№16
Декабрь 2021

MSK IX

Интернет изнутри

Тенденции будущего

SCION: Защищенная инфраструктура междоменной многопутевой маршрутизации

с. 4

Содержание:

Журнал
«Интернет изнутри»

info@internetinside.ru

Порядковый номер выпуска
и дата его выхода в свет:
Выпуск №16, дата выхода:
Декабрь 2021 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:
Татьяна Новикова

Редакционная коллегия:
Елена Воронина
Алексей Платонов

Продакшн:
Алексей Гончаров

Дизайн и вёрстка:
Дмитрий Ивлянов

Корректор:
Наталья Рябова

Обложка разработана
с использованием ресурсов
сайта Freepik.com

Взгляд в будущее

Главный редактор:
Андрей Робачевский

Дорогой читатель!

Оскар Уайльд когда-то сказал, что будущего трудно избежать. Предсказать его тоже непросто, особенно если это касается Интернета, который не раз за свою относительно короткую историю удивлял нас неожиданными инновациями.

Для многих авторов этого выпуска «Интернета изнутри» возможное будущее – это проекты, над которыми они работают сегодня. Одному из таких проектов под названием SCION мы посвятили первую статью. Сможет ли новая архитектура связности и маршрутизации, разработанная в рамках этого проекта, «завоевать» Интернет, – покажет время, но предложенный подход существенно меняет сегодняшнюю парадигму маршрутизации.

Возможные сценарии развития системы корневых серверов имен DNS обсуждает в своей статье частый гость нашего журнала – Джефф Хьюстон. Хотя он и рассматривает эту эволюцию в рамках существующей структуры, он показывает, насколько существенно меняется роль и задачи «корня» DNS. В конце концов, а почему бы не рассматривать корневую зону DNS как просто контент, с которым мы научились очень хорошо обращаться?

С виртуализацией сетевых функций нас познакомит Уильям Стеллингс. Этот подход позволяет организовать сетевую связность на достаточно абстрактном уровне и реализовать ее с помощью стандартного оборудования, используя преимущества виртуализации. В этом случае можно без особого сомнения сказать, что виртуализация определяет и будет определять развитие технологий в будущем.

Не оставили мы без внимания и наши стандартные темы. В разделе «Политика» Мадина Касенова предлагает великолепный обзор регулирования цифрового рынка в Евросоюзе. И как всегда, Павел Храмцов приглашает вас в свою рубрику «Новости науки и техники».

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

SCION: Защищенная инфраструктура междоменной многопутевой маршрутизации

Сирилл Крэхенбуль (Cyrill Krähenbühl),
Сейедали Табаеигдаеи (Seyedali Tabaeiaghdaei),
Кристель Глур (Christelle Gloor),
Джонгхун Квон (Jonghoon Kwon),
Адриан Перриг (Adrian Perrig),
Дэвид Хаушир (David Hausheer)

Развитие Интернета опережает самые оптимистичные ожидания. Он проникает во все поры и переплетается со всеми аспектами современного общества и экономики. Это даже привело к настолько серьёзной зависимости от коммуникационного обмена, что многие процессы, лежащие в основе современного общества, полностью остановятся в случае отсутствия коммуникации. Однако текущее состояние безопасности и доступности Интернета отнюдь не соответствует степени его важности. В течение последних двух десятилетий было предпринято несколько попыток перестроить Интернет для того, чтобы обеспечить его соответствие новым требованиям, предъявляемым передовыми интернет-приложениями. Один из таких проектов получил название SCION (Scalability, Control and Isolation on Next-Generation Networks — Масштабируемость, управление и изоляция в сетях следующего поколения) и представляет собой защищенную интернет-архитектуру, которая разрабатывается швейцарским университетом ETH Zurich (Федеральная высшая техническая школа Цюриха) и отделившейся от него компанией Anapaya Systems.

Введение

С самого начала своего существования Интернет пережил впечатляющую эволюцию, резко изменив то, как мы живем, работаем и общаемся друг с другом. При этом изменения практически не коснулись базовых строительных блоков самого Интернета. Однако по мере его развития и расширения и появления новых способов его использования на свет вышли многочисленные проблемы, связанные с его архитектурой. Среди них особенно важен вопрос инфраструктуры междоменной маршрутизации на базе протокола BGP (Border Gateway Protocol).

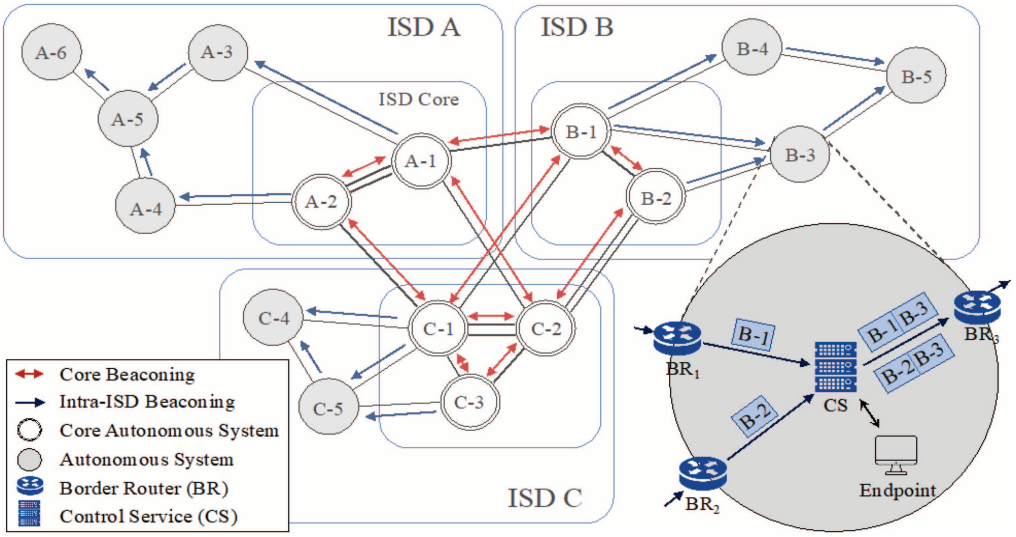
SCION (в переводе с английского «потомок» — ред.) — это защищенная архитектура Интернета следующего поколения, которая обеспечивает безопасную маршрутизацию и передачу трафика в целях достижения высокого уровня доступности даже в присутствии сетевых злоумышленников. Она основана на сетевом взаимодействии с распознаванием пути (PAN, path aware networking) — новом тренде в развитии сетей, при котором конечным точкам предоставляется больше данных и контроля за путями перемещения их пакетов. Это сильно отличается от существующего Интернета, в котором выбор пути осуществляется неявно в рамках самой сети. PAN предлагает захватывающие перспективы развития Интернета: многопутевая коммуникация способна использовать присущее Интернету разнообразие путей, выбор пути на базе приложения позволяет конечным точкам влиять на маршрутизацию и выбирать оптимальные маршруты, а быстрое преодоление отказа помогает восстанавливаться после сбоев линий связи.

Хотя методы междоменной многопутевой коммуникации уже используются в действующих сетях, большинство подобных технологий не получили крупномасштабного внедрения в основном из-за отсутствия четких стимулов для развертывания. Внедрение новой интернет-архитектуры требует значительных финансовых инвестиций, и только предостав-

ление ощутимых стимулов для пионеров её использования может обеспечить популярность архитектуры в реальном мире.

SCION представляет собой первую интернет-архитектуру PAN, достигшую практического применения. В этой статье мы рассмотрим концепцию внедрения, которая лежит в основе продуктивной сети SCION, вместе с системой стимулов для пионеров её использования. Но является ли развертывание сети SCION реалистичной и осуществимой инициативой, учитывая преобладание в настоящее время архитектуры на базе BGP? И можно ли расширить масштаб SCION до размеров Интернета?

Рис. 1. Сигнализация между центральными AS и внутри доменов ISD в рамках сети SCION.



Для ответа на эти вопросы давайте взглянем на ключевые концепции архитектуры SCION, а также на разные модели, использовавшиеся для практического развертывания SCION на аппаратном обеспечении провайдеров интернет-услуг и точек обмена интернет-трафиком (IXP).

Система именования и сетевая структура SCION

Для того чтобы сохранить экономические принципы работы современного Интернета, SCION также использует традиционную структуру автономных систем (AS, Autonomous System) и обеспечивает передачу сетевого трафика только по тем путям, которые совместимы с политиками маршрутизации. Для обеспечения масштабируемости и суверенитета вводятся домены изоляции (ISD, Isolation Domain). ISD представляет собой логическую группировку автономных систем. Такой домен управляется несколькими AS, формирующими ядро ISD. Мы называем их центральными AS. Обычно, 3–5 крупнейших провайдеров интернет-услуг ISD образуют ядро ISD. Управление ISD осуществляется с помощью политики, называемой «конфигурация корней доверия» (TRC, trust root configuration), которая согласовывается ядром ISD. TRC определяет корни доверия (источники, которым можно всегда доверять), которые используются для валидации привязки имен к открытыми ключам или адресам. Центральные AS обеспечивают связность с другими ISD и управляют корнями доверия.

Как правило, домен ISD включает также несколько обычных AS. AS присоединяется к ISD, приобретая связность у другой автономной системы AS в составе ISD. Присоединение к ISD означает принятие TRC данного домена ISD. На рис. 1 показана сеть SCION с тремя доменами ISD, каждый из которых включает две или три центральные AS.

Маршрутизация основана на кортеже ISD, AS, независимом от локальной адресации. Номера AS ведутся на базе текущего Интернета, однако 48-битовое пространство имён позволяет использовать для AS дополнительные номера SCION, которые выходят за рамки применяемого сегодня 32-битового пространства. Адресация хоста расширяет сетевой адрес за счет добавления к нему локального адреса, что приводит к образованию трёхэлементного кортежа ISD, AS, локальный адрес. Локальный адрес не используется при междоменной маршрутизации или переадресации и может, таким образом, представлять из себя, например, адрес IPv4, IPv6 или MAC.

Плоскость управления

Плоскость управления SCION обеспечивает обнаружение и распределение сегментов пути уровня AS. Сегмент пути кодирует сетевой путь с детализацией на уровне AS и соединений между AS, которые связывают два следующих друг за другом AS вдоль пути. Создание междоменных путей на уровне соединений между AS увеличивает количество доступных путей и позволяет их оптимизировать с учетом различных критериев.

Каждый сквозной путь в рамках SCION состоит не более чем из трех сегментов пути: центрального пути, пути вверх и пути вниз. К сегментам центрального пути относятся сегменты, которые содержат только центральные AS, сегмент пути вверх — это участок пути от заказчика к провайдеру внутри одного домена ISD, сегмент пути вниз — это участок пути от провайдера к заказчику внутри домена ISD. Пример: если конечная точка в домене B-3 (Рис. 1) хочет подключиться к конечной точке в домене A-4, то возможный путь состоит из следующих сегментов: путь вверх (B-3, B-2), центральный путь (B-2, B-1, A-1, A-2) и путь вниз (A-2, A-4). Для того, чтобы решить проблему субоптимальности иерархической маршрутизации, в SCION введены пиринговые соединения и укороченные пути. Укороченный путь включает только сегмент пути вверх и сегмент пути вниз, которые соединяются в общей для обоих сегментов нецентральной AS. Пиринговые связи можно добавлять к сегментам вверх или вниз, что приводит к системе, похожей на современный Интернет.

Маршрутизация в рамках SCION (или строительство сегментов путей) выполняется иерархически на двух уровнях: (1) среди всех центральных AS всех доменов ISD, что поз-

воляет создавать сегменты центрального пути, и (2) внутри каждого домена ISD, что позволяет создавать сегменты пути вверх и вниз. Процесс создания сегментов пути называют сигнализацией, в рамках которой центральные AS инициируют маркер строительства сегментов пути (PCB, Path-segment Construction Beacon) для итеративного создания сегментов.

На Рис. 1 сигнализация между центральными AS и внутри доменов ISD показана с помощью красных двунаправленных и синих стрелок соответственно. Процесс сигнализации в каждом AS выполняется маркерным (маяковым) сервером, который входит в состав сервиса управления (CS, Control Service), реализующего задачи плоскости управления. Маркерный сервер определяет, какие маркеры PCB следует передавать и через какие интерфейсы с учетом политики локальной AS. Перед тем, как передать PCB, маркерный сервер добавляет номер своей AS, а также идентификаторы входящего и исходящего интерфейсов. Кроме того, каждый маркер PCB имеет отметку времени истечения, которая задается инициатором PCB для указания срока действия пути. Важно отметить, что через сервис управления передаются только сообщения плоскости управления, тогда как трафик плоскости данных течет через внутреннюю сеть, т. е. сервис управления не становится своеобразным бутылочным горлышком для трафика плоскости данных.

(1) Сигнализация между центральными AS. Такая сигнализация представляет собой процесс создания сегментов путей между центральными AS. В её ходе центральная AS передает маркеры PCB, полученные от соседних центральных AS, ко всем соседним центральным AS. Поскольку ожидается, что количество доменов ISD будет составлять сотни, а на каждый ISD обычно приходится 3-5 центральных AS, совокупное количество организаций, принимающих участие в такой сигнализации, остаётся относительно небольшим.

(2) Сигнализация внутри доменов ISD. Она представляет собой второй уровень иерархии сигнализации и создает сегменты пути от центральных AS до нецентральных AS. В её ходе центральные AS инициируют маркеры PCB и отправляют их своим нецентральным соседям (обычно это AS заказчика). Каждая нецентральная AS продлевает полученные PCB до своих соответствующих заказчиков. Эта процедура продолжается до тех пор, пока PCB не достигнет AS без заказчика (конечная AS). В результате все AS получают сегменты пути, по которым можно достичь центральных AS своих доменов ISD. Такая ограниченная политикой лавинная маршрутизация является очень эффективной, поскольку только центральные AS способны инициировать маркеры PCB.

Распространение сегментов пути. Для распространения сегментов пути используется глобальная инфраструктура серверов пути. В рамках сервиса управления каждая AS располагает сервером пути. Эта инфраструктура имеет сходство с системой доменных имен (DNS), в которой информация выдается только по запросу. Сервер пути центральной AS хранит все сегменты пути внутри домена ISD, которые были зарегистрированы конечными AS этого домена, а также сегменты пути, необходимые для попадания на другие центральные AS.

Плоскость данных

Процесс разрешения имени (преобразования имени в адрес) в SCION приводит к образованию трёхэлементного кортежа ISD, AS, локальный адрес. Центральные сегменты и сегменты пути вниз вызываются на базе кортежа ISD, AS. После чего хост может объединить пути вверх с полученными центральными сегментами и сегментами пути вниз. Кратчайшие пути, обходящие центральную AS, возможны, если сегменты пути вверх и вниз содержат одну и ту же AS, либо если между AS в сегменте пути вверх и AS в сегменте пути вниз доступно пиринговое соединение. Криптографическая защита обеспечивает аутентичность сегментов пути и гарантирует, что возможны только авторизованные комбинации путей.

Сегменты пути содержат компактные поля переходов, в которых закодирована информация, по какому интерфейсу следует входить в AS и выходить из неё, а также данные криптографической защиты для предотвращения изменения пути. Это так называемое состояние пересылки, переносимое пакетом (PCFS, Packet-Carried Forwarding State), обеспечивает начало использования пути без отправки каких-либо сигналов, при этом не требуется переключать маршрутизаторы для путей или потоков.

Анализ ситуации: глобальное развертывание SCION

Давайте рассмотрим, каким образом SCION можно развернуть в существующих сетях и использовать для управления реальным трафиком в IXP, системах ISP и оконечных сетях. Прежде чем описывать подробности технического развертывания, необходимо рассказать о стимулах для заинтересованных сторон, которые привели к первому продуктивному применению SCION в 2017 году, и затем коротко обсудить рекомендации по развертыванию, которые требуются, чтобы проявились ярко выраженные свойства SCION.

Стимулы для заинтересованных сторон

Важным аспектом развертывания новой интернет-архитектуры являются стимулы, побуждающие к началу внедрения. Подобно сакраментальному вопросу «Кто купит первый факс?», проблема внедрения архитектуры следующего поколения представляется ещё более острой, если учесть многообразие предложений в области коммерческой коммуникации, которые доступны сегодня.

Стимулом для первоначальных заказчиков являлось то, что соединение SCION можно было использовать для замены арендованной линии связи, поскольку SCION позволяет имитировать свойства арендованной линии, плюс обещания обеспечить более высокую гибкость и уменьшение издержек в долгосрочной перспективе (так как система связи SCION по сути представляет собой «стандартное соединение», не требующее специального конфигурирования со стороны ISP). С точки зрения безопасности, SCION характеризуется такими свойствами, как геозонирование, прозрачность путей, быстрое преодоление отказа, отсутствие атак на маршрутизацию и встроенная защита от DDoS-

атак. Как результат, SCION может помочь снизить издержки — рассмотрим, например, подключение филиалов в количестве N к центрам обработки данных в количестве K, что может быть реализовано с помощью N·K арендованных линий связи или с помощью N+K соединений SCION (достигнутая экономия может быть еще больше, если требуется обеспечить резервирование).

Более долгосрочные стимулы, побуждающие к использованию SCION, включают повышение производительности и качества связи за счет применения многопутевой архитектуры и оптимизированного выбора пути на базе требований приложений (например, низкая задержка, высокая пропускная способность, низкий уровень джиттера или низкие потери (пакетов)). Однако эти долгосрочные стимулы, похоже, еще не сыграли свою роль в расширении признания новой технологии.

Начиная с августа 2017 года SCION используется в коммуникационной системе крупного банка (со стоимостью активов более 500 миллиардов долларов США), который стал первым клиентом, выразившим желание применить SCION для замены арендованных линий. К настоящему времени несколько филиалов этого банка подключены к центру обработки данных исключительно через сеть SCION. Положительный опыт их работы побудил другие коммерческие, образовательные и государственные организации, а также провайдеров интернет-услуг (ISP) принять эту технологию на вооружение. В настоящее время соединения SCION предлагают восемь ISP, а несколько банков и государственных организаций пользуются преимуществами сетевого взаимодействия без протокола BGP. Всё это показывает, что стимулы для начального развертывания были достаточными, однако для побуждения к более широкому принятию новой технологии и, в конечном счете, для достижения широкой прямой связности SCION на используемых приложениями конечных хостах требуются дополнительные стимулы.

Рекомендации по развертыванию

Учитывая, что свойства усиленной защиты SCION являются одним из важнейших стимулов использования этой технологии, даже при начальном развертывании нужно обеспечить выполнение строгих требований безопасности. Таким образом, развертывание «поверх» современного Интернета невозможно, поскольку в этом случае SCION унаследует уязвимости слабой «подложки». Проблема заключается в необходимости развернуть SCION параллельно существующим сетям экономически оправданным способом, обеспечивающим сохранение защитных свойств. В частности, работа сети SCION никак не должна зависеть от BGP.

Поскольку развертывание абсолютно новой сетевой инфраструктуры является чрезвычайно дорогим удовольствием, используются существующие внутренние сети автономных систем (AS). Однако необходимо соблюдать осторожность с тем, чтобы традиционный IP-трафик не вытеснил трафик SCION, например, при перегрузке на уровне IP.

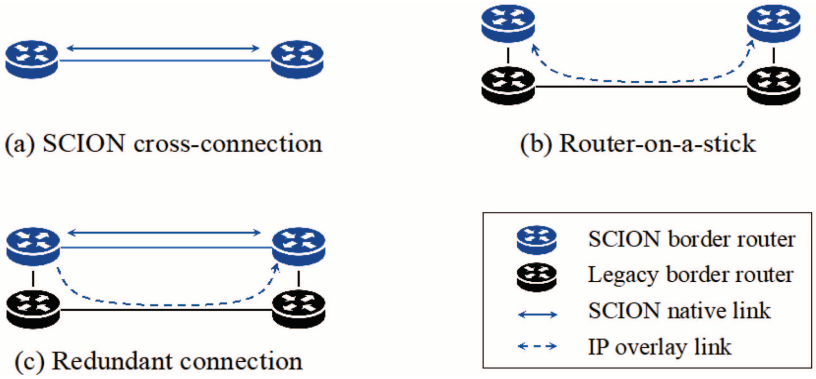
Развертывание у провайдеров интернет-услуг (ISP)

Как это показано на рис. 1, для развертывания SCION провайдеру интернет-услуг необходимо настроить граничные маршрутизаторы и запустить приложения сервиса управления. Граничный маршрутизатор и приложения сервиса управления развертываются на коммерческо-стандартных (COTS) серверах x86, которые имеют соединения с пропускной способностью до 100 Гбит/с. Для того, чтобы обеспечить для инфраструктуры SCION поддержание коммуникации внутри AS, можно повторно использовать IP- или MPLS-сеть. Если недоступны выделенные соединения, то разделение IP- и SCION-трафика можно реализовать при помощи организации очередей на внутренних коммутаторах.

Соединение с заказчиком и связь через SCION между граничными маршрутизаторами соседних ISP можно обеспечить тремя путями. В идеале, соседние ISP, инфраструктура которых поддерживает SCION, будут подключены через прямое соединение SCION (рис. 2(a)). Другими словами, два граничных маршрутизатора SCION напрямую соединяются через кросс-соединение уровня 2 в одном и том же месте точек входа в сеть, обеспечивая связность операторского класса с высокой надежностью, доступностью и производительностью. Прямое SCION-соединение устойчиво к ошибкам BGP, обеспечивая выполнение требования к развертываемости; SCION работает независимо от BGP, при этом потенциальные перебои BGP не влияют на SCION и наоборот.

Для того, чтобы свести к минимуму изменение существующей инфраструктуры, ISP могут также повторно использовать существующую сетевую инфраструктуру (т. е. модель «Маршрутизатор на палочке» (Router-on-a-stick)). Как это показано на рис. 2(b), граничные маршрутизаторы SCION могут быть присоединены к существующим граничным маршрутизаторам. Граничный маршрутизатор SCION обеспечивает IP-инкапсуляцию пакетов SCION и перенаправляет их на соседний граничный маршрутизатор SCION через короткое IP-соединение. Главные преимущества такой модели развертывания заключаются в следующем: a) ISP могут полноценно использовать уже существующую сетевую инфраструктуру для новой архитектуры сети при том, что б) ISP способны выполнять маршрутизацию и переадресацию IP-пакетов с использованием того же набора устройств. Поскольку модель Маршрутизатора на палочке представляет

Рис. 2. Сценарии развертывания у ISP. Различные модели поддерживают ранний, промежуточный и полный варианты развертывания.



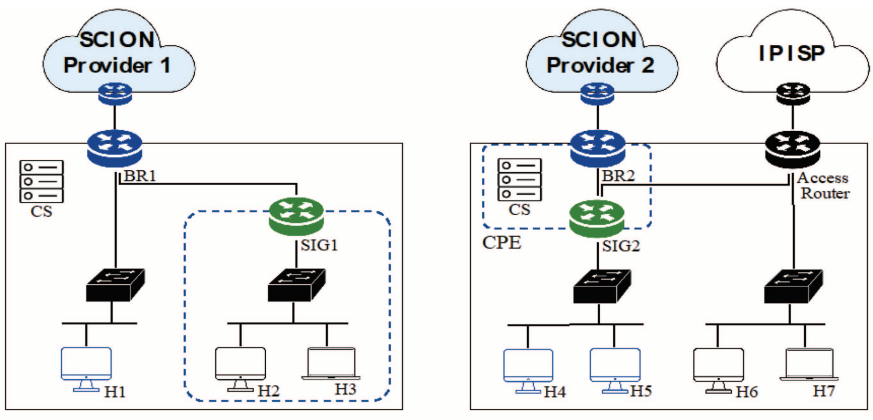
собой прямое кросс-соединение ближнего действия, потенциальные недостатки, связанные с использованием IP-инкапсуляции, например, неоптимальная маршрутизация, перехват BGP и медленная конверсия, едва ли вызовут какие-либо сложности.

И наконец, рис. 2(c) показывает развертывание резервного соединения. Оно объединяет две вышеописанные модели развертывания, устанавливая два SCION-соединения между смежными AS. Учитывая тот факт, что в рамках модели Маршрутизатор на палочке физическое соединение может быть перегружено обычным трафиком, SCION-соединение на базе IP может подвергнуться атакам, что снизит его характеристики. Однако при использовании модели Резервного соединения провайдеры интернет-услуг имеют в своем распоряжении два физически раздельных SCION-канала и сохраняют существующее соединение, что позволяет повысить доступность, улучшить взаимосовместимость и ускорить восстановление после отказа.

Поддерживающие SCION провайдеры интернет-услуг обеспечивают эффективную коммуникацию между собой даже в сценариях с частичным развертыванием; т. е. две поддерживающие SCION автономные системы необязательно должны быть смежными. В то же время, наведение мостов между двумя островами SCION, например, при помощи создания IP-туннеля для пересылки пакетов SCION через общедоступный Интернет, приводит к появлению связанных с BGP уязвимостей. Для решения этой проблемы был создан транзитный сервис SCION — глобальная магистраль для поддерживающих SCION провайдеров интернет-услуг. Транзитный сервис SCION обеспечивает создание прямых SCION-соединений, которые реализуют эксклюзивную передачу трафика SCION среди более чем 60 центров обработки данных, расположенных в Европе, Азии и на Ближнем Востоке. Благодаря широкому распространению точек присутствия провайдеры интернет-услуг могут легко устанавливать доступ (через один хоп) к глобальному транзитному сервису SCION со скоростью 1 Гбит/с или 10 Гбит/с, перенаправляя трафик SCION через сеть, в которой не используется протокол BGP.

Развертывание концевых доменов

Рис. 3. Пример развертывания для концевых доменов. Благодаря шлюзу SCION-IP концевые домены поддерживают SCION-соединения, при этом оконечные хосты остаются неизменными.



(a) Подключение заказчика к SCION напрямую

(b) Поддержка SCION с помощью абонентского оборудования (CPE)

Заказчик может использовать SCION двумя разными способами: (1) напрямую через приложения SCION и (2) посредством прозрачной конверсии IP-to-SCION (из IP в SCION). Выгода от непосредственного использования SCION заключается в том, что приложения получают доступ ко всему спектру преимуществ за счет апгрейда операционной системы и приложений функциями поддержки SCION. В краткосрочной перспективе подход (2) является предпочтительным, поскольку он использует шлюз SCION-IP (SIG, SCION-IP-Gateway), который инкапсулирует обычный IP-трафик в пакеты SCION. При этом соответствующий SIG в месте назначения выполняет декапсуляцию (расформирование) пакетов.

Заказчику надо выбрать, станет ли его домен автономной системой (AS) в составе SCION (Случай a), или он подключится к автономной системе провайдера (Случай b).

Случай a: подключение заказчика SCION напрямую

До настоящего времени все организации, осуществившие развертывание, предпочли превратить свой домен в автономную систему, поскольку в этом случае не требуются сложные конфигурации (политики) маршрутизации. Требуемые криптографические сертификаты выдаются центральными AS, а в качестве номеров AS повторно используются сегодняшние, либо при необходимости эти номера выделяются из более крупного 48-битового пространства номеров AS SCION.

Как показано на рис. 3 (a), натуральные хосты SCION (т. е. H1) могут отправлять трафик SCION непосредственно граничному маршрутизатору SCION через существующую инфраструктуру маршрутизации внутри AS. Натуральные хосты SCION оснащены стековыми компонентами SCION, которые позволяют приложениям генерировать пакеты SCION. Компонент плоскости данных (т. е. программа-диспетчер SCION) взаимодействует с протоколами более высокого уровня и осуществляет передачу пакетов. Компонент плоскости управления (т. е. демон SCION) обменивается данными с сервисом управления AS, выполняя поиск и создание пути для приложений от их имени.

Однако очевидно, что многие хосты заказчиков, возможно, не будут первоначально поддерживать SCION. Поэтому шлюз SIG (т. е. SIG1) позволяет традиционным хостам (например, H2 и H3) использовать сеть SCION. Шлюз SIG отвечает за инкапсуляцию/декапсуляцию IP-пакетов, формируя из них (расформировывая) пакеты SCION для того, чтобы обеспечить совместимость SCION и традиционных сетей. Проще всего было бы установить шлюз SIG на входе всего трафика заказчика, но возможен вариант, когда SIG задается как шлюз по умолчанию только для тех хостов, которые должны взаимодействовать со SCION.

После того как шлюз SIG получил исходящий пакет, он прежде всего определяет автономную систему (AS) SCION, к которой относится IP-адрес места назначения. Для реализации отображения между пространством IP-адресов и AS шлюз SIG хранит таблицу ASMap. Если для адреса места назначения не будет найдено соответствие (т. е. он отсутствует в таб-

лице), это означает, что хост места назначения представляет собой традиционную AS. Это приводит к тому, что SIG задает маршрутизатор доступа в качестве следующего хопа и соответствующим образом перенаправляет исходящий пакет. В противном случае SIG получает у CS путь до удаленной AS, инкапсулирует пакет с использованием заголовка SCION и направляет его через граничный маршрутизатор (BR).

Случай b: Поддержка SCION с помощью абонентского оборудования (CPE)

Заказчики, которые приобрели SCION-соединение у ISP, получают абонентское оборудование (CPE), предоставляющее им функциональность SIG, BR и CS. На рис. 3 (b) представлена высокоуровневая топология сети конечного заказчика, поддерживающая SCION с помощью CPE; конечные хосты (например, H4 и H5) настроены таким образом, чтобы SIG2 был шлюзом по умолчанию для выхода в сеть SCION.

Внутренняя маршрутизация трафика SCION

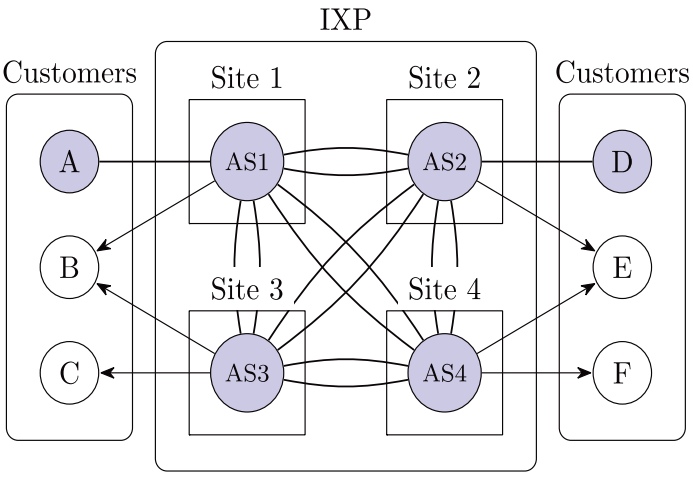
Заказчику не требуется изменять свою инфраструктуру внутренней маршрутизации для того, чтобы передавать пакеты SCION выходному BR; пакеты SCION маршрутизируются через IP-сеть при помощи протокола IGP, например, OSPF или IS-IS. Учитывая тот факт, что внутренние AS считаются заслуживающими доверия, наложение IP поверх маршрутизации первого хопа не приводит к нарушению или ухудшению защитных свойств SCION. Для обмена пакетами SCION с сетью провайдера граничные маршрутизаторы SCION на стороне заказчика напрямую подключаются к граничным маршрутизаторам на стороне провайдера с помощью, например, оптоволоконных кабелей или кросс-соединений уровня 2. Важно отметить, что текущие соединения заказчика с продуктивной сетью SCION представляют собой прямые SCION-соединения, а не совместно используемые соединения IP / SCION, т. е. хотя IP используется для маршрутизации трафика SCION внутри AS, существующие SCION-соединения заказчика не могут направлять обычные IP-пакеты.

Развертывание IXP

Точки обмена интернет-трафиком (IXP) играют в современном Интернете важную роль, поскольку они позволяют ISP, сетям доставки контента (CDN, content delivery network) и другим провайдерам обмениваться между собой трафиком. Как представляется, существуют две модели, которые описывают то, каким образом роль IXP может быть отражена в инфраструктуре SCION: либо в качестве «большого коммутатора», либо посредством раскрытия их внутренней топологии. В рамках модели большого коммутатора точки IXP рассматриваются как крупные коммутаторы L2, находящиеся между несколькими автономными системами SCION, которые служат в качестве заказчиков IXP. В этом случае роль IXP сводится к содействию работе двусторонних (пиринговых) соединений между такими AS. Эта роль абсолютно прозрачна для плоскости управления SCION. В настоящее время компания SwissIX уже использует эту модель, предлагая виртуальную локальную сеть (VLAN) специально для SCION и запрещая протокол BGP. Хотя SCION еще не предлагает прямую поддержку многостороннего пиринга, автоматическую связность автономных систем SCION через IXP можно облегчить при помощи программы согласования SCION Peering Coordinator, аналогичной современному серверу маршрутизации BGP.

На рис. 4 представлена расширенная модель, в рамках которой внутренняя топология IXP раскрыта на плоскости управления SCION. В этом случае IXP управляет собственными автономными системами SCION, при этом каждая AS представляет площадку IXP, а соединения между ними представляют резервные соединения между площадками. Такая расширенная модель позволяет заказчикам IXP использовать присущие SCION свойства многопутевой маршрутизации и быстрого восстановления после отказов для задействования внутренних связей IXP (включая резервные связи) и выбирать пути в зависимости от потребностей приложения (например, с целью оптимизации задержки или пропускной способности через сеть IXP). Эта модель может целиком заменить технологию MPLS, которую IXP сегодня чаще всего используют для управления сетями.

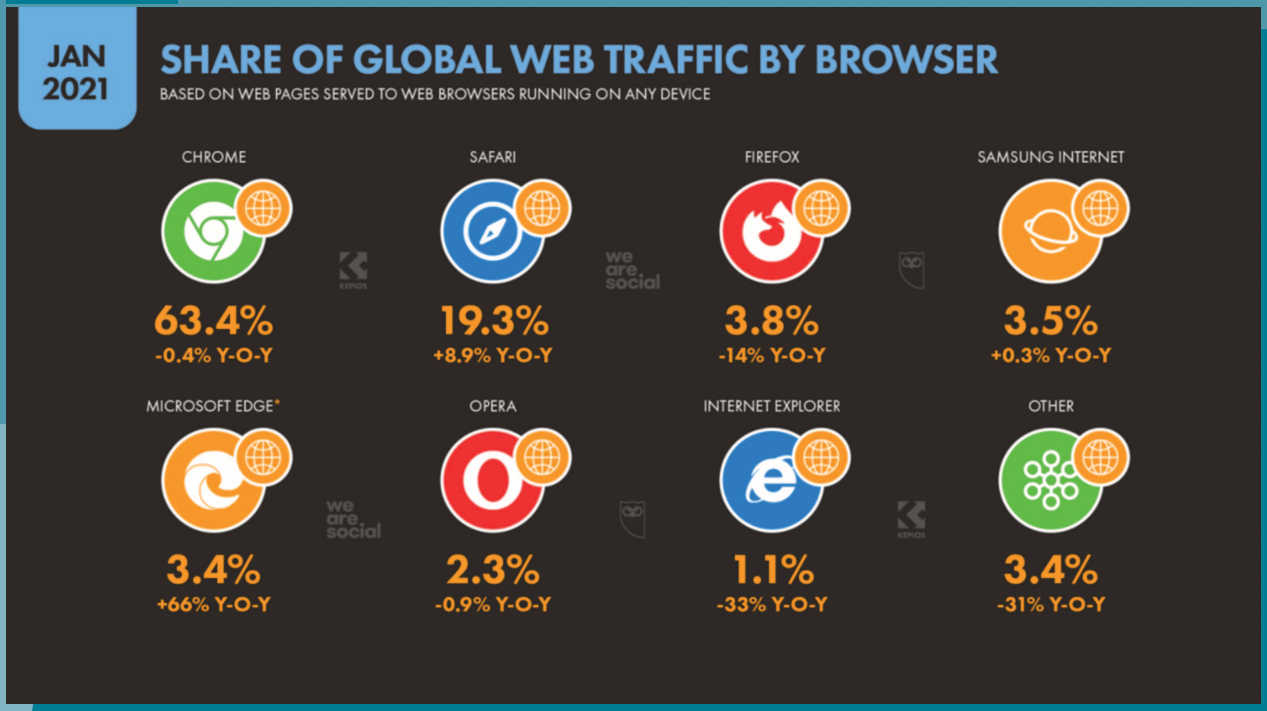
Рис. 4. Развертывание IXP.



Заключение

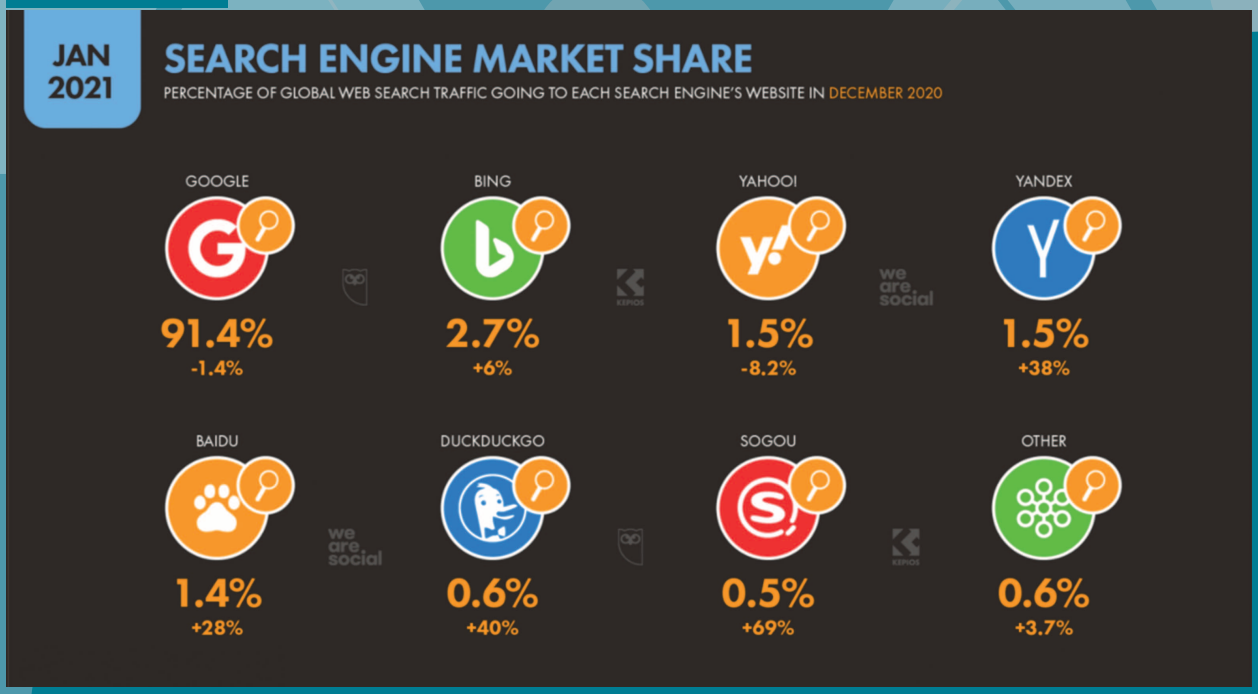
SCION предлагает широкие возможности междоменной многопутевой маршрутизации, максимизируя выгоды от присущего Интернету огромного разнообразия путей. Эта архитектура была разработана с акцентом на обеспечение защиты и высокой доступности для сквозной коммуникации, она открывает уникальные перспективы для будущих инициатив по развитию Интернета. Например, контент-ориентированным сетям требуется механизм маршрутизации, обеспечивающий доступ к источнику данных. SCION может предложить протокол маршрутизации для поддержки такой функциональности. После того, как в сервисной инфраструктуре был найден сервер либо кэш контента был обнаружен в контент-ориентированной архитектуре, двухточечная связь между конечным хостом и сервером обеспечит высокую эффективность обмена данными, поскольку чистая транспортировка данных быстрее, чем серверный или контентный поиск. Аналогичным образом SCION способен предоставить двухточечную коммуникационную матрицу в рамках ориентированной на мобильность архитектуры. Как результат, SCION содержит механизмы, которые дополняют многие ранее предлагавшиеся архитектуры Интернета.

Доля глобального веб-трафика по браузерам



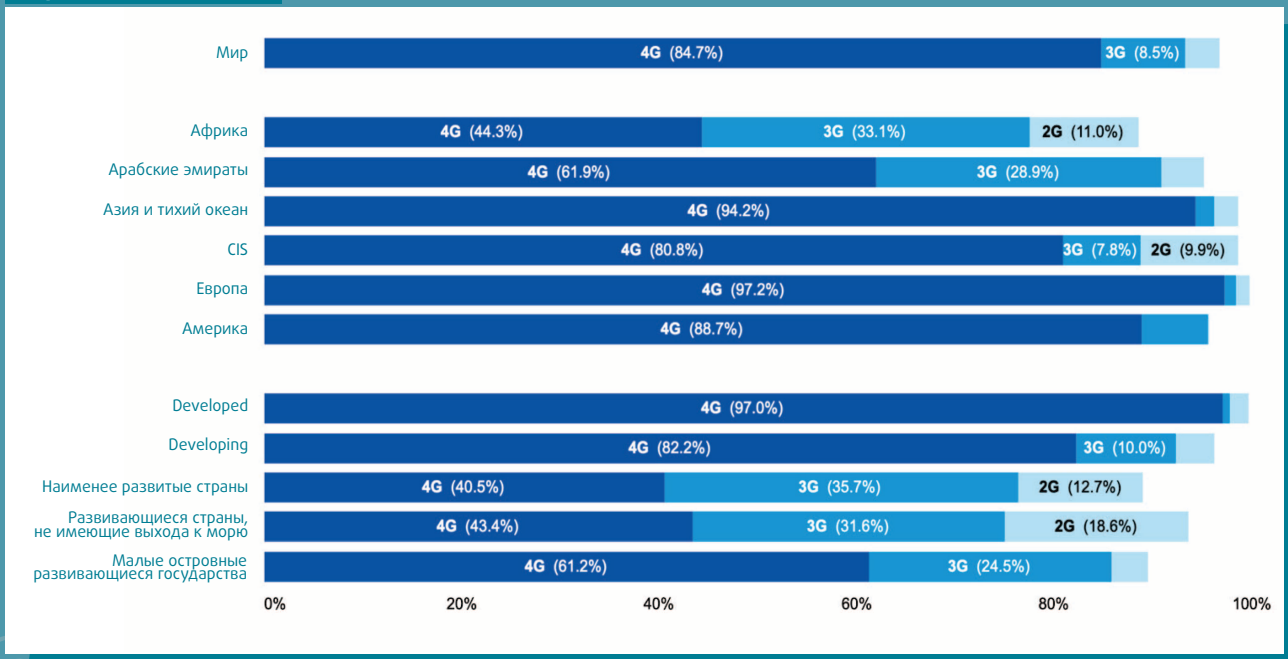
Источник:
DataReportal (2021), "Digital 2021 Global Digital Overview,"
получен из https://datareportal.com/reports/digital-2021-global-overview-report

Доля рынка поисковых систем



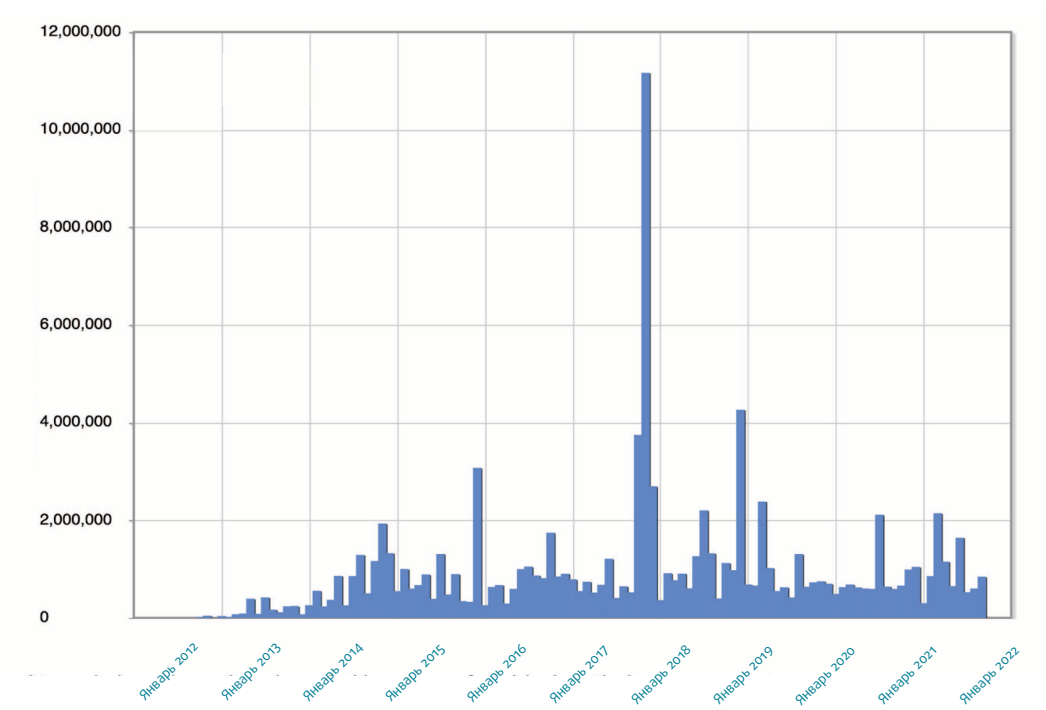
Источник:
DataReportal (2021), "Digital 2021 Global Digital Overview,"
получен из https://datareportal.com/reports/digital-2021-global-overview-report

Использование мобильных технологий в процентах населения



Источник:
МСЭ, получен от
https://public.tableau.com/app/profile/ituint/viz/ITUFactsandFigures2020/ITU2020

Общее количество переданных IP-адресов в результате интер- и интра-РИР трансферов в регионе обслуживания RIPE NCC



Источник:
RIPE NCC, https://www.ripe.net/analyse/statistics/ipv4-monthly-transferred-addresses

Виртуализация сетевых функций

Уильям Стеллингс (William Stallings)

Термин «виртуализация сетевых функций» (NFV, Network Functions Virtualization) родился в результате дискуссий между ведущими сетевыми операторами и операторами мобильной связи о том, как улучшить работу сетей в эпоху огромных объёмов мультимедийных данных. Это обсуждение привело к публикации в 2012 году экспертного доклада по NFV за авторством Группы по отраслевым спецификациям (ISG, Industry Specification Group) NFV, созданной в рамках Европейского института по стандартизации в области электросвязи (ETSI, European Telecommunications Standards Institute).[1]

В своем докладе группа указала, что общей целью NFV является использование стандартных технологий виртуализации для консолидации многочисленных типов сетевого оборудования на базе стандартных в отрасли высокопроизводительных серверов, коммутаторов и систем хранения, которые можно развернуть в центрах обработки данных, сетевых узлах и на площадках конечных пользователей.

В докладе подчёркивается мысль о том, что потребность в новом подходе возникла из-за включения в состав сетей постоянно растущего спектра самых разнообразных аппаратных устройств, а это ведёт к следующим отрицательным последствиям:

- новые сетевые услуги могут требовать установки дополнительных типов аппаратных устройств; однако нахождение для них свободного пространства и дополнительного питания становится всё более трудной задачей;
- новое аппаратное обеспечение влечёт за собой дополнительные капитальные затраты;
- после приобретения новых типов аппаратных устройств операторы сталкиваются с проблемами, связанными с дефицитом персонала, который обладает необходимыми квалификациями для проектирования, интеграции и эксплуатации всё более сложных аппаратных сред;
- срок службы аппаратных устройств быстро заканчивается, что требует повторения цикла «закупка-проектирование-интеграция-развёртывание» при нулевой или минимальной экономической отдаче;
- по мере того как ускоряется развитие инноваций в ответ на потребности всё более активно ориентирующейся на сети IT-среды, необходимость расширения спектра аппаратных платформ препятствует внедрению новых доходных сетевых услуг.

Подход на основе NFV позволяет уйти от зависимости от широкого спектра аппаратных платформ и перейти к использованию небольшого количества стандартизированных типов платформ. При этом для реализации требуемых сетевых функций используются методы виртуализации. В своём докладе группа выражает уверенность в том, что подход на основе NFV применим к любой функции обработки пакетов в плоскости данных и к любой функции плоскости управления в рамках стационарных и мобильных сетевых инфраструктур.

Технология NFV распространяется всё более широко, её используют поставщики услуг связи, поставщики облачных сервисов и даже крупный бизнес, например, банки и компании из индустрии финансовых услуг.[2] Возможно, главным стимулом к такой популярности NFV стало развертывание беспроводных сетей 5G.[3] NFV не только является составной частью 5G, стандарты 5G даже требуют внедрения этой технологии.[4]

Концепции

Виртуализация NFV основана на стандартных технологиях виртуальных машин (VM, Virtual Machine), расширенных на сетевую область. Это довольно значительное отклонение от традиционных подходов к проектированию, развёртыванию и управлению сетевыми услугами. NFV отделяет сетевые функции, например, трансляцию сетевых адресов (NAT, Network Address Translation), межсетевое экранирование, обнаружение вторжений, систему доменных имён (DNS, Domain Name System) и кеширование, от проприетарных аппаратных устройств, позволяя реализовывать эти функции как программное обеспечение в виртуальных машинах.

Технология виртуальных машин обеспечивает миграцию выделенных прикладных серверов и серверов баз данных на готовые коммерческие (COTS, Commercial Off-The-Shelf) серверы x86. Ту же самую технологию можно применить и к подсоединённым к сети устройствам, включая:

- устройства с сетевой функцией: например, коммутаторы, маршрутизаторы, точки доступа к сети и средства углублённой проверки пакетов;
- связанные с сетью вычислительные системы: например, межсетевые экраны, системы обнаружения вторжений и системы управления сетью;
- сетевые хранилища данных: подсоединённые к сети серверы файлов и баз данных.

В традиционных сетях все элементы представляют собой закрытые ящики без возможности совместного использования аппаратных ресурсов. Каждое устройство требует дополнительного аппаратного обеспечения для повышения своей мощности, но эти ресурсы простаивают, когда система работает в условиях неполной загрузки. Однако благодаря NFV сетевые элементы становятся независимыми приложениями, которые гибко развёртываются на единой платформе, состоящей из стандартных серверов, устройств хранения и коммутаторов. В результате удаётся разделить программное и аппаратное обеспечение, а мощность каждого приложения можно увеличить или уменьшить за счёт подключения или отключения виртуальных ресурсов.

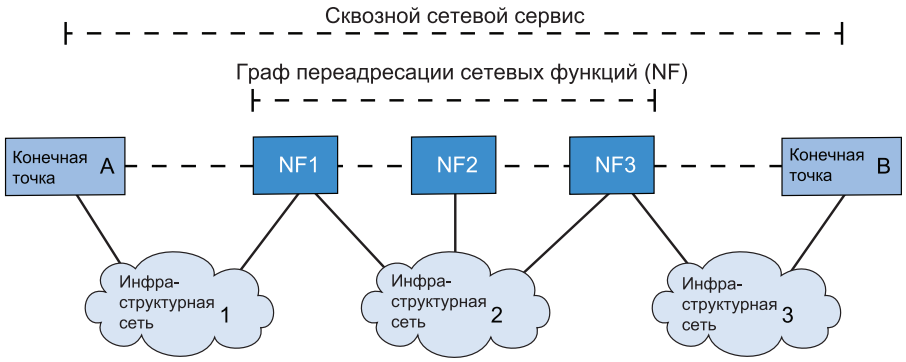
УИЛЬЯМ СТЕЛЛИНГС является независимым консультантом и автором нескольких книг, посвящённых компьютерной безопасности, построению компьютерных сетей и архитектуре компьютеров. Его последняя по времени книга называется «Беспроводные технологии 5G: обстоятельное введение» (5G Wireless: A Comprehensive Introduction, Pearson, 2021). Он ведёт подсайт, посвящённый ресурсам в области теории вычислительных систем и предназначенный для профильных студентов и специалистов. Подсайт располагается по адресу ComputerScienceStudent. com. Кроме того, он входит в редакционную коллегию издания Cryptologia и имеет степень Ph. D. в теории вычислительных систем, полученную в M. I. T. Связаться с автором можно по следующему адресу: wllmst@icloud. com

В качестве иллюстрации можно привести простой пример из документа NFV Architectural Framework (Архитектурная модель NFV). На рис. 1a показана физическая реализация сетевого сервиса. На верхнем уровне сетевой сервис состоит из оконечных узлов, соединённых графом переадресации функциональных блоков сети, которые называются сетевыми функциями (NF, Network Function). В качестве примеров сетевых функций можно привести межсетевые экраны, выравниватели нагрузки и точки доступа к беспроводной сети. В вышеприведённом документе сетевые функции рассматриваются как отдельные физические узлы. Оконечные узлы выходят за пределы спецификаций NFV, к ним относятся любые устройства заказчиков. Поэтому на представленном ниже рисунке оконечный узел A может быть смартфоном, а оконечный узел B — CDN-сервером.

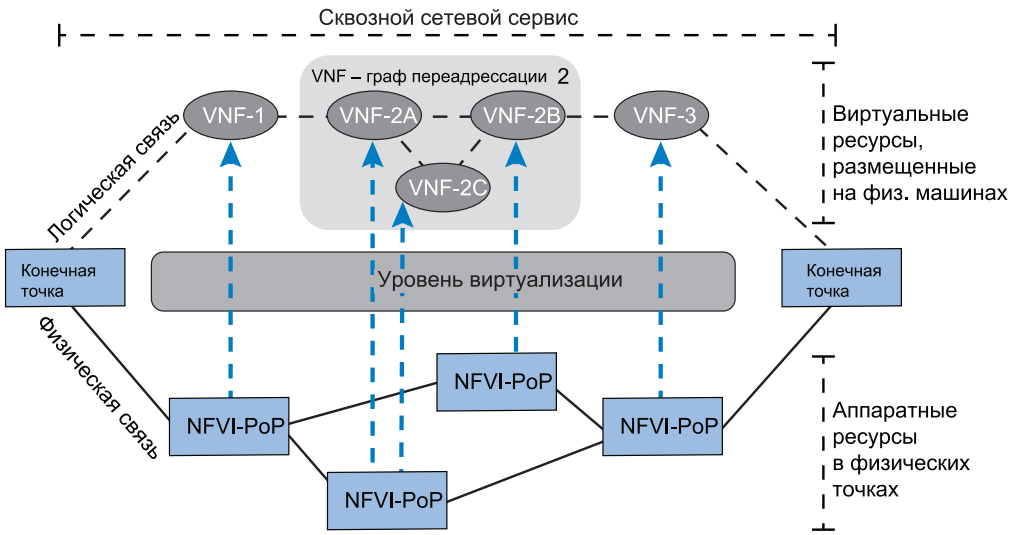
На рис. 1(a) показаны сетевые функции, релевантные для провайдера услуг и заказчика. Соединения между сетевыми функциями и оконечными узлами изображены в виде пунктирных линий, представляющих логические связи. Логические связи реализуются через физические маршруты, проложенные через инфраструктурные сети (проводные или беспроводные).

На рис. 1(b) представлена конфигурация виртуализированного сетевого сервиса, который может быть реализован на базе физической конфигурации, изображённой на рис. 1(a). Виртуальная сетевая функция (VNF, Virtual Network Function) 1 обеспечивает доступ к сети для оконечного узла A, VNF-2 — для оконечного узла B.

Рис. 1. Простой пример конфигурации NFV.



Представление в виде графа для сквозного сетевого сервиса



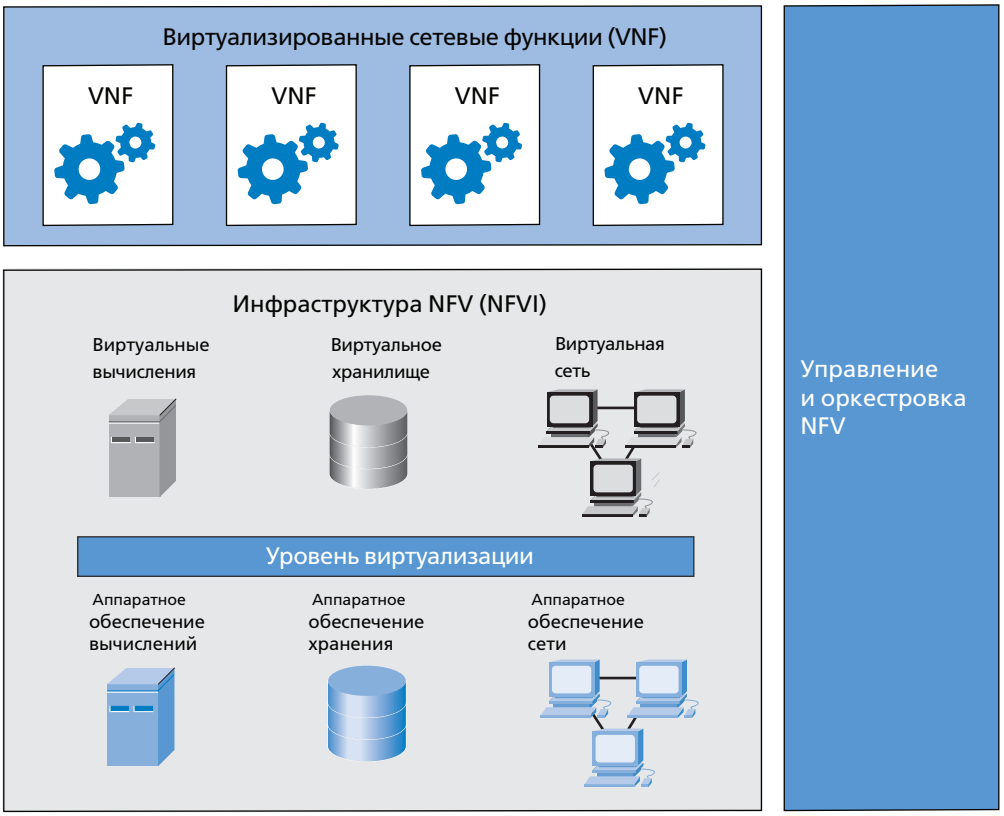
(b) Пример сквозного сетевого сервиса с вложенными графами и функциями виртуальной сети

На рис. 1 также показан вложенный граф переадресации VNF (VNF-FG-2), составленный из других функций VNF (т. е. VNF-2A, VNF-2B и VNF-2C). Все эти функции VNF исполняются как виртуальные машины, работающие на физических машинах, которые называются точками присутствия (PoP, Point of Presence). Такая конфигурация хорошо иллюстрирует несколько важных вопросов. Во-первых, VNF-FG-2 состоит из трёх функций VNF, даже несмотря на то, что в конечном счёте весь трафик внутри VNF-FG-2 проходит между функциями VNF-1 и VNF-3. Причиной является то, что исполняются три отдельные и разные сетевые функции. Например, возможно, требуется, чтобы часть потоков трафика проходила через функцию ограничения типов трафика или формирования трафика, которая реализуется посредством VNF-2C. Поэтому часть потоков может направляться через VNF-2C, тогда как остальной трафик обходит эту функцию сети.

Второе наблюдение заключается в том, что две виртуальные машины в рамках VNF-FG-2 развёрнуты на одной и той же физической машине. Поскольку эти две виртуальные машины выполняют разные функции, они

различаются на уровне виртуального ресурса, но при этом могут исполняться на одной и той же физической машине. Однако такая структура не является обязательной, и в определённый момент времени функция управления сетью может — по причинам, связанным с повышением производительности — провести миграцию одной из виртуальных машин на другую физическую машину. Такое перемещение будет прозрачным на уровне виртуальных ресурсов.

Рис. 2. Высокоуровневая архитектура NVF.



Принципы

Как показывает рис. 1, виртуальные сетевые функции представляют собой строительные блоки, из которых создаются сквозные сетевые сервисы. При создании реальных сетевых сервисов используются три ключевых принципа NFV.

- Формирование сервисных цепочек: Виртуальные сетевые функции являются модульными, при этом каждая из них обладает лишь ограниченной функциональностью (сама по себе). Учитывая конкретный поток трафика и конкретное приложение, провайдер услуг направляет поток через несколько VNF, получая требуемые сетевые функции. Такая практика называется формированием сервисных цепочек.
- Управление и оркестровка (MANO, Management and Orchestration): Эта функциональность позволяет развёртывать экземпляры VNF и управлять их жизненным циклом. В качестве примеров можно привести создание экземпляров VNF, формирование сервисных цепочек VNF, мониторинг, перераспределение, закрытие и биллинг. Кроме того, MANO управляет элементами инфраструктуры NFV.
- Распределённая архитектура: Виртуальная сетевая функция может состоять из одного или нескольких компонентов VNF (VNFC, VNF component), каждый из которых реализует некоторое подмножество функций VNF. Каждый компонент VNFC может быть развёрнут в одном или нескольких экземплярах. При этом такие экземпляры могут быть развёрнуты на отдельных распределённых хостах, обеспечивая масштабируемость и резервирование.

На рис. 2 показана высокоуровневая структура NFV, определённая Группой по отраслевым спецификациям NFV. Эта структура поддерживает реализацию сетевых функций в виде чисто программных VNF. Рис. 2 содержит обзор архитектуры NFV, которая будет более подробно рассмотрена далее.

Структура NFV включает три рабочие области:

- виртуализированные сетевые функции: представляют собой набор VNF, реализованных в виде программного обеспечения, работающего в рамках NFVI;
- инфраструктура NFV (NFVI): выполняет функцию виртуализации для трёх основных категорий устройств, работающих в среде сетевых сервисов: вычислительные устройства, устройства хранения и сетевые устройства;
- MANO: обеспечивает оркестровку и управление жизненным циклом физических и/или программных ресурсов, которые поддерживают виртуализацию инфраструктуры и управление жизненным циклом VNF. Управление и оркестровка NFV уделяет основное внимание всем связанным с виртуализацией задачам управления в рамках структуры NFV.

В документе NFV Architectural Framework указывается, что при развёртывании, эксплуатации, управлении и оркестровке VNF поддерживаются два типа отношений между VNF:

- граф переадресации VNF (VNF-FG): применяется в случаях, когда задана связность сети между VNF, например, цепочка VNF для пути к уровню веб-сервера (межсетевой экран, транслятор сетевых адресов или распределитель нагрузки);
- набор VNF: применяется в случаях, когда не задана связность сети между VNF, например, пул веб-серверов.

Эталонная архитектура NFV

На рис. 3 эталонный структурный шаблон NFV от группы ISG показан более подробно.

Архитектура состоит из четырёх основных блоков.

- Инфраструктура NFV (NFVI): К этому блоку относятся аппаратные и программные ресурсы для создания среды, в которой развёртываются функции VNF. NFVI обеспечи-

вает виртуализацию физических вычислений, хранилищ и сетевых устройств, а также распределяет их в пулах ресурсов.

- VNF/EMS: Этот набор функций VNF реализуется в рамках программного обеспечения для исполнения за счет виртуальных ресурсов вычислений, хранения и сети вместе с набором систем управления, реализующих эти функции.
- Управление и оркестровка NFV (NFV-MANO): Эта структура обеспечивает управление и гармоничное взаимодействие всех ресурсов в среде NFV, включая ресурсы вычислений, сети, хранения и виртуальных машин.
- Системы поддержки эксплуатации и бизнеса (OSS/BSS, Operational and Business Support Systems): Эту систему реализует поставщик услуг NFV.

Кроме того, полезно бывает рассматривать эту архитектуру как состоящую из трёх уровней. Инфраструктура NFVI вместе с менеджером виртуализированной инфраструктуры предоставляют среду виртуальных ресурсов и обеспечивают управление ею и лежащими в её основе физическими ресурсами.

Уровень VNF обеспечивает программную реализацию сетевых функций вместе с системами управления элементами, а также одним или несколькими менеджерами VNF. И наконец, имеется уровень управления, оркестровки и контроля, который состоит из систем OSS/BSS и оркестратора NFV.

Управление и оркестровка NFV

Средства управления и оркестровки NFV включают следующие функциональные блоки:

- оркестратор NFV: отвечает за установку и конфигурирование новых сетевых служб (NS, Network Service) и пакетов VNF; управление жизненным циклом сетевых служб; управление глобальными ресурсами; а также валидацию и авторизацию запросов на предоставление ресурсов NVFI;
- менеджер VNF: контролирует управление жизненным циклом экземпляров VNF;
- менеджер виртуализированной инфраструктуры: контролирует и управляет взаимодействием функции VNF с находящимися в распоряжении менеджера ресурсами вычислений, хранения и сети, а также их виртуализацией.

Рис. 3. Эталонный структурный шаблон NFV.

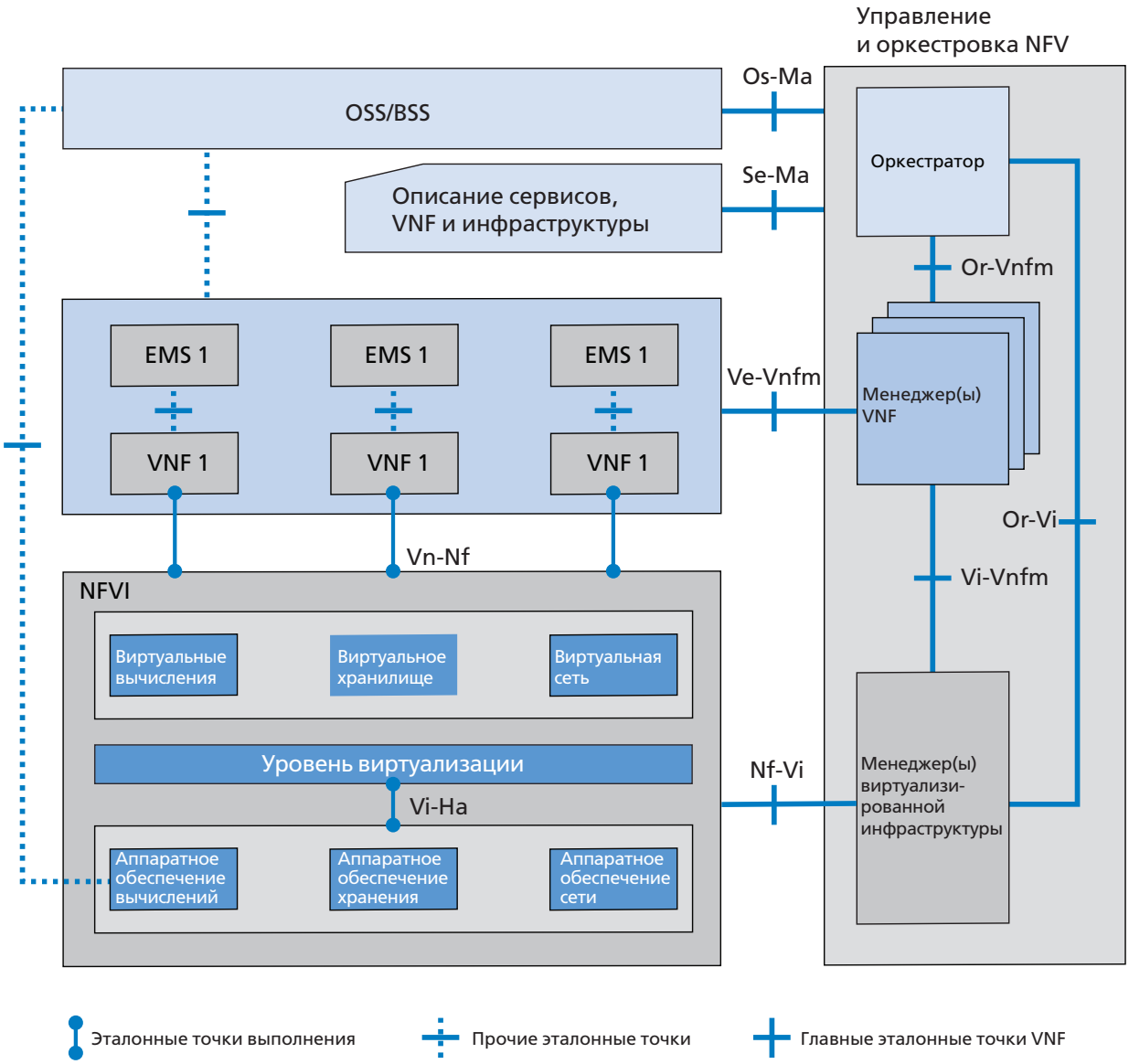
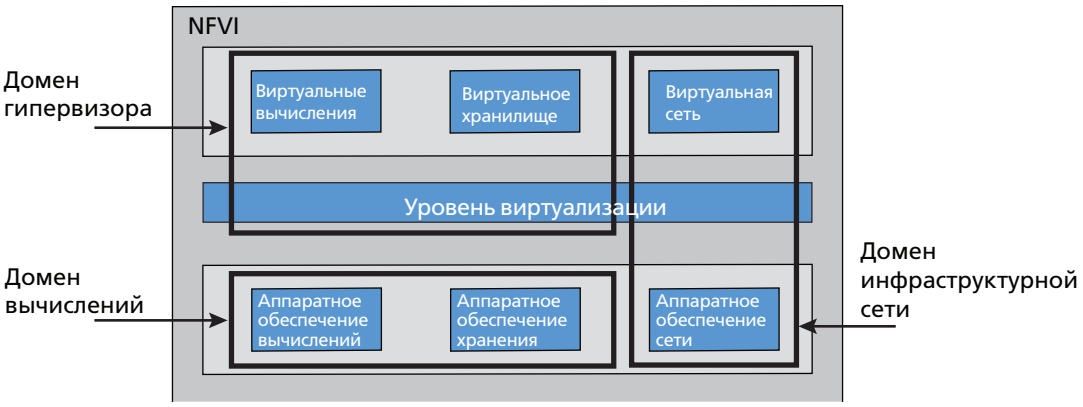


Рис. 4. Домены NFV.



машинами программных устройств, обеспечивая абстракцию аппаратных средств;

- домен инфраструктурной сети: включает все типовые высокопроизводительные коммутаторы, объединённые в составе сети, которые можно конфигурировать для предоставления сервисов инфраструктурной сети.

Инфраструктура NFV

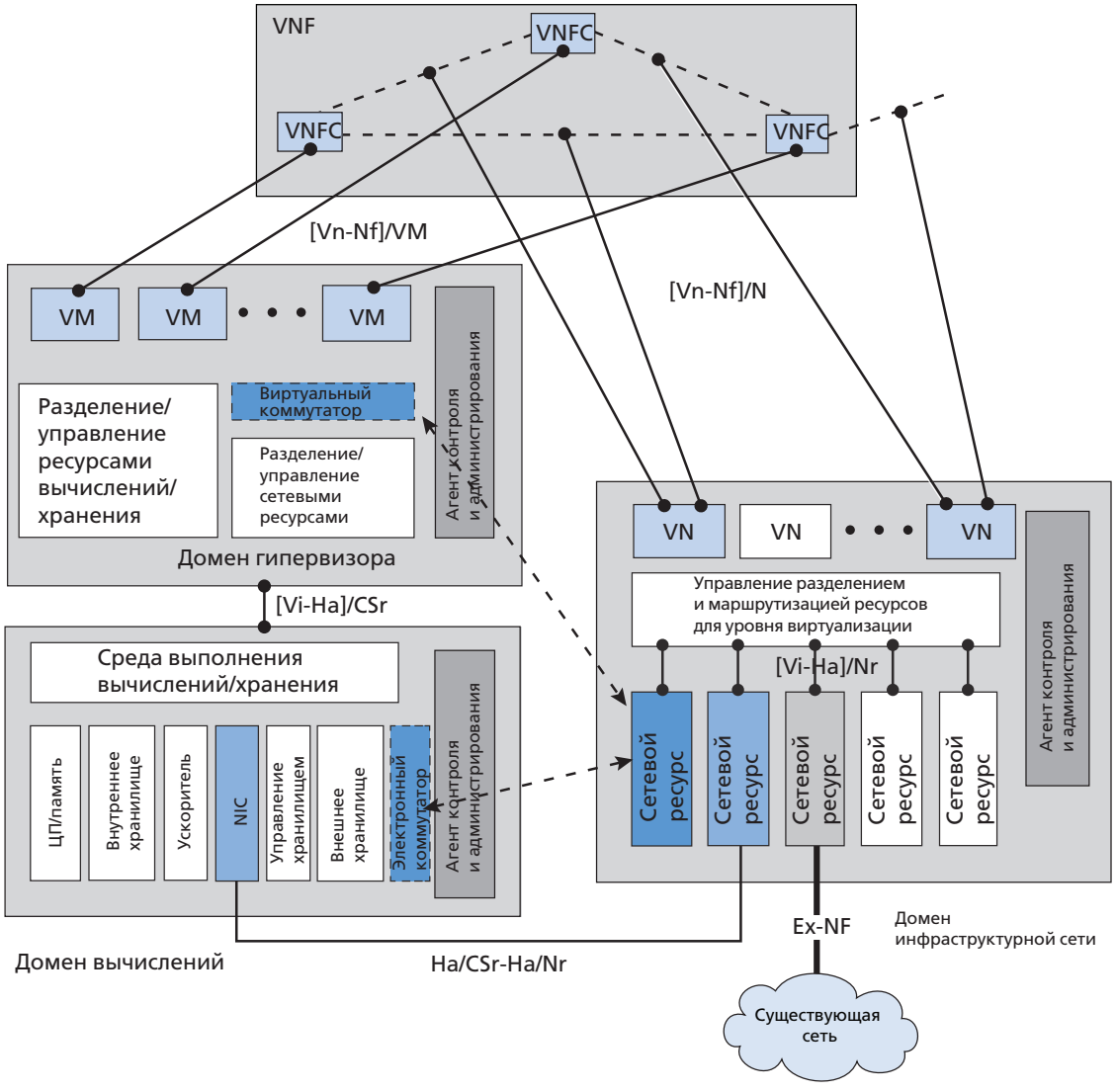
В центре архитектуры NFV находится совокупность ресурсов и функций, которая называется инфраструктурой NFV (NFVI). NFVI включает в себя три домена (рис. 4):

- домен вычислений: предоставляет готовые коммерческие (COTS) высокопроизводительные серверы и системы хранения;
- домен гипервизора: выполняет роль посредника между ресурсами домена вычислений и виртуальными

Логическая структура доменов NFVI

Составленные группой ISG документы для стандартов NFV разъясняют логическую структуру доменов NFVI и их взаимосвязи. Конкретика фактической реализации для элементов этой инфраструктуры будет меняться в ходе реализации как инициатив открытого исходного кода, так и проприетарных проектов. Логическая структура доменов NFVI предоставляет фундамент для такого развития и определяет интерфейсы между главными компонентами, как это показано на рис. 5.

Рис. 5. Логическая структура доменов NFVI.



Домен вычислений

Основные элементы типового домена вычислений могут включать следующее.

- ЦП/память: готовый коммерческий процессор с основной памятью, который исполняет код VNFC.
- Внутреннее хранилище: энергонезависимое запоминающее устройство, установленное в той же структуре аппаратной части, что и процессор, например, флеш-память.
- Ускоритель: функции ускорителя для защиты, сетевых взаимодействий и обработки пакетов.
- Внешнее хранилище с контроллером внешней памяти: доступ к вспомогательным устройствам памяти.
- Сетевая интерфейсная карта (NIC, Network Interface Card): установленная в компьютере плата адаптера, которая обеспечивает физическое соединение с сетью; реализует физическое взаимодействие с доменом инфраструктурной сети.
  - Агент контроля и администрирования: подключается к Менеджеру виртуализированной инфраструктуры (VIM, Virtualized Infrastructure Manager); см. рис. 2.
  - Электронный коммутатор (eswitch): встроенный в сервер коммутатор; функция электронного коммутатора, которая описывается ниже, реализована в домене вычислений, однако функционально она является составной частью домена инфраструктурной сети.
- Среда выполнения вычислений/хранения: среда выполнения, которую сервер или устройство хранения предоставляет для программного обеспечения гипервизора.

Для того, чтобы понять работу электронного коммутатора, необходимо, прежде всего, обратить внимание на то, что, если не вдаваться в детали, функции VNF имеют дело с двумя разными видами рабочих нагрузок: в плоскости управления и в плоскости данных. Рабочие нагрузки в плоскости управления включают работу с протоколами сигнализации и протоколами плоскости управления, как, например, BGP. Как правило, такие нагрузки связаны больше с использованием ресурсов процессора, чем системы ввода/вывода, и сильно не нагружают последнюю. Рабочие нагрузки в плоскости данных связаны с маршрутизацией, коммутацией, ретрансляцией или обработкой полезных нагрузок сетевого трафика. Такие нагрузки могут требовать большой пропускной способности от системы ввода/вывода.

В такой виртуализированной среде, как NFV, весь сетевой трафик VNF проходит через виртуальный коммутатор в домене гипервизора, который требует работы прослойки программного обеспечения, находящейся между виртуализированным ПО VNF и сетевым аппаратным обеспечением хоста. Это может привести к значительному снижению производительности. Электронный коммутатор обеспечивает обход ПО виртуализации и предоставляет функциям VNF путь к сетевой интерфейсной карте через прямой доступ к памяти (DMA). Такой подход ускоряет обработку пакетов, не требуя дополнительных ресурсов процессора.

Домен гипервизора

Домен гипервизора представляет собой программную среду, которая обеспечивает абстрагирование «железа» и реализует такие сервисы, как запуск виртуальной машины, прекращение работы виртуальной машины, а также реализацию политик, масштабирование, динамическую миграцию и высокую доступность. Ниже перечислены основные элементы домена гипервизора.

- Разделение/управление ресурсами вычислений/хранения: управляет этими ресурсами и обеспечивает виртуальным машинам доступ к виртуализированным ресурсам.
- Разделение/управление сетевыми ресурсами: управляет этими ресурсами и обеспечивает виртуальным машинам доступ к виртуализированным ресурсам.
- Управление виртуальными машинами и прикладной программный интерфейс Virtual (API): предоставляет среду выполнения для отдельного экземпляра VNFC.
- Агент контроля и администрирования: подключается к Менеджеру виртуализированной инфраструктуры; см. рис. 3.
- Виртуальный коммутатор (vswitch): функция виртуального коммутатора, которая описывается ниже, реализована в домене гипервизора, однако функционально она является составной частью домена инфраструктурной сети.

Виртуальный коммутатор — это реализованный гипервизором коммутатор Ethernet, который обеспечивает коммутацию виртуальных сетевых интерфейсных карт (NIC), виртуальных машин с картами NIC вычислительного узла. Если две функции VNF расположены на одном и том же физическом сервере, то они соединяются через один и тот же виртуальный коммутатор. Если две функции VNF расположены на разных серверах, то соединение проходит через первый виртуальный коммутатор до карты NIC и затем идёт на внешний коммутатор. Последний перенаправляет соединение на карту NIC требуемого сервера, которая, наконец, устанавливает соединение с внутренним виртуальным коммутатором и затем с целевой функцией VNF.

Домен инфраструктурной сети

Домен инфраструктурной сети (IND, Infrastructure Network Domain) выполняет множество ролей. Он обеспечивает:

- канал связи между компонентами VNFC распределённой функции VNF;
- канал связи между разными функциями VNF;
- канал связи между функциями VNF, а также их оркестровку и управление ими;
- канал связи между компонентами NFVI, а также их оркестровку и управление ими;
- средства для удалённого развёртывания компонентов VNFC;
- средства для соединения с существующей сетью оператора связи.

Очень важно проводить различие между функцией виртуализации, предоставляемой доменом гипервизора, и аналогичной функцией, предоставляемой доменом инфраструктурной сети. При виртуализации в рамках домена гипервизора технология виртуальных машин (VM) используется, чтобы создать среду выполнения для отдельных компонентов VNF.

При виртуализации в домене инфраструктурной сети создаются виртуальные сети для соединения компонентов VNFC друг

с другом и с сетевыми узлами за пределами экосистемы NFV. Последний тип узлов называют функциями физической сети (PNF, Physical Network Function).

Виртуализированные сетевые функции

VNF представляет собой виртуализированную реализацию традиционной сетевой функции. В таблице 1 приведены примеры функций, которые могут быть в будущем подвергнуты виртуализации.

Как уже упоминалось выше, функция VNF состоит из одного или нескольких компонентов VNF (VNFC). Компоненты VNF отдельной функции VNF соединены друг с другом внутри самой функции. Такая внутренняя структура не видна другим функциям VNF или пользователю VNF. Функции VNF обладают очень важным свойством — эластичностью (растяжимостью), что позволяет им поддерживать следующие действия:

- увеличение масштаба (локальное): увеличение мощности за счет добавления ресурсов для отдельной физической или виртуальной машины;
- уменьшение масштаба (локальное): уменьшение мощности за счет удаления ресурсов из отдельной физической или виртуальной машины;
- горизонтальное увеличение масштаба: увеличение мощности за счет добавления дополнительных физических или виртуальных машин;
- горизонтальное уменьшение масштаба: уменьшение мощности за счет удаления физических или виртуальных машин.

Каждая функция VNF имеет связанный с ней параметр эластичности: отсутствие эластичности, только (локальное) увеличение/уменьшение масштаба, только горизонтальное увеличение/уменьшение масштаба или как (локальное) увеличение/уменьшение масштаба, так и горизонтальное увеличение/уменьшение масштаба.

Таблица 1.
Потенциальные сетевые функции для виртуализации

Элемент сети	Функция
Элементы коммутации	Широкополосные сетевые шлюзы, трансляция сетевых адресов операторского класса и маршрутизаторы
Узлы мобильной сети	Реестр собственных абонентов/опорный абонентский сервер, шлюз, узел поддержки GPRS, контроллер радиосети и различные функции Node B (базовой станции нового поколения)
Оборудование в помещениях заказчика	Основные маршрутизаторы и абонентские приставки
Элементы туннельных шлюзов	Шлюзы виртуальной частной сети IPSec/SSL
Анализ трафика	Измерения для углублённой проверки пакетов (DPI) и качества взаимодействия (QoE)
Контроль	Система обеспечения гарантированного качества услуг, мониторинг соглашений об уровне обслуживания (SLA), тестирование и диагностика
Сигнализация	Пограничные контроллеры сеансов и компоненты мультимедийной IP-подсистемы
Плоскость управления/функции доступа	Серверы AAA (аутентификации, авторизации и учёта), платформы тарификации и управления политиками, серверы DHCP
Оптимизация приложений	Сети доставки контента, серверы кеширования, выравниватели нагрузки и ускорители
Безопасность	Межсетевые экраны, антивирусные сканеры, системы обнаружения вторжений и средства защиты от спама
Поддержка общих топологий (а не только коммутационных матриц DC)	Нет

Функция VNF масштабируется за счет масштабирования одного или нескольких VNFC, входящих в её состав. Горизонтальное увеличение/уменьшение масштаба реализуется посредством добавления/удаления экземпляра(ов) VNFC, входящего(их) в состав масштабируемой функции VNF. Увеличение/уменьшение масштаба (локальное) реализуется посредством добавления/удаления ресурсов для существующего экземпляра(ов) VNFC, входящего(их) в состав масштабируемой функции VNF.

Резюме

Технология виртуализации сетевых функций (NFV) позволяет взять на вооружение действенный и не зависящий от конкретного поставщика подход к реализации комплексных сетей с динамическими потребностями. Виртуализация сетевых функций основана на использовании хорошо себя зарекомендовавших технологий, включая виртуальные машины, контейнеры и виртуальные сети. Благодаря растущему спросу со стороны поставщиков услуг 5G и облачных сервисов, а также больших компаний с крупномасштабными внутренними сетями, NFV приобретает всё большую популярность.

Дополнительные материалы

Многие обзорные статьи рассматривают технические аспекты NFV гораздо более подробно.[5, 6, 7, 8] Европейский институт стандартов по телекоммуникациям (ETSI) поддерживает вебсайт NFV, на котором можно найти спецификации ETSI NFV, экспертные доклады, информационно-обучающие пособия, а также целый спектр других документов и ссылок (https://www.etsi.org/technologies/nfv/). Подробное обсуждение роли NFV для услуг 5G можно найти здесь [9].

Список использованной литературы

1. ISG NFV, «Network Functions Virtualization: An Introduction, Benefits, Enablers, Challenges & Call for Action», ISG NFV White Paper, October 2012.
2. Bloomberg L. P., «Network Function Virtualization (NFV) Market Worth $36.3 Billion by 2024», January 15, 2020. https://www. bloomberg. com/press-releases/2020-01-15/ network-function-virtualization-nfv-market-worth- 36-3-billion-by-2024-exclusive-report-by-marketsandmarkets
3. ISG NFV, «Network Operator Perspectives on NFV Priorities for 5G», ISG NFV White Paper, February 2017.
4. ITU-T, «Requirements of the IMT-2020 Network», ITU-T Recommendation Y.3101, April 2018.
5. Mijumbi, R., et al. «Network Function Virtualization: State- of-the-Art and Research Challenges», IEEE Communications Surveys & Tutorials, First Quarter, 2016.
6. Li, Y., and Chen, M. «Software-Defined Network Function Virtualization: A Survey», IEEE Access, December 16, 2016.
7. Li, X.,andQian, C.«A Survey of Network Function Placement». 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016.
8. Veeraraghavan, M., et al. «Network Function Virtualization: A Survey», IEEE Transactions on Communications, November 2017.
9. Stallings, W., 5G Wireless: A Comprehensive Introduction, ISBN-13: 9780136767145, Pearson Education, Inc., 2021.

Network Functions Virtualization, Internet Protocol Journal, Vol. 24, Number 2, July 2021
https://ipj.dreamhosters.com/wp-content/uploads/2021/07/242-ipj.pdf

Масштабирование корневой зоны DNS

Джефф Хьюстон (Geoff Huston)

DNS — исключительно простая система. Ты отправляешь в неё запросы и получаешь ответы. Внутри системы используется столь же простой принцип: получивший запрос DNS-резолвер может не знать ответа, поэтому он, в свою очередь, отправляет запросы глубже в систему и получает ответы. Процесс отправки запроса и получения ответа одинаков и применяется рекуррентно. Всё очень просто.

Однако простоту DNS можно сравнить с простотой шахмат или го. Все они характеризуются ограниченной средой, управляемой небольшим набором строгих правил. Тем не менее, эти игры характеризуются поразительной сложностью.

Простые системы могут обладать очень глубокой сложностью. И это является основной темой исследования формальных систем. Изучение математики в XIX столетии двинулось в сторону головокружительных высот самоанализа. Исследователи пытались ответить на следующий вопрос: Каковы формальные предпосылки, на базе которых была построена вся суперструктура математики? Хорошим примером здесь являются аксиомы Пеано для натуральных чисел. Если взять эти аксиомы и применить к ним операции только из ограниченного и чётко определённого набора, то возможно ли получить каждое известное истинное (доказуемо корректное) утверждение в математике? Попытки ответить на этот вопрос подвигли Уайтхеда и Рассела написать в начале XX столетия фундаментальный трёхтомный труд Principia Mathematica, целью которого было построить всё здание математики, используя только начальные принципы и символическую (математическую) логику. Частично их труд был порождён интересом к логицизму, согласно которому все математические истины являются логическими. При этом математика рассматривалась как «чистая» форма философского исследования, чьи истины не зависели от наблюдателя или естественной системы. Курт Гёдель использовал указанный труд для того, чтобы прощупать границы такого подхода. Его книга «Теоремы о неполноте» (Incompleteness Theorems) содержит две теоремы математической логики, которые демонстрируют врождённые ограничения каждой формальной аксиоматической системы, которая способна смоделировать базовую арифметику. Эти результаты важны как для математической логики, так и для философии математики. Первая теорема о неполноте утверждает, что никакая непротиворечивая система аксиом, чей список теорем может быть составлен при помощи эффективной процедуры, не способна доказать все истины в отношении арифметики натуральных чисел. Для любой такой непротиворечивой формальной системы всегда будут существовать утверждения о натуральных числах, которые являются истинными, но которые нельзя доказать в рамках этой системы. Вторая теорема о неполноте, которая является продолжением первой, показывает, что такая система не может продемонстрировать собственную непротиворечивость.

Учитывая нашу всеобъемлющую веру в управляемые правилами автоматизированные системы, которые в основном заправляют современным цифровым миром, мысль о том, что ограничения такого взгляда на мир были четко установлены Куртом Гёделем в 1931 году, кажется отрезвляющей. Почему я об этом вспомнил? Если перевести работы Гёделя на простой язык, то можно сказать, что любая формальная система, которая обладает достаточной мощностью, чтобы быть полезной, также становится подверженной парадоксам. Или, на ещё более простом языке, любая ограниченная простая система, обладающая достаточной полезностью для выражения составных концепций, также способна на проявление непостижимой сложности. И именно здесь в бой вступает DNS!

Корневая зона

DNS не является словарем какого-либо естественного языка, хотя, когда мы сегодня используем термины вроде «facebook.com» в качестве имени собственного, может произойти смешение двух концепций! DNS представляет собой иерархическое пространство имен. Имена доменов составляются, используя упорядоченную последовательность меток. Такая упорядоченная последовательность меток служит для реализации целого ряда функций, но, возможно, самая полезная из них заключается в том, что её можно использовать в качестве неявной процедуры для трансляции имени домена в связанный с ним атрибут, используя для этого протокол разрешения имен DNS.

Например, я управляю веб-сервером, доступ к которому осуществляется с помощью DNS-имени www. potaroo. net. Если вы укажете это имя в своём браузере (адресной строке браузера), то браузеру сначала потребуется транслировать это имя в IP-адрес, чтобы знать, куда отправлять IP-пакеты для осуществления транзакции с моим сервером. Именно здесь используется структура имени. В данном случае DNS-система отправит корневому серверу запрос на трансляцию имени в соответствующий IP-адрес, а в качестве ответа получит набор серверов имен, которые полномочны, или авторитетны, для зоны «.net». Если запросить любой из этих. net-серверов в отношении того же имени, то в качестве ответа будут получены адреса серверов, которые полномочны для зоны «potaroo. net». Если запросить любой из этих potaroo. net-серверов в отношении того же имени, то в ответ будет прислан искомый IP-адрес. Точно таким же образом можно разложить любое DNS-имя. При

этом само имя определяет порядок для процесса разрешения имени.

Для каждой операции по разрешению DNS-имени существует единая начальная точка: корневая зона. Существует направление научной мысли, которое порицает особое отношение к корневой зоне DNS. Это просто ещё одна зона, подобная любой другой. Набор её авторитетных серверов получает запросы и отвечает на них подобно любой другой зоне. В корневой зоне нет никакой магии и повышенное внимание к ней совершенно необоснованно.

Однако, по моему мнению, это ведет к недооценке важности корневой зоны DNS. Систему DNS можно рассматривать как обширную распределенную базу данных. И действительно, она так обширна, что не существует единой статичной карты, которая идентифицирует каждый авторитетный источник информации и набор точек данных, в отношении которых он полномочен. Вместо этого мы используем процесс динамического обнаружения, в ходе которого сначала DNS-имя направляется с целью обнаружения авторитетного сервера, который располагает данными об имени, которое требуется преобразовать, после чего на этот сервер отправляется соответствующий запрос. Такая система прекрасна тем, что запросы на обнаружение и конечный запрос в каждом случае идентичны.

Однако для всего требуется начальная точка. Рекурсивный преобразователь (резолвер) DNS заранее не знает обо всех авторитетных серверах DNS и никогда не будет знать. Но он знает кое-что другое. IP-адрес по крайней мере одного из корневых серверов. С этой начальной точки всё остальное можно построить в процессе работы. Резолвер может запросить у корневого сервера имена и IP-адреса всех остальных корневых серверов (так называемый подготавливающий запрос, priming query) и сохранить этот ответ в локальном кэше. После того, как преобразователь получит имя для разрешения (преобразования), он начинает с отправки корневому серверу запроса на поиск следующей точки в иерархии делегирования имени и продолжает в том же духе.

Работай так система DNS на самом деле, очевидно, что она буквально расплавилась бы через несколько секунд. Что делает такой подход жизнеспособным, так это локальное кэширование. Резолвер DNS сохраняет ответы в локальном кэше и использует эту локально хранящуюся информацию для ответа на последующие запросы в течение всего срока жизни кэшированной записи. Вероятно поэтому более точное утверждение о роли корневых серверов заключается в том, что каждая операция преобразования DNS начинается с обращения к кэшированному состоянию корневой зоны. Если на запрос нельзя ответить с помощью локального кэша, то запрашивается корневой сервер.

Однако на задворках этого утверждения затаилось неудобное замечание. Если корневые серверы станут недоступными, то прекратит работу вся система DNS. Возможно, во многих отношениях это является театральным преувеличением, поскольку такое событие не повлечет за собой внезапного коллапса системы DNS и остального Интернета вместе с ней. В гипотетической ситуации, когда станут недоступными все экземпляры корневых серверов, резорлверы DNS продолжат работу, используя сохраненную в локальном кэше информацию. Однако по мере истечения срока жизни записей кэша они будут удаляться из локальных преобразователей, поскольку не будет происходить их обновления посредством отправки повторных запросов на корневые серверы. Огни DNS будут постепенно гаснуть по мере превышения лимита времени для кэшированных записей. Именно это отличает корневую зону DNS от любой другой зоны. Она является местом главного поиска для всех остальных зон. Именно поэтому она заслуживает особого внимания.

Благодаря локальному кэшированию серверы корневой зоны не запрашиваются при каждом поиске DNS. Теоретически, корневые серверы должны получать запросы только в случае отсутствия данных в кэше. При относительно небольшой корневой зоне и относительно малом наборе резолверов DNS нагрузка на корневую зону не должна быть значительной. Даже если принять во внимание рост базы пользователей Интернета, нагрузка (в виде запросов) не обязательно должна расти. Если следовать данной теории о работе корневого домена DNS, то именно количество резолверов DNS определяет нагрузку корневых серверов.

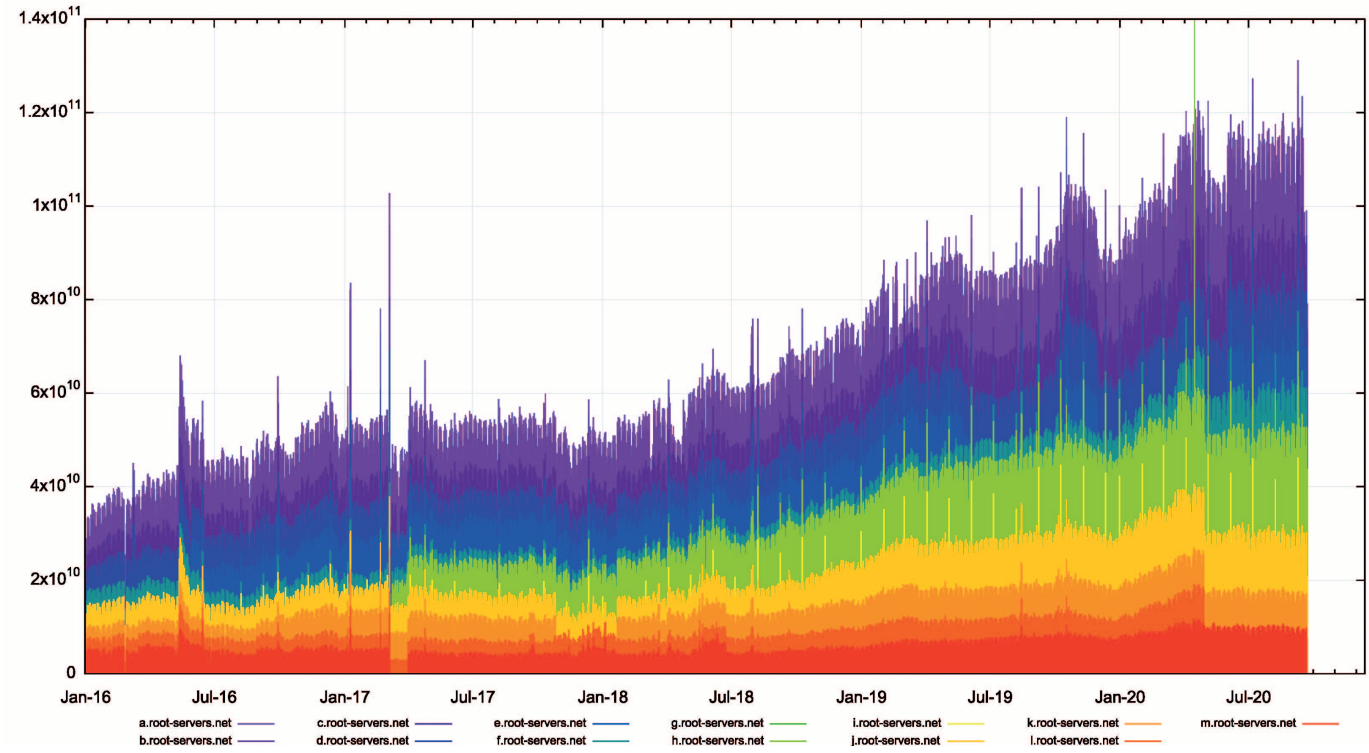
Однако эта теория не выдерживает проверки практикой. Почему же наблюдается непрерывная тенденция роста количества запросов к совокупности корневых серверов? Общее количество запросов в день, зарегистрированное корневыми серверами, показано на рис. 1.

Как представляется, за последние четыре года количество запросов к совокупности корневых серверов увеличилось в три раза. Какие же меры принимаются в ответ на это?

Данные, опубликованные корневыми серверами, используют структуру согласно документу RSSAC002 (https://www.icann.org/en/system/files/files/rssac-002-measurements-root-06jun16-en.pdf) и генерируются независимо большинством операторов корневых серверов. (Термин «большинством» означает, что я не смог найти данные об общем количестве запросов для корней B, E или G и данные о ежедневном количестве кодов ответа для корней A, B, E, F, G или J. Кроме того, нельзя сказать, что такие данные публикуются каждый день.)

Как можно в целом описать корневую службу (https://root-servers.org)? Обескураживающий ответ: как неполную и незаконченную. Можно получить лишь частичную картину того, что происходит в корневой системе, при этом не очень понятно, до какой степени публикуемые данные являются непротиворечивыми по времени, и не ясно, в какой степени они соотносятся с общим массивом данных. Составляют ли публикуемые данные 70% от общего объема? Или 95%? Или что-то в промежутке между этими значениями? Никто не знает. Утверждая, что за последние четыре года количество запросов «как представляется, увеличилось в три раза», я позволил себе значительную вольность при обращении с этим неполным набором данных. Это вызывает сожаление, поскольку без прочного информационного фундамента довольно проблематично выносить важные суждения о характеристиках корневой системы. Например, как повлияло кэширование NSEC на объемы корневых запросов? Или использование локального корневого пространства? Как быстро

Рис. 1. Общее количество запросов к корневым серверам в день (данные RSSAC002).



растет количество запросов? Почему оно растет? Как мы можем на это отреагировать?

Как и с множеством других вещей, с которыми люди сталкиваются в этом мире, мы получаем то, за что заплатили. Корневая служба предоставляется бесплатно, из чистого альтруизма, а не является платной договорной услугой. Поэтому вполне вероятно, что этот искаженный и неполный набор данных представляет собой даже нечто большее, чем можно получить за потраченные деньги!

Масштабирование корневой зоны

Работы по увеличению мощностей корневой зоны никогда не прекращаются. На рис. 1 видно, что в середине 2018 года на большинство корневых серверов подавалось 60 миллиардов запросов в день и это количество возросло до 120 миллиардов в середине 2020 года. Как на это реагируют операторы корневых серверов?

Первый набор ответных реакций на эти проблемы с масштабированием заключался в построении корневых серверов с более высокой сетевой пропускной способностью и увеличенной производительностью. Но поскольку со всей нагрузкой справляются лишь 13 серверов, невозможно обеспечить их масштабирование с той же скоростью, с которой растет Интернет. Потребуется нечто большее. Следующий шаг состоял в переходе от технологии unicast (отправка данных единственному получателю) к технологии anycast (отправка данных ближайшему из группы получателей). Хотя существует лишь 26 уникальных IP-адресов для корневых серверов (13 в протоколе IPv4 и 13 в IPv6), но каждый из обслуживающих их операторов теперь использует технологию anycast для репликации корневого сервиса в разных локациях. Текущее количество инсталляций с корневыми серверами описывается на сайте root-servers.org.

Таблица 1. Инсталляции anycast для корневых серверов (данные на сентябрь 2020 г. — прим. ред.)

Корень	Инсталляции anycast
A	16
B	6
C	10
D	149
E	254
F	242
G	6
H	8
I	64
J	118
K	73
L	147
M	3

В сумме это 1098 площадок, где имеются экземпляры корневых серверов.

Количество серверных систем превышает количество инсталляций, поскольку сегодня обычно задействуют несколько серверных систем в рамках одной инсталляции, а кроме того, компании используют несколько интерфейсных подсистем распределения запросов для распространения входящей нагрузки (в виде запросов) среди многих серверных систем.

Однако даже такой формы распределенной сервисной организации может оказаться недостаточно. Через два года потребуется удвоить мощности корневых сервисов, а ещё через два года понадобится очередное удвоение. И ещё раз, и ещё раз, и ещё раз. Экспоненциальный рост очень трудно выдержать.

Между тем, эта задача, возможно, окажется ещё более сложной и не ограничится простым масштабированием. Необходимо будет подумать о деньгах.

Крупица альтруизма в насквозь коммерциализированном Интернете

Не вызывает сомнений, что используемая корневым сервисом модель является анахронизмом для современного Интернета.

Двенадцать организаций, управляющих экземплярами корневых серверов, делают это без всякой оплаты или компенсации расходов. Когда «Администрация адресного пространства Интернет» (IANA) первый раз регистрировала организации, желающие взять на себя эту роль, Интернет был в основном исследовательским проектом, который лишь делал первые шаги по превращению в глобальную сеть. Выбор операторов корневых серверов был основан на стремлении разместить серверы таким образом, чтобы это размещение соответствовало тогдашнему контингенту пользователей. При этом требовалось обеспечить автономный режим работы без каких-либо обязательств по централизованному финансированию. В то время предполагалось, что эксплуатация корневых серверов не будет финансироваться.

За прошедшие 30 лет Интернет очень сильно поменялся во многих аспектах. Однако один аспект остался неизменным. В нем по-прежнему не существует организованной модели финансирования для корневой службы. Администраторы доменов верхнего уровня, список которых находится в корневой зоне, никак не платят — ни напрямую, ни косвенно — за инфраструктуру, которая поддерживает запросы корневой зоны. Различные резолверы, передающие запросы серверам корневой зоны, также никак за это не платят. Никто ни за что не платит. Эта служба по-прежнему работает из чистой благотворительности.

Совокупные мощности, предоставляемые операторами корневой службы, должны удваиваться приблизительно каждые два года, но это приходится делать без каких-либо общих или запланированных договоренностей о финансировании. И если не произойдёт резких изменений в том, как используется система DNS, это удвоение будет продолжаться. Поэтому со временем задача развертывания новых мощностей, соответствующих растущим нагрузкам, станет всё более накладной.

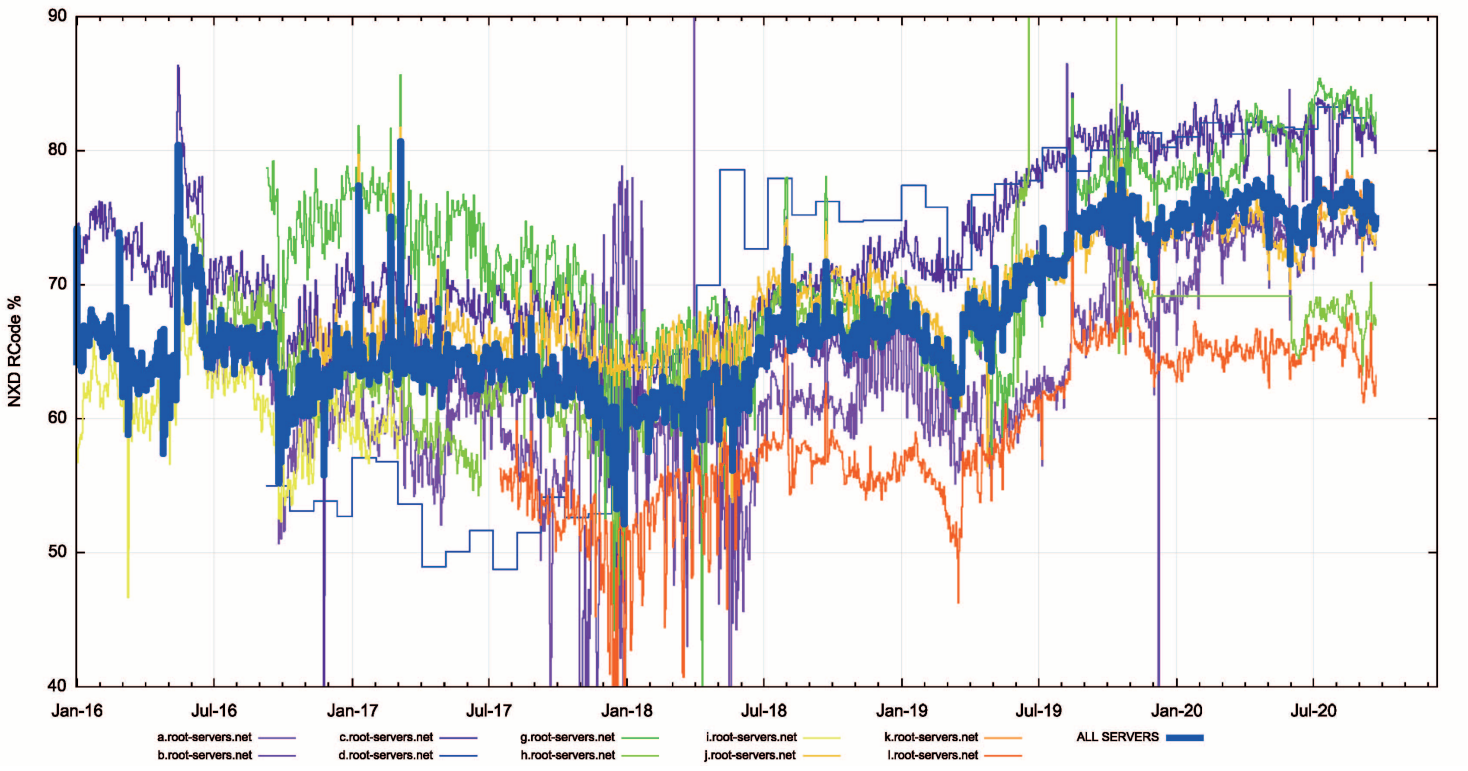
Однако я должен сказать, что эта проблема точно не является непреодолимой и в ближайшее время нас не ждёт связанный с ней кризис. Корневая служба по-прежнему хорошо справляется с текущими нагрузками (в виде запросов) и даже способна поглотить большинство видов направленных против неё DDoS-атак. Между тем, продолжающееся чрезмерное техническое усложнение корневой системы свидетельствует о тенденции использовать грубую силу, что требует непрерывного роста мощностей. Существуют ли другие подходы, позволяющие снизить объем трафика, поступающего на корневые серверы? Что нам известно обо всех этих запросах, направляемых в корневую зону? Возможно ли использование других подходов для снижения этого трафика? Для ответа на эти вопросы может быть полезно взглянуть на трафик запросов, поступающих на корневые серверы.

Корневые запросы

За последние десятилетия было проведено большое число исследований корневой службы и поведения системы DNS. Если корневые серверы были изначально предназначены для использования только в случае отсутствия данных в кэше преобразователей DNS, то происходящее в корневой зоне не полностью соответствует модели промахов кэша. Мы фактически не очень ясно представляем, что происходит в корневой зоне!

Сообщается, что большинство запросов к корневым серверам приводит к ответам NXDOMAIN (отсутствие запрашиваемого имени/метки — прим. ред.). При просмотре опубликованных данных о кодах ответов создаётся впечатление, что примерно 75% запросов корневой зоны приводят к ответам NXDOMAIN (рис. 2), причём в последние пару лет эта пропорция даже выросла.

Рис. 2. Пропорция ответов NXDOMAIN на запросы в корневую зону в день (данные RSSAC002).



Очень любопытный аспект этого поведения заключается в том, что процентная доля запросного трафика, по-видимому, сильно различается (до 20%) для каждой буквы корневой службы. Во многих отношениях корневые серверы намеренно делают идентичными, и такие колебания профилей запросов корневой зоны довольно необычны.

Согласно сообщению Дуэйна Весселса (Duane Wessels) из компании Versign на состоявшейся в июне 2020 года встрече DNSOARC 32, браузер Chrome генерирует три DNS-запроса, состоящих из одной метки длинной от 7 до 15 символов-букв. До февраля 2015 года используемый этим браузером код генерировал только 10-символьные метки, а переход к рандомизированной длине, а также к рандомизированным меткам произошел в версиях кода за февраль 2015. Механизм браузера отправляет такие запросы при его запуске, а также при изменениях локального IP-адреса и локального DNS-сервера.

Мотивы, по которым браузер Google Chrome это делает, довольно очевидны. Многие интернет-провайдеры выполняют в своих DNS-резолверах замену NXDOMAIN, заменяя ответ «no such domain» (такого домена не существует) на синтетический указатель, ведущий на их собственную страницу поиска, что позволяет им монетизировать все подобные опечатки пользователей. Однако Google не очень хорошо воспринимает такую замену NXDOMAIN. Поиск является основным способом размещения рекламы, а реклама — это главный источник доходов Google. Так каким же образом Google Chrome обнаруживает сетевые среды, в которых происходит замена NXDOMAIN? Всё очень просто. Необходимо протестировать систему DNS, используя собственные запросы с одноразовой случайной строкой, и определить таким образом, происходит ли замена NXDOMAIN.

Такое, казалось бы, безобидное зондирование системы DNS должно по идее быть довольно безвредным. Но браузер Chrome сегодня использует множество людей. По многим оценкам, примерно две трети используемых в современном Интернете браузеров являются браузерами Chrome, и это количество ещё больше возрастает, если учесть такие продукты, как Edge, которые основаны на ядре Chrome. Поэтому неудивительно, что согласно упомянутому выше докладу, доля таких зондирующих запросов составляет сегодня до 50% от совокупного трафика корневых серверов (рис. 3).

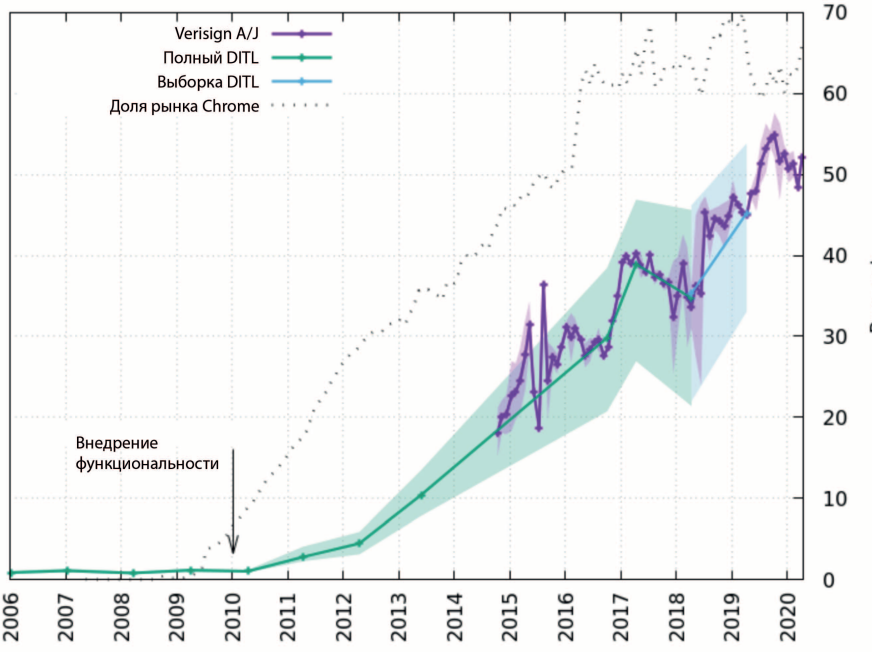
Частично сила Интернета основана на расщеплённом характере его сетевой инфраструктуры, в рамках которой многие поставщики сервисных компонентов работают только в выбранной ими нише, а общее слаживание коллективных усилий оставляется на волю рынка. Никто не возглавляет Интернет. Но эта сила может в некоторых случаях превращаться в слабость, особенно когда возникает потребность в изменении структуры издержек. Решение разработчиков Chrome зондировать корневую зону в поисках замен NXDOMAIN с помощью запросов с одноразовыми метками практически не увеличивает предельные издержки для браузера Chrome или пользователей Chrome. В то же время это решение приводит к значительным расходам операторов корневой службы, учитывая тот факт, что на него приходится половина их совокупной нагрузки (от запросов).

Но даже если принять во внимание смещение издержек и выгод, инструменты для исправления ситуации находятся в руках третьих лиц. Если бы все резолверы и их фронтальные балансировщики нагрузки эффективно выполняли NSEC-кэширование (и, предположительно, валидацию DNSSEC), то эти случайные запросы Chrome к верхнему уровню были бы поглощены кэшем NSEC в рекурсивном преобразователе.

В рамках централизованно координируемой среды издержки и выгоды можно было бы сравнивать напрямую, после чего развертывать экономически эффективные решения. Без такого взаимодействия существует слишком мало стимулов для того, чтобы либо группа, занимающаяся разработкой Chrome в рамках корпорации Google, либо операторы рекурсивных преобразователей потратили своё время и силы на снижение нагрузки от этого класса запросов. Поэтому корневые серверы остаются наедине со своей проблемой, не имея никаких средств, чтобы стимулировать любую другую сторону на её решение.

В то же время будет несправедливым приписывать весь этот трафик запросов исключительно браузеру Chrome. Если посмотреть на то, как ответы NXDOMAIN обрабатываются в системе DNS, можно обнаружить, что система DNS сама является частью проблемы. Мы изучили поведение DNS в тех случаях, когда браузер отправлял в DNS запрос, на который ответом было значение NXDOMAIN, проведя этот тест с участием примерно семи миллионов пользователей со всех концов Интернета (https://www.potaroo.net/ispcol/2019-02/nxd.html). На авторитетных серверах для этого имени домена мы обна-

Рис. 3. Запросы браузера Chrome к корневой зоне. Информация взята из доклада Intranet Redirect Detector or Pseudo Random Subdomain Attack?, Дуэйн Весселс, Verisign, июнь 2020.



https://indico.dns-oarc.net/event/35/contributions/767/attachments/743/1260/OARC32achromium_queries_root.pdf

ружили в среднем 2,2 запроса на каждый исходный запрос браузера, что более чем в два раза превышало наши наивные ожидания. Поэтому вполне возможно, что вклад Chrome составляет только 25% от общей нагрузки на корневые серверы, а инфраструктура резолверов DNS обеспечивает удвоение отправляемого на них количества запросов.

Кроме того, существует дополнительный усиливающий фактор. В системе DNS имеется значительная доля «зомби»-трафика. Проведённое компанией APNIC Labs исследование с использованием динамической метки DNS, которое включало время создания метки, установило, что примерно 25% всех DNS-запросов, полученных нашим авторитетным сервером, были не связаны с первоначальным использованием этой DNS-метки (https://www.potaroo.net/ispcol/2016-03/zombies.pdf). Существует целый ряд причин, по которым «старые» запросы повторно воспроизводятся в системе DNS. Там есть много точек, где запросы фиксируются и регистрируются в журналах, а анализ этих журналов связан, по-видимому, с повторной отправкой запроса. В других случаях создается впечатление, что преобразователь зацикливается в петле программного кода и отправляет огромное количество повторных запросов (миллиарды в течение нескольких недель) для одного и того же имени DNS.

Хотя всё это напрямую не связано с механизмом браузера Chrome, отправляй он эти запросы в более глубокую зону иерархии DNS по сравнению с корневой, это позволило бы значительно уменьшить исходную и добавленную нагрузки на корневую зону. Корневые серверы избавились бы более чем от половины свой текущей запросной нагрузки.

Наряду с этим значительным компонентом трафика существует фактор утечки имен. Многие среды используют локально определяемые зоны DNS для того, чтобы пометить сервисы, и даже когда устройства перемещаются из этих локальных доменов, они по-прежнему запрашивают локально определяемые имена. Запросы в корневую зону для неделегированных зон включают метки верхнего уровня. home, .corp, .local и. mail, а также целый ряд наименований поставщиков CPE (https://www.potaroo.net/presentations/2014-06-24-namecollide.pdf). Делегирование этих меток позволило бы вывести такие запросы из корневой зоны, но одновременно может создать целый ряд проблем безопасности, когда имена, предназначенные для интерпретации в одном сетевом контексте, интерпретируются в другом, что способно привести к удивительным и потенциально угрожающим результатам. Хотя в некоторых отдельных случаях такие утечки запросов в корневую зону можно исправить за счет изменения поведения приложений или устройств в рамках эксплуатационных обновлений, другие случаи поведения укоренились более глубоко и их исправление сопряжено с более значительными трудностями.

Перенаправление запросов

Изменение поведения устройств и приложений с целью использования делегированных доменов даже в частных контекстах с тем, чтобы увести запросы из корневой зоны, представляется одним из возможных подходов к ограничению экспоненциального роста количества запросов в корневую зону. У меня нет большого оптимизма по поводу того, что это окажется очень эффективным, поскольку текущее распределение издержек в системе DNS работает против данного подхода. Использование корневой зоны является самой быстрой и к тому же бесплатной опцией, а корневые серверы очень внимательно относятся к приватности данных. Применение неделегированных частных доменов или случайных имён в случае Chrome — это бесплатная опция, а последующие данные запросов являются в основном частными. Любой альтернативный подход потребует переноса нагрузки на другие серверы, что может привести к переносу издержек на приложение или поставщика устройств. При этом пользоваться корневой зоной можно бесплатно и быстро, и она просто работает! Какие могут быть проблемы? Возможно, потребуется рассмотреть другие подходы. Каким ещё способом можно «отфутболить» эти запросы от системы корневых серверов? Здесь нам могут помочь следующие два подхода.

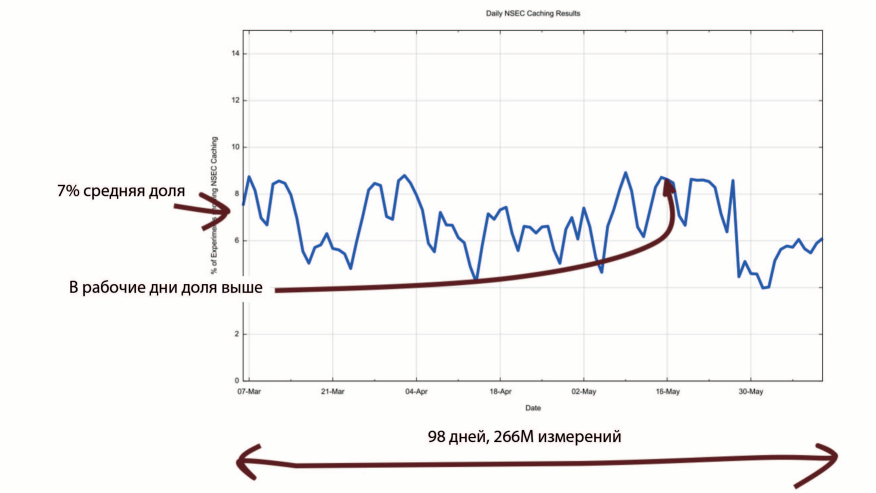
Кэширование NSEC

Первый описывается в документах RFC8198 и представляет собой кэширование NSEC. Если метка верхнего уровня не существует в подписанной с помощью DNSSEC зоне и запрос имеет активный флаг DNSSEC EDNS(0), то ответ NXDOMAIN от корневого сервера включает подписанную запись NSEC, выдающую две метки, которые существуют в корневой зоне и которые «окружают» несуществующую метку. Записи NSEC сообщают нечто большее, чем «эта метка отсутствует в данной зоне». Они указывают, что в зоне не существует каждая метка, которая в лексикографическом смысле расположена между двумя вышеупомянутыми метками. Если резолвер поместит эту запись NSEC в кэш, то он сможет её использовать для ответа на все последующие запросы, содержащие имена в данном диапазоне меток, точно так же, как он обычно использует «положительные» записи кэша.

Если все резолверы будут использовать кэширование NSEC, то количество запросов, получаемых в корневой зоне от резолверов, включая связанные с запросами Chrome, практически сведется к нулю. Поэтому так важно внедрить кэширование NSEC для резолверов. Программа BIND (Berkeley Internet Name Domain) поддерживает эту функцию начиная с версии 9.12. Резолверы Unbound поддерживает её начиная с версии 1.7.0. Резолверы Knot поддерживает её начиная с версии 2.0.0. Тем не менее, количество запросов, поступающих в корневую зону, продолжает расти.

С помощью компании APNIC Labs мы провели измерение кэширования NSEC и отчитались о результатах своей работы на собрании DNS OARC в октябре 2019 года (https://www.potaroo.net/presentations/2019-10-31-oarc-nseccaching.pdf). Результаты оказались не то чтобы обнадёживающими. Мы применили методологию, которая использует два запроса: первый запрос генерировал ответ NXDOMAIN и запись NSEC, если у резолвера для запроса был установлен флаг DNSSEC, после чего ждали две секунды и отправляли в диапазон NSEC второй запрос. Теоретически, мы должны были увидеть только первый, но не второй запрос. Примерно 30% пользователей находятся в сфере действия DNS-резолверов, которые устанавливают в запросах флаг DNSSEC и, по наблюдениям, выполняют валидацию DNSSEC. Поэтому можно было ожидать, что такой эксперимент покажет уровень внедрения кэширования NSEC соответствующий приблизительно 30% пользователей. Однако мы наблюдали гораздо меньшую долю — 7% пользователей (рис. 4).

Рис. 4. Измерение кэширования NSEC, апрель 2019 г.



Возможно, мы слишком рано взялись за этот эксперимент. При измерении минимизации имени запроса в августе 2019 года развертывание этой функции составляло 3%, а через год, в августе 2020, те же измерения показали 18%. Поэтому мы, предположительно, проявили нетерпение и провели измерения слишком рано, а аналогичные результаты для сегодняшнего дня могут быть выше. Кроме того, надо признать, что метод измерения не очень хорошо соответствовал используемой сегодня модели инфраструктуры DNS. В настоящее время значительная доля инфраструктуры DNS-резолверов размещается в «фермах», на которых фронтальный распределитель передаёт каждый входящий запрос на одну из резолверных систем, развернутых на заднем плане. Хотя фронтальный распределитель, возможно, пытается оптимизировать работу кэша для запросов с тем же именем домена и направляет все такие запросы в одну систему, тот же самый подход не обязательно окажется эффективным для диапазонов имен — и запросы с разными метками могут отправляться разным резолверным системам. И наконец, существует вероятность, что кэширование NSEC уже хорошо работает! Доля ответов NXDOMAIN оставалась постоянной на уровне 75% за последние 12 месяцев, а общее количество корневых запросов оставалось относительно неизменным последние четыре месяца. Возможно, кэширование NSEC уже работает. (К сожалению, к этому утверждению применимы все оговорки в отношении качества и непротиворечивости отчетов корневых серверов, и нам остается лишь спекулировать на эту тему в отсутствие надежных данных.) Мы не можем точно знать на основе доступных данных. Кэширование NSEC может уже работать в системе DNS, и продолжающееся внедрение этой технологии в DNS-резолверах может в ближайшие месяцы привести как к снижению доли ответов NXDOMAIN, так и к уменьшению общего количества запросов.

Однако кэширование NSEC — это лишь тактический ответ на проблемы масштабирования корневой зоны, оно не является стратегическим решением. Всё по-прежнему зависит от инфраструктуры корневых серверов и использования запросного метода для распространения контента корневой зоны. Фактически, ничего не меняется в модели корневой службы. Кэширование NSEC лишь позволяет резолверам полноценно использовать информацию, содержащуюся в ответе NSEC. Больше ничего не изменилось.

Локальная корневая зона

Еще одна опция состоит в том, чтобы выйти за пределы модели запрос/ответ при изучении контента корневой зоны и просто загрузить всю корневую зону в рекурсивные резолверы. Идея этого подхода в том, что если в рекурсивный резолвер загружена копия корневой зоны, то он сможет работать автономно от корневых серверов в течение всего срока действия копии контента корневой зоны. Он больше не будет отправлять запросы на корневые серверы. Процедуры, используемые для загрузки локальной корневой зоны, детально задокументированы в RFC8806. При этом необходимо также отметить сервис LocalRoot (https://localroot.isi.edu/), который отправляет сообщения DNS NOTIFY в случае изменений в корневой зоне.

На сегодняшний день у этого подхода есть свои недостатки. Его неудобно использовать. Как узнать, что обслуживаемая зона является подлинной корневой зоной на текущий момент? Да, зона подписана, но подписан не каждый элемент, находящийся в зоне (например, записи NS). Клиенту требуется выполнить валидацию каждой цифровой подписи в зоне, и на сегодня их насчитывается 1376. До тех пор, пока не будет подписана вся корневая зона (это предложение сейчас оформлено в виде проекта для IETF: https://tools.ietf.org/html/draft-ietf-dnsop-dns-zone-digest-09 — этот проект был стандартизован в феврале 2021 и опубликован как RFC8976 (https://datatracker.ietf.org/doc/html/rfc8976) — прим. ред.), никто не может быть уверен в том, что она является подлинной.

В то же время, эта модель может изменить саму природу корневой службы, в отличие от кэширования NSEC. Если есть что-то, что мы в последнее время научились делать исключительно хорошо, то это распределение контента. И действительно, мы сконцентрировали на этой области такие усилия, что весь Интернет кажется не более чем небольшим набором сетей распространения контента (CDN, Content Distribution Network). Если корневая зона будет полностью подписана подписями зоны, что позволит рекурсивному резолверу подтвердить её действительность и актуальность, и затем передана в распределительные системы просто как очередной объект, то инфраструктура CDN идеально подходит для передачи этой информации всей совокупности рекурсивных резолверов. Возможно, если изменить режим управления корневой зоны и генерировать новый файл зоны каждые 24 часа согласно строгому расписанию, то удастся избавиться от всей надстройки, обеспечивающей создание уведомлений. Например, каждая итерация контента корневой зоны публикуется заранее за два часа и остаётся действительной в течение ровно 24 часов.

Опции? Не мелочиться и брать всё!

Корневая служба используется в современном виде, поскольку до сих пор она работала достаточно хорошо. Но это не обязательно должно продолжаться вечно. В настоящее время у нас имеются опции для развития этой службы.

Благодаря перенаправлению части текущей нагрузки на точки делегирования, которые находятся ниже в иерархии доменов, можно добиться значительного снижения нагрузки от корневых запросов.

Научив резолверы лучше использовать подписанные записи NSEC, можно смягчить часть самых неотложных проблем, связанных с дальнейшим масштабированием корневой системы.

Но скорее всего, этого будет недостаточно. Мы можем либо продолжать в том же духе в ожидании коллапса системы и затем попытаться спасти DNS из месива обломков, либо можем исследовать альтернативы и попробовать уйти от модели распространения корневого контента на базе запросов, относясь к корневой зоне как к очередному массиву контента, находящемуся в более крупной экосистеме его распределения. Если нам удастся обеспечить экономичную загрузку текущей копии корневой зоны в каждый рекурсивный резолвер — а в настоящее время это не является сколько-нибудь трудной проблемой, — то у нас, возможно, получится избавиться от проблем масштабирования для системы корневых серверов, чтобы они могли отправлять ещё большее количество ответов «НЕТ!» всё более требовательным клиентам!

"Scaling the Root of the DNS"
(https://www.potaroo.net/ispcol/2020-09/root.html)

Защита пути

А. Робачевский

Незащищенность глобальной системы маршрутизации Интернета известна на протяжении нескольких десятилетий. Существует инструментарий, позволяющий сетям осуществить проверки полученных маршрутов и улучшить уровень «гигиены» в системе. По мере внедрения все более технологичных механизмов проверки все более остро встает задача удостоверения не только маршрута и его источника, но и цепочки сетей, через которые прошел анонс этого маршрута. Решение этой задачи позволит избежать разрушительных аварий.

Вы, наверное, не раз слышали, что протокол маршрутизации BGP, являющийся, так сказать, нервной системой Интернета, был изобретен без особого внимания к безопасности. В то время, в конце 80-х — начале 90-х прошлого века, Интернет находился в опьяняющей фазе стремительного развития базовой инфраструктуры, и требования к масштабированию и простота внедрения являлись основными. Хотя червь Морриса (Morris worm) уже успел наделать шума, все же плохое поведение скорее ожидалось от пользователей оконечных устройств — компьютеров, чем от операторов базовой сетевой инфраструктуры.

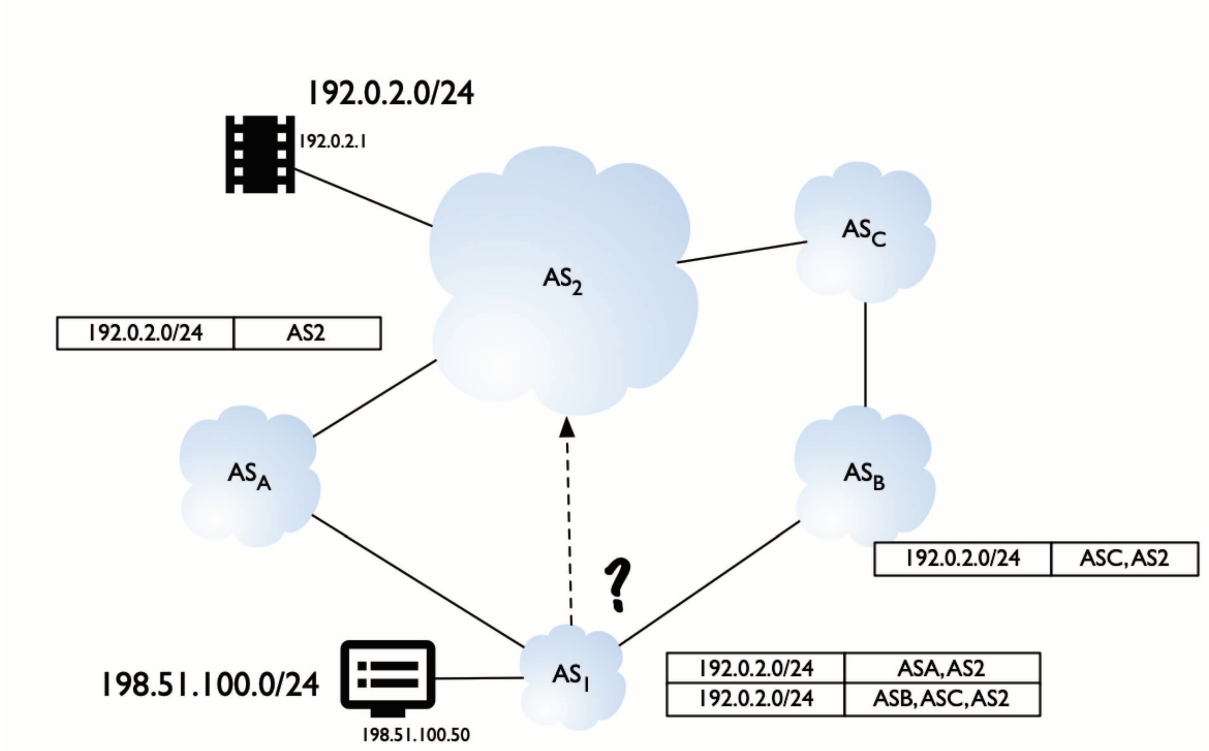
Для того, чтобы понять суть проблемы, давайте кратко остановимся на том, как работает BGP. Согласно модели BGP Интернет состоит из произвольным образом соединенных независимых сетей — так называемых автономных систем (Autonomous System, AS). Другими словами, BGP не накладывает каких-либо требований на топологию связности — сети могут соединяться, образуя иерархическую структуру, или формировать паутину.

Каждая AS обменивается со своими соседями маршрутами или анонсами BGP, содержащими информацию о доступных путях к другим сетям, а именно о последовательности AS, через которые должен быть передан трафик, чтобы достигнуть сеть получателя. Таким образом, каждая AS имеет собственное представление о различных путях, но не о топологии Интернета в целом.

«Маршрут» в терминах BGP называется NLRI (Network Layer Reachability Information, дословно — информация досягаемости сетевого уровня) и содержит префикс и его длину, что необходимо для поддержки CIDR. Например, NLRI /24, 198.51.100 указывает на маршрут к устройствам с IP-адресами в диапазоне 198.51.100.0 — 198.51.100.255.

Помимо NRLI в сообщении BGP (BGP Update) также содержаться т. н. атрибуты — параметры, связанные с анонсированным NLRI, которые используются при выборе «лучшего» маршрута и реализации политики маршрутизации. Атрибут, который имеет отношение к сегодняшнему разговору, это AS_PATH, содержащий список номеров авто-

Рис. 1. Передача анонсов в BGP.



номных систем, через которые было передано сообщение BGP. По мере передачи анонса каждая сеть добавляет свой номер автономной системы. Таким образом, сеть-получатель анонса знает, через какие сети он уже прошел, и может использовать эту информацию при выборе оптимального пути.

Проблема безопасности заключается в том, что эта информация о пути в BGP не защищена и может быть модифицирована любой из сетей в процессе передачи анонса. К чему это может привести?

Во-первых, информация о сети-получателе трафика может быть фальсифицирована. Номер автономной системы, пославший изначальный анонс NLRI и таким образом оповестившей остальных, что она является местом назначения для трафика к этим сетям, стоит первым в атрибуте пути AS_PATH (поскольку AS_PATH растет справа налево, номер автономной системы-получателя самый правый), может быть заменен на номер системы атакующего. Соответственно, трафик к сетям, указанным в NLRI, будет направлен в сеть атакующего с различными последствиями: ложные сервисы сети могут быть выданы за оригинальные или трафик может быть вообще отброшен, что приведет к атаке отказа в услугах. Так, кстати, произошло с сервисом YouTube в 2008 году (https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study). Это — так называемая атака захвата префикса, или prefix hijacking.

Во-вторых, номера других автономных систем в AS_PATH также могут быть фальсифицированы. Это означает, что при выборе лучшего пути автономная система не может доверяться AS_PATH. Для атакующего это дает возможность лучше замаскироваться для атаки, описанной выше, и представиться не в качестве лжесистемы-получателя, а в качестве легитимного провайдера истинной системы-получателя. Для этого ему всего-навсего нужно переписать начало AS_PATH, поставив истинного получателя после номера собственной системы.

Оговорюсь, хотя в примерах выше я использовал термины «атака» и «атакующий», в большинстве случаев такие сбои маршрутизации происходят в результате ошибочной конфигурации. Это, впрочем, не делает последствия менее разрушительными.

Решения

Итак, безопасность и надежность системы маршрутизации во многом зависит от возможности правильного ответа на три вопроса:

1. Является ли префикс, полученный в сообщении BGP, правомерным (т. е. представляющим законно распределенное адресное пространство и право на его использование)?
2. Является ли автономная система-отправитель сообщения BGP правомочным источником префикса?
3. Соответствует ли атрибут AS_PATH, полученный в сообщении BGP, действительному пути, который прошло данное сообщение в сети Интернет?

Для получения ответа на первые два вопроса сетевыми операторами издавна использовались так называемые интернет-регистратуры маршрутизации (IRR, Internet Routing Registry). Суть их сводится к следующему: оператор регистрирует специальные объекты — «route», — которые документируют префиксы, анонсируемые данной автономной системой. Соответственно, обращаясь к регистратуре, другие операторы могут получить ответы на первые два вопроса. Проблема заключается в качестве данных — многие из регистратур не имеют достаточных механизмов контроля, что позволяет регистрировать ложные или хранить устаревшие данные. В результате отсутствует механизм надежной валидации полученных ответов.

Система, построенная на основе RPKI, призвана решить эти проблемы. Фундаментом системы является система открытых ключей (Public Key Infrastructure, PKI), элементами которой являются сертификаты интернет-ресурсов. На основе этих сертификатов держатели ресурсов могут создавать криптографически заверенные объекты, например, ROA (Route Origin Authorization), указывающие на список автономных систем, которые могут являться источником определенного маршрута.

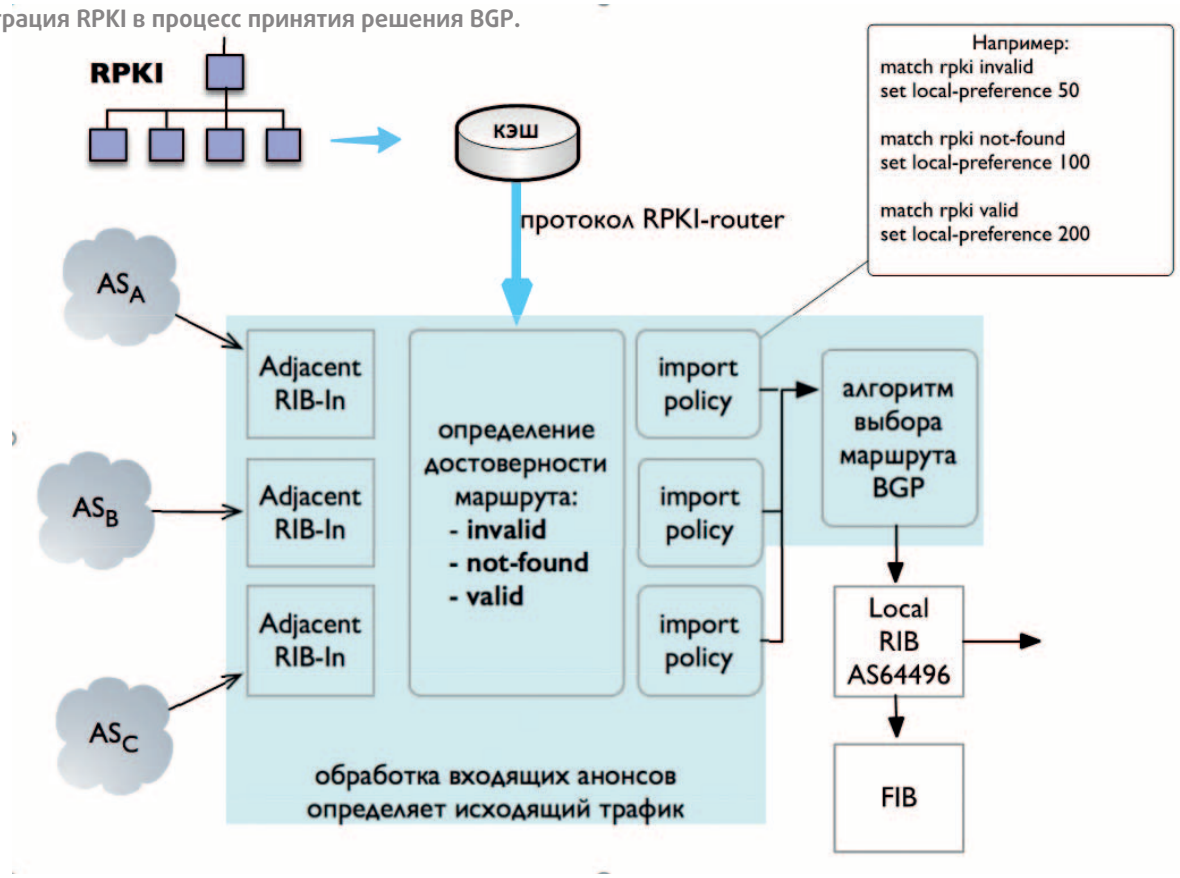
Во-первых, данные о распределенных номерных ресурсах предоставляются в стандартной форме цифровых сертификатов со стандартными расширениями (расширения X.509, собственно, и содержат список ресурсов, привязанных к открытому ключу сертификата). Во-вторых, достоверность и свежесть данных может быть проверена с использованием криптографических средств третьими лицами. Как и в стандартном PKI, для проверки необходима конфигурация доверия только к одному сертификату — т. н. «точке доверия» (Trust Anchor, TA). В-третьих, сертификаты ресурсов могут использоваться их владельцами (держателями адресного пространства) для, например, электронной авторизации определенных автономных систем для анонсирования этого адресного пространства, выполняя, таким образом, функцию объектов «route» традиционных IRR.

Использование ROA возможно как для построения фильтров, так и в качестве дополнительного правила в процессе выбора пути BGP. Логично предположить, что интеграция информации, полученной от системы RPKI, в процесс BGP является более масштабируемым решением.

Архитектура такого решения схематично представлена на рисунке 2. Предполагается, что сервис-провайдер хранит собственную копию всех объектов глобальной системы RPKI, проверяет их достоверность и периодически обновляет. Результирующая база данных содержит только достоверную информацию (достоверный кэш, содержащий т. н. проверенные данные ROA — validated ROA payload, или VRP) и может быть непосредственно использована процессом BGP маршрутизатора.

При получении очередного сообщения BGP маршрутизатор запрашивает базу данных на предмет наличия префиксов, указанных в сообщении BGP. В случае, когда атрибуты NRLI и AS_PATH (первая AC пути — источник анонса) полученного анонса соответствуют какому-либо из VRP в кэше, это означает, что маршрут достоверный, и его состояние маркируется как «valid».

Рис. 2. Интеграция RPKI в процесс принятия решения BGP.



Если же база данных не содержит VRP для указанных префиксов, это означает, что система RPKI не содержит ни одного правомерного объекта ROA для этих префиксов. Причин этому может быть несколько. Например, просроченный сертификат в цепочке проверки подлинности ROA или просто отсутствие ROA как такового. Учитывая, что внедрение данной системы будет происходить постепенно, данная ситуация скорее свидетельствует, что сеть еще не использует преимущества RPKI, и такой маршрут может быть принят при отсутствии более надежного. В этом случае результатом определения достоверности маршрута будет «not-found».

Напротив, если база данных содержит VRP, описывающие префиксы, указанные в анонсе BGP, но не соответствующие автономным системам-отправителям, указанным в атрибуте AS_PATH, возможно, это является свидетельством захвата префикса (prefix hijacking), и такой маршрут следует использовать с большой осторожностью. Скорее всего, его следует отбросить, даже если он единственный. Результат определения достоверности такого маршрута — «invalid».

Описанную процедуру проверки достоверности маршрута с использованием RPKI часто называют ROV (Route Origin Validation, проверка достоверности источника маршрута).

В любом случае, результат ROV является одним из критериев выбора маршрута в BGP, наряду с другими атрибутами BGP: длиной пути (AS_PATH), ORIGIN, MED. В конечном счете интерпретация этой информации является частью политики маршрутизации данной сети. Например, на начальном этапе внедрения RPKI более разумной может быть политика занижения приоритета маршрутов «invalid» с помощью параметра LOCAL_PREF, как показано на рис. 2.

А как же быть с ответом на третий вопрос — как установить, соответствует ли атрибут AS_PATH, полученный в сообщении BGP, действительному пути, который прошло данное сообщение в сети Интернет?

BGPSEC

На сегодняшний день RPKI является наиболее технологичным способом обеспечения безопасности маршрутизации, хотя и он, даже будучи внедрен всеми операторами, не обеспечивает ее полностью. Дело в том, что пока не будет поддержана возможность установления подлинности пути передачи сообщения BGP — AS_PATH, остается возможность обмана.

Например, злоумышленник может утверждать, что автономная система, указанная в ROA, является его клиентом, путем присоединения номера этой АС в атрибут AS_PATH своих анонсов BGP. Другими словами, хотя RPKI не сможет полностью защитить глобальный Интернет от фабрикации адреса отправителя, атак типа Pilosov и YouTube, его внедрение и, главное, применение сопутствующих технологий сервис-провайдерами позволит ограничить вред, наносимый маршрутизационными атаками.

Поэтому в IETF были разработаны стандарты, обеспечивающие возможность проверки криптографической подлинности анонса маршрута и достоверности пути, по которому этот анонс был передан.

Например, представим анонс маршрута 192.168/16 сетью AS 1 сети AS 2 и затем AS 3. По получению этого анонса сеть AS 4 сможет удостовериться, что AS 1 является правомочным

«владельцем» маршрута 192.168/16, который она анонсировала сети AS 2. Сеть AS 2 получила этот маршрут от сети AS 1 и передала его сети AS 3. Сеть AS 3 получила этот маршрут от сети AS 2 и передала его сети AS 4.

Идея решения этой проблемы основана на расширении возможностей самого протокола BGP. Это расширение реализуется с помощью нового атрибута BGP — BGPSEC_Path_Signatures. Атрибут этот содержит последовательность цифровых подписей для каждой сети (точнее — автономной системы), через которую был передан данный анонс маршрута.

Для лучшего понимания, как это работает, представим три сети — AS1, AS2 и AS3 (см. рис. 3). Допустим, что AS1 анонсирует маршрут 192.168/16 сети AS2. При использовании BGPsec этот анонс будет содержать атрибут BGPSEC_Path_Signatures, состоящий из префикса 192.168/16, сети-источника AS1 и сети-пира, которой этот маршрут передан — AS2. Вся эта информация заверена подписью AS1. В свою очередь, когда сеть AS2 передаст этот анонс сети AS2, она также заверит своей подписью информацию, полученную от AS1, плюс номер автономной системы-пира, которой передается анонс, — AS3. Схематично это показано на рисунке 3.

Заметим, что с точки зрения передачи анонсов, от граничных маршрутизаторов требуется только наличие секретного ключа своей автономной системы для подписания атрибута BGPSEC_Path_Signatures.

Если AS3 захочет удостовериться в подлинности полученного анонса, ей придется проделать несколько проверок. Сначала она должна будет убедиться, что AS1 действительно авторизована держателем соответствующего адресного пространства анонсировать этот маршрут. Для этого AS3 проверит наличие и достоверность соответствующего объекта ROA системы. Затем она должна будет последовательно проверить подписи, содержащиеся в атрибуте BGPSEC_Path_Signatures полученного анонса, чтобы убедиться в их подлинности и соответствию пути прохождения анонса.

Для возможности проверки подписей граничных маршрутизаторов BGPSEC определяет дополнительный тип сертификата, связывающего открытый ключ маршрутизатора с номером его автономной системы. Этот сертификат является дочерним по отношению к сертификату RPKI данной автономной системы. Таким образом при проверке анонса проверяющая сторона сможет создать цепочку доверия, используя глобальную систему RPKI.

Более прагматичные решения

Но по мнению многих операторов, внедрение BGPSEC не является реалистичным в обозримом будущем. Производители сетевого оборудования тоже не спешат реализовать эту функциональность.

Во-первых, постепенное внедрение проблематично с экономической точки зрения, так как любая AS на пути, которая не поддерживает BGPSEC, сводит на нет все усилия и преимущества, делая валидацию невозможной. А таких AS на начальном этапе будет очень много. Во-вторых, BGPSEC не защищает от другого вида атак — так называемых утечек маршрута (route leak).

Суть этой атаки можно проиллюстрировать на простом примере. Допустим, сеть AS1 является клиентом двух провайдеров транзита — AS A и AS B, как показано на рис. 4. В случае, если этот клиент реанонсирует маршрут к Google Public DNS (8.8.8.0/24), полученный от AS B, другому провайдеру — сети AS A, а последняя примет его, то произойдет утечка маршрута. В результате весь трафик клиентов AS A к Google будет направлен через клиентскую сеть AS1, вероятнее всего, с катастрофическими последствиями для последней.

Рис. 3. Схема работы BGPSEC.

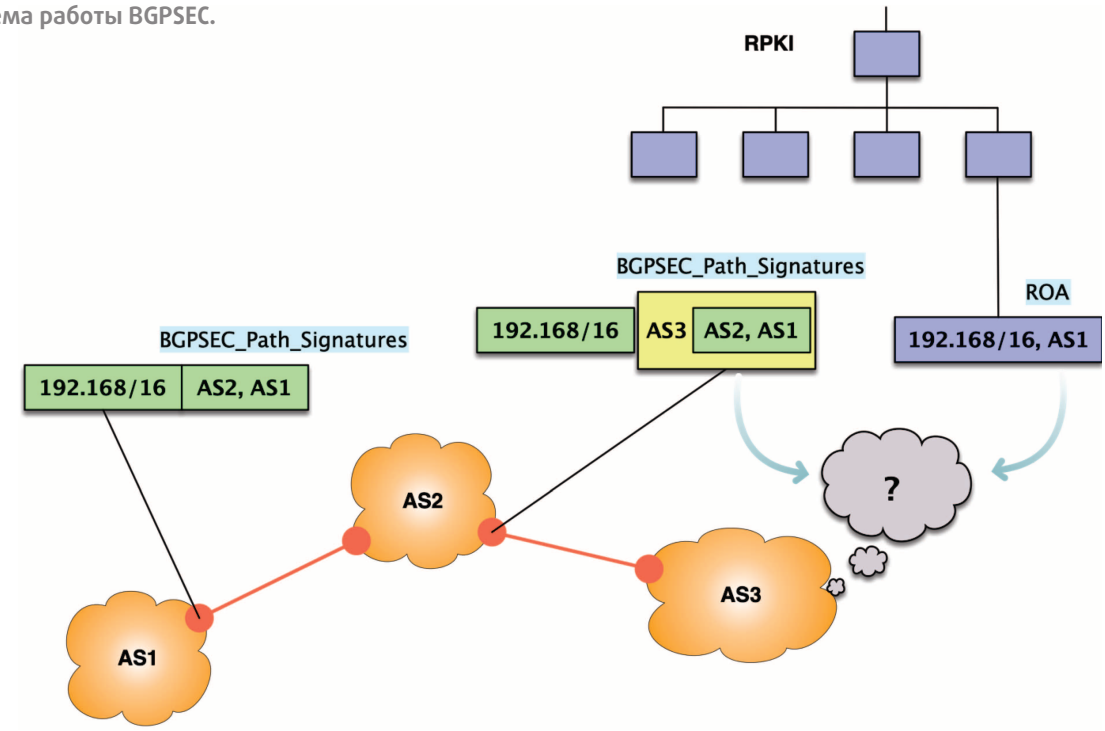
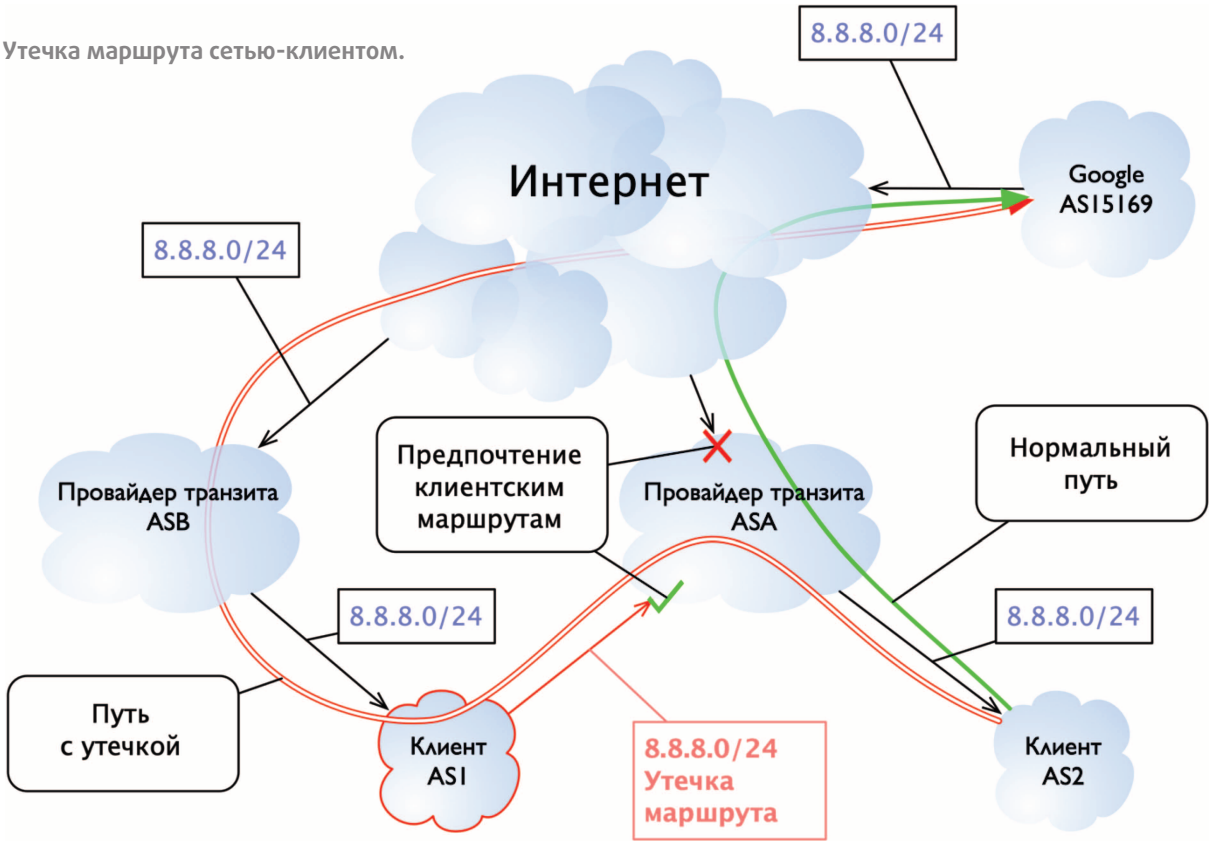


Рис. 4. Утечка маршрута сетью-клиентом.



Без дополнительных проверок со стороны сети AS A так и произойдет, поскольку типичная политика маршрутизации предполагает, что маршруты, полученные от клиентов, имеют предпочтение. При этом, конечно, политика предполагает, что клиент анонсирует только свои собственные сети, а не чужие сети где-то в Интернете, о которых он узнал от другого провайдера. Другими словами, в данном случае мы имеем дело с нарушением политики, а не манипуляцией пути. BGPSEC в данной ситуации бессилен.

Но если на BGPSEC рассчитывать не приходится, какие возможности улучшения защищенности маршрутизации есть в распоряжении сетевых операторов?

Peer-lock

Peer-lock (peer-locking) — это механизм, предложенный Джобом Сняйдерсом (Job Snijders, в то время работавший в NTT), обеспечивающий определенную защиту от утечек маршрутов, поступающих от пиров. В отличие от утечки, вызванной сетью-клиентом, как показано на рис. 4, утечки такого типа происходят в результате нарушения пиринговой политики — пиры должны анонсировать только собственные сети и сети своих клиентов. Если пир анонсирует сети, полученные от других пиров, — это приводит к утечке маршрута.

Механизм peer-lock основан на активной координации и требует кооперации от сети-пира, которая желает стать «защищенной» («protected ASN»). В самом простом варианте анонсы, включающие эту AS, позволены только через прямое пиринговое соединение. Анонсы, содержащие эту AS, но полученные от других пиров, будут отброшены.

Схема работы peer-lock показана на рисунке 5. Сеть NTT является провайдером, обеспечивающим механизм. Защищенная сеть «peer A» указывает на возможность альтернативного транзита через сеть «peer B». В этом случае анонсы, содержащие B в пути, будут приняты NTT только непосредственно от A или от B. Анонс с сетью B, полученный от сети C, будет отброшен. Таким образом, даже если сети A и C обмениваются маршрутами в режиме пиринга, peer-lock предотвратит возможную утечку маршрута через C.

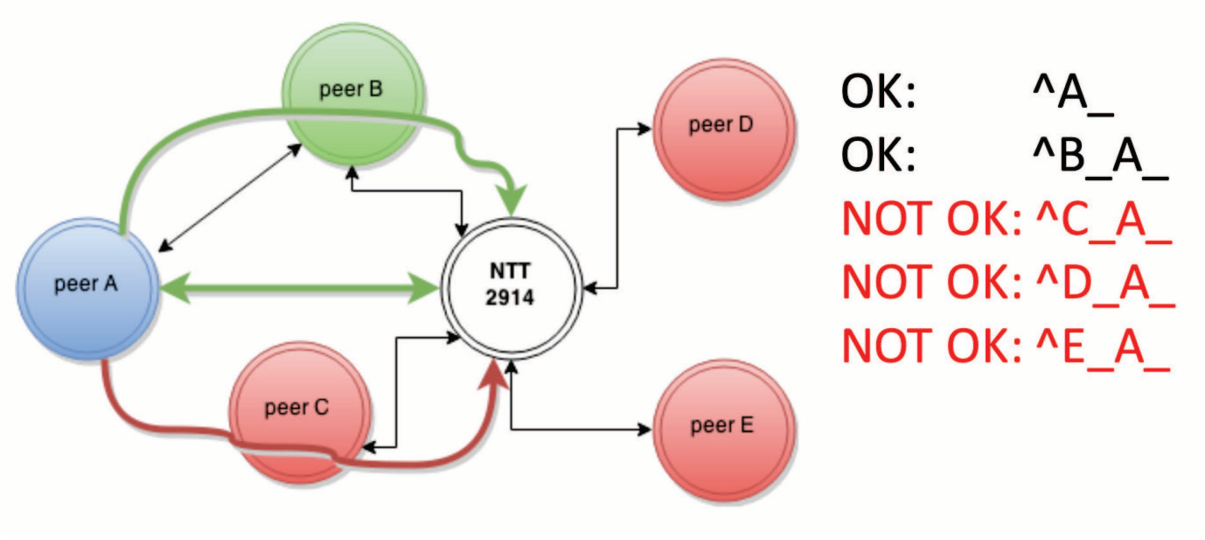
Механизм может быть адаптирован с учетом географической распределённости сетей, более подробное описание доступно здесь — https://instituut.net/~job/peerlock_manual.pdf.

Была также предпринята попытка расширить и автоматизировать механизм с использованием атрибута community BGP, https://datatracker.ietf.org/doc/draft-heitz-idr-route-leak-community/, но дальше изначального предложения дело не пошло. Некоторые из этих идей были использованы в другом предложении, https://datatracker.ietf.org/doc/draft-ietf-grow-route-leak-detection-mitigation, работа над которым продолжается в IETF.

ASPA

ASPA, сокращенное от Autonomous System Provider Authorization, или авторизация провайдеров автономной системы, позволяет автономной системе указать ее непосредственных провайдеров транзита. Подход основан на регистрации

Рис. 5. Механизм работы peer-lock.



Источник: Job Snijders, https://archive.nanog.org/sites/default/files/Snijders_Everyday_Practical_Bgp.pdf

объектов ASPA, криптографически сертифицированных с помощью системы RPKI.

Согласно интернет-драфту «Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization» (https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/) ASPA — это объект с цифровой подписью, который связывает для выбранного адресного пространства AFI (например, IPv4 или IPv6) набор номеров AS провайдеров с номером AS клиента (с точки зрения анонсов BGP, а не бизнеса) и подписывается владельцем AS клиента. ASPA подтверждает, что владелец клиентской AS (CAS) авторизовал набор провайдеров AS (Set of Provider ASes, SPAS) для дальнейшего анонсирования сетей клиента, например, провайдерам выше по потоку или пирам.

В этом смысле механизм похож на только что рассмотренный нами peer-lock. Однако peer-lock трудно автоматизировать, и информация о возможных транзитных провайдерах предназначена для конкретной сети, реализующей peer-lock, а не является частью глобального репозитория, как это предполагается в ASPA.

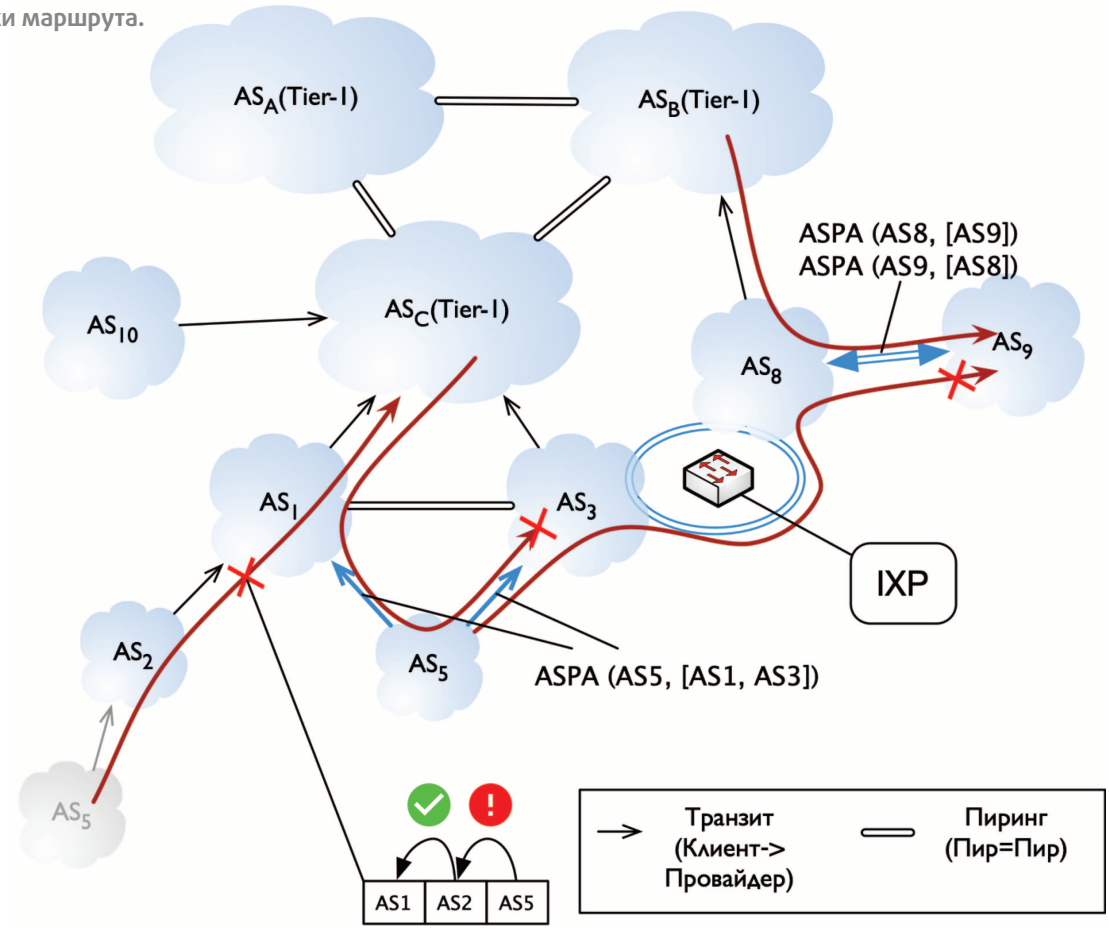
В отличие от BGPSEC, который позволяет проверить всю цепочку пути анонса, ASPA позволяет определить валидность фрагментов пути. Процедура проверки сводится к следующему, при этом предполагается, что проверяющая сторона, например, сеть, осуществляющая фильтрацию неверных анонсов, имеет доступ к кэшу всех криптографически правильных объектов ASPA. Допустим, проверяющей стороне требуется проверить валидность фрагмента пути AS_PATH (AS1, AS2, AFI), а именно предположения, что в случае, если AS1 является клиентской AS, AS2 является законным провайдером транзита для адресного пространства AFI.

1. Проверяющая сторона запрашивает из кэша все объекты ASPA, у которых CAS имеет значение AS1. Объединенное множество всех SPAS является потенциальными провайдерами.
2. В случае, если это множество пусто, проверка заканчивается с результатом «Unknown» (Неизвестно).
3. Если AS2 является членом этого множества, проверка заканчивается с результатом «Valid» (Верно).
4. В противном случае проверка заканчивается с результатом «Invalid» (Неверно).

Как уже обсуждалось, одной из задач защиты пути является предотвратить так называемые замаскированные захваты маршрута, когда атакующий представляется провайдером атакуемой системы. Так, на рис. 6 AS2 может модифицировать AS_PATH анонсов сетей AS5 провайдеру AS1, добавив AS5 в качестве клиента. Проверка с помощью ROA (ROV) в этом случае не поможет, поскольку формально AS5 является источником анонсированных маршрутов. Хотя такой маршрут является менее «конкурентоспособным» в силу увеличенной длины, для многих сетей он может все же являться лучшим маршрутом, что приведет к успешной атаке.

Если же AS5 зарегистрирует своих транзитных провайдеров с помощью ASPA (AS5, [AS1, AS3]), атакующему будет гораздо сложнее представиться провайдером AS5 — фрагмент пути (AS2, AS5) будет отмечен как неверный в процессе проверки ASPA (см. рис. 6). Чем больше фрагментов пути

Рис. 6. ASPA позволяет предотвратить замаскированные захваты и утечки маршрута.



будут зарегистрированы с помощью ASPA, тем меньше шансы у атакующего провести успешный захват маршрута.

Поскольку ASPA указывает на отношения между сетями (клиент-провайдер) и связанную с ними стандартную политику маршрутизации, этот механизм можно использовать для обнаружения утечек маршрутов. Так, AS3 сможет установить, если AS5 «протекла» с маршрутами, полученными от другого провайдера транзита AS1, а AS9 сможет остановить утечку маршрутов через последовательных пиров. Эти примеры приведены на рис. 6.

Важным свойством ASPA является то, что выгоды от его использования растут пропорционально масштабу внедрения этой технологии. В отличие от BGPSEC, который требует значительного, если не тотального внедрения, прежде чем будет получен ощутимый эффект.

* * *

Система маршрутизации в Интернете слишком сложна, чтобы можно было рассчитывать на простые решения. Ни один из рассмотренных нами подходов не является панацеей. Это — строительные блоки, из которых создаются конкретные решения конкретными операторами.

Так, например, многие операторы используют ROV и фильтруют маршруты с результатом «Invalid». Более строгий контроль за анонсами, получаемыми от клиентских сетей, всегда полезен. Для одноуровневых клиентских конов хорошо работают фильтры, явно указывающие клиентские сети.

Для более сложных топологий определенный контроль правильности пути поможет избежать серьезных происшествий. Наиболее простой способ — следить за так называемыми основными сетями или сетями первого уровня (Tier-1).[1] Эти сети являются «ядром» Интернета, они не являются ничьим клиентом и обмениваются трафиком между собой в режиме равноправного пиринга. Поэтому эти сети не могут присутствовать в пути маршрутов, полученных от клиентской сети. В более общем случае в пути полученного маршрута не должно присутствовать более двух таких сетей, и они должны следовать друг за другом. Несоблюдение этого условия является признаком утечки маршрута.

Многие «строительные блоки» защищённой маршрутизации доступны сегодня, а новые уже на подходе. Слово за операторами!

[1] Эти номера автономных систем считаются «ядром» Интернета : 7018, 174, 209, 3320, 3257, 286, 3356, 3549, 2914, 5511, 1239, 6453, 6762, 12956, 1299, 701, 2828, 6461. https://ru.wikipedia.org/wiki/Tier-1-операторы

Онлайн-платформы как структурный элемент цифровой экономики: о концептуальных регуляторных инициативах Европейского Союза

Мадина Касенова

Сбой в работе Facebook 4 октября 2021 года еще раз продемонстрировал, насколько важным структурным элементом цифровой экономики государств являются онлайн-платформы. Расширяющееся в трансграничном масштабе применение цифровых технологий обусловливает совершенствование и стремительные новации бизнес-моделей, усиливает роль действующих десятков тысяч онлайн-платформ. При этом на современных цифровых рынках лишь несколько онлайн-платформ крупнейших технологических компаний (таких как Google, Apple, Facebook, Amazon и др.) занимают ключевые позиции и устойчивое положение. Технологические, экономические и социальные возможности таких компаний (потенциально глобальных по своим свойствам) позволяют им зачастую выступать в качестве посредников при осуществлении большинства транзакций для широкого круга пользователей, а также создавать на базе своих онлайн-платформ собственные конгломератные экосистемы цифровых услуг.

При этом порядок и условия предоставления услуг пользователям таких крупных онлайн-платформ зиждется на установленных самими платформами нормативных правилах и практиках, позволяющих, в частности, осуществлять онлайн трекинг-контроль и профилирование конечных пользователей, расширяя возможности платформы для целевой онлайн-рекламы, что само по себе не обязательно является проблемным моментом, но неизбежно сопрягается с необходимостью обеспечения того, чтобы такого рода деятельность осуществлялась контролируемым и прозрачным образом с точки зрения конфиденциальности, правомерного использования данных и защиты потребителей. Сложившаяся ситуация приводит к существенному контролю доступа к цифровым рынкам со стороны крупных онлайн-платформ, ставит в «зависимость» от них (зачастую значительную) иные онлайн-платформы (мелкого и среднего бизнеса, стартапы и проч.), а это не может не оказывать негативного влияния на доступ к рынкам, эффективность и действенность конкурентной среды в цифровом секторе, не способствует внедрению инноваций, расширению возможностей выбора потребителей при получении цифровых услуг и т. д.

Регуляторные инициативы государств в цифровом секторе с точки зрения определения порядка функционирования онлайн-платформ, прежде всего крупных, не могут полностью устранить «критические эффекты» их деятельности, а устанавливаемые в этом плане государствами регуляторные механизмы с очевидностью свидетельствуют о концептуально разных (если не противоположных) подходах. Например, в России 1 июля 2021 года принят федеральный закон № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети „Интернет“ на территории РФ». Реализация этого федерального закона конкретизируется подзаконными актами, в частности, приказами Роскомнадзора, а в числе последних следует назвать приказ от 13.08.2021 [1]№ 157 «Об утверждении Требований к содержанию информации о нарушении законодательства РФ иностранным юридическим лицом, иностранной организацией, не являющейся юридическим лицом, иностранным гражданином, лицом без гражданства, осуществляющими деятельность в информационно-телекоммуникационной сети „Интернет“ на территории РФ, в целях информирования пользователей информационного ресурса такого иностранного лица»[2] и приказ от 13.08.2021 № 158 «Об утверждении Порядка направления Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций операторам поисковых систем, распространяющим в информационно-телеком-

[1] Федеральный закон от 01.07.2021 N 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» // СПС КонсультантПлюс. Этот Федеральный Закон в «журналистском клише» назван «Закон о «приземлении» иностранных IT-компаний».

[2] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 13.08.2021 № 157// СПС КонсультантПлюс.

муникационной сети „Интернет" рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории РФ, требования о прекращении выдачи по запросам пользователей сведений об информационном ресурсе иностранного лица».[3] Российскими отраслевыми регуляторными органами применительно к рассматриваемой сфере деятельности также приняты соответствующие акты, например, можно назвать документ Банка России «Экосистемы: подходы к регулированию»,[4] принятый для целей общественных консультаций; документ Министерства цифрового развития, связи и массовых коммуникаций РФ — «Концепция общего регулирования деятельности групп компаний, развивающих цифровые сервисы на базе одной „экосистемы"»,[5] «Концепцию общего регулирования деятельности групп компаний, развивающих различные цифровые сервисы на базе одной «экосистемы» (3760п-П10), подготовленную Минэкономразвития РФ и утвержденную правительством РФ (14.04.2021).[6] Заинтересованный читатель, обратившись к содержанию названных российских правовых актов, может самостоятельно сопоставить их с концептуальными регулирующими инициативами Европейского Союза, анализ которых представлен далее в настоящей статье.

Законодательный пакет Европейского Союза

Системный и комплексный подход, обеспечивающий общие рамки единого рынка Европейского Союза, получил свое дальнейшее развитие в связи с обновлением правил механизма функционирования цифрового сектора рынка в плане установления «новаций» регулирования предоставления цифровых услуг, определения условий использования и оборота широкого спектра европейских данных (к примеру, не персональных данных в их корреляции с персональными данными и иных категорий данных). Этот подход закреплен в предложениях относительно принятия в формате регламентов трех законодательных актов вторичного права Евросоюза, конкретно закрепленных в двух регламентах Европейского парламента и Совета (15.12.2020) о конкурентных и справедливых рынках в цифровом секторе (далее — «Регламент о цифровых рынках» (Digital Markets Act, DMA), или «Регламент DMA») [7]и регламентом о едином рынке цифровых услуг (далее — «Регламент о цифровых услугах» (Digital Services Act, DSA), или «Регламент DSA»),[8] а также регламентом Европейского парламента и Совета (25.11.2020) в отношении управления использованием европейских данных (далее — «Регламент об использовании европейских данных» (Data Governance Act, DGA), или «Регламент DGA).[9] Предваряя последующее изложение, отметим несколько моментов следующего свойства.

Во-первых, предлагаемые к принятию регламенты призваны придать динамику дальнейшему развитию транспарантной регламентации и правовой определенности функционирования единого европейского рынка и его цифрового сегмента в целом. С одной стороны, регламенты разработаны и предложены к принятию в т. н. пакетном варианте, с другой стороны, непосредственно связаны и коррелируют действующим законодательным актам права ЕС. Во-вторых, имеет значение тот факт, что рассматриваемые далее регламенты исходят из т. н. «ex ante регулирования»,[10] при котором в законодательном порядке устанавливается значительное число конкретных предписаний, запретов и ограничений для минимизации ожидаемых негативных событий, что приводит к увеличению регуляторной нагрузки и обременению субъектов права. В Евросоюзе, как правило, вариации ex ante регулирования распространяются, к примеру, на вновь возникающие отношения, которые имеют существенную значимость в целом. Применяя ex ante регулирование, органы Евросоюза стремятся выявить оптимальную регуляторную модель для такого рода отношений. Как правило, в Евросоюзе ex ante регулирование носит временный характер. В-третьих, сфера действия предлагаемых к принятию регламентов распространена на государства-члены Европейского экономического пространства (European Economic Area, EEA), а конкретно на Исландию, Лихтенштейн, Норвегию (кроме Швейцарии).[11] В-четвертых,

3 Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 13.08.2021 № 158 // СПС КонсультантПлюс.

4 «Экосистемы: подходы к регулированию» / URL: https://www.cbr.ru/Content/Document/File/119960/Consultation_Paper_02042021.pdf

5 «Концепция общего регулирования деятельности групп компаний, развивающих цифровые сервисы на базе одной «экосистемы»» / URL: https://www.economy.gov.ru/material/file/cb29a7d08290120645a871be41599850/koncepciya_21052021.pdf

6 Текст документа доступен: СПС КонсультантПлюс и приведен в соответствии с публикацией на сайте https://economy.gov.ru по состоянию на 28.05.2021.

7 Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act). (Text with EEA relevance) // COM/2020/842 final. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

8 Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC. (Text with EEA relevance) //COM/2020/825 final / URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

9 Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act). (Text with EEA relevance) // COM/2020/767 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

10 В правовых системах европейских государств существует два способа нормативно-правового регулирования общественных отношений – «ex ante регулирование» («до события») и «ex post регулирование» («после события»). Регулирование «ex post», в отличие от «ex ante регулирования», законодатель использует в том случае, когда те или иные отношения сформировались и в отношении них регуляторная модель ясна; при «ex post регулировании» регуляторная нагрузка существенно снижена, однако это не означает отсутствия запретов, ограничений или наличия обязательств императивного характера.

11 О Европейском экономическом пространстве (European Economic Area, EEA), Европейской ассоциации свободной торговли (EACT), а также Соглашении о Европейском экономическом пространстве см. подробнее, например: URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Aeuropean_free_trade_association

значительный объем текстов предлагаемых к принятию регламентов позволяет в формате статьи отметить лишь некоторые нормативные положения принципиального характера, высвечивающие концептуальные подходы порядка регулирования функционирования онлайн-платформ как значимого структурного элемента цифрового рынка Евросоюза и ЕЭП.

Регламент о цифровых рынках (Digital Services Act, DSA)

Регламент DMA исходит из того, что лишь несколько крупных онлайн-платформ обладают характерными свойствами, сочетание которых дает им возможность пользоваться массой преимуществ (например, иметь доступ к большим объемам данных, включая их последующее использование в различных секторах экономики и социальной сфере), создавать и контролировать целые экосистемы платформ (platform ecosystems) цифровой экономики и т. д. Регуляторные инициативы ряда государств-членов ЕС, нацеленные на установление в рамках своих национальных правопорядков нормативных правил и мер административного характера применительно к деятельности таких платформ, не только способны привести к фрагментации внутреннего европейского рынка, подорвать конкурентоспособность в его цифровом сегменте, но и не могут эффективно влиять на функционирование крупных онлайн-платформ. В этой связи логика принятия Регламента DMA обусловлена закреплением в масштабе Евросоюза общего порядка и правил деятельности онлайн-платформ как важного элемента структуры цифровой экономики ЕС и ЕЭП, с акцентом на комплекс обязательств, предназначенных для крупных онлайн-платформ, с учетом их ключевого положения и значимости на европейском рынке, с тем, чтобы поддерживать действенную конкуренцию, обеспечивать равные условия и возможности для всех участников европейских цифровых рынков, минимизировать риски установления крупными онлайн-платформами недобросовестных нормативных практик (включая ценообразование, качество оказания услуг и т. д.) при предоставлении ими услуг европейским потребителям, расширить возможности выбора европейских потребителей и гарантировать соблюдение их прав.

Регламент DMA, устанавливающий порядок деятельности онлайн-платформ на современном цифровом рынке Евросоюза и ЕЭП, формулирует адаптивный подход, определяющий правовую категоризацию и квалификацию платформ, включая услуги, предоставляемые поставщиками платформ. В категориальных понятиях Регламента DMA крупные онлайн-платформы именуются «ключевыми платформами» (core platforms), а к их числу отнесены те, которые обладают возможностью, в том числе, создавать на своей базе собственные конгломератные экосистемы цифровых услуг, встроенные в их онлайн-платформы; контролировать доступ к цифровым рынкам, устанавливать нормативные правила и практики при предоставлении соответствующих услуг платформ. Такого рода возможности «ключевых платформ» в европейском цифровом секторе, в частности, позволяют платформам, помимо их основной деятельности, формировать целые экосистемы (platform ecosystems), а также порождают зависимость от них значительного числа пользователей, что препятствует доступу на цифровые рынки иных заинтересованных участников и подрывает конкуренцию на внутреннем рынке. Соответственно, Регламент DMA призван урегулировать такого рода проблемы.

Фактор присутствия ограниченного числа ключевых платформ обусловил не только необходимость определения услуг, предоставляемых в рамках такой платформы, но и осуществить квалификацию соответствующих «поставщиков услуг ключевой платформы» (providers of core platform services). В этой связи Регламент DMA закрепил неисчерпывающий перечень характерных свойств услуг ключевой платформы, позволяющих им выступать в качестве важных посредников, или шлюзов (gateways), при осуществлении транзакций между конечными пользователями и бизнес-пользователями, что приводит (или может привести) к слабой конкуренции этих услуг и рынков, на которых подобные платформы действуют.

Согласно Регламенту DMA, основные услуги ключевой онлайн-платформы включают: a) услуги онлайн-посредничества (включая торговые площадки, магазины приложений и онлайн-посреднические услуги в иных секторах); b) онлайн-поисковики; c) услуги социальной сети; d) услуги платформ видеообмена; e) услуги межличностной коммуникации, не зависящие от номера; f) операционные системы; g) услуги облачных вычислений; h) рекламные услуги, в том числе различные рекламные сети и рекламные биржи, а также иные услуги рекламного посредничества, в которых подобная реклама связана с одной или несколькими услугами ключевой платформы, упомянутыми п. п. a)-g).

Регламент DMA исходит из порядка «категорирования» поставщиков услуг платформ и принципиальным фактором является квалификация поставщиков услуг ключевой платформы, именуемых в значении данного Регламента «гейткиперами» (Gatekeeper). Представляется целесообразным использовать именно такой перевод на русский язык, т. е. посредством транслитерации указанного понятия, что связано не только с отсутствием такового в русском языке, но также с тем, что понятие «гейткипер» (gatekeeper), является производным от термина «gateway» (шлюз). [12]

Конкретный поставщик услуг ключевой платформы может быть признан в качестве гейткипера (т. е. получить статус гейткипера), когда он: a) оказывает значительное влияние на внутренний рынок; b) осуществляет управление одним или несколькими важными шлюзами для клиентов с учетом количественных пороговых значений охвата конечных пользователей; c) пользуется или потенциально может занять устойчивое и прочное положение на цифровом рынке. Статус «гейткипера», в частности, предполагает

[12] Термин «gateway» (как, например, «application gateway») интерпретируется и применяется в т.ч. для обозначения систем, выполняющих преобразование из одного формата в другой; так, примером шлюза может служить межсетевой транслятор адресов NAT, широко применяемый в Интернете.

соблюдение единообразного императивного комплекса норм (в том числе ограничительных) в отношении обязательств гейткипера и каждой из услуг ключевой платформы, включая порядок и условия предоставления таких услуг; дает возможность гейткиперу взаимодействовать с Еврокомиссией в рамках нормативного регуляторного диалога (regulatory dialogue) и т. д. Еврокомиссия компетентна принимать решения, связанные с признанием поставщика услуг в качестве гейткипера, что имеет важное значение в связи с тем, что «гейткиперы» как правило осуществляют свою бизнес-деятельность в глобальном масштабе, соответственно, без применения общих институциональных механизмов и единообразных, согласованных и императивных норм на уровне Евросоюза сложно избежать регуляторной фрагментации пространства услуг ключевых платформ. Немаловажно обратить внимание на положения Регламента DMA о том, что гейткиперы должны гарантировать выполнение обязательств в полном соответствии с иными законодательными актами права Евросоюза в сфере защиты и конфиденциальности персональных данных и защиты прав потребителей.

Уместно заметить в скобках, что упомянутый ранее документ Министерства цифрового развития, связи и массовых коммуникаций РФ также использует понятие «гейткипер» (в его транслитерированной форме) и дает его определение: «владелец бизнес-правила (gatekeeper) — лицо, обладающее полномочием создавать, изменять или отменять бизнес-правило, владелец бизнес-модели — лицо, обладающее полномочием создавать, изменять или отменять бизнес-модель».[13] В сравнении с Регламентом DMA содержательный объем в приведенном выше определении российского документа имеет совершенно иной смысл и значение.

В лапидарной форме можно сделать обобщающий вывод о том, что Регламент DMA направлен на устранение причин, могущих привести к экономическому дисбалансу функционирования цифрового сектора и конкурентоспособности цифровой экономики ЕС и ЕЭП в целом, а также предотвращение недобросовестной деловой практики гейткиперов, включая негативные последствия их деятельности в плане ослабления конкуренции на «рынках онлайн-платформ».

Закрепленные Регламентом о цифровых рынках (DMA) положения, используемые в нем основные понятия, включая их содержательный объем, и т. д., в полной мере коррелируют Регламенту о едином рынке цифровых услуг (DSA).

Регламент о цифровых услугах (Digital Services Act, DSA)

Регламент DSA в первую очередь связан с регламентацией порядка и условий предоставления посреднических услуг (intermediary services) и платформ (онлайн-торговые площадки, социальные сети, платформы для обмена контентом, магазины приложений и онлайн-платформы для путешествий и проживания и т. д.), с учетом действия крупных и сверхкрупных онлайн-платформ (very large online platforms), которые в рамках услуг информационного общества становятся значительной частью экономики Евросоюза и повседневной жизни лиц ЕС. Регуляторная сфера действия Регламента DSA охватывает широкие предметные области и круг субъектов. Предметно сфера действия регламента охватывает любые услуги информационного общества, предоставляемые поставщиками посреднических услуг (providers of intermediary services) за вознаграждение либо дистанционно, либо электронным способом, либо по индивидуальному запросу получателя.[14] По кругу субъектов Регламент DSA распространяется не только на европейских поставщиков, но и на иных поставщиков посреднических услуг вне зависимости от места их учреждения или постоянного местопребывания, если они предоставляют услуги в масштабе Евросоюза и когда это подтверждается существенной связью с ЕС (или предполагает такую связь). Определение наличия такого рода существенной связи с Евросоюзом у не учрежденных в ЕС поставщиков посреднических услуг, но предлагающих услуги в ЕС, основывается на четких критериях и, кроме того, регламент устанавливает императивные обязательства для таких поставщиков, включая меры их ответственности.

В связи со значительным объемом нормативных положений Регламента DSA, которые сложно осветить в формате статьи, представляется возможным отметить некоторые нормативные положения, структурно охватывающие квалификацию услуг платформ поставщиков посреднических услуг; соответствующие обязательства и ответственность поставщиков, в частности, связанные с регулированием контента; вопросы, относящиеся к развитию общего институционального механизма в этом плане.

В таблице[15] приведены обязательства, накладываемые Регламентом DSA на различные организации, дифференцируемые по размеру и типу деятельности.

Кумулятивные/совокупные обязательства по обеспечению безопасной и подотчетной онлайн-среды (согласно Регламенту DSA)

[13] «Концепция общего регулирования деятельности групп компаний, развивающих цифровые сервисы на базе одной «экосистемы»» / URL: https://www.economy.gov.ru/material/file/cb29a7d0829012064 5a871be41599850/koncepciya_21052021.pdf

[14] Данное положение коррелирует Директиве (ЕС) 2015/1535 Европейского парламента и Совета от 9.09.2015, предусматривающей порядок в отношении предоставления информации в сфере технического регулирования и правил услуг информационного общества. (Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services. Официальный Журнал ЕС. Право, 241, 17.9.2015, с. 1.

[15] Источник: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en#new-obligations

Кумулятивные/совокупные обязательства по обеспечению безопасной и подотчетной онлайн-среды (согласно Регламенту DSA) [16]	Посреднические услуги (Intermediary services)	Услуги хостинга (Hosting services)	Онлайн-платформы (Online platforms)	Сверхкрупные онлайн-платформы (Very large platforms)
Предоставление отчетности о транспарентности/прозрачности (Transparency reporting)	*	*	*	*
Требования к условиям оказания услуг с должным учетом основополагающих прав (Requirements on terms of service due account of fundamental rights)	*	*	*	*
Взаимодействие с национальными органами по соблюдению предписаний (Cooperation with national authorities following orders)	*	*	*	*
Учреждение точек контакта и, при необходимости, законного представителя (Points of contact and, where necessary, legal representative)	*	*	*	*
Уведомление, принятие мер и обязательств по предоставлению информации пользователям (Notice and action and obligation to provide information to users)		*	*	*
Механизм претензий и компенсаций, а также внесудебное урегулирование споров (Complaint and redress mechanism and out of court dispute settlement)			*	*
Доверенные флаггеры (Trusted flaggers)			*	*
Меры против оскорбительных уведомлений и встречных уведомлений (Measures against abusive notices and counter-notices)			*	*
Проверка надежности сторонних поставщиков (Vetting credentials of third party suppliers "KYBC" (Know your business customer) [17]			*	*
Информационная открытость рекламы для пользователя (User-facing transparency of online advertising)			*	*
Предоставление отчетности по уголовно наказуемым деяниям (Reporting criminal offences)			*	*
Обязательства по управлению рисками и комплаенс-офицеры [18] (Risk management obligations and compliance officer)				*
Внешний аудит рисков и публичная отчетность (External risk auditing and public accountability)				*
Транспарентность/прозрачность рекомендательных систем и выбор пользователя относительно доступа к информации (Transparency of recommender systems and user choice for access to information)				*
Совместный с уполномоченными органами и исследователями доступ к данным (Data sharing with authorities and researchers)				*
Кодексы поведения (Codes of conduct)				*
Взаимодействие по антикризисному реагированию (Crisis response cooperation)				*

В целях обеспечения ответственных и добросовестных действий поставщиков посреднических услуг Регламент DSA должен применяться, когда эти поставщики оказывают посреднические услуги, состоящие из: a) услуг, известных как «простое средство передачи» (mere conduit), b) «кэширования» (caching) и c) «услуг хостинга» (hosting' services). В смысле Регламента DSA услуга «простое средство передачи» означает передачу по коммуникационной сети информации, предоставленной получателем услуги, или в предоставлении доступа к коммуникационной сети. Услуга «кэширование» заключается в передаче по коммуникационной сети информации, предоставляемой получателем услуги, включая автоматическое, промежуточное и временное хранение такой информации, с единственной целью повышения эффективности дальнейшей передачи информации другим получателям по их запросу. Услуга «хостинга» означает хранение информации, предоставленной получателем услуги и по запросу получателя услуги, при этом в качестве поставщиков услуг хостинга Регламент DSA определяет онлайн-платформы (социальные сети или онлайновые торговые площадки), которые не только хранят информацию, предоставленную получателями услуги по их запросу, но и распространяют такую информацию среди неопределенного круга лиц в ответ на их запрос.

С учетом разности характеристик деятельности поставщиков посреднических услуг («простое средство передачи», «кэширование» и «хостинг»), а также различий в их статусе и круге правомочий при оказании услуг информационного общества, Регламент DSA специфицирует правила и обязательства (в т. ч. освобождение от обязательств) применительно к статусу поставщиков и соответствующим видам их деятельности. На два обстоятельства следует обратить внимание.

Первым обстоятельством является законодательное разграничение в праве Евросоюза сферы регулирования применения коммуникационных технологий и регулирования контента. Достаточно в этом плане сослаться на Европейский

[16] The Digital Service Act: ensuring a safe and accountable online environment. URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en#new-obligations

[17] Know your business customer (KYBC) означает обязательства, связанные с сокращением незаконного контента с минимальным бременем для посредников и предприятий, действующих на законных основаниях. См. подробнее, например: URL: https://www.kybc.eu/

[18] Комплаенс-офицер (compliance officers), т.е. сотрудник, ответственный за обеспечение соблюдения требований, правил и проч., как внутрикорпоративных, так и общеправового характера.

Телекоммуникационный кодекс,[19] а также на Директиву (ЕС) 2000/31 об электронной коммерции,[20] положения которой являются исходными для Регламента DSA, последовательно детализируются и развиваются. Так, Директива (ЕС) 2000/31 предусматривает (п.(а) Статьи 12), что при оказании услуги информационного общества, состоящей в передаче по коммуникационной сети информации, предоставленной получателем услуги, или предоставления доступа к коммуникационной сети, поставщик услуг не несет ответственности за передаваемую информацию при условии, что поставщик не инициирует передачу.[21] Данному положению коррелирует общее правило Регламента DSA: «ни обязательства общего характера по мониторингу информации, которую поставщики посреднических услуг передают или хранят, ни активный поиск фактов или обстоятельств, свидетельствующих о незаконной деятельности, не должны быть возложены на таких поставщиков», а также положения о том, что не должны нести ответственность поставщики услуг «простого средства передачи» за переданную информацию; поставщики услуг «кэширования» — за информацию, когда они не связаны с передаваемой информацией; поставщики услуг «хостинга» — за хранящуюся по запросу получателя услуги информацию. Вместе с тем, освобождение от ответственности поставщиков, согласно Регламенту, должно обусловливаться соблюдением детализированных условий оказания посредниками названных услуг («простое средство передачи», «кэширование» и «хостинг») и не должно влиять на возможность суда или административного органа государств-членов предъявлять требования к поставщику услуг прекратить или не допускать нарушений, предусмотренных в их национальных правопорядках.

Сказанное приобретает существенную значимость в аспекте определения Регламентом DSA содержания понятий «незаконный контент» и «модерация контента» в их широком значении, в том числе с охватом информации, связанной с незаконным контентом, продукцией, услугами и деятельностью поставщиков посреднических услуг и функционированием онлайн-платформ. В значении регламента «незаконный контент» (illegal content) означает любую информацию, которая сама по себе или посредством ссылки на действие, в том числе на продажу продукции или предоставление услуг, не соответствует праву Евросоюза или праву государства-члена, независимо от точного предмета или сущности такого права«; «модерация контента» (content moderation) означает действия, предпринимаемые поставщиками посреднических услуг, нацеленные на обнаружение, идентификацию и решение проблем, относящихся к незаконному контенту или информации, несовместимой с положениями и условиями поставщиков посреднических услуг, которые они предоставляют получателям услуги, включая принятие мер, которые воздействуют на возможность использования, визуализацию и доступность такого незаконного контента или такой информации, как, например, понижение статуса, блокировка доступа или удаление незаконного контента или информации, либо воздействуют на возможность получателя предоставлять такую информацию, в том числе аннулирование или приостановка действия учетной записи получателя«.

Второе обстоятельство сопряжено с тем, что диапазон установленных и детализованных Регламентом DSA обязательств, применимых ко всем поставщикам посреднических услуг и вне зависимости от того, учреждены ли поставщики в ЕС или нет, — расширяет круг вовлеченных лиц, и рассматриваемый регламент определяет статус таких лиц, их предметную и функциональную компетенцию. В частности, круг таких лиц, согласно Регламенту DSA, охватывает законных представителей, назначаемых поставщиком посреднических услуг, когда он не учрежден в ЕС, но предлагает услуги в одном из государств-членов ЕС; координаторов цифровых услуг (Digital Services Coordinator), назначаемых в каждом государстве-члене ЕС в качестве органов для взаимодействия и надзора; комплаенс-офицеров (compliance officers), которых сверхкрупные онлайн-платформы должны назначить для мониторинга их соответствия и соблюдения Регламента DSA; доверенных флаггеров (Trusted Flaggers), статус и компетенция которых нуждается в уточняющем пояснении.

Регламент предусматривает дополнительные обязательства для поставщиков посреднических услуг хостинга, в частности, закрепляя положение о том, что все поставщики услуг хостинга, вне зависимости от их масштаба, обязаны внедрить механизмы уведомлений, направленные на регистрацию поставщиком конкретных объектов информации, которые уведомляющая сторона оценивает в качестве незаконного контента, и способствующие тому, чтобы соответствующий поставщик услуг хостинга мог принять решение об удалении или запрете доступа к такому контенту. Такие механизмы уведомления предполагают также принятие мер по обработке претензий/жалоб, что, в свою очередь, объясняет появление таких лиц как «доверенные флаггеры». Наряду с прочим, функциональная компетенция доверенных флаггеров связана с получением претензий/жалоб в т. ч. о незаконном контенте, с последующим уведомлением соответствующего поставщика онлайн-платформы для того, чтобы платформа обработала и приняла решение по таким уведомлениям в первоочередном порядке. Такого рода уведомления доверенные флаггеры вправе предоставлять в электронной форме и через программные интерфейсы приложений.

Регламент DSA также затрагивает общеевропейский институциональный аспект регулирования порядка и условий предоставления посреднических услуг и деятельности онлайн-платформ в Евросоюзе. Упомянем предусмотренный регламентом Европейский совет по цифровым услугам

[19] Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972

[20] «Директива об электронной коммерции» (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). (Официальный Журнал ЕС. Право, 178, 17.7.2000, с. 1)

[21] Целесообразно также упомянуть содержащуюся в праве США аналогичную норму: обязательства на технологические компании не возлагаются при простой передаче информации (без вмешательства в передаваемую информацию), предоставленной поставщиком информации, (§) 230 Кодекса США). См. 47 U.S. Code § 230 (Protection for private blocking and screening of offensive material). URL: https://www.law.cornell.edu/uscode/text/47/230

(European Board for Digital Services), который должен способствовать достижению общего понимания Евросоюза в отношении трендов развития цифровых услуг в ЕС, участвовать в разработке соответствующих типовых проформ и кодексов поведения, обеспечивать согласованное в масштабе ЕС применение Регламента DSA и т. д. В организационном плане Европейский совет по цифровым услугам должен объединять координаторов цифровых услуг и их представителей, функционировать под председательством Еврокомиссии. Регламент DSA исходит из того, что особенности организационной деятельности внутреннего функционирования Европейского совета по цифровым услугам будут дополнительно определены в его правилах процедур.

Регламент об использовании европейских данных (Data Governance Act, DGA)

Регламент DGA в русскоязычном варианте переведен именно таким образом, поскольку в оригинальной английской версии использует слово «Governance». Наиболее точный и адекватный перевод на русский язык, содержательно соответствующий существу значения слова «governance», это «регулирование использованием», «порядок использования», «регулирование использования», но не «управление», поскольку содержательная коннотация английского слова «governance» не подразумевает наличия «вертикального» управляющего воздействия, которое свойственно русскоязычной интерпретации слова «управление». Соответственно, предложенный в этой статье перевод содержательно соответствует существу словосочетания «data governance», на структурно-технологическом уровне de facto сводящегося к установлению и соблюдению правил и процедур, регламентирующих порядок распоряжения и использования разнообразных видов/типов данных различными лицами, включая порядок трансграничного перемещения данных. Представленное пояснение имеет принципиальное значение.

В общем плане Регламент DGA нацелен на создание «гуманитарно-ориентированного» единого цифрового рынка в контексте экосистемы использования данных, основанной на развитии механизмов обмена данными, с допуском повторного использования данных государственного сектора в общественно-полезных целях, включая обмен такими данными. Регламент EDG исходит из необходимости «горизонтального режима» регулирования использования данных в Евросоюзе для того, чтобы создать в масштабах ЕС базовые рамки порядка доступа к данным и их использования.

Сфера действия Регламента DGA не затрагивает положения законодательных актов права Евросоюза, относящихся к доступу или повторному использованию конкретных категорий данных или требований, связанных с обработкой персональных или не персональных данных. В этой связи целесообразно отметить, что правовые основы регламента нацелены на регулирование возможности повторного использования данных государственного сектора, выходящих за сферу действия Директивы об открытых данных.[22] Среди прочих аспектов, регламент устанавливает правовую основу для повторного использования данных государственного сектора, на которые распространяются права третьих лиц, а именно: данных, защищенных правами интеллектуальной собственности (ИС), а также конфиденциальных данных не персонального характера, равно как и персональных данных, с учетом действующей приоритетной применимости Общего регламента по защите данных (GDPR) при регулировании персональных данных и действия Директивы о конфиденциальности и электронных коммуникациях (e-Privacy).[23]

Регламент DGA непосредственно устанавливает: 1) условия, направленные на повторное пользование (re-use) конкретных категорий данных, которыми владеют органы государственного сектора в масштабах Евросоюза; 2) основы организации уведомления и надзора над предоставлением услуг по распространению данных (data sharing services); 3) основы организации относительно добровольной регистрации организаций, которые собирают и обрабатывают данные, предоставляемые в альтруистических целях (altruistic purposes), т. е. альтруистических данных. Кратко очертим некоторые моменты, относящиеся к указанным предметным сферам.

1) Условия, направленные на повторное пользование (re-use) конкретных категорий данных, сформулированы в контексте компетенции органов государственного сектора, с учетом того факта, что такие органы аккумулируют (владеют или контролируют) значительный объем данных. В этой связи значимым является содержательное определение в Регламенте DGA ключевого понятия — «повторное использование» (re-use), означающее использование физическими или юридическими лицами данных, которыми владеют органы государственного сектора в коммерческих или некоммерческих целях, отличных от первоначальной цели в рамках государственной задачи, для которой были получены данные, за исключением обмена данными между органами государственного сектора сугубо для выполнения их государственных задач.

Посредством понятия «повторное использование данных» Регламент DGA устанавливает рамки «режим повторного использования данных», который должен применяться к данным, предоставление которых является частью общественных задач соответствующих органов государственного сектора, а такого рода задачи следует определять либо в целом для государственных органов, либо дифференцировано для конкретных органов государственного сектора. Регламент DGA нацелен на создание «гуманитарно-ориентированного» единого цифрового рынка в контексте экосистемы использования данных, основанной на развитии механизмов обмена данными, с допуском повторного использования данных государственного сектора

[22] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.172.01.0056.01.ENG

[23] «Директива 2002/58/ЕС о конфиденциальности и электронных коммуникациях». URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

в общественно-полезных целях, включая обмен такими данными.

2). В значении Регламента DGA, основы организации уведомления и надзора над предоставлением услуг по распространению данных сопрягаются с установлением порядка и условий деятельности поставщиков услуг по распространению данных (data sharing providers). Ключевым элементом для таких поставщиков рассматривается нейтральность (neutrality) их деятельности при обмене данными между владельцами данных (прежде всего государственными органами) и пользователями данных. Для того, чтобы избежать возможных и потенциальных конфликтов, Регламент DGA предусматривает, что услуги по распространению данных должны оказываться только юридическими лицами, учрежденными в Евросоюзе, а когда поставщики услуг по распространению данных не учреждены в Евросоюзе, но предлагают услуги в масштабах Евросоюза, они должны назначить своего представителя в ЕС.

Регламент DGA предусматривает комплекс императивных условий, применимых к поставщикам услуг по распространению данных. Помимо этого, положения регламента связываются с рядом надзорных параметров, касающихся деятельности поставщиков услуг по распространению данных. В частности, соответствующие компетентные государственные органы, органы по защите данных, национальные органы по вопросам конкуренции, органы, отвечающие за кибербезопасность, иные отраслевые органы должны обмениваться информацией, связанной с осуществлением деятельности поставщиков услуг по распространению данных. Кроме того, на Еврокомиссию, согласно Регламенту DGA, возлагается обязанность ведения реестра поставщиков услуг по распространению данных.

3). Отмеченный выше факт, что Регламент DGA исходит из необходимости «горизонтального режима» регулирования использования данных в Евросоюзе, также касается услуг, основанных на альтруизме данных (data altruism), включая сбор и обработку таких данных. Содержание понятия «альтруизм данных», согласно Регламенту, означает «согласие субъектов данных на обработку персональных данных, относящихся к ним, или разрешения иных владельцев данных на использование их не персональных данных без требования вознаграждения для целей, представляющих общественный интерес, таких как научные исследования или совершенствование услуг общего пользования».

Регламент DGA закрепляет, что организации могут быть зарегистрированы в качестве «организаций альтруизма данных», когда они являются юридическим лицом, созданным для достижения целей, представляющих общественный интерес; действуют на некоммерческой основе и независимы от любой организации, которая работает на некоммерческой основе; выполняет деятельность, связанную с альтруизмом данных, осуществляемую через юридически независимую структуру, которая отделена от иных видов ее деятельности. Соответствие юридического лица таким условиям является основанием для его внесения в национальный реестр признанных организаций по альтруизму данных, компетенция по ведению которого возложена на назначаемый орган государства-члена ЕС. На уровне Евросоюза ведение соответствующего реестра признанных организаций по альтруизму данных Евросоюза возложена на Еврокомиссию.

Для содействия сбору данных, основанных на альтруизме данных, Регламент DGA исходит из необходимости принятия имплементирующих актов Еврокомиссией в целях разработки «европейской формы согласия на альтруизм данных». Такая форма должна обеспечить, чтобы субъекты данных могли давать согласие (и отзывать согласие) по единому формату в масштабе Евросоюза в отношении конкретной операции обработки данных с учетом требований Регламента GDPR.

* * *

Рассмотренные в формате статьи предложения о принятии Регламентов DSM, DSA и DGA, как представляется, отнюдь не отражают всей палитры концептуальных подходов регулирования Евросоюзом единого рынка и его цифрового сектора, но позволяют очертить принципиальные моменты цифровой стратегии Евросоюза в этой области. В настоящее время обозначенные регламенты находятся в режиме редактирования. Это обусловлено, с одной стороны, необходимостью учета представленных критических комментариев относительно содержания нормативных положений, регуляторных новаций и параметров их применения, в связи с прямым действием и непосредственным применением регламентов в национальных правопорядках государств-членов ЕС и ЕЭП, с другой стороны, форматом их согласования в плане соразмерности и пропорциональности на уровне общих институциональных механизмов Евросоюза. Вместе с тем, предусмотренные Регламентами DSM, DSA и DGA общие концептуальные подходы регулирования едва ли претерпят существенные изменения.

Что будет после...

Павел Храмцов

Мы все сейчас живем в ожидании того, что будет «после...». После пандемии, после каких-нибудь выборов, после очередного скандала, одним словом, «после...». В этом контексте можно рассматривать разные альтернативы, новые открывшиеся возможности или ограничения.

Одним из важных моментов в этой связи является будущее «живого» общения. С одной стороны, это вопрос, прямо не относящийся к «достижениям науки и техники», а с другой — именно на конференциях и семинарах проходят предварительное обсуждение все новые интересные идеи.

Корпорация ICANN провела опрос среди участников ежегодных конференций о том, как они видят будущее формата таких мероприятий, при каких условиях они согласны присутствовать лично на площадке конференции[1]. Правда, если быть более точным, то речь в опросе шла о конкретной конференции в Сиэтле (октябрь 2021), что, безусловно, накладывало свой отпечаток на результат.

[1] https://cdn.filestackcontent.com/content=t:attachment,f:%22Future%20of%20ICANN%20Meetings%20Presentation_17June2021_v2%5B1%5D-RU-Final.pdf%22/AJ3iq3nFRfKiX3Z3fGNG

Рис. 1. Согласие на личное посещение конференции.

Рис. 2. О желании и возможности посетить конференцию ICANN в Сиэтле в октябре 2021.

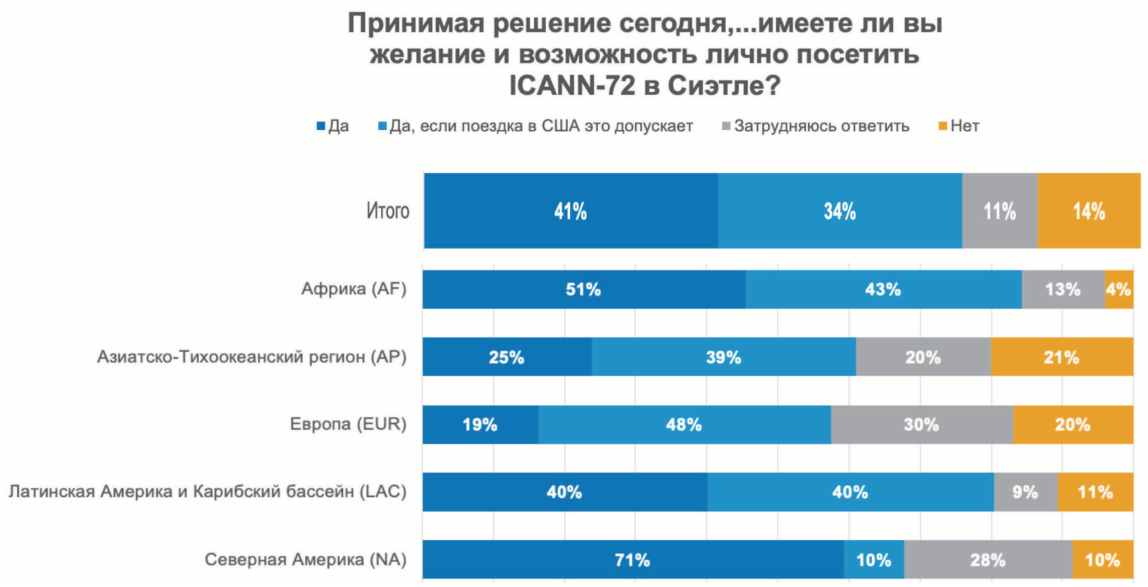
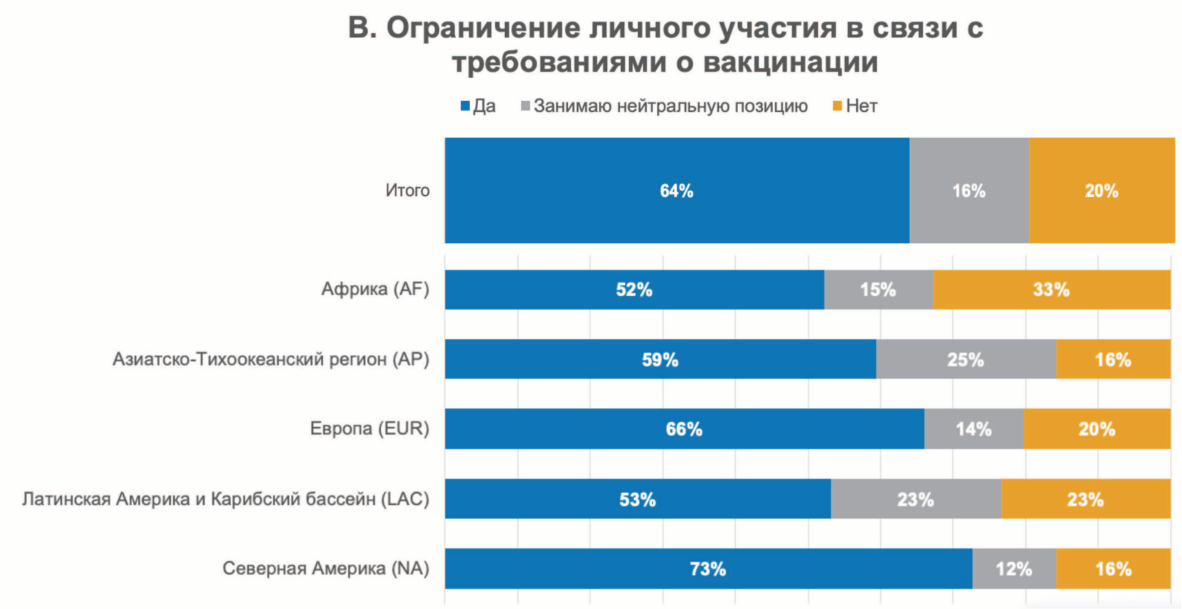


Рис. 3. Мнение по поводу допуска на площадку конференции только вакцинированных.



Опрос состоял из 12 вопросов, посмотрим только на некоторые из них. Итак, на вопрос «Готовы ли вы посетить конференцию лично при соблюдении следующих условий?» (список) подавляющее большинство ответило утвердительно (рис. 1). Любопытно, что вопрос об участии в конференции без ограничений вообще не ставился.

Но вот уже при ответе на следующий вопрос «Принимая решение сегодня, ... имеете ли желание и возможность лично посетить ICANN-72 в Сиэтле» энтузиазм поубавился (рис. 2).

Если африканские члены сообщества участников конференций ICANN готовы лично присутствовать, то вот европейцы и представители Азиатско-Тихоокеанского региона таким желанием не отличаются. Причем скепсис не зависит от возможности поездки в США.

И еще один интересный момент — это ограничения личного участия при условии вакцинации. При обсуждении этого момента поднимался вопрос о типе вакцины. Понятно, что ответ на этот вопрос зависит от позиции санитарных врачей (читай «властей»), а не совета директоров ICANN, но тем не менее, представители Африки и Латинской Америки его при обсуждении результатов опроса задавали.

Вообще-то, представители этих регионов высказали больше всего скепсиса по поводу такого сорта ограничений (рис. 3). А наиболее горячо требование вакцинирования поддержали представители Северной Америки.

В конце концов октябрьскую конференцию ICANN решено было проводить в онлайн-формате, т. к. существенного ослабления ковидных ограничений осенью не предвидится. А вот о формате весенней конференции, проведение которой предполагается в Пуэрто-Рико, предложено было подумать.

Раз уж речь зашла об ICANN, то имеет смысл поговорить о концепции Hyperlocal для системы авторитетных серверов корня системы DNS, о которой говорил представитель офиса технического директора ICANN Рой Арендс (Roy Arends) на традиционной конференции TLDCON2021. К слову сказать, ее планировалось проводить в гибридном формате в Ташкенте, но все кончилось гибридным форматом в Москве.

Анализ этой концепции представлен в документе «Hyperlocal Root Zone Technical Analysis».[2]

В чем суть идеи. Hyperlocal root service (сервис по размещению корневой зоны DNS максимально близко к локальным резолверам) — это подход, который позволяет сделать «содержание»/»поиск по содержанию» в корневой зоне DNS более доступным для резолверов за счет размещения этого корня локально, в том числе прямо на резолверах (RFC-8806 [3]).

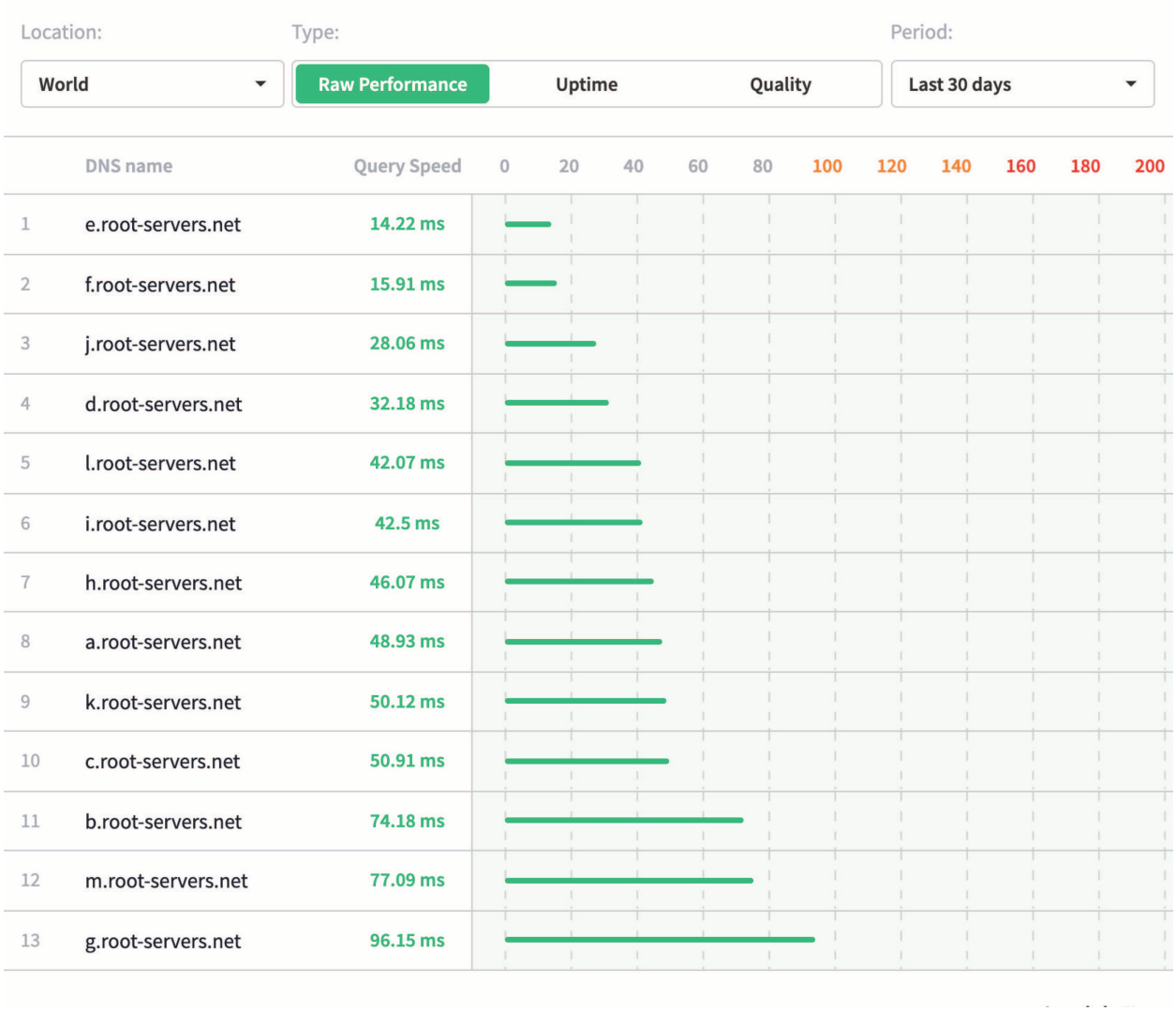
В ICANN провели анализ этой концепции в нескольких плоскостях: соблюдение приватности данных, надежность/доступность сервиса, задержки/RTT, защищенность, масштабируемость, централизованный мониторинг и непрерывность сервиса.

С точки зрения приватности было отмечено, что данные не уходят в этом случае к операторам корневых серверов DNS. Они остаются в рамках локального обмена. В этом смысле полностью соблюдаются рекомендации RFC-8932. [4]

Локальное размещение корневой зоны относится не только к ISP, но и таким публичным сервисам, как Google, Cloudflare, Cisco, UncensoredDNS и др. Реализация концепции DoH/DoT этими провайдерами полностью локализует приватную информацию в рамках соответствующих экосистем.

[2] https://www.icann.org/en/system/files/files/octo-027-25aug21-en.pdf
[3] https://datatracker.ietf.org/doc/html/rfc8806
[4] https://datatracker.ietf.org/doc/html/rfc8932

Рис. 4. Среднее время отклика корневых серверов системы DNS.



Конечно, исключить попадание к третьим лицам информации о DNS-запросах и в случае Hyperlocal нельзя, но по крайней мере, это шаг в правильном направлении. Сейчас, в сентябре 2021, кстати, 34% резолверов используют технологию QNAME minimization для того, что соблюсти приватность запросов. [5]

С точки зрения доступности сервиса Hyperlocal позволяет оперативно реагировать на DDoS-атаки на системы корневых серверов. Точнее, в этом случае обращение к штатному корню отсутствует в принципе, а значит DDoS не влияет на доступность сервиса.

Понятно, что можно осуществить атаку и на сам резолвер, но в данном случае его работоспособность не зависит от наличия или отсутствия у резолвера поддержки корневой зоны.

С точки зрения задержек концепция также имеет ряд преимуществ. В частности, как утверждается в отчете, время отклика от сети anycast штатных корневых серверов в среднем около 100 мс.

Если смотреть по статистике сайта dnsperf. com[6] (рис. 4), то оно, конечно, поменьше.

Но так «зелено» данные выглядят не для каждого региона. Например, для Африки картинка несколько другая (рис. 5): пять из 13 anycast-сетей показывают результаты существенно хуже 100 мс.

Понятно, что развертывание локального рута существенно улучшает эту картину.

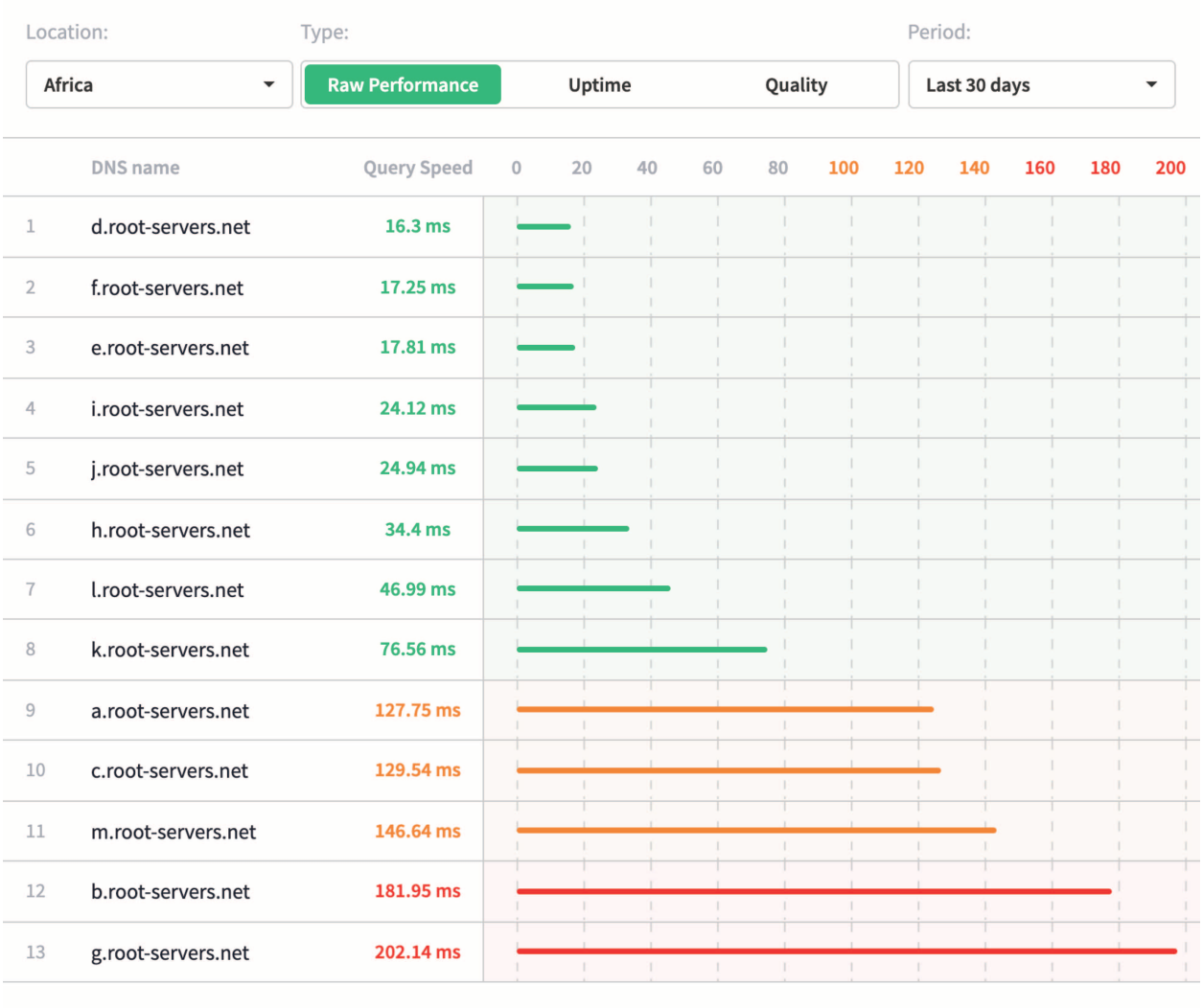
Целостность данных — это еще один момент, которому должно быть уделено повышенное внимание. Здесь важна роль DNSSEC и защищенности каналов передачи данных корневой зоны для размещения на локальном сервере. В целом, защита канала может лежать за рамками самой технологии DNS, но могут применяться и уже известные механизмы типа TSIG.

Создание локальных рутов снижает возможности мониторинга обращений к данным корневой зоны со стороны операторов штатных корневых серверов DNS (так называемая DNS-телеметрия), но в этом есть как свои минусы, так и свои плюсы. Из минусов — часть информации становится недоступной, а из плюсов — повышается защищенность приватности данных.

И напоследок — непрерывность сервиса и масштабируемость корневой зоны. Корневая зона довольно часто меняется. При ее обновлении используется технология уведомления вто-

[5] https://ithi.research.icann.org/graph-m3.html
[6] https://www.dnsperf.com/#!dns-root-servers

Рис. 5. Доступность корневых серверов DNS в регионе «Африка».



ричных серверов первичными, когда на последних происходят изменения. В Hyperlocal такого механизма нет. Но никто не отменял параметры SOA, а также возможность чаще «срисовывать» корневую зону из официальных источников, чем это указано в параметрах SOA-записи.

По поводу масштабируемости можно сказать следующее: в рамках программы new gTLD в зону было добавлено почти две тысячи доменов, и это по большому счету никак не сказалось на сервисе. По этой причине не стоит ожидать каких-либо сюрпризов и при развертывании Hyperlocal, тем паче, что данная концепция уже используется, как минимум, в том же Google DNS.

И, кстати, система, запущенная в РФ с 1 января 2021 года в соответствии с федеральным законом от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации», разве не похожа на Hyperlocal?

История с Hyperlocal на публичных резолверах имеет еще один интересный аспект. Для многих пользователей современный Интернет — это либо веб, либо социальные сети. Что скрыто «под капотом», их не очень волнует. А там много интересного.

Если включить утилиту tcpdump, то в момент запуска браузера Chrome можно увидеть вот такие, например, запросы к DNS:

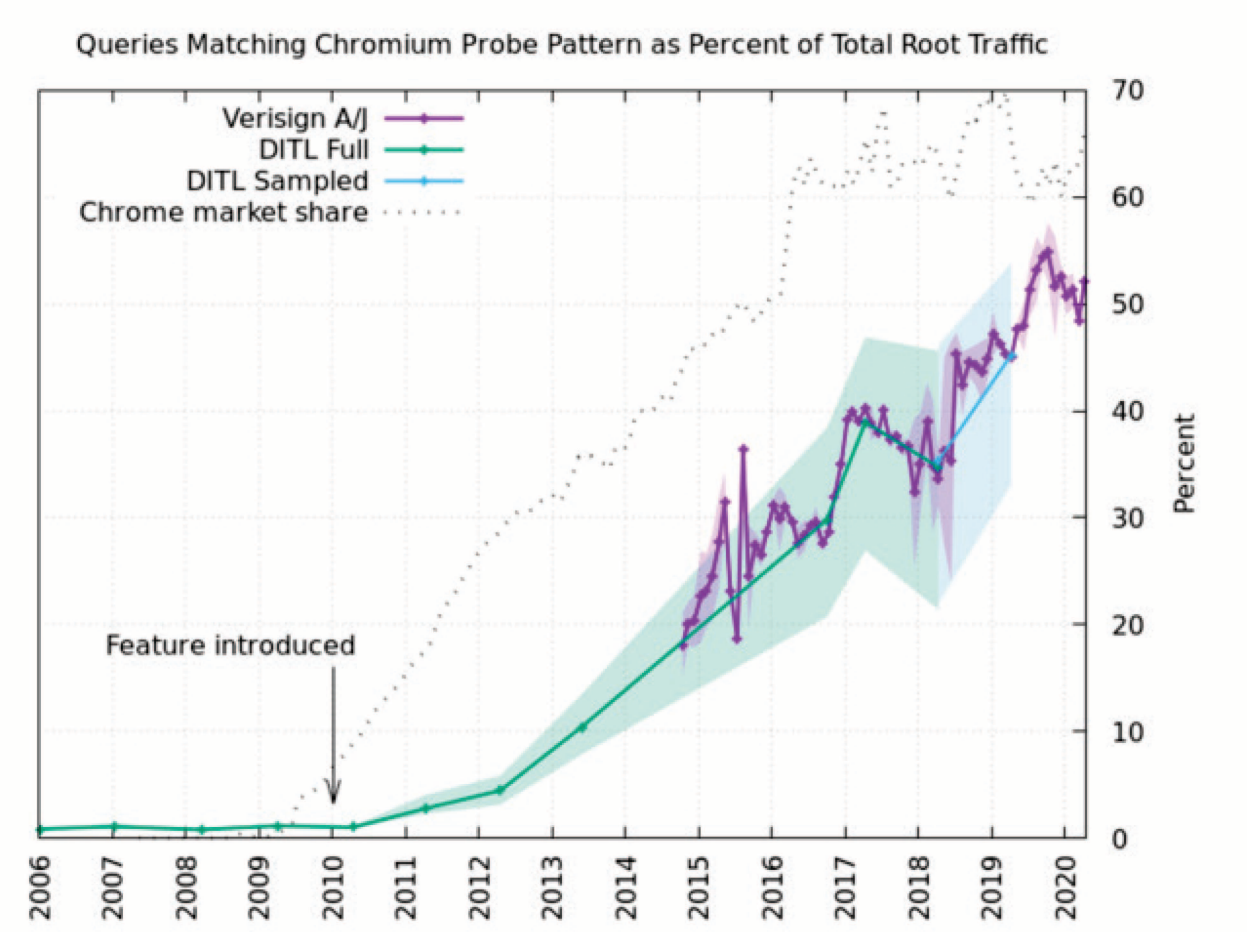
11:54:09.023742 IP 172.20.10.3.55977 > 172.20.10.1.domain: 10771+ A? qyvkldvgt. (27)
11:54:09.023814 IP 172.20.10.3.61664 > 172.20.10.1.domain: 4708+ A? fwznlnupbcz. (29)
11:54:09.024975 IP 172.20.10.3.53585 > 172.20.10.1.domain: 57807+ A? kobdqsdtupqx. (30)
11:54:09.073725 IP 172.20.10.1.domain > 172.20.10.3.53585: 57807 NXDomain 0/1/0 (105)
11:54:09.080514 IP 172.20.10.1.domain > 172.20.10.3.55977: 10771 NXDomain 0/1/0 (102)
11:54:09.080967 IP 172.20.10.1.domain > 172.20.10.3.61664: 4708 NXDomain 0/1/0 (104)
или:
11:54:03.056617 IP 172.20.10.3.50485 > 172.20.10.1.domain: 59996+ Type65? pki-goog. l. google. com. (39)

В первом случае проверяется перехват системой ISP обращений пользователей к системе DNS в целях, например, коммерческой рекламы. Во втором случае речь идет о возможности получать DNS-резолвинг через HTTPS.

Все запросы о несуществующих доменах отправятся на корневые серверы DNS. В Verisign подсчитали, как это влияет на нагрузку их авторитетных серверов корня DNS[7] (рис. 6). Таким образом, до 50% трафика на авторитетные серверы корня DNS — это запросы а-ля Chromium. Всего же запросы к несуществующим доменам составляют порядка 75% по дан-

[7] https://blog.apnic.net/2020/08/21/chromiums-impact-on-root-dns-traffic/

Рис. 6. Доля NXDOMAIN от Chromium в статистике Verisign.



ным RSSAC (Комитет советников ICANN по управлению системой корневых серверов — Root Server System Advisory Committee).[8] В Google обещали поправить ситуацию, введя соответствующий параметр настроек, но пока ничего не поменялось.

При использовании локальной реплики корня, Hyperlocal, все такие запросы придут к этой реплике. Если речь идет о крупном провайдере с большим количеством конечных пользователей, то количество таких запросов будет довольно приличным. Вообще, все такого сорта централизованные сервисы, на которые перенаправляются запросы DNS, превращаются в «сливной бачок», т. к. все, что можно закэшировать, кэшируется на резолверах провайдера, а все, что не кэшируется, отправляется на резолвинг.

В общем, подход Hyperlocal разгрузит сети штатных серверов корня DNS, но нагрузит сети, которые решатся его применить.

Пока в ICANN думают о форматах конференций и концепции Hyperlocal, случились Олимпийские Игры. В рамках конференции APNIC52 о них рассказал Ватару Саито (Wataru Saito).[9] Понятно, что речь шла не о достижениях спортсменов, а о технологиях связи. И это тем интереснее, что Олимпиада проходила практически при пустых трибунах. Только 26 соревнований провели при местных зрителях, а 724 — вообще без зрителей. На церемонию открытия было допущено только 950 официальных лиц. Фактически, Олимпиада в Японии была виртуальным, дистанционным шоу со зрительской точки зрения.

В пике на пятый день соревнований нагрузка на сети, обслуживающие Олимпиаду, составила 20 Гб/с, что почти в три раза больше, чем на Олимпиаде в Лондоне. Основную нагрузку давала видеотрансляция соревнований.

Но что нам Лондон! Интересно взглянуть на эти цифры на фоне Олимпиады в Сочи. Аккуратно сравнить эти цифры с данными Олимпиады в Сочи не получится.

Из официальных сообщений министерства цифрового развития, связи и массовых коммуникаций Российской Федерации удалось узнать, что «пропускная способность магистральной сети „Ростелекома“ на участке Сочи-Москва увеличена до 140 гигабит в секунду, мультисервисной — до 40 гигабит в секунду»,[10] а «для обеспечения максимального качества телевизионного изображения „Ростелеком“ предоставит Олимпийской вещательной службе и правообладателям, 30 компаниям-вещателям из разных стран мира, высокоскоростной канал передачи данных емкостью 110 гигабит в секунду».

[8] https://circleid.com/posts/20200926-scaling-the-root-of-the-dns

[9] https://conference.apnic.net/52/assets/files/APBS588/operating-the-network-for-the-tokyo-2020-olympic-and-paralympic-games.pdf

[10] https://digital.gov.ru/ru/events/30210/

Таким образом, потенциально инфраструктура в Сочи могла принять нагрузку японской Олимпиады.

В контексте доминирования видеотрансляций в трафике олимпиад логично было бы перейти к обсуждению еще одного аспекта современного Интернета — качества предоставления сервиса для конечного пользователя, тем более что именно этому был посвящен семинар IAB (Internet Architecture Board) «Measuring Network Quality for End-Users, 2021»,[11] который прошел в сентябре 2021 года.

Качество предоставления сервиса — это, на самом деле, довольно древняя тема. Она существует с момента сравнения технологий коммутации пакетов и технологии коммутации каналов в сетях передачи данных еще с 80-х годов прошлого века. Утверждалось, что сети коммутации каналов дают лучшее резервирование и гарантированное качество, но медленны и дороги.

Но в итоге оказалось, что гарантированное качество далеко не всегда нужно, а цена имеет существенное значение. Бенефициарами этого подхода стали сети типа TCP/IP, Ethernet и Wi-Fi.

Однако история с гарантированным качеством возвратилась с новыми требованиями по качеству связи. Она стала реализовываться в протоколах типа QUIC[12], New IP[13] и Flexilink.[14]

Если QUIC не меняет сути текущего стека протоколов TCP/IP, то New IP и особенно Flexilink — это протоколы, которые можно отнести к категории NIN (Non-IP Networking).

В конечном счете все упирается в описание этого самого качества предоставления сервиса в измеримых параметрах. А вот с этим проблемы. Требования от сервиса к сервису разнятся. И общего подхода пока не выработано.

И в заключение хотелось бы упомянуть о выборах. Но не о выборах в Государственную Думу Российской Федерации, которые случились в этом сентябре, с их электронным голосованием и переголосованием, а о выборах президента США, в которых победил Трамп.

Поводом для этого стала публикация в блоге Krebsonsecurity. com[15] о том, как бдительные американские граждане поделились своими наблюдениями о возможной связи между Trump Organization и российским Альфа-банком с компетентными американскими органами.

Суть истории вкратце такова: в октябре 2016 года средства массовой информации сообщили, что данные, собранные некоторыми из самых известных мировых экспертов по кибербезопасности, выявили частые и необъяснимые связи между почтовым сервером, используемым Trump Organization, и Альфа-банком, одним из крупнейших финансовых учреждений России. Эти публикации породили предположения о возможном секретном обратном канале связи, а также серию судебных исков и расследований, кульминацией которых стало предъявление обвинения бывшему федеральному прокурору по киберпреступлениям, который довел эти данные до сведения ФБР.

Собственно, никакой связи с почтовым сервером никто не наблюдал. В основу подозрений легли DNS-запросы. А эксперты вынесли вердикт, что они не случайны, а предполагают наличие канала связи между администраторами серверов.

Не подвергая сомнению мнение экспертов, хочется понять, а как эти записи DNS-обмена попали к этим экспертам. Для анализа DNS-запросов нужно иметь доступ либо к трафику, либо к логам DNS-серверов. Данные можно получить либо с канала связи, т. е. у ISP (DoH еще не был популярен в те времена, да и сейчас он особенно не распространен при взаимодействии резолверов с авторитетными серверами), либо у DNS-провайдеров, либо у операторов сервисов типа Passive DNS. В любом случае передача информации третьей стороне — это нарушение приватности, а возможно, и договора между оператором и пользователем.

Поскольку подозрения получили публичную огласку в прессе, то Альфа-банк нанял юристов и инициировал разбирательства по поводу высказанных подозрений в американских судах. Претензии были предъявлены 49 физическим лицам и организациям, а как минимум 15 экспертов были вынуждены давать показания под присягой.

Пикантность ситуации состоит в том, что сведения об исследовании DNS-запросов предоставлялись на условиях неразглашения. Т. е. эксперты были уверены, что все так и останется в недрах ФБР, а не получит публичной огласки. Но в рамках судебных разбирательств документы «всплыли». А также выяснилось, что один из тех, кто обратился в ФБР, в тот момент работал на избирательный штаб Клинтон, но сообщил, что он независимый эксперт. В общем, получилось некрасиво.

Интересно в этой истории несколько моментов:

В основу инициирования расследования были положены соображения, основанные на технических данных системы DNS. До сих пор утверждалось, что на основании такого сорта данных ничего определенного утверждать нельзя.

Во-вторых, экспертам пришлось в суде публично отвечать за свои слова, к чему они оказались совершенно не готовы. И автор блога выразил опасения, что теперь люди трижды подумают, прежде чем делиться данными с компетентными органами.

Так что «бумеранги» возвращаются не только в родном Отечестве, и, возвращаясь к началу статьи по поводу того, что будет «после...», следует признать, что мир меняется. И меняется он не только технологически. И эти технологические изменения кардинально меняют привычные границы и условия повседневной жизни.

[11] https://www.iab.org/activities/workshops/network-quality/
[12] https://datatracker.ietf.org/doc/html/rfc9000
[13] https://www.huawei.com/us/technology-insights/industry-insights/innovation/new-ip
[14] http://www.ninetiles.com/Flexilink_details.html
[15] https://krebsonsecurity.com/2021/09/lawsuits-indictments-revive-trump-alfa-bank-story/#more-57039

+7 495 737-92-95

WWW.MSK-IX.RU

MSK IX

10
ГОРОДОВ

500+
УЧАСТНИКОВ

42
ПЛОЩАДКИ

21
УЗЛЕЛ DNS-СЕТИ

ПОДКЛЮЧЕНИЯ ДО
100G

ТРАФИК
3,3Тбит/с

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

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

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

Интернет изнутри