Медиа, 2012 С. 549 562 // СПС Консультант Плюс

16. *International Emergency Economic Powers Act, IEEPA.* https://www.law.cornell.edu/uscode/text/50/chapter-35

17. *National Emergencies Act.* https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter34&edition=prelim

18. *United States Code (section 301 of title 3).* https://www.law.cornell.edu/uscode/text/3/301

19. *Executive Order 13873 of May 15, 2019 «Securing the Information and Communications Technology and Services Supply Chain».* https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

Covid, DNS и геолокация

Павел Храмцов

Весь этот год принято говорить о влиянии пандемии Covid-19 на развитие тех или иных трендов Интернета. Речь идет как об увеличении трафика, так и об увеличении количества регистраций мошенниками доменов на около Covid-ные темы, об общем снижении темпов регистрации новых доменов из-за сокращения в экономике доли среднего и малого бизнеса и о многих других последствиях пандемии.

Отправленные на удаленную работу визионеры и прочие исследователи интернетов, выключенные из круговорота офлайн-конференций, стали уделять больше внимания исследованиям текущего состояния Сети. Это положительным образом сказалось на качестве проводимых исследований и прикладном значении полученных результатов. Конференции, на которых эти результаты докладывались, были переведены в онлайн. О некоторых из них мы сегодня и поговорим.

APTLD78 и вопросы безопасности

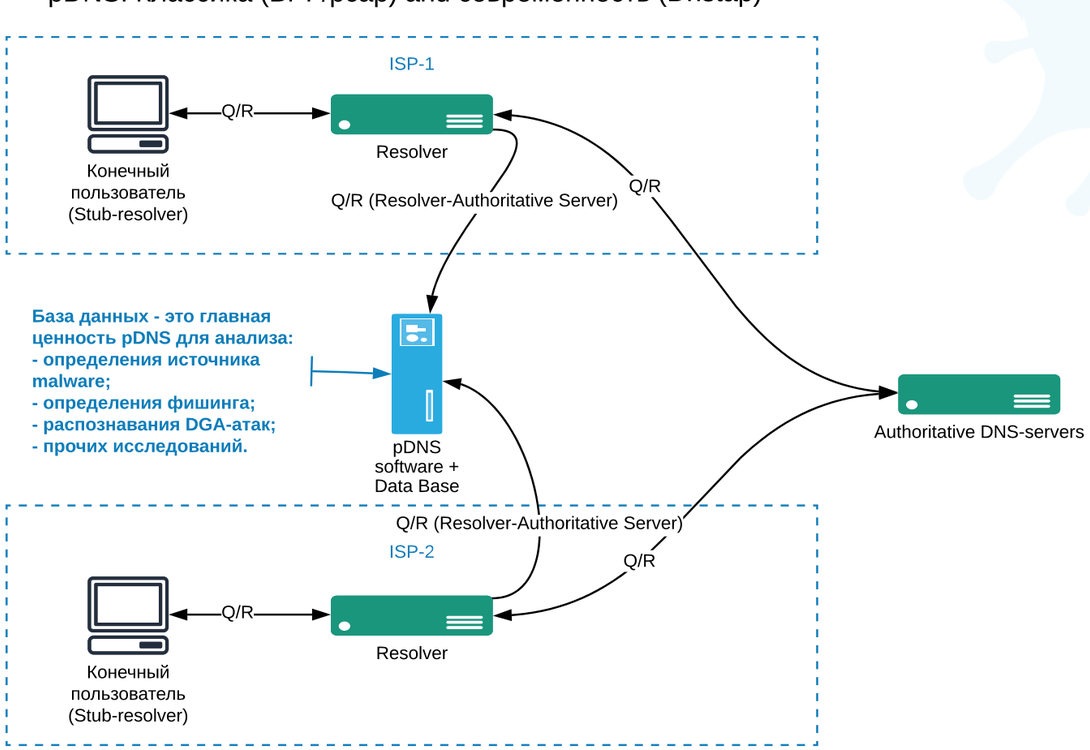
Август и сентябрь традиционно являются сезоном конференций. 2020 год не стал в этом смысле исключением. В техническом блоке конференции APTLD[1] основной темой стала дискуссия о безопасности DNS и инструментах детектирования DNS-атак посредством инструментов passive DNS. В контексте удаленной работы внимание к вопросам информационной безопасности выглядит вполне уместным.

Passive DNS – это технология складывания в хранилище DNS-запросов и DNS-ответов, которые проходят через рекурсивный резолвер, для последующего анализа.

В общих чертах это выглядит так, как показано на рисунке 1.

Важный момент тут состоит в том, что данные в классической схеме собираются на интерфейсе резолвера, который смотрит в сторону авторитетного сервера. Именно через этот интерфейс выполняется рекурсивная процедура поиска ответов на запросы конечного пользователя. Таким образом достигается защита приватных данных конечного пользователя, т.е. происходит обезличивание запроса. Многие из

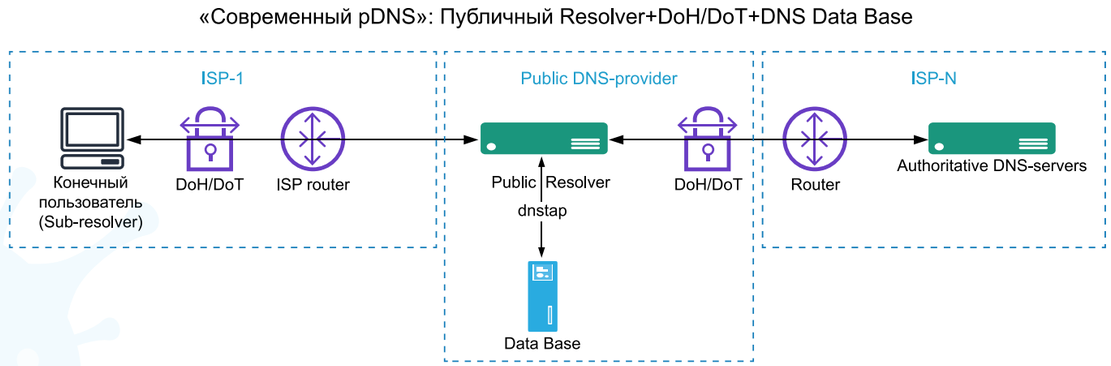
Рис. 1. Схема сбора данных для БД pDNS.



апологетов pDNS обязательно обращают особое внимание на эту особенность данной технологии. Приватность остается в рамках договоренностей между провайдером DNS-резолвинга и конечным пользователем.Современная история отличается от классической тем, что в качестве провайдера DNS-резолвинга выступает публичный резолвер. Например, резолвер Google или резолвер CloudFlare. В этом случае соединение между конечным пользователем и резолвером защищено. Соединение с авторитетным сервером также может быть защищено. Например, авторитетные серверы Facebook уже сейчас поддерживают взаимодействие с резолверами по протоколам DoT/DoH.

Снять трафик с интерфейса в этом случае не получится. Придется использовать модули dnstap, которые собираются непосредственно с резолвером (рис. 2).

Рис. 2. Получение данных о запросах/ответах через dnstap.



Важным в этой схеме является следующее:

- Теоретически могут быть собраны приватные данные, т.к. их собирают непосредственно с резолвера, а не с интерфейса.
- Незащищенные запросы можно собирать не только на интерфейсе сервера, но и на маршрутизаторах за счет, например, репликации трафика. В случае защиты каналов обмена запросами/ответами такой подход работать не будет.
- Анализом данных pDNS обычно занимаются специализированные исследователи, например, Farsight Security Inc. Пола Викси; будет ли тот же Google делиться информацией с третьей стороной – это большой вопрос.

Есть и технологический аспект, связанный с производительностью резолвера. Когда трафик собирается независимо от самого резолвера, то это не влияет на его производительность. Когда сам резолвер начинает логировать трафик, то его производительность непременно падает.

Требования к производительности резолверов, времени их отклика и их доступности более или менее определены:

- доступность сервиса: не ниже 99,98% и до 99,999%;
- производительность сервиса: не ниже 500 000 запросов в секунду для UDP и 100 000 запросов в секунду для TCP;
- время отклика для запросов: не хуже 10 мс (без учета сетевой задержки[2]);
- поддержка протоколов безопасности: DNSSEC, DoT, DoH.

Если посмотреть на тесты DNSPerf, то наиболее популярные публичные резолверы близки к приведенным выше параметрам (рис. 3).

Рис. 3. Показатели времени отклика публичных резолверов для региона Европа.

	DNS name	Query Speed	0 20 40 60 80 100
1	1.1.1.1	8.56 ms	
2	OpenDNS/Umbrella	18.32 ms	
3	Google	18.45 ms	

В настоящее время более 20% пользователей Интернета используют публичные резолверы. Их доля постепенно растет. Снижается ли при этом безопасность в контексте сложности применения технологии pDNS, пока не понятно.

Компании, которые специализируются на информационной безопасности, утверждают, что исключение из числа инструментов безопасности pDNS приведет к снижению надежности детектирования возможных угроз.

TLDCON2020 и «ковидный» трафик

Повестка TLDCON2020[3] в ее технической части была более традиционной – обсуждение влияния Covid-19 на Сеть.

Из любопытного – скачкообразный рост трафика на площадках МСК-IX (рис. 4).

Рис. 4. Динамика трафика на площадках МСК-IX в 2020 году.

На графике хорошо детектируется апрельский всплеск с последующим снижением и плавным прогнозируемым ростом в дальнейшем.

Также любопытны и данные по объему DNS-трафика на авторитетных серверах национальных доменов РФ (рис. 5).

Совершенно очевидно, что «ковидный» трафик превосходит по величине и трафик олимпиады в Сочи, и трафик Чемпионата Мира по футболу. Но он существенно уступает объемам трафика, с которыми система DNS должна была справляться накануне выборов президента РФ. Все-таки вероятность масштабной атаки на инфраструктуру в преддверии политических событий, как показывает опыт, существенно выше, чем в период пандемии.

Кроме увеличения трафика речь шла и о количестве обращений к около-«ковидным»[4] доменам (рис. 6).

Совершенно очевидно, что количество обращений к доменам этой категории значимо выросло. Относительно всего объема трафика на пике доля таких обращений не превышала 20% от общего количества обращений, что, вообще говоря, довольно много. Для сравнения, доля обращений к несуществующим доменам почти в два раза выше.

Резюмируя дискуссии на TLDCON2020, можно сказать, что влияние пандемии на инфраструктуру DNS есть, и оно достаточно велико. Во всяком случае, статистически значимо заметно.

А трафик растёт

Если рассматривать проблемы DNS более широко, а не только в контексте пандемии Covid-19, то можно выделить два интересных момента: рост количества обращений к корневым серверам системы DNS и постоянное «распухание» кэшей DNS-резолверов, как корпоративных, так и публичных. Такое «распухание» чревато отказами в обслуживании запросов конечных клиентов.

В принципе, оба вопроса сводятся к особенностям технологии кэширования, которая реализована в современных резолверах.

Любопытный анализ использования DNS-резолверов привел Джеф Хьюстон в своей статье в блоге APNIC[5]. Для начала, сославшись на отчет RSSAC, он приводит рост трафика на авторитетных серверах корневой зоны (рис. 7).

Согласно этому графику, объем трафика удваивается каждые два года. Выглядит это странно, т.к. количество резолверов в мире растёт не столь быстро, а кроме того, должен работать механизм DNS-кэширования.

Исследования показали, что часть этого роста связана с использованием браузеров на основе Chrome. Программное обеспечение Google таким образом борется с политикой провайдеров, которые перехватывают ответы авторитетных серверов на своих резолверах и в случае ответа NXDOMAIN (запрашиваемый домен отсутствует) производят перенаправление конечного пользователя на свои рекламные ресурсы.

Рис. 5. Ретроспектива DNS-трафика к авторитетным серверам домена .ru. Число запросов в последний день месяца.

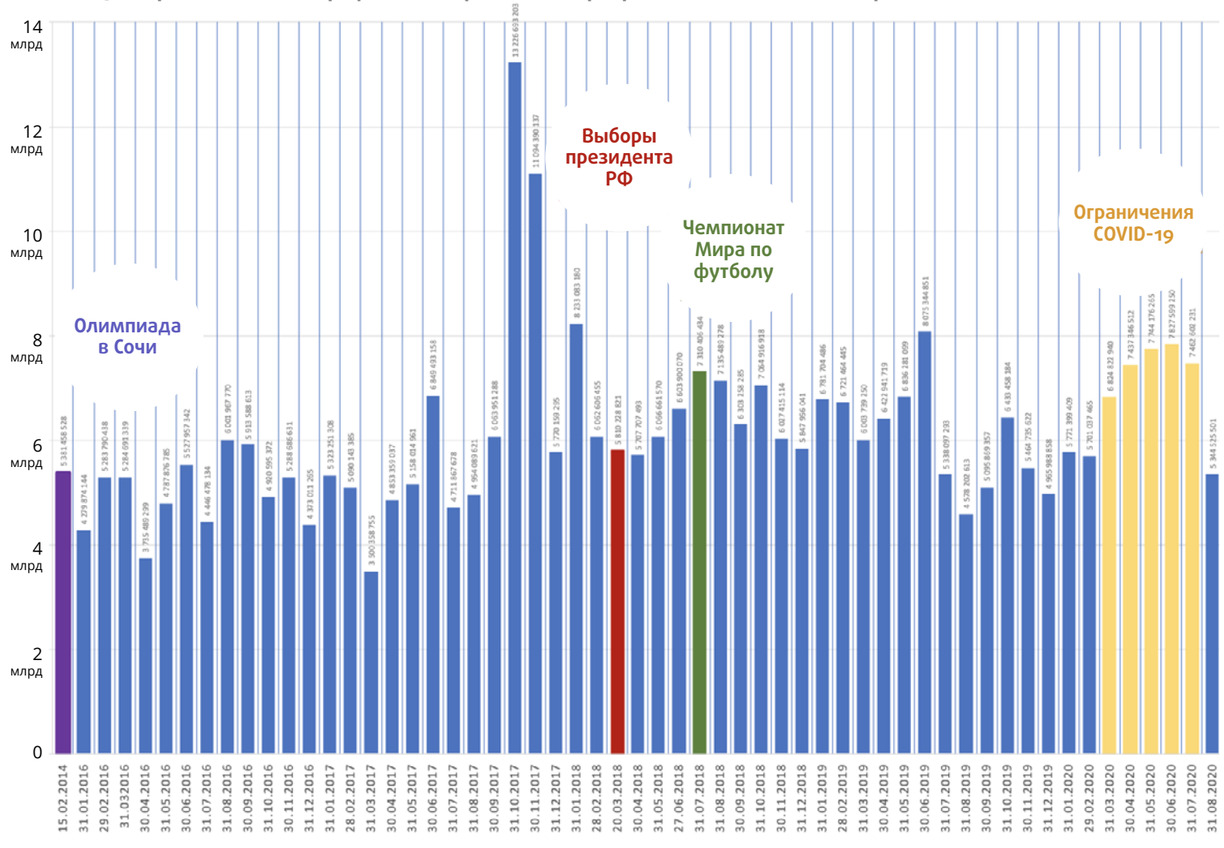
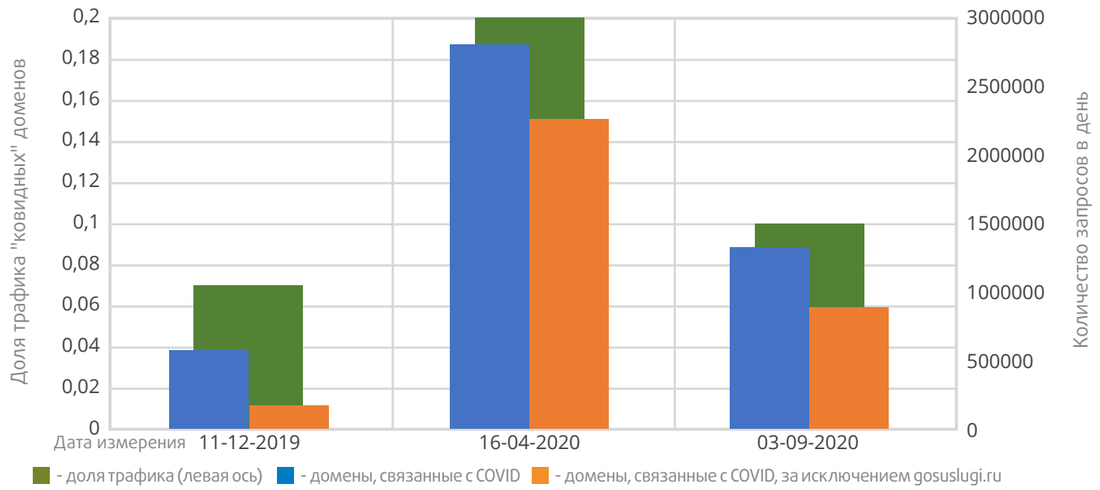


Рис. 6. Количество обращений к «ковидным» доменам и их доля в общем объеме трафика.



Google не согласен с такой обработкой несуществующего домена и борется с этим явлением, обременяя DNS-провайдеров (в случае корневой зоны – провайдеров корня системы DNS) огромным количеством запросов к несуществующим доменам, что приводит к необходимости затрат DNS-провайдеров на расширение своей инфраструктуры. При этом за «этот банкет» никто дополнительных средств провайдерам не дает.

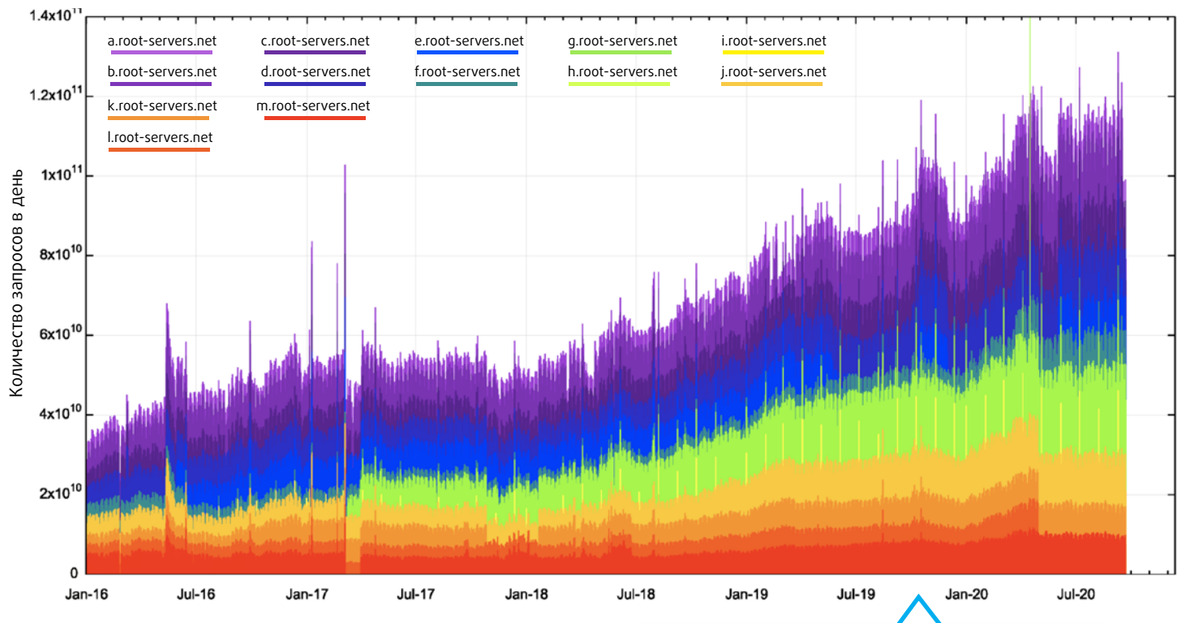
Вообще говоря, DNS имеет механизмы контроля таких обращений. Как минимум – это NSEC и Root on loopback.

При кэшировании NSEC резолвер в состоянии определить, стоит ли обращаться к авторитетным серверам, если он получает запрос с именем домена, которое лежит в интервале между двумя закэшированными метками NSEC. Т.е. домена с таким именем в зоне нет и отправлять запрос к авторитетным серверам не имеет смысла.

Во втором случае корневая зона размещается непосредственно на резолвере. В этом случае также нет необходимости опрашивать авторитетные серверы корневой зоны.

Но тем не менее, оба этих механизма в настоящее время работают недостаточно эффективно, а потому появляются

Рис. 7. Рост трафика на авторитетных серверах корневой зоны системы DNS.



новые предложения по детектированию несуществующих имен без обращения к авторитетным серверам[6].

Речь идет о размещении в зонах записей, которые позволяли бы строить специальные фильтры, на основе которых резолверы бы принимали решение об обращении к авторитетному серверу.

Побуждающим мотивом для поиска решений по снижению обращений резолверов к авторитетным серверам в данном случае является атака на авторитетные серверы, известная как DNS Water Torture Attack. В случае этой атаки ботнет через публичные резолверы направляет большое количество запросов о несуществующих доменах к авторитетному серверу и тем самым блокирует его работу.

Авторы предлагают разместить в зоне TXT-запись с Cuckoo-фильтром[7], которая позволила бы резолверу фильтровать запросы от клиентов об информации о несуществующих доменах. Утверждается, что такая процедура, с одной стороны, снизит трафик, а с другой стороны, не повлияет на производительность резолверов.

Немного о точности геолокации при анализе трафика

И в заключение отвлечемся от темы DNS. При анализе любого трафика, как правило, появляется необходимость определить, откуда и куда он направляется. В настоящее время трудно представить себе дашборд какой-либо системы мониторинга и управления, в котором не было бы карты размещения узлов с их географической привязкой или демонстрации маршрутов движения сообщений.

При этом всегда есть необходимость определения транзитных узлов и их географического размещения. В свете определения политик по регулированию национальных интернетов геолокация становится одной из ключевых технологий. Можно сказать, что критической - с точки зрения отчетности по достижению поставленных целей локализации и фрагментации.

Любопытный анализ использования DNS-резолверов привел Джеф Хьюстон в своей статье в блоге APNIC. Для начала, сославшись на отчет RSSAC, он приводит рост трафика на авторитетных серверах корневой зоны. Согласно этому графику, объем трафика удваивается каждые два года. Выглядит это странно, т.к. количество резолверов в мире растёт не столь быстро, а кроме того, должен работать механизм DNS-кэширования.

Соответственно, появляется необходимость ответа на вопрос: а насколько точна геолокация?

Группа исследователей из Норвегии выполнила измерения[8] точности определения геолокации IP-адресов точек маршрутов трафика на уровне стран. Для этого они проанализировали сервисы MaxMind и IP2Location и две технологии уточнения геолокации на основе времени отклика (HLOC и RIPE's IPmap). Точность таких сервисов определяется площадью того объекта, к которому нужно привязать адрес. Для стран точность должна быть наивысшей. Но привязать адрес – это одно, а вот привязать путь между двумя адресами – это совсем другое.

Исследование показало, что для маршрутов (промежуточных точек на маршрутах) в пространстве IPv4 как минимум одна страна выпадает (корректно не определяется) в 42% случаев, а в пространстве IPv6 таких случаев 32%.

Если норвежцы правы, то для достижения целей контроля «зацикливания» национального трафика в пределах одной страны существующих баз данных геолокации и маршрутно-адресной информации явно недостаточно, а отчетность по достижению соответствующих целей будет, мягко скажем, недостаточно достоверной.

Вместо заключения

Пандемия Covid-19 поставила перед Интернетом новые задачи и высветила старые проблемы. Вопросы фрагментации сети по национальным или корпоративным сервисам не ушли с повестки дня. Они стали еще более актуальными.

С 22 по 25 сентября 2020 года прошел шестой раунд пленарных слушаний по дополнительному протоколу к Конвенции Совета Европы о киберпреступности (Будапештская конвенция). Обсуждались вопросы прямого взаимодействия правоохранителей разных стран с операторами связи и провайдерами прочих сетевых услуг, находящихся на территории чужой юрисдикции. В частности, обсуждался вопрос доступа к данным WHOIS и вопрос их достоверности.

Повод новый – пандемия, цель старая – персональные данные, к которым легитимного доступа у правоохранителей нет.

В большинстве стран Конвенции обсуждаемые вопросы прямо противоречат местному законодательству. РФ не является участником Конвенции. Только наблюдателем.

Вот и понаблюдаем, к каким техническим решениям это всех нас приведет. А в том, что эхо политических баталий коснется вопросов технических, сомнений нет. Вспомните пики DNS-атак в преддверии президентских выборов в РФ с рисунка 5.

К слову сказать, количество обращений российских правоохранителей к регистратурам и регистраторам в период пандемии по поводу мошенничества в Сети увеличилось в 2,5 раза.

Ссылки

1. http://aptld78.tw/

2. Под сетевыми задержками понимаются задержки, возникающие на пути от конечного пользователя до DNS-узла. В случае размещения DNS-узла топографически наиболее близко к конечному пользователю задержки будут минимальными - от 1 до 10 мс. Если DNS-узел разместить во Владивостоке, а опрашивать его из Москвы, то задержка будет порядка 100 мс.

3. https://tldcon.ru/

4. Около-«ковидный» домен – это домен, в имени которого есть термины на тему заболевания или лечения новой коронавирусной инфекции Covid-19.

5. https://blog.apnic.net/2020/09/28/scaling-the-root-of-the-dns/

6. https://blog.apnic.net/2020/10/06/enabling-privacy-aware-zone-exchanges-among-authoritative-and-recursive-dns-servers/

7. https://smartech.gatech.edu/handle/1853/60577

8. https://dl.acm.org/doi/pdf/10.1145/3404868.3406664

Новости доменной индустрии

ENOG 17

2020 год внес в нашу жизнь много нового и необычного. В частности, новый формат проведения профессиональных конференций не позволил участникам встретиться и пообщаться лично, но появилось больше возможностей для участия в международных и региональных мероприятиях. Не нужно собирать чемоданы, долго лететь, бороться с джет-лагом… Достаточно просто включить ноутбук.

Так, крупнейшей за все годы проведения (1224 человека из 85 стран) стала конференция ENOG 17 | RIPE NCC Regional Meeting, прошедшая 9-13 ноября в онлайн-режиме, организованная RIPE NCC при поддержке Координационного центра доменов .RU/.РФ.

Координационный центр многие годы является партнером форума Евразийской группы сетевых операторов ENOG. Это уникальное в нашем регионе мероприятие, которое собирает технических экспертов, представляющих самые разные компании телекоммуникационной отрасли: вендоров, сервисных операторов, интернет-провайдеров и т.д. Идея организовать форум ENOG возникла в 2010 году и стала логическим продолжением проведения региональных конференций RIPE NCC в России и в других странах нашего региона. Первая конференция ENOG была организована RIPE NCC в 2011 году и прошла при поддержке Координационного центра, Технического центра Интернет (TCI), MSK-IX.

Участников «первого в истории виртуального ENOGa» приветствовали председатель программного комитета ENOG **Алексей Семеняка**, глава сообщества RIPE **Мириам Кюне** и управляющий директор RIPE NCC **Ханс Петер Холен**. Мириам Кюне, ставшая главой сообщества совсем недавно, рассказала о приоритетах и ближайших задачах RIPE, среди которых активизация работы в регионе и налаживание взаимодействия с потенциальными членами сообщества.

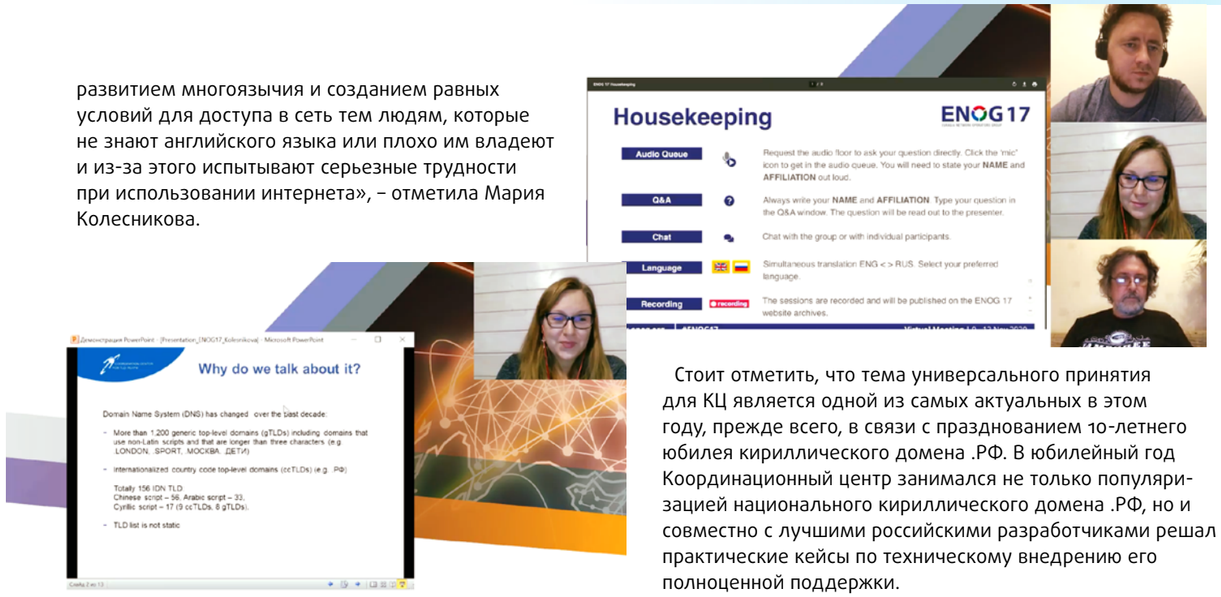
Представители Координационного центра постоянно участвуют в RIPE митингах. Наибольший интерес представляют вопросы, связанные с DNS. Еще одна тема, которая представляет для нас непосредственный интерес с точки зрения работы наших доменов .RU и .РФ, это Система мониторинга TLD доменов, которую представил специалист нашего технологического партнера – компании MSK-IX – Александр Ильин.

Тема развития системы доменных имен прозвучала и на других заседаниях ENOG 17. О новом исследовательском проекте ICANN ITHI (Identifier Technology Health Indicator) рассказал руководитель по взаимодействию с заинтересованными сторонами в Восточной Европе и Центральной Азии **Михаил Анисимов**. По его словам, при помощи этого проекта возможно оценить, как функционирует система доменных имен, выявлять закономерности и аномалии. Он также призвал операторов DNS и провайдеров интернета принять участие в проекте: «ITHI обрабатывает данные, получаемые от партнеров проекта. Как и всегда в такого рода исследованиях, полнота картины зависит от количества участников. Чем больше данных мы получаем, тем точнее сможем определять тренды и особенности работы системы доменных имен».

Одной из тем ENOG 17 стало универсальное принятие интернационализированных доменных имен и почтовых адресов в интернете и существующие форматы международного и регионального сотрудничества в этой области. С докладом «Новости и задачи универсального принятия» выступила главный аналитик КЦ, председатель локальной инициативы по универсальному принятию в странах СНГ и Восточной Европе **Мария Колесникова**.

Сегодня в доменном пространстве существует 156 интернационализированных доменов верхнего уровня, 17 из них – кириллические. И универсальное принятие – это концепция, которая подразумевает, что все доменные имена и адреса электронной почты вне зависимости от алфавита, набора или количества символов (например, .РФ, .PHOTOGRAPHY) одинаково поддерживаются всеми интернет-приложениями, устройствами и системами. Мария Колесникова подробно рассказала об отчете «Оценка принятия адресов электронной почты веб-сайтами разных стран в 2020 году», который был подготовлен Группой управления по универсальному принятию (UASG). Кроме того, на его основе Координационный центр выпустил отчет «Анализ уровня универсального принятия адресов электронной почты веб-сайтами в России и мире в 2020 году»[1], куда вошли дополнительные исследования, проведенные КЦ по поддержке кириллицы.

По данным исследований, приведенным в отчете, всего 11% популярных веб-сайтов в мире поддерживают почтовые адреса с Unicode-символами, и чуть менее 10% почтовых серверов сконфигурированы для этого. В России ситуация несколько лучше: почти каждый пятый популярный в России веб-сайт (19%) принимает адреса электронной почты, полностью записанные на кириллице. Это второй результат в мире, а самый высокий уровень принятия электронной почты, записанной полностью на национальном языке, зафиксирован в Германии – 28%. Также Мария рассказала о мероприятиях и проектах, проводимых Координационным центром и Региональной группой по универсальному принятию стран СНГ и Восточной Европы – о проекте Поддерживаю.РФ и программе IDN Bug Bounty, о тренингах и хакатонах по теме универсального принятия, которые были проведены в 2020 году. «Скорейшее внедрение универсального принятия – задача не только технологическая. Этот процесс напрямую связан с обеспечением инклюзивности интернета, развитием многоязычия и созданием равных условий для доступа в сеть тем людям, которые не знают английского языка или плохо им владеют и из-за этого испытывают серьезные трудности при использовании интернета», – отметила Мария Колесникова.



Стоит отметить, что тема универсального принятия для КЦ является одной из самых актуальных в этом году, прежде всего, в связи с празднованием 10-летнего юбилея кириллического домена .РФ. В юбилейный год Координационный центр занимался не только популяризацией национального кириллического домена .РФ, но и совместно с лучшими российскими разработчиками решал практические кейсы по техническому внедрению его полноценной поддержки.

Ссылки

1. https://cctld.ru/upload/iblock/7a3/UA_Report_2020.pdf

Координационный центр национального домена сети Интернет поздравляет MSK-IX с 25-летним юбилеем!

Мы вспоминаем далекий 1995 год, когда семь провайдеров заключили соглашение о создании точки взаимного обмена IP-трафиком, чтобы объединить российский интернет-сегмент, а в ноябре 1995 года на телефонной станции М9 заработал первый узел «Московского Internet eXchange».

С момента запуска проекта команда MSK-IX непрерывно работала над новыми идеями и решениями для цифровых компаний и организаций. Сегодня MSK-IX – многопрофильная платформа для развития интернет-сетей с присутствием в 10 городах и технологический акселератор для развития сетевых сервисов. По объемам пирингового взаимодействия MSK-IX входит в топ-5 крупнейших мировых IX, сохраняя лидерство в России и в Восточной Европе. С MSK-IX работает более 800 клиентов – интернет-компаний из 100 городов и 20 стран мира.

В мае этого года президент России В. В. Путин наградил почетными грамотами генерального директора АО «ЦВКС МСК-IX» Елену Воронину и руководителя проектов DNS АО «ЦВКС МСК-IX» Павла Храмцова «за заслуги в становлении и развитии российского сегмента информационно-телекоммуникационной сети Интернет».

Поздравляем команду MSK-IX с юбилеем и желаем уверенного движения вперед, новых встреч и открытий! Координационный центр гордится и дорожит профессиональными отношениями с коллективом MSK-IX и ее генеральным директором Еленой Павловной Ворониной.

Андрей Воробьёв
Директор Координационного центра доменов .RU/.РФ

MSK IX

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

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

Интернет изнутри

2020