

# Интернет изнутри



## СВЯЗНОСТЬ

**Влияние развития периферийных сетевых вычислений на Интернет**

Сохранит ли Интернет свою основополагающую роль на фоне появления новых видов сетевой архитектуры и приложений?

с. 2

**Эволюция связности в эпоху нулевого доверия**

Как развитие прикладных применений Интернета влияло на способность сети передавать данные

с. 10

**Управление интернет-связностью**

Анализ принципов и методов оптимизации связности на примере магистральных операторов

с. 18

**Роль точек обмена трафиком в цифровом прогрессе Ближнего Востока**

Свежий отчет RIPE NCC с анализом успехов и неудач ближневосточных IXP

с. 40

**Многофакторный анализ функционирования системы спутниковой связи Starlink**

Что в ней хорошего, плохого и «злого»?

с. 62

**Виноделие и цифровое вино**

Как новые технологии меняют сельское хозяйство

с. 78

**Мария Колесникова: «Домен .rf меняет сознание разработчиков»**

Национальный кириллический домен .rf отмечает свое 15-летие!

с. 82

# Содержание:

	с. 2	Влияние развития периферийных сетевых вычислений на Интернет
	с. 10	Эволюция связности в эпоху нулевого доверия
Интернет в цифрах	с. 14	Инфографика
Технология в деталях	с. 18	Управление интернет-связностью
	с. 24	Эволюция развития и «связанности» голосового трафика в России и мире
	с. 28	Особенности практического применения архитектуры Spine&Leaf в реалиях современного высоконагруженного CDN
Инфраструктура связности	с. 36	MSK-IX – на острие технологий
	с. 40	Роль точек обмена трафиком в цифровом прогрессе Ближнего Востока
	с. 49	К вопросу о прочности подводных интернет-кабелей
	с. 54	Спутниковые сети связи, или как «поймать всю рыбу в одну сеть»
	с. 62	Многофакторный анализ функционирования системы спутниковой связи Starlink. Что в ней хорошего, плохого и «злого»?
Наука и образование	с. 66	Связность и идентификаторы Интернета
Технология и право	с. 74	Некоторые аспекты дефиниции «Connectivity»
Вокруг технологии	с. 78	Виноделие и цифровое вино
Юбилей 2025	с. 82	Мария Колесникова: «Домен .рф меняет сознание разработчиков»
Новости	с. 86	Новости науки и техники
	с. 88	Новости доменной индустрии

Сетевое издание  
Журнал «Интернет изнутри»  
info@internetinside.ru

Выпуск №22, дата выхода:  
Апрель 2025 г.

Свидетельство о регистрации  
СМИ в Федеральной службе  
по надзору в сфере  
связи, информационных  
технологий и массовых  
коммуникаций.  
Регистрационный номер:  
ЭЛ № ФС 77 — 85232 от 25.04.2023  
ISSN: 2949-1967

Все статьи размещаются  
и индексируются в НЭБ «e-Library»

Издатель: **Фонд развития  
сетевых технологий «ИнДата»**

Главный редактор:  
**Алексей Платонов**

Выпускающий редактор:  
**Ирина Пыжова**

Редакционная коллегия:  
**Елена Воронина  
Марат Биктимиров  
Алексей Платонов**

Продакшн:  
**Алексей Гончаров**

Дизайн и вёрстка:  
**Антон Иванов**

Корректор:  
**Наталья Рябова**

Обложка разработана  
с использованием ресурсов сайта  
Freepik.com

# Сетевая связность

Дорогой читатель,

Коммуникации и связь являются основой Интернета, и потому эта тема присутствует так или иначе во всех выпусках нашего журнала. Однако говоря о связи в Интернете, мы часто используем другой термин – связность (от англ. Connectivity), который более соответствует многоплановости сетевого взаимодействия в этой экосистеме. Начнём с того, что в отличие от традиционной телефонии, связь между двумя точками в Интернете не предусматривает создания выделенного канала. В Интернете все каналы передачи данных виртуальны и динамичны, они могут изменяться в отношении как топологии, так и пропускной способности и других параметров производительности. Во-вторых, взаимодействие в Интернете на уровне приложений имеет характер транзакций, для обеспечения которых могут создаваться десятки, если не сотни разнообразных сеансов связи – от создания динамического контента страницы до загрузки удалённых ресурсов и рекламы.

Другими словами – связность гораздо более сложное и многогранное понятие, чем просто связь. Неудивительно, что мы опять вернулись к этой теме (в 2016 году мы также выбрали связность в качестве ключевой темы выпуска № 3).

Открывают журнал две статьи – «Влияние развития периферийных сетевых вычислений на Интернет» и «Эволюция связности в эпоху нулевого доверия», в которых авторы рассматривают процесс эволюции связности от «классического» Интернета 90-х годов прошлого столетия до сегодняшнего дня. Поражают как прогресс, который эта коммуникационная экосистема совершила за последние 30 лет, так и тот факт, что развитие все эти годы шло без какого-либо единого плана и управления.

Мы, конечно, поговорим о технологиях и инфраструктуре передачи данных. Ряд интересных статей представлены в традиционном разделе «Технология в деталях», а также под новой рубрикой «Инфраструктура связности».

В разделе «Образование и наука» Павел Храмцов предлагает краткий обзор системы идентификаторов Интернета и их роли в обеспечении связности. А в статье «Виноделие и цифровое вино» Сергей Зимин рассуждает о том, чем похожи телекоммуникации и виноделие и в чём разница между ними, а также даёт советы по правильному винопитию всем работникам IT-отрасли.

Не обошли мы вниманием и факт, что в этом году отмечается сразу два юбилея. MSK-IX исполняется 30 лет, и в юбилейной статье Елена Воронина и Евгений Морозов вспоминают этапы большого пути и рассуждают о будущем развитии. А первый национальный кириллический домен .рф 12 мая 2025 года отметит свое 15-летие, и о том, как сегодня себя чувствуют кириллические домены в мировом доменном пространстве, расскажет руководитель проекта «Поддерживаю.РФ» Мария Колесникова.

Ну и конечно, мы продолжаем поддерживать наши традиционные разделы. В разделе «Политика» Мадина Касенова анализирует понятие «связность» в контексте нормативной и регуляторной деятельности в России и за рубежом. А в «Новостях» мы познакомим вас с интересными фактами и событиями, произошедшими в Интернете и доменной индустрии в последнее время.

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](mailto:info@internetinside.ru).



# Влияние развития периферийных сетевых вычислений на Интернет

Олаф Колкман, Андрей Робачевский,  
Карл Ганберг, Хусейн Бодран –  
«Общество Интернета»



## Аннотация

Постепенное повышение требований к скорости доступа к интернет-ресурсам и снижению времени отклика вызвало изменения в системе передачи данных Интернета, а именно размещение вычислительных мощностей и хранилищ данных ближе к конечным потребителям. Это повлекло за собой внедрение новой телекоммуникационной инфраструктуры, характеристики которой отличаются от традиционных характеристик Интернета.

В данной статье рассматривается ряд вопросов, связанных с эволюцией Интернета в плане поддержки периферийных вычислений. Затрагиваемая в работе проблематика позволит понять, станет ли развитие технологии периферийных вычислений решающим фактором в эволюции Интернета в целом и приведёт ли это к появлению новой телекоммуникационной инфраструктуры, работа которой будет построена на принципиально других началах. Иными словами, сохранит ли Интернет свою основополагающую роль на фоне появления новых видов сетевой архитектуры и приложений, продолжит ли он существовать и развиваться?

## Введение

Выступая в роли «сети сетей», Интернет обеспечивает связность на глобальном уровне. Можно сказать, что он выступает в качестве наиболее значимого фактора начавшейся в последние десятилетия XX века цифровой трансформации. Этот процесс продолжит играть определяющую роль в нашем обществе на всём протяжении XXI века. Авторы входят в коллектив «Общества Интернета» (Internet Society, ISOC) – организации, выступающей за полноценное развитие Интернета в соответствии с принципами глобальности, открытости, безопасности и достоверности. В основе этого развития лежит то, что мы называем «отличительными свойствами Интернета» или «сетевым взаимодействием на основе принципов работы Интернета» (Internet Way of Networking) [8]. Такой подход подразумевает использование инфраструктуры с универсальным протоколом, модульной архитектуры, а также обеспечение взаимосвязанности сетей на добровольной основе для формирования единой сети сетей, в которой

прикладная функциональность расположена на периферии. Интернет развивается и меняется на наших глазах. Всё большую актуальность приобретают так называемые периферийные сети, например, сети широкополосного доступа и доставки контента, работа которых определяется ожидаемыми потребностями потребителей и бизнеса. В этой связи встаёт следующий вопрос: будут ли такие периферийные сети играть определяющую роль в развитии Интернета, что приведёт к созданию новой коммуникационной инфраструктуры и изменению её основных характеристик? Может ли Интернет продолжить существовать и успешно развиваться в качестве фундамента для других сетевых архитектур и приложений? Поскольку ставить точку в том, что касается эволюции Интернета, на данный момент представляется преждевременным, авторы не будут пытаться дать читателю окончательный ответ на эти вопросы. Вместо этого они представят свою точку зрения и сформулируют ряд вопросов и тезисов, которые помогут лучше понять рассматриваемую проблематику.

Во втором разделе авторы разъясняют, что они понимают под полноценным, то есть нормальным функционированием Интернета, а в третьем разделе рассматривают факторы, способствующие распространению сетевых технологий на базе периферийных вычислений как, например, потребительский спрос. В четвертом разделе сравниваются четыре модели-этапа развития Интернета. В пятом разделе изложены те вопросы, которые призваны дать нам возможность лучше понять сформулированную в начале предыдущего абзаца проблему.

## Свойства Интернета

Чтобы понять, насколько нормально и полноценно развивается Интернет, нам потребуется установить определённый целевой показатель или взять за основу определение так называемого здорового Интернета. В этих целях воспользуемся руководством Internet Way of Networking [8]. «Общество Интернета» провело серию круглых столов и исследований в рамках интернет-сообщества для выявления основных, критически важных характеристик Интернета, которые определяют его развитие и адаптацию к современным реалиям. Эти характеристики стали залогом экономического и технологического развития в глобальном масштабе. Ниже приводится краткое описание этих критически важных характеристик и их преимуществ.

Основополагающие характеристики	Преимущества
1. Доступная инфраструктура с общим протоколом, характеризующаяся открытостью и низким входным порогом.	Обеспечение неограниченного доступа и использование общих протоколов обеспечивают глобальную связность и способствуют развитию сети. По мере подключения всё большего числа участников Интернет приобретает всё большее значение и становится всё более ценным ресурсом для всех его пользователей.
2. Открытая архитектура взаимозаменяемых, многократно используемых составляющих, основанных на открытых стандартах, внедрение и использование которых сообществом пользователей осуществляется на добровольной основе.	Использование открытой архитектуры позволяет создавать общие, взаимосвязанные и взаимодополняющие услуги, обеспечивающие ускоренное внедрение инноваций без необходимости получения каких-либо разрешений. Инклюзивный процесс стандартизации и внедрение решений, исходя из запросов и потребностей пользователей обеспечивает принятие полезных нововведений и отмирание невостребованных элементов.

3. Децентрализованное управление и единая гибкая система распределённой маршрутизации, поддающаяся масштабированию.	Распределённая маршрутизация обеспечивает устойчивость и адаптивность сети автономных подсетей, позволяя оптимизировать их работу на локальном уровне, при этом сохраняя глобальную связность.
4. Система общих глобальных идентификаторов, которые являются однозначными и универсальными.	Наличие общей системы идентификаторов обеспечивает стабильную работу систем адресации и позволяет рационализировать функционирование всей сети, избежав её фрагментации или деления.
5. Простая и адаптивная технологически нейтральная сеть общего назначения.	Применение общих подходов обеспечивает гибкость. Сообщество интернет-пользователей очень разнообразно и постоянно меняется. То же самое можно сказать о сферах применения Интернета. Технологически нейтральная сеть общего назначения может обеспечить поддержку такой динамической среды без каких-либо существенных изменений.

Эти критически важные характеристики представляют собой своего рода идеалы, сформулированные в технологически нейтральных терминах. Соответственно, при ослаблении этих характеристик получить те преимущества, которые призван обеспечивать Интернет, будет сложнее. В своём нынешнем виде Интернет не соответствует всем этим характеристикам. Например, в том, что касается первой характеристики, можно сказать, что в настоящее время интернет-протокол (IP) выступает в качестве общепринятого протокола. Однако он существует в двух вариантах - IPv4 и IPv6. Очевидно, что переход на IPv6 не соответствовал первой характеристике. Это свидетельствует о необходимости использования таких механизмов перехода, как 6rd [5], 6rd [9] и NAT64 [4], для того, чтобы пользователи сетей, в которых используется исключительно протокол IPv6, могли в полной мере воспользоваться теми преимуществами, которые призван обеспечивать Интернет.

Возникает вопрос: не оказывает ли развитие периферийных вычислений негативного воздействия на эти критически важные характеристики?

## Эволюция Интернета

Цель данного раздела – создать общее представление об эволюции Интернета, выявив при этом четыре этапа в его

развитии<sup>1</sup>, что позволит лучше понять суть рассматриваемой проблематики.

**Классический период:** эпоха интернет-классицизма. Классическая эпоха в развитии Интернета завершилась в 1990-х годах. В это время Интернет представлял собой транспортную сеть сетей с минимальной функциональностью ядра для поддержки приложений. Ни серверы, ни клиенты не обладали возможностью оптимизации трафика и не пользовались такими решениями. Если клиенту в одном уголке мира нужно было получить какие-то данные с другого конца света, пакеты данных отправлялись в длительное путешествие. Тогда время отклика составляло от 10 до 100 мс, тогда как скорость подключения конечных пользователей составляла от нескольких сотен килобит до 1 мегабита в секунду. Инфраструктура действовала в глобальном масштабе.

**Начало освоения кеш-памяти:** гибридный Интернет, периферийные вычисления на региональном уровне. 1990-е годы и начало нового тысячелетия отмечены растущим применением технологии кеширования и увеличением числа точек обмена и центров хранения и обработки данных. Серверы теперь размещаются ближе к пользователям, что, в первую очередь, было призвано сократить издержки при передаче информации. Наблюдается развитие решений, которые сейчас принято называть облачными технологиями. Размещение серверов для их обслуживания производится по региональному принципу. Динамическая система доменных имён [RFC2136] и технология аникаст [RFC3258] обеспечили максимальную оперативность доступа к запрашиваемому контенту. Двухсторонняя задержка составляет от 10 до 100 мс, тогда как скорость подключения выросла, достигнув диапазона от 10 до 100 мегабит в секунду. Поскольку инфраструктура преимущественно строилась по региональному принципу (покрытие в радиусе порядка 1000 км), мы назвали данное решение «удалённым облаком».

**Гипермасштабирование:** гибридный Интернет, приближение периферийных вычислений к пользователю. Период с 2010 по 2020 годы прошёл под знаком виртуализации сетевых и компьютерных технологий, а также автоматизации технологических процессов сборки, настройки и развёртывания программного обеспечения, что привело к распространению гипермасштабирования. Это сделало возможным развитие различных услуг, включая потоковую передачу видео и интерактивные компьютерные игры в высоком разрешении. Время отклика снизилось до примерно 10 мс, а иногда и даже ниже этого уровня, тогда как скорость подключения пользователей достигла диапазона от сотен мегабит до нескольких гигабит в секунду. Облачные хранилища теперь размещаются ближе к пользователям и носят более децентрализованный характер, находясь в радиусе примерно 100 км. Размещение инфраструктуры всё больше осуществляется по региональному принципу. Ещё одной отличительной чертой данного пе-

риода стало строительство крупными операторами доставки контента своих собственных опорных сетей с целью снижения зависимости от инфраструктуры Интернета в её классическом исполнении.

**Расслоение Интернета:** трансформация услуг в соответствии с принципами функционирования телекоммуникационной отрасли. Характерной чертой 2020-х годов стала идея ожидаемого расслоения в рамках архитектуры сетей 5G [2]. Хранилища и компьютерная инфраструктура располагаются в десятках или сотнях километров от пользователя, что позволило снизить время задержки до миллисекунды, а то и ниже, тогда как скорость подключения превысила 1 гигабит в секунду. Необходимая инфраструктура становится ещё ближе и нередко размещается в одном населённом пункте с пользователем.

Хотя в реальной жизни такая архитектура пока встречается редко, идея её воплощения в жизнь то и дело всплывает в различных программных документах, в которых её описывают как провозвестницу эпохи Web 3.0, которая бы обеспечила возможность развивать голографические решения, дополненную реальность и метавселенную.

Существует мнение, что для освоения таких технологий потребуются специализированные сети, которые бы обеспечили соответствующее качество взаимодействия с точки зрения снижения искажения сигнала, времени задержки, повышения пропускной способности или всё это одновременно (см., например, доклад «Сеть 2030» Сектора стандартизации электросвязи МСЭ [1]).

В данной модели функционирование каждого слоя определяется соответствующей услугой, а привязка сетевых мощностей к оказанию конкретной услуги (с возможностью взимать за это отдельную плату) во многом напоминает принятые в телекоммуникационной отрасли модели. Соответственно, данную модель можно назвать «телекоммуникационной» сетью. Это не означает, что такие услуги оказываются существующими телекоммуникационными операторами – любое лицо, представленное на местном рынке и располагающее необходимым финансированием, может оказывать такие услуги.

## Сравнение четырёх моделей

Таким образом, перед нами четыре модели-этапа развития Интернета: так называемая классическая эпоха, время развития периферийной инфраструктуры по региональному принципу, максимальное приближение такой инфраструктуры к пользователю и переход на оказание услуг по модели телекоммуникационных операторов. Первые три модели представляются закономерными этапами в развитии Интернета, поскольку основные свойства Интернета оставались неизменными. В основе всех этих технологий лежат общие идентификаторы, а Интернет в них рассматривается в качестве общедоступного средства связи, функционирует за счёт стандартных элементов, а его работа определяется принципами распределённого масштабирования и самостоятельного, децентрализованного принятия решений отдельными субъектами.

<sup>1</sup>Авторы осознают, что выступают с позиций стран Северной Америки и Западной Европы, которые находились в авангарде описываемых процессов. Очевидно, что развитие периферийных сетей может усугубить цифровое неравенство. Признав этот факт, отметим, что данная тема находится за рамками рассматриваемой в данной статье проблематики.



Однако на стадии максимального приближения инфраструктуры к пользователям намечается изменение моделей распределения потоков данных и формируется тенденция к созданию операторами инфраструктуры гипермасштабируемых сетей собственных систем связи. Иногда (но не всегда) в основе таких решений лежат традиционные интернет-технологии. Таким образом, возникает вопрос о необходимости и целесообразности такой трансформации [3].

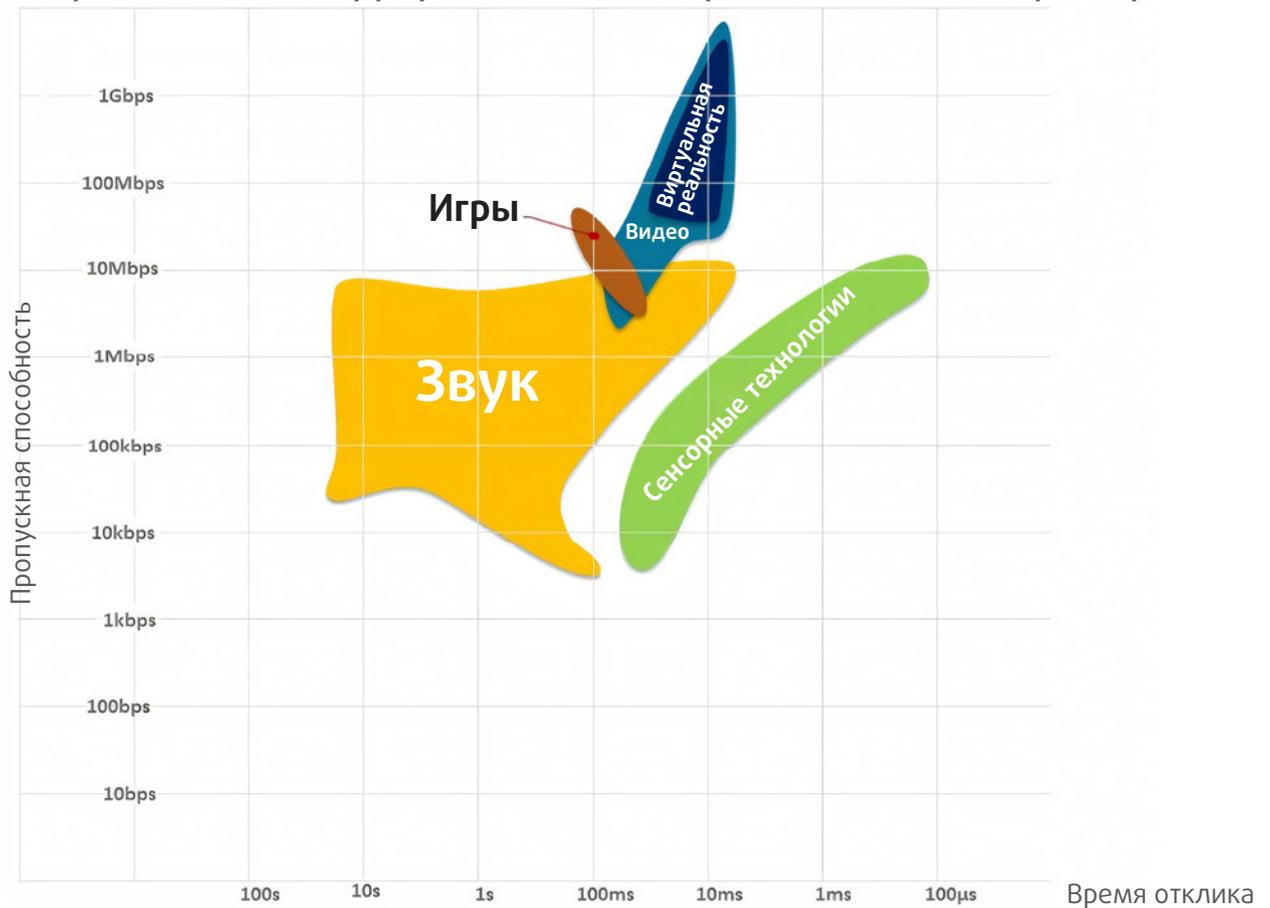
В недавно опубликованном докладе британского Управления по делам радио, телевидения и предприятий связи [6] приводятся данные по требуемым показателям пропускной способности и времени задержки в зависимости от приложения. На рисунке 1 показана диаграмма, отражающая прогнозируемые требования к таким параметрам. Можно сделать вывод, что при повсеместном распространении инфраструктуры периферийных вычислений в непосредственной близости от пользователя интернет-технологии могут обеспечить функционирование многих видов деятельности и приложений, тогда как для решения ограниченного круга задач потребуются специализированные сети.

Вопрос во многом спорный. Для снижения времени задержки свыше 10 мс и пропускной способности, не превышающей 1 гигабита, достаточно инфраструктуры регионального или глобального уровня. Соответственно, для снижения времени задержки ниже 10 мс и увеличения пропускной способности выше 1 гигабита в секунду, скорее всего, потребуется максимально приблизить инфраструктуру к пользователю с её привязкой к

конкретному назначению. В результате может получиться так, что обычные интернет-сети не справятся с определёнными видами виртуальной реальности, основанными на сенсорном интерфейсе, системами или услугами Интернета вещей в их преимущественно промышленном исполнении. Во всех остальных сферах с экономической точки зрения представляется целесообразным продолжить пользоваться более простой сетевой архитектурой и недорогими сетевыми стеками на базе IP. Перенос в сеть избыточных вычислительных мощностей может оказаться слишком дорогим удовольствием (аргумент Сальцера относительно сквозной (end-to-end) архитектуры в его первоначальном виде заключается в том, что стоимость оптимизации функционирования сети может оказаться неоправданной по сравнению с полученным результатом [7]).

Специализированные сети из четвёртой модели могут потребовать несовместимого с Интернетом или конкретным приложением способа использования стека (некоторых элементов), что приведёт к фрагментации сетевого пространства. При этом высока вероятность сосуществования и возникновения взаимозависимости этих двух видов сетевых технологий, то есть глобального Интернета и универсального протокола с одной стороны и специализированных сетей с другой стороны. Работу большинства таких специализированных сетей необходимо будет координировать и обеспечивать соответствующим образом, чтобы они могли хотя бы отчасти задействовать преимущества Интернета. В такой среде стандартным решением представляется использование шлюзов.

Требования по качеству услуг для использования решений в области «Интернета чувств»



Требования по качеству услуг для использования решений в области «Интернета вещей»

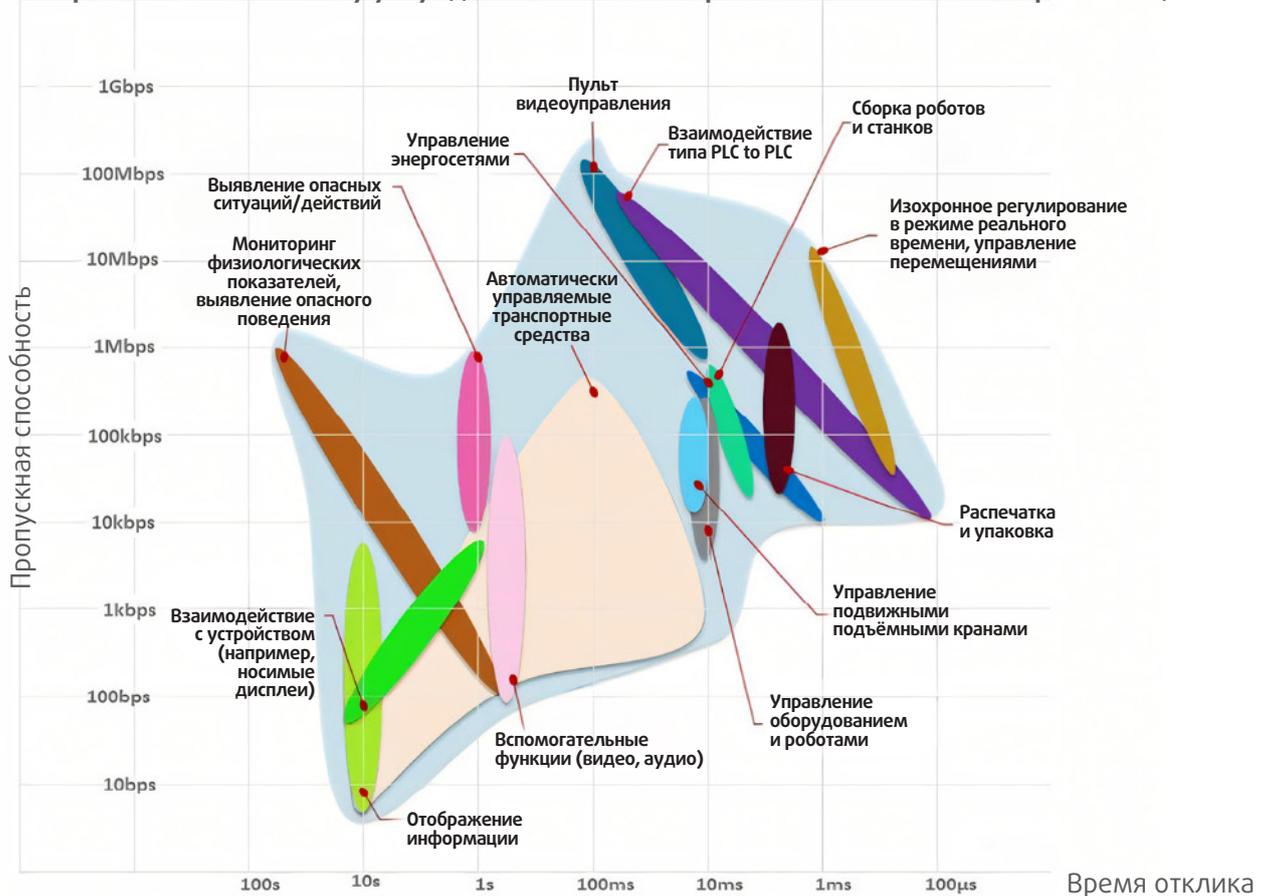


Рис. 1. Пропускная способность и требования по задержке отклика для приложений различных классов.

Источник: Доклад Ofcom «Будущее интернета» [6].

## Вопросы, вопросы, вопросы

Описанный выше процесс изменения и развития Интернета начинается с эпохи классического Интернета, затем переходит в стадию размещения вычислительных мощностей по региональному принципу, после чего эти мощности максимально приближаются к пользователю, а обслуживание переходит на принятую среди телекоммуникационных операторов модель. Эти тенденции могут свидетельствовать о постепенном замещении традиционных архитектур радикально новыми решениями. Главный вопрос в этой связи заключается в том, останется ли Интернет в его классическом исполнении незаменимым инфраструктурным элементом или его постепенно вытеснят другие виды архитектуры. Что же это означает для общества? Сохранят ли свою актуальность преимущества от построения сетей по заложенным в основу Интернета принципам?

«Общество Интернета» изучает влияние программных и технологических изменений и предложений через призму основных характеристик Интернета, а также в свете приведённых нами основополагающих вопросов.

### Стоит ли развивать сети, исходя из лежащих в основе Интернета принципов?

Чтобы понять, каким образом описанные этапы в развитии Интернета соотносятся друг с другом, важно ответить на вопрос, остаётся ли устаревшая инфраструктура востребованной и зависят ли появившиеся на следующем этапе услуги от принятых ранее решений. Если это так, то можно говорить о сосуществовании относящихся к разным этапам развития Интернета решений, а не о постепенном замещении одних технологий другими. В таком преломлении становится понятнее, в чём заключается ценность основополагающих принципов функционирования Интернета. В какой степени новейшие системы доставки контента, облачные технологии, периферийные вычисления и так далее зависят от технологий, созданных в так называемую эпоху классического Интернета? В какой степени способность Интернета брать на себя функции, которые до этого на него никогда не возлагались, то есть ещё не появившиеся модели и решения в области построения сетей, можно считать новым видом общественного достояния, которое нужно оберегать и защищать, чтобы такие преимущества были доступны для всех?

### Возможна ли миграция инноваций?

Одним из преимуществ подхода Internet Way of Networking является то, что он способствует внедрению инноваций без необходимости получать для этого какие-либо разрешения. Это результат того, что сеть универсальна, технологически нейтральна и доступна для всех.

Это преимущество сохранилось, несмотря на развитие облачных технологий с созданием соответствующей инфраструктуры на региональном уровне. Это никак не препят-

ствует использованию интернет-серверов, где бы они ни находились, для размещения инноваций и их масштабирования по мере увеличения спроса. Для того, чтобы развивать какую-нибудь услугу, крупных инфраструктурных капиталовложений или проведения переговоров с местными провайдерами не требуется. Возможность масштабирования рассматривается выходящими на рынок небольшими прямыми поставщиками контента как операционный расход. Конечно, доступ к расположенному в непосредственной близости от передатчика центру хранения данных обойдётся дороже, причем лишь немногие смогут воспользоваться таким преимуществом. Кроме того, объём хранилища тоже ограничен. Вероятно, доступ к таким объектам смогут получить только те, кто имеет возможность отстаивать свои интересы и/или представлен на местном рынке.

Возникает вопрос: можно ли ждать повсеместного перехода приложений, нуждающихся в таком доступе, на инновационные решения?

Можно также спросить, будут ли специализированные приложения обладать достаточной степенью открытости, чтобы воспользоваться теми преимуществами, которые может дать им Интернет? Можно ли предположить, что их запуск в обособленной среде исключит возможность их использования в Интернете?

### Куда направлены инвестиции?

Если специализированные сети и сегменты станут прибыльными и конкурентоспособными, сохранится ли возможность привлекать инвестиции для развития универсальной инфраструктуры? Как уже было отмечено, сторонники гипермасштабирования активно вкладываются в развитие отдалённых и приближенных периферийных вычислений. Увеличится ли роль универсальных интернет-решений в том, что касается оказания и согласования услуг, по мере приближения вычислительных мощностей и центров хранения данных к пользователям?

Насколько велик потенциал успешных бизнес-моделей для привлечения инвестиций в традиционные интернет-технологии?

### И ещё вопросы...

Эти процессы сопряжены ещё с целым рядом вопросов. Каким образом качество интернет-услуг определит дальнейшее развитие этого сектора? Будет ли развитие Интернета способствовать его сохранению вместе с обеспеченными им преимуществами или же эти процессы приведут к большей фрагментации инфраструктуры и ограничению степени её децентрализации? Ответов на эти вопросы у нас нет, что не мешает нам стремиться выявить те факторы, которые обеспечивают эффективное развитие Интернета, а также продолжать обсуждать эту тему.

<sup>2</sup>На данном этапе считается, что такое требование противоречит приведённой в таблице третьей ключевой характеристике Интернета, поскольку для обеспечения высокого качества обслуживания в различных сетях и юрисдикциях потребовалось бы применение законодательных и надзорных механизмов, которые подразумевают наличие централизованного управления в той или иной форме.

## Заключение

В данной статье мы описали развитие Интернета - от модели глобальной универсальной связности до фрагментации инфраструктуры хранения данных и вычислений по региональному принципу. По нашему мнению, в некоторых случаях переход на специализированные сетевые решения представляется оправданным. Также делается утверждение, что это не означает исчезновения универсальных интернет-технологий, которые будут сосуществовать со специализированными сетями. Наконец, обозначен ряд вопросов, которые позволят нам лучше понять эти процессы и ответить на вопрос о потенциальной общественной пользе этих изменений. Хочется верить, что данная статья будет способствовать продолжению дискуссии о развитии одного из основополагающих элементов созданной человечеством инфраструктуры.

## Благодарности

Данная статья – результат обсуждения затрагиваемой проблематики небольшой группой специалистов «Общества Интернета». Хотелось бы особо отметить вклад Акрити Бопанна и выразить ей нашу благодарность. ■

## Список литературы:

- [1] FG-NET2030 - Focus Group on Technologies for Network 2030. 2020. Network 2030 - Gap Analysis of Network 2030 New Services, Capabilities and Use cases. Technical Report. ITU-T. [https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Gap\\_analysis\\_and\\_use\\_cases.pdf](https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Gap_analysis_and_use_cases.pdf)
- [2] Xenofon Foukas, Ahmed Elmokashfi, Georgios Patounas, and Mahesh K. Marina. 2017. Network Slicing in 5G: Survey and Challenges (12 May 2017), 94–100 pages. <https://doi.org/10.1109/MCOM.2017.1600951>

- [3] Geoff Huston. 2016. The death of transit (2016). <https://blog.apnic.net/2016/10/28/the-death-of-transit/>
- [4] Xing Li, Mohamed Boucadair, Christian Huitema, Marcelo Bagnulo, and Congxiao Bao. 2010. IPv6 Addressing of IPv4/IPv6 Translators. Request for Comments RFC 6052. Internet Engineering Task Force. <https://doi.org/10.17487/RFC6052> Num Pages: 18.
- [5] Masataka Mawatari, Masanobu Kawashima, and Cameron Byrne. 2013. 464XLAT: Combination of Stateful and Stateless Translation. Request for Comments RFC 6877. Internet Engineering Task Force. <https://doi.org/10.17487/RFC6877> Num Pages: 14.
- [6] Ofcom. 2021. Internet Futures, Spotlight on the technologies which may shape the Internet of the future (July 2021). [https://www.ofcom.org.uk/\\_\\_data/assets/pdf\\_file/0013/222205/internet-futures.pdf](https://www.ofcom.org.uk/__data/assets/pdf_file/0013/222205/internet-futures.pdf)
- [7] J. H. Saltzer, D. P. Reed, and D. D. Clark. 1984. End-to-end arguments in system design. ACM Trans. Comput. Syst. 2, 4 (Nov. 1984), 277–288. <https://doi.org/10.1145/357401.357402>
- [8] Internet Society. 2020. Internet Impact Assessment Toolkit (Sept. 2020). <https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/>
- [9] Mark Townsley and Ole Trøan. 2010. IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) – Protocol Specification. Request for Comments RFC 5969. Internet Engineering Task Force. <https://doi.org/10.17487/RFC5969> Num Pages: 18.

## Об авторах

Olaf Kolkman, Andrei Robachevsky, Carl Gahnberg, and Hosein Badran. 2022. Evolution of the Edge, what about the Internet? In ACM SIGCOMM 2022 Workshop on Future of Internet Routing & Addressing (FIRA '22), August 22, 2022, Amsterdam, Netherlands. ACM, New York, NY, USA, 5 pages. <https://doi.org/10.1145/3527974>



# Эволюция связности в эпоху нулевого доверия



Константин Чумаченко

## Аннотация

Интернет сегодня — это не только «сеть сетей», но и основа для множества сервисов. В статье исследуется, как развитие прикладных применений Интернета влияло на способность сети передавать данные и меняло значение термина «связность».

## Ключевые слова:

маршрутизация, облачные платформы, CDN, DDoS-атаки, концепция Zero Trust, фрагментация Интернета.

## Введение

Я пишу этот текст в онлайн-редакторе, даже не задумываясь о том, какие потоки информации порождает каждое нажатие клавиши. В это время через сетевой интерфейс моего ноутбука проходит череда интернет-соединений: десятки запросов к серверам по всему миру — авторизация, загрузка шрифтов, обновление счётчиков, работа трекеров. Всё это происходит автоматически, без моего участия, и обретает форму в окне браузера. Если что-то пойдёт не так, мне будет непросто найти причину, хотя я работаю в сфере интернет-технологий не первый год.

Когда-то Интернет был другим. Чтобы открыть файл на удалённом компьютере или прочитать новости, требовалось вручную установить соединение. Возможных результатов было всего два: успех либо ошибка, отображавшаяся в командной строке.

На протяжении десятилетий мы используем IP-протокол, обеспечивающий «связность» — способность устройств, сетей и систем взаимодействовать через Интернет. Инфраструктура сети неоднократно менялась под влиянием технологий, новых моделей поведения пользователей, требований бизнеса и политических процессов. Сегодня «связность» стала сложным, многогранным понятием, охватывающим широкий спектр технологий, и даже профессионалы порой затрудняются дать ей точное определение.

Давайте проследим, как развитие прикладных применений Интернета придало термину «связность» новые значения. Для этого обратимся к ключевым этапам этой эволюции, которые, накатываясь друг на друга, как волны, сформировали современный Интернет.

## Первый бум доткомов

С появлением в конце 1990-х годов таких компаний, как Amazon, eBay и Yahoo!, люди открыли для себя новые возможности: от покупок без походов в магазин до мгновенного доступа к информации и общению. Спрос на подключение резко вырос, Интернет перестал быть инструментом для избранных и стал быстро расширяться.

## Рост операторских сетей и пользовательских подключений

Интернет-провайдеры начали активно расширять свои сети и улучшать качество доступа. К 2000 году число интернет-пользователей в мире достигло 400 миллионов (в 1995 году — всего 16 миллионов). Этот рост был вызван не только удобством новых сервисов, но и снижением стоимости подключения. Количество автономных сетей (AS) выросло с пяти тысяч в 1995 году до десяти тысяч в 2000 году [1].

## Владельцы сетей ищут альтернативы транзиту

Этот период также ознаменовался появлением первых точек обмена интернет-трафиком, IXP (Internet eXchange Points), которые помогли улучшить маршрутизацию и снизить затраты на передачу данных между автономными сетями провайдеров [2]. В 1995–1998 годах были созданы AMS-IX (Амстердам), DE-CIX (Франкфурт), LINX (Лондон) и MSK-IX (Москва), впоследствии ставшие крупнейшими центрами концентрации пирингового трафика в мире.

## Что изменилось?

Бурный рост интернет-инфраструктуры в 1990-х годах заложил основу для современного цифрового мира, в котором связность стала базовой потребностью человека.

## Видеоконтент приходит в сеть

Широкое использование мультимедиа и интерактивных элементов в вебе обострило проблему доставки «тяжёлого» контента (видео, изображений, анимации) через перегруженные межоператорские соединения. Это привело к появлению в конце 1990-х годов сетей доставки контента (CDN, Content Delivery Networks), которые оптимизировали маршруты трафика, кешируя данные на распределённой сети серверов ближе к пользователям. Пионером индустрии стала компания Akamai, основанная в 1998 году.

Внедрение CDN сразу улучшило время отклика сайтов для пользователей, но настоящая революция в интернет-инфраструктуре произошла в период 2005–2015 годов из-за стремительного роста потребления видео. Видео стало доминирующей формой интернет-трафика благодаря YouTube, Netflix, TikTok, сервисам прямой трансляции и пиратскому контенту, распространяемому через P2P-сети. С 2005 года ежегодный отчёт Cisco Visual Networking Index фиксировал кратный рост IP-трафика, а к 2016 году объёмы годового трафика превысили 1 зеттабайт (миллиард терабайтов) [3].

**CDN принесли с собой важные перемены в структуре потоков данных:**

- 1. Глобальное распределение трафика.** CDN используют сложные алгоритмы для балансировки нагрузки между своими узлами по всему миру. Эти алгоритмы могут учитывать состояние серверов, сетевые задержки, загрузку межоператорских соединений и даже стоимость размещения в конкретных дата-центрах. Перенаправление пользовательских запросов осуществляется средствами прикладных протоколов DNS и HTTP. Алгоритмы балансировки CDN стали новой формой маршрутизации данных.
- 2. Локализация трафика.** Чтобы сократить маршруты доставки контента, CDN размещают кеширующие узлы непосредственно в сетях интернет-провайдеров (ISP), активно участвуют в частных пиринговых соглашениях и присутствуют на точках обмена трафиком (IXP). Такая локализация трафика позволяет избежать длинных маршрутов через множество межоператорских стыков и значительно снижает вероятность потерь при доставке контента.

## Что изменилось?

По мере аккумуляции «контрольного пакета» в 60–80% сетевого трафика интересы владельцев CDN — провайдеров услуг и видеосервисов — стали определять пути контента к пользователю. На одной из интернет-конференций я наблюдал горячую дискуссию: операторы, вынужденные справляться с непредсказуемыми всплесками трафика на стыках с CDN, активно выражали недовольство. Тем не менее, благодаря CDN задержки и буферизация перестали быть проблемой для любителей 4K-видео на больших экранах.

## Интернет связывает IT-ландшафт предприятий

Бизнес быстро осознал преимущества удалённого доступа к программам и вычислительным ресурсам через Интернет. В 1999 году компания Salesforce представила онлайн-сервис управления продажами, на долгие годы заняв лидирующие позиции в сегменте SaaS (Software-as-a-Service). В 2006 году Amazon Web Services дала старт эпохе облачных инфраструктурных сервисов, позволив компаниям арендовать серверные мощности без владения физическим оборудованием.

**Популярность облачных сервисов, появление компаний со множеством филиалов, а также тренд на удалённую и мо-**

**бильную работу стимулировали развитие новых технологий управления маршрутизацией и доступом пользователей.**

## Централизация управления маршрутами

Компаниям потребовалась связность с критически важными приложениями с гарантированной пропускной способностью и низкой задержкой. Изначально основой для распределённых корпоративных сетей служили каналы магистральных операторов. Однако растущие потребности в гибкости привели к появлению в начале 2010-х годов технологии SD-WAN (Software-Defined Wide Area Network) [4]. SD-WAN позволяет централизованно управлять подключениями головного офиса и филиалов, абстрагируясь от типа соединения (Ethernet, Wi-Fi, LTE и др.) Единый контроллер обеспечивает гибкую сегментацию сети, настройку политик безопасности и оптимизацию передачи данных. Это позволяет создавать сложные системы «туннелей» для различных типов трафика и приложений, обеспечивая высокую производительность и безопасность.

## Гранулярный контроль доступа пользователей

С внедрением облачных сервисов и веб-приложений границы корпоративных сетей стали размываться, а принцип доверенного периметра устарел. Предприятиям потребовались гарантии, что доступ к приложениям получают только авторизованные пользователи и устройства, независимо от их местоположения. В популярной концепции Zero Trust [5] идентичность и права пользователя проверяются при каждом обращении к ресурсу. Следующие ей современные решения, такие как Secure Access Service Edge (SASE) [6], объединяют компоненты безопасности в сетях и в облачных платформах, интегрируя политики доступа с маршрутизацией.

## Что изменилось?

Сегодня каждая транзакция — будь то доступ к почте или загрузка файлов в облако — проверяется на соответствие политикам доступа. Например, сотрудник, подключающийся к VPN, должен пройти двухфакторную аутентификацию, а его устройство — соответствовать требованиям безопасности, иметь актуальные обновления и антивирус. Политики доступа влияют на сетевые маршруты, например, трафик из офиса к облачному серверу может быть перенаправлен через защищённый канал, чтобы минимизировать риски утечки данных.

Таким образом, современные сети компаний стали не просто «трубами» для передачи данных, а интеллектуальными системами, поведение которых определяется целями безопасности и контроля доступа.

## Сети и облака против кибератак

На фоне стремительного развития интернет-сервисов сетевая безопасность долгое время оставалась второстепенной задачей. Однако с ростом значимости веб-сайтов, приложений и облачных платформ ущерб от кибератак стало невозможно игнорировать. Большой ущерб стали наносить атаки типа Distributed Denial of Service (DDoS), в которых злоумыш-

ленники использовали множество заражённых устройств для генерации огромных объёмов вредоносного трафика.

DDoS-атаки быстро эволюционировали, эксплуатируя слабые пароли устройств (например, IoT-ботнет Mirai), уязвимости протоколов (NTP amplification) и программного обеспечения (Memcached, LDAP reflection), а также ошибки в логике CPU (Meltdown, Spectre). Мощность атаки ботнета Mirai в 2016 году превысила 1 Тбит/с, а в 2024 году его вариация породила атаку в 5,6 Тбит/с [7].

Как показала практика, эффективно противостоять таким атакам могут только системы сопоставимого масштаба.

## Фильтрация DDoS-атак в операторских сетях

Рост вычислительных мощностей сетевого оборудования и развитие технологий анализа данных сделали возможным появление интеллектуальных механизмов анализа IP-пакетов и TCP-соединений. Большинство крупных интернет-провайдеров (ISP) внедрили системы очистки трафика на основе Deep Packet Inspection (DPI), которые интегрированы с машинным обучением и внутрисетевой маршрутизацией. Такие системы позволяют выявлять аномалии на сетевом и транспортном уровнях и блокировать вредоносный трафик ещё до его попадания в сеть клиента.

## Облачные платформы защищают от атак на уровне приложений

Сегодня большинство кибератак осуществляется на уровне приложений. Для таких атак DPI-анализ неэффективен в связи с повсеместным применением шифрования трафика протоколов HTTP и DNS. Ситуация усугубляется тем, что многие атаки на уровне приложений не создают аномального сетевого трафика и выглядят для операторов как обычная пользовательская активность, за которой скрывается эксплуатация уязвимостей веб-ресурсов.

Для эффективного устранения таких угроз необходим анализ запросов к веб-ресурсам с раскрытием TLS/SSL-соединений. Эту возможность реализовали компании Akamai и Cloudflare, подобные сервисы разработаны также в России, в частности, в компании NGENIX, где работаю я. Архитектура распределённых облачных платформ, в которые эволюционировали CDN, эффективно масштабируется как для обработки всплесков легитимного трафика, так и для отражения масштабных атак. Анализ HTTP- и DNS-запросов позволяет выявлять источники вредоносной активности с точностью до конкретного устройства и снизить долю false positives — ошибочных блокировок легитимных запросов.

## Что изменилось?

Кибератаки наглядно показали, что всеобщая связность в

Интернете — это не только благо, но и источник рисков. Количество потенциально уязвимых сетевых устройств уже невозможно подсчитать, поэтому потребность в защите растёт. Системы фильтрации вредоносного трафика на базе операторских сетей и распределённых облачных платформ стали неотъемлемой частью интернет-инфраструктуры, обеспечивая стабильность и безопасность цифровых сервисов.

## Фрагментация Интернета вокруг якорей доверия

**Якорь доверия (trust anchor)** — это критически важный объект или механизм, который служит основой для установления доверия в ходе цифровых транзакций. Вот некоторые примеры якорей доверия в Интернете:

- 1. Корневые DNS-серверы.** Система доменных имён (DNS) полагается на корневые серверы как на якоря доверия для преобразования доменных имён в IP-адреса [8]. В управлении и обеспечении работы корня DNS принимают участие различные организации: ICANN, Verisign, а также организации-операторы корневых серверов. Кроме того, с внедрением DNSSEC появился ещё один якорь — ключ корневой зоны. Эта система управляется ICANN (IANA) и Verisign под надзором международной общественности (Trusted Community Representatives). С 2021 года якорем доверия для российских национальных доменов .ru и .рф является Национальная система доменных имён (НСДИ).
- 2. Удостоверяющие центры (Certificate Authorities, CAs).** Корневые удостоверяющие центры (УЦ) являются якорями доверия в системах цифрового обмена с использованием открытых ключей (Public Key Infrastructure, PKI). Они выпускают подписанные цифровые сертификаты, которые используются для подтверждения идентичности нижестоящих УЦ, веб-сайтов, устройств и отдельных лиц. Например, для проверки подлинности веб-сайта браузер проверяет, что SSL/TLS-сертификат сайта может быть удостоверен корневым удостоверяющим центром напрямую или через цепочку промежуточных сертификатов. При успешной проверке пользователь видит замочек в адресной строке браузера. Статус корневого УЦ для систем PKI может устанавливаться законодательно, быть результатом отраслевого соглашения или определяться единолично владельцем системы. Примерами корневых УЦ в мире являются организации GlobalSign и Let's Encrypt, для юридически значимого обмена в России эту функцию выполняют Минцифры и ФНС.
- 3. Серверы точного времени.** В системе серверов точного времени, поддерживающих протокол NTP, роль якорей доверия играют серверы, получающие сигнал непосредственно от спутниковых систем, таких как GPS, ГЛОНАСС или китайской Beidou. Эти серверы выступают в качестве источника точного времени для NTP-серверов нижестоящих уровней.

В широком контексте управления Интернетом роль якорей доверия могут выполнять технологические стандарты (например, шифрование в соответствии с ГОСТ [9]), а также нормативные акты. Например, законы ФЗ-152 в России и GDPR в странах ЕС устанавливают требования к обработке персо-

нальных данных в соответствующих юрисдикциях и вводят ограничения на их трансграничную передачу.

## Что изменилось?

Интернет стал неотъемлемой частью сложных общественно-политических отношений. Фрагментация Интернета вокруг различных якорей доверия, ограничения трансграничных потоков данных, блокировки противоправного контента обусловлены соображениями контроля и безопасности, которые превалируют в сегодняшнем мире.

## От IP к AI и дальше

Как видно из примеров выше, хотя протокол IP сохраняет глобальную совместимость устройств, на связность — возможность обмена данными — влияет множество факторов:

- 1. Техническая возможность подключения и качество соединения.** Потери пакетов, задержки, джиттер и другие параметры, определяющие качество связи.
- 2. Масштабируемость и устойчивость сетей.** Способность операторов справляться с растущим трафиком и обеспечивать стабильность работы.
- 3. Межоператорское взаимодействие.** Условия пиринга и транзита между сетями.
- 4. Балансировка и оптимизация нагрузки.** Распределение трафика умными алгоритмами при доступе к веб-ресурсам и приложениям.
- 5. Политики маршрутизации и управления доступом.** Особенности работы корпоративных сетей и облачных платформ.
- 6. Защита от DDoS-атак и вредоносной активности.** Системы фильтрации, обеспечивающие безопасность и доступность сервисов.
- 7. Доверие и безопасность.** Выбор якорей доверия (например, корневых сертификатов) для проверки подлинности транзакций, определение источников доверенной информации и правил обработки данных.

Этот список далеко не исчерпывающий. Например, применение рекомендательных алгоритмов, определяющих, какие видеоролики показывать пользователям, или антифрод-систем, дающих красный или зелёный свет финансовым транзакциям, также можно считать факторами, влияющими на связность.

**Можно быть уверенным, что перспективные технологии, старт которых мы наблюдаем сегодня, в очередной раз изменят потоки данных и создадут новые формы связности в сети.**

- 1. 5G и спутниковые сети.** Операторы мобильных сетей и спутниковых группировок (например, Starlink и Qianfan) обещают повсеместный высокоскоростной доступ для пользователей и IoT-устройств, устраняя «белые пятна» в покрытии.
- 2. Децентрализованные архитектуры.** Технологии, такие как блокчейн и децентрализованные вычисления, могут снизить зависимость от облачных провайдеров, вернув нас к эпохе одноранговых сетей.

- 3. Периферийные вычисления (Edge Computing).** Облачные провайдеры развёртывают инфраструктуру ближе к пользователям, чтобы снизить задержки и улучшить производительность SaaS-приложений.
- 4. Искусственный интеллект (AI).** Как прогнозирует Сатья Наделла из Microsoft, SaaS скоро прекратит своё существование, уступив место веб-интерфейсам для AI-агентов [10]. Это сделает связность с AI-платформами критически важной для веб-приложений.

Связность Интернета продолжает развиваться благодаря накоплению знаний и потребности решать с помощью сети всё более сложные задачи. В биологии эволюция часто ведёт к усложнению организмов. Будем надеяться, что Интернет, как «цифровой организм», сможет адаптироваться к изменениям среды и успешно справиться с вызовами завтрашнего дня. ■

## Список литературы:

- [1] G. Houston, The 32-bit AS Number Report, <https://www.potaroo.net/tools/asn32>, дата обращения: март 2025.
- [2] I. Castro, Shaping the Internet: History and Impact of IXP Growth, 2019, [https://labs.ripe.net/author/ignacio\\_castro/shaping-the-internet-history-and-impact-of-ixp-growth](https://labs.ripe.net/author/ignacio_castro/shaping-the-internet-history-and-impact-of-ixp-growth), дата обращения: март 2025.
- [3] Cisco, Press Release Cisco Visual Networking Index, 2014, <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2014/m06/cisco-visual-networking-index-predicts-annual-internet-traffic-to-grow-more-than-20-percent-reaching-1-6-zettabytes-by-2018.html>, дата обращения: март 2025.
- [4] Palo Alto Networks, What Is SD-WAN?, <https://www.paloaltonetworks.com/cyberpedia/what-is-sd-wan>, дата обращения: март 2025.
- [5] J. Kindervag, Build Security Into Your Network's DNA: The Zero Trust Network Architecture, Forrester Research, 2010, [https://www.virtualstarmedia.com/downloads/Forrester\\_zero\\_trust\\_DNA.pdf](https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf), дата обращения: март 2025.
- [6] Palo Alto Networks, What is SASE?, <https://www.paloaltonetworks.com/cyberpedia/what-is-sase>, дата обращения: март 2025.
- [7] The Cloudflare Blog, Record-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4, 2025, <https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/>, дата обращения: март 2025.
- [8] IANA, Root Zone Management, <https://www.iana.org/domains/root>, дата обращения: март 2025.
- [9] ТЦИ, «Веб-серверы и ГОСТ-криптография», 2023, <https://tcinet.ru/press-centre/articles/7759>, дата обращения: март 2025.
- [10] Satya Nadella on the Future of SaaS, 2025, <https://www.youtube.com/watch?v=GuqAUv4UKXo>, дата обращения: март 2025.

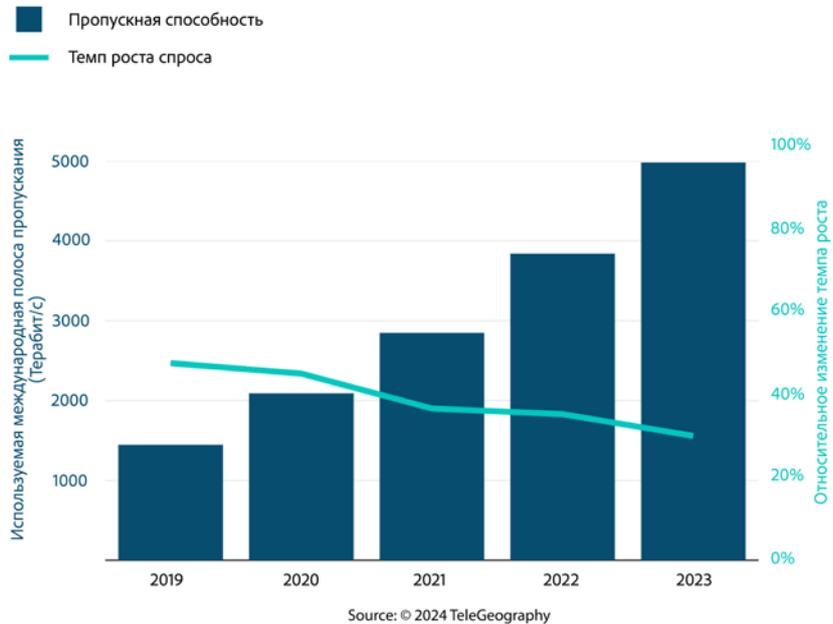
## Об авторе:

Чумаченко Константин Викторович,  
генеральный директор компании NGENIX

# Интернет в цифрах

## Рост международной пропускной способности

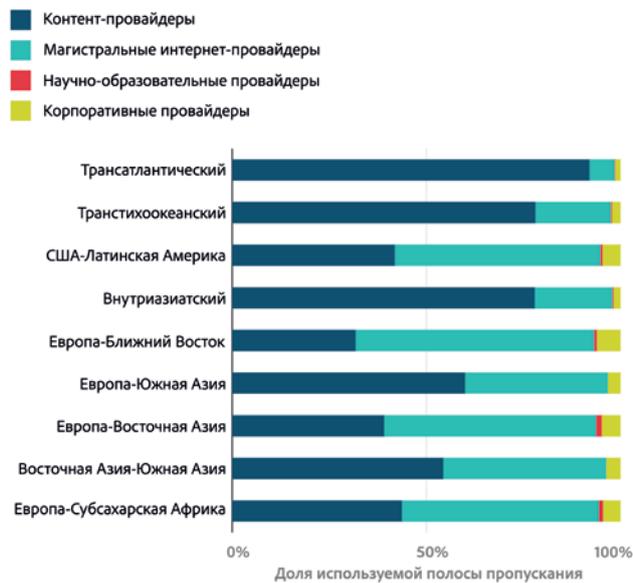
Темп роста мирового годового спроса на увеличение пропускной способности международных каналов замедлился, однако, согласно последним данным TeleGeography, сам совокупный спрос за период с 2019 по 2023 годы увеличился втрое и достиг рекордных 5 Петабит/с.



Source: © 2024 TeleGeography  
 Источник: <https://blog.telegeography.com/used-international-bandwidth-reaches-new-heights>

## Доля используемой полосы пропускания на основных маршрутах

По состоянию на 2023 год более 70% полосы пропускания приходилось на контент-провайдинг. На некоторых крупнейших маршрутах контент-провайдеры обеспечивают подавляющее большинство спроса, тогда как другие маршруты остаются более ориентированными на магистральные интернет-провайдеров.

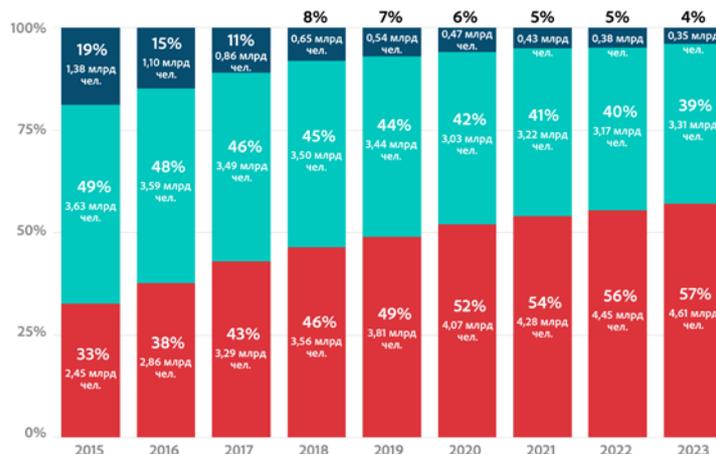


Source: © 2024 TeleGeography  
 Источник: <https://blog.telegeography.com/used-international-bandwidth-reaches-new-heights>

### Глобальное подключение к мобильному Интернету

В конце 2023 года примерно 57% населения земного шара пользовались на своих устройствах мобильным Интернетом. Более 90% прироста его потребления в 2023 году пришлось на страны с низким и средним уровнем дохода, где проживает 95% населения, не имеющего доступа к Интернету. Из 3,45 миллиарда человек, которые по-прежнему не подключены к мобильному Интернету, 90% живут в районах, которые уже охвачены мобильной широкополосной связью, но не пользуются мобильным Интернетом. Тем не менее, в настоящее время разрыв в использовании мобильного Интернета в девять раз превышает разрыв в покрытии.

- Абоненты мобильного Интернета
- Разрыв в использовании
- Разрыв в покрытии

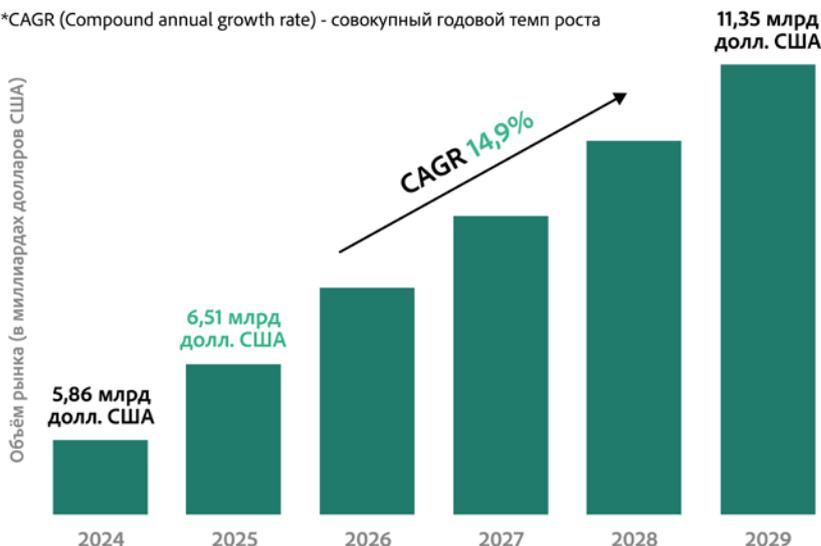


Источник: <https://www.gsma.com/r/wp-content/uploads/2024/10/The-State-of-Mobile-Internet-Connectivity-Report-2024.pdf>

### Прогноз роста мирового рынка спутникового Интернета

Ожидается, что в ближайшие несколько лет объем рынка спутникового Интернета будет стремительно расти. Основные тренды включают расширение группировки спутников на низкой околоземной орбите (LEO), интеграцию с сетями 5G, внедрение передовых спутниковых технологий в решения для интернета вещей (IoT) и беспилотного транспорта, появление доступных пользовательских терминалов, правительственные инициативы и субсидии в области космической связи.

\*CAGR (Compound annual growth rate) - совокупный годовой темп роста

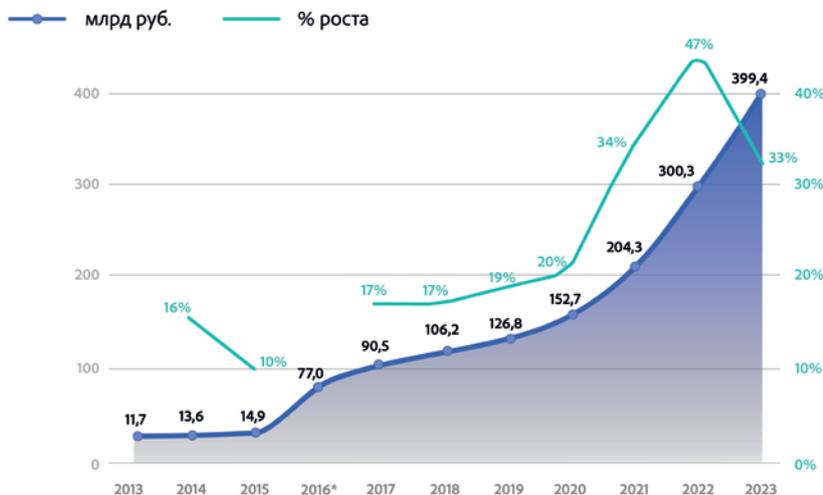


Источник: <https://www.thebusinessresearchcompany.com/report/satellite-internet-global-market-report>

# Интернет в цифрах

## Динамика развития инфраструктурного рынка Рунета

Наибольшая доля рынка приходится на облачную инфраструктуру (включая IaaS, PaaS, DBaaS, облачный хостинг, а также ЦОД). Её объём в 2023 году оценивается РАЭК в 349,5 млрд рублей. Наибольший спрос отмечается в отношении IaaS-решений. Рост стимулируется нехваткой собственных вычислительных мощностей и санкционными ограничениями. Растёт востребованность услуг PaaS (платформа как сервис) и сервисов со встроенными инструментами искусственного интеллекта без необходимости создания собственной инфраструктуры.



\*в 2016 году в объём инфраструктурного сегмента был включён рынок облачной инфраструктуры

РАЭК Экономика Рунета

Источник: <https://raec.ru/live/raec-news/14444/>

## Динамика развития рынка цифрового контента Рунета

Рост объёма рынка относительно 2022 года составил 99%. Он обусловлен изменением как самой структуры, так и методологии оценки. Наибольшая доля рынка приходится на стриминговые сервисы, и её объём оценён РАЭК в 98 млрд рублей. Существенную долю в 2023 году также заняли онлайн-игры с объёмом в 75 млрд руб. Оставшуюся часть рынка поделили цифровые книги и «пиратский» контент, доля которого неуклонно снижается. Одним из существенных факторов роста рынка цифрового контента стала государственная поддержка.

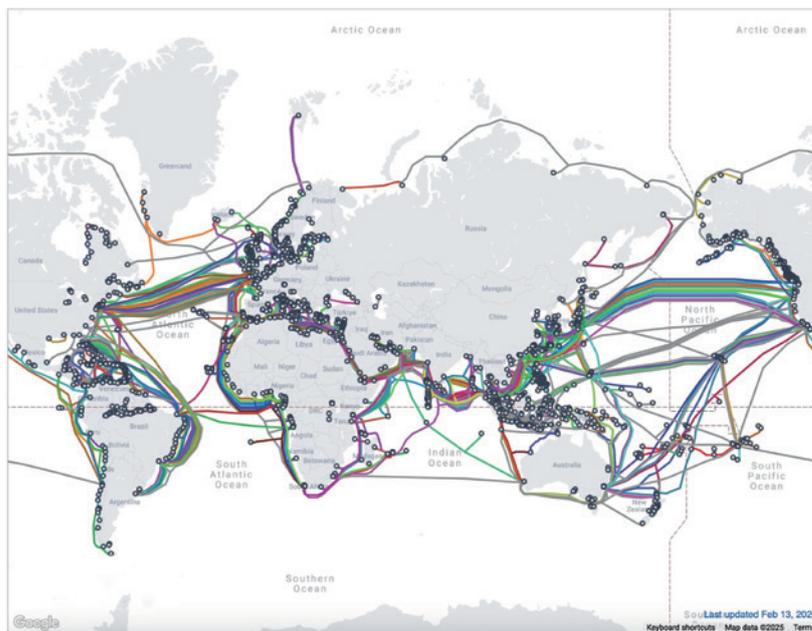


РАЭК Экономика Рунета

Источник: <https://raec.ru/live/raec-news/14444/>

## Мир подводных кабелей

По экспертным оценкам в мире насчитывается порядка 550 подводных кабелей общей протяжённостью около 1,4 миллиона километров. На них приходится 95% объёма всего международного сетевого трафика.



Источник: <https://www.submarinecablemap.com>

## Мировая распространённость точек интернет-обмена (IXP)

Общепризнано, что в мире по разным оценкам существует от 300 до 1000 IXP, с учётом неактивных и планируемых. Согласно данным TeleGeography, отображённым на карте, всего насчитывается более 300 активных IXP.



Source: © 2025 TeleGeography

Источник: <https://www.internetexchangemap.com>

# Управление интернет-связностью

Алексей Кипчатов

Илья Гуденко



## Аннотация

Интернет-связность — способность клиентских устройств подключаться к Интернету и обмениваться данными с интересующими сервисами и серверами. Качество связности определяется доступностью (стабильностью) соединения, его скоростью, задержкой и джиттером. Качество связности оператора пропорционально количеству непосредственно подключённых к его сети интернет-игроков из спектра интересов его клиентов. Интересы интернет-пользователей — социальное понятие, это распределение клиентских предпочтений по источникам контента или сервисам. В разрезе межоператорских отношений ключевым ориентиром для установления пиринговой связности является распределение интересов пользователей по трафику.

Экономика операторского бизнеса, как правило, подразумевает максимизацию доходов на стороне клиентов с минимизацией расходов на связность на стороне апстрим и пиринговых подключений. В настоящей статье анализируются принципы и методы оптимизации связности на примере магистральных операторов национального уровня на базе российских интересов пользователя и их эволюции последнего времени.

## Ключевые слова:

интернет-связность, интересы пользователей по трафику, автономная система, пиринг.

## Введение

Интернет-связность (англ. internet connectivity) — многогранное понятие, часто используемое в оценочном смысле как один из критериев качества оператора. В целом, чем больше у оператора IP-сети или Internet Service Provider (ISP) связей с другими операторами и владельцами контент-ресурсов и сетевых сервисов, тем выше ценность его связности.

Межоператорские связи плодотворнее всего описывать на языке BGP-взаимодействия автономных систем.

**BGP — Border Gateway Protocol** — это протокол маршрутизации, формализующий обмен информацией между сетевыми устройствами разных операторов о доступности через них сетей с другими автономными системами. BGP на настоящий момент является ключевым протоколом для глобальной маршрутизации в сети Интернет (RFC 4271).

**Автономная система — (Autonomous System, AS)** — это группа нескольких связанных IP-сетей, управляемая одним или несколькими сетевыми операторами, которая имеет единую и чётко определённую политику маршрутизации. Автономная система идентифицируется уникальным номером (ASN — Autonomous System Number) (RFC 1930).

Оценка связности оператора с каким-то конкретным сервисом или источником контента является простой технической задачей, так как число базовых измеряемых характеристик конечно: это доступность, задержка, джиттер.

**Доступность услуги (Service Availability)** — это метрика, отражающая долю времени, в течение которого услуга (например, интернет-соединение, облачный сервис, VoIP) функционирует в штатном режиме и доступна для пользователей. Это ключевой параметр качества обслуживания (QoS) и соглашений об уровне услуг - SLA (ITU-T Y.1540).

**Джиттер (jitter)** в характеристиках интернет-соединений — это нестабильность задержки (вариация времени задержки) между пакетами данных при их передаче по сети (RFC 3550).

Соответственно, операторы в конкретной локации по качеству связности с одним конкретным источником контента могут быть сравнены на основании измеримых характеристик. С точки зрения BGP важной измеряемой характеристикой является число транзитных AS (AS Path). Тот оператор, у которого меньше на маршруте чужих AS, предоставит более стабильные услуги, так как в зоне его ответственности лежит большая часть маршрутизации. Тот оператор, у которого меньше джиттер и реже случаются потери пакетов, имеет достаточный запас полосы до нужного ресурса. Тот, у которого меньше задержка, включён физически более коротки-

ми маршрутами (протяжённость каналов связи). Для оценки связности оператора с ресурсом остаётся выбрать, что важнее конечному потребителю, вернее, за что тот готов платить больше. Улучшение этого параметра без существенных расходов даёт оператору конкурентные преимущества в борьбе за клиентов.

Пользователи взаимодействуют не с одним конкретным ресурсом, а с различными типами контента и сервисов: видео, новости, развлечения, образование, интернет-торговля, работа, хобби и т.п., - размещёнными на различных площадках и представленных разными приложениями, сайтами, порталами, платформами, сетевыми технологиями. Поэтому критерии качества связности раскладываются по спектру клиентских интересов и набору измеряемых характеристик. Для совокупности клиентов число измеряемых величин и их сочетаний становится бесконечно большим, и простая задача оценки качества связности оператора переходит в статистическую, в которой базовым понятием становится распределение интересов пользователя по потребляемому трафику.

## Интересы пользователей по трафику

Трафик в сети формируется конечными пользователями. Именно пользователи выбирают ресурсы, к которым они обращаются в соответствии со своими интересами. И ответы этих ресурсов формируют трафик в сторону пользователя и нагрузку на сети транзитных ISP.

**Интересы интернет-пользователей — это вкусовые предпочтения пользователей в потребляемом контенте или сервисах, которые определяют их поведение в сети.**

Интересы пользователей — многомерные массивы данных, несущие в себе отражение социальной динамики в части выявления паттернов поведения пользователей в сети и задействования ими сетевых ресурсов. Методы измерения интересов пользователей многообразны и направлены на осознание их закономерностей для различного применения, а именно:

- развития пользовательских интерфейсов приложений;
- улучшения механизмов продвижения рекламы;
- повышения эффективности производства и доставки контента;
- совершенствования пользовательских устройств;
- формирования требований к инфраструктуре и географии размещения серверов с данными по дата-центрам;
- оптимизации межсетевого взаимодействия в части выбора пиринговых партнёров и географического распределения межоператорских стыков.

Для различных целей можно различать интересы конечных пользователей по языковому пристрастию, по возрасту, по культурным и национальным чертам и т.п. Собирают данные по клиентам с целью их идентификации, классификации, анализировать и пытаться управлять их вниманием. И именно в таком смысле понимают интересы пользователей, как правило, производители контента и IT-сервисов [1, 2].

С точки зрения операторов, разумно не дифференцировать клиентские поведения, а интегрировать и выделять ключевые группы клиентов в целях оптимизации качества связности для них. В настоящее время профиль трафика в операторских сетях более чем на 90% определяется запросами конечных клиентов и их пристрастиями к тяжелым видео- и мультимедиа-ресурсам. Поэтому рассмотрение интересов конечных клиентов по трафику от наиболее популярных тяжёлых ресурсов можно полагать базовым при оптимизации связности.

Интересы пользователей по трафику, определяемые по достаточно большой клиентской выборке, не зависят от технических параметров сети. Они зависят от эволюционного состояния социума, уровня образования, цифрового уровня государственных институтов, проникновения сетей в быт, коммерцию, деловой оборот. То есть интернет-интересы пользователей — продукт прежде всего социального устройства, настроения в обществе, моды, и потому интересы клиентов являются внешними, и именно они задают трафик на сетях операторов.

Интересы пользователей достаточно стабильны и медленно меняются во времени. Они меняются по времени суток и дням недели, но сохраняются в среднем за период времени от недели и более на достаточной клиентской выборке.

Операторские расходы на техническое развитие и эксплуатацию своей сети, в основном, пропорциональны требуемой полосе пропускания сети по направлениям передачи трафика, а полоса, в свою очередь, определяется (i) числом конечных клиентских устройств, чей трафик идет по сети, (ii) профилем интересов пользователей по трафику и (iii) набором межсетевых стыков, необходимых для пропуска клиентского трафика из Интернета, то есть от других сетей.

Интернет — совокупность IP-сетей, каждое устройство в которых имеет свой уникальный IP-адрес, сообщает его маршрутизатору, с которым оно соединено, маршрутизаторы обмениваются между собой информацией об IP-адресах присоединённых устройств и на этих данных формируют таблицы маршрутизации, в соответствии с которыми они переправляют пакеты данных по сети. Маршрутизаторы, являясь устройствами, принадлежащими разным сетям, соединены друг с другом там, где получилось, и полоса соединения устанавливается такой, которой достаточно. В заголовке каждого IP-пакета есть обязательные поля с IP-адресами хоста отправителя пакета (Source Address) и IP-адресом получателя пакета (Destination Address). Маршрутизаторы читают адрес получателя и на каждом шаге маршрутизации по таблицам маршрутизации выбирают порт, за которым находится самый выгодный маршрут до адреса получателя в соответствии с известными маршрутизатору BGP-атрибутами. В то же самое время наличие адреса отправителя позволяет собрать, накопить и проанализировать все адреса отправителей пакетов, проходящих через сеть в каком-то из её срезов. Суммируя количество пакетов, идущих с пространства адресов автономных систем за некий временной интервал сбора данных, можно построить вершину распределения трафика по источникам. Наиболее часто встречающиеся автономные системы да-

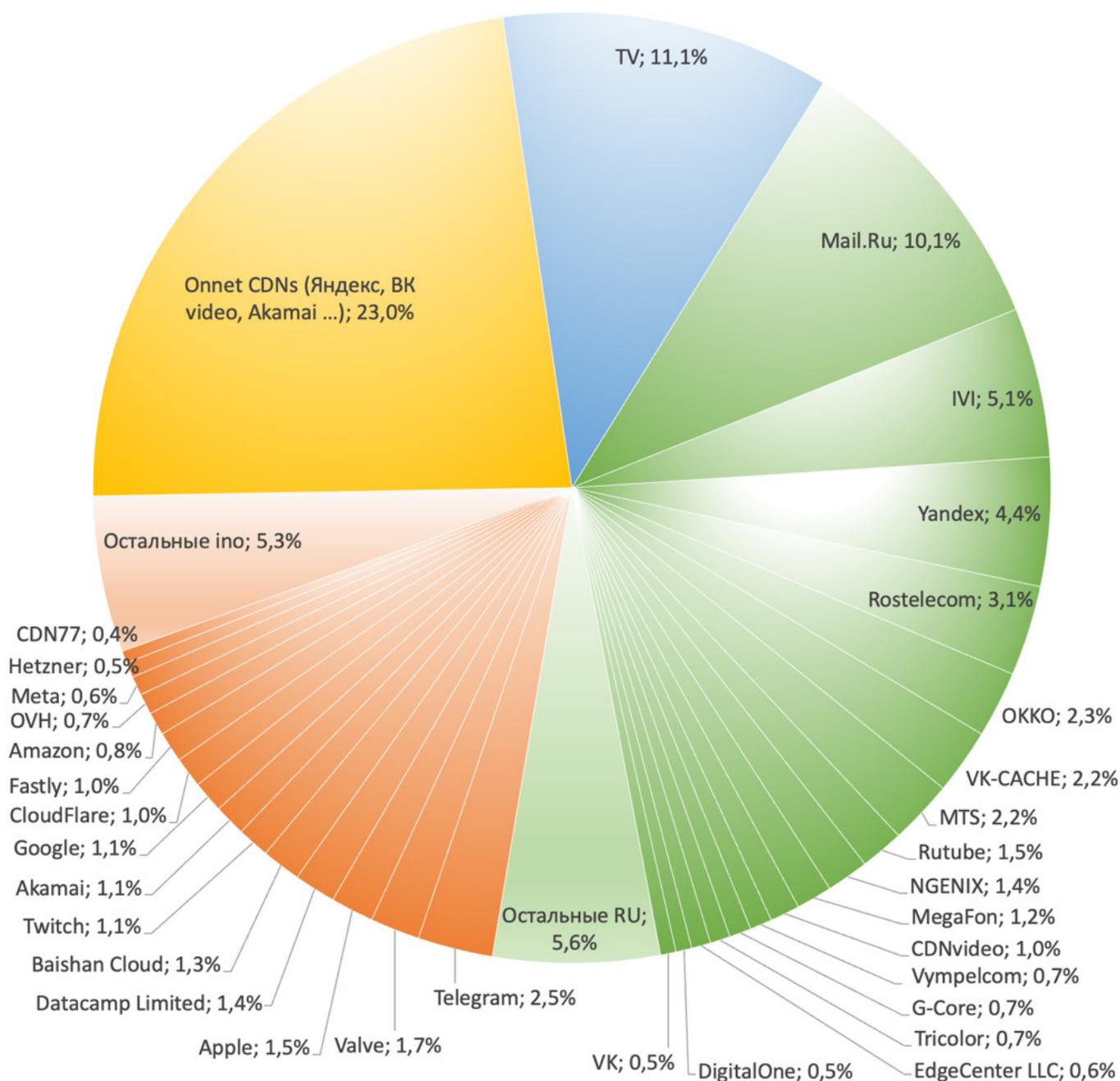


Рис. 1. Пример распределения потребляемого конечными клиентами трафика. Срез на февраль 2025 года.

дут картину популярного тяжёлого контента, затребованного клиентами, несущего основную нагрузку на сеть.

На рисунке 1 представлен пример распределения потребляемого клиентами трафика по автономным системам, в адресном пространстве которых размещены те или иные сервисы или тот или иной контент, запрашиваемый клиентами. Диаграмма построена по реальным данным за февраль 2025 года, полученным на контуре примерно 50 тысяч клиентов нескольких провайдеров широкополосного доступа. С целью сглаживания естественных суточных и недельных циклов в интересах пользователей данные усреднены на недельном интервале.

Исходящий к клиентам трафик состоит из локальной части трафика с CDN-серверов магистрального оператора (Akamai, «Яндекс», VK, ...), количество которого составляет 23% в спектре интересов, трафика потребления мест-

ным операторским IPTV-сервисом — 11%, остальные 2/3 трафика приходят с межоператорских стыков магистрального оператора.

«Дальнесетевого» трафика в клиентском потреблении 55%, и он исходит всего из 32 автономных систем, а остальные миллионы интернет-ресурсов всего мира находятся в длинном хвосте распределения и составляют менее 1/10 интересов пользователей по трафику. При этом трафик, приходящий к клиентам с источников с IP-адресами зарубежных отправителей, составлял на февраль 2025 года 22%. Таким образом, имея перед глазами картину интересов пользователя по трафику и вполне счётное количество важных AS-источников контента, утилизирующих сети и внимание клиентов, можно осмысленно оптимизировать межоператорские стыки по месту включения, по полосе, по типу подключения, по расходам.

Распределение интересов пользователей по долям потребления популярных ресурсов стабильно и сохраняется под внешними воздействиями. Темы контента в зависимости от повестки дня меняются быстро, а вот платформы концентрации тяжёлого контента, каналы общения и время, потраченное потребителями на них, меняются очень медленно. Это проявление закона подобия в самоорганизующихся системах – профиль потребления массы клиентов в среднем подобен сам себе и достаточно медленно эволюционирует во времени.

## Типы межоператорских связей

Клиенту не важно, каким путём трафик до него дошёл – через CDN, через апстрим (вышестоящего оператора) из-за рубежа, через пир (равнозначный обмен) на IX (Internet Exchange – точка обмена трафиком) или через прямой пир. Клиенту важно, чтоб трафик дошёл без потерь. Интернет – совокупность связанных напрямую или друг через друга IP-сетей, и путь доставки трафика – через каких операторов и какие типы стыков прошёл трафик – важен операторам, так как он определяет стоимость доставки.

**В номенклатуре типов межоператорских связей есть три вида взаимоотношений по их ролевому значению и по настройкам маршрутизации:**

- покупка связности;
- продажа связности;
- условно-бесплатный обмен связностью.

Покупающий оператор называется даунстрим-провайдером (downstream – вниз по потоку, нижестоящий в иерархии), продающий – апстрим-провайдером (upstream – вверх по потоку, вышестоящий в иерархии), обменивающиеся стороны называются пирами (peer, peering – ровня, равный в иерархии). Пиринг – вид взаимодействия со специфической маршрутизацией, когда взаимодействующие операторы обмениваются друг с другом только своими связностями вниз по потоку, то есть связностями со своими клиентами, их апстримы и прочие пиры в обмене не участвуют [3].

Граничные маршрутизаторы ISP определяют список BGP соседей, анонсирующих, что за ними есть IP-адреса, совпадающие с адресом назначения пакета. При прочих равных условиях в метриках BGP выбирается предпочитаемое направление отправки пакетов соседям: самым предпочитаемым направлением являются клиентские стыки, второе – пиринговые стыки, последнее – апстрим. Благодаря такому порядку предпочтений выстраивается вся пирамида интернет-провайдинга от маленьких местных операторов внизу до нескольких глобальных гигантов уровня Tier-1 – глобальные провайдеры первого уровня, находящиеся на вершине пирамиды интернет-связности, имеющие пиринговые связи только между собой и продающие связность всем остальным. В результате

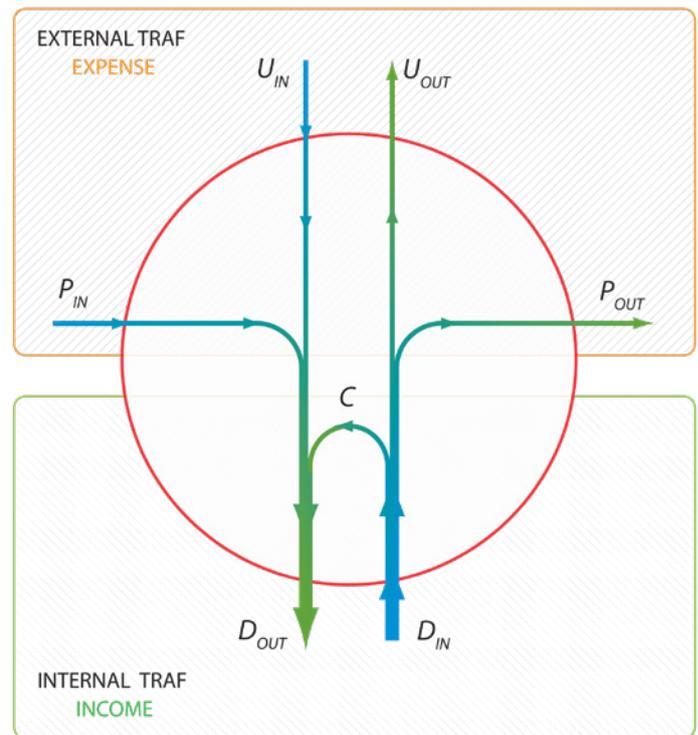


Рис. 2. Баланс трафика на сети ISP в соответствии с иерархией его взаимодействия с другими ISP: сверху находится совокупность апстрим-операторов U, внизу находятся клиенты D, на экваторе – пиринговые партнеры P. C – замкнутый сетью оператора межклиентский трафик.

стремления ISP к максимизации связности, ограниченного экономическими факторами, формируется вся мировая интернет-экосистема [4].

Интернет – это, прежде всего, адресация всех устройств и маршрутизация пакетов данных между ними. Все конечные пользователи, потребляющие трафик, и все серверы с данными и сервисами, порождающие трафик, являются даунстрим-подключениями к IP-сетям. IP-сети сами не рожают и не потребляют трафик, они лишь передают его между своими граничными стыками. В здоровой сети должен выполняться баланс трафика – весь входящий в сеть трафик должен быть равен всему исходящему из сети трафику:

$$\sum_i U_{in_i} + \sum_j P_{in_j} + \sum_k D_{in_k} = \sum_i U_{out_i} + \sum_j P_{out_j} + \sum_k D_{out_k}$$

где:

$U_{in_i}, U_{out_i}$  – входящий и исходящий трафик  $i$  штук апстрим-подключений;

$P_{in_j}, P_{out_j}$  – входящий и исходящий трафик  $j$  штук пиринговых подключений;

$D_{in_k}, D_{out_k}$  – входящий и исходящий трафик  $k$  штук даунстрим-подключений.

Графически направления трафика на границах сети представлены на рисунке 2. Часть сетевого трафика операторов является замкнутым межклиентским трафиком C, то

есть трафиком, исходящим с одних клиентов и входящим на других клиентов оператора.

Трафик, приносящий доходы оператору, это, как правило, исходящий на клиентов трафик:

$$\sum_k D_{out_k} = \sum_i U_{in_i} + \sum_j P_{in_j} + C$$

Трафик апстримов  $U_{in_i}$  – это операционные затраты операторов, пропорциональные количеству входящего с них трафика. Пиринговый трафик  $P_{in_j}$ , как правило, тоже требует расходов на оплату присутствия на точках обмена трафика IX – Internet Exchange – или на достижение и организацию прямых межоператорских стыков PNI – Private Network Interconnect. Лишь замкнутый межклиентский трафик  $C$  не несёт прямых расходов на его получение. Количество замкнутого трафика пропорционально размеру сети оператора и количеству его клиентов.

**Последнее соотношение делает очевидными возможные мероприятия по оптимизации расходов на связность для провайдеров любого уровня:**

- максимизация замкнутого между клиентами трафика  $C$  – для этого надо стремиться делать все включения клиентскими, так как клиенты несут и доходы, и связность;
- интернет-ресурсы, которые не удаётся сделать своими клиентами, предпочтительнее подключать на пиринговых настройках, причём популярные ресурсы из вершины распределения интересов пользователей выгоднее включать прямыми пиринговыми условно-бесплатными стыками PNI, а связность с большим числом интернет-игроков из середины распределения интересов пользователей целесообразнее получать скопом на точках обмена трафиком IX с оплатой за полосу присутствия на точке обмена;
- апстримы  $U$  должны обслуживать лишь хвост интересов пользователей по трафику с малопопулярных ресурсов, с которыми отсутствует возможность или экономическая целесообразность установления пиринговых отношений.

## География связности

На заре развития Интернета новые участники подключались к общей обменной сети (интернет-бэкбон, Backbone), которая была основой научных сетей и оплачивалась американским научным фондом NSF – National Science Foundation [5]. Затраты на подключение определялись построением цифровых каналов связи для достижения бэкбона. По мере роста трафика и коммерциализации Интернета финансирование обслуживания и развития интернет-бэкбона взяла на себя группа коммерческих операторов, которые друг с другом соединялись пиринговы-

ми стыками, а все остальные покупали связность с любым из них. Позже операторов бэкбона назвали Tier-1-операторами, и они стали «центром» Интернета, через который проходила вся интернет-связность. Соответственно, расходы провайдеров на подключение к Интернету складывались из оплаты канала связи до ближайшего интернет-узла и оплаты подключения к нему как к апстриму. Параллельно процессу разрастания сети Интернет росли так называемые кампусные IP-сети, внутри которых развивались локальные ресурсы. Последнему способствовала открытость интернет-технологий, энтузиазм пользователей и постоянный дефицит цифровых каналов связи до бэкбона на фоне растущего трафика и расходов на него. Между «кампусными сетями» и отдельно развивающимися веб-ресурсами раннего Интернета устанавливались пиринговые отношения, обогащая друг друга связностью с интернет-сосеями без петель через далёкий и дорогой «центр» Интернета. Некоторое время спустя «кампусные сети» стали прообразом коммерческих провайдеров местного доступа, а наиболее удачливые масштабировались до регионального уровня.

**Эта очень грубая картина структуры раннего Интернета даёт картинку понимания следующих деталей интернет-провайдинга:**

- **географическое разнесение типов межоператорских подключений** – на территории покрытия сети подключаются клиенты, связность покупается где-то на далёких узлах у Tier-1-операторов или у магистральных операторов, сети которых дотягиваются до «центра Интернета», а с провайдерами на соседних территориях поднимаются пиринговые стыки;
- **функциональная сущность бизнеса провайдера** – «фабрика» по производству связности в интересах клиентов;
- **целевая модель роста:**
  - вверх по иерархии – стать Tier-1-оператором, чтобы не нести расходы на покупку связности, а только продавать её вниз по иерархии и поддерживать «бесплатный» пиринг с другими Tier-1;
  - вниз по иерархии – покрыть всю территорию своими сетями доступа и сделать всех своими клиентами для максимизации доходов.

## Конкуренция как критерий разумности

Конкуренция провайдеров в борьбе за доходы от клиентов и минимизацию расходов на связность пронизывает все уровни провайдинга. С одной стороны, два соседствующих оператора являются добрыми пир-партнёрами ровно до того момента, пока их сети не пересекаются и они не начинают бороться за одних и тех же клиентов. Обострение конкуренции часто влечёт за собой местный

депиринг – каждый провайдер полагает, что ухудшение связности с ним его конкурента ухудшит связность этого конкурента. В результате локальный трафик уходит на более далёкие пиринговые площадки, на которых присутствуют эти конкуренты, или вообще разворачивается на апстримы конкурирующих операторов.

С другой стороны, для магистральных провайдеров на межоператорском рынке становится очень важным сокращать длину BGP-маршрутов – AS Path – между источниками трафика и потребителями. Ведь маршрутизаторы просчитывают возможные маршруты и выбирают наилучший с наименьшим числом скачков через автономные системы (AS hop). Выигрывает тот оператор, у которого наиболее прямая связность с интересным клиенту контентом, и поэтому для получения конкурентного преимущества приходится нести расходы на приближение своей сети ближе к контенту и организацию пиринга с далёким контентом на его территории.

Ещё одно яркое конкурентное проявление, влияющее на географию пиринга, происходит при продвижении глобальных Tier-1 по национальным территориям с достаточно высоким уровнем локализованного трафика, таких как Рунет. В Рунете меньше четверти трафика доставляется из-за рубежа, остальной контент рождается внутри страны. В такой ситуации западный Tier-1-оператор, пришедший на российский рынок, может предложить лишь западную связность. Поэтому для старта на рынке ему интересно максимально быстро набрать местную связность, и он, вопреки своим пиринговым принципам, готов пириться с местными ресурсами и даже покупать местный Интернет, что портит экономические показатели его продвижения на национальные рынки. Если какой-то из операторов Рунета решит купить IP-транзит на территории Российской Федерации у пришедшего сюда западного игрока, то он получит худший AS Path с как минимум одним лишним AS hop этого оператора по сравнению с тем, что он мог организовать себе сам путём бесплатных пиров, например, во Франкфурте.

Поэтому одним из важных моментов в межоператорской игре за своё место под солнцем является географическое разнесение зон, где оператор продаёт, где он покупает, где имеет рестриктивную пиринговую политику, а где открыт и гибок для пиринга. На территории своих коммерческих интересов, как правило, провайдер не пирится с другими операторами даже за деньги, даже если они Tier-1. Но так было давно, в эпоху, когда Интернетом правили веб-технологии. С тех пор связность в соответствии с распределением интересов пользователей сконцентрировалась на конечном числе больших контент- и сервис-игроков, таких как Google, «Яндекс», VK, Telegram, Rutube и т.п. Современным потребителям Интернета не нужна связность друг с другом напрямую. Они взаимодействуют на развлекательном и бизнес-уровнях через сервисы популярных глобальных платформ, которые развивают bigtech-игроки. Для хорошей современной связности надо заботиться о прямых подключениях лишь счётного числа критически важных популярных ресурсов, а при наличии поддерживать размещение их кеширующих серверов на своей сети, наращивая их эффективность максимизацией числа своих клиентов.

## Заключение – взгляд с другой стороны

С другой стороны (со стороны контента) есть свои аналогичные метрики связности и экономические ценности. Для контента важна короткая связность с аудиторией на территориях продвижения своих сервисов, и соответствующая экономика достижения этой связности – покупать ли её, получать через пиринг, размещать CDN-серверы ближе к своим пользователям или строить свои магистрали от дата-центров в сторону пользователей. У разных владельцев контент/сервис-платформ разные стратегические ценности, и потому нахождение паритета интересов между интернет-провайдерами (ISP) и контент-игроками – это бесконечная игра в поисках тонкого баланса экономики и интересов. Картина мира, изложенная в статье, в деталях отражает взгляд ISP. Надеемся, в обозримом будущем представители условного «Яндекса» или VK опубликуют аналогичное исследование, отражающее их взгляд на связность. ■

### Список литературы:

- [1] Rand FishkinMarch, Who Sends Traffic on the Web and How Much?, 11.2024 <https://sparktoro.com/blog/who-sends-traffic-on-the-web-and-how-much-new-research-from-datos-sparktoro/>
- [2] Omri Wallach, The World's Most Used Apps, by Downstream Traffic, 09.2021 <https://www.visualcapitalist.com/the-worlds-most-used-apps-by-downstream-traffic/>
- [3] А.А. Кипчатов, Физика пиринга и химия депиринга, 03.2008 <http://kipchatov.ru/blog/-p=202.htm>
- [4] William B. Norton, Internet Peering Playbook, Connecting to the Core of the Internet, DrPeering Press, 2011 – The Global Internet Peering Ecosystem, 354 p.
- [5] NSFNet, Википедия - <https://ru.wikipedia.org/wiki/NSFNet>

### Об авторах

А.А. Кипчатов, к.ф.-м.н., руководитель направления, компания «ТрансТелеКом», Москва

И.Д. Гуденко, руководитель департамента развития, компания «ТрансТелеКом», Москва



# Эволюция развития и «связанности» голосового трафика в России и мире

Юлия Цветкова  
Владимир Бойков



## Аннотация

В статье рассмотрены основные аспекты развития голосовых услуг в России, от аналоговых систем до современных способов передачи по IP-протоколам. Основные вызовы перед отраслью в связи с увеличением фродовых схем. Регуляторные аспекты деятельности операторов голосовых услуг, вызовы и пути развития.

## Введение

Голосовой трафик, несмотря на его долгую историю и развитие, продолжает оставаться важным элементом телекоммуникационных сетей. Однако изменения в технологиях, рыночных условиях и пользовательских предпочтениях кардинально трансформировали этот сегмент, поэтому крайне важно рассмотреть эволюцию голосового трафика и его текущее состояние. Также нужно отметить, что «связанность» голосового трафика совершенно не равна связанности в сети Интернет. И если для сетей передачи данных связанность — это в первую очередь наличие прямых стыков между всеми сетями и наполнение сетей трафиком контент-генераторов, то в голосовых сервисах такой необходимости нет, наличие прямых соединений обусловлено лишь экономическими интересами (чтобы сократить затраты на пропуск трафика) и никаким образом не влияет на качество услуг для конечных пользователей. Чтобы данный тезис обосновать, мы рассмотрим историческое развитие голосового трафика в мире и России, проанализируем современное состояние голосовых услуг, оценим влияние технологий борьбы с фродом и спамом, а также обозначим перспективы развития этого важнейшего сегмента телекоммуникаций.

## История развития голосового трафика

Голосовая связь как основа телекоммуникаций претерпела радикальные изменения за последние десятилетия. От аналоговых телефонных линий до облачных решений на базе искусственного интеллекта (ИИ) эволюция голосового трафика отражает не только технологический прогресс, но и трансформацию потребностей общества.

В прошлом голосовая связь базировалась на телефонных сетях общего пользования, где аналоговые сигналы передавались по медным проводам. В 1980-х годах начался переход к цифровым технологиям, таким как ISDN, что повысило качество и надёжность связи. Однако настоящим прорывом стало внедрение VoIP в конце 1990-х. Технология, преобразующая голос в цифровые пакеты, позволила передавать данные через Интернет, снизив затраты и упростив интеграцию с другими сервисами [1].

Итак, голосовая связь, с чего всё начиналось. А начиналось всё с аналоговых телефонных сетей, которые полагались на коммутируемые каналы.

Традиционные системы телефонной связи основывались на принципе коммутации каналов, где для каждого соединения выделялся отдельный физический или логический канал на всё время разговора. Эта модель обеспечивала стабильное качество связи, но была неэффективна с точки зрения использования ресурсов сети. Учитывая, что в этот период был активный рост рынка операторов фиксированной телефонной связи, присоединение каждого оператора к каждому для обеспечения дозвона абонентов всех сетей было невыгодно экономически, поскольку несло за собой огромные затраты, в том числе и на транспортную составляющую. Особенностью российского рынка стало выделение на сетях существенных операторов связи, которые владеют большим ресурсом фиксированной нумерации в регионе. Данные операторы регулировались законодательством вплоть до установки максимально возможных тарифов, не имели права отказать в присоединении к своей сети общего пользования. По факту это дало возможность фиксированным альтернативным операторам иметь только одно присоединение к существенному оператору, которое давало ему полную связанность с другими операторами сети [2].

История передачи голоса через интернет-протоколы началась задолго до массового распространения смартфонов и высокоскоростных мобильных сетей. Технология терминирования звонков, ставшая основой для современных решений VoIP, появилась еще в 1983 году, когда компания VBN впервые осуществила экспериментальный звонок между офисами с использованием кодеков ИКМ (импульсно-кодовая модуляция) и АДИКМ (адаптивная дифференциальная импульсно-кодовая модуляция), а также интернет-протоколов и специального оборудования. Этот успешный эксперимент положил начало развитию целой индустрии, которая коренным образом изменила подход к голосовой коммуникации [3].

С развитием цифровых технологий появились более совершенные протоколы, такие как ISDN (Integrated Services Digital Network) и SS7 (Signaling System No. 7), которые улучшили функциональность телефонных сетей, но сохранили принцип коммутации каналов. Эти протоколы до сих пор используются в некоторых сегментах телекоммуникационной инфраструктуры России, особенно в традиционных телефонных сетях общего пользования [2].

## Революция VoIP и современное состояние голосовых услуг

Революционным шагом в развитии голосовых коммуникаций стало появление протоколов, базирующихся на принципе коммутации пакетов. Центральное место среди них занял протокол инициирования сеансов (Session Initiation Protocol, SIP), разработка которого началась в 1996 году Хенингом Шульзри (Henning Schulzrinne) из Колумбийского университета и Марком Хэндли (Mark Handley) из Университетского колледжа Лондона. В ноябре 2000 года SIP был утверждён в качестве протокола сигнализации проекта 3GPP и основного протокола архитектуры IMS [1].

Протокол SIP стал одним из ключевых протоколов для передачи голоса через Интернет наряду с более старым стандартом H.323. В основу SIP разработчики заложили принципы простоты (протокол включает всего шесть методов или функций) и независимости от транспортного уровня. Простота реализации и гибкость SIP способствовали его широкому распространению [1].

В России переход на SIP в сетях фиксированной связи начался в середине 2000-х годов и значительно ускорился в 2010-х. Этот переход был обусловлен не только технологическими преимуществами SIP, но и экономическими факторами. Он позволяет существенно сократить капитальные и операционные затраты на телекоммуникационную инфраструктуру, обеспечивая при этом более широкий спектр возможностей для конечных пользователей [1].

Все указанные новые протоколы позволили развиваться современным технологиям передачи голосового трафика в телефонных сетях. Голосовая связь по IP-протоколу (VoIP) представляет собой технологию, позволяющую осуществлять голосовые вызовы через Интернет, а не посредством традиционных телефонных линий. В основе этой технологии лежит процесс конвертации аналоговых голосовых сигналов в цифровые данные и их последующая передача по IP-сетям. Такой подход обеспечивает значительную гибкость в использовании и управлении голосовым трафиком, открывая новые возможности для оптимизации телекоммуникационных процессов. И фактически более десяти лет данная технология активно развивалась для фиксированных телефонных сетей России. Однако конвертация голосового трафика в каналы передачи данных создала и угрозы, в первую очередь, возможность фродовых схем, поскольку появилась воз-

возможность подмены номера абонента. И с этой угрозой пришлось считаться и решать её совместно с регулятором. В 2023 году в закон «О связи» были внесены изменения, которые обязали всех операторов голосовых услуг подключиться к единой платформе верификации телефонных вызовов (ЕПВВ) «Антифрод» Главного радиочастотного центра (ГРЧЦ). Основной целью данного проекта является недопущение мошенничества с использованием подмены телефонного номера и защита населения от фродовых атак. Т.е. по состоянию на начало 2025 года каждый вызов на территории страны проходит верификацию на платформе ЕПВВ, что фактически исключает подмену номера абонента. На примере «Билайна» видим, что только в первые месяцы работы платформы были заблокированы миллионы вызовов с подменным номером.

С появлением мобильной связи (2G, 3G) голосовой трафик стал мобильным. Однако даже с развитием 4G сохранялось разделение между голосовыми вызовами и данными. Это изменилось с внедрением VoLTE, где голос передается через IP-сети, обеспечивая более высокое качество и скорость установления соединения.

С 2015 года объёмы международного голосового трафика через традиционные сети операторов связи начали снижаться. Это связано с ростом популярности OTT-приложений (Over-the-Top), таких как WhatsApp, Viber и Telegram. Эти приложения предоставляют бесплатные или дешёвые альтернативы традиционной телефонии, используя Интернет для передачи данных.

Голосовой трафик продолжает эволюционировать, адаптируясь к вызовам цифровой эпохи. Технологии вроде AI и 5G не только улучшают качество связи, но и требуют новых подходов к безопасности. Будущее голосовой коммуникации лежит в интеграции с иммерсивными технологиями и устойчивыми к атакам инфраструктурами. Однако успех этих инноваций зависит от сотрудничества регуляторов, операторов и разработчиков.

Важным аспектом современного голосового трафика является его масштабируемость. Голосовые системы быстро адаптируются к обслуживанию растущего числа пользователей без значительных изменений в инфраструктуре, так как не требуют установки дорогого оборудования и прокладки кабелей. Однако развитие технологий голосового трафика сопровождается и определёнными вызовами.

## Борьба с мошенничеством и спамом

Проблема фрода и спама в голосовом трафике становится всё более актуальной по мере развития технологий передачи голоса через Интернет. Злоумышленники используют различные схемы мошенничества, эксплуатируя уязвимости телекоммуникационных систем и доверчивость пользователей. В ответ на эти угрозы разрабатываются и

внедряются различные методы противодействия фроду и спаму, направленные на защиту как конечных пользователей, так и операторов связи. Как уже было сказано выше, одним из эффективных способов борьбы с фродом стала верификация всех вызовов посредством платформы ЕПВВ. Эта система является частью комплексного подхода к обеспечению безопасности голосовых коммуникаций, включающего как технологические, так и регуляторные компоненты.

Также одним из способов борьбы с фрод-мошенничеством стал анализ записей о вызовах. Операторы внедряют системы, которые выявляют наиболее подозрительные модели звонков и алгоритмически определяют вероятность фрода. Эти системы используют методы машинного обучения и анализа больших данных для выявления аномальных паттернов в голосовом трафике, что позволяет оперативно реагировать на потенциальные угрозы и предотвращать мошеннические действия.

Современные технологии борьбы с фродом и спамом включают также идентификацию голоса, блокировку подозрительных номеров и маршрутов, а также применение специальных протоколов аутентификации для верификации звонящего. Эти меры не только повышают безопасность пользователей, но и укрепляют доверие к операторам связи [4].

Современная российская телекоммуникационная инфраструктура переживает фундаментальную трансформацию, затрагивающую все аспекты передачи голосового трафика. Технологические инновации последних десятилетий кардинально изменили способы взаимодействия между пользователями и бизнесом, обеспечивая новые возможности и повышая эффективность коммуникаций. Одновременно с этим растущие проблемы безопасности и мошенничества вынуждают государство внедрять новые регуляторные механизмы, направленные на защиту потребителей и обеспечение прозрачности телекоммуникационного рынка. Предстоящие изменения в законодательстве 2025-2026 годов знаменуют новый этап развития IP-телефонии в России, который потребует адаптации как со стороны операторов связи, так и конечных пользователей.

26 декабря 2024 года правительством РФ было подписано постановление № 1898, которое создаёт регуляторные механизмы, препятствующие использованию VoIP-схемы в мошеннических целях и обеспечивающие дополнительный контроль за рынком. Ожидаемые изменения в законодательстве в 2025-2026 годах направлены на дальнейшее регулирование и стандартизацию VoIP-сервисов, что может привести к значительным изменениям на рынке телекоммуникаций. Операторам и пользователям придётся адаптироваться к новым требованиям, но в долгосрочной перспективе эти изменения должны способствовать повышению качества и безопасности услуг связи в России.

Одним из ключевых вызовов будущего развития голосовых коммуникаций в России будет поиск баланса между необходимостью регулирования для обеспечения безопасности и потребностью в пространстве для технологи-

ческих инноваций. Слишком жёсткие регуляторные рамки могут замедлить развитие отрасли, в то время как недостаточное регулирование создаёт риски безопасности и конфиденциальности пользователей.

Новые законодательные изменения, вступающие в силу в 2025 году, представляют собой попытку найти такой баланс, фокусируясь на противодействии мошенничеству, но сохраняя возможности для развития легитимных сервисов IP-телефонии. Успех этого подхода будет зависеть от того, насколько эффективно регуляторы и участники рынка смогут взаимодействовать для решения возникающих проблем и адаптации к изменяющимся технологическим условиям.

Несмотря на предстоящие регуляторные изменения, перспективы развития рынка голосовых коммуникаций в России остаются позитивными. Прогнозируемый рост рынка разговорного ИИ до 561 миллиона долларов к 2025 году свидетельствует о сохраняющемся высоком потенциале этого сегмента.

## Заключение – перспективы развития голосового трафика

**Будущее голосовых коммуникаций в России будет определяться несколькими ключевыми технологическими трендами:**

- дальнейшее развитие искусственного интеллекта и его интеграция в системы голосового взаимодействия. Современные решения уже достигли высокого уровня человекоподобности, и эта тенденция будет усиливаться, делая автоматизированные системы ещё более естественными и эффективными;
- расширение возможностей унифицированных коммуникаций, объединяющих голосовую связь с видеоконференциями, обменом сообщениями и другими формами цифрового взаимодействия в единой экосистеме;
- повышение безопасности и приватности голосовых коммуникаций с использованием передовых технологий шифрования и аутентификации;
- развитие голосовых технологий в контексте Интернета вещей (IoT), позволяющих управлять различными устройствами и системами с помощью голосовых команд.

Эволюция голосовых коммуникаций в России прошла долгий путь от традиционных аналоговых телефонных сетей до современных IP-решений, основанных на протоколе SIP и других передовых технологиях. Этот переход обеспечил значительное расширение функциональных возможностей, повышение эффективности и снижение стоимости связи для бизнеса и частных пользователей.

Предстоящие в 2025-2026 годах законодательные изменения направлены на создание более безопасной и прозрачной экосистемы IP-телефонии, минимизацию возможностей для мошенничества и недобросовестного использования технологий. При этом для большинства пользователей и добросовестных операторов связи эти изменения не должны привести к существенным ограничениям или неудобствам.

Будущее голосовых коммуникаций в России будет характеризоваться дальнейшей интеграцией искусственного интеллекта, развитием унифицированных коммуникационных платформ и повышением безопасности. Ключевым фактором успешного развития отрасли станет способность находить баланс между инновациями и регулированием, обеспечивая как технологический прогресс, так и защиту интересов пользователей. ■

### Список литературы:

- [1] Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. «Сети связи». Санкт-Петербург: БХВ-Петербург, 2022.
- [2] Самуйлов К. Е., Чукарин А. В. «Сети и системы передачи информации: телекоммуникационные сети». Москва: Юрайт, 2023.
- [3] Компьютерные сети и телекоммуникации / Под ред. В.К. Попова. Москва: ИНФРА-М, 2024.
- [4] Миронов Л.В. «Нормативно-правовое регулирование телекоммуникационной отрасли в Российской Федерации». Санкт-Петербург: Юридический центр, 2023.

### Об авторах

Цветкова Юлия Валерьевна, к.т.н., ПАО «Вымпелком», Москва

Бойков Владимир Викторович, к.т.н., ПАО «Вымпелком», Москва

# Особенности практического применения архитектуры Spine&Leaf в реалиях современного высоконагруженного CDN

Арсений Великород

## Аннотация

В статье рассматриваются вопросы оптимизации использования архитектуры Spine&Leaf на высоконагруженной сети оператора сети доставки контента. Производится анализ проблемы оптимального использования портовой ёмкости в рамках архитектуры Spine&Leaf

## Ключевые слова:

дата-центр, центр обработки данных, CDN, high-load, spine&leaf, datacenters.



## Проблематика

Целью данной статьи является попытка практической рационализации архитектурной модели S&L (Spine&Leaf), которая сегодня широко применяется при построении сетевой инфраструктуры в дата-центрах. Первым принципиальным отличием её от классической трёхуровневой модели является то, что S&L — двухуровневая. В ней spine совмещает функции агрегации и ядра (поэтому spine является ещё и маршрутизатором), в него включаются leaf-узлы. По своему функционалу это L2+ коммутаторы. Именно к ним подключается конечное оборудование (серверы) в дата-центрах. Основным фокусом статьи являются проблемы практического применения данного типа архитектуры на высоконагруженных сервисах, в частности, на инфраструктуре оператора сети доставки контента (Content Delivery Network, CDN).

Выбор столь узкой проблематики продиктован, с одной стороны, опытом проектирования, строительства и эксплуатации автором статьи реальной сетевой инфраструктуры оператора сети доставки контента, с другой стороны — возникшими фундаментальными вопросами к реализации теоретической модели в реальном дата-центре и на реальном оборудовании.

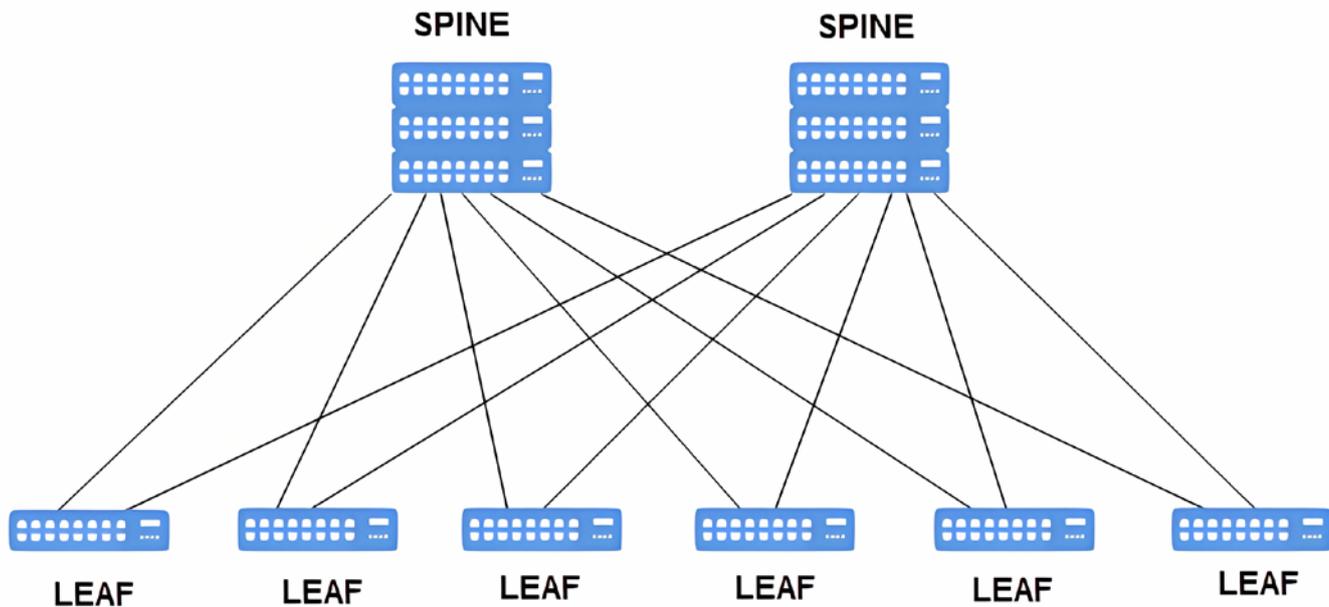


Рис. 1. Взаимодействие между leaf- и spine-узлами.

В частности, основная проблема, с которой приходится сталкиваться, — это проблема портовой ёмкости. В чистом S&L все spine соединяются со всеми leaf так, как показано на рисунке 1. Но в своей практике мы редуцировали эту схему за счёт размещения нескольких локаций<sup>1</sup> в одном дата-центре. Ведь каждый spine-коммутатор должен быть связан со всеми leaf-коммутаторами каналами достаточной ёмкости, но если на сети приходится иметь дело с тяжелым трафиком (VOD (Video On Demand), онлайн-трансляции), то каждый из узлов CDN может генерировать трафик, трёх- или четырёхкратный объём которого может полностью утилизировать полосу 100 Гбит/с. В этой ситуации существует вполне разумное решение — увеличить ширину канала между spine и таким leaf, куда включены подобные серверы сети. Но данное решение в условиях использования коммутаторов класса datacentre может серьёзно уменьшить количество портов, которые используются для включения соединений всех уровней (spine-spine, spine-leaf, leaf-leaf). Если же следовать экстенсивному пути развития этой архитектуры и наложить серьёзные структурные ограничения на возможности соединений типа leaf-leaf с попутным масштабированием структуры по размеру, при этом стараясь сохранить потребную для каждого типа трафика необходимую полосу, то можно очень быстро прийти к вопросам экономической целесообразности, а также, что более важно с точки зрения высокой доступности сервиса, возможности резервирования как самого сетевого оборудования, так и доступности внешних каналов.

## Условия применимости рассматриваемых моделей

Прежде всего оговоримся, что далее мы будем рассматривать работу сетевой инфраструктуры в рамках резервированной на программном уровне сети доставки контента. Здесь подразумевается такая программная модель CDN, когда падение одного физического сервера (ноды) не при-

водит к остановке сервиса, а приводит к переводу или перераспределению нагрузки между другими нодами кластера.

Также отдельно отметим, что рассматриваемая ситуация и модели применимы к дата-центрам, которые не относятся к топ-классу. Сегодня подавляющее большинство коммерческих дата-центров в России (Москва, Санкт-Петербург, Екатеринбург, Новосибирск, Иркутск, Хабаровск) предлагают чаще всего электрическую ёмкость 5 кВт (с резервированием двумя «лучами» или без. Данные сведения были собраны за период с января 2024 по сентябрь 2024 года). Так как основная задача CDN — это обеспечить раздачу контента из места, находящегося как можно ближе (в сетевом смысле) к конечному потребителю, что продиктовано соображениями минимизации задержки (RTT), то мы столкнёмся либо с ограничениями по предлагаемым в дата-центре условиям, либо с необходимостью применения модели, предусматривающей возможность самой гибкой адаптации к местным условиям. Поэтому мы исходим из условий, когда на стойку 48U выделяется средняя стандартная электрическая мощность 5 кВт. Тот факт, что на большой локации сети необходимо размещать большое количество нагруженных сетевым трафиком серверов с большими объёмами дисковых массивов, ставит серьёзные ограничения по энергетике для каждой стойки.

Вышесказанное, в свою очередь, влияет на форм-фактор выбираемого сетевого оборудования (в подавляющем случае — маршрутизирующих коммутаторов), его портовую ёмкость и энергетические эксплуатационные параметры. В частности, исходя из баланса технических условий и финансово-экономических показателей, первым выбором чаще всего являются коммутаторы серий, адаптированных под дата-центры форм-фактора 1-2U.

<sup>1</sup>Локацией мы называем инстанс дерева архитектуры S-L, объединённый одной политикой маршрутизации. У этого инстанса существуют свои каналы вовне, свой домен BGP-маршрутизации, своё адресное пространство. Технически это самостоятельная стойка (группа стоек с нодами, leaf-коммутаторами и spine-маршрутизаторами, к которым имеется доступ из публичной сети Интернет).

## Проблема портовой ёмкости как основная

Проблема распределения и оптимального использования портовой ёмкости на узле CDN с высокой нагрузкой — это основная проблема, с которой нам пришлось столкнуться в процессе проектирования новых и модернизации старых узлов (локаций). Структурно каждая локация представляет из себя от одной до трёх-четырёх стоек. Нами изначально была применена архитектура Spine&Leaf, но в силу естественных причин роста и развития наша реальная инфраструктура не была «чиста» в плане архитектурном — горизонтальные связи типа L-L (leaf-leaf), пиринговые присоединения на leaf'ax, «последовательная» группировка leaf'ов — всё это существовало и со временем, из-за значительного роста трафика, стало представлять проблему из-за возникновения многих точек на сети, склонных к перегрузкам на большом трафике.

Вышесказанное относится к подавляющему большинству сетевых инфраструктур, которые выросли из маленьких проектов. И это нормально, но самым главным этапом на пути этого роста является верный выбор архитектурной модели сети, которая должна не только учитывать конкретные особенности бизнеса и трафика, но и обеспечивать масштабируемость без больших капитальных затрат.

Сегодня сети доставки контента обслуживают практически весь спектр медиаданных, начиная от мелкой статики и заканчивая VOD и онлайн-трансляциями. Данная ситуация навязывает оператору сети в том числе и требования по классификации трафика (traffic affinity), что в свою очередь приводит и к раздельному обслуживанию трафика. Таким образом, мы приходим к тому, что разные типы трафика обслуживаются на разных серверах локации (см. объяснение термина в сноске выше). Каждая категория трафика обладает своим уникальным профилем — это касается как временных характеристик (волнообразность трафика или его равномерность в течение суток), так и качественно-количественных характеристик (проектируемая мощность сервера на отдачу трафика, соотношение входящего и исходящего трафика на порту сервера, его способность по распределению между каналами в Интернете и пирами локации, или же наоборот — его поляризация в какой-то из них).

В целом, если говорить о больших локациях, то на сети приходится иметь дело с широким спектром трафика, который, в идеальной ситуации, равномерно и пропорционально заполняет внешние каналы локации.

Однако, как было ранее отмечено, разные серверы раздают по-разному, и поэтому здесь возникает вопрос о планировании портовой ёмкости под все типы трафика, учитывая все неравномерности и колебания трафика, запроектированную пиковую нагрузку, а также требования к каналам по работе без перегрузки, как внешним, так и внутренним по отношению к локации.

В этой задаче мы рассмотрим несколько возможных моделей планирования портовой ёмкости с целью определить самые оптимальные, но стараясь не выйти за пределы архитектуры S&L, а также за условия, обозначенные ранее.

Также следует сделать важное замечание. В рамках внутренних соединений на локации мы считаем важным переход на порты с линейными скоростями 25/40/100 Гбит/с. Это продиктовано несколькими обстоятельствами: объёмом нагрузки на серверы (в особенности на те, которые обслуживают тяжёлые виды трафика (Live video или VOD)), пространённостью сегодня как сетевых карт на 25 Гбит/с, так и коммутаторов с комбинированными портами 10/25G, неэффективностью использования портовой ёмкости коммутатора при обслуживании скоростей раздачи более 30 Гбит/с (для таких соединений нужно включать серверы агрегатами из 10G портов, одновременно появляются издержки на расходные материалы, кроме того, такие агрегаты требуют большего внимания при эксплуатации и особенно тонкой настройки со стороны сервера).

Архитектура Spine&Leaf предоставляет широкие возможности по резервированию оборудования. На теоретическом уровне сегодня в дата-центрах мы видим разумным и более прогрессивным по сравнению с технологией стекирования (stack) [1] использование технологии MC-LAG [2] для резервирования каждого уровня (spine, leaf). Прежде всего, это связано с её большей гибкостью по сравнению со стекированием (априорное сохранение независимой конфигурации для каждого шасси). В рассматриваемых ниже ситуациях, если у нас есть MC-LAG-объединённые шасси для узла spine (S-S') и такие же для leaf (L-L'), то межуровневые соединения будут выполнены соответственно: S-L и S'-L'.

Однако мы намеренно редуцируем эти моменты в нашем последующем описании, т.к. на уровне архитектуры они ничего не меняют, а на практическом уровне нам не пришлось применять такое в силу определённой самостоятельности каждой локации и нашего изначального программного дизайна, который позволяет практически безболезненно вывести из работы любую локацию. Отдельные моменты особенностей применения технологий Stack и MC-LAG, а точнее, нашего не-выбора в их сторону в нашем частном случае будут оговорены далее

## Равномерное распределение

Прежде всего, мы рассмотрим такой способ использования портовой ёмкости на локации, когда все серверы включаются равномерно как в leaf'ы, так и частично в spine. И если для тех из них, которые оказываются подключёнными непосредственно к spine, не возникает каких-либо ограничений по скорости раздачи, кроме как по суммарной ёмкости аплинков, то для серверов, включённых в leaf'ы, возникает ограничение по пропускной способности канала S-L (spine-leaf). Эксплуатация последовательно соединённых leaf'ов в таком случае становится ещё более затруднительной в силу полного исчерпания портовой ёмкости под соединения между коммутаторами.

Поясним этот момент. В рассматриваемой модели мы стараемся включать серверы равномерно во все коммутаторы локации. В этом случае в каждом свитче должно оказаться примерно поровну серверов, которые обслуживают разные

Соединения между свитчами выполнены на линиях по 100Gbit/s  
 100G серверы включены агрегатами на 4 линка по 25Gbit/s  
 40G серверы включены агрегатами на 4 линка по 10Gbit/s

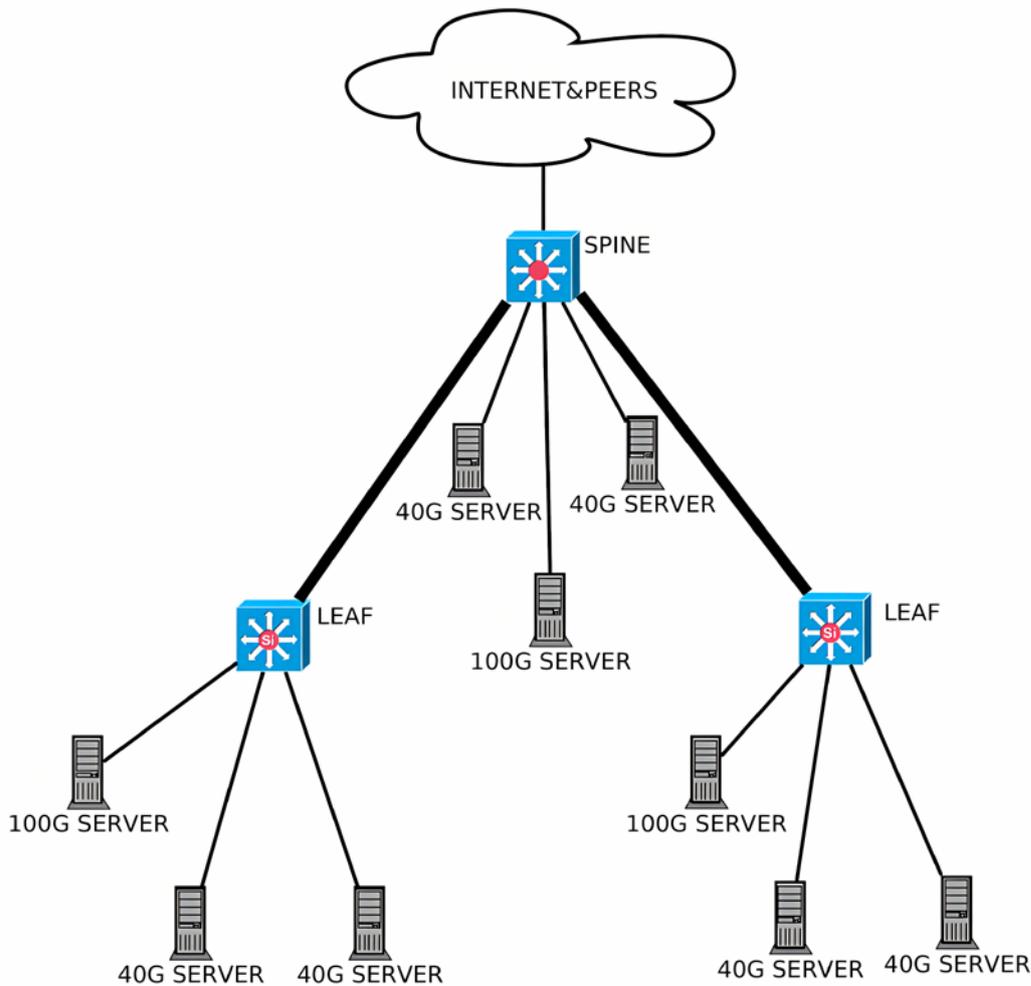


Рис. 2. Схема включения серверов при равномерном распределении.

типы трафика. Соответственно, объем суммарного трафика с каждого leaf планируется иметь примерно одинаковым по объёму. При включении только по одному leaf в порт spine проблем не возникает, так как не нужно планировать ёмкость для второго leaf'a. Однако, нарушив архитектуру и включив leaf в другой leaf, необходимо будет предусмотреть удвоенную ёмкость соединений как минимум между spine и первым leaf в этой ветке. Поэтому более разумно будет его включить отдельным портом. Здесь мы косвенно находим первое существенное ограничение этой модели — ограничение полосы между spine и leaf, которое, как мы увидим далее, является фундаментальным.

Но картина остаётся стабильной до тех пор, пока мы имеем дело с относительно умеренным трафиком с leaf и серверы, подключённые в него в час наибольшей нагрузки (ЧНН), отдают объём трафика не более чем 75% линейной скорости порта на коммутаторе (на самом деле, это очень мало, учитывая тот факт, что каждый сервер мы включаем как минимум двумя линками, чтобы, если даже один линк упал, то второй работал и сервер был доступен).

В этом случае максимальная эмпирическая нагрузка для 48-портового leaf-коммутатора с шестью 100-гигабитными портами будет выглядеть как:

$$(48 \times (10 \text{ Гбит/с} \times 0,75) \times 0,5) \times 0,55 = 99 \text{ Гбит/с.}$$

Коэффициент 0,55 был получен нами практическим путём как действующая величина поправки от неравномерности нагрузки. Применение коэффициента 0,5 связано с необходимостью включать сервер как минимум двумя портами в агрегате.

Как только мы захотим отдавать с сервера более чем 100% линейной скорости одного порта (обычного, не в сторону другого коммутатора) на leaf'e, мы очень быстро придём к существенным ограничениям по связи «наверх» — к spine. Прежде всего это связано с тем, что при использовании портов 25G необходимость раздавать с сервера 30–40 Гбит/с в ЧНН ведёт нас к быстрому исчерпанию 100 Gbit соединения со spine.

В этом случае максимальная эмпирическая нагрузка для такого же leaf-коммутатора будет выглядеть как:

$$(48 \times (10 \text{ Гбит/с} \times 1,3) \times 0,5) \times 0,55 = 171,6 \text{ Гбит/с.}$$

Конечно, такой трафик возможно пропустить только через два порта 100 Гбит/с.

В этом случае можно было бы, конечно, перейти на горизонтальное расширение — принципиально ограничиться одним «тяжёлым» сервером на leaf, а при необходимости добавления еще одного — организовывать еще один leaf и к нему присоединять этот сервер. Однако это приведёт к необходимости закупки в качестве spine коммутаторов с большим количеством 100G интерфейсов. В таком случае все leaf будут подключены к нему одним-двумя соединениями на 100G и проблема, казалось бы, исчерпана.

Тем не менее, проблема исчерпывается только на теоретическом уровне. Такие схемы могут быть эффективны только в развитых дата-центрах с большим количеством свободных стойко-мест и адекватным запасом по энергетике. Это касается в основном коммерческих дата-центров в Москве и Санкт-Петербурге. В регионах же, во-первых, мало где можно найти достаточно места под такие локация, а во-вторых, до сих пор существует проблема с наличием портов с линейной скоростью более 10G у операторов связи.

Отдельным ограничивающим условием становится тот факт, что не в каждом дата-центре присутствует достаточное с точки зрения CDN количество операторов. Конечно, существует практика «партнёрских локаций», которые размещаются у заинтересованных региональных операторов, объём трафика на которые достаточно высок (обычно это крупные региональные операторы), но такие локация редко разрастаются на более чем одну стойку 48U. Поэтому кроме «партнёрских локаций» важно иметь по одной крупной локация как минимум на ФО (федеральный округ). В этом случае все партнёрские локация, расположенные в том же ФО, будут снабжены не только качественным трафиком того типа, под который они планировались, но и всеми остальными. В таких крупных региональных локациях всё равно приходится проектировать достаточные ёмкости на раздачу трафика. Сегодня запросы на услуги CDN растут, на рынок приходят новые клиенты, и всё чаще это клиенты с тяжёлыми видами трафика. И здесь сеть доставки контента оказывается между потребностью обеспечить необходимую под все типы трафика ёмкость под раздачу в регионе и реальным наличием такой ёмкости у операторов — как портовой, так и суммарной в регионе. Именно последним продиктована рекомендация располагать локация там, где имеется максимальное количество операторов — и федеральных, и региональных, — чтобы не концентрировать весь трафик раздачи в одном операторе. У такого оператора, возможно, существуют ограничения по ширине стыков с другими операторами в этом регионе или, что хуже, их в регионе нет вообще, а они находятся в соседнем. Здесь не стоит забывать о первоочередной задаче CDN — на раздаче быть ближе всего к конечному потребителю.

Таким образом, в реальных условиях предложенная выше модель становится трудноосуществимой в условиях необходимости множественного размещения. Выбор дата-центра под локация зажат в узких рамках технических и экономических требований. Это и умеренная стоимость размещения, и отсутствие проблем по энергетике, наличие стойко-мест, наличие нескольких операторов, у которых должны быть технические возможности на включение

запрошенной ёмкости. В этих условиях, если наш spine в локация будет иметь только 100G порты, то для присоединения к оператору понадобится, как минимум, один коммутатор с портами 10/25G. Также не стоит забывать, что, скорее всего, в этот коммутатор будут включаться несколько других операторов, и его соединение со spine будет одной из точек отказа. Вопрос планирования портовой ёмкости под каналы в сеть Интернет и под точки обмена трафиком останется за пределами этой статьи, однако стоит сказать, что решение и этого вопроса на практике не всегда оказывается простым делом.

Подводя итог, можно сказать, что модель равномерного распределения серверов между коммутаторами в локация видится излишне утяжелённой, как по капитальным затратам, так и по спектру вопросов, которые нужно будет решить попутно, если такую модель выбрать при включении серверов, раздающих на скоростях, сопоставимых с 40 Гбит/с. При этом такая модель организации локация несёт в себе значительное количество ограничений и необходимость организации множественных точек контроля. Также её возможности по масштабируемости напрямую связаны с капитальными затратами и расширением списка используемого сетевого оборудования, к которому нужно иметь ЗИП (и/или возможность быстро купить и заменить вышедший из строя модуль или весь коммутатор целиком).

## Распределение с учётом максимальной нагрузки

Преодолеть проблемы предыдущей модели распределения нагрузки по портовой ёмкости мы можем, если при выборе места включения сервера будем принимать во внимание его планируемую способность к раздаче трафика. В частности, как ранее было указано, серверы, раздающие в ЧНН на скорости большей, чем линейная скорость одного порта (10 или 25 Гбит/с), являются основной причиной неоптимального использования портовой ёмкости. Однако, если такие серверы включать непосредственно в spine-коммутатор портами по 25 Гбит/с, а все остальные серверы, не создающие столь тяжёлый трафик, включать в leaf-коммутаторы, то можно достичь существенной оптимизации использования как портовой ёмкости, так и соединений между spine и его leaf'ами.

Это достигается тем, что самые загруженные серверы локация оказываются ближе всего к внешним каналам, и на этот трафик не требуется тратить ёмкость соединений между коммутаторами. А нагрузка от серверов, величина которой более адаптирована к линейной скорости портов, оказывается включенной в leaf'ы, соединения к которым хоть и выполнены чаще всего соединениями на линейной скорости 40 или 100 Гбит/с, но всё же обладают меньшей пропускной способностью, чем внутренняя шина коммутатора. В этом случае максимальная эмпирически рассчитанная нагрузка от leaf-коммутатора поддаётся расчёту по первой формуле из предыдущего раздела.

Соединения между свитчами выполнены на линках по 100Gbit/s  
 100G серверы включены агрегатами на 4 линка по 25Gbit/s  
 40G серверы включены агрегатами на 4 линка по 10Gbit/s

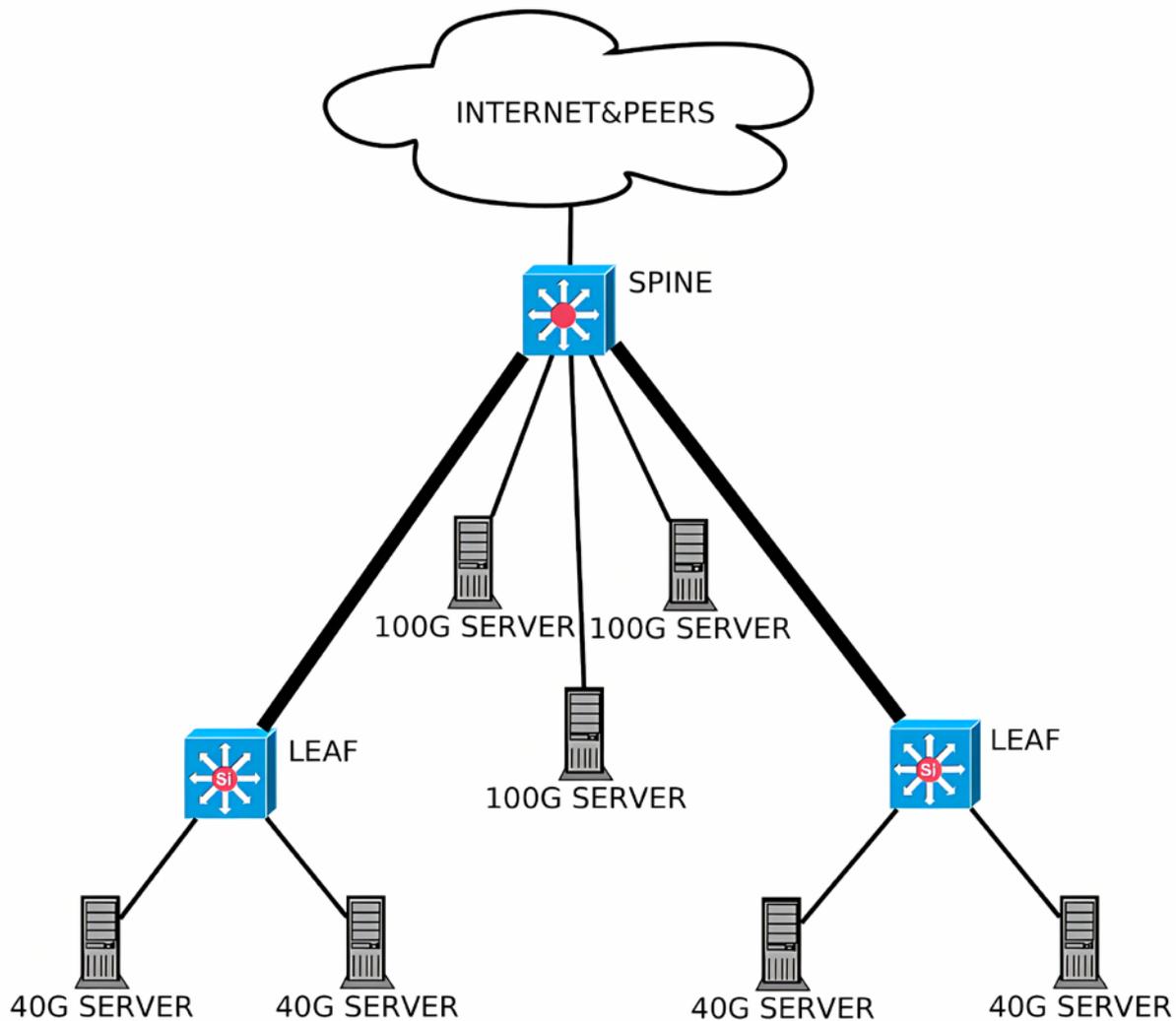


Рис. 3. Схема включения серверов с учетом нагрузки от них по трафику.

В целом, за счёт включения большой нагрузки как можно ближе к внешним каналам, можно добиться сбалансированности «дерева» по величине трафика. В особых случаях, если это позволяют объёмы трафика, допускается подключение к одному leaf-коммутатору другого leaf-коммутатора. Несмотря на некоторый отход от архитектуры, эта схема включения позволяет сэкономить порты по направлению «вниз» на spine-коммутаторе, к которым обычно подключаются leaf'ы. Таким образом, возможно выделять места включения сервисных систем, которые не обслуживают напрямую продуктивный трафик, но необходимы для функционирования внутренних систем (статистика, базы данных, хранение конфигурации и её резервирование, различные репозитории и пр.)

Можно, конечно, возразить, что ничто не мешаеткратно уменьшить объём отдачи с серверов, которые обрабатывают VOD и LIVE-трафик, а также другие его виды, которые требуют большой полосы на одну сессию, или же длительность сессии составляет более 5 секунд. Но здесь действуют соображения энергетической эффективности, которые не могут быть проигнорированы ни в каком дата-центре. Кратное уменьшение максимальной отдачи с сервера влечёт за собой необходимость кратного увеличения количества серверов,

а значит, многократного увеличения потребления электроэнергии.

В своей практике мы пришли к пониманию, что все серверы, включённые в spine, должны иметь линки 25G. Это оправданно экономически и не создаёт накладных расходов по переключению портов 25G в режим 10G, что на коммутаторах Huawei и Juniper возможно только группами портов (обычно по четыре порта в группе).

Также ощутимым преимуществом модели с учётом нагрузки от включаемых серверов является то, что мы не оказываемся перед необходимостью ставить высокопроизводительные leaf-коммутаторы с комбинацией портов на 25/100 Гбит/с. Вполне возможно обойтись и более старыми линейками с комбинацией линейных портов на 10/40 Гбит/с. Также существуют переходные линейки с комбинацией портов 10/100 Гбит/с.

Отдельно отметим, что схемы расширения портовой ёмкости за счёт технологий MC-LAG и уж тем более стекирования (Stack) перестали нами рассматриваться в процессе эксплуатации из-за необходимости соблюдения баланса трафика

между всеми физическими шасси, включёнными в стек или объединёнными через mc-lag, что на практике означало бы наличие линка в каждое физическое шасси из каждого физического сервера. Учитывая практику установки по одному коммутатору в стойку, все возможные удобства от таких технологий нивелируются необходимостью межстоечных соединений.

В целом, рассмотренная модель распределения нагрузки по локации позволяет добиться оптимального использования портовой ёмкости и мощностей сетевого оборудования. Самый тяжёлый трафик оказывается ближе к внешним каналам, серверы, обслуживающие его, включаются в spine-коммутатор, а лёгкий трафик приходит из leaf-коммутаторов. Кроме того, такая модель оказывается экономически эффективной, когда есть необходимость в активном наращивании ёмкости локации по раздаваемому трафику, но нет одномоментной возможности провести комплексную модернизацию сетевой инфраструктуры локации. В этом случае цикл ротации оборудования обеспечивает наибольший срок его эксплуатации.

## Гибридизация архитектуры Spine&Leaf

Тем не менее, существуют ситуации, где и учёт нагрузки не может покрыть требования к оптимальному использованию портовой ёмкости и внешних каналов.

Представим себе ситуацию, что в дата-центре А, где у нас уже стоит локация, закончилось место, и какой-то оператор предлагает разместиться у себя, а также предлагает трафик по хорошей цене.

В этой ситуации возможно рассмотреть вариант с организацией отдельной локации в ДЦ этого оператора. Однако в то же время не хочется и останавливать развитие существующей локации. В дата-центре Б, который, по сути, является дата-центром оператора, есть физическое размещение, но нет предположительно того спектра других операторов связи, который представлен в дата-центре А. Развитие отдельной локации в дата-центре Б может существенно нарушить баланс раздачи в том смысле, что раздача контента из новой локации будет вестись только через одного оператора. В случае проблем у оператора на сети, особенно если он предлагает нам канал в сеть Интернет полосой не менее 40 Гбит/с, мы можем существенно потерять в региональной ёмкости раздачи.

Если всё же мы решаемся развить существующую локацию в дата-центре А за счёт размещения в дата-центре Б и дополнительного включения там предлагаемого канала в Интернет, мы сталкиваемся с нестандартной задачей с точки зрения архитектуры.

Сделать коммутатор, установленный в дата-центре Б, просто leaf'ом того spine'a, который стоит в дата-центре А, видится самым простым решением. Но в таком случае мы

не сможем полноценно решить обе задачи: и эффективно использовать новый канал в сеть Интернет, и размещать в дата-центре Б серверы для раздачи. В противном случае придётся соединять дата-центры А и Б весьма широким каналом. Но даже при наличии такого канала, при его падении мы получим не только падение одного внешнего канала на локации, но и недоступность тех серверов, которые находятся в дата-центре Б.

Для того чтобы решить эту проблему, мы решили воспользоваться гибридизацией, где коммутатор в дата-центре Б становится маршрутизатором. В него включается доступ в Интернет от оператора в дата-центре Б, устанавливается BGP-сессия с этим оператором. Но кроме того, через канал между дата-центрами устанавливается BGP-сессия со spine-коммутатором в дата-центре А. Подробно осветить выбор в этой схеме между IBGP и EBGP, к сожалению, мы здесь не можем т.к. каждый раз это определяется местными условиями, предпочтениями, конфигурацией сети и возможностями сетевого оборудования. Но общий смысл сводится к тому, что в итоге обе стойки (в дата-центрах А и Б) начинают пользоваться внешними каналами друг друга, они обмениваются не только внутренними маршрутами к L3-интерфейсам в серверные сегменты, но и маршрутами вовне.

Как результат, мы получим схему, резервированную лучше, чем та, которую бы мы получили, если бы сделали leaf в стойке дата-центра Б и включили бы в него канал доступа в Интернет от оператора связи. В нашей схеме отсутствие связанности по соединению между дата-центрами не приведёт к остановке сервиса ни в одной стойке. Возможно, потребуется поправить балансировку нагрузки, но это не приведёт к полному отсутствию сервиса. Такое включение даёт более гибкие возможности по расширению существующей инфраструктуры оператора CDN за счёт использования новых площадок, географически разделённых с основным дата-центром.

## Заключение

В данной статье мы постарались изложить наш опыт и решённые проблемы реализации архитектуры Spine&Leaf на сетевой подсистеме высоконагруженного CDN. Наш опыт является скорее рационализаторством, чем инновацией. Описанный опыт — это попытка сократить издержки за счёт продуманного подхода к проектированию, развитию и эксплуатации, при этом не потеряв в надёжности сервиса.

В целом, из всего описанного можно сделать вывод, что вполне допустимо отходить от «чистой архитектуры» во имя результатов. Однако это не должно пониматься как полное пренебрежение принципами выбранной архитектурной модели и «изобретательство велосипеда». Наоборот, важен сбалансированный подход и долгосрочное планирование. В частности, это позволяет прийти к более гибким решениям, которые будет возможно развивать без особых проблем. Основные проблемы на сетевой ин-

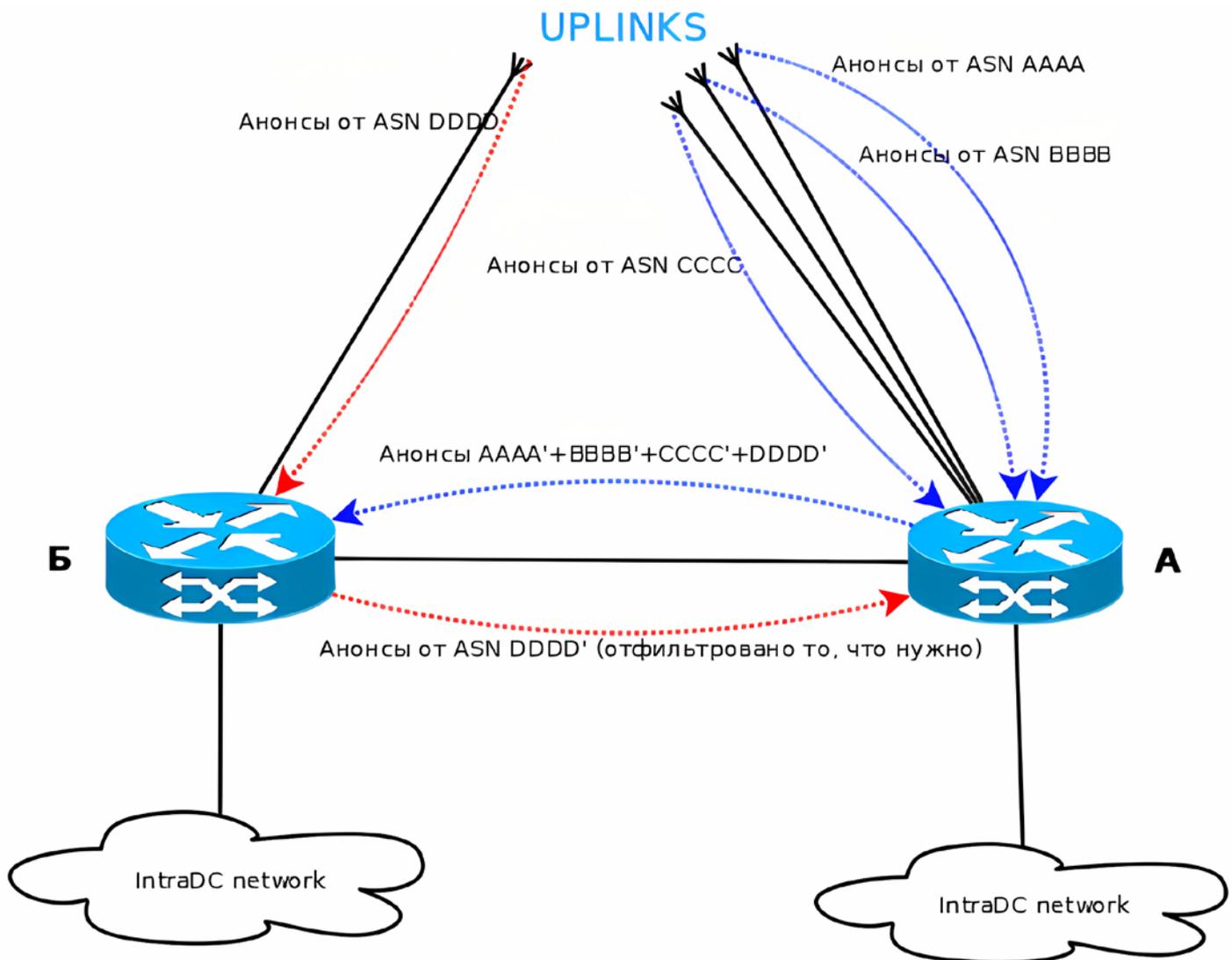


Рис. 4. Принципиальная схема гибридации (одна из возможных схем) с иллюстрацией возможного обмена маршрутной информацией внутри локации.

фраструктуре узла CDN возникают с приходом реально большой нагрузки. В этой статье мы предложили читателю некоторые практические приёмы, позволяющие лучше адаптировать сетевую инфраструктуру под всю гамму нагрузок в т.ч. в случае, если серверы раздают на больших скоростях в довольно узком коридоре технических требований, реальных условий и финансово-экономических показателей.

Мы постарались совместить и теорию, и практику. Но основным вопросом всё же остаётся метод решения этих задач в реальных условиях реального дата-центра. Сегодня именно операторы сетей доставки трафика сталкиваются с огромными объёмами трафика, которые необходимо эффективно и оптимально распределить по подчас скромным ёмкостям региональных операторов связи. Эта задача требует особого подхода, один из аспектов которого мы попытались изложить в данной статье, совершенно не претендуя на исчерпывающее решение. ■

### Список литературы:

- [1] <https://www.osp.ru/lan/2000/12/131492>
- [2] [https://en.wikipedia.org/wiki/Multi-chassis\\_link\\_aggregation\\_group](https://en.wikipedia.org/wiki/Multi-chassis_link_aggregation_group)

### Об авторе

Арсений Валентинович Великород,  
старший сетевой инженер CDN-Video, Россия, Москва

# MSK-IX – на острие технологий

В 2025 году MSK-IX отмечает своё 30-летие. Старейшая и крупнейшая точка обмена трафиком России, одна из крупнейших IX мира имеет на рынке репутацию стабильного и надёжного игрока, быстро реагирующего на технологические инновации, внедряющего современные и актуальные решения для телекома, а иногда и вовсе задающего тренды для развития других IX. О пути, который прошла компания за три десятилетия, и о планах на будущее рассказывают генеральный директор MSK-IX Евгений Морозов и советник генерального директора Елена Воронина.



## - В этом году MSK-IX исполняется 30 лет. Как вы оцениваете путь, который прошла компания за эти годы?



**Елена Воронина:** Давайте начнём с ключевых моментов, которые были решающими для развития MSK-IX. Прежде всего, это замечательная идея, идея на все времена – peer-to-peer, отношения равных. И она появилась именно тогда, когда рынок этого потребовал.

Создание эффективной команды единомышленников, которая занималась этим проектом, – также важный момент. Многие из членов этой команды работают у нас на протяжении всех 30 лет: это высококвалифицированные сотрудники, умеющие решать сложнейшие технологические задачи.

Но, конечно, не нужно сбрасывать со счетов то, что и менеджмент был неплохой, и удача способствовала. Без неё никуда. Пожалуй, так начинал и начинает любой стартап, который успешно развивается. А дальше главное – это расти вместе с рынком и стараться улавливать тренды и направление развития.



**Евгений Морозов:** Важно, что в течение 30 лет Интернет менялся, а проект «MSK-IX» всё время оставался актуальным, эволюционировал, развивал дополнительный функционал и новые услуги, в каждый момент отвечал вызовам рынка телекоммуникаций и общей рыночной ситуации.

## Из истории компании:

Сеть обмена трафиком между провайдерами MSK-IX (Московский Internet Exchange) появилась на свет в 1995 году, её участниками стали семь московских интернет-провайдеров, а инициатором проекта и базой первого российского Internet eXchange стал Российский НИИ развития общественных сетей (РосНИИРОС – учреждён Институтом атомной энергии им. Курчатова в 1992 году). Первое соглашение о создании MSK-IX было напечатано на пишущей машинке, и вскоре после его подписания заработал первый коммутатор М9-IX (первое историческое название MSK-IX), располагавшийся на телефонной станции М9 на улице Бутлерова.

**Сегодня сеть MSK-IX состоит из 46 узлов, размещённых в 10 городах России.**

Сайт: [www.msk-ix.ru](http://www.msk-ix.ru)



Фото 1. Первый коммутатор MSK-IX.



Фото 2. Объединенный коллектив РосНИИРОС и MSK-IX, 2004 год.

### - Где сегодня место MSK-IX среди других крупнейших точек обмена трафиком - и российских, и мировых?



**Е.В.:** В целом, рынок точек обмена трафиком и в России, и за рубежом активно развивается, точек обмена трафиком и новых проектов в этой сфере с каждым годом появляется всё больше. Это, с одной стороны, подчёркивает актуальность этой технологии, а с другой стороны, держит в постоянном тонусе: компания работает на конкурентном рынке, и приходится всё время совершенствоваться, сравнивая себя с другими крупнейшими игроками.

MSK-IX всегда делала акцент в своём развитии на высокий уровень эксплуатации, передовые технологии и высокое качество предоставляемых услуг. Сильная сторона – это то, что компания в данный момент не сосредоточена лишь на одной услуге обмена трафиком. MSK-IX сегодня – это экосистема для сетей самого разного уровня и назначения.



**Е.М.:** MSK-IX занимает лидирующие позиции в рейтингах мировых точек обмена трафиком по пиковому трафику и количеству участников. Наше ключевое преимущество заключается в значительном количестве уникальных участников, а также в высочайшем уровне надёжности и отказоустойчивости. Это результат большой работы, результат тех подходов, которые содержатся в «ДНК» MSK-IX.

Цифровизация экономики привела к тому, что сегодня услуги MSK-IX становятся всё более востребованными для клиентов b2b. Для нас важна репутация, и любая модернизация, которую совершает MSK-IX, рассматривается с точки зрения отказоустойчивости: будь то резервирование каналов связи или резервирование питания на наших узлах связи – мы не

экономим на инфраструктуре для того, чтобы предоставить лучший SLA и максимальный уровень качества услуг.

### - А как на развитие MSK-IX повлияли санкции?



**Е.М.:** Безусловно, санкции оказали влияние на российский телеком-рынок в целом и на MSK-IX в частности. Изменился состав участников. Многие проекты, которые использовали MSK-IX для обмена трафиком, ушли с российского рынка, и, естественно, эти игроки перестали быть нашими клиентами. Но при этом объёмы трафика увеличились, потому что точка обмена стала ещё более значимой с точки зрения локализации трафика. Пользователи стали больше смотреть российский контент, вырос трафик на отечественных видеоплатформах, и это привело к тому, что мы выполнили свою ключевую роль по локализации трафика. Темпы роста трафика в 2024 году значительно выше предыдущих лет, и в этом плане санкции, скорее, сработали нам на руку - и это позитивный момент.

Конечно, есть и негативные стороны. Увеличились сроки поставки оборудования, увеличилась стоимость оборудования.

Но, скажем так, это всё те преграды, которые преодолимы, и они в конечном итоге не сказались на качестве тех услуг, которые мы оказываем своим клиентам.



**Е.В.:** Кроме того, у MSK-IX появились новые зарубежные клиенты – из стран дальнего зарубежья, из Южной Америки, из Азии, клиенты, которых раньше не было среди участников MSK-IX. Мы это связываем в первую очередь с интересом к локальному контенту в России – и это тоже прямое следствие санкций.



Фото 3. Узел точки обмена трафиком.

**- А какие сейчас наиболее значимые вызовы и узкие места существуют в обеспечении бесперебойного и эффективного обмена трафиком? И как MSK-IX с этим справляется?**



**Е.В.:** Есть устоявшийся термин «обмен трафиком», и каждый понимает его по-своему. Но этот термин неверно воспринимать «напрямую», как товарно-денежный обмен – речь идёт о том, что создаётся возможность для прямого прохождения трафика между сетями. С технологической точки зрения IX — это большой перекрёсток, это общая точка для многих сетей.

Поэтому, когда мы говорим о бесперебойном эффективном обмене трафиком для операторов, мы говорим, в том числе, что должна быть создана инфраструктура, которая, во-первых, стабильно работает, во-вторых, имеет достаточную пропускную способность. Для того, чтобы организовать такую инфраструктуру, безусловно, требуется производственная база, аппаратное, программное и техническое обеспечение. Один из самых значимых на сегодня вызовов – это состояние аппаратной базы. И мы очень внимательно следим за развитием этого направления в Российской Федерации.

**- Но несмотря на эти сложности, компания развивает множество новых проектов – как уже раньше говорилось, свою настоящую экосистему. Расскажите про них подробнее?**



**Е.М.:** Одним из наших знаковых проектов стал проект «Медиалогистика», появившийся восемь лет назад. На мой взгляд, это удачное дополнение к точке обмена трафиком, которое появилось в очень актуальный момент, поймав тренд по переходу доставки телевизионных сигналов со спутника на наземные каналы связи. Своим появлением и развитием «Медиалогистика» усилила этот тренд, позволив участникам MSK-IX не только обмениваться трафиком с другими операторами и контент-провайдерами, но и получать пакеты телесигналов, которые им необходимы для организации услуги IPTV для своих конечных абонентов.

Ещё один наш флагманский проект связан с темой безопасности. На стыке технологий IX и безопасности был создан продукт, который мы назвали «Защищённые пиринговые группы». Это технология, которая позволяет заинтересованным компаниям обмениваться служебным трафиком между собой, не используя публичный доступ в Интернет. Фактически, это отдельная ветка развития IX для b2b-пользователей.

Наш совсем новый проект – платформа «Медиабаза», продолжение эволюционного развития проекта «Медиалогистика». Это маркетплейс для размещения и покупки контента b2b-компаниями.



**Е.В.:** Одним из старейших сервисов MSK-IX является распределённое DNS-облако. В первую очередь эта услуга предназначена для наших национальных доменов .ru и .rf, но также и для других российских доменов верхнего уровня, для госструктур, для крупного бизнеса – в общем, для всех, кому необходимо быстрое, безопасное и надёжное облако DNS. Облако территориально распределённое. Для оптимальной доступности DNS-сервера из любой точки сети Интернет используется технология IP-anycast. Также есть специальное DNS-решение для операторов мобильной связи, предназначенное для эксплуатации в высоконагруженных системах.

За 30 лет работы были созданы комплементарные дополнительные услуги для клиентов, функционирует сеть NTP-серверов, на сети установлены зеркала корневых серверов DNS и многое другое. Это на самом деле настоящая экосистема со множеством сервисов.

**- Вы сказали, что у вас часть людей работает с момента основания компании, и эти люди, думаю, с полным правом могут считать себя основателями MSK-IX. Как строятся их отношения с молодой частью коллектива?**



**Е.В.:** Мы стремились создать такую экосистему для нашего коллектива, когда важны не только профессиональные качества, но и человеческие, когда новый сотрудник может поддерживать дружеские и приятные отношения с остальными членами коллектива.



**Е.М.:** Но, разумеется, любой из новых сотрудников должен быть достаточно компетентен для того, чтобы своими новыми знаниями и компетенциями дополнять и усиливать существующую команду.

Команда должна прирастать новыми людьми, и мы с удовольствием принимаем людей на работу, но внимательно смотрим на их компетенции. Нам удалось достичь такого взаимопроникающего эффекта, когда наши коллеги, которые проработали в компании много лет и имеют очень глубокие компетенции в своих темах, делятся своими знаниями, но при этом они готовы принимать новые знания и новые точки зрения от тех людей, которые приходят. И этот симбиоз обновляет компанию.

**- Как вы видите будущее MSK-IX? И как вы считаете, может ли на смену IX через какое-то время прийти что-то другое, например, все переключатся на спутниковый Интернет?**



**Е.В.:** Технологии развиваются очень быстро, но уверена, что MSK-IX идёт в ногу с технологиями и всегда будет соответствовать тем требованиям, которые предъявляет время. Будут новые проекты на базе MSK-IX.



**Е.М.:** Технология IX настолько гениальна в своей простоте, что мне кажется, сколько будет существовать Интернет, столько будет существовать необходимость оптимизировать его, ускорять, уменьшать задержки, и другого инструмента, кроме как точки

обмена трафиком, для этого, по большому счёту, не существует. Я к точкам обмена трафиком отношусь как к социально-технологическому явлению, основной миссией которого является оптимизация маршрутов трафика в Интернете, чтобы это было удобно и технологично использовать большому количеству пользователей.

Поэтому я верю в то, что Интернет будет меняться, будет происходить процесс цифровизации экономики во всём мире, но при этом роль точек обмена трафиком в этих процессах будет такой же значимой, как и на сегодняшний момент. ■



Фото 4. Музей MSK-IX.

# Роль точек обмена трафиком в цифровом прогрессе Ближнего Востока



## Примечание редакции

Данный отчет печатается в сокращённом виде. Полная версия отчета доступна на <https://labs.ripe.net/author/jadelcham/unlocking-digital-growth-the-role-of-ixps-in-the-middle-east/>

## История вопроса

Цифровая трансформация на Ближнем Востоке преобразует экономику, общество, образ жизни и условия трудовой деятельности. Свою незаменимую роль в этой трансформации играет сетевая инфраструктура – в частности, точки обмена трафиком (IXP), которые ускоряют обмен данных.

На Ближнем Востоке хорошо понимают насущность данных перемен. Правительства и частный сектор инвестируют в цифровую инфраструктуру, навыки и инновации. Тем не менее, один из главных компонентов трансформации – точки обмена трафиком – часто упускается из виду.

Точки обмена трафиком – это объекты, где обеспечивается связность между сетями, такими как интернет-провайдеры, провайдеры контента, гипермасштабируемые центры обработки данных, компании или учебные заведения. Точки обмена трафиком являются основополагающим компонентом инфраструктуры Интернета, который обеспечивает его эффективность, устойчивость и в целом положительный пользовательский опыт.

До 2010-х годов IXP выполняли ограниченную функцию и не играли заметной роли в системе связности на Ближнем Востоке. В этот период появилось несколько IXP с ограниченными возможностями. Большая часть интернет-трафика проходила через Европу или Азию, что увеличивало время отклика и делало передачу данных очень затратной.

Понимая необходимость развития внутренней цифровой инфраструктуры, разные структуры, включая технические, общественные и государственные организации, инициировали создание точек обмена трафиком. Первой IXP в регионе является до сих пор функционирующая Бейрутская точка обмена трафиком, которая заработала в декабре 2007.

В последние десять лет наблюдается скачок развития в сфере пиринга и обмена данными в регионе. В настоящий момент в десяти странах находятся 15 работающих IXP (рис. 1).

## 1. Сохранение локальности трафика

### 1.1. Подключение поставщиков услуг для комфортного обмена трафиком

В ходе изучения развития Интернета на Ближнем Востоке можно обнаружить закономерность: имеется местная монополия или малая олигополия, которая строго контролирует международные шлюзы соответствующих стран. Обладая заметными преимуществами, это явление также скрывает в себе значительные недостатки.

Эти монополии и олигополии базируются на экономическом принципе, согласно которому избранной группе игроков, единолично контролирующей международные каналы связи, экономически выгодно сохранять движение локального трафика внутри своей страны. Предполагаемое преимущество заключается в том, что маршрутизация всех локальных коммуникаций через внутреннюю инфраструктуру эффективнее, чем затратный транзит через международные каналы. В теории таким образом формируется более экономически целесообразная модель для доминирующих участников.

Но недостаток этого, казалось бы, прагматичного подхода становится очевиден, если взглянуть на ограничения, которые он создаёт для сферы телекоммуникаций в более широком смысле. В подобных сценариях доминирующий участник или маленькая олигополия, контролирующая международные шлюзы, начинают диктовать, кто может иметь доступ к международным каналам связи и на каких условиях. Эта ограничивающая среда подавляет конкуренцию и инновации, мешая росту других участников рынка, чьи модели развития предполагают доступ к международным каналам связи помимо тех, которые санкционированы доминирующим участником.

Актуальный пример – Ливан, где национальный оператор связи и Министерство телекоммуникаций всё еще полностью контролируют международные шлюзы. В ответ на это в 2007 году возникла первая IXP в регионе – Beirut IX, которая функционирует по сей день.



Beirut IX функционирует в рамках модели управления с участием нескольких членом. Beirut IX выполняет функцию кооперативной платформы, при этом за её развитие совместно отвечают организации-участники. Согласно данной модели, каждый участник обладает значительным весом в процессе принятия решений IXP. Уровень участия прямо определяет степень влияния участника на формирование правил работы.

В других ближневосточных странах возникла иная модель управления, согласно которой IXP как платформа принадлежит правительству и подлежит надзору соответствующими органами. Правительство и надзорный орган активно участвуют в

самом владении, а также в управлении IXP и её работе, формируя правила и процессы в соответствии с более широкими общестрановыми стратегиями и задачами телекоммуникаций. Примерами IXP, работающих по такой модели, являются Kuwait IX (создана в 2018 году) и Palestine IX (создана в 2020 году).

В некоторых IXP применяется модель многостороннего управления со множеством заинтересованных лиц, которая имеет характеристики обеих моделей, описанных ранее. Активными участниками здесь являются правительства, надзорные органы, операторы телекоммуникационных услуг и другие равноправные члены. Пример такого подхода

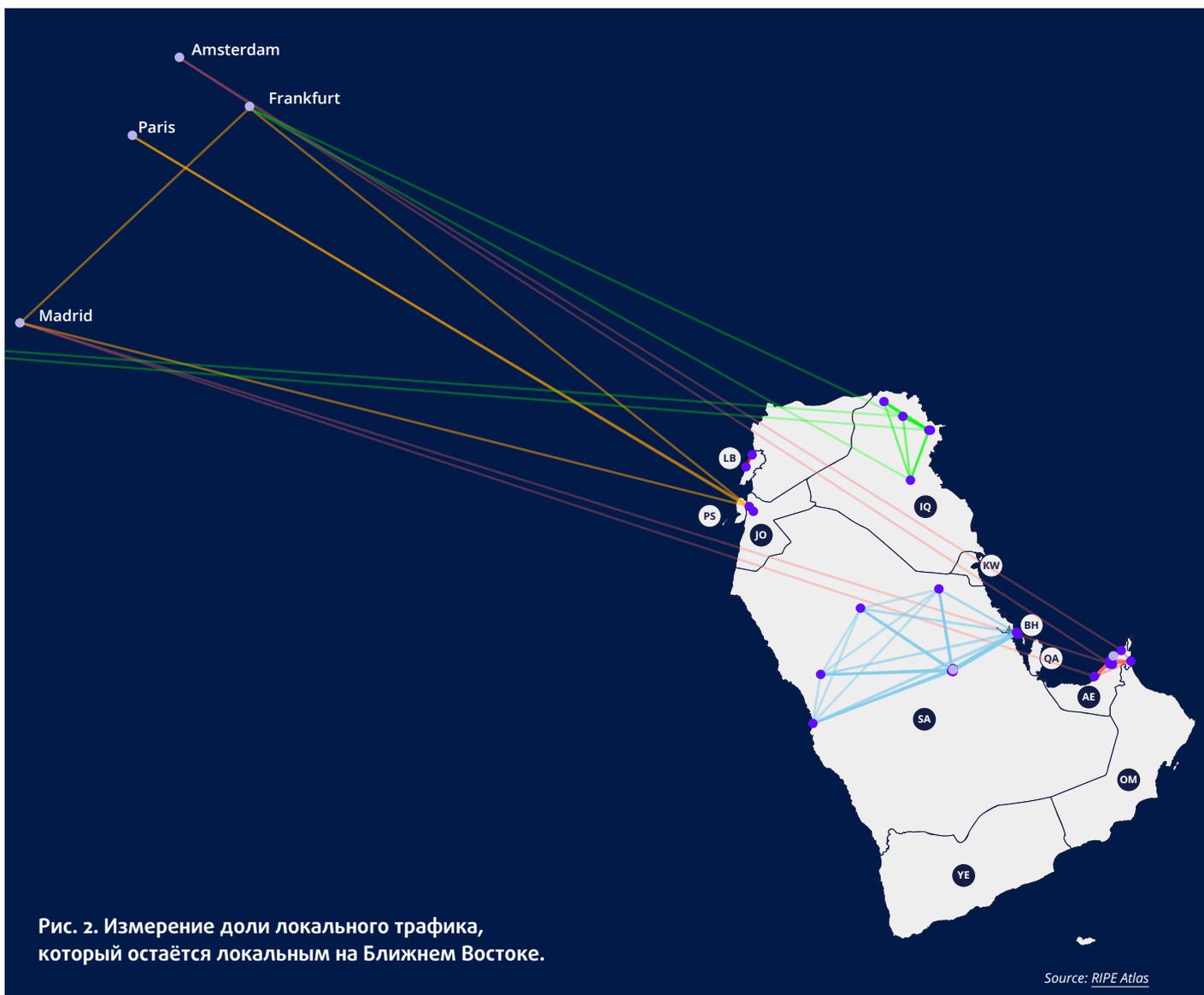


Рис. 2. Измерение доли локального трафика, который остаётся локальным на Ближнем Востоке.

наблюдается в структуре управления точкой обмена трафиком SAIX (создана в 2017 году) в Саудовской Аравии, а также в предлагаемой структуре точки обмена трафиком LEB-IX (ещё не запущена) в Ливане.

С другой стороны, есть такие страны, как Бахрейн, где в начале 2000-х состоялись первые реформы сектора телекоммуникаций. Этот смелый шаг имел целью уйти от традиционной модели контроля за счёт концентрации рынка к рынку телекоммуникационных услуг с меньшим набором ограничений. Модель позволила множеству участников свободно создавать и приобретать международные каналы связи. Однако в ней выявились и серьёзные препятствия.

Одно из таких препятствий – отсутствие нейтральных IXP в Бахрейне. В отличие от описанной выше модели контроля за счёт концентрации рынка, где доминирующий участник строго контролирует международные шлюзы, либерализация позволяет различным операторам связи обмениваться трафиком таким образом, чтобы это лучше соответствовало их планам по расширению. Тем не менее, отсутствие нейтральных IXP создало парадоксальную ситуацию для операторов, которые с осторожностью относились к пирингу со своими локальными конкурентами и предоставлению им

доступа к своей инфраструктуре, размещаемому контенту и пользователям. Боясь обеспечить конкурентам возможность зарабатывать на своих инвестициях в сеть, они старались не создавать условия для локального пиринга.

Это привело к появлению так называемой тромбонной маршрутизации, при которой данные шли обходными маршрутами через международные IXP за пределами региона. Как результат – задержки, более высокие потребности относительно пропускной способности и дополнительные затраты, так как, прежде чем попасть в место назначения внутри страны, данные проходили через протяжённые каналы за её пределами.

Как дополнительный фактор, участники выбирали обходные и менее эффективные маршруты из-за высокой стоимости локальной инфраструктуры. Динамика стоимости и отсутствие нейтральной среды способствовали тому, что операторы, из соображений конкуренции или финансовой выгоды, отдавали предпочтение не пирингу внутри страны, а международному транзиту трафика.

Данная ситуация выявила необходимость достижения тонкого баланса на либерализованном рынке телекоммуникаций. В то время как реформы способствовали развитию кон-

курении и разнообразия на рынке, отсутствие нейтральных IXP, нежелание отказаться от конкурентных преимуществ и забота операторов о стоимости привели к непредвиденным последствиям.

Чтобы выяснить, в какой степени локальный трафик остаётся локальным (через локальные IXP или через другие каналы связи), были произведены замеры в пяти странах (Саудовская Аравия, Ливан, ОАЭ, Иордания и Ирак) с использованием аппаратных устройств для сбора информации о трафике системы RIPE Atlas (рис. 2). Были измерены трассировки маршрутов между аппаратными устройствами одной страны, а затем проанализированы пути этих трассировок. В Саудовской Аравии и на четырёх аппаратных устройствах в Ливане не были обнаружены зарубежные IP-адреса. Есть вероятность, что некоторые данные выходили из страны (геолокация IP несовершенна), но известно наверняка, что в этом процессе не участвовали зарубежные IXP. Для ОАЭ карта тоже «чистая», имеются только две точки с IP-адресами в Европе. В Саудовской Аравии и ОАЭ локальные IXP берут на себя значительную часть маршрутизации. В Ираке и Иордании наблюдается выход из страны, что говорит о возможности оптимизировать локальную маршрутизацию.

На рисунке 3 представлен анализ трассировки маршрутов между аппаратными устройствами RIPE Atlas, которые используются в различных ASN в Саудовской Аравии. Голубые квадраты показывают, где сетевой маршрут проходит через SAIX Riyadh. Это способствует сохранению локального трафика внутри страны (когда источник и конечный пункт также являются локальными).

## 1.2. Локализация контента

В начале 2010-х роль владельца контента была сопряжена с большими трудностями и невероятно высокими затратами на локальный хостинг. Финансовые препятствия побудили многих владельцев контента изменить стратегию и разместить свой контент в странах с более продвинутыми рынками. Несмотря на неизбежные задержки, перспектива существенно сэкономить на этих развитых рынках выглядела очень привлекательной.

Предлагая местным пользователям доступ к контенту, созданному внутри страны, но размещённому на зарубежных хостингах, интернет-провайдеры столкнулись с непреодолимым препятствием: затратами на международный транзит данных при извлечении контента. Вместо того, чтобы вкладывать средства в создание надёжных дата-центров внутри страны и развитие разнотипных инфраструктурных маршрутов внутри своей страны, владельцы контента не могли устоять перед экономически выгодными решениями на более продвинутых рынках.

На практике это означало, что для предоставления локальным пользователям доступа к локальному контенту, размещённому на хостингах за рубежом, интернет-провайдеры несли расходы из-за передачи данных за рубеж и обратно, вместо того, чтобы потратить те же средства на создание хорошо отлаженных дата-центров внутри страны и на развитие разнотипных инфраструктурных маршрутов в стране.

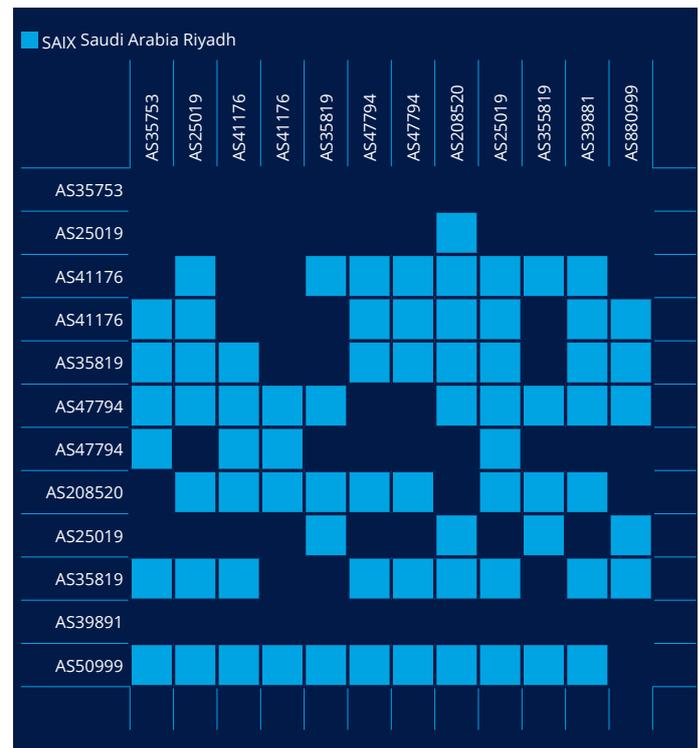


Рис. 3. Номера автономных систем (ASN), идущие через SAIX Riyadh (Саудовская Аравия).

С появлением сетей доставки контента (CDN), облачных сервисов и гипермасштабируемых центров обработки данных возникли новые эффективные и доступные по стоимости варианты. Имея огромный охват и выгодную позицию в переговорах, глобальные игроки пользовались предпочтением при размещении локального контента. Способность оптимизировать доставку контента через локальный кеш, а также более целесообразные затраты на инфраструктуру, которые обсуждались на мировом уровне, обеспечили глобальным хостингам моментальный успех и популярность среди операторов и правительств.

Влияние на развитие локальной инфраструктуры было заметным. Появление CDN и гипермасштабируемых центров обработки данных способствовало открытию местных дата-центров и точек обмена трафиком, спровоцировав новую волну возможностей в регионе.

Несмотря на растущие преимущества локальной интернет-среды, глобальные компании продолжают доминировать. В конкуренции с глобальными гигантами, которые могут похвастаться большими ресурсами, обширными портфолио контента и более выгодными сделками, локальные хостинг-провайдеры испытывают серьёзные трудности и сталкиваются с рисками для выживания своего бизнеса. Кроме того, растущая зависимость от глобальных игроков ведёт к большей централизованности интернет-сферы. Экспертов волнует возможное влияние на развитие локальной индустрии и на разнообразие цифровой экосистемы.

Присутствие глобальных игроков несомненно способствовало улучшению локальной инфраструктуры, но невыгодное положение местных компаний создаёт сложности для развития внутри страны. Какими могут быть долгосрочные последствия более централизованного и глобально зависимого Интернета?

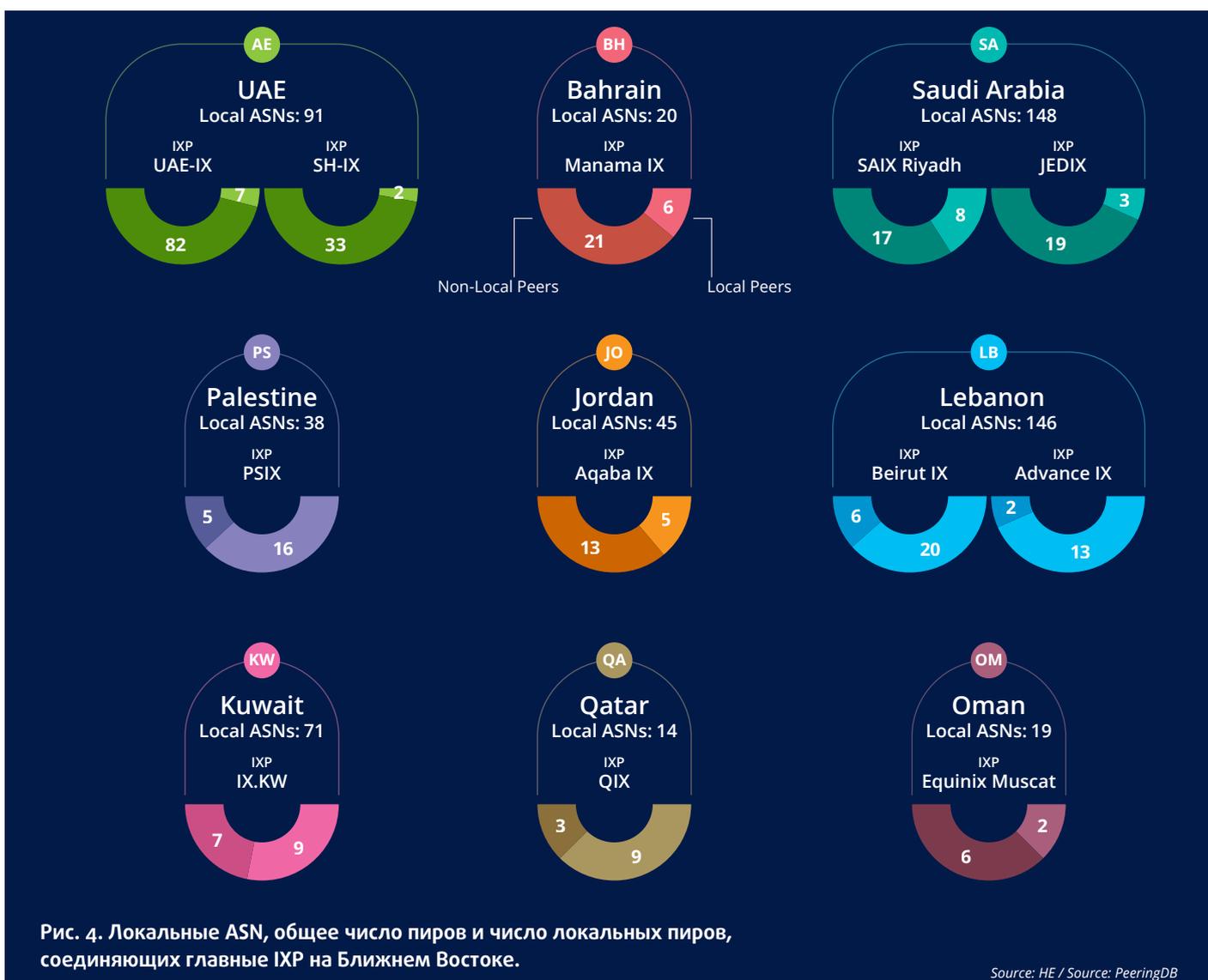
Достижение равновесия между глобальным сотрудничеством и сохранением внутривосточной автономии – необходимое условие для обеспечения отлаженной и разнообразной цифровой экосистемы.

В современной цифровой индустрии всё чаще признаётся необходимость оптимизировать маршрутизацию и сохранять локальный интернет-трафик в пределах страны. Для лидеров индустрии, законодателей и регуляторов всё яснее видны преимущества этих стратегий, и предпринимаются шаги для улучшения локализации цифровой инфраструктуры на Ближнем Востоке.

Нормативная база, которая поощряет справедливую конкуренцию и открытый доступ к IXP по доступным тарифам, способствует инновациям и обеспечивает равные возможности подключения и обмена трафиком для всех сетевых операторов.

## 2. Поддержка локального пиринга для развития цифровой экономики

В постоянно меняющейся цифровой экономике Ближний Восток стоит на серьёзном перепутье, где для значительного повышения скорости и дальнейших инноваций требуется пересмотреть традиционные стратегии относительно IXP. Точки обмена трафиком воспринимались в регионе как место сопряжения исключительно лицензированных интернет-провайдеров, при этом невольно отодвигались на задний план важные сетевые операторы, включая правительственные, корпоративные и учебные сети. Отчасти это было результатом внешних факторов: нормативное регулирование в некоторых странах, ограничивающее категории сетей, которые могут подключаться к IXP, отсутствие необходимых локальных абонентских каналов и провайдеров каналов связи, которые бы по разумным тарифам подключали других сетевых операторов. Эти исключительные условия привели к такой ситуации, когда небольшая группа лицензированных провайдеров (часто рассматривающих друг друга как конкурентов) сомневается в необходимости своего участия в создании и развитии IXP в своих странах.



Ещё одним сложным обстоятельством является то, что лицензированные провайдеры рассматривают других сетевых операторов в стране как клиентов и опасаются потерять прибыль, если данные операторы получают доступ к локальным IXP. Опасения создают серьёзный барьер, мешая локальному развитию пиринга и взаимодействия. Наблюдается большой конфликт интересов, если IXP работает под зонтиком провайдера.

IXP – это простой и эффективный способ для сетевых операторов в стране получить больше контроля над формированием и отправкой потоков трафика. В сочетании со способностью IXP снижать время отклика и затраты на передачу данных это позволяет стартапам эффективно развиваться и оказывать услуги. Ускоренные инновации незаменимы для поддержания конкурентоспособности в цифровую эпоху.

В отчёте «Общества Интернета» (Internet Society) по точкам обмена трафиком в Кении и Нигерии подчёркнуты определённые преимущества, включая упрощённый доступ к электронному правительству, более широкое использование сетей в образовательных и исследовательских целях, а также возвращение ранее экспортированных финансовых платформ онлайн-банкинга обратно в Нигерию.

IXP не работают по отдельности: для успешного развития им нужна экосистема, в которой принято делиться знаниями и обмениваться опытом. Развитие культуры сотрудничества среди пилов IXP способствует накоплению коллективных знаний и передовых практик.

На рисунке 4 показано число локальных пилов, которые подключаются к IXP в своих странах, относительно числа нелокальных пилов в этих IXP. Чтобы показать количество сетевых операторов в стране, также дано количество локальных номеров автономных систем (ASN).

**Примечание:** не все локальные ASN должны присутствовать в IXP. Они указаны здесь, чтобы показать потенциальный объём локального незанятого рынка.

### 3. Привлечение глобальных гипермасштабируемых центров обработки данных и поставщиков контента

Успех IXP в регионе напрямую зависит от активного участия различных категорий заинтересованных сторон. Интернет-провайдеры, поставщики контента, провайдеры облачных сервисов, гипермасштабируемые центры обработки данных и дата-центры находятся в сердце пиринговой экосистемы, и каждый из этих участников играет уникальную роль в улучшении качества связности, устранении задержек и в содействии инновациям.

Гипермасштабируемые центры обработки данных, провайдеры облачных сервисов и контента, в том числе гло-

	SAIX RU	JEDIX	Equinix Jeddah	Equinix Muscat	UAE-IX	MN-IX	Number of IXPs	Total Port Capacity
Facebook/Meta				200		100	2	300
Google	200				200	100	3	500
Kaopu Cloud	100	100	100				3	300
Medianova	100	200			100		3	400
Zenlayer	100	100			100		3	300
Edgio		100		100	100		3	300
Amazon					200	400	2	600
Baishan	100	100					2	200
Microsoft					200		1	200
Fastly					100		1	100
Edgeuno	100						1	100
Metaversecloud	100						1	100
ACE CDN		200					1	200
Bigo		100					1	100
Akamai					100		1	100
MBC					100		1	100
Oracle					100		1	100

Source: Transformation of peering in the Middle East, Bernd Spiess, DE-CIX/UAE-IX, MEMOIG 23

Рис. 5. Лидеры облачных сервисов, CDN и OTT, участвующие в IXP Ближнего Востока. Посчитаны только порты 100 Гб. Данные от 3 сентября 2023 г.

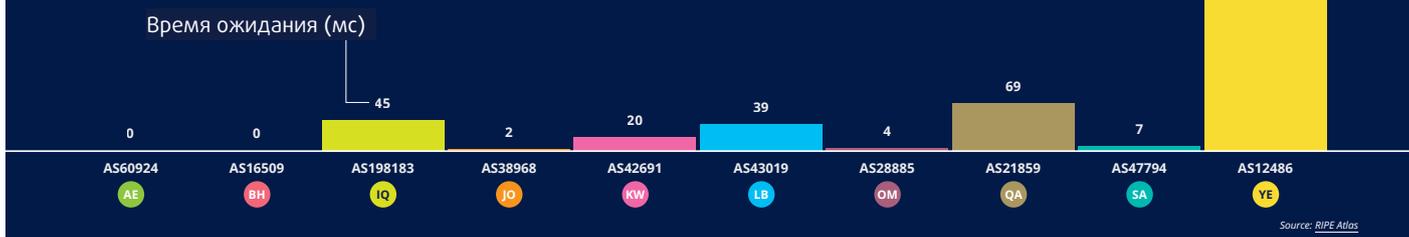
бальные техногиганты и локальные создатели контента, одинаково важны для пиринговой экосистемы. Они генерируют и размещают на своих хостингах цифровой контент: сайты, приложения и сервисы потокового контента. Подключение к IXP позволяет им доставлять контент конечным пользователям в регионе более эффективно, снижать время ожидания и улучшать пользовательский опыт. Локальный хостинг контента на IXP ещё больше ускоряет доставку контента, способствуя росту индустрии цифрового контента.

Ближний Восток успешно привлекает и размещает у себя в регионе хабы для мировых игроков, что не только улучшает связность и цифровые возможности региона, но и помогает региону стать ключевым участником глобальной цифровой среды.

В 2023 году провайдеры облачных сервисов (AWS, Microsoft и Google), сети доставки контента (Cloudflare и Akamai), а также OTT-сервисы (Meta (признана в России экстремистской организацией), Shahid) установили пиринговые связи в большинстве точек обмена трафиком в регионе. Не все эти игроки представлены во всех странах региона, их распределение отражает потребности рынка и другие коммерческие и нормативные соображения.

На рисунке 5 представлены IXP региона, где присутствуют (в разном качестве) провайдеры контента и облачных сервисов.

Рис. 6. Выход на региональную платформу электронной коммерции на хостинге облачного провайдера.



Была выполнена серия измерений (рисунок 6) с помощью аппаратных устройств RIPE Atlas на Ближнем Востоке с целью определить производительность и время отклика на запросы с этих аппаратных устройств региональной платформы электронной коммерции на локальном облачном сервисе.

Из всех стран региона только в Катаре и Йемене наблюдались существенные задержки отклика. Время ожидания снижается благодаря близости к серверам или доступу к этим серверам в соседних странах посредством межрегионального пиринга.

## Дата-центры

Дата-центры предоставляют физическую инфраструктуру и услуги размещения оборудования, которые необходимы для эффективной работы IXP. Они служат нейтральным местом встречи, где поставщики сервисов, контента и другие сетевые операторы могут взаимодействовать. Дата-центры обеспечивают высокую доступность, безопасность и масштабируемость, позволяя точкам обмена трафиком справляться с растущими объёмами. Кроме того, дата-центры могут предлагать дополнительные платные услуги: например, хостинг на облаке, аварийное восстановление и дальнейшее обогащение экосистемы IXP.

Тем не менее, следует отметить, что на Ближнем Востоке значительная доля дата-центров принадлежит операторам связи, которые также управляют их работой. Как правило, IXP показывают наиболее высокие результаты в нейтральных условиях, предоставляя среду для самых разных сетевых операторов, которые размещают свою инфраструктуру независимо от влияния какого-либо одного оператора связи. Широкое распространение «нейтральных» дата-центров создаёт более диверсифицированную

среду, дополнительные варианты для хостинга, пиринга и взаимодействия.

Разнообразие играет основополагающую роль в развитии конкуренции, инноваций и устойчивой цифровой инфраструктуры региона. Недавно в регионе появилась точка обмена трафиком Equinix, которая работает в Омане и ОАЭ, предлагая клиентам возможности для пиринга и взаимодействия. Стимулирование роста нейтральных дата-центров крайне важно для развития конкуренции, инноваций и устойчивой цифровой инфраструктуры.

## 4. Хаб для обмена региональным трафиком

### 4.1. Развитие региональных и глобальных цифровых связей

Помимо локальных плюсов IXP играет важную роль в улучшении региональных и глобальных цифровых связей. Расположившись на стыке между Азией и Европой, Ближний Восток занимает стратегическую позицию как хаб для международного трафика данных. Это уникальное позиционирование делает регион всё более привлекательным для глобальных инвестиций, сотрудничества и распространения контента.

Эта тенденция показывает, что глобальные участники сферы сетевой доступности формируют партнёрства с точками обмена трафиком в регионе, чтобы расширить цифровые связи за пределы своих границ и даже удалённо подключить сети к этим точкам обмена трафиком. Поэтому для каналов передачи данных важна экономическая интеграция, которая принесёт больше пользы клиентам.

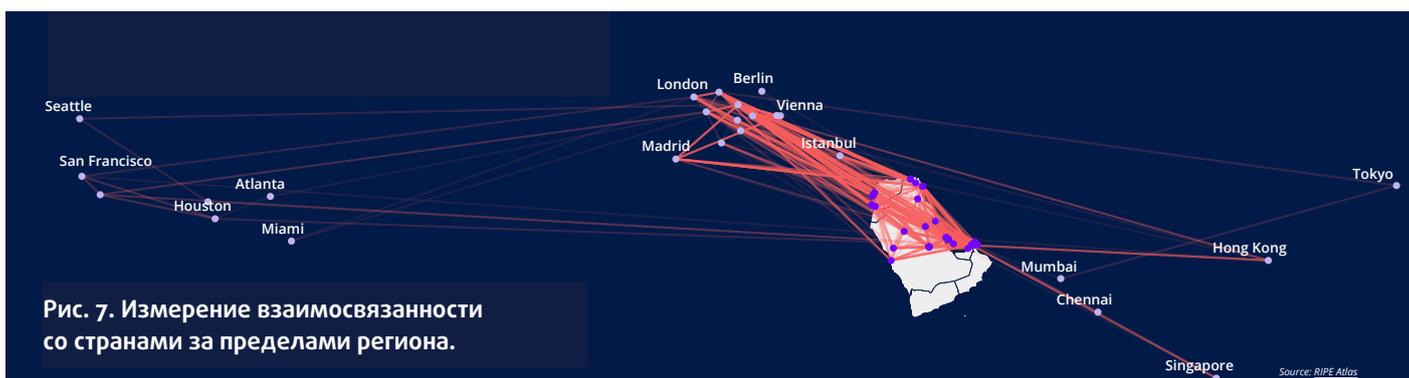


Рис. 7. Измерение взаимосвязности со странами за пределами региона.

Чтобы лучше увидеть региональный ландшафт, была проведена серия измерений с использованием аппаратных средств RIPE Atlas, размещённых на Ближнем Востоке. Измерения касались трассировки маршрутов между парами аппаратных устройств в разных странах. Маршруты, описанные в результатах (исходя из данных геолокации), приведены на рисунке 7.

Если внимательно посмотреть на регион (рисунок 8), то можно увидеть дополнительные детали.

Заметное количество маршрутов между аппаратными устройствами Atlas действительно проходят мимо IXP LAN (UAE-IX, SH-IX, SAIX, Manama-IX, JEDIX и Advance-IX в Ливане), но также отмечается определённое количество маршрутов, выходящих из региона и идущих вплоть до Токио и Сан-Франциско. В этой сфере есть пространство для роста.

В глобальных масштабах IXP Ближнего Востока участвуют в децентрализации интернет-трафика. Таким образом, снижается зависимость от немногочисленных международных шлюзов и сокращаются риски, связанные с появлением узких мест или нарушением работы сети. Диверсификация глобальных интернет-маршрутов повышает стабильность и безопасность всей цифровой экосистемы.

Более того, развитие глобальной связности напрямую влияет на конкурентоспособность региона. Страны реги-

она становятся привлекательными местами присутствия для международных компаний, которым нужны стратегические центры распространения данных. Наплыв международных бизнесов приносит инвестиции, новые рабочие места, передачу опыта и знаний и впоследствии стимулирует экономический рост и цифровые инновации.

Это преимущество становится ещё более значимым при наличии региональных операторов, осуществляющих пиринг на IXP в соседних странах. Как было отмечено ранее, большинство провайдеров облачных сервисов и контента пришли в регион, однако не все из них присутствуют во всех странах региона. Чем больше региональных операторов осуществляют пиринг в соседних странах, тем ниже время ожидания в пределах региона.

Ситуацию в пиринге и цифровых связях кардинально изменила точка обмена трафиком UAE-IX в Дубае, заработавшая в 2012 году. Она сыграла ключевую роль в изменении парадигмы и восприятия IXP в регионе, послужив моделью для других стран. Плотность региональных операторов связи, осуществляющих пиринг в UAE-IX в Дубае, привела к значительному снижению времени ожидания при обращении к контенту, размещённому в IXP (а следовательно, и в ОАЭ в целом), из соседних стран. Чтобы протестировать этот вариант, были проведены измерения с использованием аппаратных устройств RIPE Atlas на Ближнем Востоке. Измерялась производительность и время отклика на запрос от аппаратных устройств в определённых направлениях в региональных IXP.

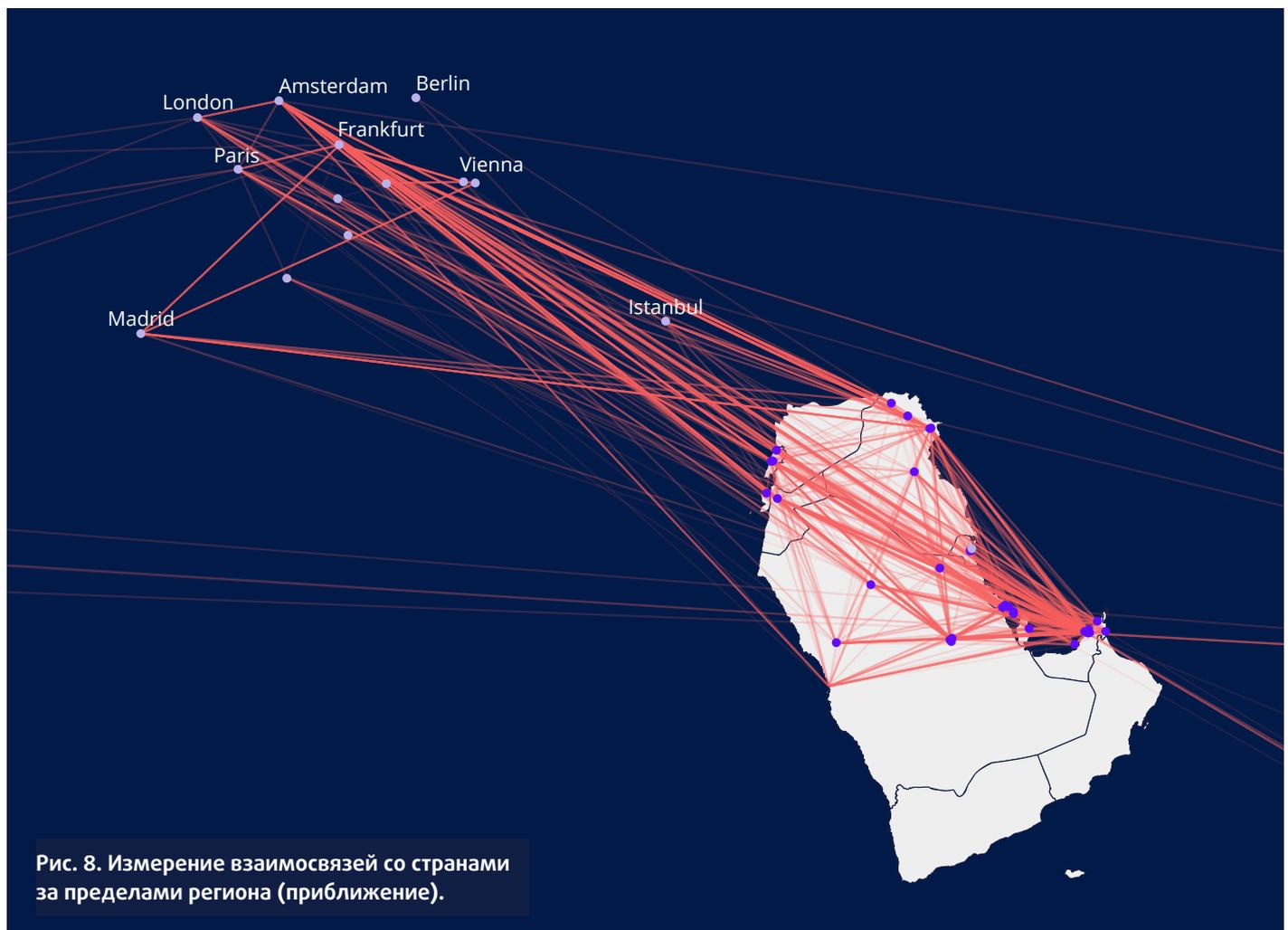


Рис. 8. Измерение взаимосвязей со странами за пределами региона (приближение).

Рис. 9. Выход на провайдера гейминг-платформы в UAE-IX с использованием конечной точки IPv4.



Беглый анализ этих данных (рисунок 9) показывает, что аппаратные устройства в Ливане и Йемене испытывали значительные задержки (около 150 мс) при выходе на гейминговую платформу по сравнению с аппаратными устройствами в Бахрейне или Саудовской Аравии (9 и 12 мс соответственно, при выходе на то же направление). Задержка происходила по причине отсутствия операторов и каналов передачи данных из Ливана и Йемена, которые осуществляли бы пиринг в UAE-IX.

Техническое сотрудничество между интернет-провайдерами принципиально необходимо для эффективной маршрутизации и обмена трафиком. Работая вместе над оптимизацией сетевых конфигураций, интернет-провайдеры и другие сетевые операторы могут повысить общую производительность IXP. В реальности самого присутствия в IXP недостаточно для оптимизации обмена трафиком. Необходимы также техники управления трафиком и формирования трафика в сочетании со взаимными договорённостями между соответствующими сетями.

В то время как более ранние измерения (рисунок 9) выхода на гейминговую платформу, размещённую в UAE-IX, показывают существенно низкое время ожидания отклика от аппаратных устройств в восьми из десяти стран, подобный тест (рисунок 10) выхода на региональную платформу потокового контента, размещённую в UAE-IX, показывает низкое время ожидания отклика с аппаратных устройств только в пяти из десяти стран.

## 5. Выводы и перспективы

На Ближнем Востоке можно ожидать тенденцию к расширению доступа к точкам обмена трафика – например, в форме лицензий IXP, которые позволят большему числу нейтральных операторов выйти на рынок.

Страны с широким географическим и демографическим распределением могут увидеть прогресс в сторону распределённой платформы IXP, где один оператор IXP присутствует в разных городах.

В то же время большее количество зарубежных операторов IXP будут создавать свои собственные IXP в регионе. Новые IXP, скорее всего, не будут расти так же быстро в силу небольшого размера самих стран в регионе и низкой плотности операторов и интернет-провайдеров.

Необходимость региональных подключений растёт, и давление рынка помогает ослабить нормативные требования относительно трансграничных подключений в регионе. Благодаря этому не только крупные операторы, но и другие участники рынка могут получить доступ к ресурсам (например, поставщики облачных сервисов и контента) в соседних странах. Вместе с этим объём трафика, которым обмениваются IXP, скорее всего, вырастет в ответ на спрос на контент и облачные продукты. Тем не менее, эти тенденции могут измениться при возникновении соответствующих условий – например, при несоблюдении благоприятствующего нормативного регулирования. ■

Рис. 10. Выход на региональную платформу потокового контента в UAE-IX с использованием конечной точки IPv4.



A large blue and red cable reel is mounted on a yellow ship deck. The reel has a central hub and many spokes. The ship's hull is yellow and red. The background shows a green hillside and some buildings.

# К вопросу о прочности подводных интернет-кабелей

Джефф Хьюстон



На моем столе лежит трубка. Совсем небольшая. Диаметр каких-то 2 сантиметра на 6 сантиметров в длину. С виду может показаться, что сделана она из обычного белого поликарбоната. Но если посмотреть на срез, оказывается, что пластик лишь оболочка – внутри скрывается медная трубка, а в ней ещё один слой поликарбоната, который окутывает стальную трубку ещё меньшего диаметра. По ней проходит тонкая стальная нить и оптические волокна. Никакой стальной обшивки или каких-либо дополнительных оболочек в трубке нет. Что же это за трубка? Передо мной небольшой кусок подводного оптоволоконного кабеля. Такие используются при прокладке подводных коммуникаций по морскому дну. Почему же они лишены дополнительной защиты? Дело в том, что прокладывают такие кабели на огромной глубине, где, помимо окружающей их воды, особой опасности повреждения нет. Якоря бороздящих морские просторы кораблей и рыболовные снасти обычно до таких глубин не достают. Здесь единственная угроза исходит от подводной сейсмологической активности, но такие случаи крайне редки, да и предсказать их, в любом случае, чрезвычайно сложно. Так что в случае таких подводных толчков оператору всё равно придётся кабель чинить. Если же кабель проходит на меньшей глубине в зонах рыбного промысла, по пути следования кораблей или рядом с портами, его обычно снабжают дополнительными слоями защиты из переплетённой стальной проволоки. Такая стальная оболочка не гарантирует не-

уязвимость кабеля – якорь крупного судна всё равно может его порвать. Но такая защита не лишена смысла и делает своё дело. Если же нужно максимально снизить риск случайного разрыва кабеля, используется траншеекопатель. С его помощью кабель закапывают в толщу дна, если, конечно, его структура позволяет выкопать такую траншею.

Это, конечно, помогает обеспечить сохранность кабеля и гарантировать его непрерывную работу на небольшой глубине, но полностью исключить возможность разрыва такие меры не позволяют. Разрывы на мелководье всё равно случаются. В конце января вьетнамские интернет-провайдеры сообщили о выходе из строя кабелей AAG (Азия - Америка) и APG (Азия - Тихий океан). Недалеко от Гонконга возникли перебои в работе кабеля AAE-1 (Азия - Африка - Европа), а близ Сингапура что-то пошло не так с Внутриазиатским кабелем. В результате практически одновременно оказались повреждены четыре из пяти подводных кабелей, которыми вьетнамские интернет-провайдеры пользуются для соединения с мировым Интернетом.

На починку подводных кабелей уходят недели, а то и месяцы. Ремонтное судно должно подплыть как можно ближе к месту разрыва, поднять кабель и заменить повреждённую секцию, а затем снова погрузить кабель на дно. Если речь идёт о разрезе в нескольких местах, такую процедуру при-



Рис. 1. Сечение подводного оптоволоконного кабеля.

дётся повторить несколько раз. Обычно специализированные суда и персонал нанимают для починки сразу нескольких кабелей, так что в случае множественных разрывов на ремонт отдельного кабеля может уйти время.

В случае с Вьетнамом во время ремонтных работ оставшийся нетронутым пятый кабель – речь шла о сегменте Сингапур – Вьетнам кабеля SMW-3 – также не работал на полную мощность по состоянию на 22 февраля (<https://e.vnexpress.net/news/news/vietnam-s-lastfunctional-undersea-cable-now-malfunctoned-4573176.html>) (рис. 2).

Южно-Китайское море является относительно мелководным. В то же время интенсивность морских перевозок там высокая и ведётся активное рыболовство. Соответственно, инциденты с подводными кабелями вполне возможны, но довольно странно, когда сразу все пять отдельно проложенных кабелей дают сбой. При этом нельзя забывать про политический контекст в этом районе в свете противоречащих друг другу претензий ряда стран на различные участки Южно-Китайского моря ([https://en.wikipedia.org/wiki/Territorial\\_disputes\\_in\\_the\\_South\\_China\\_Sea](https://en.wikipedia.org/wiki/Territorial_disputes_in_the_South_China_Sea)).

С аналогичными проблемами в работе подводных кабелей столкнулся и Тайвань. Два таких кабеля связывают находящиеся вблизи материкового Китая острова Мацзу с Тайванем. По поступившим в конце февраля сообщениям, китайское рыболовецкое судно повредило один из них, а второй пострадал от неизвестного грузового судна ([https://www.theregister.com/2023/02/21/taiwan\\_vietnam\\_submarine\\_cable\\_outages/](https://www.theregister.com/2023/02/21/taiwan_vietnam_submarine_cable_outages/)).

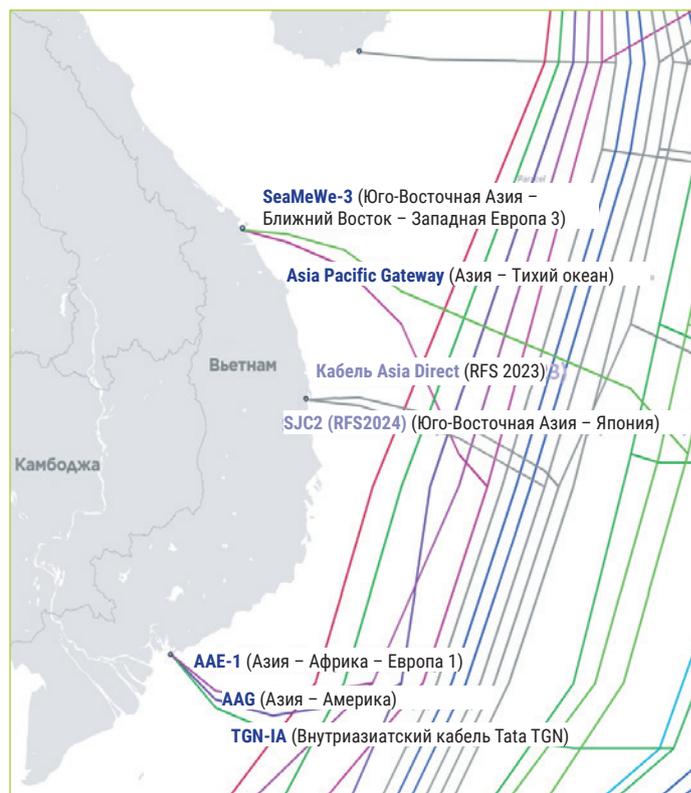
Речь идет о 27-м по счёту повреждении ведущих к островам Мацзу интернет-кабелей за последние пять лет. Повторим, что такое большое число разрывов представляется достаточно нетипичным, если не сказать больше. Можно сослаться на мелководность Тайваньского пролива между Тайванем



и островами Мацзу, где глубина составляет около 60 метров. Можно вспомнить, что за несколько лет до этого проводились работы по углублению дна и что это район активного рыболовства и морских перевозок. И тем не менее, такое количество повреждений не может не вызвать подозрений.

Как же обеспечить подключение к Интернету в ситуации, когда существующие интернет-кабели так часто страдают от подобных сбоев?

Рис. 2. Используемые Вьетнамом интернет-кабели (данные Teleglobe).



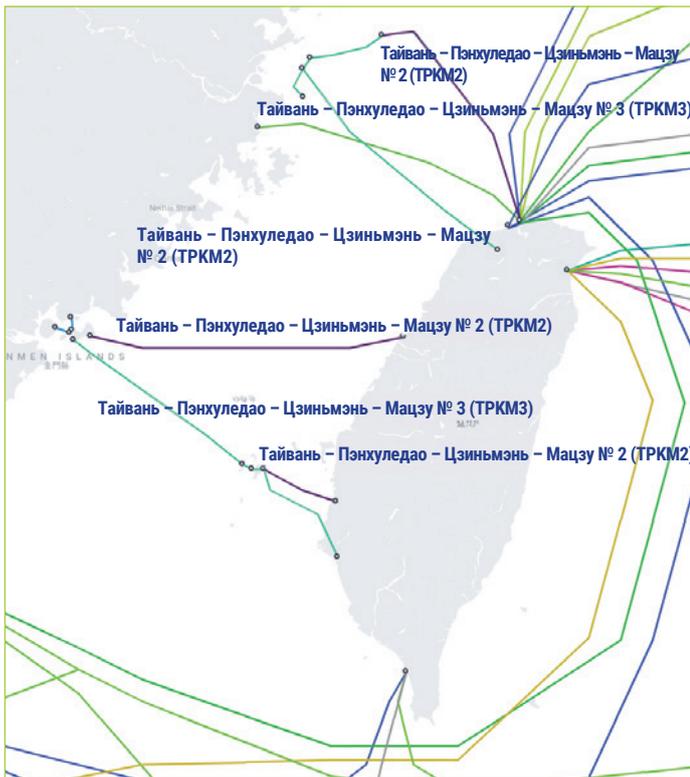


Рис. 3. Интернет-кабели, обслуживающие острова Цзиньмэнь и Мацзу (данные Teleglobe).

Вьетнам пошёл по пути увеличения числа кабелей (<https://e.vnexpress.net/news/news/vietnam-toown-three-undersea-cables-by-2025-information-ministry-4570649.html>). Речь идёт об ответвлениях, ведущих к кабелю Asia Direct и кабелю Юго-Восточная Азия – Япония 2. Таким образом, конечные точки этих кабелей во Вьетнаме равноудалены от конечных точек существующих кабелей.

#### История знает множество примеров преднамеренного вывода из строя кабелей связи.

Так, 5 августа 1914 года, через несколько часов после объявления войны Соединённым Королевством против Германии, британское судно разорвало пять немецких подводных кабелей, связывавших Эмден с Виго, Тенерифе, Азорскими островами и США.

В результате Германия лишилась прямой связи с неевропейскими странами, в первую очередь, с США. Пришлось пользоваться альтернативными маршрутами доставки сообщений, но их можно было легко перехватить, поскольку они проходили через Соединённое Королевство.

Вступление США в войну против Германии в 1917 году было во многом обусловлено перехватом так называемой телеграммы Циммермана, в которой речь шла о создании союза между Мексикой и Германией и поддержке нападения Мексики на США. Зашифрованная телеграмма сначала поступила в Копенгаген, а затем в Лондон для последующей передачи в Вашингтон по трансатлантическим кабелям, связывавшим Соединённое Королевство и США. Перехват и расшифровка «телеграммы Циммермана» стали непосредственным результатом разрыва немецких кабелей.

Казалось бы, что мешает подключиться к Гонконгу, до которого совсем недалеко? Но тут возникает вопрос о продолжающихся трениях между США и Китаем. Такое впечатление, что США перестали выдавать разрешения на размещение на своей территории кабельных систем, связанных с Китаем или Гонконгом. Это уже вынудило компании, работающие с большими объёмами данных, такие как Alphabet и Meta (признана в России экстремистской организацией), сконцентрироваться на Сингапуре и сделать его своим главным региональным центром по оказанию услуг. При этом Соединенные Штаты рассматривают всё Южно-Китайское море как зону повышенного риска. Проложенные недавно с участием компаний Google и Meta азиатские интернет-кабели Vifrost и Echo полностью обходят Южно-Китайское море, минуя также Тайвань и Вьетнам (рис. 4 и 5 на следующем развороте).

Если сбои в работе подводных коммуникаций носят случайный характер, то разумным решением представляется увеличение числа кабелей с утолщённой стальной прокладкой и их укладкой в траншеи. Но что, если это преднамеренные акты саботажа? Как может государство защитить свою телекоммуникационную инфраструктуру от преднамеренных действий по выводу её из строя? Если речь идёт о поиске альтернатив подводным кабелям, следует рассмотреть возможность использования радиосвязи.

Микроволновая связь позволяет покрывать расстояние до 150 километров. Это достаточно распространённое решение при передаче информации на средние расстояния в свете её небольшой затратности. Для концентрации радиосигнала между двумя точками можно использовать зеркальные антенны. Двухточечная радиосвязь используется по такой схеме уже многие десятилетия и зарекомендовала себя эффективным решением при средних и высоких параметрах широкополосности. Однако такая связь уязвима, поскольку третьи лица могут создавать препятствия для передачи сигнала или глушить его, если злоумышленник создаёт радиосигналы, вносящие помехи в работу оператора микроволновой связи. Но главным недостатком микроволновой связи является её ограниченная дальность. При превышении дистанции в 150 километров приходится отрываться от поверхности Земли и задействовать широкополосную спутниковую связь.

Спутниковая передача данных используется интернет-отраслью уже несколько десятилетий. Возможность её использования для передачи информации на большие расстояния не вызывает сомнений. Такой подход в 1990-е годы активно применяла Австралия, пока шла работа по прокладке подводных кабелей по дну Тихого океана. При передаче сигнала на спутник и обратно возникает нежелательная задержка, но зато таким способом можно сразу охватить целое полушарие. Можно ли как-то препятствовать передаче данных с помощью систем геостационарной спутниковой связи? К сожалению, существует целый набор эффективных способов глушения сигнала. Злоумышленник может направить на приёмник спутника энергоёмкий сигнал, настроив его на ту же частоту, что и оператор связи, что с большой долей вероятности приведёт к выводу системы передачи данных из строя.

Что же касается связи с использованием низкоорбитальных

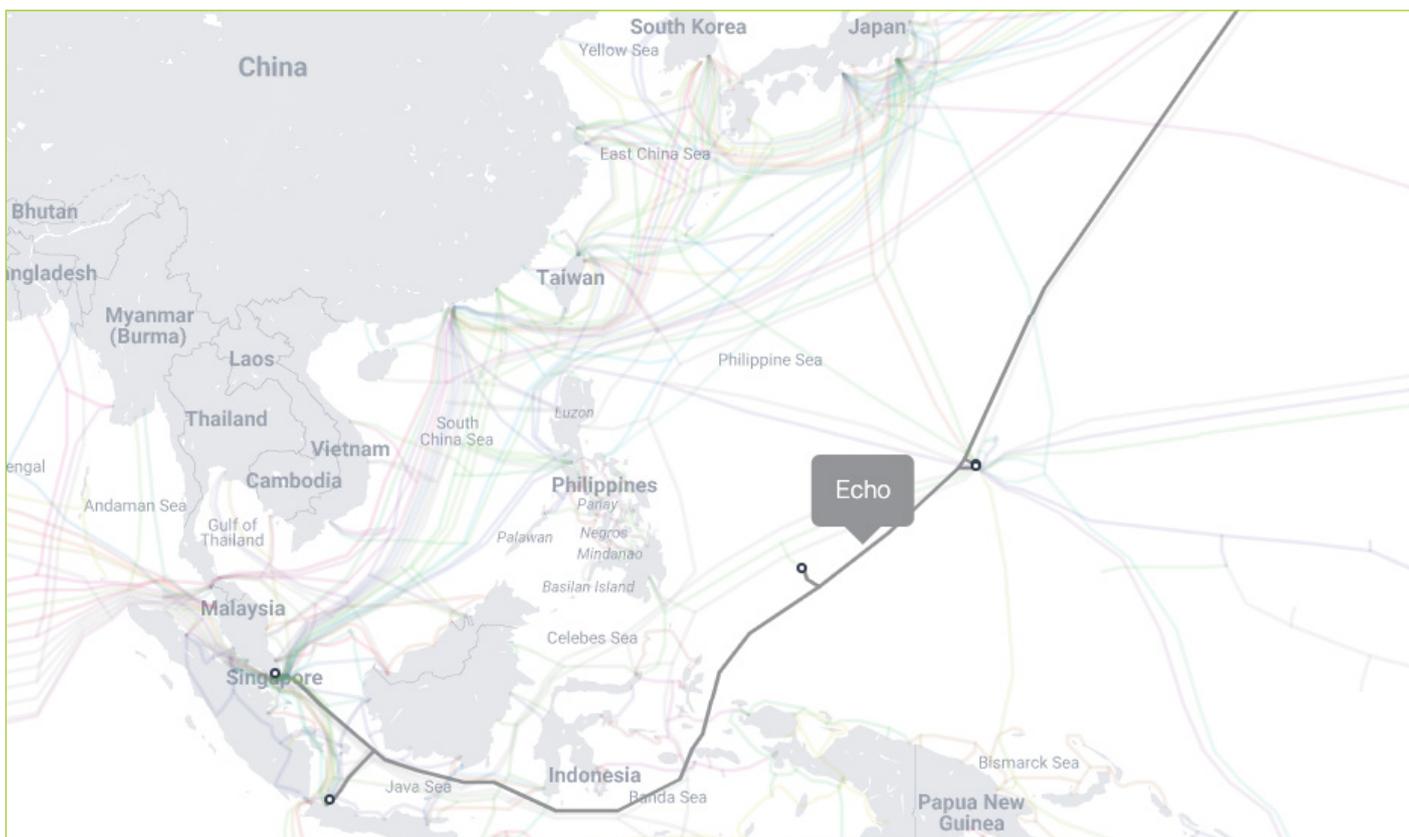


Рис. 4. Маршрут прокладки интернет-кабеля Google Echo (данные Teleglobe).

спутников вместо геостационарных, то в некоторых случаях такое решение представляется целесообразным, и компании O3B и Starlink сейчас оказывают такие услуги во многих странах мира. При этом компания Starlink отдаёт приоритет розничному рынку, тогда как O3B удовлетворяет потребности делового сообщества и государственных заказчиков. Как правило, системы низкоорбитальной спутниковой связи представляют собой достаточно простые решения радиорелейной связи, когда получатель и наземная станция оказываются в «ячейке» одного спутника при его прохождении по орбите. То есть речь идёт об ограниченном диапазоне действия, что имеет как свои преимущества, так и недостатки. В целом это обеспечивает высокую скорость и ёмкость канала спутниковой связи при малой задержке. Учитывая ограниченность зоны покрытия каждого передатчика, для глушения радиосигнала нужно находиться в непосредственной близости либо от пользователя, либо от наземной станции.

По вопросу о низкоорбитальной спутниковой связи важно отметить ещё два важных аспекта. Во-первых, введение в эксплуатацию второго поколения спутников Starlink призвано установить межспутниковые линии связи. Это в некоторой степени затрудняет создание радиопомех, поскольку теперь конечные точки могут и не находиться в пределах определённого расстояния друг от друга. Кроме того, это теоретически расширяет диапазон покрытия услуг низкоорбитальной спутниковой связи, хотя пока конкретных данных от Starlink по этому вопросу нет, так что остаётся только гадать, как будет работать линия межспутниковой связи и как это отразится на оказываемых компанией Starlink услугах в сфере низкоорбитальной спутниковой связи.

Второй вопрос также носит умозрительный характер и состоит в том, сколько всего операторов могут работать в сфере низкоорбитальной спутниковой связи.

**Вопрос непростой, поскольку требуется определить, насколько высоко нужно забраться, чтобы выйти из сферы действия суверенного права стран на воздушное пространство и перейти в область «космического права». Согласно договору от 1967 года, ратифицированному более чем ста странами, суверенные права государств на космическое пространство не распространяются. Участвовавшие в составлении этого договора страны не дали чёткого определения самого понятия «космическое пространство» и не прописали, где именно оно начинается. Некоторые страны выступают за точку отсчёта на высоте 100 километров, другие расположили эту границу чуть ниже, на уровне 80 километров, а третьи предлагают считать началом расстояние в 160 километров от поверхности Земли.**

Дело в том, что для работы в космическом пространстве операторам систем низкоорбитальных спутников не нужно получать какие-либо разрешения от конкретных стран. Согласование требуется только в отношении используемых ими наземных станций, в связи с чем вопрос об экономической целесообразности низкоорбитальной спутниковой связи во многом обусловлен переговорами о наземной инфраструктуре. Каких-либо общих ограничений на национальном уровне или согласно международным договорам в отношении деятельности государств и компаний в космическом пространстве не существует.

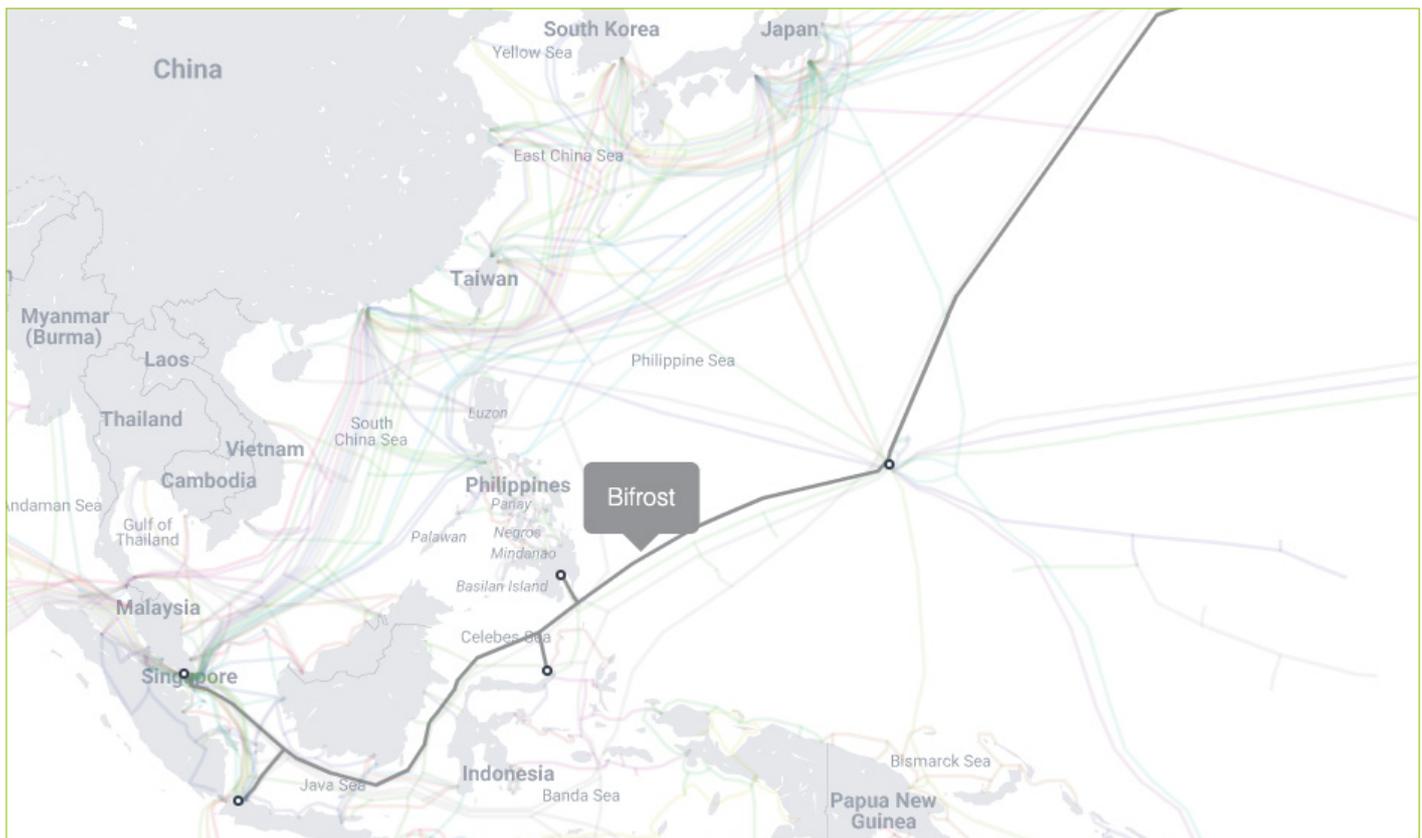


Рис. 5. Маршрут прокладки интернет-кабеля Bifrost (данные Teleglobe).

Если есть ракета-носитель для доставки груза в космос, то далее вы можете делать с выведенными в космос космическими аппаратами всё, что угодно. Несколько десятилетий назад в рамках проекта Iridium было установлено, что главным препятствием в этом отношении выступает получение доступа к частотному спектру в соответствующих странах, чтобы обеспечить приём сигнала на Земле.

К Starlink и ОзВ теперь решила присоединиться компания Amazon, объявив о планах по созданию спутниковой группировки Kuiper в 3,2 тысячи единиц, которые бы находились на высоте от 590 до 630 километров. В СМИ в течение уже долгого времени регулярно упоминается аналогичный проект Китая на 12 тысяч спутников. В результате, вокруг Земли появится множество низкоорбитальных спутников, в связи с чем важно понимать, что с ними делать после их выхода из эксплуатации. Вопрос космического мусора стоит уже давно. Например, его скопление может вызвать цепную реакцию: при достижении определённого критического объёма такого мусора на определённой высоте можно ожидать непредсказуемых и спонтанных столкновений с действующими спутниками, что повлечёт за собой дальнейшее увеличение объёма космического мусора. Когда космические просторы заполнятся им, это пространство уже никто не сможет использовать, причём достаточно долго.

Поэтому на вопрос о том, способны ли системы радиосвязи стать альтернативой услугам кабельной связи, можно ответить утвердительно. Но радиосвязь тоже не застрахована от попыток целеустремлённых и обеспеченных необходимыми ресурсами злоумышленников помешать её работе. Используемые нами телекоммуникационные

системы уязвимы, и полностью гарантировать надёжность таких услуг, идёт ли речь о кабельной или радиосвязи, крайне сложно с технической точки зрения. Построить мощную и общедоступную телекоммуникационную инфраструктуру и при этом обеспечить её абсолютную устойчивость перед лицом обладающего обширными ресурсами и целеустремлённого противника невозможно. А коль скоро мы не в состоянии создать компоненты телекоммуникационной инфраструктуры, полностью защищённой и неуязвимой для попыток препятствовать её работе, нам придётся согласиться с тем, что единственным эффективным решением является создание механизмов, которые вынудят государства сообща отказаться от таких действий путём заключения международных договоров. ■

## Правовая оговорка

Изложенные в данной статье взгляды могут не совпадать с позицией или точкой зрения Азиатско-Тихоокеанского сетевого информационного центра.

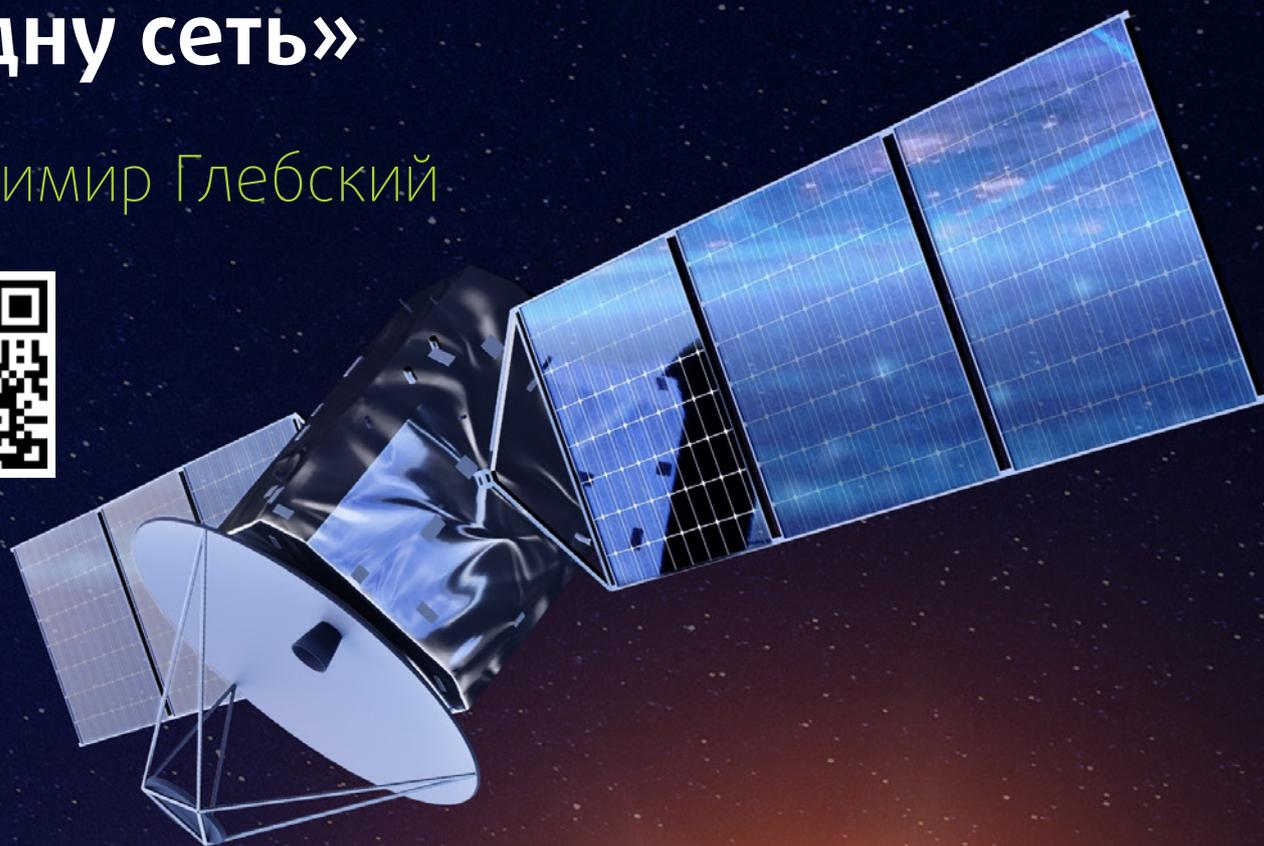
## Об авторе

Джефф Хьюстон имеет степени бакалавра и магистра наук. Занимает должность ведущего научного сотрудника Азиатско-Тихоокеанского сетевого информационного центра, регионального интернет-регистратора Азиатско-Тихоокеанского региона.

[www.potaroo.net](http://www.potaroo.net)

# Спутниковые сети связи, или Как «поймать всю рыбу в одну сеть»

Владимир Глебский

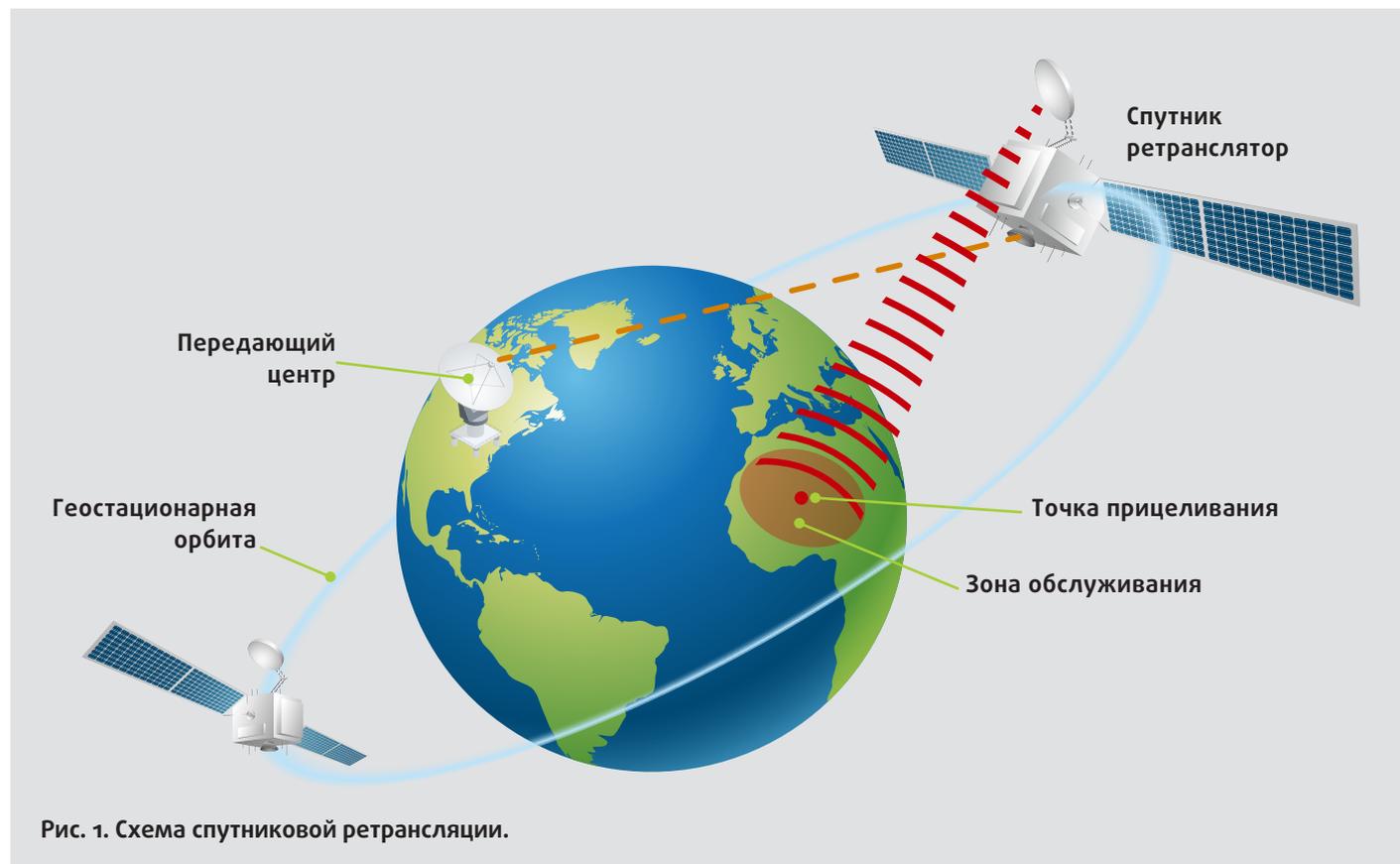


## Аннотация:

Если воспользоваться терминологией рыбаков, то можно сказать, что «ячейки» спутниковых сетей становятся всё меньше, а «площадь» этих сетей и их плотность – все больше. За последние десятилетия цифровые технологии и развитие Интернета изменили сети спутниковой связи до неузнаваемости. От аналоговых технологий, огромных антенн и внушительных размеров пользовательских терминалов цифровая спутниковая связь и Интернет приходят в смартфоны обычных пользователей, а наземные и спутниковые сети Интернета превращаются в единую систему, взаимодействие в которой требует выработки новых подходов и правил.

## Ключевые слова:

спутник, орбита, частотный диапазон, связь, телевидение, сеть, сопряжение, Интернет, смартфон.



Ландшафт рынка услуг спутниковой связи за последнее время изменился до неузнаваемости. Когда-то связной спутник был всего лишь ретранслятором, он так и назывался «спутник-ретранслятор», и вся его задача, по сути, заключалась в том, чтобы взять исходный сигнал из одной точки поверхности Земли, где стояла наземная передающая станция, принять на частоте приёма, усилить, переместить на частоту передачи и сбросить этот же самый сигнал в зону обслуживания спутника, где была расположена одна или несколько приёмных станций. Вся прелесть спутника, работающего с аналоговыми сигналами, заключалась в размерах этой самой зоны обслуживания, которая у спутника, расположенного, к примеру, на геостационарной орбите (ГСО), огромна – площадь поверхности Земли, которую спутник «видит» с расстояния в 36 тысяч километров, составляет сотни и тысячи квадратных километров (рисунок 1).

По сути, установив один спутник в нужную орбитальную позицию, небольшое государство могло решить вопрос подъёма из любой точки и доставки сигнала в любую точку на своей территории. Во всей видимой со спутника зоне можно было располагать как передающие станции (сеть передающих станций), так и приёмные (сеть приёмных станций), которые могли работать с различными частотами и типами сигналов, от узких телефонных каналов до полос частот, в которых передавались широкополосные телевизионные каналы или потоки данных [4]. Такое решение позволяло не тянуть километры проводов по всей стране от пункта к пункту, делало ненужным строительство и поддержание сложной и дорогостоящей системы наземных коммуникаций. Надо сказать, что для покрытия такой огромной по площади страны, как Россия,

имеющей к тому же несколько часовых поясов, даже с ГСО одного спутника было недостаточно, поэтому, например, схема телевизионного вещания (ТВ) всегда строилась на нескольких спутниках-ретрансляторах (рисунок 2, положение спутников на ГСО указано в градусах восточной долготы).

В аналоговую эпоху спутник был элитным и профессиональным решением для государственных и корпоративных потребителей. Частный гражданин прямого доступа к нему практически не имел, диаметр приёмных и передающих антенн доходил до десятков метров. Ни разместить у себя в хозяйстве, ни унести такую махину с собой у него не было никакой возможности. Исключение составляли терминалы подвижной связи, например, международной системы подвижной спутниковой связи Inmarsat<sup>1</sup>, работающие в других диапазонах частот, но поскольку количество каналов связи в них было сильно ограничено, то стоимость такой связи, как и оборудование для неё, для рядового потребителя долгое время также оставались недоступными, ими оснащались преимущественно крупные объекты (корабли, буровые платформы и т.п.).

Нужно сказать, что в технологическом плане особенностью аналоговой жизни различных сетей спутниковой связи являлась их обособленность и разобщённость. Чтобы не мешать друг другу, каждая спутниковая сеть имела свои закреплённые диапазоны частот и работать могла

<sup>1</sup>Inmarsat – американская компания, созданная в 1979 году и оказывающая услуги глобальной подвижной связи морским, авиационным и другим потребителям по всему миру. <https://www.inmarsat.com/en/index.html>

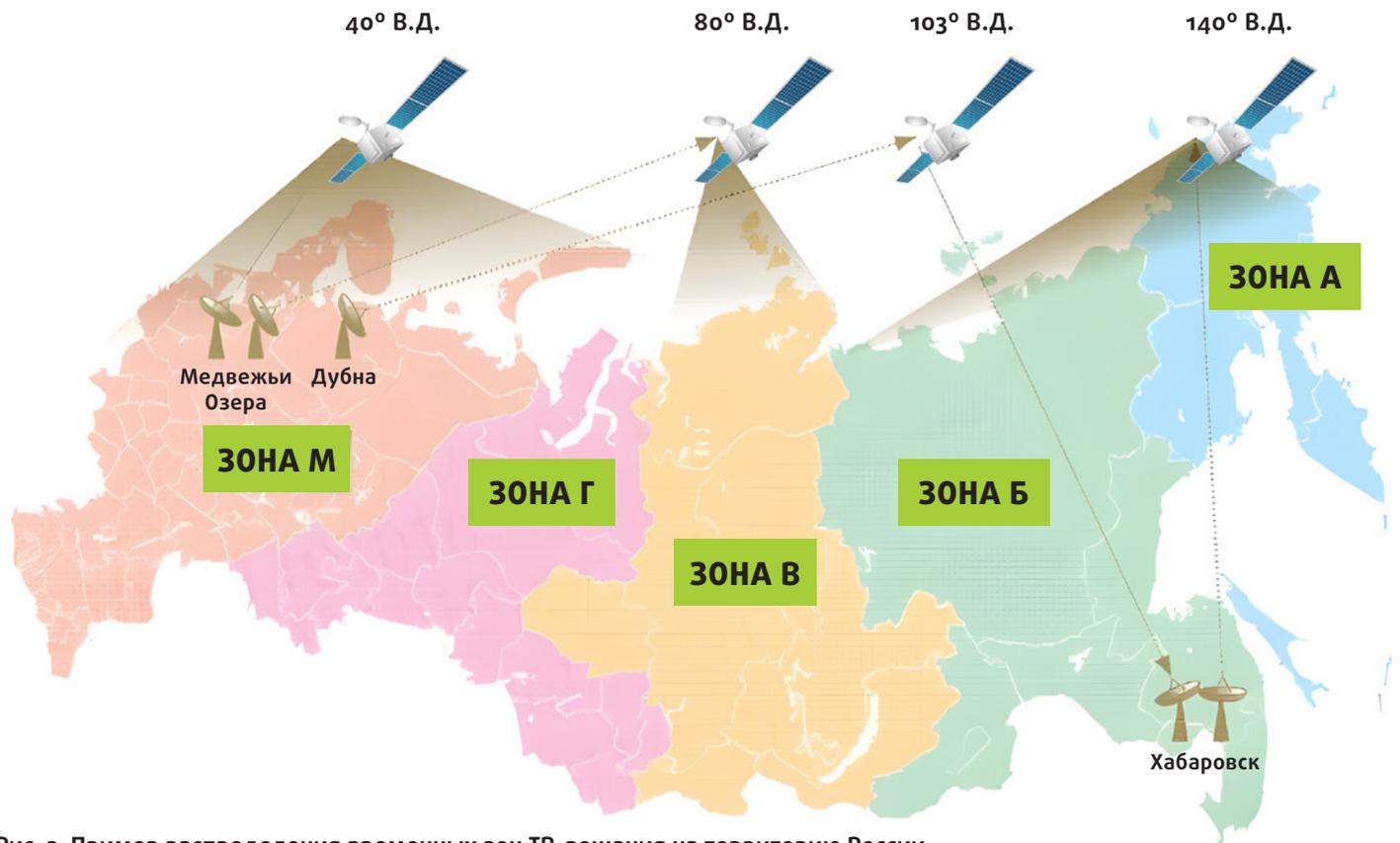


Рис. 2. Пример распределения временных зон ТВ-вещания на территорию России.

только в них! Физическая природа распространения радиосигналов диктует свои жёсткие условия, и на этом уровне ничего не меняется и измениться не может. Порядком в этом «мире беспроводных технологий» заведует Международный союз электросвязи (МСЭ<sup>2</sup>), регламенты которого определяют распределение радиочастотного спектра для всех видов сетей связи: спутниковых и наземных, стационарных (фиксированных) и подвижных. Революцию произвела именно «цифра», а динамику процесса задали активно развивающаяся сеть Интернет. Именно они изменили и экономику отрасли спутниковой связи, и принципы взаимодействия различных сетей.

Первое, к чему привёл переход на цифровые технологии передачи сигналов, – это возможность более эффективного использования радиочастотного спектра. Это очень дорогой ресурс, поскольку его объёмы ограничены немолыми законами физики. Если МСЭ определил для работы вашей сети соответствующую полосу частот, то выйти за её пределы вы уже не можете, но «выжимать» в её пределах всё больше и больше мегабит передаваемой информации, используя всевозможные цифровые усовершенствования типа методов помехозащищённого кодирования и новых методов цифровой обработки, можно сколько вашей душе угодно!

Первый шок от перехода на цифровые технологии испытало спутниковое телевидение в 2000-х годах, когда в стандартной полосе спутникового телевизионного транспондера 36 МГц С-диапазона вместо одной аналоговой телевизионной программы стало возможно передать цифровой телевизионный пакет из шести-восьми программ стандартного качества. Сначала спутниковые операторы приуныли – где взять столько новых программ? Казалось, что в новых цифровых реалиях спутники будут просто стоять пустыми. Однако два момента сыграли колоссальную роль: а) цена вещания одной программы упала в те же шесть-восемь раз и б) появление цифровых технологий создания и обработки телевизионного контента удешевили и подстегнули его рост. В итоге, как грибы после дождя, начали появляться новые региональные и коммерческие программы, плавно заполнившие всю высвободившуюся спутниковую ёмкость [2]. Параллельно шли процессы уплотнения каналов телефонной связи и передачи данных. Ну а появление Интернета и активное развитие его сетей и вовсе привели к тому, что ёмкости на спутниках связи стало катастрофически не хватать, особенно в период 2000-х годов. Сети спутниковой связи всегда обладали неоспоримыми преимуществами перед наземными сетями: быстротой развёртывания и возможностью организации каналов связи практически в любой точке Земли, где может отсутствовать любая другая инфраструктура. При высоком спросе на услугу (а Интернет стал тем воздухом, без которого сегодня не может дышать ни одно предприятие или индивидуум) и готовности за неё платить спутник очень быстро закрывал эту потребность. Для распространения потоков Интернета в основном применялись две схемы: «точка-точка» (для

<sup>2</sup>Международный союз электросвязи (International Telecom Union, ITU) – организация, регулирующая вопросы международного использования радиочастот. <https://www.itu.int/en/Pages/default.aspx>

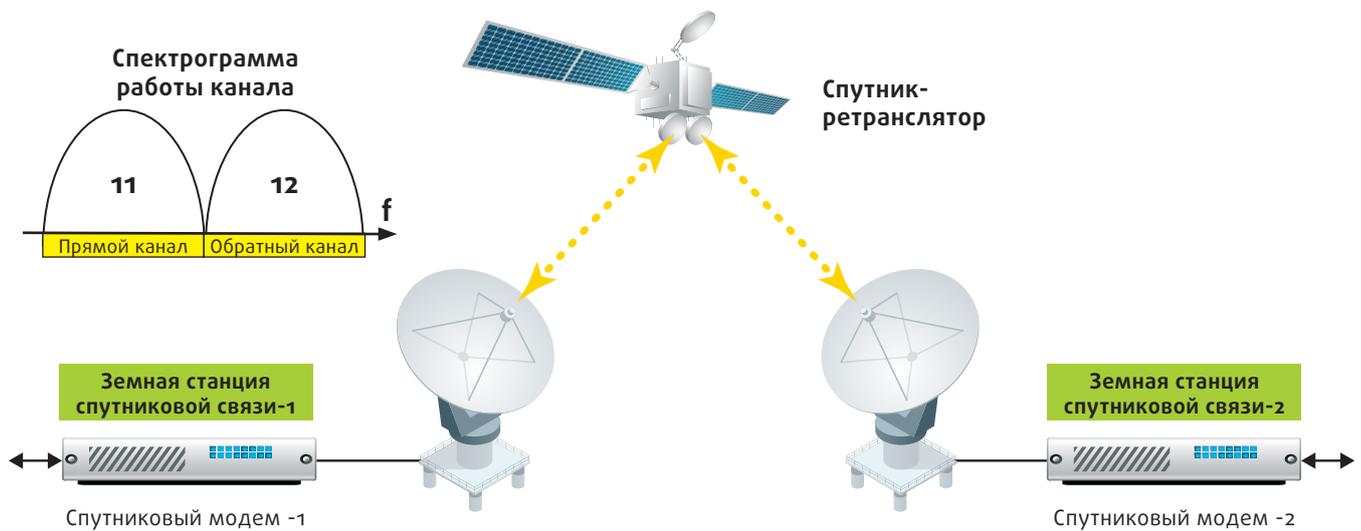


Рис. 3. Пример спутниковой сети связи «точка-точка».

широких магистральных каналов с большими потоками данных в населённые пункты и регионы, см. рисунок 3) и «точка-многоточка» (для организации менее скоростных каналов Интернета корпоративным и частным потребителям, см. рисунок 4).

В этот период базовым решением организации каналов Интернета для средних потребителей стало создание сетей VSAT (Very Small Aperture Terminal) с антеннами диаметром менее 2,5 м [3]. Наиболее ходовую антенну размером 1,2 м мог себе позволить установить владелец небольшого коттеджа и организовать себе прямой канал

связи с доступом в Интернет даже в глухой деревне. Такие сети получили достаточно широкое развитие в Северной Америке (примером могут являться сети известной компании Хьюз<sup>3</sup>, набравших сотни тысяч потребителей), но не в России, где гораздо ниже доходы населения и, одновременно, ниже затраты на мобильную связь, из-за

<sup>3</sup>Hughes – один из крупнейших в США провайдеров спутникового Интернета, предлагающий широкий спектр услуг государственным и частным потребителям как в США, так и за пределами Америки на базе геостационарной спутниковой системы и спутников Jupiter (Юпитер), <https://www.hughes.com/resources/press-releases>

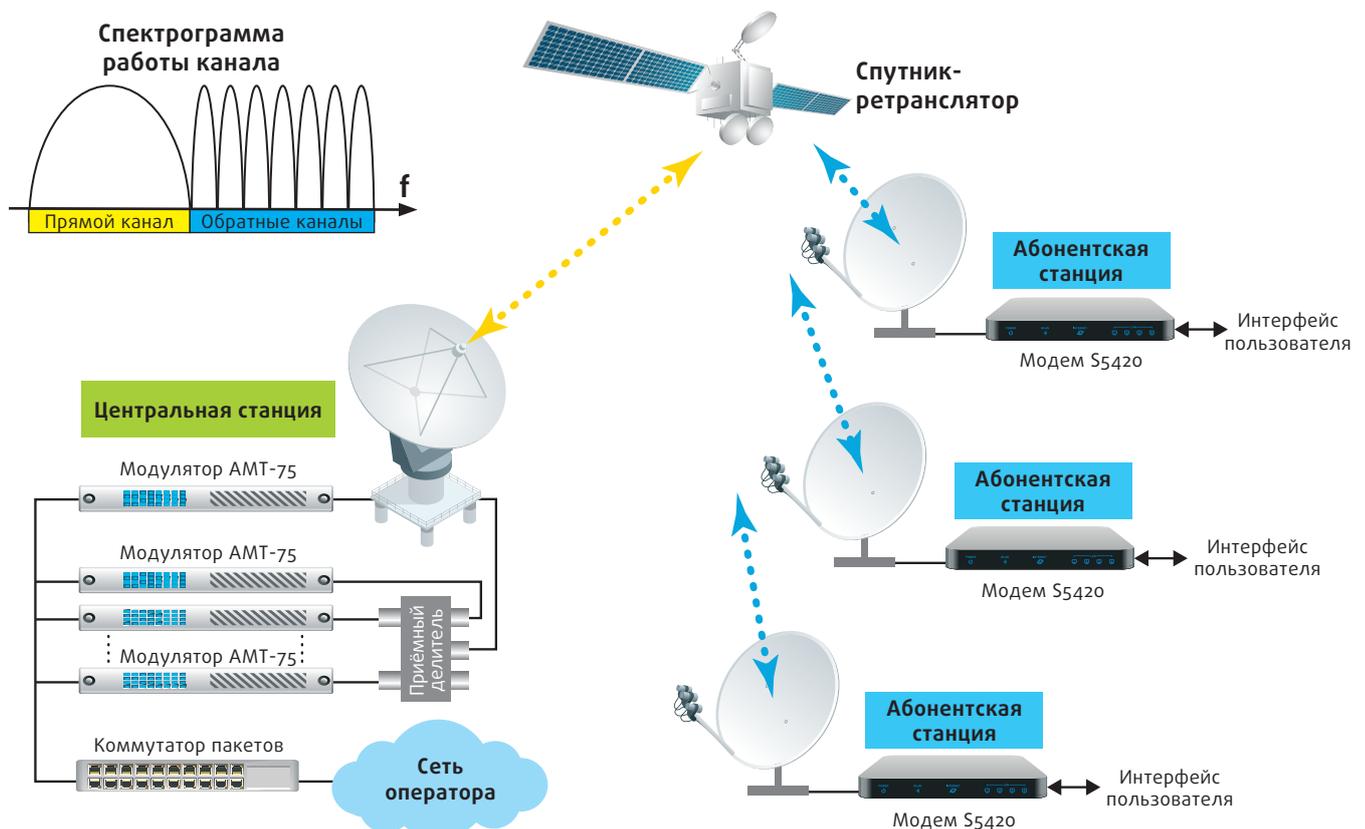


Рис. 4. Пример спутниковой сети связи «точка-многоточка».

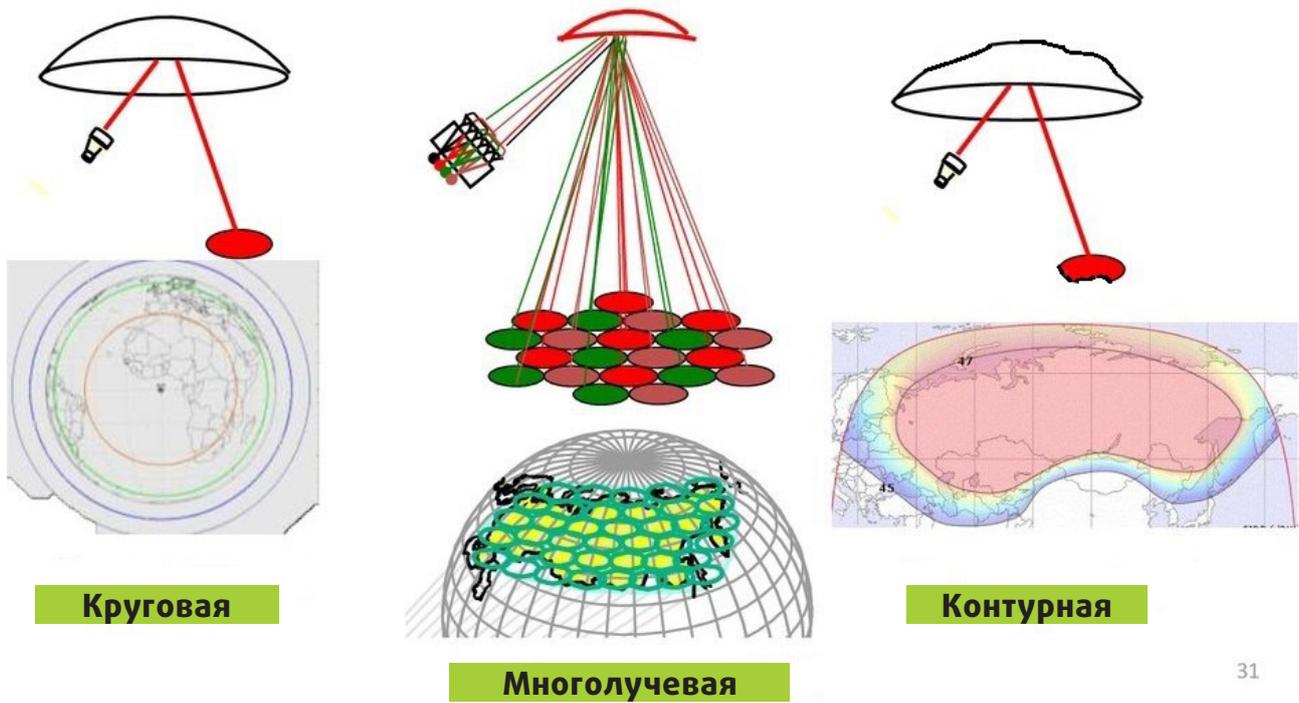


Рис. 5. Примеры различных зон обслуживания геостационарного спутника ФСС.

чего данный сегмент не достиг даже 100 тысяч работающих терминалов. В ещё более бедных странах такую связь могли себе позволить только компании, но не обычные жители.

Кроме того, как только в населённые пункты приходило оптоволокну и мобильные сети, спутниковые сети на технологиях VSAT конкуренции не выдерживали. Пропускная способность геостационарных спутников ограничивалась единицами Гбит/с, а организуемые через них каналы сотнями (магистральные) и десятками (корпоративные и частные) Мбит/с, тогда как по оптоволокну потоки Интернета были на несколько порядков больше. В итоге спутниковые операторы теряли клиентов, снимали оборудование и уходили из мест, которым они зачастую сами дали путёвку в жизнь и стимулировали активное развитие.

Такая конкуренция заставляла спутниковых операторов и изготовителей спутников связи искать пути снижения затрат на создание своих систем и, одновременно, придумывать новые технологии увеличения пропускной способности спутникового и наземного сегментов. Если сформулировать кратко, то цель этих поисков сводилась к одному: максимально приблизить цену Мбит/с в спутниковой сети к цене такого же Мбит/с в наземной сети (в беспроводной, а в идеале, и в проводной). При этом преимущество спутниковой сети в возможности дать услугу клиенту в любом месте практически мгновенно никуда не исчезает. Цель настолько же амбициозна, насколько и сложна.

Масштабную попытку удешевить спутниковый Интернет предприняла американская компания Viasat<sup>4</sup>, запустив

проект создания нескольких геостационарных спутников сверхвысокой пропускной способности (VHTS – Very High Throughput Satellite). В этом проекте пропускная способность каждого спутника составляет несколько сотен Гбит/с (к примеру, Viasat-2 имеет параметр в 300 Гбит/с) и уже подбирается к одному терабиту на спутник (космический аппарат ультрапропускной способности UHTS Viasat-3). Добиться этого позволило применение новой технологии многократного переиспользования спектра. Если прежние геостационарные спутники фиксированных спутниковых служб (ФСС) для обслуживания широкой сервисной зоны (круговой или контурной) использовали скоординированные для них МСЭ полосы частот однократно (чаще всего в С-, Ku- и Ka-диапазонах), в лучшем случае используя две поляризации для увеличения пропускной способности спутника, то в новых спутниках HTS и VHTS (UHTS) зона обслуживания стала формироваться из большого числа узких круговых или эллиптических зон, формируемых узкими направленными лучами, полосы частот которых многократно повторяются. Отличие в том, что повторяющиеся полосы частот располагаются не рядом, а чередуются через другие лучи с другими частотами, чтобы избежать ненужной интерференции, так как для обеспечения сплошного покрытия эти лучи краями пересекаются друг с другом (рисунок 5, пример многолучевой зоны в центре, чередование полос частот в лучах выделено цветом).

Однако помимо преимуществ в скорости развёртывания и грандиозных размерах зон обслуживания, спутниковые геостационарные сети имеют и свои недостатки для Интернета по сравнению с сетями наземными и спутниковыми сетями на более низких орбитах: примерно на порядок (!) большую задержку сигнала (грубо: 500 мс вместо 50 мс, зависит от параметров сетей и оборудования); кроме того, геостационарные спутники располагаются в плоскости экватора и поэтому практически не видны в приполярных областях, а также закрываются высокими объектами

<sup>4</sup>Viasat – также один из крупнейших американских провайдеров спутникового Интернета, обеспечивающего глобальное покрытие Земли, <https://www.viasat.com/>

(здания, лесные массивы, горы – чем дальше от экватора, тем больше «зоны затенения»).

Поэтому конкуренты, стремящиеся охватить услугой спутникового Интернета как можно больше клиентов и при этом дать условия и цены, максимально отвечающие их ожиданиям, которые однозначно формировались сетями наземными (напомним, что при их приходе спутниковым провайдерам приходилось поспешно ретироваться), всерьез занялись освоением низких, негеостационарных орбит (НГСО, рисунок 6), расположенных примерно в 500 км от Земли и выше.

Из наиболее крупных и нашумевших проектов стоит отметить проект O3b (от other three billion, изначально позиционировавшийся как система народного Интернета для неохваченных трёх миллиардов земного населения) компании SES<sup>5</sup>, британский проект OneWeb и уже всем известный Starlink Илона Маска, заявившего, что его спутниковая сеть Интернета соберёт миллиарды доходов, необходимые для реализации гран-

диозного проекта освоения Марса. Все эти проекты, в отличие от реализованных до них спутниковых связанных проектов на НГСО типа Iridium<sup>6</sup>, Globalstar и прочих, использовавших выделенные МСЭ полосы частот для подвижных спутниковых служб (ПСС), которые из-за низких диапазонов частот позволяли передавать потоки интернета менее 1-2 Мбит/с (а значит, не могли претендовать на сколько-нибудь серьёзную клиентскую базу Интернета), дерзко и нередко презирая установленные МСЭ правила, устремились в диапазоны частот так называемых фиксированных спутниковых служб (ФСС), а также наземных подвижных служб (ПС), которые позволяют организовывать потоки Интернета на пользовательское устройство в десятки и даже сотни Мбит/с.

Если не вдаваться глубоко в подробности архитектуры построения различных спутниковых сетей Интернета, то, по сути, смысл всех этих сетей заключается в организации систем, соединяющих потоки Интернета из наземных сетей (наземной сети общего пользования) через так на-

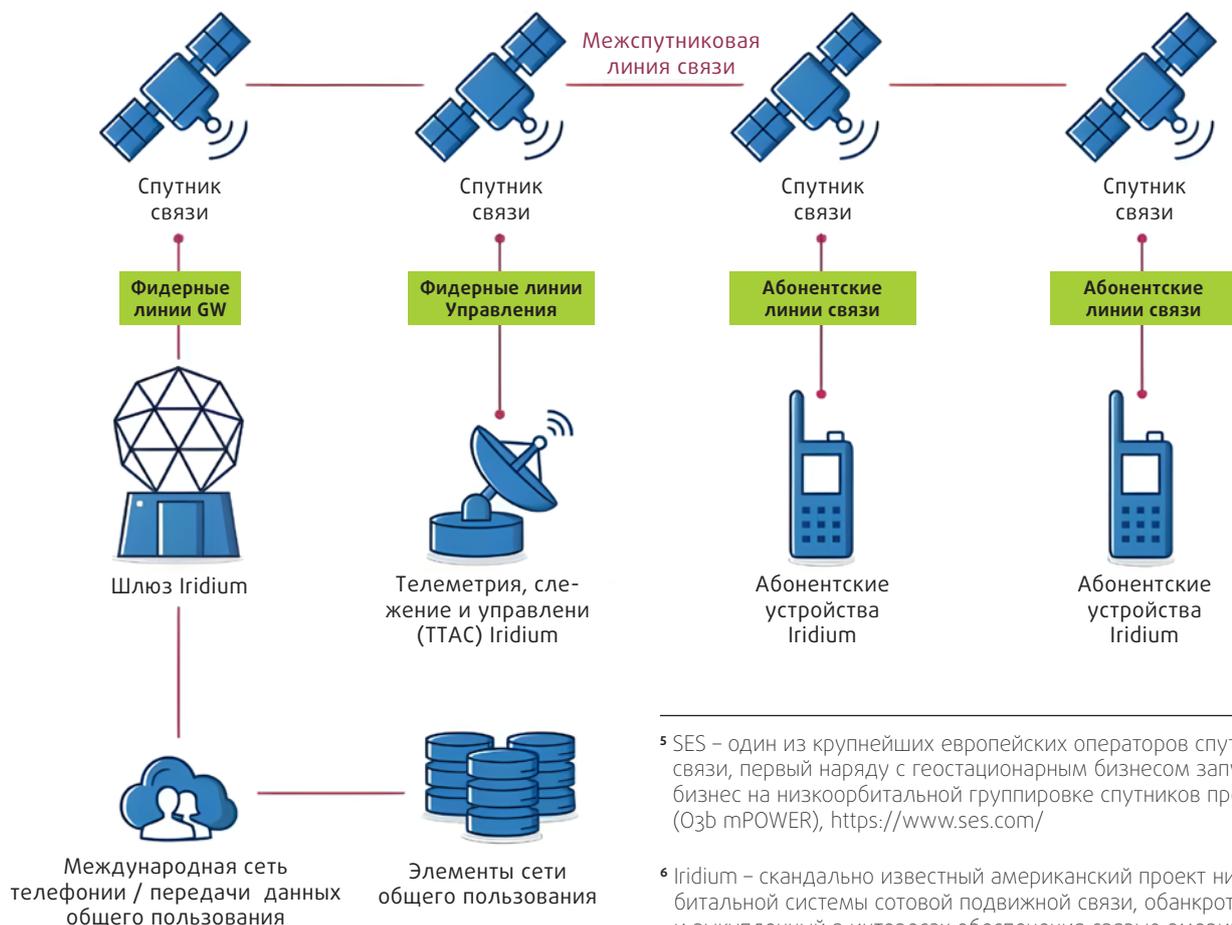
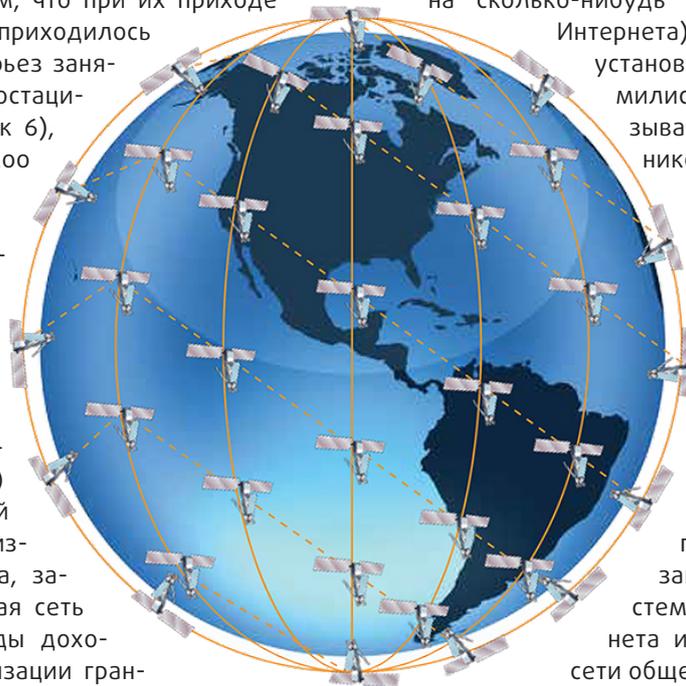


Рис. 6. Пример построения спутниковой системы на НГСО (система Iridium).

<sup>5</sup> SES – один из крупнейших европейских операторов спутниковой связи, первый наряду с геостационарным бизнесом запустивший бизнес на низкоорбитальной группировке спутников проекта O3b (O3b mPOWER), <https://www.ses.com/>

<sup>6</sup> Iridium – скандально известный американский проект низкоорбитальной системы сотовой подвижной связи, обанкротившийся и выкупленный в интересах обеспечения связью американских военных, сегодня помимо интересов правительства США обслуживает и коммерческих потребителей в других странах, <https://www.iridium.com/>

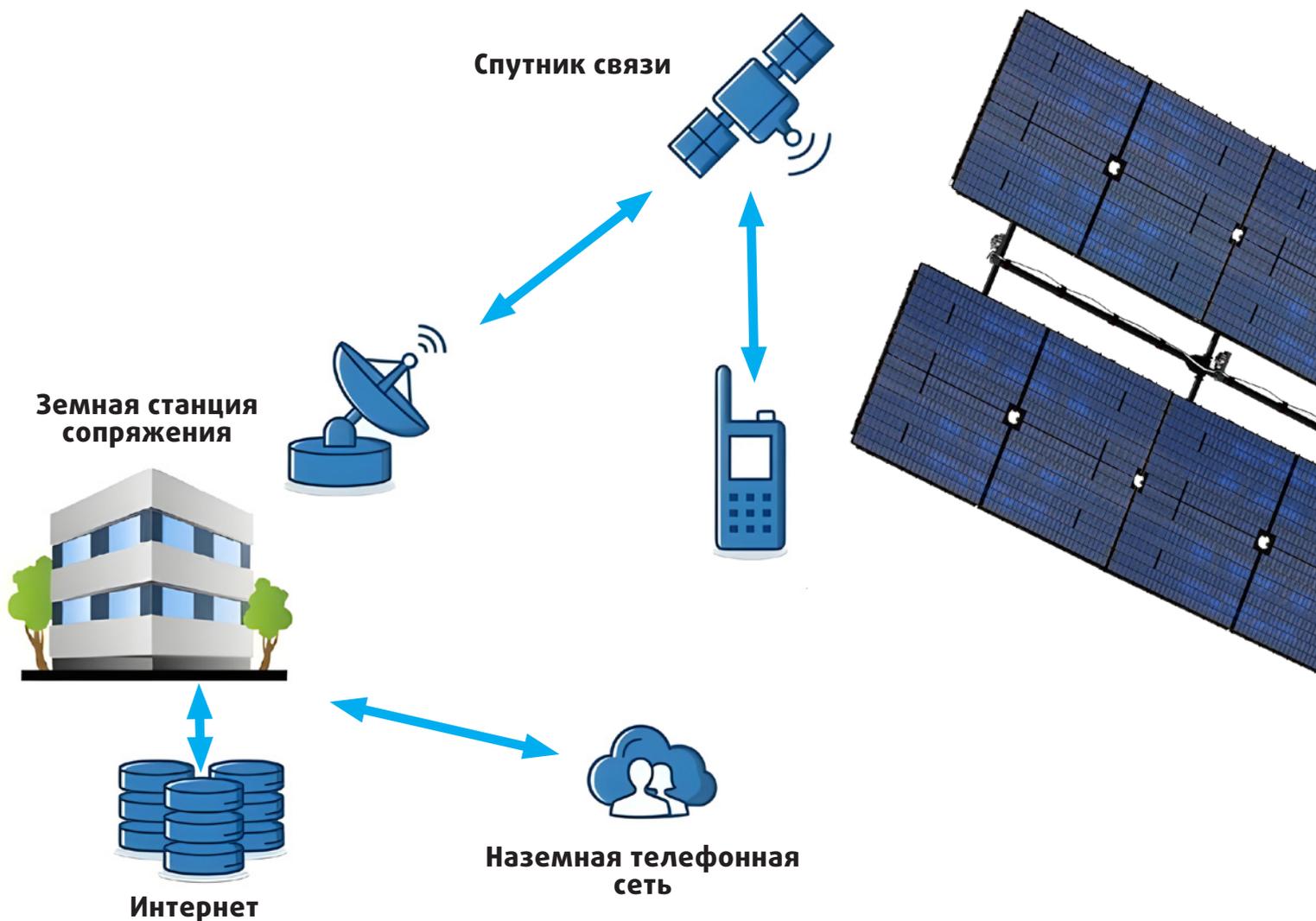


Рис. 7. Объединение наземных и спутниковых сетей через станции сопряжения.

зываемые станции сопряжения (рисунок 7) со спутниковыми сетями, распределяющими эти потоки до клиентов и обратно, формируя тем самым взаимоувязанную глобальную сеть приёма-передачи данных Интернета.

Таким образом, мы имеем то, что различные спутниковые сети работают в разных диапазонах, позволяют передавать потоки Интернета различной скорости на различные пользовательские устройства (спутниковые терминалы, телефоны и т.д.) вплоть до перехода к прямой работе с устройствами клиентов (смартфонами), изначально созданными для работы в наземных мобильных сетях. Активно развивающееся в настоящее время создание спутников и систем для организации прямой спутниковой связи со смартфонами для услуги D2D (direct to device) или D2C (direct to cell), по сути, замыкает круг взаимосвязи наземных и спутниковых сетей Интернета [4]. В МСЭ давно идут и ещё предстоят новые серьезные баталии по поводу установления правил пользования частотами между новыми спутниковыми и наземными сетями, однако, похоже, что альтернативы такому объединению нет, с точки зрения технологий круг уже замкнулся, всё что осталось – это разложить по полочкам правила доступа и пользования соответствующими частотами. Пока сервисы D2D обладают скромными скоростями линий связи

для передачи SMS и голоса, но уже появились проекты, обещающие реализовать прямую передачу данных на смартфоны со скоростями до 35 Мбит/с (например, стартап компании AST SpaceMobile) [5].

Интересно, что такое объединение сетей различной природы и назначения во многом стало возможно именно из-за того, что Интернет как технология послужил не только средством распространения информации в цифровых сетях, но и средой и средством управления этими сетями, что позволяет создавать различные стандарты и алгоритмы их взаимодействия между собой. Процессы объединения различных спутниковых сетей продолжают на самых разных уровнях, при этом каждая технология занимает своё место в зависимости от своей эффективности и востребованности.

Подводя итог, можно сказать, что спутниковые сети Интернета как часть единой мировой сети постепенно из огромных геостационарных «неводов для крупной рыбы» (государственных и корпоративных клиентов) превратились во множество плотно расставленных сетей различной конфигурации и возможностей, стремящихся постепенно охватить всех, даже самых скромных по размерам кошелька потребителей.



### Список литературы:

- [1] <https://bigenc.ru/c/sputnikovoe-televizionnoe-veshchanie-zoc6e3>
- [2] <https://web.archive.org/web/20210419162526/https://moris.rtrs.ru/prof/live-broadcasting/broadcasting/>
- [3] <https://ru.wikipedia.org/wiki/VSAT>
- [4] <https://habr.com/ru/companies/ruvds/articles/804127/>
- [5] <https://www.ixbt.com/news/2024/08/06/ast-spacemobile-poluchila-zelenyj-svet-dlja-zapuska-pervyh-pjati-sputnikov-dlja-prjamoj-svjazi-so-smartfonami.html?ysclid=m8e0sb7i5w224298618>

### Об авторе

Владимир Леонидович Глебский, директор отдела развития региональных проектов Международной организации космической связи «Интерспутник».

# Многофакторный анализ функционирования системы спутниковой связи Starlink. Что в ней хорошего, плохого и «злого»?

Найтиндер Мохан



## Аннотация:

Что представляет собой система связи Starlink по сравнению с наземными интернет-провайдерами? Какие именно факторы влияют на её работу? В рамках нового многофакторного исследования как активных, так и пассивных измерений автор постарался пролить свет на эффективность системы Starlink по принципу «хороший, плохой, злой», то есть выявить её преимущества, недостатки и факторы риска.

## Ключевые слова:

Atlasresearch, конкуренция, измерения, интернет-инфраструктура.

Ничего нового в использовании орбитальных спутников для связи нет. Первые такие спутники стали запускать в космос ещё в конце 1950-х годов, а сама идея их применения появилась лет за десять до этого. Однако за последние пять лет в этой отрасли произошли поистине революционные перемены после того, как специализирующаяся на производстве и запуске космических аппаратов компания SpaceX объявила о своих планах по запуску и эксплуатации системы спутниковой интернет-связи Starlink.

По состоянию на сегодняшний день система Starlink представляет крупнейшую группировку из более чем шести тысяч спутников. При этом планируется вывести на орбиту ещё столько же. Уже сам размер этой группировки дал оператору Starlink возможность обеспечить глобальное высокоскоростное покрытие.

Таким образом, за счёт глобального покрытия и высокой пропускной способности подключения Starlink стала первой системой связи, способной серьёзно конкурировать с аналогичными наземными сетями. Более того, с помощью своих спутников Starlink охватывает всю планету, что даёт ей возможность обеспечивать связь даже в самых отдалённых уголках планеты и выступать в качестве поистине «глобального» интернет-провайдера.

Чтобы понять, как работает система Starlink в глобальном масштабе, а также какие факторы определяют её функционирование, было проведено детальное многофакторное исследование с задействованием как активных, так и пассивных измерений. Результаты опубликованы в материалах Ассоциации по вычислительной технике по итогам интернет-конференции 2024 года (Proceedings of the ACM on Web Conference 2024).

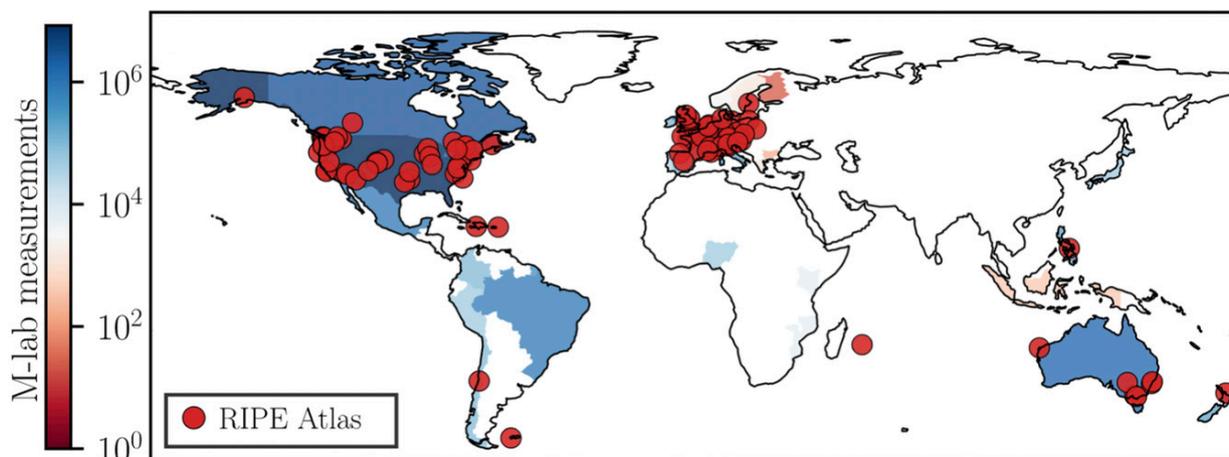


Рис. 1. Обзорная диаграмма измерений системы Starlink по методикам систем тестирования и измерения M-Lab и RIPE Atlas.

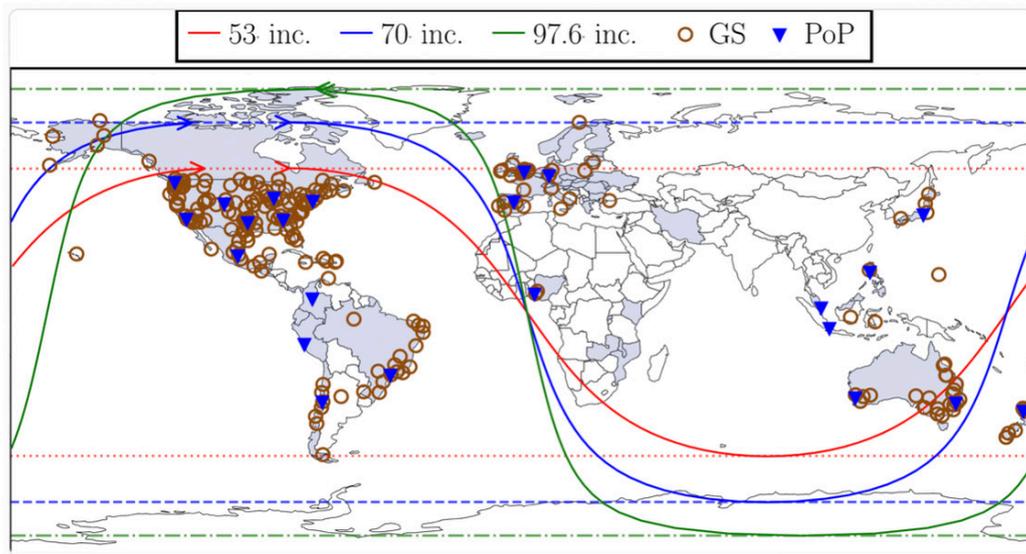


Рис. 2. Орбиты спутников Starlink с учётом угла наклона по отношению к наземным станциям – шлюзам и точкам присутствия.

В данной статье приводятся основные выводы по итогам проведённых измерений при выполнении следующих задач: (i) оценка функционирования в глобальном масштабе по системам M-Lab и RIPE Atlas (получено почти 20 миллионов измерений из 34 стран – см. рис. 1), (ii) оценка качества использования Zoom и облачных игровых сервисов и (iii) изучение внутреннего функционирования сети Starlink с использованием измерений и контрольных показателей.

## Функционирование системы связи Starlink: первый взгляд

Спутники Starlink вращаются вокруг Земли в орбитальных группировках разного наклона по отношению к экватору. Большинство из ныне действующих четырёх тысяч спутников Starlink имеют наклон орбиты в 53 градуса, что обеспечивает покрытие лишь части земного шара (см. рис. 2), тогда как спутники, двигающиеся по орбите с наклоном в 70 и 97,6 градуса, позволяют охватить приполярные территории. Однако в этих орбитальных группировках спутников меньше.

Помимо спутниковой группировки, функционирование сети Starlink обеспечивается целым рядом важных наземных компонентов. На рис. 3 показаны основные элементы системы. Конечные пользователи выходят в Интернет с помощью абонентских терминалов, называемых «тарелочками» (Dish; примечание редакции: полное название терминалов Starlink – Dishy McFlatface, используется игра слов: dish – «тарелка» и dishy – «шикарный»). Эти устройства взаимодействуют со спутниками в зоне видимости под углом более 25 градусов с использованием фазированных антенн Ku-диапазона. Спутники, в свою очередь, взаимодействуют с наземными станциями в Ka-диапазоне. Такие шлюзы подсоединяются по частной сети к точке присутствия, что и обеспечивает подключение к Интернету.

Система связи по схеме «тарелка – спутник – шлюз» формирует архитектуру ретрансляции, в рамках которой и абонентский терминал, и шлюз находятся в пределах зоны покрытия спутника (около 1 тысячи км), что и обеспечивает ретрансля-

цию сигнала. На рис. 2 приведена карта размещения наземных шлюзов Starlink и точек присутствия. Получается, что ретрансляция сигнала в некоторых случаях невозможна, особенно в отдалённых районах Африки и Южной Америки. Для решения этой проблемы в новейшее поколение спутников Starlink добавлены системы лазерной связи для обеспечения межспутниковых коммуникаций – получается расширенная ретрансляционная сеть, которая даёт возможность абонентам подключаться к Интернету через наземные станции, расположенные вне зоны покрытия ближайшего спутника.

## Хорошее

Один из основных выводов проведённого исследования заключается в том, что Starlink в глобальном масштабе способен составить конкуренцию операторам наземной интернет-связи. В ряде регионов, в особенности в США, Starlink находится примерно на одном уровне с операторами наземных интернет-сетей с точки зрения качества оказываемых услуг. За пределами США результаты по Starlink, как правило, немного уступают существующим наземным интернет-провайдерам, однако в большинстве случаев разница между ними незначительна, причём качество связи для абонентов Starlink обычно вполне удовлетворительно.

При рассмотрении использования конкретных приложений установлено, что система Starlink вполне конкурентоспособна по сравнению с наземными оптоволоконными сетями и операторами

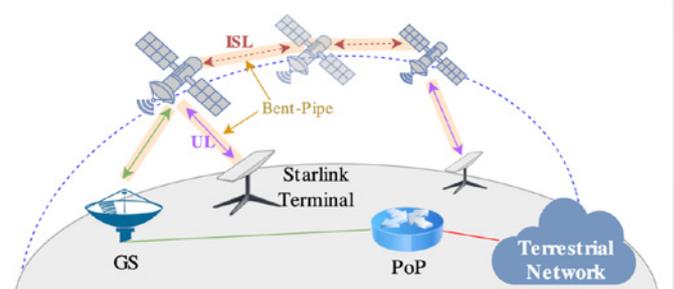
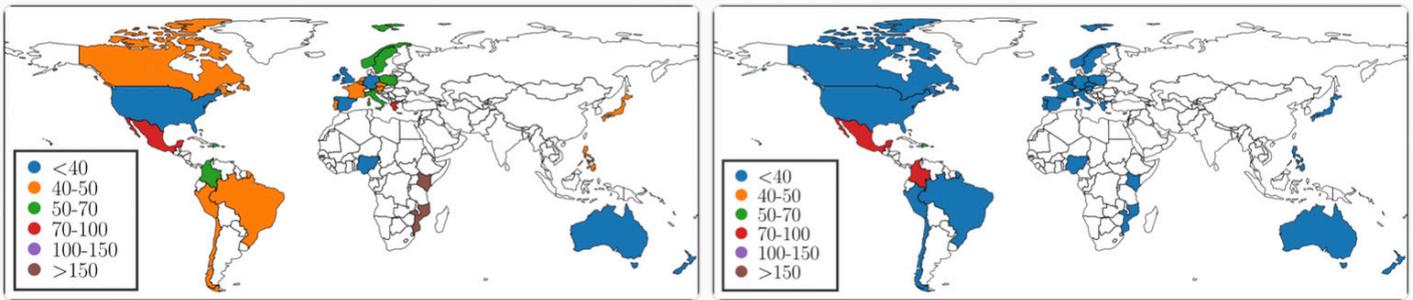


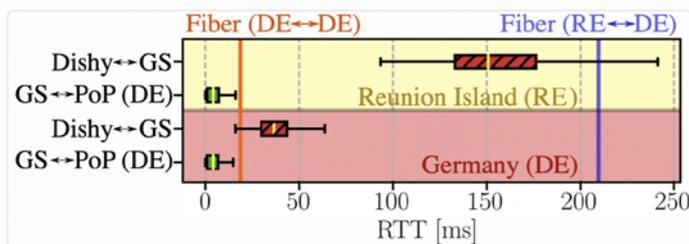
Рис. 3. Для связи с наземными точками присутствия система Starlink задействует режим ретрансляции типа «изогнутая труба».



**Рис. 4.** Медианный показатель минимального времени передачи данных в обоих направлениях по отношению к ближайшему серверу M-Lab в миллисекундах для Starlink (слева) и трёх ведущих и действующих интернет-провайдеров (справа) соответствующей страны.

мобильной интернет-связи в том, что касается работы в режиме реального времени приложений, требующих большой пропускной способности, а именно приложений Zoom для проведения видеоконференций и облачного игрового ресурса Amazon Luna. Оба приложения для нормальной работы требуют низких показателей задержки прохождения сигнала при высокой пропускной способности. Разница лишь в том, что работа облачных игровых ресурсов определяется временем кругового обращения сигнала и работой нисходящего канала связи, тогда как при проведении видеоконференций большое значение, помимо нисходящего канала связи, приобретает и исходящая скорость. В ходе проведённого исследования установлено, что наземные системы связи (оптоволоконные и мобильные сети) и система Starlink обладают примерно одинаковыми показателями эффективности, причём в том, что касается облачных игровых ресурсов, Starlink опередила мобильные сети пятого поколения.

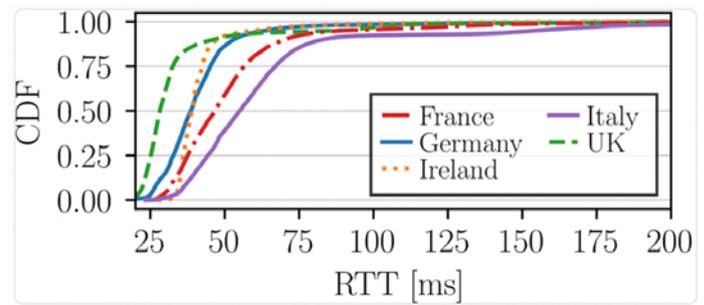
Исследователи сконцентрировались на изучении работы системы в отдельно взятом географическом регионе и взяли в качестве примера остров Реюньон в Индийском океане. Остров связан с наземными системами связи двумя подводными кабелями, с помощью которых интернет-трафик направляется либо в Азию, либо в Южную Америку. У системы Starlink наземной инфраструктуры на о. Реюньон нет. Тем не менее, показатели круговой задержки для абонентов Starlink оказались ниже, чем у наземных интернет-провайдеров, что объясняется наличием у Starlink возможности доставить интернет-трафик средствами межспутниковой связи до соответствующей точки присутствия в Германии на расстоянии около 9 тысяч километров. Эти замеры доказали способность системы Starlink обеспечивать связь с отдалёнными регионами, причём качество такой связи выше, чем у аналогичных услуг операторов наземной связи.



**Рис. 5.** Сравнение скорости ретрансляции для острова Реюньон (жёлтый сегмент) и Германии (красный сегмент) при подсоединении к одной и той же точке присутствия в Германии. Более высокие показатели по задержке для о. Реюньон от терминала до наземной станции объясняются спецификой работы межспутниковой связи. При передаче сигнала в Германию задержка ниже по сравнению с наземной сетью (синяя вертикальная линия).

## Плохое

Помимо таких обнадеживающих результатов, в рамках проведённого исследования также установлено, что абоненты Starlink могут сталкиваться с существенным снижением качества обслуживания в определённых регионах.



**Рис. 6.** Показатели минимального времени прохождения сигнала в обоих направлениях по версии M-Lab с использованием системы Starlink из ряда европейских городов.

Взяв за основу работу системы в Европе, авторы обнаружили, что в Дублине, Лондоне и Берлине время задержки сопоставимо с показателями США, тогда как для Рима и Парижа показатели оказались хуже. Возможно, разница обусловлена различиями между конкретными городами в том, что касается плотности размещения наземной инфраструктуры Starlink, то есть точек присутствия – они выполняют функцию шлюзов между локальным трафиком Starlink и Интернетом. Подтверждение обоснованности такой гипотезы получено по результатам проведения долгосрочного исследования работы системы на Филиппинах, где удалось проследить, как установка новой точки присутствия в мае 2023 года сказалась на быстродействии системы (см. рис. 7). До размещения точки присутствия в стране абоненты на Филиппинах сталкивались с высоким временем задержки. Дело в том, что в рамках системы Starlink трафик поступал на размещённую на Филиппинах наземную станцию, но оттуда перенаправлялся на ближайшую точку присутствия в Японии посредством подводного кабеля, а затем отправлялся обратно на Филиппины на местный сервер. Благодаря созданию точки присутствия на Филиппинах от этой нерациональной системы маршрутизации можно было отказаться, значительно упростив схему передачи сигнала, что привело к значительному улучшению показателей задержки.

Как отмечалось выше, компания SpaceX считает своим приоритетом обеспечение стабильной работы системы в глобаль-

ном масштабе. Однако в рамках проведённого исследования установлено, что такие системы внеземной связи, как Starlink, не могут служить универсальным решением, избавляющим интернет-провайдеров от необходимости вкладывать значительные суммы в развитие наземной инфраструктуры. Без таких инвестиций всё равно не обойтись, хотя Starlink и позволяет тратить на эти цели меньше средств, чтобы вкуче с внеземными сетями обеспечивать приемлемую и стабильную связь. Кроме того, внеземная инфраструктура, то есть спутники, тоже требует определенных вложений. Помимо этого, в полярных широтах качество связи снижается, поскольку спутников, обслуживающих абонентов в таких регионах, меньше.

## «Злое»

Конечно, описанные ранее в статье проблемы со скоростью работы системы Starlink можно если не полностью преодолеть, то хотя бы смягчить за счёт инвестиций в наземную и космическую инфраструктуру. Однако в ходе исследования также установлен заложенный в систему планирования Starlink фактор, из-за которого могут происходить серьёзные колебания с точки зрения качества связи. Соответственно, речь идёт о глубинном факторе, затрагивающем специфику построения самой сети. В работу системы планирования заложены 15-секундные интервалы реконфигурации, позволяющие обновить и изменить параметры подключения каждого пользователя.

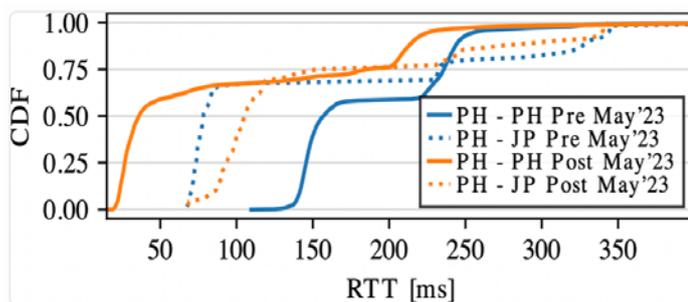


Рис. 7. Медианный показатель минимального времени прохождения сигнала в обоих направлениях при проведении замеров в Маниле по отношению к серверам M-Lab на Филиппинах и в Японии до и после установки точки присутствия на Филиппинах.

По итогам проведённых тонких измерений установлено, что такие интервалы реконфигурации оказывают явное воздействие на работу системы, в особенности на стыках между такими интервалами. В такие моменты наблюдалось существенное изменение показателей задержки в обе стороны, а также существенное, хоть и краткосрочное снижение доступной пропускной способности. Среди специалистов установилась точка зрения, что такие фиксированные 15-секундные интервалы используются системой Starlink при смене спутников, что и является основной причиной снижения качества связи. Однако в

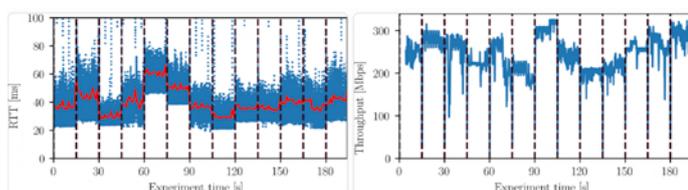


Рис. 8. Периодические 15-секундные колебания времени задержки и пропускной способности системы Starlink, что свидетельствует о реконфигурации сети.

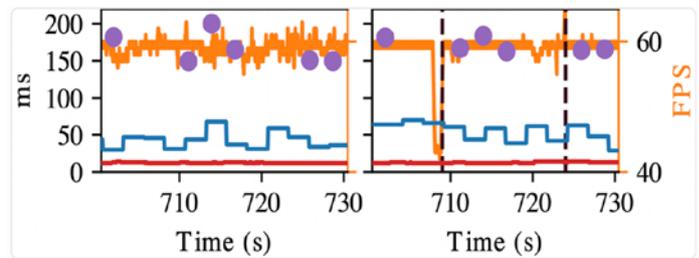


Рис. 9. Использование облачных игровых ресурсов в сетях пятого поколения (слева) и в сети Starlink (справа). Вертикальные пунктирные линии обозначают 15-секундные интервалы реконфигурации.

рамках проведённых специализированных экспериментов, при которых было сделано так, чтобы терминал Starlink подключался исключительно к спутникам с наклоном орбиты в 72 и 97,6 градуса, выявлены такие же колебания качества связи на стыках интервалов реконфигурации даже тогда, когда терминал оставался подключённым к одному и тому же спутнику.

Кроме того, установлено, что такие колебания оказывают существенное воздействие на работу приложений с использованием Starlink. На примере экспериментов с приложениями Zoom и Amazon Luna выявлены соответствующие колебания с точки зрения качества связи. В приложении Zoom наблюдалось колебание односторонней задержки, тогда как в случае с Amazon Luna время от времени наблюдалось снижение кадровой частоты, причём в обоих случаях эти сбои совпадали с началом или завершением интервалов реконфигурации. Самым, возможно, важным выводом стало выявленное изменение количества отправленных пакетов исправления ошибок, причём эти колебания опять же накладывались на стыки между интервалами.

## Заключительные соображения

Решив понять, насколько система Starlink способна конкурировать с операторами наземных систем интернет-связи, мы установили, что Starlink представляет из себя конкурентоспособное и быстро развивающееся решение. Однако внеземные сети нельзя считать универсальным решением, поскольку качество работы сети обеспечивается вложениями в её развитие, причём как спутников, так и наземной инфраструктуры, о чём нередко забывают. Кроме того, выявлена специфика внутрисетевого планирования и управления со стороны SpaceX, объясняющая нестабильность связи. Эту проблему следует устранить как на уровне систем передачи данных, так и на уровне приложений. ■

## Об авторе

Найтиндер Мохан (Nitinder Mohan), Делфт, Нидерланды  
Найтиндер Мохан занимает должность доцента факультета вычислительной техники Делфтского университета технологий в Нидерландах. До этого он работал старшим научным сотрудником Мюнхенского технического университета в Германии. В сферу его научных интересов входят периферийные вычисления, сетевые приложения нового поколения и проведение крупномасштабных измерительных исследований Интернета. Имеет степень Ph.D. Хельсинского университета, Финляндия. Обладатель премии «Выдающаяся диссертация 2020» Технического комитета по масштабируемым вычислениям Инженерного института электротехники и электроники (IEEE TCSC).

# Связность и идентификаторы Интернета

Павел Храмцов



## Аннотация

У компании Sun Microsystems (поглощена компанией Oracle в 2010 году) был слоган: «The Network is the Computer». Это показывает, насколько многогранно понятие «Сеть» («Network»). Мы как раз и будем рассматривать термин «Сеть» («Network») в контексте сети Интернет, т.е. сети TCP/IP. В статье мы введём понятие связности. Опираясь на модель стека TCP/IP, рассмотрим «связность» на каждом из четырёх уровней этой модели. Определим, какую роль играют идентификаторы на каждом из этих уровней. Обнаружим, что никакой статической связности в Интернете нет. Она, возможно, была в DARPA NET или в NSFNET, но в настоящее время связность динамическая – это краеугольный камень построения сетей передачи данных на основе стека протоколов TCP/IP.

## Ключевые слова:

Интернет, стек TCP/IP, графы, модели, протоколы, маршрутизация, приложения, MAC-адрес, связность.

## Общие замечания относительно понятия «связность» и интернет-идентификаторов

Довольно часто слово «связность» отождествляют с английской калькой термина «connectivity» – «коннективность». А правильно ли это?

Google переводит слово «connectivity» как «возможность подключения». Искусственный интеллект в лице DeepSeek (куда же без него) даёт более развёрнутое определение, «например, «internet connectivity» означает возможность подключения к Интернету», т.е. речь идёт о возможности установления такой связи.

Для установки связи нужно знать адрес отправителя и адрес получателя. Эти адреса, их отдельные компоненты (части) или дополнительная информация являются идентификаторами, которые определяются в стандартах и используются в протоколах взаимодействия.

**Документ RFC-1122 определяет только четыре уровня протоколов. Структурная модель сети TCP/IP определена в разделе 1.1.3 RFC-1122 и состоит из:**

- протоколов обмена данными уровня приложений (application layer);
- протоколов транспортного уровня (transport layer);
- протоколов сетевого уровня (internet layer);
- протоколов канального уровня (уровень взаимодействия с сетью, или link layer).

Интернет – это сеть сетей, по этой причине возможность установки связи на уровне канала, т.е. «на уровне взаимо-

действия с сетью» не даст ответа на вопрос о возможности установления связи между двумя хостами из разных сетей. Основным идентификатором на уровне канала является MAC-адрес интерфейса.

На уровне протоколов межсетевого обмена (Internet Protocol – IP) идентификаторы этого уровня – это IP-адреса и их агрегаты.

На транспортном уровне в TCP/IP используются два основных протокола – UDP и TCP.

Приложения «привязаны» к так называемым транспортным портам. Общий список портов ведётся в реестре IANA – «Service Name and Transport Protocol Port Number Registry» [4]. Основными идентификаторами в протоколах TCP/UDP являются номера портов.

## Связность в графах

Сеть Интернет (TCP/IP) – это сеть коммутации пакетов. IP-пакет путешествует от одного хоста (узла сети) к другому хосту через систему шлюзов – хостов, которые по определённым правилам передают пакеты из одной локальной сети в другую.

Сами правила передачи и процесс их определения и трансформации называют маршрутизацией. В рамках этих процессов применяют разные протоколы маршрутизации. Например, OSPF (Open Shortest Path First) [6] сетевого уровня или протоколы прикладного уровня типа RIP (Routing Information Protocol) [7], или BGP4 (Border Gateway Protocol 4).

Протоколы маршрутизации опираются на математические модели. Например, в протоколе RIP применяется алгоритм

Форда-Фалкерсона [8] (известен также как алгоритм Белмана-Форда), а в протоколе OSPF применяется алгоритм Дейкстры [9].

Исследования сходимости BGP-таблиц (устойчивое состояние всех таблиц BGP) основано также на графовых моделях с применением различных топологий (иерархическая сеть, кольцо, смешанная сеть) [10]. В теории графов существуют понятия пути и маршрута, и связность, таким образом, – это возможность существования путей и маршрутов в каждый конкретный момент времени.

**Перечисленные модели – это алгоритмы решения задач на графах.**

**Теория графов – область дискретной математики, особенностью которой является геометрический подход к изучению объектов. Основным объектом теории графов – граф и его обобщения [1].**

**Формально граф, согласно этой теории [2], определяют как:**

$G = (V(G), E(G))$ , где

$V(G)$  – множество вершин графа  $G$ ,

а  $E(G)$  – множество рёбер графа  $G$ .

**Нас интересуют связные графы, т.е. графы, в которых между двумя любыми вершинами графа существует хотя бы один «путь».**

**Определим «путь» через «маршрут».**

**Если две вершины  $v_1$  и  $v_2$  связывает дуга  $e_{12}$ , то вершина  $v_1$  и дуга  $e_{12}$  инцидентны. Это же верно и для вершины  $v_2$  и дуги  $e_{12}$ .**

**Маршрут в графе – чередующаяся последовательность вершин и рёбер, в которой любые два соседних элемента инцидентны. Если начальная вершина и конечная вершина последовательности совпадают, то маршрут замкнут, иначе – открыт.**

**Путь – последовательность рёбер (в неориентированном графе) и/или дуг (в ориентированном графе), такая, что конец одной дуги (ребра) является началом другой дуги (ребра).**

## Стек протоколов, идентификаторы и связность

Мы имеем четыре уровня стека протоколов TCP/IP. Вообще говоря, стек в том виде, как его используют сейчас, появился не сразу. В статье «A Protocol for Packet Network Intercommunication» [3], которая дала начало внедрению сетей TCP/IP, Vinton G. Cerf и Robert E. Kahn обсуждали только один протокол.

## Уровень канала

На уровне взаимодействия с сетью (уровне канала) принято говорить о MAC – Media Access Control.

Основным идентификатором является MAC-адрес. Каждое устройство подключения к сети, будь то Ethernet-карточка или Wi-Fi-модуль, имеют MAC-адрес.

Адрес нужен тогда, когда к одной среде подключено сразу несколько устройств, как, например, в Ethernet или Wi-Fi.

Исторически первые MAC-адреса для идентификации устройств в локальной сети появились в Ethernet. Ethernet относится к технологиям множественного доступа к общей передающей среде в локальной компьютерной сети с контролем коллизий CSMA/CD [4] (IEEE 802.3). На рисунке 1 представлен формат MAC-адреса.

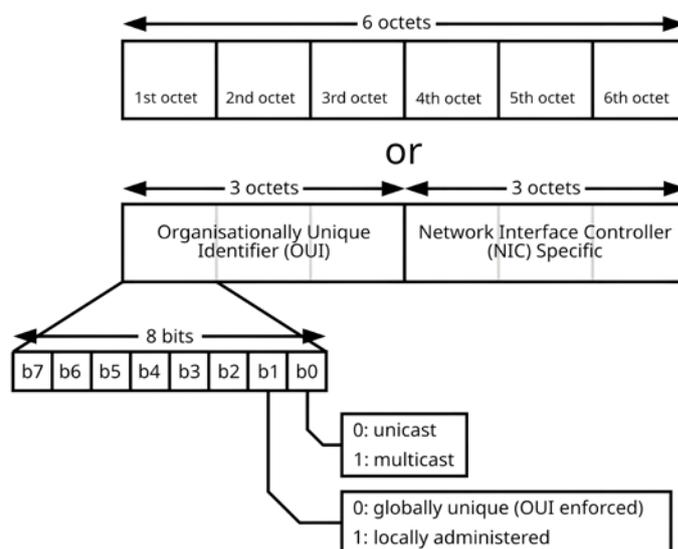


Рис. 1. Формат 48-битового MAC-адреса.

Отметим, что первый октет адреса начинается с идентификатора организации. Выделяет адреса производителям оборудования реестр IEEE Registration Authority [5]. Каждый адрес уникален. IEEE относит группу протоколов 802.3 к протоколам не только канального уровня, но и физического уровня модели OSI.

Уровень канала в общем случае позволяет теоретически построить «большую» сеть на MAC-адресах. Но практически так по разным объективным причинам не поступают.

Адресация в сетях TCP/IP обеспечивается на сетевом уровне или уровне межсетевых обменов за счёт введения IP-адресов.

Классическим протоколом канального уровня для определения соответствия «MAC-IP» является протокол ARP [6]. В RFC826 название протокола звучит буквально так: «An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware». Реализации протокола поддержива-

ют таблицу соответствия между IP-адресами версии IPv4 и MAC-адресами.

В IPv6-сетях ARP не применяют. При инициализации интерфейса используется 64-битный EUI-64 [7] идентификатор, при вычислении которого используют MAC-адрес. На основе EUI назначается локальный IPv6-адрес. Затем по запросу ICMP или DHCPv6 можно получить IPv6 для отправки/получения данных из Интернета.

Следует отметить, что часто для обеспечения информационного обмена на уровне канала используются протоколы прикладного уровня. Например, протокол DHCP (Dynamic Host Configuration Protocol) [8] в сетях IPv4.

Итак, на уровне канала в качестве идентификатора используются MAC-адреса и строятся таблицы соответствия между этими адресами и IP-адресами.

## Уровень сети

При обсуждении сетевого уровня протоколов самое время вспомнить о том, что сети TCP/IP – это сети коммутации пакетов. Во-первых, любое сообщение при отправке по такой сети разбивается на блоки – пакеты. Потом эти пакеты отправляются в путешествие по сети. В таких сетях, в общем случае, заранее неизвестно, существует ли маршрут от одного узла сети к другому узлу или нет, т.е. заранее неизвестно, есть связность или нет.

К слову сказать, в контексте сетевого уровня протоколов правильно говорить именно о маршрутах, как мы их определили ранее.

К сетевому уровню стека протоколов (internet layer) TCP/IP принято относить IPv4 [9], IPv6 [10], ICMP [11], NDP [12], IGMP [13], IPSec [14] и ряд других.

Ядро протоколов этого уровня – это Internet Protocol версий 4 и 6.

Основное назначение интернет-протокола IP – это передача пакета битов (an internet datagram) от источника данных к получателю данных через систему взаимосвязанных сетей. При этом в протоколе нет механизмов контроля надёжности передачи, последовательности приёма/передачи или других, которые характерны для обмена данными по протоколам типа «хост-хост».

Единственным механизмом, который позволяет передавать пакет по множеству взаимосвязанных сетей, является анализ IP-адреса.

Особую роль в процессе маршрутизации имеет структура IP-адреса. Старшие биты адреса определяют адрес сети, а младшие – адрес хоста в этой сети. При чём этот принцип общий и для протокола версии 4, и для протокола версии 6.

Как распределяются части IP-адреса, определено в Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan [15] (RFC-4632).

IP-адреса уникальны. Здесь придётся сделать небольшое отступление и рассказать, как устроено распределение такого ограниченного ресурса, как адресное пространство.

## IANA-функции, или Кто управляет Интернетом

Распределение адресного пространства является одной из так называемых IANA-функций. ICANN в своём информационном буклете [16] описывает их как:

- а) IANA-functions: protocol parameters;
- б) IANA-functions: internet number resources;
- в) IANA-functions: root-zone management of the domain name system;
- г) IANA-functions: other services.

В первом блоке речь идёт о таких параметрах, как, например, порты транспортного уровня стека протокола, закреплённые за определёнными сервисами (WKS – Well Known Services), или медиа-типы, которые используются в HTTP-протоколе при передаче контента.

Работы по стандартизации в соответствии с меморандумом о взаимопонимании (MOU – memorandum of understanding) между ICANN, IETF, IAB [17] ведутся в IETF, а IANA как часть ICANN обеспечивает контроль и бесплатный доступ к этой информации.

С 2016 года функции IANA переданы в учреждённую ICANN некоммерческую организацию PTI – Организация по открытым техническим идентификаторам [18].

Вторая функция, наиболее интересная для нас, – распределение адресного пространства. Для реализации этой функции создан иерархический механизм, в который входят разные организации в разных регионах и странах.

Описание этой системы изложено в RFC7020 – «The Internet Numbers Registry System» [19].

На вершине иерархии распределения ресурсов находится IANA. В контексте документа – это не организация, а функция начального распределения блоков адресов и номеров AS. Организационно эта функция возложена на ICANN, сейчас ее выполняет PTI.

**Блоки распределяются по региональным интернет-реестрам (Regional Internet Registries – RIRs). Сейчас определено пять таких реестров:**

- AfriNIC** – Африканский регион;
- APNIC** – Азиатско-Тихоокеанский регион;
- ARIN** – Северо-Американский регион и часть Карибского региона;
- LACNIC** – регион Латинской Америки и часть Карибского региона;
- RIPE NCC** – Европейский регион, Регион Ближнего Востока и часть Азиатского региона.

Эти региональные реестры созданы в соответствии с политикой ICANN [20].

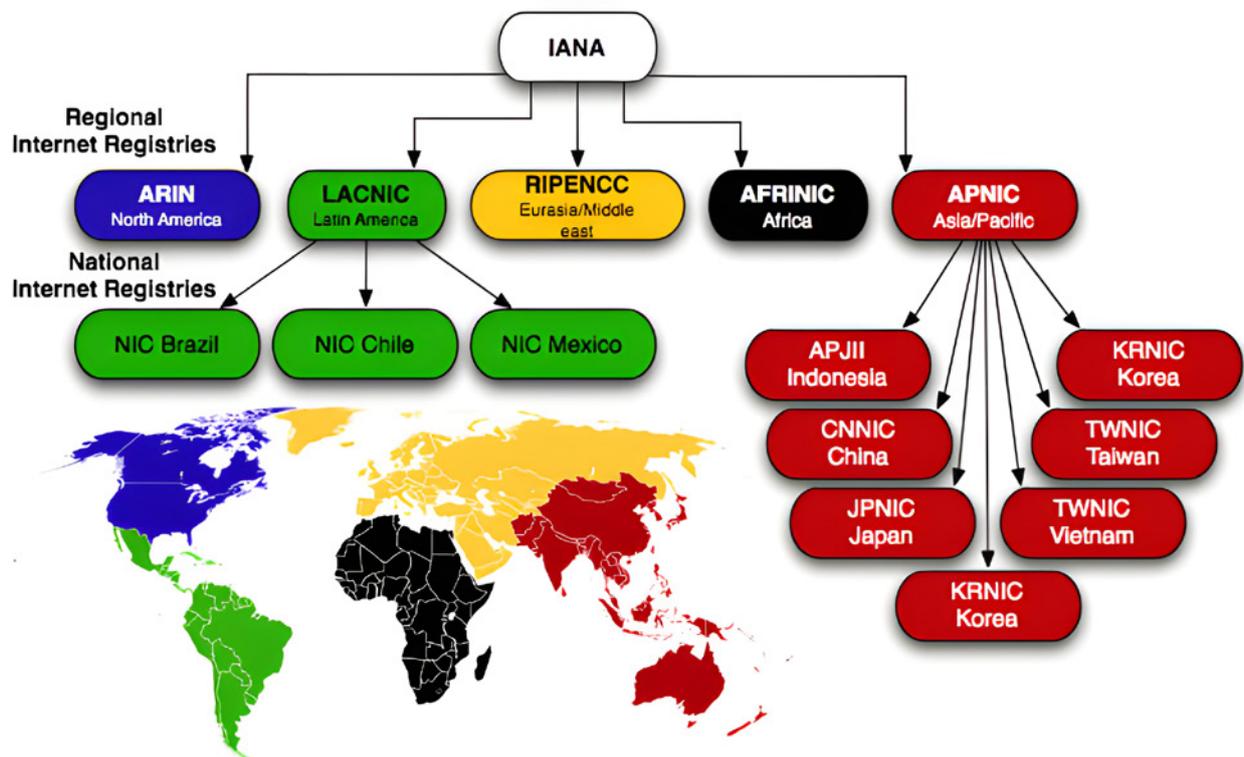


Рис. 2. Распределение мирового адресного пространства.

Региональные реестры из выделенных им блоков выделяют подблоки локальным интернет-реестрам – LIR-ам (Local Internet Registry), которые обычно являются интернет-провайдерами, хотя, например, один из крупнейших российских LIR-ов – РосНИИРОС [21] – реально таковым не является.

Локальные интернет-реестры уже распределяют адреса между своими клиентами, которые назначают их хостам.

Есть регионы, где между RIR и LIR есть ещё один уровень иерархии - National Internet Registries (NIRs). Например, национальные реестры есть в Азиатско-Тихоокеанском регионе и регионе Латинской Америки:

- **IDNIC-APJII** (Индонезия и Полинезия);
- **CNNIC** (Китай);
- **JPNIC** (Япония);
- **KRNIC** (Южная Корея);
- **TWNIC** (Тайвань);
- **VNNIC** (Вьетнам);



Рис. 3. Стоимость адреса IPv4.

- **IRINN** (Индия);
- **NIC Mexico** (Мексика);
- **NIC.br** (Бразилия).

Адресное пространство – это ограниченный ресурс. Например, свободных блоков адресов для работы в Интернете по протоколу IPv4 формально уже не осталось. Они, конечно, есть. Но их осталось немного, и их реально продают. Просто вдумайтесь: 232 (4 294 967 296) адресов распределено по провайдерам Интернета [22].

На рисунке 3 представлена цена за адрес в зависимости от времени и размера блока адресов. А на рисунке 4 - общий объём рынка адресов IPv4.

В RIPE блоки закончились в 2019 году, объёмы трансферов начали расти с 2013. На свои максимальные показатели вышли в 2022, но уже в 2017 нехватка ощущалась, судя по графику на рисунке 4, достаточно остро.

Проблем с выделением адресного пространства IPv6 не наблюдается. Количество сетей, которые поддерживают эту реинкарнацию Интернета, постоянно растёт [23]. Google ve-



Рис. 4. Оценка объёма глобального рынка адресов IPv4.

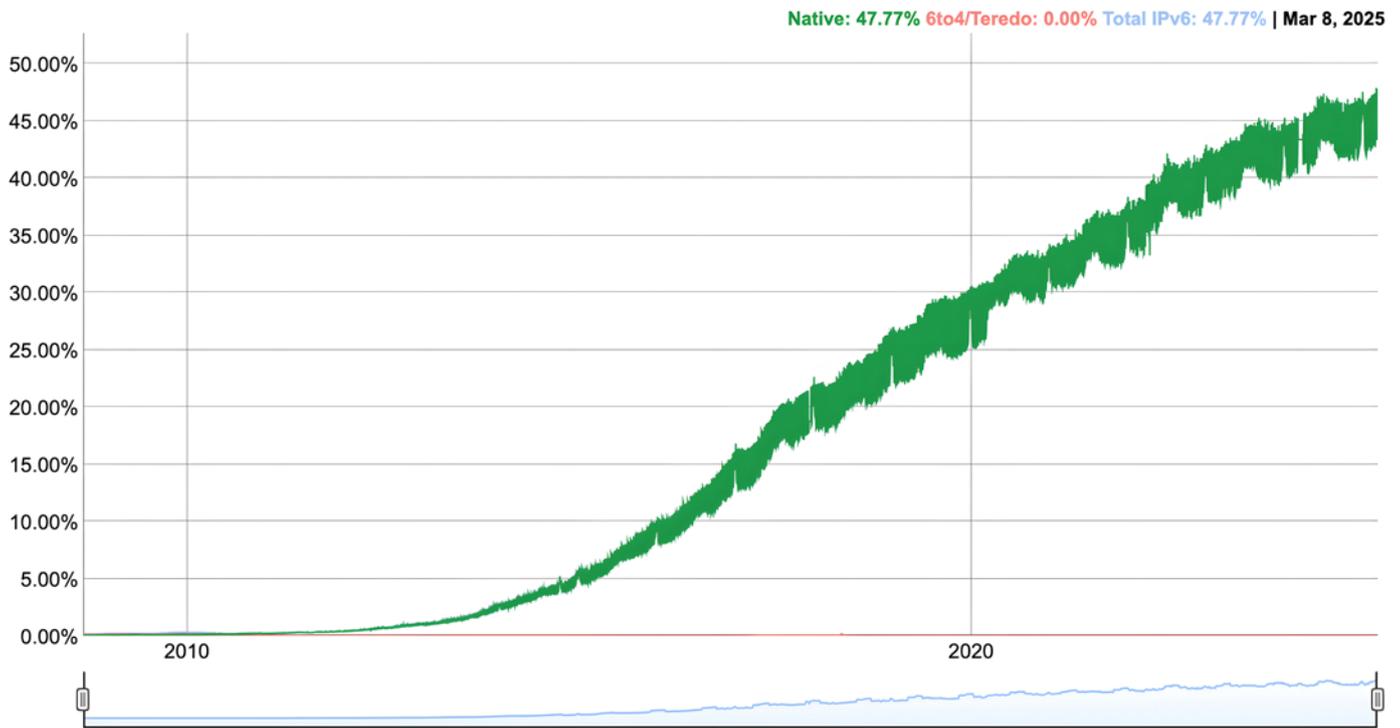


Рис. 5. Доля пользователей Google с адресами IPv6.

дёт статистику обращений конечных пользователей из разных типов IP-сетей (представлена на рисунке 5). Она показывает, что пользователей с адресами IPv6 чуть меньше 50% от общего числа пользователей Google, и этот процент продолжает увеличиваться. Для России Google даёт оценку в 45,97% (рисунок 6) от общего числа обращений из России. Но вот оценкам по России от Google доверять следует с осторожностью. Ряд организационных решений компаний в 2022 году существенно ограничили трафик из России на сервисах, что неизбежно сказалось на их репрезентативности [24].

Теперь о том, «кто управляет Интернетом». Считается [25], что управляет тот, кто выделяет необходимые для работы в Интернете ресурсы. Нет IP-адреса – нет связности. Нет возможности отправить пакет по сети.

Вывод: на сетевом уровне стека протоколов TCP/IP основным идентификатором и ограниченным ресурсом является IP-адрес.

### Уровень транспорта

На уровне транспорта стека TCP/IP находятся два протокола: TCP и UDP. Назначение TCP – обеспечить потокоориентированный надёжный способ передачи данных от приложения на одном хосте приложению на другом хосте. К UDP требований надёжности и обеспечения потокоориентированности не выставляется. Контроль целостности сообщений между приложениями возложен на сами эти приложения.

Протокол UDP довольно часто использовался там, где сами размеры пакетов данных были невелики: например, в DNS (53 порт UDP). Основным ограниченным ресурсом на

уровне транспорта являются порты, к которым привязаны приложения.

В IANA/PTI существует справочник стандартных номеров портов для публичных сервисов, таких как почта (25 порт TCP), веб (HTTP – 80 TCP, HTTPS – 443), SSH (22 -TCP) и т.п. Вообще говоря, если приложение-сервер и приложение-клиент делает один разработчик, то он волен выбрать любые порты, но желательно, выше 1024. Тем не менее, например, протокол прикладного уровня MTPProto (Telegram) стандартно использует 80, 443, 5222 порты TCP непосредственно (plain TCP socket) [26].

Здесь мы рассмотрели классический транспортный уровень, например, упомянутый выше MTPProto может в качестве транспорта использовать Websocket-протокол [27]. Таким образом, транспорт может быть многослойным.

Итак, для транспортного уровня основным ограниченным ресурсом являются транспортные порты. Проверка наличия связности на уровне транспорта при использовании протокола TCP происходит на уровне TCP-handshake [27].

### Уровень приложений

Мы уже упоминали протокол DHCP. Протокол используется при подключении хоста к сети TCP/IP. В этот момент у хоста нет IP-адреса. Хост свой адрес, адрес шлюза и адрес кеширующего DNS-резолвера (опционно) получает по этому протоколу. Соответственно, заполнение ARP-таблицы и таблицы маршрутизации происходит только после того, как будет завершён обмен информацией по DHCP.

DHCP использует в качестве транспорта UDP [28]. Клиент обращается к серверу по 67 порту, а сервер отвечает на 68 порт.

интернет

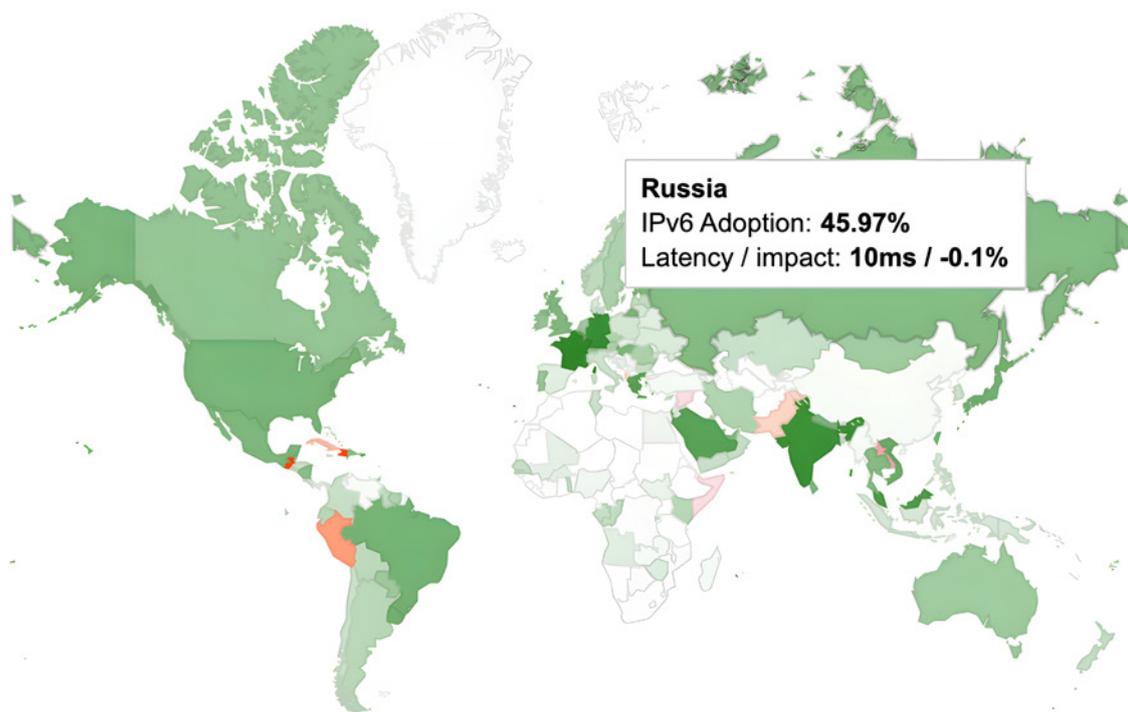


Рис. 6. Использование адресов IPv6 в России по оценке Google.

Здесь следует сделать несколько замечаний о связности. Получение IP-адреса хостом – это вопрос связности в рамках локальной сети. Получение хостом адреса шлюза – это вопрос связности в рамках сети Интернет на уровне транспорта. А вот получение адреса кеширующего DNS-резолвера – это уже вопрос связности на уровне приложений, большинство из которых используют либо непосредственно DNS для поиска IP-адресов, либо в качестве части URL (универсального локатора ресурсов) [29].

Теперь поднимаемся по стеку протоколов выше, на уровень IP. Здесь мы имеем дело с таблицами маршрутизации. В простейшем виде такая таблица на хосте может быть заполнена при применении DHCP. Но заполнить таким образом таблицу маршрутизации шлюза представляется сложным.

Для этой цели используют протоколы обмена маршрутной информацией. Например, такие, как RIP. Протоколы базируются на алгоритмах, разработанных в своё время на основе алгоритма Форда-Фалкерсона для графовой модели.

Протокол RIP использует для обмена маршрутной информацией 520 порт UDP. Таблицы маршрутизации в первой версии протокола обновляются каждые 25-35 секунд – и за это время процесс формирования таблиц должен завершиться (сойтись, т.е. динамический граф конечен).

Протокол BGP<sub>4</sub>, в отличие от RIP и OSPF, которые относятся к типу протоколов «внутренней» маршрутизации, является протоколом «внешней» маршрутизации.

Собственно, в этом месте мы подобрались к ещё одному ограниченному ресурсу идентификаторов, распределе-

ние которого входит в понятие IANA-functions – это номера автономных систем.

Мы будем опираться на определение AS, которое дано в RFC1930 [30]: «Автономная система – это одна или несколько IP-сетей, которая управляется одним или несколькими операторами в соответствии с единственной чётко определённой политикой маршрутизации».

Собственно, в этом определении суть Интернета как сети автономных систем. «Внутренняя» маршрутизация – это маршрутизация IP-пакетов внутри автономной системы. «Внешняя» маршрутизация – это маршрутизация IP-пакетов между автономными системами.

В качестве графа в BGP рассматривается граф, где в качестве вершин выступают AS, а в качестве дуг – связи между ними.

Транспортным протоколом для сообщений BGP является протокол TCP (порт 179). Протокол обеспечивает проверку наличия связности между автономными системами, а по сути, между их маршрутизаторами. Если нельзя установить TCP-соединение, то и связности между системами нет.

Количество автономных систем растёт. Согласно данным проекта iddb.ru [31], всего IANA/PTI через RIR выделено 118 394 автономные системы. Из них для российских LIR выделено 5759, причём 5758 номеров выделено через RIPE, а один номер – через APNIC. При этом, по данным APNIC, активно используются 76 709 номеров AS [32]. Самой большой российской автономной системой является одна из автономных систем «Ростелекома» (ROSTELECOM-AS, 12389).

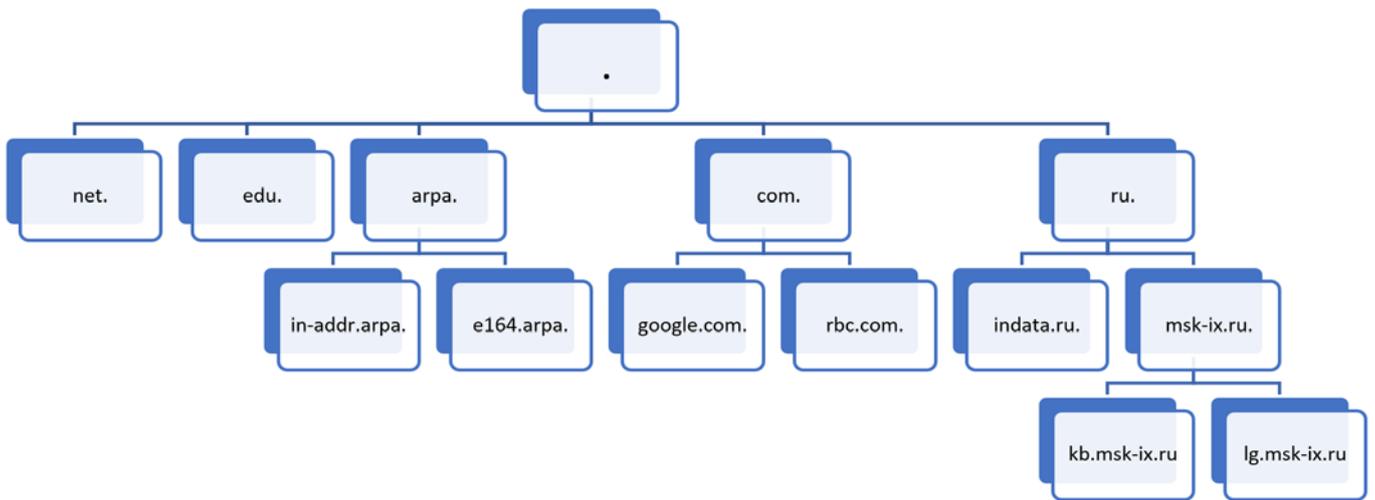


Рис. 7. Фрагмент иерархии доменных имён.

Теперь обратимся к понятию связности непосредственно на уровне приложений. Приложений много. Это и браузеры, которые используют для доступа к сайтам, и электронная почта, и мобильные приложения, стриминговые платформы, мессенджеры и множество других программ.

Рассмотрим только одну – DNS.

Domain Name System (DNS) – это ещё одна сторона IANA-функций. DNS обеспечивает независимость имени информационного ресурса в сети Интернет от IP-адреса. Да и запоминать доменные имена значительно проще, чем IP-адреса.

DNS – это распределённая информационная система, построенная вокруг протокола DNS [33].

Распределённая база данных DNS – это описание соответствий между доменными именами и идентификаторами информационных ресурсов; эту базу данных поддерживает множество авторитетных серверов.

Иерархический характер БД DNS определяется структурой доменных имён. Фрагмент этой иерархии представлен на рисунке 7.

Каждый узел этой иерархии поддерживается несколькими (не менее двух) авторитетными DNS-серверами. Задача этих серверов – хранить описание зоны домена и отвечать на запросы информации из этой зоны.

В качестве инструмента поиска в DNS используется распределённое множество кеширующих DNS-резолверов, которые осуществляют поиск запрошенного соответствия в БД DNS.

Зона домена в формате загрузки на авторитетный сервер – это файл, содержащий ресурсные записи. В ответ на запросы резолверов авторитетный сервер отдаёт соответствующий запросу список ресурсных записей. Если сервер этих записей не отдаст, то никакой связности не будет.

На уровне приложений количество идентификаторов, ответственных за связность, возрастает драматически. Каждый протокол, который стандартизирован в RFC, имеет

свой набор. Приложения написаны разными людьми в разных компаниях, но за счёт открытых стандартов эти приложения оказываются совместимыми и работоспособными.

## В качестве заключения

В этой статье мы бегло прошли по проблеме связности в стеке протоколов TCP. На каждом уровне стека рассмотрели протоколы, модели, на которых они построены, и основные идентификаторы, которые обеспечивают совместимость программных модулей стека и, как следствие, связность.

Совершенно очевидно, что никакой априорно заданной связности в сети Интернет нет. Её наличие обнаруживается только в тот самый момент, когда инициируется запрос на обслуживание в сети Интернет.

Кстати, о графах. World Wide Web – это тоже граф. Гипертекстовый. 

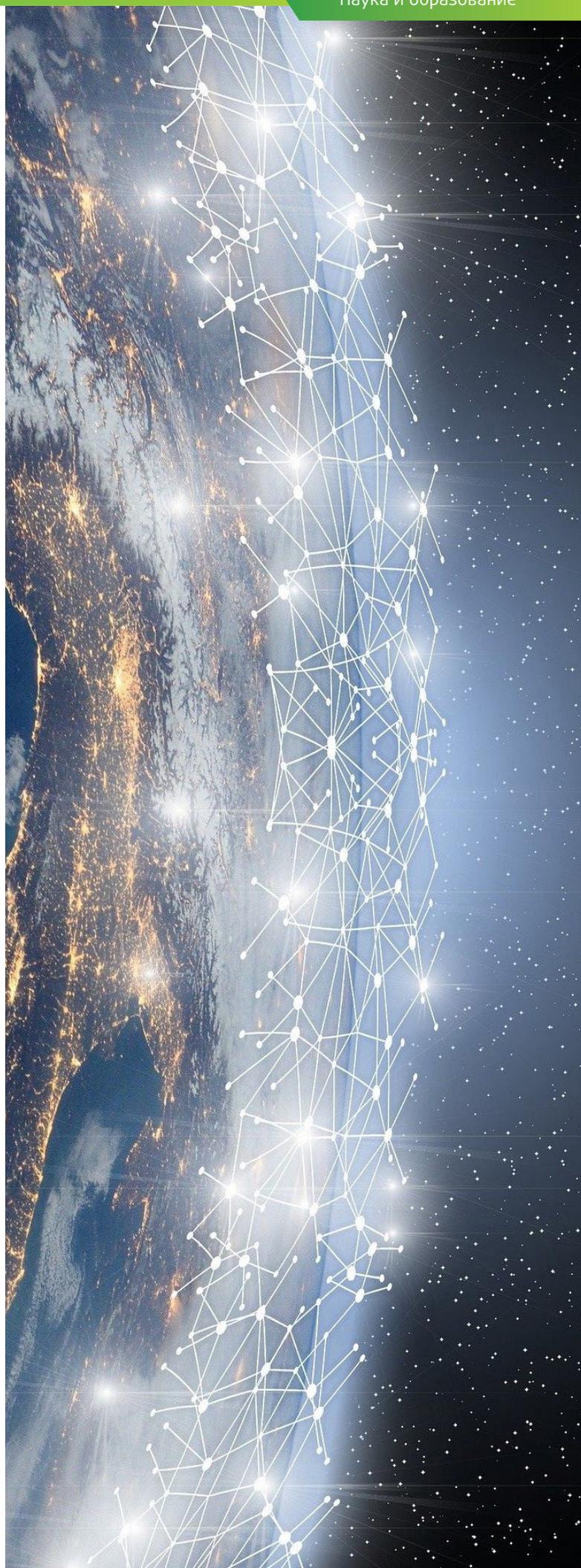
## Список литературы:

- [1] ISO, 35-100, Open System Interconnection, <https://www.iso.org/ics/35.100/x/>
- [2] Д.И. Карлов, Теория графов, МЦНМО; ISBN: 978-5-4439-1690-3; 2022, [https://logic.pdmi.ras.ru/~dvk/graphs\\_dk.pdf](https://logic.pdmi.ras.ru/~dvk/graphs_dk.pdf)
- [3] Vinton G. Cerf and Robert E. Kahn, A Protocol for Packet Network Intercommunication, IEEE Trans on Comms, Vol Com-22, No 5 May 1974, <https://www.cs.princeton.edu/courses/archive/fallo6/cos561/papers/cerf74.pdf>
- [4] IEEE, 802.3-2022 - IEEE Standard for Ethernet, <https://ieeexplore.ieee.org/document/9844436>
- [5] IEEE SA, Registration Authority, <https://standards.ieee.org/products-programs/regauth/>
- [6] David C. Plummer, RFC826 - An Ethernet Address Resolution Protocol - or - Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware, MIT-MC, 1982, <https://data-tracker.ietf.org/doc/html/rfc826>
- [7] IEEE, Guidelines for 64-BIT Global Identifier (EUI-64) Registration Authority, <https://web.archive.org/web/20100706041937/http://standards.ieee.org/regauth/oui/tutorials/EUI64.html>
- [8] R. Droms, RFC2131 - Dynamic Host Configuration Protocol, Bucknell

- University, 1997, <https://datatracker.ietf.org/doc/html/rfc2131>
- [9] DARPA, RFC791 Internet Protocol, 1981, <https://datatracker.ietf.org/doc/html/rfc791>
- [10] S. Deering, R. Hinden, RFC8200 – Internet Protocol Version 6 (IPv6) Specification, Check Point Software, 2017, <https://datatracker.ietf.org/doc/html/rfc8200>
- [11] J. Postel, RFC792 - Internet Control Message Protocol, 1981, <https://datatracker.ietf.org/doc/html/rfc792>
- [12] N. Narten, E. Nordmark, W. Simpson, H. Soliman, RFC4861 - Neighbor Discovery for IP version 6 (IPv6), 2007, <https://datatracker.ietf.org/doc/html/rfc4861>
- [13] W. Renner, RFC2236 - Internet Group Management Protocol, Version 2, Xerox PARC, 1997.
- [14] S. Kent, K. Seo, RFC4301 - Security Architecture for the Internet Protocol, BBN Technologies, 2005.
- [15] V. Fuller, T. Li, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan, 2006, <https://datatracker.ietf.org/doc/html/rfc4632>
- [16] IANA, <https://www.iana.org/about/informational-booklet.pdf>
- [17] B. Carpenter, F. Baker, V. Roberts, RFC2860 - Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority, IAB, IETF, ICANN, 2000, <https://datatracker.ietf.org/doc/html/rfc2860>
- [18] PTI, <https://pti.icann.org/>
- [19] R. Housley, J. Curran, G. Huston, D. Conrad, RFC7020 - The Internet Numbers Registry System, 2013, <https://www.rfc-editor.org/rfc/rfc7020>
- [20] RIPN, <https://ripn.su/>
- [21] IPv4 Market Group, IPv4 Transfer Pricing, <https://ipv4marketgroup.com/ipv4-pricing/>
- [22] Google, IPv6, <https://www.google.com/intl/en/ipv6/statistics.html>
- [23] Храмов Павел, Повторение – мать учения, или Конференция TLD-CON 2024 (5-6 сентября 2024, Минск) Интернет изнутри, №21, стр. 34-41, [https://www.ccni.ru/download/InternetInside/InternetInside\\_N21.pdf](https://www.ccni.ru/download/InternetInside/InternetInside_N21.pdf)
- [24] RIGF, <https://rigf.ru/>
- [25] Telegram, <https://core.telegram.org/mtproto/transport>
- [26] I. Hickson, draft-hixie-thewebsocketprotocol-76, Google, Inc, 2010, <https://datatracker.ietf.org/doc/html/draft-hixie-thewebsocketprotocol-76>
- [27] W. Eddy, Ed, RFC9293 - Transmission Control Protocol (TCP), MTI Systems, 2022, <https://datatracker.ietf.org/doc/html/rfc9293#handshake>
- [28] R. Droms, RFC2131 - Dynamic Host Configuration Protocol, Bucknell University, 1997, <https://datatracker.ietf.org/doc/html/rfc2131>
- [29] T. Berners-Lee, R. Fielding, L. Masinter, RFC985 - Uniform Resource Identifier (URI): Generic Syntax, 2005, <https://datatracker.ietf.org/doc/html/rfc3986>
- [30] J. Hawkinson, N. Bates, RFC1930 - Guidelines for creation, selection, and registration of an Autonomous System (AS), MCI, 1996, <https://datatracker.ietf.org/doc/html/rfc1930#section-3>
- [31] Фонд «ИнДата», IDDB, <https://www.iddb.ru/rir/>
- [32] APNIC, <https://thyme.apnic.net/current/data-summary>
- [33] P. Mackapetris, RFC1035 - Domain Names - Implementation and Specification, ISI, 1987, <https://datatracker.ietf.org/doc/html/rfc1035>
- [34] IANA, Resource Record (RR) Types, <https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4>

## Об авторе:

Храмов Павел Брониславович, к.т.н., доцент, руководитель проектов DNS «МСК-IX», научный руководитель учебных проектов Фонда развития сетевых технологий «ИнДата», лауреат награды Virtuti Interneti 2025



# Некоторые аспекты дефиниции «Connectivity»



Мадина Касенова

## Аннотация

В статье затронут вопрос формальных и содержательных характеристик дефиниции «Connectivity», которая переводится на русский язык словом «связанность» (или «связность» – ред.), а также транслитерированным словом «коннективность». Отмечается, что ключевым технологическим фактором, обуславливающим существо и содержательные аспекты рассматриваемой дефиниции, выступает инфраструктура сети Интернет. Автор обращает внимание читателя на специфику использования и толкования дефиниции «Connectivity», обуславливаемую целями, задачами и регуляторным назначением определённого нормативного документа или акта (национального или международного), либо контекстно диктуемую параметрами конкретного исследования.

## Ключевые слова:

ИКТ, цифровизация, информационное общество, Интернет, связь, связанность, типы связанности.

Тенденции универсализации применения информационных и коммуникационных технологий (ИКТ), ключевым ядром которых выступает Интернет, определяют параметры развития современного информационного общества и динамично расширяющийся ландшафт «цифровизации реальности», что комплексно диверсифицирует практически весь спектр общественных отношений, трансформирует сложившиеся форматы социального взаимодействия, содействует дальнейшей модификации и новации технологических ресурсов, средств и способов коммуникации. В предметно-объектной сфере ИКТ (в их «широком» значении) и Интернета устойчивое применение в настоящее время получает не только сама дефиниция «Connectivity», но и ряд соотносимых с ней понятий и терминологических конструкций, а это в целом объясняет актуальность обращения к вопросу о содержательной сути упомянутой дефиниции как в общем, так и в практическом плане.

Аксиоматичным является то, что любая дефиниция отражает в той или иной форме суть социальных явлений, давая представление об объективных процессах действительности, при этом одновременно очевидна объективная недостижимость универсально точного, однозначного и исчерпывающего определения сущности и специфики явления или процессов посредством одной, единственной и однозначно сформулированной дефиниции. Сказанное в полной мере приложимо к дефиниции «Connectivity», поскольку, с одной стороны, она является отражением многоплановых и сложных явлений действительности, имманентно связанных с использованием сети Интернет; с другой стороны, не существует универсального определения, которое однозначно формулирует содержательный объём рассматриваемой дефиниции. Соответственно, дефиниция «Connectivity» определяется вариативно: в одних случаях – с акцентом на аппаратные средства

обработки и передачи данных в телекоммуникационных сетях (условно-обобщённо – «технологический аспект»); в иных случаях, с учётом характеристик и специфики интернет-технологий, акцент делается на обеспечении возможностей взаимодействия пользователей в цифровой среде при передаче информации, данных, контента и т.д. (условно – «человеческий аспект»); нередко рассматриваемая дефиниция определяется комплексно, охватывая и аппаратные средства, и программные продукты, и пользовательские ресурсы, и обмен данными и контентом, и т.д. [1] При этом такие обобщённые формулировки дефиниции «Connectivity» с очевидностью свидетельствуют о том, что ключевым технологическим фактором, обуславливающим существо и содержательные аспекты рассматриваемой дефиниции, выступает инфраструктура сети Интернет.

Анализируя дефиницию «Connectivity», невозможно игнорировать то формальное обстоятельство, что в предметно-объектной сфере ИКТ в целом и Интернета в частности доминирует иностранная лексика, в связи с чем существенное значение приобретает адекватность перевода на «национальный язык» конкретных понятий, дефиниций, терминологических конструкций, поскольку таковые формируются в конкретной языковой среде, получая соответствующую интерпретацию и значение. В русскоязычном переводе дефиниции «Connectivity» используется слово «связанность» (или «связность» – ред.), а также транслитерированное слово «коннективность» [2], и упомянутые слова зачастую рассматриваются как тождественные. С лексической точки зрения русскоязычные эквиваленты рассматриваемой дефиниции, по-видимому, приемлемы в практическом плане. Между тем, целесообразно обратить внимание на англоязычную интерпретацию дефиниции «Connectivity» (в значении «связанность») в силу значимости её разграничения от близкого ей понятия «Connection» (соединение/связь/подключение). Необходимость такого разграничения аргументируется тем обстоятельством, что «связанность» поддерживается на протяжении всего жизненного цикла коммуникационного устройства или сети, тогда как «соединение/связь/подключение» всегда имеет начальную и конечную точку, что не влияет на возможность установления сетевого подключения или «связанность» как таковую [3]. В этом смысле дефиниции «Connectivity» и «Connection» являются в большей степени самостоятельными, взаимосвязанными и взаимообусловленными, нежели чем тождественными или идентичными. Представляется также целесообразным обратить внимание на два следующих момента.

Первый момент. Вне контекста дефиниции «Connection» рассматривается характеристика содержательного объёма дефиниции «Connectivity» через призму определения «типов связанности» (Connectivity Types). К числу основных «типов связанности» отнесены, в частности, коммутируемый доступ в Интернет; мобильная связь (мобильные устройства, сотовые телефоны, смартфоны, планшеты, ноутбуки и проч.); Wi-Fi; широкополосный доступ, обеспечивающий постоянное подключение к Интернету; DSL; кабельное соединение; волоконно-оптическое соединение; спутниковое соединение. Второй момент. Именно дефини-

ция «Connectivity» (но не «Connection») осуществляет «некую кумулятивную функцию», обуславливает использование таких понятийно-терминологических конструкций, как «универсальная/всеобъемлющая связанность» (Universal Connectivity) [4]; «стандартизированная связанность» (Standards-based Connectivity) [5]; «окружающая среда связанности» (Ambient Connectivity) [6]; «сетевая связанность» (Network Connectivity) [7]; «цифровая связанность» (Digital Connectivity) [8]; «интернет-соединение/интернет-связанность» (Internet Connectivity) [9] и др. Обозначенные моменты свидетельствуют о самостоятельной значимости дефиниции «Connectivity», что объясняет логику её разграничения от дефиниции «Connection».

В настоящее время дефиниция «Connectivity», равно как и соотносимые с ней понятийно-терминологические конструкции, устойчиво используется в различного рода документах и актах национального [10] и международного [11] уровня (технического, программно-политического, нормативно-стратегического и проч. характера). При этом существенно важно обратить внимание на то, что следствием отсутствия универсального и однозначного определения содержательного объёма дефиниции «Connectivity» является так называемый бланкетный формат её использования. В текущих реалиях это означает, что специфика применения дефиниции «Connectivity», равно как и её содержательное толкование, контекстно диктуется и всецело зависит от целей, задач и регуляторного назначения конкретного программного, политико-стратегического и проч. документа или нормативного акта (национального или международного).

Дефиниция «Connectivity» получает устойчивое закрепление в действующих официальных документах таких диаметрально противоположных институциональных структур, как Европейский союз – международная организация интеграционного типа, обладающая международной правосубъектностью, и Ассоциация мобильных операторов GSMA – национальное юридическое лицо, созданное в организационной форме некоммерческой организации, деятельность которой основана на принципе членства (Ассоциация объединяет операторов мобильной связи по всему миру) [12].

Европейский союз (далее – «Евросоюз» или «ЕС») нацелен на то, чтобы сделать Европу самым «связанным» континентом к 2030 году, а в нынешнем (2025) году достигнуть связанности («Connectivity») сетей, обладающей пропускной скоростью 100 Мбит/с, не только для обеспечения связанности всех европейских домохозяйств, но также для создания возможности последующей модернизации и дальнейшего увеличения скорости сетей. Эти цели сформулированы Евросоюзом в ряде программных, политико-стратегических и нормативно-рекомендательных документов, а также в законодательных актах ЕС, в системе которых основными являются:

- «Цифровое десятилетие Европы: цифровые цели на 2030 год» [13];
- «Белая книга» Евросоюза (2024). Как удовлетворить потребности Европы в цифровой инфраструктуре [14];

- Регламент (ЕС) 2024/1309 Европейского парламента и Совета (29.04.2024) о мерах по снижению стоимости развёртывания гигабитных сетей электронной связи, вносящий поправки в Регламент (ЕС) 2015/2120 и отменяющий Директиву 2014/61/ЕС (Акт о гигабитной инфраструктуре – Gigabit Infrastructure Act, GIA) [15], вступивший в силу 11.05.2024, действие которого начинается в ноябре 2025 года;
- Директива (ЕС) 2018/1972 Европейского парламента и Совета от 11.12.2018, устанавливающая Европейский телекоммуникационный кодекс (переработанный) [16];
- Программа политики радиочастотного спектра, основанная на Решении № 243/2012/ЕС Европейского парламента и Совета (14.03.2012) об учреждении многолетней программы политики в области радиоспектра [17];
- Рекомендация по нормативному содействию гигабитной связанности (06.02.2024) [18];
- Инициатива WiFi4EU [19].

В упомянутых документах и актах Евросоюза дефиниция «Connectivity», во-первых, не получила однозначно сформулированного определения, во-вторых, используется в разных аспектах: её содержательное значение толкуется различным образом. Вместе с тем, «гармонизированный нормативный ландшафт» Евросоюза определяющим образом влияет на то, что дефиниция «Connectivity» рассматривается как через призму «технологического аспекта» (цифровые сети – мобильные и стационарные – коммуникационные структуры, Интернет, разнообразные кабели, спутники и проч.), так и через призму «социального аспекта» («человеческое измерение» [20]). Сказанное в общем плане подтверждается некоторыми примерами нюансного определения содержания дефиниции «Connectivity»:

- возможность и способность аппаратных устройств или программных пакетов одной сети связи подключаться к устройствам или программным пакетам других сетей для взаимодействия и передачи данных;
- сетевая доступность и подключаемость ресурсов и ПО одной подсети к ресурсам и ПО иных подсетей;
- обеспечение взаимного соединения и установления межсетевого взаимодействия аппаратных ресурсов различных сетей связи, а также способность аппаратных устройств или программных пакетов пользователей различных подсистем связи подключаться друг к другу, передавать и обмениваться данными;
- возможность подключения к Интернету широкого круга пользователей для межсетевого соединения и взаимодействия ресурсов различных аппаратных средств и программных пакетов.

Ассоциация GSMA [21], масштабно вовлечённая в процесс обеспечения стабильной связанности («Connectivity»), в своей деятельности опирается на сотни операторов мобильной связи, в т.ч. содействующих функционированию

мобильного Интернета. Ассоциация GSMA публикует свои ежегодные отчёты о развитии экосистемы фиксированных, мобильных и беспроводных сетей и включает в эти отчёты обзор складывающихся «мировых тенденций» в области связанности («Connectivity») в мировом масштабе. В опубликованный GSMA документ «Отчёт о состоянии мобильной интернет-связанности (2024)» [22] в т.ч. включены данные индекса мобильной связанности по 173 странам, которые базируются на четырёх всеобъемлющих факторах: технологическая инфраструктура, доступность/ценовая доступность, состояние подготовленности потребителей, а также контент и услуги. Индекс мобильной связанности CSMA, разработанный в рамках обязательств мобильной индустрии по стимулированию мобильного интернет-подключения и интернет-связанности в целом [23], безусловно, контекстно отражает содержательные аспекты дефиниции «Connectivity».

\*\*\*

Представленное изложение сосредоточено лишь на некоторых аспектах дефиниции «Connectivity», однако даже такое очень фрагментарное изложение даёт основание для некоторых обобщающих выводов:

- дефиниция «Connectivity» отражает многоплановые и сложные явления реальной действительности, имманентно связанные с использованием сети Интернет;
- ключевым технологическим фактором, обуславливающим существо и содержательные аспекты рассматриваемой дефиниции, выступает инфраструктура сети Интернет;
- не существует универсального, однозначного определения рассматриваемой дефиниции, а содержательный объём дефиниции не только формулируется вариативно, но и зависит от целей, задач и назначения документа, в котором закрепляется дефиниция «Connectivity». ■

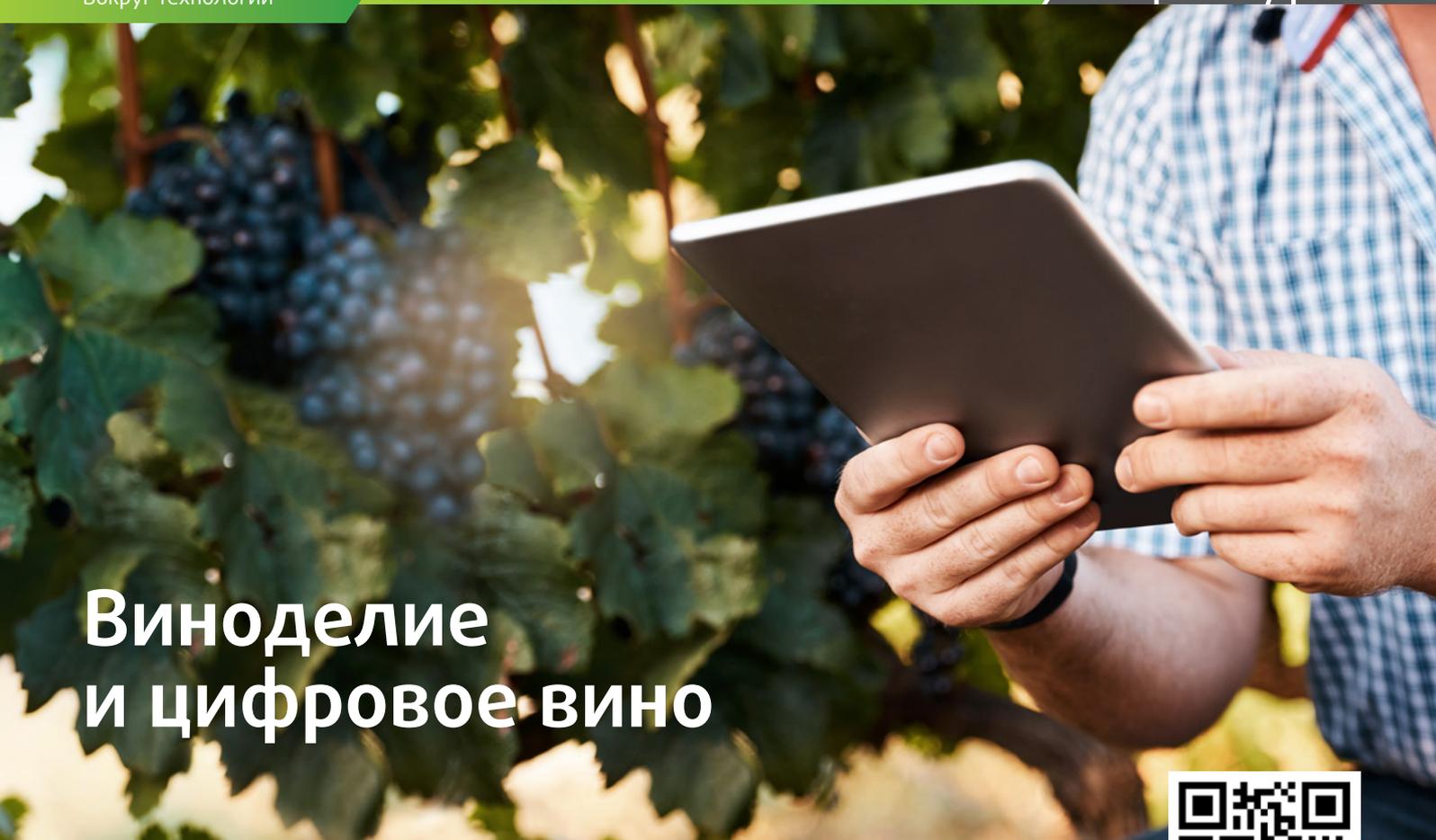
### Список литературы:

- [1] См. подробнее, например: Cybersecurity Glossary. <https://nordvpn.com/ru/cybersecurity/glossary/network-connectivity/> В частности, ряд упомянутых аспектов рассмотрены в исследовании Belli D., Barsocci P., Connectivity Standards Alliance Matter: State of the art and opportunities. [https://www.researchgate.net/publication/375920455\\_Connectivity\\_Standards\\_Alliance\\_matter\\_State\\_of\\_the\\_art\\_and\\_opportunities](https://www.researchgate.net/publication/375920455_Connectivity_Standards_Alliance_matter_State_of_the_art_and_opportunities)
- [2] О термине «коннективность» см., например, Викисловарь. <https://ru.wiktionary.org/wiki/> См. также: Робачевский А. Интернет изнутри. Архитектура экосистемы Интернета/ Андрей Робачевский. – 3-е изд., перераб. и дополн. – М.: Серпантин Эдженси. 2024.

- [3] См. подробнее: Connectivity: understand why it is the power that is driving the digital age (What is the difference between connection and connectivity?). <https://odatacolocation.com/en/blog/connectivity/>
- [4] Achieving Universal Connectivity (The United Nations Secretary-General's Roadmap Digital Cooperation). [https://www.un.org/digital-emerging-technologies/sites/www.un.org.tech-envoy/files/general/Universal\\_Connectivity\\_Summary\\_PDF.pdf](https://www.un.org/digital-emerging-technologies/sites/www.un.org.tech-envoy/files/general/Universal_Connectivity_Summary_PDF.pdf) Accelerating progress is key in race toward universal and meaningful connectivity. <https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx>
- [5] Satellite Networks for IoT: Standards-Based Vs. Proprietary. <https://www.iotforall.com/satellite-iot-standards-vs-proprietary>
- [6] См., например: Frankston B. Ambient Connectivity: An Introduction. [https://circleid.com/posts/ambient\\_connectivity\\_an\\_introduction](https://circleid.com/posts/ambient_connectivity_an_introduction)
- [7] См. подробнее: Cybersecurity Glossary. <https://nordvpn.com/ru/cybersecurity/glossary/network-connectivity/> Types of network connectivity. <https://www.telefonica.com/en/communication-room/blog/types-network-connectivity/>
- [8] См., например: A Councilor's Guide to Digital Connectivity. <https://www.local.gov.uk/councillors-guide-digital-connectivity>
- [9] The State of Mobile Internet Connectivity 2023. URL: <https://data.gsmaintelligence.com/research/research/research-2023/the-state-of-mobile-internet-connectivity-2023>
- [10] См., например: распоряжение правительства РФ от 24.11.2023 N 3339-р «Об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года». СПС КонсультантПлюс; Технические нормативные спецификации, разрабатываемые Корпорацией Open ID Foundation (USA). <https://openid.net/10-years-on-openidconnect-published-as-iso-spec/>
- [11] К примеру, см. международные стандарты ISO/IEC 26131:2024; ISO/IEC 26132:2024; ISO/IEC 26133:2024 и др. (основанные на спецификациях Open ID). <https://standards.iteh.ai/catalog/standards/iso/444186ad-7d67-4936-97b9-71801a5e0f1c/iso-iec-26131-2024?srsltid=AfmBOorUjN7e5-pljk-SIK0oorQaCCuPvrXcuorMYU2ejXvHSEFaRyson>
- [12] Материнская компания GSM Association – юридическое лицо (право Швейцарии), деятельность которого поддерживается дочерними компаниями различных юрисдикций. <https://www.gsma.com/about-us/>
- [13] Europe's Digital Decade: digital targets for 2030. [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en)
- [14] White Paper - How to master Europe's digital infrastructure needs? <https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs>
- [15] Regulation (EU) 2024/1309 of the European Parliament and of the Council of 29 April 2024 on measures to reduce the cost of deploying gigabit electronic communications networks, amending Regulation (EU) 2015/2120 and repealing Directive 2014/61/EU (Gigabit Infrastructure Act) (Text with EEA relevance). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-03A32024R1309>
- [16] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (Text with EEA relevance). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex-03A32018L1972>
- [17] Decision No 243/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing a multiannual radio spectrum policy programme (Text with EEA relevance). [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legisum:310502\\_1](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legisum:310502_1)
- [18] Recommendation on the regulatory promotion of gigabit connectivity. <https://digital-strategy.ec.europa.eu/en/library/recommendation-regulatory-promotion-gigabit-connectivity>
- [19] The WiFi4EU Initiative. <https://digital-strategy.ec.europa.eu/en/related-content?topic=116>
- [20] What is connectivity? <https://digital-strategy.ec.europa.eu/en/policies/connectivity>
- [21] GSMA. <https://www.gsma.com/about-us/>
- [22] The State of Mobile Internet Connectivity Report 2024 (GSMA 2024). <https://www.gsma.com/r/wp-content/uploads/2024/10/The-State-of-Mobile-Internet-Connectivity-Report-2024.pdf>
- [23] Mobile Connectivity Index Methodology. [https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/gsma\\_resources/mobile-connectivity-index-methodology/](https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/gsma_resources/mobile-connectivity-index-methodology/)

## Об авторе:

Мадина Балташевна Касенова, доктор юридических наук, профессор кафедры теории и истории частного права, ФГБН «Исследовательский центр частного права имени С.С. Алексеева при Президенте РФ»



# Виноделие и цифровое вино



Сергей Зимин

## Аннотация

За последние 30 лет бурный технический прогресс и огромное количество новых технологий, основанных на научных открытиях, дали толчок бурному развитию не только IT-индустрии и телекома, но и многих других отраслей; например, не избежала этой участи и такая отрасль сельского хозяйства, как виноделие...

## Ключевые слова:

виноделие, телекоммуникации, новые технологии, цифровое вино, NFT.

Телекоммуникация – это передача информации на расстоянии. С её помощью люди утоляют свою жажду общения и получения новой информации. Виноделие – отрасль сельского хозяйства, которая позволяет нам утолять жажду в прямом смысле этого слова. Самые ранние свидетельства существования виноделия имеют возраст около восьми тысяч лет, а желание получить новые знания присуще человечеству со времён появления «человека разумного». Но долгое время никакого заметного прогресса не происходило ни в скорости передачи информации, ни в технологиях виноделия. Собрали урожай винограда, подавили ягоды и оставили сок сбраживаться или в глиняном кувшине, или в ёмкости из кожи животного. Хорошо, если это вино доживало до урожая следующего года, а обычно через несколько месяцев оно превращалось в уксус. И для того, чтобы напиток можно было употреблять, людям приходилось добавлять в вино пряные травы, а то и хлеб с сыром крошить, как рассказывал нам Гомер.

Только с заметным развитием науки в последние два столетия, с появлением относительно недорогих машин и

механизмов, развитием технологий мы наблюдаем качественный и количественный рост в производстве вина. Открытие электричества, а также открытие Пастером природы брожения позволило подойти к виноделию с научной точки зрения. Вторая половина XX века со своими открытиями в области химии и биологии дала толчок развитию сельского хозяйства. Открытие цикла трикарбоновых кислот (цикл Кребса) позволило понять, как живые организмы получают энергию для своей жизни и развития, а разработка промышленного производства удобрений и инсектицидов привела к устойчивому производству качественного и стабильного сырья для виноделия.

На первый взгляд процесс виноделия за прошедшие тысячелетия никак не изменился, основные этапы остались прежние: собрать виноград, выдавить из него сок и дать этому соку сбродиться – вот и вино! Но это только на первый взгляд. Современное виноделие – это наукоёмкое и технологичное производство. Виноград надо собрать в правильной степени зрелости, для чего постоянно контролируются уровни сахара и кислоты в ягоде. Степень зрелости может быть разной

для разных видов вина — например, для игристого нужно собрать виноград пораньше, когда степень кислотности высокая, а сахаров накопилось не по максимуму. Потом урожай надо довести в целости и сохранности до винодельни. Если он подавится при транспортировке, то брожение может начаться раньше срока, и результат может быть не тот, что ожидает винодел.

После доставки урожая на винодельню начинается обработка винограда: белые сорта отделяют от кистей, отжимают сок и направляют его в бродильные ёмкости. Сорта на красное вино прессуют в основном вместе с кистями и отправляют в ёмкости вместе с ними и шкурками с косточками. Это потом придаст цвет красному вину, так как у большинства сортов винограда сок белый, прозрачный.

Ёмкости для брожения имеют разнообразие форм, размеров и изготовлены из различных материалов: тут могут быть представлены и нержавейка, и дерево, и бетон. Форма ёмкости, как и материал, тоже вносит свою лепту в получившееся вино, брожение по-разному происходит в бетонном яйце на 1000 литров и в чане из нержавейки на 20 000 литров. Зачастую все эти ёмкости — не просто ёмкости, а технологичные устройства. В современном виноделии без этого никуда: ёмкости обладают так называемой рубашкой, по которой циркулирует вода, которая или подогревает, или, наоборот, охлаждает сусло, бродящее в них. Кстати, для производства белого вина температура должна быть ниже, чем для производства красного — 16-20 градусов против 22-28 градусов. Температура брожения, как и значение сахара, спирта, кислотности в сусле контролируется ежедневно.

Скажу несколько слов и о дрожжах. Мало кто из виноделов пускает процесс брожения на самотёк, гарантировать из года в год стабильный результат и качество на «диких» дрожжах невозможно. Поэтому химическая промышленность выпускает специальные дрожжи для вина. Видов этих дрожжей существует немало, так как для каждого сорта винограда нужен свой вид, который максимально раскроет органолептические свойства именно этого сорта винограда. То есть дрожжи для «каберне совиньон» совсем не подходят для сорта «совиньон блан» — они работают при разных температурах, разным уровне кислотности и спирта.

Много факторов приходится учитывать виноделу при работе. Чистота — это не только залог здоровья человека, но и залог здоровья вина. Не менее трети рабочего времени тратится на уборку и мытьё всех механизмов и площадей винодельни. В противном случае занесённые штаммы дрожжей или микробов приведут к тому, что будет испорчен урожай не только текущего, но и последующих годов, что приведёт к большим тратам на дезинфекцию.

После того, как брожение закончится, виноделу придётся решить, что делать с полученным материалом. С большой вероятностью для красных вин потребуется провести малолактическую (яблочно-молочную) ферментацию. Белым винам это требуется в значительно меньшей степени. Малолактическая ферментация сглаживает остроту яблочной кислоты, преобразуя её в молочную. Регулируется такой процесс не только добавлением специальных бактерий, но и температурой, ведь при понижении температуры процесс

замирает. В случае белых вин яблочно-молочная ферментация в основном используется для сортов, которые потом могут быть отправлены на выдержку, например, «шардоне». Это придаёт готовому вину аромат сливочного масла.

Затем вина отстаиваются в нейтральных металлических ёмкостях перед розливом в бутылки. Те вина, которые по своим органолептическим свойствам или по месту происхождения и способу производства требуют дальнейшей выдержки, отправляются в бочки.

Вот так в общих чертах выглядит процесс производства вина. Несмотря на всю простоту в описании, этот процесс требует значительных знаний химии, биологии и даже физики. А потом подключается и экономика, и маркетинг — вино ведь нужно продать! Часто цена определяется не только затратами на производство, но и местностью, где вино изготовили, и именем винодела. Например, в Пьемонте есть небольшая зона Бароло, где красные вина весьма недешёвы. А чуть севернее находится зона Роэро, где вина из того же сорта винограда («неббиоло») стоят дешевле, и по качеству не хуже. Вот такая вот маркетинговая составляющая. А есть и экономическая — то же бароло надо по правилам выдерживать перед продажей не менее двух лет в бочках, а потом ещё год — в бутылках. А это затраты — ваши деньги просто лежат у вас в виде бутылок с вином, да ещё и занимают место на складе.

Но виноделие использует не только достижения в области химии или биологии. Информационные технологии, телекоммуникации имеют большое значение — если не во время производства, то уж точно во время продаж. Да и при регулировании отрасли со стороны государства ИТ применяются повсеместно. Кроме очевидного — сайтов виноделен, на которых можно ознакомиться с характеристиками и ассортиментом всей выпускаемой продукции, а также и заказать себе вина, записаться на экскурсию, есть ещё и сайты отдельных винных коммун и зон производства. Там можно ознакомиться с правилами производства вин в этой местности, посмотреть карты виноградников, ознакомиться с





последними законами и актами регулирующих органов. Но это уже, скорее, полезная информация для виноделов, а для потребителей, конечно, интересней покупка или посещение винодельни с экскурсией. Многие винодельни присутствуют и в соцсетях, что упрощает общение и позволяет иногда в «прямом эфире» следить за работой мастеров.

Что касается нашей страны, то с 2007 года онлайн-торговля алкогольной продукцией у нас запрещена. Можно только посетить сайты винных сетей или отдельных магазинов и сделать заказ, который потом придётся забрать из выбранного магазина. Некоторые крупные сети выпускают и приложения для смартфонов, позволяющие совершить покупку, не поднимаясь с дивана (хотя чтобы забрать заказ, все-таки придётся с него встать). Есть винодельни, которые помещают на свои этикетки QR-коды, пройдя по которым, можно узнать много интересного про вашу конкретную бутылку. А если что-то осталось невыясненным или есть сомнения, можно воспользоваться сервисом от Росалкогольконтроля и проверить эту бутылку по акцизной марке. Сделать это можно на сайте <https://public.fsgar.ru/checkmark> или установив на свой смартфон приложение «Антиконтрафакт Алко». Там можно даже просмотреть всю цепочку перемещений каждой отдельной бутылки. Ну чем не блокчейн!

Блокчейн, кстати, всё-таки добрался и до маркетинга в вине, уже есть первые ласточки применения технологии NFT в продажах вина. NFT (non-fungible token) – это уникальный цифровой сертификат, который хранится в блокчейне и не

может быть клонирован. Он гарантирует оригинальность любого объекта. В частности, это касается винных NFT как нового инструмента для коллекционирования и купли-продажи вин. Релиз Chateau Angélu из Бордо в 2021 году создал прецедент для винных NFT в Европе. Винодельня совместно с британской компанией винных инвестиций Cult Wines выпустила NFT на владение бочкой вина Angélu 2020 и оригинальным трёхмерным цифровым произведением искусства, а также VIP-посещение шато. В июле 2021 года анонимный покупатель приобрел NFT на платформе OpenSea за сумму, эквивалентную 110 тысячам долларов ([http://www.spaziovino.com/articles/investment/italianwines\\_metaverse\\_blockchain\\_nft/](http://www.spaziovino.com/articles/investment/italianwines_metaverse_blockchain_nft/)). Появилось такое цифровое вино и у нас. Как писал портал «РБК Вино» (<https://www.rbc.ru/wine/news/67aef80d9a7947acc2698014>), Альфа-банк совместно с виноторговой компанией Luding Group 14 февраля 2025 года запустили новые гибридные цифровые права (ГЦП) на вино, общий объём эмиссии составит более 85,5 миллиона рублей. Гибридные цифровые права представляют собой комбинацию цифровых финансовых активов (ЦФА) и утилитарных цифровых прав (УЦП). Инвесторы могли приобрести цифровой аналог алкоголя, а физически забрать бутылку смогут с 14 апреля по 11 августа 2025.

Правда, винная индустрия настороженно воспринимает этот цифровой мир. Винодельческие хозяйства в целом не имеют достаточных знаний и плохо понимают механизмы функционирования новых технологий. Единицы виноделов хорошо ориентируются в цифровой теме, а общая нестабильность

рынка NFT и криптовалют, спекулятивные цены, лопнувшие пузыри и другие проблемы, связанные с молодостью системы, дают повод виноделам опасаться этого нового дивного мира. Есть минусы и для желающих вложить деньги – это технические сложности, так как потенциальному инвестору придётся разбираться с платформами, ПО, кошельками, цифровыми подписями и т.д. Да и сами винные токены пока не обладают высокой ликвидностью. Но есть и плюсы: технология блокчейн имеет комбинацию преимуществ, которые не всегда гарантированы в привычном нам физическом мире. В первую очередь – это полная аутентификация продукта, отслеживание сделок и прозрачность процессов.

## Напоследок - несколько практических советов.

- Приблизительно 90% вин сделаны так, что их надо выпить в первые три года после производства. Особенно это относится к белым и розовым винам, их желательно выпивать в первые год-два после производства. Вин, которые подходят для выдержки, производится не так уж и много, ведь сортов винограда и виноделен, где они производятся, существует совсем небольшое количество. Настоящие выдержанные вина предназначены для коллекционеров или особых случаев. А вот выдержанные вина в простом универмаге – это, скорее всего, неликвид, вполне вероятно, ещё неправильно хранившийся. Велика вероятность потратить серьёзные деньги и не получить удовольствия. Так что настоящие выдержанные вина лучше покупать в специализированных магазинах, где есть консультанты-кависты.
- Доверять ли рейтингам? Рейтинги бывают двух основных видов: составленные специалистами и «народные». Тут уж решайте, что вам важнее, отведать вина, полностью соответствующего своим сортовым признакам и месту производства согласно местным законам, или насладиться вином, которое просто нравится большинству. Хотя эти рейтинги могут и совпасть, но чтобы это понять, надо пробовать, пробовать и пробовать. Без собственной статистической картины никуда. Специалисты оценивают вино по чётко структурированным параметрам – аромат, вкус, цвет, кислотность, алкоголь. И может оказаться так, что по всем параметрам это вино на 95 баллов из 100, а вам не зашло, а вот вино на 80 баллов для вас подойдёт идеально. С народными рейтингами тоже надо быть осторожным, может оказаться, что вино на все 5 баллов из 5 по оценкам тысяч людей вам совсем не понравится. Тот же способ (пробовать, пробовать...) вам поможет и здесь. Нароботав некоторую базу из опробованного, создав свои собственные статистические выводы в сравнении со вкусами других людей, вы уже сможете по описанию понять, понравится вам вино или нет. Где же посмотреть такие рейтинги? Самый известный «народный» – это Vivino, но он существует только в виде приложения для смартфона. Наша страна за последние лет 10 достигла значительных успехов в виноделии, поэтому могу порекомендовать несколько рейтингов для российского

вина: это «Первый Гид» ([https://firstguide.ru/w\\_ratings](https://firstguide.ru/w_ratings)) или «Лучшие российские вина по версии SWN» (<https://swn.ru/best-wines/wines/>). В бумажном виде можно приобрести авторский гид Артура Саркисяна «Российские вина». В мировом масштабе рейтингов существует немало, они составлены по совершенно разным критериям: и по стране производства, и по сортам винограда, и по авторам – авторские рейтинги известнейших винных критиков. Вот несколько примеров: Роберт Паркер (Robert Parker) и группа экспертов из журнала Wine Advocate, Wine Spectator, Decanter. Gambero Rosso для вин Италии, Guia Penin – гид по испанским винам от Хосе Пинина (José Peñín) - и много других.

- Из каких стран лучше пить вина? Да из любых, где их делают! В любой стране, производящей вино, можно найти прекрасные экземпляры. Не стоит думать, что если в стране стаж виноделия насчитывает несколько тысяч лет, то там-то уж точно знают, как делать вино. Ведь не факт, что в те давние времена это была та же страна, что и сейчас. Да и современные технологии уже сильно отличаются от старых. Больше внимания лучше обращать на опыт винодела, на отзывы о его винах, есть ли у него собственные виноградники или он покупает сырьё, какие приёмы он применяет при работе.
- При посещении ресторана не стесняйтесь обращаться к сомелье для помощи в выборе вина к тем блюдам, что вы решили заказать. Это может значительно украсить ваш вечер. ■

### Об авторе:

Сергей Зимин, инженер NOC MSK-IX, выпускник школы сомелье





# Мария Колесникова: «Домен .рф меняет сознание разработчиков»



12 апреля 2025 года российский национальный кириллический домен .рф отмечает своё 15-летие. Домен во многом уникальный: как своим взлётом в 2010 году, когда менее чем за сутки после старта открытой регистрации в нём было зарегистрировано 240 тысяч доменных имён, и этот рекорд не удалось повторить никому, так и своим стабильным лидерством среди IDN-доменов. Сегодня в домене .рф зарегистрировано 760 тысяч доменных имён, и это крупнейший национальный IDN в мире.

Но для того, чтобы домен .рф (и почти 1500 других доменов верхнего уровня, среди которых есть как домены на национальных алфавитах, так и домены на латинице, но отличающиеся по своей длине от классических 2-3-буквенных) рос, развивался и был доступен всем в Интернете, необходимо проделать очень большую работу: сделать так, чтобы всё ПО понимало и принимало все допустимые домены и адреса электронной почты с их использованием. Этим и занимается команда проекта «Поддерживаю.РФ», созданного Координационным центром доменов .RU/.RF в год 10-летия домена .рф. Руководитель проекта Мария КОЛЕСНИКОВА рассказала нашему корреспонденту о том, как живёт и растёт домен .рф и почему нужно менять привычки у технических специалистов.

**- Давай начнём с истоков. Откуда в принципе возникла идея внедрить доменные имена не на латинском алфавите? Насколько я помню, она появилась чуть ли не в начале 90-х, когда мало кто мог представить, что Интернетом будет пользоваться баба Зина или мальчик из африканской деревни. И все, кто пользовался Интернетом, в той или иной степени знали английский. Так что же стало отправной точкой для начала этого процесса?**

- Дело в том, что в доменных именах изначально разрешалось использовать только символы ASCII (буквы a-z, цифры 0-9 и дефис «-»). Впервые идея создания доменных имён с символами национальных алфавитов была выдвинута Мартином Дюрстом (Martin J. Duerst) в декабре 1996 года, когда он выступил с докладом на эту тему на одной из международных конференций и представил проект RFC Internationalization of Domain Names (<https://www.webcitation.org/65t9MQja2?url=http://tools.ietf.org/html/draft-duerst-dns-118n-00>). Считается, что именно с этого момента международное сообщество поддержало идею и началась её техническая проработка. Инженерная группа интернета (IETF), начиная с 2003 года, выпустила ряд стандартов (RFC), описывающих технические принципы использования интернационализированных доменных имён в приложениях (IDNA, Internationalized Domain Names in Applications). Использование IDN-доменов было реализовано через специальный механизм преобразования Punycode, позволяющий обеспечить корректную работу в Интернете доменных имён с использованием символов, которые поддерживаются в стандарте Unicode, например, 普遍接受-测试.世界, ڪاٺو لڳو, тестовая-зона.рф и т. д. Сама система доменных имён (DNS) по-прежнему работает с кодировкой ASCII, но на уровне приложений благодаря стандарту IDNA происходит преобразование интернационализированных доменных имён в символы Unicode, поэтому пользователи имеют возможность работать с доменными именами на своём родном языке.

**- А почему ты сама начала заниматься этой темой? Профессиональный интерес, женское любопытство, возможности развития?**

- У меня было несколько подходов к этой теме. Еще в 2007-2008 годах, когда я работала в Координационном центре в отделе маркетинга, я с самого начала подключилась к проекту по созданию домена .рф. Я даже администрировала страничку в Wikipedia, которая была специально разработана ICANN для будущих IDN-доменов, там был текст на английском про этот мировой проект, про идею создания интернационализированных доменов, и я его переводила на русский язык, следила за его актуальностью, собирала комментарии, отвечала на вопросы пользователей. Это был пилотный проект для информирования сообщества в разных странах, я вела русскоязычную версию. Потом проект был закрыт, но появилась рабочая группа в рамках ICANN, которая уже вплот-

ную занялась вопросами создания национальных IDN для заинтересованных стран. Я вошла в эту группу вместе с тогдашним директором КЦ Андреем Колесниковым.

Итогом работы этой группы стал так называемый Fast Track-процесс, который позволил по ускоренной процедуре создавать страновые домены на национальных языках. И именно по этой процедуре и был создан домен .рф. Перед его появлением мы проводили опросы общественного мнения у нас в России о том, интересно было бы сообществу поддерживать кириллический домен или нет, работать с ним. Были тесты с Microsoft, мы проверяли работу браузеров с IDN-доменами. В общем, проводилась очень большая подготовительная работа, готовилась база для того, чтобы домен .рф появился. А вот в самом появлении домена .рф на свет я по своим личным причинам не участвовала – прямо перед появлением .рф на свет появилась моя старшая дочь.

К теме IDN-доменов я вернулась в 2011-2013 годах, когда участвовала в проекте по созданию новых общих доменов верхнего уровня, тогда у нас был создан кириллический домен .дети. Потом у меня был ещё один перерыв, ну а с 2019 года я полностью погрузилась в эту тему, и был инициирован проект «Поддерживаю РФ».

Идея появления такого проекта, где бы обсуждались технические аспекты внедрения универсального принятия всех допустимых доменных имён и почтовых адресов в программном обеспечении и предлагались пути их решения, возникла незадолго до 10-летия домена .рф. Тогда всем уже стало понятно, что IDN-домены, конечно, работают, что они стали неотъемлемой частью Интернета, но не всегда и не везде они поддерживаются на 100%, в первую очередь, в сервисах электронной почты. Кроме того, к этому моменту стала складываться и международная практика по работе над внедрением универсального принятия. Ведь сложности с универсальным принятием касаются не только доменов на национальных алфавитах, но и новых латинских доменов общего пользования, появившихся в ходе программы ICANN New gTLD, длина которых составляет более трёх латинских символов в отличие от привычных .com, .net, .org, а также с адресами электронной почты, включающими такие доменные имена после знака @. С появлением такого большого количества новых доменов верхнего уровня выяснилось, что не всё программное обеспечение способно их обрабатывать. При этом новыми доменами – и IDN, и с использованием латинского алфавита – стали пользоваться всё больше и больше людей, и волей-неволей на это пришлось обратить внимание и интернет-компаниям, и международным организациям, и компаниям-разработчикам. Фактически это стало новой волной, когда в процесс обеспечения универсального принятия включилось много разных заинтересованных сторон.

Большую роль в раскручивании этой темы сыграли бизнес-интересы крупных международных компаний, в некоторых странах подключилось государство. Тогда и мы в Координационном центре решили, что надо более внимательно отнестись к этому вопросу, надо его изучить и посмотреть, как можно улучшить поддержку нашего домена .рф во всём программном обеспечении как на российском уровне, так и на международном.

**- Как думаешь, если вдруг удастся достичь вселенского универсального принятия – это повлияет на число регистраций доменных имён в «нелатинских» доменных зонах, в первую очередь, в .рф?**

- Честно говоря, я для себя такой задачи не ставлю. Мне эта тема импонирует тем, что она направлена на то, чтобы обеспечить стопроцентную работоспособность тех услуг для интернет-пользователей, которые уже существуют. Мы заинтересованы в том, чтобы услуги, которые так или иначе связаны с доменом .рф и базируются на этом домене, например, хостинг или почтовые сервисы с использованием доменов .рф, должны быть доступны и оказываться качественно, так, чтобы пользователи, выбравшие для себя эту доменную зону и зарегистрировавшие доменное имя в зоне .рф, не испытывали никаких трудностей, когда они с этим доменом работают. Для пользователей это всё должно происходить незаметно и не должно быть разницы, когда они используют домен традиционный латинский или домен в .рф; везде, где происходит обработка доменного имени, всё должно проходить гладко и без ошибок.

Если посмотреть на статистику домена .рф, то мы видим, что домен, можно сказать, стабилен, в домене регистрируется 500-600 новых доменных имён ежедневно. Это рыночный спрос на доменные имена в этой зоне сегодня. Полагаю, что этот спрос может увеличиваться по мере роста цифровой грамотности пользователей и роста их желания разместить в сети свой сайт с уникальным адресом или зарегистрировать электронную почту на русском языке.

Сегодня созданием сайтов занимаются в основном предприниматели, бизнес, продвигающие себя и свои сервисы в Интернете. Поэтому, если экономика развивается, создаются новые компании, новые проекты или, возможно, появятся совершенно новые онлайн-сервисы, которые будут так или иначе использовать доменные имена, домен .рф, несомненно, будет ещё расти.

**- Согласно статистике 2024 года, русский язык находится на шестом месте по объёму контента в Интернете, при этом именно русскоязычный домен .рф является самым крупным IDN-доменом как среди кириллических, так в целом среди всех IDN в мире. А вот в Китае зарегистрировано 57 доменов верхнего уровня на китайских иероглифах, при этом китайский язык не входит в топ-10 самых распространённых языков по объёму контента в Интернете. Так в чём уникальность домена .рф? В чём его сила?**

- Думаю, что на это влияет несколько факторов. По данным международных исследований, на русском языке в мире говорит около 255 миллионов человек. Русский язык входит в топ-10 самых распространённых языков по числу говорящих. В России на русском языке говорят 146 миллионов человек, и это государственный язык нашей страны. То есть в мире существует достаточно большое русскоговорящее сообщество, а в России русскому



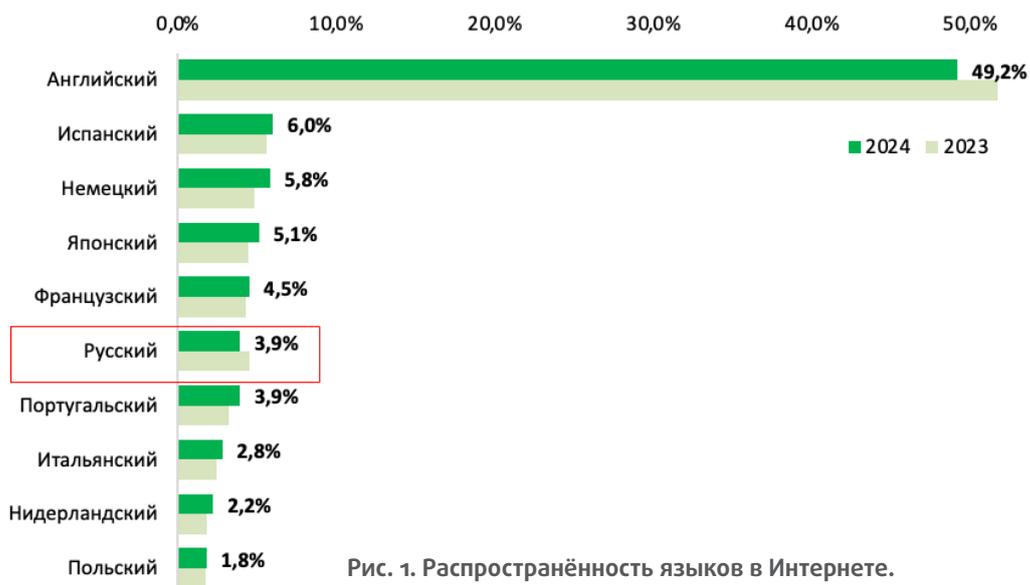


Рис. 1. Распространённость языков в Интернете.

языку уделяется основное внимание.

Одно из следствий такой распространённости языка — то, что большинство программных продуктов, и российских, и зарубежных, локализованы на русском языке. Есть пользовательские интерфейсы, документация, служба поддержки на русском языке и так далее. Это способствует тому, что пользователи, которые владеют русским языком, совершенно спокойно могут использовать различные онлайн-сервисы, приложения и сайты на русском языке, потреблять и создавать русскоязычный контент.

Ещё один важный фактор — это высокий уровень проникновения Интернета в нашей стране, 93%, то есть к Интернету подключено практически всё население России. У нас прекрасно работают государственные электронные сервисы, развит онлайн-банкинг, доступны маркетплейсы, социальные сети, и даже дети в начальной школе уже выполняют цифровое домашнее задание. Для российских пользователей Интернет действительно стал частью реальности, частью повседневной жизни.

Мы проводим в Интернете по 5-6 часов в день и обычно для этого нам не нужно переключаться на какой-то другой язык, практически все возможности Интернета доступны на русском. Мы счастливые люди. Но вот когда речь идёт про доменные имена и адреса электронной почты, тут почему-то получается, что без переключения на английский язык не обойтись. И идея создания домена .rf во многом заключалась и заключается в том, чтобы предоставить пользователям возможность даже адреса в сети Интернет набирать на своём родном языке. Кроме этого, русскоговорящим пользователям действительно легко запоминать и удобно набирать адреса сайтов или электронной почты по-русски, даже сложные аббревиатуры или длинные адреса набирают без опечаток и ошибок в написании. Так, по статистике, больше всего доменных имен в .rf содержат от семи до 11 символов.

**- А как ты считаешь, зависит ли рост объёма контента на русском языке от того, сколько доменных имён зарегистрировано в домене .rf?**

- Мне кажется, что есть обратная зависимость. IDN-домены, по

сути, сообщают пользователю о том, на каком языке ему будет предложен контент сайта. И поскольку сайты на русском языке создаются и продвигаются, то для их владельцев логичнее использовать русскоязычные доменные имена, чтобы сразу показать, что их проекты или сервисы предназначены для людей, говорящих на русском языке. Естественно, каждый бизнес, каждый предприниматель хочет сделать свои сервисы более удобными и доступными для клиентов. И когда вдруг в рамках русскоязычной коммуникации возникают латинские символы, это вызывает диссонанс.

**- Каким ты видишь будущее домена .rf, например, через 25 лет?**

- Мне кажется, что мы плавно движемся к тому, чтобы такие домены, как .rf, да и в целом интернет-идентификаторы на национальных языках стали естественной частью Интернета. Интернет сегодня сильно отличается от того, каким он был 25 лет назад. Тогда в Интернете только-только начали появляться пользователи, а сегодня из 8,2 миллиарда населения планеты почти 5,6 миллиарда людей подключены к Интернету, и это 68% землян. Ещё через 25 лет, предполагаю, подключение к сети будет 100-процентным, ну или близко к этому показателю. То есть все люди будут иметь доступ к цифровому миру. Но надо понимать, что это люди из разных стран, и здесь есть интересный момент.

Например, на английском говорят 1,5 миллиарда жителей Земли, а Интернетом пользуются 5,6 миллиарда человек. Получается, что англоговорящих среди пользователей где-то около 20%, а объём контента на английском языке стал снижаться ниже 50%. То есть Интернет уже многоязычен, и сейчас нет такого правила, что, выходя в Интернет, ты должен знать английский язык. Поэтому можно с уверенностью сказать, что Интернет на национальных языках будет расти и развиваться — ведь прирастать сеть будет в дальнейшем в основном не-англоговорящими пользователями.

Возможно, появятся какие-то новые сервисы на базе искусственного интеллекта, которые научатся за человека осуществлять некое автоматическое переключение между языками, будут развиваться онлайн-переводчики, которые станут моментально переводить с одного языка на другой и письменную,

и устную речь, да ещё и с учётом культурных особенностей или стилистики, уместной в той или иной ситуации.

А поддержка доменных имён и адресов электронной почты на национальных языках — это часть этой большой работы по развитию многоязычного Интернета.

Система доменных имён (DNS) была создана на заре развития Интернета, но до сих пор активно используется и пока для неё нет замены. Кстати, те, кто говорят, что электронная почта доживает свои последние дни, тоже неправы. По последним исследованиям люди, в том числе молодёжь, активно пользуются электронной почтой — речь идёт о 70–75% пользователей.

Поэтому очень важно обеспечить совместимость программного обеспечения. ПО должно уметь работать со всем ассортиментом доменных имён, независимо от того, на каком они языке или сколько в них символов — два, три или больше, верхний уровень или это четвёртый уровень доменного имени. И тут очень важно, чтобы разработчики, производители ПО и сервисов начали шире смотреть на свои продукты и внедрять принципы поддержки многоязычия, в том числе в части обработки многоязычных доменных имён и адресов электронной почты.

#### - Проект «Поддерживаю.РФ» работает уже шесть лет. Какие, на твой взгляд, главные результаты этих шести лет и какие планы на будущее?

- Собственно, проект мы запускали для того, чтобы помочь разработчикам и производителям ПО создавать продукты, которые способны работать с многоязычными доменами и с многоязычными адресами электронной почты. И так как Координационный центр сам не является разработчиком ПО, то мы решили, что будем аккумулировать на специально созданном сайте доступные инструменты и практическую информацию по данной тематике для технического сообщества. Мы отслеживаем, что происходит в этой сфере на международном уровне, переводим и публикуем интересные материалы, сами делаем различные исследования, тестируем программные продукты, собираем и публикуем мануалы по установке ПО, проводим онлайн-семинары и тренинги, консультируем, даже предоставляем кириллические почтовые адреса для тестирования ПО. У нас можно получить подтверждение о реализации критериев

универсального принятия домена .рф в вашем программном продукте.

За время работы проекта мы поняли, что далеко не все технические специалисты знают о том, что существуют интернет-стандарты по работе с интернационализированными доменными именами (IDNA) и интернационализированной электронной почтой (EAI), т.е. RFC, которые были разработаны международным сообществом в IETF. Первый RFC, описывающий стандарт IDNA, появился ещё в 2003 году, а новая версия этого стандарта доступна с 2008 года. Что касается стандарта EAI, то этот набор RFC был разработан в 2012 году. Кстати, информация о ключевых стандартах тоже доступна на нашем сайте.

Поэтому мы пытаемся упростить поиск информации и материалов по теме, собираем всё в одном месте, плюс объясняем на практике, как это применять. На самом деле, вся документация, необходимая обычно техническим специалистам, уже разработана, есть примеры готового ПО, библиотек с поддержкой IDN и EAI, есть инструменты для тестирования.

Наша главная цель — это создание экосистемы программного обеспечения, которая бы корректно работала с доменом .рф и с кириллической почтой в первую очередь, а также с любыми интернационализированными доменными именами и почтовыми адресами на всех языках, которые поддерживаются в стандарте Unicode.

Два года назад мы также начали работать с российскими вузами, которые готовят технических специалистов, а иногда и лингвистов. И здесь наша цель — подготовить молодые кадры и обеспечить их знаниями и навыками, которые помогут им в дальнейшем развивать Интернет и новые технологии с учётом принципов многоязычия. Нам важно, чтобы в их сознании интернационализированные домены и почтовые адреса уже являлись неотъемлемой частью Интернета, и они захотели двигаться дальше, придумывать новые полезные сервисы с их использованием. ■

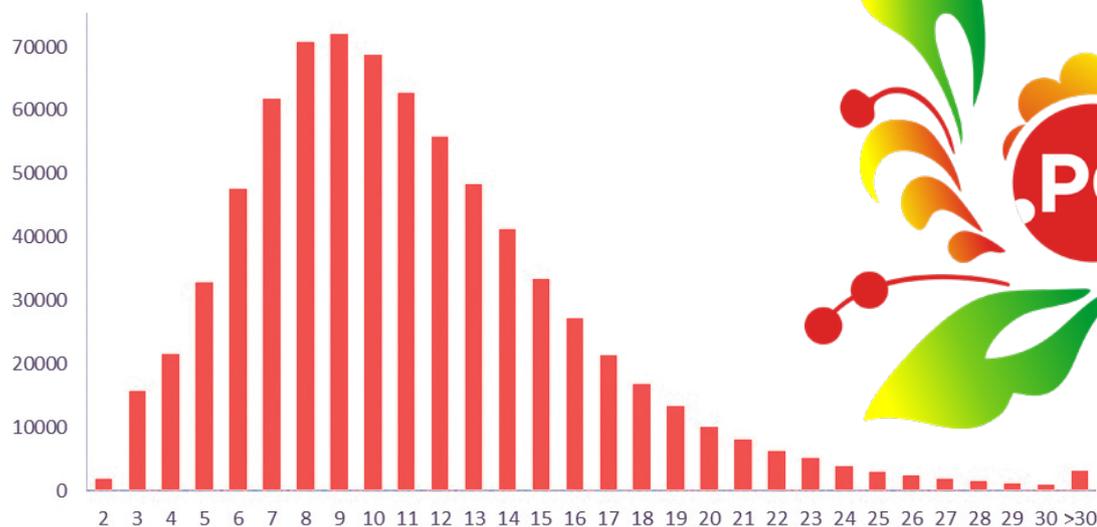


Рис. 2. Распределение доменных имён в домене .рф по количеству символов.

# Новости науки и техники

## Власти Чили изучат возможность прокладки подводного оптоволоконного кабеля связи в Антарктиду

*Решение о прокладке кабеля может быть принято в конце 2026 года*

Министерство транспорта и телекоммуникаций Республики Чили совместно с Банком развития Латинской Америки и Карибского бассейна заключило контракт с исследовательскими компаниями Pioneer Consulting и Saliency Consulting. Компаниям предстоит изучить возможность прокладки подводного оптоволоконного кабеля связи между Чили и Антарктидой. Предполагается, что кабель протяжённостью не менее 1000 километров может быть проложен между населённым пунктом Пуэрто-Уильямс, который находится неподалёку от Мыса Горн и спорит с Пунта-Аренас за право считаться самым южным городом на планете, и антарктическим островом Кинг-Джордж.

Антарктида является единственным континентом Земли, не имеющим оптоволоконных кабелей связи. Можно объяснить это тем, что она необитаема, но это не совсем верно. Даже в суровое зимнее время численность персонала антарктических научных станций составляет порядка тысячи человек, летом же она возрастает до 4,4 тысячи человек. Ещё около тысячи человек постоянно находятся на судах в прибрежных антарктических водах. Кроме того, летом тот же остров Кинг-Джордж посещают многочисленные туристические группы. Все эти люди нуждаются в быстром и надёжном интернет-соединении, которое может быть особенно важно для передачи научных данных. В настоящее время связь обеспечивается спутниковыми терминалами, возможности которых, естественно, несопоставимы с возможностями волоконно-оптического кабеля.

Впрочем, интерес Чили к прокладке кабеля, вполне возможно, имеет и другие причины. Как предполагается, Антарктида обладает огромными запасами полезных ископаемых, включая нефть и газ. Добыча их на континенте запрещена международными договорами, но срок действия договоров истекает через 20 с небольшим лет. И нельзя исключать, что соглашения не будут продлены. В этом случае контроль над единственным оптоволоконным кабелем, соединяющим Антарктиду с миром, станет крупным козырем для властей Чили. Исследование, которое изучит технические и экономические возможности прокладки кабеля, а также юридические и экономические вопросы, связанные с его прокладкой, планируется завершить в конце 2026 года.

Источник:  
Total Telecom, <https://totaltele.com/studies-begin-on-chile-antarctica-submarine-cable/>

## Компания Vodafone будет «латать дыры» в сети с помощью дронов

*Технология беспроводной оптической связи позволяет передачу данных с помощью лазера на расстояние до 20 км*

Компания Vodafone сообщила о том, что проводит тестирование нового метода восстановления сети в случае повреждения кабелей связи. Метод предусматривает использование пары беспилотных летательных аппаратов, оснащённых оборудованием от Taara Project. Это проект компании X (не путать с бывшим Twitter), входящей в Alphabet, родительский холдинг Google.

Ранее она работала над проектом Loop, который предусматривал создание беспроводной сети с помощью дрейфующих в стратосфере аэростатов. В 2021 году проект был закрыт ввиду низкой рентабельности. Однако в ходе работы над ним была создана технология беспроводной оптической связи (Free Space Optical Communications - FSOC). Она предусматривает передачу данных в прямой видимости с помощью лазера со скоростью до 20 Гб/с.

Развитием этой технологии и занимается Taara Project. По словам представителей Vodafone, предварительные испытания, проведённые в испанской Севилье, продемонстрировали успешную передачу данных между двумя дронами на расстояние 3 км. Впрочем, испытания самого проекта Taara Project еще в 2021 году показали возможность передачи данных с помощью FSOC на расстояние до 20 км.

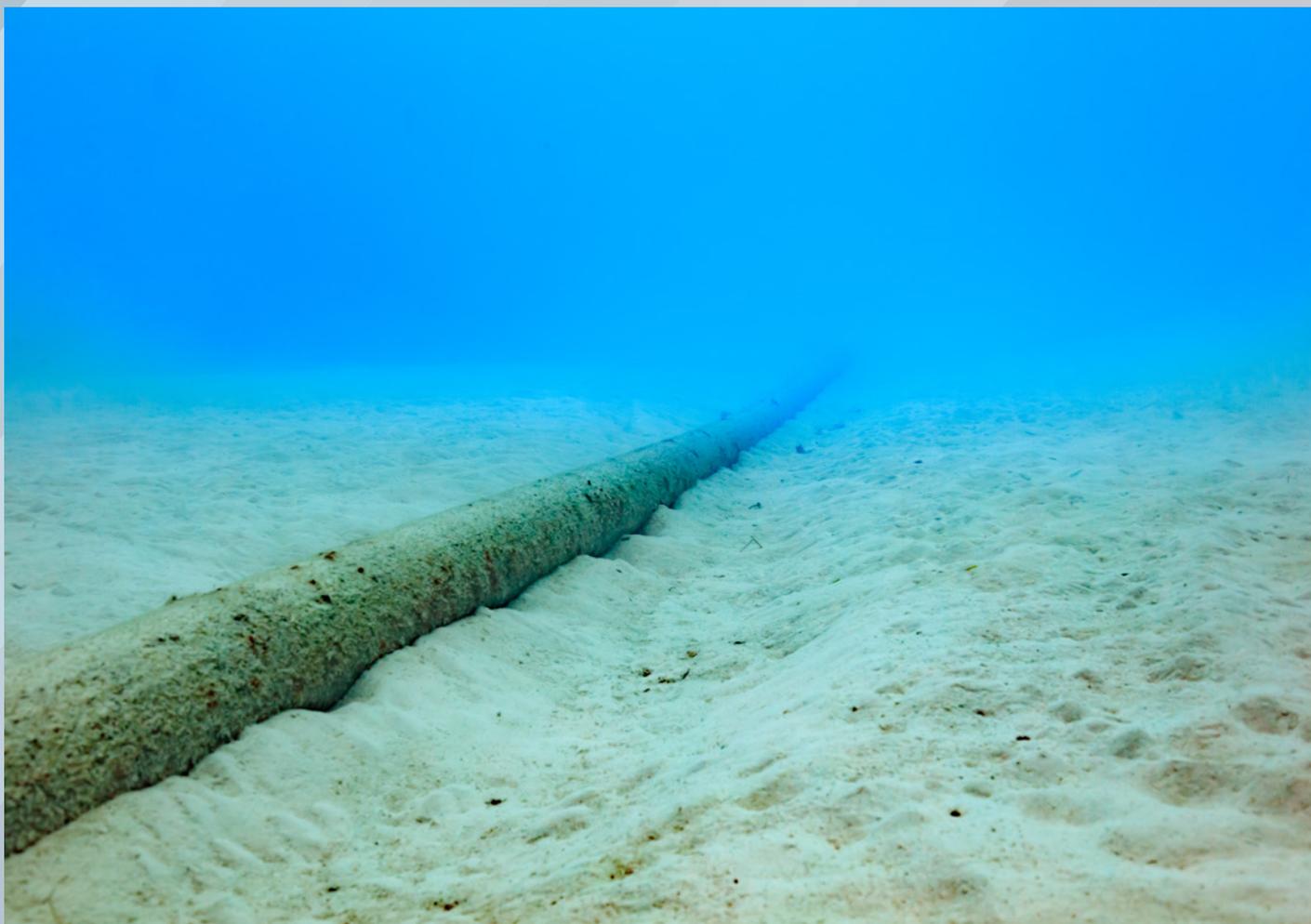
Использование дронов позволит операторам связи максимально оперативно восстанавливать соединение при повреждении кабелей, например, вследствие строительных работ или в результате актов вандализма. Также этот метод может быть чрезвычайно полезен для быстрого восстановления связи в зонах, пострадавших от стихийных бедствий или техногенных катастроф.

Источник:  
Total Telecom, <https://totaltele.com/vodafone-using-drones-to-plug-holes-in-damaged-networks/>

## Подводные коммуникационные кабели могут служить для получения данных о состоянии мирового океана

*Что препятствует внедрению кабелей SMART*

Подводные волоконно-оптические коммуникационные кабели служат сегодня основой связности мировой информационной сети. Их общая протяжённость составляет уже порядка 1,4 миллиона километров, а скорость передачи данных по ним достигает 300 Тб/с. Развитие технологий искусственного интеллекта и необходимость создания всё более



мощных дата-центров неизбежно влекут за собой и потребность во всё большем числе подводных коммуникационных кабельных систем.

Но эти кабели могут использоваться не только для передачи данных. Международный союз электросвязи, Всемирная метеорологическая организация и Межправительственная океанографическая комиссия ЮНЕСКО развивают инициативу SMART - аббревиатура от Scientific Monitoring and Reliable Telecommunications («научный мониторинг и надёжные коммуникации»). Она предусматривает использование нового типа кабелей, оснащённых сенсорами. Такие кабели полезны прежде всего их операторам: датчики отслеживают уровень вибрации и предупреждают об опасности повреждения, например, якорями судов. Но кроме того, информация этих сенсоров потенциально позволяет оперативно предупредить о подводных землетрясениях - и, значит, о зарождающихся цунами. А данные датчиков температуры воды помогли бы лучше понимать и прогнозировать глобальные климатические изменения.

Ряд стран - и прежде всего Португалия и Франция - уже активно инвестируют в создание таких кабелей. Но в целом прогресс приходится признать крайне медленным: впервые идея кабелей SMART была высказана еще в 2010 году, но на сегодняшний день реализуются лишь два проекта с их использованием. Тому есть несколько причин, и первая из них - законодательного характера. Прокладка подводных коммуникационных кабелей регулируется главным образом Конвенцией ООН по морскому праву от 1982 года. Есте-

ственно, ни в ней, ни в более поздних межгосударственных соглашениях нет упоминания кабелей SMART. Это создаёт серьезные трудности с согласованием прокладки кабелей нового поколения. Более того, в условиях геополитической напряжённости власти некоторых стран могут рассматривать оснащённые сенсорами кабели как инструмент сбора в том числе и разведывательных данных.

Есть и трудность экономического порядка. По оценкам экспертов, оснащение кабелей сенсорами повышает их стоимость примерно на 15%. И у операторов кабельных сетей нет очевидных способов компенсировать дополнительные траты. Вероятно, в данном случае не обойтись без государственной поддержки - в виде субсидий или налоговых льгот.

И тем не менее, переход к использованию кабелей SMART, несомненно, принесёт значительную пользу. Кстати, в феврале нынешнего года компания Meta (признана экстремистской организацией и запрещена в РФ) анонсировала проект Waterworth Project. Он предусматривает прокладку самой масштабной в мире подводной коммуникационной кабельной системы протяжённостью порядка 50 тысяч километров, которая соединит все пять континентов. Если хотя бы часть использованных при реализации Waterworth Project кабелей будут кабелями SMART, это станет отличным стимулом для более активного их использования.

Источник:  
The Conversation, <https://theconversation.com/submarine-cables-keep-the-world-connected-they-can-also-help-us-study-climate-change-251046>

# Новости доменной индустрии

## Координационный центр доменов .RU/.РФ стал хранителем «ключа от Интернета»

*Ключ в КЦ передал Дмитрий Бурков – отставной криптоофицер Западного центра ICANN*

Пятого февраля в Координационном центре доменов .RU/.РФ состоялась торжественная церемония передачи на хранение первичного металлического ключа от сейфа-хранилища, в котором находится смарт-карта хранения модулей HSM корневой зоны DNSSEC, отвечающая за проверку подлинности данных в системе доменных имён (DNS). Ключ в Координационный центр передал Дмитрий Бурков, доверенный представитель сообщества и закончивший свою работу криптоофицер Западного центра ICANN.

В церемонии приняли участие представители Координационного центра – руководитель отдела по работе с регистраторами и пользователями Георгий Георгиевский, заместители директора КЦ Ирина Данелия и Сергей Копылов, сотрудники отдела внешних коммуникаций. Подпись на акте передачи ключа поставили директор Координационного центра Андрей Воробьёв и Дмитрий Бурков.

«Сегодня Координационный центр принял на хранение уникальный «ключ от Интернета», имеющий историческую и культурную ценность. Дмитрий Бурков – настоящая легенда российского Интернета, в течение многих лет с 2010 года он входил в число 14 криптоофицеров – «хранителей ключей», которые отвечают за безопасность мирового Интернета. И хотя роль этого конкретного ключа теперь уже чисто символическая, он имеет огромную историческую и культурную ценность, и ответственность за его сохранность возложена на Координационный центр», – отметил Андрей Воробьёв.

«Церемонии подписания ключом DNSSEC корневой зоны DNS проводятся уже много лет – как на мировом уровне, так и на уровне отдельных доменных зон. Для доменных зон .ru и .rf генерация ключей KSK (key signing key, «ключ подписи ключа» – ключ для подписи ресурсной записи DNSKEY, содержащей параметры DNSSEC для домена верхнего уровня) проходит ежегодно, а отвечают за сохранность и безопасность ключа четыре криптоофицера: два сотрудника Координационного центра и два сотрудника «Технического центра Интернет», – рассказал Георгий Георгиевский.

Напомним, что внедрение технологии DNSSEC началось в конце 2000-х годов. DNSSEC использует два типа ключей – одним подписывается зона (ZSK, zone signing key), другим подписывается



набор ключей (KSK, key signing key). DNSSEC работает на основе криптографических подписей, которые подтверждают подлинность и целостность информации в DNS. Сегодня технологию DNSSEC используют большинство национальных и практически все крупнейшие общие домены верхнего уровня. Российские домены верхнего уровня .ru и .rf были подписаны в конце 2012 года.

Источник:  
сайт Координационного центра доменов .RU/.РФ, <https://cctld.ru/media/news/kc/37477/>

## Официально истёк «срок жизни» протокола Whois

*Регистратуры и регистраторы имеют право более не поддерживать предоставление данных о регистрантах доменных имён посредством Whois*

Протокол Whois уходит в историю. День 28 января 2025 года обозначен в регистрационных соглашениях корпорации ICANN с регистратурами и аккредитационных соглашениях с компаниями-регистраторами как последний день срока, на протяжении которого предоставление данных о регистрантах доменных имён являлось обязательным. Дальнейшее использование

Whois является исключительно добровольным, и отказ от него не повлечёт за собой каких-либо санкций.

На смену Whois окончательно приходит протокол доступа к данным о регистрациях Registration Data Access Protocol (RDAP). Впрочем, ресурс Domain Incite, сообщая эту новость, выражает уверенность в том, что ещё на протяжении долгого времени многие регистратуры и регистраторы будут параллельно использовать и RDAP, и Whois. Более того, вполне возможно, что и сам протокол RDAP многие люди, тесно связанные с доменным бизнесом, продолжают по старой памяти называть Whois - настолько это понятие «вошло в ДНК» доменной индустрии.

При этом данные, предоставляемые RDAP, во многом совпадают с данными Whois. А те, кто запрашивает их посредством веб-интерфейса - например, сервиса lookup.icann.org на сайте корпорации ICANN, - вероятнее всего, вообще не заметят никакой разницы. Зато проблемы возникнут у тех, кто использует специализированное ПО для доступа к Whois через порт 43: им придётся повозиться с настройками, чтобы получаемые в ответ на запрос данные RDAP отображались в адекватном формате.

Самое же главное состоит в том, что персональные данные регистрантов, скрытые теперь в Whois, точно так же не будут отображаться и в RDAP: Общий регламент по защите данных (GDPR), принятый Европейским Союзом, и другие законы, направленные на защиту конфиденциальности, в равной степени распространяются на него в той же мере. Единственная возможность получить доступ к этим данным - подать запрос непосредственно регистратору доменного имени или через сервис Registration Data Request Service корпорации ICANN. И надеяться, что этот запрос будет сочтён достаточно обоснованным.

Источник:  
Domain Incite, <https://domainincite.com/30696-whois-officially-died-today>

## Компания Tucows без всякой помпы объявила о предстоящем крупнейшем в истории транзите доменной зоны

*Новым техническим оператором национального домена Индии .in станет компания Tucows*

Компания Tucows станет новым техническим оператором национального домена Индии .in, сменив в этом качестве компанию GoDaddy. Ресурс Domain Incite, сообщая эту новость, обращает внимание на то, насколько буднично и обыденно объявил о ней глава Tucows Эллиот Носс (Elliot Noss). Информация о заключении контракта с регистратурой National Internet Exchange of India (NIXI), управляющей индийской доменной зоной, оказалась помещена лишь на четвертую страницу доклада Носса по итогам четвертого квартала прошлого года.

Между тем, речь идёт о весьма важном и даже исключительном событии. Предстоящая смена технического оператора домена .in станет транзитом самого большого числа доменных имён за всю историю системы DNS. Ранее рекордным был транзит национального домена Австралии .au в 2018 году от компании Neustar к Afilias. На тот момент количество регистраций

в доменной зоне .au составляло порядка 3,1 миллиона. Регистратура NIXI не публикует информацию о числе зарегистрированных имён в домене .in, однако, согласно данным последнего отчёта Domain Name Industry Brief от компании Verisign, по состоянию на конец 2024 года в национальном домене Индии насчитывалось около 4,1 миллиона регистраций.

Каким образом Tucows удалось выиграть конкуренцию у компании GoDaddy, выполнявшей функции технического оператора .in ранее, неизвестно. Но логично предположить, что предложенная ею стоимость обслуживания оказалась более низкой. Наблюдатели отмечают, что столь крупные контракты вообще редко оказываются очень уж прибыльными для технических операторов. Однако они, безусловно, повышают авторитет и укрепляют репутацию компаний, позволяя рассчитывать на новые выгодные сделки в будущем.

Источник:  
Domain Incite, <https://domainincite.com/30758-largest-back-end-switch-ever-as-godaddy-loses-deal>

## WordPress предлагает регистрацию доменных имён сроком на 100 лет

*Регистрантам предлагается верить в то, что компания Automattic просуществует ещё не менее века*

Компания Automattic, дочерним предприятием которой является популярнейший сервис WordPress, объявила о любопытном новшестве. Будучи ещё и аккредитованным корпорацией ICANN доменным регистратором, она предлагает своим клиентам возможность регистрации доменного имени сроком на 100 лет. Услуга распространяется на имена в общих доменах верхнего уровня .com и .net (регистратура Verisign), .org (Public Interest Registry) и .blog (регистратурой которого выступает сама же компания Automattic). Стоимость услуги составляет 2 тысячи долларов.

Трудно сказать, насколько это окажется выгоднее ежегодного продления регистрации доменного имени в тех же доменах .com или .net на протяжении ста лет. Но главный вопрос даже не в этом, а в том, просуществует ли сама компания Automattic или любая из упомянутых регистратур столь долгий срок. И сами регистратуры предпочитают более осторожный подход: ни одна из них не предлагает возможности регистрации доменного имени сроком более чем на 10 лет. Впрочем, Automattic - не первая компания, которая делает столь далеко идущее предложение. Так, ресурс Domain Name Wire, сообщая эту новость, напоминает, что доменный регистратор Erik еще в 2018 году представил план «вечного продления» регистрации доменных имён - и всего за 420 долларов. С тех пор компания успела прекратить свое существование в прежнем виде, а её клиенты пытаются вернуть свои деньги через суд - и пока с переменным успехом.

Источник:  
Domain Name Wire, <https://domainnamewire.com/2025/02/12/wordpress-introduces-100-year-domain-registrations/>



Интернет изнутри ➞