№25
Ноябрь 2026

indata
ФОНД РАЗВИТИЯ СЕТЕВЫХ ТЕХНОЛОГИЙ «ИНДАТА»

Интернет изнутри

ИЗМЕРЕНИЯ В ИНТЕРНЕТЕ

Взгляд со стороны
Зачем нам нужен RIPE Atlas и что это вообще такое?
с. 11

Графы как представления моделей Интернета
Какую роль играют графы для визуализации логики взаимодействия элементов вычислительных сетей?
с. 30

Измерение DNS поверх IPv6
Сегодня уже около 75% пользователей Интернета способны выполнять DNS-запросы по протоколу IPv6
с. 50

Эпоха цифровой прозрачности
Как меняется регулирование российских национальных доменов в зонах .ru, .рф и .su
с. 62

Исследование российского рынка фиксированной связи
Результаты исследования российского рынка фиксированной связи на основе данных Роскомнадзора и ФНС о деятельности региональных операторов
с. 66

От секундомера до микросекунды
Эволюция и технологии хронометража в лёгкой атлетике
с. 86

Интернет-измерения: каков вопрос, таков ответ

Измерять в Интернете можно по-разному — всё зависит от того, какую задачу мы решаем

с. 16

Содержание:

Интернет в цифрах
с. 2 Инфографика

Измерения в Интернете
с. 4 Измерения, выполняемые при обеспечении целостности и устойчивости функционирования сети связи общего пользования

с. 11 Взгляд со стороны: использование RIPE Atlas для мониторинга связности, маршрутизации и DNS

Технология в деталях
с. 16 Интернет-измерения: каков вопрос, таков ответ

с. 26 Использование обратного трафика (backscatter) QUIC для анализа конфигураций развёртывания гипергигантов

с. 30 Графы как представления моделей Интернета

с. 36 Matisse: визуализация задержек в Интернете в виде многообразий

Инфраструктура
с. 44 Платформа для макроскопических исследований российской интернет-инфраструктуры: архитектура, методы измерений и визуализация данных

с. 50 Измерение DNS поверх IPv6

с. 56 Контроль качества инфраструктуры Интернета – ICANN SLAM

с. 62 Эпоха цифровой прозрачности: как меняется регулирование российских национальных доменов в зонах .ru, .рф и .su

Технологии и рынок
с. 66 Исследование российского рынка фиксированной связи: от агрегированных оценок к анализу отдельных операторов и регионов

Образование и наука
с. 73 Методика измерений и оценка компромисса параметров передачи данных телеметрии IoT-устройств в помещениях по радиоканалу LoRa

Технология и право
с. 80 Понятие и специфика исследований измерений Интернета

Вокруг технологии
с. 86 От секундомера до микросекунды: эволюция и технологии хронометража в лёгкой атлетике

Новости
с. 92 Новости науки и техники

с. 94 Новости доменной индустрии

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

Выпуск №25,
дата выхода:
Ноябрь 2026 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

Omnia in mensura

Дорогой читатель,

Как и всякая открытая система, Интернет предоставляет неисчерпаемые возможности для измерений. И в то же время Интернет является одной из наиболее сложных и масштабных технических систем, созданных человечеством. Его развитие, надёжность и безопасность невозможно оценивать без постоянных наблюдений и измерений. Однако в отличие от традиционных инженерных объектов Интернет не имеет единого центра управления и представляет собой распределённую систему, состоящую из сотен тысяч сетей, устройств и сервисов. Поэтому измерение Интернета — это не только техническая задача, но и отдельная научная дисциплина, объединяющая сетевые технологии, математику, статистику, анализ данных и визуализацию.

В этом номере мы хотим познакомить читателей с современными подходами к измерению Интернета, показать существующие исследовательские и операционные практики, а также продемонстрировать, как результаты измерений используются для принятия технических, организационных и бизнес-решений.

В рубрике «Технология в деталях» мы подобрали интересные исследования по измерению различных параметров Интернета и услуг. Например, в статье Йонаса Мюкке «Использование обратного трафика QUIC для анализа конфигураций развёртывания гипергигантов» рассказывается, как изучение «нежелательного трафика», отражённого от серверов QUIC, позволяет идентифицировать детали инфраструктуры, включая конфигурации балансировщиков нагрузки и схемы развёртывания в сетях. Джефф Хьюстон рассказывает о неочевидных аспектах измерения доступности услуги DNS по протоколу IPv6. А Павел Храмцов предлагает философский взгляд на проблему измерений в Интернете в целом в своей статье «Интернет-измерения: каков вопрос, таков ответ».

Второй блок статей, объединённый под рубрикой «Инфраструктура», поднимает вопросы инфраструктурных измерений, но также рассказывает и об измерительной инфраструктуре как таковой. Так, в статье «Взгляд со стороны: использование RIPE Atlas для мониторинга связности, маршрутизации и DNS» рассматривается система распределённых измерительных зондов RIPE Atlas и её применение для мониторинга качества услуг. А Николай Гавриченко рассказывает об исследовательской платформе Фонда развития сетевых технологий «ИнДата», предназначенной для макроскопического исследования связности и качества взаимодействия в российском сегменте сети Интернет.

Конечно, мы продолжаем поддерживать наши стандартные разделы. В разделе «Образование и Наука» мы познакомим вас с методикой измерений параметров передачи данных телеметрии IoT-устройств в помещениях по радиоканалу LoRa. В разделе «Технология и Право» Мадина Касенова предлагает анализ проблематики измерений Интернета. А в «Новостях» мы познакомим вас с интересными фактами об Интернете и доменной индустрии.

Наконец, в разделе «Вокруг технологии» Александр Бабаев рассказывает захватывающую историю эволюции спортивного хронометража.

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**.

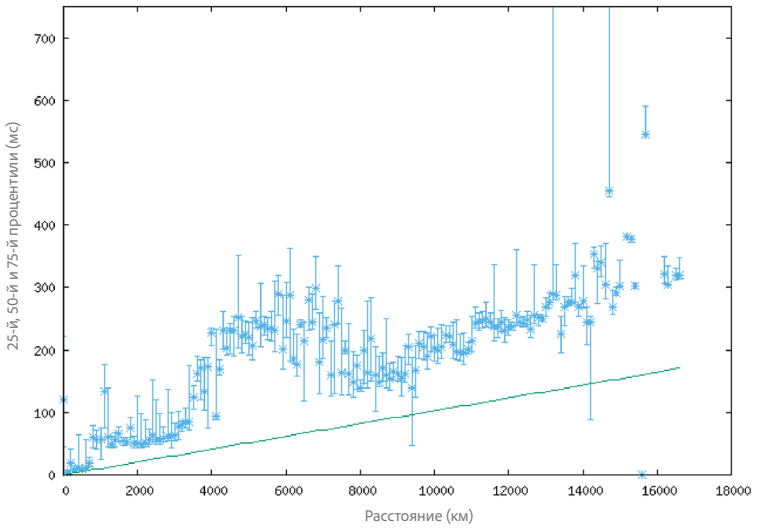
Редакция журнала



Интернет в цифрах

Квартили RTT в зависимости от географического расстояния

На графике показаны квартили — 25-й, 50-й и 75-й процентили — времени круговой задержки (RTT) в зависимости от географического расстояния от измерительного узла CAIDA в Москве. Сопоставление RTT с географическим расстоянием позволяет оценить, насколько именно расстояние определяет скорость передачи пакетов по сети. Представление данных в виде квартилей позволяет исключить влияние отдельных выбросов и получить более наглядное представление о характерных значениях RTT. Как правило, для измерительного узла, имеющего высокоскоростное соединение с остальной частью Интернета, медианное значение RTT должно примерно линейно возрастать с увеличением расстояния.



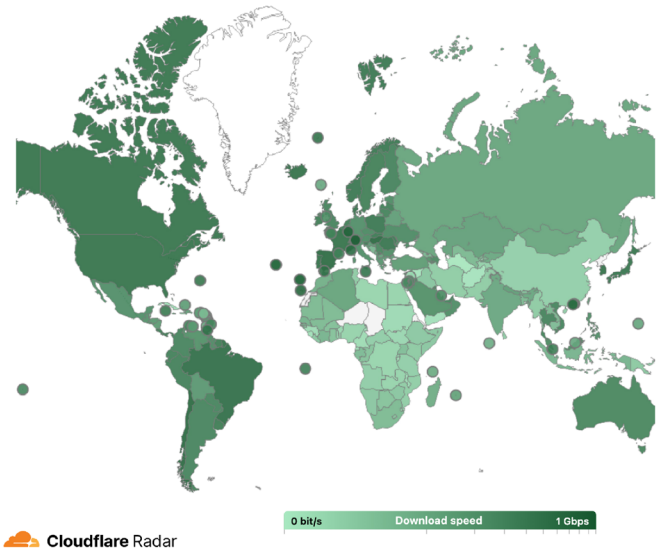
Примечание: Координаты промежуточного узла маршрута определяются по IP-адресу из базы данных NetAcuity. Расстояние между узлами рассчитывается по географическим координатам. Заданные интервалы: 3 мс для RTT и 100 км для расстояния. Зелёная линия показывает теоретически минимальное время RTT для соответствующего расстояния.

Источник: CAIDA Archipelago Monitor Statistics.
https://www.caida.org/projects/ark/statistics/monitor/osf-ru/med_rtt_vs_dist_v6.html

Качество соединения: скорость входящего потока данных

Скорость входящего потока данных (скачивания) остаётся одним из основных показателей качества соединения, хотя для современных сервисов также важны скорость исходящего потока данных и задержка.

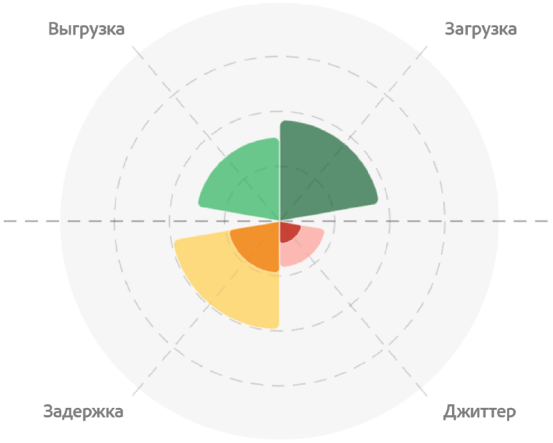
Карта показывает среднюю скорость входящего потока данных в разных странах и регионах мира по результатам тестов, проведённых пользователями на сайте speed.cloudflare.com в 2025 году. Cloudflare агрегировал результаты этих измерений для сравнения качества интернет-соединений в разных локациях.



Источник: Cloudflare, Inc. "Connection quality: Download speed". Cloudflare Radar. Accessed October 1, 2026. https://radar.cloudflare.com/quality#connection-quality-download-speed

Качество связи в РФ по результатам тестов Cloudflare за 90 дней

Такие диаграммы отражают производительность для конкретных стран или ASN в заданный период, где показатели качества соединения включают скорость загрузки и выгрузки данных, задержку (время прохождения пакетов в оба конца) и колебания задержки – джиттер (стабильность времени прохождения пакетов в оба конца).
В верхней части представленной диаграммы указана пропускная способность, где чем больше значение, тем выше качество. А в нижней части диаграммы указаны задержка и джиттер, где чем меньше значение, тем качество ниже.



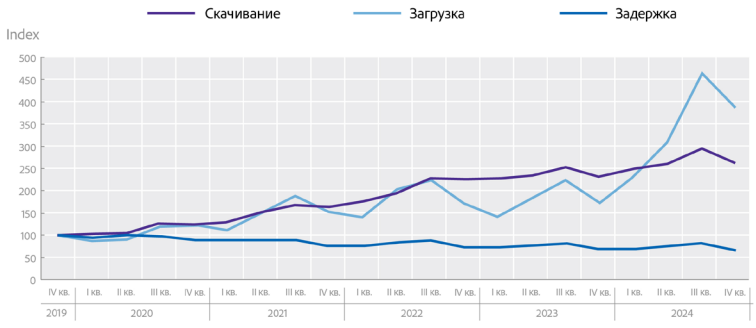
Cloudflare Radar

Скорость загрузки	102 Мбит/с	
Скорость выгрузки	70 Мбит/с	
Задержка	58 мс (без нагрузки)	188 мс (под нагрузкой)
Джиттер	20 мс (без нагрузки)	50 мс (под нагрузкой)

Источник: Cloudflare, Inc. "Performance summary in Russian Federation". Cloudflare Radar. Accessed September 22, 2026. https://radar.cloudflare.com/quality/ru#performance-summary

Индекс территориальных различий в скоростях фиксированного Интернета и задержке сигнала

Разрыв между метрополиями и удалёнными регионами по скорости фиксированного Интернета за последние пять лет увеличился, а различия по задержке сигнала незначительно сократились. Вероятно, это связано с тем, что в ответ на растущий спрос модернизация сетей в первую очередь проводилась в столичных регионах.



Примечание: Индекс разрыва (Index) между средними показателями метрополий стран ОЭСР и удалённых регионов для фиксированного доступа в Интернет по скорости загрузки/скачивания данных (Мбит/с) и по задержке сигнала (мс).

Источник: OECD Closing Broadband Connectivity Divides for All,
https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/closing-broadband-connectivity-divides-for-all_17ee89fa/d5ea99b2-en.pdf?

Измерения, выполняемые при обеспечении целостности и устойчивости функционирования сети связи общего пользования

Сергей Семёнов, Екатерина Семёнова

Аннотация

В настоящей статье рассмотрены вопросы измерения параметров сетей тактовой сетевой синхронизации, измерения параметров временной синхронизации и измерения параметров сетей передачи данных. Рассказано, какое оборудование используется в качестве источников эталонных сигналов частоты и времени и какие характеристики нормированы. Рассказано об источниках точного времени в сети Интернет. Приведены результаты измерений синхронизации шкалы времени по протоколам NTP системного времени ПЭВМ с операционной системой Windows программным и инструментальным методами и результаты измерений синхронизации шкалы времени по NTP- и PTP-протоколу. Дополнительно приведены сведения об эталоне количества информации (данных).

.

Ключевые слова:

сетевая синхронизация, погрешность по частоте, ОВИ, МОВИ, ДВИ, шкала времени, UTC(SU), NTP, PTP, количество информации (данных)

Введение

Интернет – это сложная структура, затрагивающая четыре уровня модели OSI: прикладной, транспортный, межсетевой и канальный. Для обычного потребителя Интернет – это социальные сети, развлекательный контент, электронная почта, банковские приложения, магазины и т.п. Но как только эта информация поступает к провайдеру (поставщику услуг связи), Интернет превращается в сетевое оборудование, которое должно взаимодействовать друг с другом и, главное, с другими сетями связи (операторами связи). Для успешного взаимодействия операторы связи руководствуются стандартами, определяемыми международными организациями. Так, архитектурные принципы и сетевые протоколы Интернета разрабатываются Инженерным советом Интернета (IETF, Internet Engineering Task Force). В свою очередь, международные рекомендации по физическому и канальному уровням, а также требования к сетевой и временной синхронизации формируются Международным союзом электросвязи (МСЭ, ITU), в который входят 193 страны. Рекомендации МСЭ хотя и носят рекомендательный характер, но облегчают развитие и взаимодействие как производителей сетевого оборудования и средств передачи данных, так и операторов связи.

Помимо технической части вопроса есть и законодательная сторона. В соответствии с частью 5 статьи 5 федерального закона от 26.06.2008 № 102-ФЗ «Об обеспечении единства измерений», пунктом 2 статьи 12 федерального закона от 07.07.2003 № 126-ФЗ «О связи» и пунктом 1 положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утверждённого постановлением правительства РФ от 02.06.2008 № 418 утверждён приказ Минцифры от 19.12.2019 № 870 «Об утверждении перечня измерений, относящихся к сфере государственного регулирования обеспечения единства измерений и выполняемых при обеспечении целостности и устойчивости функционирования сети связи общего пользования, и обязательных метрологических требований к ним, в том числе показателей точности измерений».

По указанному выше приказу выполняются следующие измерения: измерения параметров сетей передачи данных, измерения параметров сетей тактовой сетевой синхронизации, измерения параметров временной синхронизации, измерения параметров цифровых стыков и синхронной цифровой иерархии [1].

Тактовая сетевая синхронизация в сетях связи

Основой успешного взаимодействия операторов связи является система тактовой сетевой синхронизации. Все сигналы передаются по каналам связи, будь то оптоволоконные линии, кабельные линии (витая пара), коаксиальные кабели (соединения высокочастотного оборудования) или беспроводные каналы (радиоканалы) – такие как радиорелейные линии, спутниковые каналы связи, сотовые сети, беспроводные локальные сети (Wi-Fi, Blutooth, Zigbee) и оптические

каналы. Сами сигналы преимущественно цифровые, так как несут закодированную информацию в бинарном виде «0» или «1». Аналоговые сигналы практически не используются в силу малого объёма передаваемой информации, в то время как цифровые сигналы устойчивы к помехам и шумам, легко поддаются шифрованию и сжатию, а также передаются на большие расстояния без потери качества.

Наилучшим режимом функционирования цифровой сети является синхронный режим, при котором есть один задающий генератор – и все сетевые устройства по нему подстраиваются. Псевдосинхронный режим подразумевает несколько операторов связи, задающие генераторы которых по относительной погрешности по частоте отличаются не более чем на $\pm 1{,}0 \cdot 10^{-11}$. Плезиохронный режим работы подразумевает в своём составе задающий генератор, работающий в режиме запоминания частоты, относительная погрешность по частоте которого не должна превышать $\pm 1{,}0 \cdot 10^{-9}$. Самый худший вариант, когда задающий генератор не способен запомнить частоту. В этом случае отличие его частоты от эталонной может достигать значений от $\pm 1{,}0 \cdot 10^{-8}$ до $\pm 4{,}6 \cdot 10^{-6}$. Такой режим называется асинхронный, при котором качество голосовой связи приемлемо, а вот передача данных практически невозможна [2].

Для формирования эталонной частоты на сетях связи используют синхронную цифровую иерархию со следующими источниками синхросигналов: первичный эталонный генератор (ПЭГ), вторичный задающий генератор (ВЗГ), местные задающие генераторы, блоки сетевой синхронизации, мультиплексоры, аппаратура распределения сигналов синхронизации и преобразователи сигнала синхронизации.

ПЭГ – это комплекс аппаратуры, содержащий три первичных эталонных источника (ПЭИ) и одного ВЗГ. В качестве ПЭИ могут использоваться цезиевые, водородные и рубидиевые стандарты частоты и времени, в том числе с возможностью синхронизации по сигналам глобальных навигационных спутниковых систем (ГНСС) ГЛОНАСС/GPS.

ВЗГ представляют собой рубидиевые генераторы. Остальные источники синхросигналов в качестве опорного генератора используют кварцевые генераторы.

Основные параметры синхросигналов, которые подлежат нормированию и измерениям в процессе эксплуатации:

- относительная погрешность по частоте;
- долговременная нестабильность частоты (дрейф частоты или систематическое изменение частоты за сутки/за год);
- параметры блуждания фазы:
  - ошибка временного интервала (ОВИ);
  - максимальная ошибка временного интервала (МОВИ);
  - девиация временного интервала (ДВИ).

Из всех определяемых величин (единиц измерений) частота может быть определена с наивысшей точностью. При этом, если мы имеем дело не с цезиевым стандартом частоты, измерение частоты имеет квазистационарный характер: на малых интервалах времени наблюдений измерения стабильны, на больших интервалах – систематическое изменение частоты становится очевидным. Именно поэтому генераторам, представляющим из себя ПЭИ и ВЗГ, требуется корректировка действительного значения частоты в процессе эксплуатации с периодичностью около года.

Синхронизация времени в сетях связи

Синхронизация времени в сетях связи подразумевает распространение точного времени и календарной даты по сети связи. Источником точного времени на территории Российской Федерации является Государственный первичный эталон единиц времени, частоты и национальной шкалы времени ГЭТ 1-2022. Эталонные сигналы частоты и времени от ГЭТ 1-2022 передаются через разветвлённую сеть средств передачи: ДВ специализированные радиостанции РБУ и РТЗ; КВ специализированную радиостанцию РВМ; радиостанции связи СДВ-диапазона и радионавигационные станции ДВ-диапазона; ГНСС ГЛОНАСС; средства передачи точного времени через глобальную сеть Интернет. Основными источниками точного времени могут быть устройства синхронизации времени, например, NTP (PTP) серверы, получающие сигналы точного времени по сигналам ГНСС ГЛОНАСС, либо NTP-серверы ФГУП «ВНИИФТРИ», IP-адреса которых приведены в таблице 1.

Таблица 1. IP-адреса NTP-серверов ФГУП «ВНИИФТРИ»

Адрес	Место нахождения
ntp1.vniiftri.ru (89.109.251.21)	Московская область, г. Солнечногорск, пгт. Менделеево
ntp2.vniiftri.ru (89.109.251.22)	
ntp3.vniiftri.ru (89.109.251.23)	
ntp4.vniiftri.ru (89.109.251.24)	
ntp1.niiftri.irkutsk.ru (46.254.241.74)	г. Иркутск
ntp2.niiftri.irkutsk.ru (46.254.241.75)	
vniiftri.khv.ru (212.19.6.218)	г. Хабаровск
vniiftri2.khv.ru (212.19.17.26)	
ntp.sstf.nsk.ru (80.242.83.227)	г. Новосибирск
timesstf.sstf.nsk.ru (80.242.83.228)	

Требования приказа Минцифры от 19.12.2019 № 870 регламентируют погрешность измерения разности (расхождения) шкал времени в сетях связи операторов связи относительно национальной шкалы времени Российской Федерации UTC(SU) 0,3 с. Такое значение необходимо при учёте оказания услуг связи, биллинг которого ведётся в секундах.

Требования синхронизации в сетях связи регламентируется стандартами МСЭ-Т серии G.827x и ГОСТ Р 71148-2023, где точностные характеристики строго зависят от технологий.

Таблица 2. Допустимые смещения шкал времени

№ п/п	Технология связи	Допустимое смещение шкал времени
1	5G NR	от ±130 нс до ±1,5 мкс
2	4G LTE	не более ±1,5 мкс
3	3G	от ±2,5 мкс до ±10 мкс
4	Проводной доступ Ethernet	от ±1 мкс до ±50 мкс
5	Биллинг, логирование данных или мониторинг сети связи (Alarms)	до ±500 мс

Синхронизация времени может быть обеспечена по следующим технологиям, приведённым в таблице 3.

Таблица 3. Допустимые смещения шкал времени

№ п/п	Синхронизация времени	Допустимое смещение шкал времени
1	ГНСС	не более ±1 мкс
2	1PPS (1 Гц)	не более ±1 мкс
3	IRIG	от ±10 мкс до ±1 мс
4	NTP(SNTP)	от ±0,5 мс до ±100 мс
5	PTP	не более ±1 мкс

Для синхронизации времени по сигналам ГЛОНАСС или ГЛОНАСС/GPS устройство оснащается приёмным модулем, кабелем и антенной ГНСС. Для работы необходимы максимальный обзор небесной полусферы, отсутствие помех, в том числе таких, как демпинг или спуфинг.

Сигнал 1PPS (1 Гц) – импульсный сигнал, передний фронт которого синхронизирован с национальной шкалой времени UTC(SU). Источником обычно являются высокостабильные стандарты частоты и времени. Предназначены для автономного хранения формируемой шкалы времени.

IRIG – протокол, который содержит информацию о текущем значении времени и календарной дате.
NTP и SNTP – сетевые протоколы времени.
PTP – сетевой протокол времени, более точный по сравнению с NTP.

Измерение времени в Интернете

Самым распространённым инструментом синхронизации времени в сетях связи является NTP-протокол. В качестве источника точного времени используются NTP-серверы. Системное время ПЭВМ при синхронизации времени по NTP-серверу можно представить в виде формулы (1) [3]:

$$T(t) = T(to) + R(t-to) + D(t-to)2 + x(t), \quad (1)$$

где: t – текущее время;
to – время в момент последней синхронизации;
T – смещение времени;
R – относительная погрешность по частоте;
D – дрейф частоты;
x(t) – стохастическая составляющая погрешности.

Первая составляющая погрешности T(to) включает в себя погрешность формирования шкалы времени NTP-сервером и погрешность, обусловленную работой протокола NTP.

В качестве примера NTP-сервера рассмотрим сервер точного времени ССВ-1Г производства ООО «Комсет-сервис» (средство измерений утверждённого типа, регистрационный номер в Федеральном информационном фонде обеспечения единства измерений 58301-14). На выходе ССВ-1Г формирует сигнал 1 Гц, синхронизированный по сигналам ГЛОНАСС/GPS с национальной шкалой времени UTC(SU) с погрешностью ±110 нс. При этом привязка шкалы времени относительно национальной шкалы времени UTC(SU) по протоколу NTP через интерфейс Ethernet составляет уже ±10 мкс. Если рассматривать аналогичные средства измерений, то у других значение погрешности будет порядка ±100 мкс.

Погрешность, обусловленная работой протокола NTP, зависит от загруженности сети связи и удалённости от NTP-сервера. Как известно, протокол NTP содержит информацию, представленную на рисунке 1.

Из всего перечня значимой информацией является уровень сервера в иерархии (stratum), значение смещения шкалы времени (offset), задержка прохождения NTP-пакета до сервера и обратно (delay) и джиттер, или стандартное отклонение результатов измерений смещения шкалы времени (jitter).

Уровень сервера Stratum I подразумевает, что NTP-сервер получает информацию о точном значении времени от атомных часов, по сигналам ГЛОНАСС/GPS или радиосигналу. В этом случае можно полагать, что погрешность формирования шкалы времени составляет ±(10-100) мкс.

Значения offset, delay и jitter дают представление о вкладе протокола NTP в общую погрешность. Как известно, основным источником ошибки является асимметрия канала связи, при которой смещение времени определяется по формуле (2) [3]:

$$offset = [(T2-T1) - (T4-T3)]/2 = D/2, \quad (2)$$

NTP Status:

	Remote	Refid	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
*	129.6.15.28	NIST	1	Unicast server	27	128	357	138.902	-0.2	3.353
#	129.6.15.29	NIST	1	Unicast server	67	128	377	135.248	1.402	2.538
*	129.6.15.30	NIST	1	Unicast server	81	128	377	134.39	1.058	2.157
#	129.6.15.26	NIST	1	Unicast server	79	128	377	137.543	2.266	4.287

Рис. 1. Информация, передаваемая NTP-протоколом.

где T1, T2, T3, T4 – значения времени, проставляемые в NTP-пакетах, при отправке запроса клиентом, времени получения и отправки пакета NTP-сервером и времени получения пакета клиентом соответственно.

Поэтому максимальная погрешность определяется временем прохождения NTP-пакета в обе стороны.

Если сервер находится в Москве и подстраивает свой ПЭВМ по NTP-серверам ФГУП «ВНИИФТРИ», то значения задержек будут такими:

≈ 8 мс по NTP-серверам пгт. Менделеево;
≈ 60 мс по NTP-серверам г. Новосибирск;
≈ 75 мс по NTP-серверам г. Иркутск;
≈ 110 мс по NTP-серверам г. Хабаровск.

Но несмотря на столь большие значения задержек, каналы имеют квазисимметричный канал связи, поэтому смещения шкал времени составляют не более 4 мс [4, 5].

Для оценки погрешности формирования текущего времени ПЭВМ с операционной системой Windows проведён ряд экспериментов [4, 5]. Схема измерений приведена на рисунке 2.

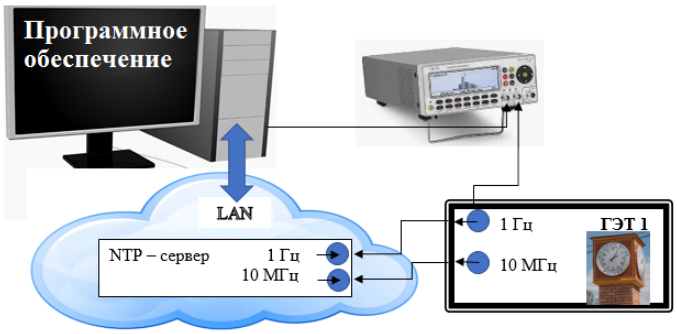


Рис. 2. Схема для определения погрешности формирования системной шкалы времени ПЭВМ.

На ПЭВМ установлено специальное программное обеспечение AccurateClock, разработанное ФГУП «ВНИИФТРИ» (существует в двух исполнениях – для Windows и для Linux), которое формирует импульсный сигнал частотой 1 Гц при смене номера секунды системного времени. Полученный сигнал сравнивался с национальной шкалой времени UTC(SU). Параллельно на ПЭВМ была запущена программа NTPD, которая позволяет оценить параметры протокола NTP согласно данным, представленным на рисунке 1.

Результаты измерений системной шкалы времени приведены на рисунках 3 и 4.

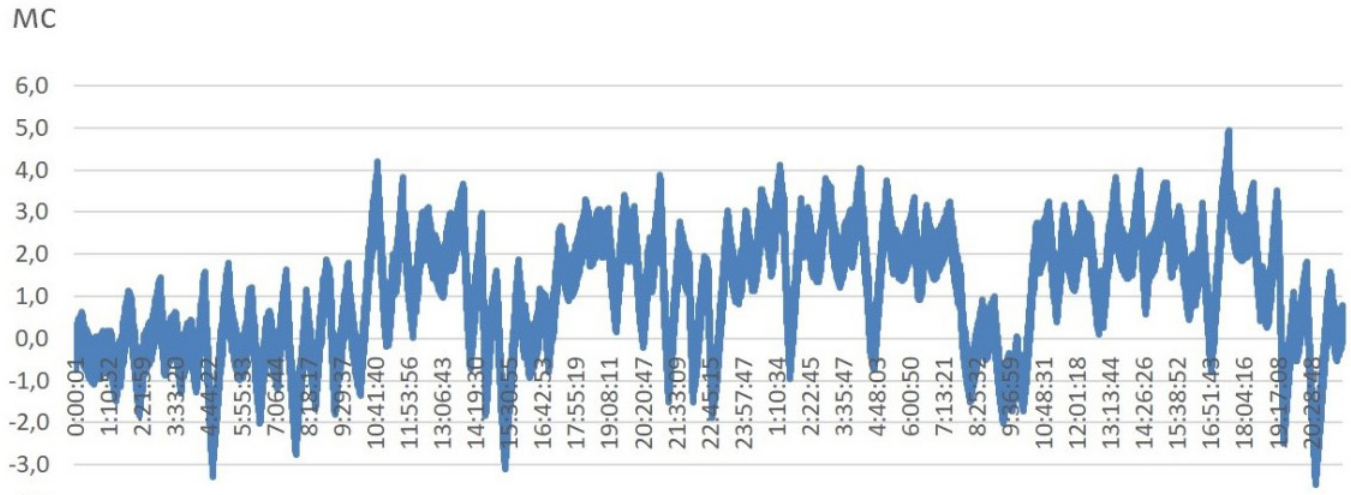


Рис. 3. Смещение шкалы системного времени ПЭВМ относительно национальной шкалы времени UTC(SU) при измерении с помощью частотомера универсального CNT-90.

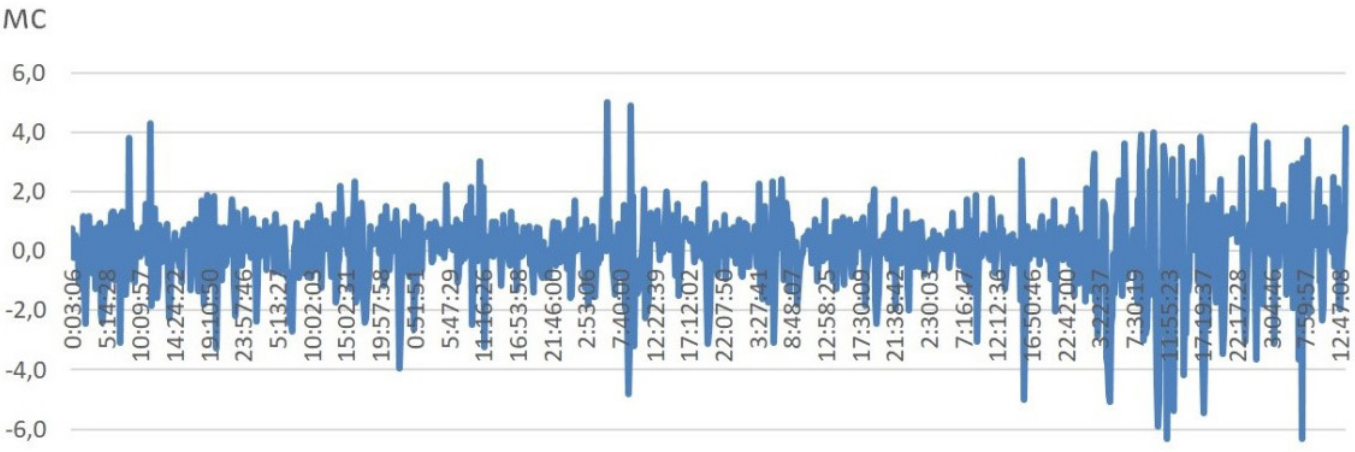


Рис. 4. Смещение шкалы системного времени ПЭВМ относительно национальной шкалы времени UTC(SU) при измерении с помощью утилиты NTPD (NTP Time Server Monitor by Meinberg 1.05).

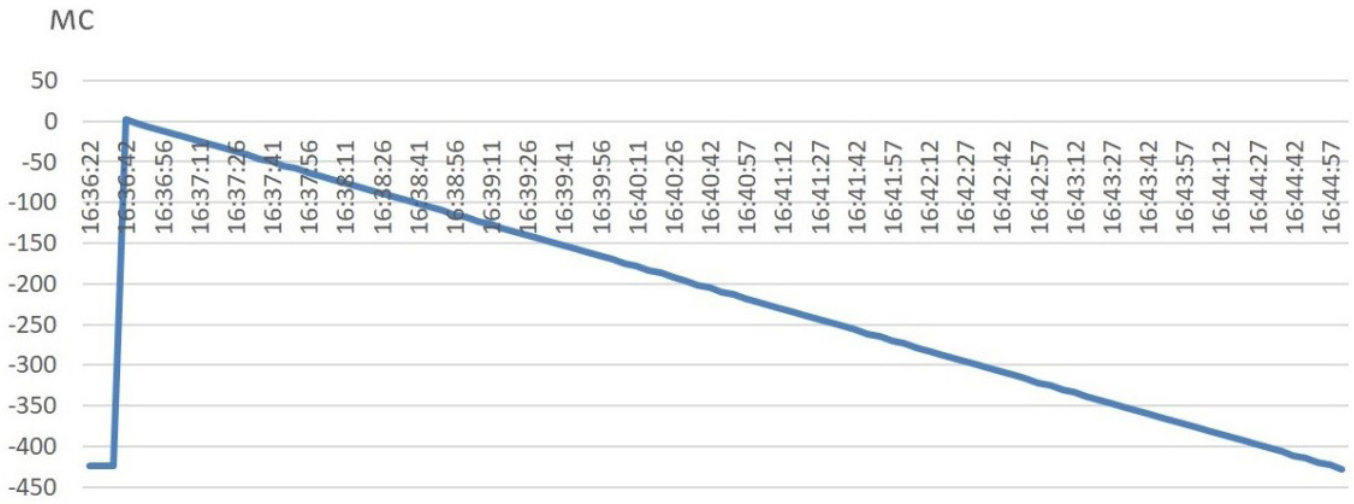


Рис. 5. Смещение шкалы системного времени ПЭВМ после единовременной синхронизации по NTP-серверу.

Исследование системной шкалы времени ПЭВМ методом измерения физического сигнала 1 Гц и программными средствами показало сходимость результатов измерений в пределах ±10 мс.

Далее проведён эксперимент по хранению формируемой шкалы времени ПЭВМ. Системная шкала времени ПЭВМ, работая по тактовой частоте процессора, изменилась на 0,5 секунды за менее чем 10 минут. Результаты измерений приведены на рисунке 5.

На практике приемлема точность времени порядка нескольких миллисекунд, и для этого ПЭВМ должен синхронизировать время с NTP-сервером не реже чем раз в 15 минут.

Для измерения времени в сетях связи стоит упомянуть отечественное средство измерений – тестер-анализатор пакетных сетей «МАКС-ЕМК», производства АО «НПП «Кометех» (средство измерений утверждённого типа, регистрационный номер в Федеральном информационном фонде обеспечения единства измерений 63631-17). «МАКС-ЕМК» имеет встроенный приёмник сигналов ГЛОНАСС/GPS, по этим сигналам формирует собственную шкалу времени и может измерять разность шкал времени удалённых NTP(PTP) серверов или смещение шкалы времени по внешнему сигналу 1 Гц. Прибор содержит набор измерительных функций для реализации основных задач тестирования и паспортизации пакетных сетей и услуг.

Результаты измерений синхронизации шкалы времени по NTP- и PTP-протоколу

NTP- и PTP-серверы широко используют в том числе в локальных вычислительных сетях LAN (далее – ЛВС). Как известно, ЛВС имеют простую структуру построения, и загрузка в них практически отсутствует. Какую же в таких ЛВС можно ожидать погрешность синхронизации времени? Чтобы это выяснить, проведено два эксперимента на примере устройства синхронизации времени «TOPAZ Метроном PTS» (регистрационный номер в Федеральном информационном фонде по обеспечению единства измерений 72378-18). Устройство работает под управлением операционной системы TOPAZ Linux. Используется в качестве NTP- или PTP-сервера в режиме дисциплинирования по сигналам ГНСС. В различных модификациях имеет коммутационные порты для подключения одномодового или многомодового оптического волокна, а также витой пары со скоростями передачи данных 100 Мбит/с или 1000 Мбит/с. На устройстве реализован выход сигнала 1 PPS (1 Гц) – формируемая устройством шкала времени.

Эксперимент 1.

В качестве NTP-сервера уровня Stratum I (синхронизированного по сигналам ГЛОНАСС/GPS) использовалось устройство синхронизации времени «TOPAZ Метроном PTS». В качестве NTP-сервера уровня Stratum II использовалось устройство синхронизации частоты и времени «Метроном» версии 1000 (аналог Meinberg IMS-M1000). Оба устройства подключены к одной ЛВС.

«Метроном» версии 1000 синхронизировался по NTP-протоколу и на основе встроенного опорного генератора формировал собственную шкалу времени (сигнал 1 PPS (1 Гц)). Следует уточнить, что в таком режиме практически все устройства подстраивают частоту собственного опорного генератора и в случае перехода в автономный режим работы могут в течение продолжительного времени хранить шкалу времени с установленными параметрами, обычно от десятков мкс до сотен мс за сутки. Выходной сигнал 1 PPS (1 Гц) сравнивался с эталонным сигналом 1 Гц с помощью измерителя интервалов времени (частотомера универсального CNT-90, регистрационный номер в Федеральном информационном фонде по обеспечению единства измерений 41567-09). Суммарная погрешность средств измерений и метода измерений не превысила ±0,1 мкс.

Результаты формирования шкалы времени NTP-сервера уровня Stratum II приведены на рисунке 6.

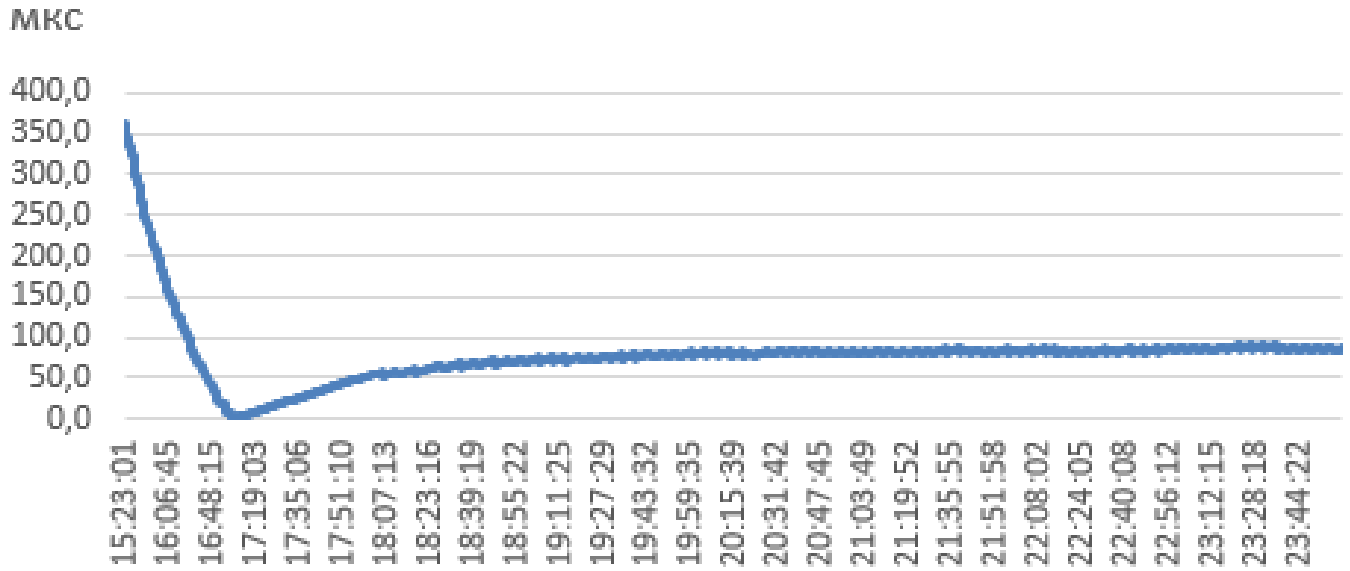


Рис. 6. Результаты формирования шкалы времени NTP-сервера уровня Stratum II.

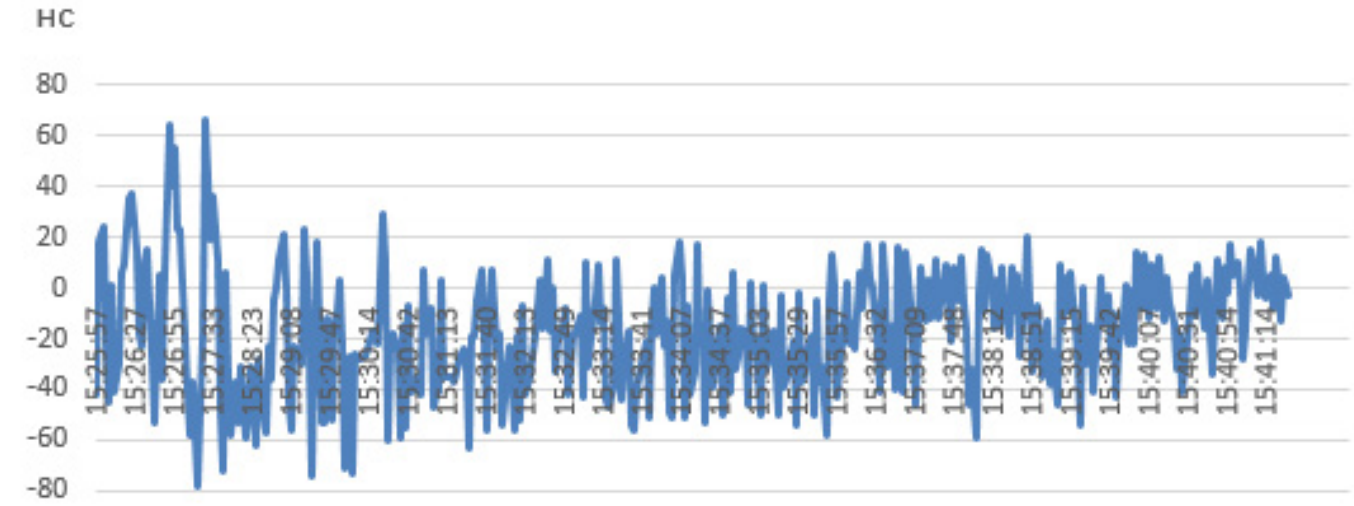


Рис. 7. Результаты формирования шкалы времени PTP-клиента относительно PTP-мастера.

При подключении серверов непосредственно друг к другу патчкордом результаты измерений получались идентичными.

Эксперимент 2.

В качестве PTP-мастера и PTP-клиента использовались два устройства синхронизации времени «TOPAZ Метроном PTS». Устройства подключены к ЛВС через один коммутатор.

С помощью измерителя интервалов времени (частотомера универсального CNT-90) сравнивались два сигнала 1 PPS (1 Гц). Результаты измерений приведены на рисунке 7.

В данном эксперименте учтены задержки в подключаемых к измерителю времени кабелях. Погрешность измерений не превысила ±5 нс.

При увеличении трафика через коммутатор (без поддержки PTP-протокола), к которому подключены PTP-мастер и PTP-клиент, смещение формируемой шкалы времени измерялось в мкс.

По результатам измерений можно сделать следующие выводы:

- погрешность синхронизации шкалы времени по протоколу NTP в локальной сети может достигать точностей в десятки мкс;
- погрешность синхронизации шкалы времени по протоколу PTP в локальной сети может достигать точностей в десятки нс.

Эталон объёма информации

При оказании услуг связи (в первую очередь это касается операторов сотовой связи) случается так, что возникают ошибки в пакетах передаваемой информации, что ведёт к перезапросу и повторной передаче данных. Данный трафик тарифицируется. Также следует упомянуть, что в пакетах

помимо полезной информации передаётся и служебная, за которую платит конечный потребитель. В целях обеспечения единства измерений разработан и утверждён приказ Росстандарта от 18.08.2023 г. № 1707 «Об утверждении государственной поверочной схемы для средств измерений количества передаваемой (принятой) информации (данных) и величин параметров пакетных сетей передачи данных». Государственная поверочная схема для средств измерений количества переданной (принятой) информации (данных) и величин параметров пакетных сетей передачи данных устанавливает порядок передачи единицы количества переданной (принятой) информации (данных) и единиц величин параметров пакетных сетей передачи данных от государственного первичного эталона (ГПЭ) рабочим эталонам и средствам измерений с указанием показателей точности эталонов, средств измерений и основных методов передачи единиц [6].

ГПЭ состоит из комплекса следующих технических средств и вспомогательных устройств: файл-сервер эталонных объёмов цифровой информации; IP-формирователь соединений «Амулет-М»; измеритель количества информации «Вектор-ИКИ»; имитатор параметров сетей «ВИМАН»; эталонный измеритель параметров пакетных сетей со скоростью передачи до 10 Гбит/с «ВИМАН-И»; сервер точного времени «Метроном-PTP-1U»; формирователь-измеритель соединений «СИГМА-2»; модуль синхронизации для цифровых осциллографов; осциллограф MSOS804A; частотомер 53220A; стандарт частоты и времени рубидиевый Ч1-1020; набор устройств фиксированной задержки.

ГПЭ предназначен для измерения количества передаваемой (принятой) информации (данных); задержки передачи пакетных данных; вариации задержки передачи пакетов; пропускной способности канала передачи данных; коэффициента потерь пакетов данных.

Вывод

Строгое соблюдение требований нормативно-правовой базы в сочетании с комплексным контролем параметров тактовой сетевой синхронизации (ОВИ, МОВИ, ДВИ) и точности синхронизации времени является ключевым условием для обеспечения целостности и устойчивой работы сетей связи общего пользования. Соблюдение допустимых смещений шкал времени напрямую предотвращает сбои и гарантирует качество передаваемых данных. Интеграция всех этих параметров в единую систему мониторинга обеспечивает высокую надёжность сети.

Для обеспечения надёжного функционирования современных высокоскоростных сетей связи (LTE, 5G) и корректности тарификации услуг связи протокол NTP недостаточно точен, в связи с чем необходимо применение протокола PTP (обеспечивающего наносекундную точность) и государственное регулирование с опорой на государственный первичный эталон единиц времени, частоты и национальной шкалы времени.

Список литературы:

[1] Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 19.12.2019 № 870 «Об утверждении перечня измерений, относящихся к сфере государственного регулирования обеспечения единства измерений и выполняемых при обеспечении целостности и устойчивости функционирования сети связи общего пользования, и обязательных метрологических требований к ним, в том числе показателей точности измерений».

[2] Колтунов М.Н., Леготин Н.Н., Шварц М.Л., «Сетевая синхронизация в системах связи», 2007.

[3] Mills David L. Computer network time synchronization – 2nd edition. – CRC Press, 2010.

[4] Семёнов С.А., «Методика оценки корректности формирования текущего значения времени устройствами синхронизации времени с использованием NTP серверов ФГУП «ВНИФИТРИ» при проведении поверки» Метрология в XXI веке. Материалы X научно-практической конференции молодых ученых, аспирантов и специалистов, 2023, с. 243-253.

[5] Каган С.Н., Пестерев С.В., «Результаты экспериментальных исследований реальной неопределённости шкал времени потребителей NTP серверов уровня Stratum 1». Альманах современной метрологии № 8, 2016, с. 75-86.

[6] Приказ Росстандарта от 18.08.2023 № 1707 «Об утверждении государственной поверочной схемы для средств измерений количества передаваемой (принятой) информации (данных) и величин параметров пакетных сетей передачи данных».

Об авторах:

Семёнов Сергей Александрович, AuthorID: 1201354, SPIN-код: 3149-1337, ФГУП «ВНИИФТРИ», Россия, пгт. Менделеево.

Семёнова Екатерина Игоревна, ФГУП «ВНИИФТРИ», Россия, пгт. Менделеево.

Взгляд со стороны: использование RIPE Atlas для мониторинга связности, маршрутизации и DNS

Андрей Юров

Аннотация

В статье рассматривается распределённая система измерительных зондов, разработанная и сопровождаемая RIPE NCC – RIPE Atlas. Благодаря размещению зондов в пользовательских сетях и сетях предприятий, система даёт возможность измерять производительность различных онлайн-услуг именно с точки зрения потребителя. А широкий географический охват позволяет исключить локальные проблемы связности, что делает RIPE Atlas надёжным инструментом мониторинга. В статье представлены практические примеры применения системы и её интеграции в системы управления сетевых операторов и операторов услуг.

Ключевые слова:

измерительный зонд, мониторинг, RIPE Atlas

Введение

RIPE Atlas – это платформа для проведения измерений в сети Интернет, разработанная и поддерживаемая организацией RIPE NCC. Она была запущена в начале 2010-х годов с целью создания масштабной распределённой инфраструктуры для оценки связности и производительности сети из множества географических точек. Платформа выросла из более ранней инициативы RIPE NCC под названием RIPE TTM (т.н. измерения «Test Traffic») и расширилась благодаря участию сообщества: организации и частные лица размещают измерительные зонды в своих сетях.

В основе RIPE Atlas лежит распределённая сеть измерительных зондов. Эти компактные устройства (аппаратные или программные) размещаются волонтёрами, сетевыми операторами, исследователями и другими организациями по всему миру. Зонды служат точками наблюдения и позволяют выполнять такие тесты, как ping, traceroute, а также измерения параметров DNS, TLS и HTTP для заданных целей. Поскольку зонды распределены по различным сетям и географическим локациям, RIPE Atlas обеспечивает возможность внешнего мониторинга таких показателей, как доступность ресурсов, задержка, потеря пакетов и маршруты передачи данных.

Платформа располагает централизованной инфраструктурой управления и обработки данных, которую обслуживает RIPE NCC. Пользователи создают задания на измерения, указывая такие параметры, как целевой объект, тип измерения, частота выполнения и набор используемых зондов. Инфраструктура RIPE Atlas планирует выполнение этих заданий, отправляет инструкции соответствующим зондам, собирает результаты и предоставляет доступ к данным через веб-интерфейс и API. Результаты также могут обрабатываться программно (в том числе через потоковый API RIPE Atlas), что позволяет интегрировать систему с инструментами мониторинга и визуализации сети.

Архитектура, охват и доступные услуги системы

С архитектурной точки зрения RIPE Atlas можно разделить на три основных компонента: распределённые агенты измерений (зонды), центральная платформа управления и обработки данных, а также программный интерфейс (API) и инструментарий для доступа к результатам и их анализа. Такая архитектура позволяет сетевым операторам и исследователям наблюдать за поведением сети Интернет извне собственной инфраструктуры. Для сетевого оператора или оператора услуг DNS RIPE Atlas представляет особую ценность как дополнительный уровень мониторинга, позволяющий, например, проверять соблюдение условий SLA, выявлять региональные проблемы со связностью, сравнивать производительность IPv4 и IPv6, а также анализировать изменения маршрутов передачи данных.

RIPE Atlas также открывает простор разнообразным исследованиям и измерениям Интернета. Многочисленные научно-исследовательские статьи, публикуемые на сайте RIPE Labs, являются тому доказательством.

В RIPE Atlas используются два типа измерительных зондов – аппаратные и программные. Аппаратные зонды – это компактные специализированные устройства с питанием от USB, которые подключаются к порту Ethernet на маршрутизаторе с помощью сетевого кабеля (UTP). Программный зонд устанавливается на персональный компьютер и выполняет измерения аналогичным образом. Эти устройства проводят различные измерения и передают полученные данные в RIPE NCC, где они объединяются с данными, поступающими от остальных участников сети RIPE Atlas. Наиболее типичным местом установки зонда является домашняя сеть пользователя, но они также широко используются сервис-провайдерами и даже корпоративными сетями, например, для мониторинга качества услуг и SLA.

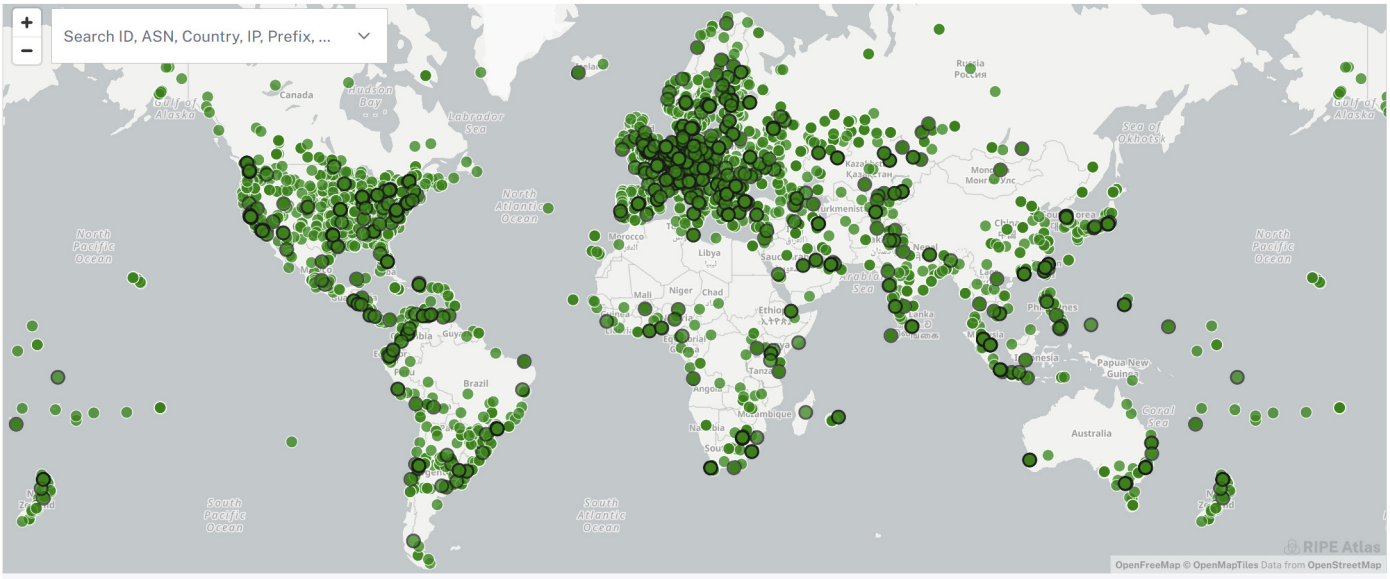


Рис. 1. Географический охват измерительной платформы RIPE Atlas.

Существует и третий тип измерительного агента – анкер. Анкеры RIPE Atlas – это одновременно и усовершенствованные зонды RIPE Atlas с расширенными возможностями проведения измерений, и мощные региональные узлы, служащие опорными точками для измерений в рамках глобальной сети RIPE Atlas. Они предоставляют ценную информацию о локальной и региональной связности и доступности в сети Интернет.

Сеть RIPE Atlas насчитывает более 14 тысяч подключённых измерительных зондов по всему миру, включая примерно 13,4 тысячи стандартных зондов и почти тысячу анкеров. В недавнем научном обзоре [1] платформы отмечается, что, несмотря на неравномерность географического охвата, сеть RIPE Atlas распространяется на 178 стран и более чем четыре тысячи автономных систем.

Использование системы

Использование системы основано на так называемых кредитах. За создание и проведение измерительных экспериментов или задач мониторинга пользователи расплачиваются кредитами. Самым простым способом заработать кредиты является размещение зонда в своей сети, но их также можно получить, разместив у себя анкер, выступив спонсором RIPE Atlas или получив перевод от другого пользователя RIPE Atlas. Хост получает 15 кредитов за каждую минуту подключения зонда к сети — таким образом, при непрерывном подключении зонда пользователь зарабатывает примерно 21 600 кредитов в сутки.

Размещение зонда в сети является в принципе бесплатным. Для этого необходимо создать запрос – и в случае одобрения заявки, RIPE NCC пришлёт вам аппаратный зонд, который вы сможете подключить к своей сети (обычно непосредственно к домашнему маршрутизатору) и зарегистрировать его на портале RIPE NCC Access. При рассмотрении заявки оценивается планируемое местоположение зонда, чтобы определить, принесёт ли размещение зонда пользу сети RIPE Atlas. В случае использования программного зонда, его также необходимо запросить, но его запуск сводится к установке программного обеспечения.

Применение RIPE Atlas для мониторинга сетей

Благодаря своему географическому охвату RIPE Atlas позволяет оценивать работу услуги с тысяч независимых точек наблюдения, расположенных преимущественно в сетях домашних и корпоративных пользователей. Благодаря этому система отлично подходит для проверки доступности и производительности услуг с точки зрения реального пользователя.

Основные компоненты

Типы измерений. Зонды могут выполнять проверки ping, traceroute, DNS, получать SSL/TLS-сертификаты и взаимодействовать с NTP-серверами для произвольных целевых узлов. HTTP-измерения ограничены использованием анкеров в качестве целей. Для анализа связности и соблюдения SLA основную роль играют ping (доступность, RTT, потери), traceroute (изменения маршрута, локализация деградации) и DNS (задержка и корректность разрешения имён). TLS-измерения полезны для выявления истечения срока действия сертификатов или несоответствий, наблюдаемых из определённых сетей.

Пользовательские измерения. Пользователь может создавать разовые или периодические измерения через веб-интерфейс или REST API. Выбор зондов возможен по стране, номеру автономной системы (ASN), префиксу, региону или конкретным идентификаторам зондов. Каждое измерение требует определённого количества кредитов.

Анкеры. Если вы размещаете анкер, он автоматически становится целью для перекрёстных измерений (mesh measurements), выполняемых другими анкерами и множеством обычных зондов. Вы получаете непрерывные базовые данные о том, как внешние сети взаимодействуют с вашей сетью, не расходуя при этом кредиты. Кроме того, анкеры служат более качественными точками обзора по сравнению с домашними зондами, так как на них практически не влияют помехи, характерные для «последней мили».

Строительные блоки

Проверки состояния (Status checks). Каждое периодическое измерение (пинг) предоставляет API-эндпоинт для проверки состояния, который оценивает недавние результаты на соответствие заданным вами пороговым значениям (например, медианному RTT, максимальному уровню потери пакетов и временному окну анализа). Система возвращает общий статус (OK или ALERT) и детализацию по отдельным зондам, что позволяет легко интегрировать этот механизм с такими системами мониторинга, как Nagios или Icinga.

Потоковая передача данных (Streaming). Для конвейеров обработки данных, работающих в режиме, близком к реальному времени, потоковый API передаёт результаты через WebSockets или HTTP GET по мере их поступления от зондов. Это позволяет самостоятельно вычислять метрики и настраивать оповещения на их основе, не полагаясь на встроенную логику проверки состояния.

Инструментарий. Python-библиотеки RIPE берут на себя выполнение большинства технических задач: Cousteau отвечает за создание измерений и взаимодействие с API, Sagan преобразует «сырые» результаты в объекты, а ripe-atlas-tools предоставляет интерфейс командной строки (CLI) для проведения оперативных проверок во время инцидентов. Исторические данные доступны через API и в виде ежедневных архивов, что помогает определять базовые показатели и проводить анализ после инцидентов.

Оповещения о статусе зондов. Если вы размещаете зонды, то можете получать уведомления об их отключении. Для небольших площадок это само по себе может служить простым средством мониторинга сетевой связности.

Давайте теперь остановимся на некоторых конкретных примерах использования RIPE Atlas для мониторинга работы инфраструктуры и услуг.

Мониторинг связности и маршрутизации

RIPE Atlas предоставляет компании независимый взгляд извне на то, как её цифровая цепочка поставок фактически функционирует в Интернете. Как я уже отметил, система RIPE Atlas опирается на тысячи измерительных зондов, размещённых в сетях домашних пользователей, корпоративных сетях и центрах обработки данных по всему миру. Размещая зонды на собственных объектах и используя общедоступные зонды в сетях поставщиков и клиентов, организация может отслеживать связность в обоих направлениях: от своих офисов и облачных сред к критически важным сервисам и, наоборот, со стороны сетей партнёров. Такой двусторонний мониторинг важен, поскольку маршруты в Интернете зачастую асимметричны.

На базовом уровне система обеспечивает непрерывный контроль доступности, задержек, потерь пакетов, разрешения DNS-имён и состояния TLS-сертификатов для критически важных оконечных точек, а также включает встроенную систему

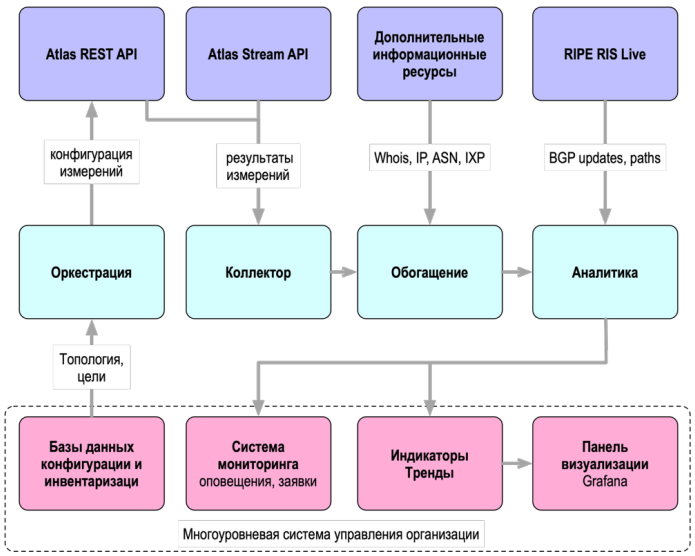


Рис. 2. Пример интеграции платформы RIPE Atlas с системой управления организации.

оповещения, которую легко интегрировать с существующими системами мониторинга.

Уникальной возможностью является мониторинг маршрутизации. Трассировки (traceroute) в системе Atlas позволяют увидеть реальный путь трафика — сеть за сетью, точка обмена трафиком за точкой обмена трафиком. В сочетании с BGP-коллекторами RIPE, отслеживающими анонсирование и распространение маршрутов, эти данные могут помочь выявить перехваты и утечки маршрутов (route hijacks, route leaks) и их влияние на пути передачи трафика организации и её поставщиков. Кроме того, это поможет отличить аномалию маршрутизации, заметную лишь в таблицах маршрутизации, от проблемы, реально влияющей на прохождение трафика.

Анализ этих данных в динамике позволяет ответить на стратегический вопрос, который редко рассматривается в соглашениях об уровне обслуживания (SLA) с отдельными поставщиками: насколько диверсифицированы зависимости организации. Поставщики, кажущиеся независимыми, могут пользоваться услугами одного и того же транзитного провайдера, DNS-хостинга или сети доставки контента (CDN). Резервные каналы связи могут сходиться в одну точку на более ранних этапах маршрута. Выявление таких скрытых точек концентрации превращает результаты измерений сети в ценную информацию для управления рисками, связанными с третьими сторонами, и обеспечения операционной устойчивости.

У этого подхода есть естественные ограничения. Atlas видит только публичный Интернет, но не частные каналы связи или внутреннюю структуру VPN. Результаты измерений являются общедоступными, а значит, детальная настройка мониторинга может непреднамеренно раскрыть информацию о связях организации с поставщиками. Трассировка не всегда возможна и может давать ошибочные результаты («When Traceroutes Lie: How TTL Jumps Can Give Us a False Impression of the Internet's Topology»). Тем не менее, в этих рамках система даёт ценные сведения: объективные данные о связности в цепочке поставок, полученные независимо от самой компании или её провайдеров.

Мониторинг DNS

Аналогичным образом, система RIPE Atlas позволяет организации наблюдать за работой DNS так, как она воспринимается в реальной сети, а не с единичной точки.

Зонды могут отправлять запросы либо непосредственно на выбранный сервер имён, либо через локальный резолвер (обычно тот, который назначен интернет-провайдером или сетью, где размещён зонд). Это обеспечивает получение двух дополняющих друг друга картин. Прямые запросы позволяют проверить саму инфраструктуру авторитетных серверов имён. Запросы через локальные резолверы показывают, какие ответы получают реальные пользователи сети при поиске доменного имени. При этом могут использоваться любые распространённые типы записей, протоколы UDP или TCP, а также запрашиваться данные DNSSEC. Результаты фиксируют время отклика, содержание ответов и коды ответов по всей совокупности зондов.

Для операторов авторитетных DNS-серверов (будь то обслуживание собственных доменов или предоставление услуг сторонним клиентам) RIPE Atlas обеспечивает непрерывный мониторинг доступности и задержек из множества сетей и регионов одновременно. Самым ярким примером такого применения является служба мониторинга DNS от RIPE NCC – DNSMON. Она предоставляет всестороннюю, объективную и актуальную информацию об обеспечиваемом серверами корневой зоны DNS качестве обслуживания доменов верхнего уровня (TLD) и некоторых инфраструктурных доменов, таких как in-addr.arpa.

Мониторинг с помощью RIPE Atlas особенно ценен при использовании технологии anycast. Запрашивая серверы идентифицировать себя с помощью запросов NSID или запросов класса CHAOS (например, hostname.bind, id.server или version.bind, в зависимости от программного обеспечения сервера), оператор может увидеть, с каким именно экземпляром anycast-сервера соединяется та или иная сеть. Это позволяет составить карту покрытия сервиса, выявить непредвиденный дисбаланс нагрузки между экземплярами и обнаружить случаи, когда изменения маршрутизации приводят к перенаправлению трафика. Запрос записей SOA из множества точек наблюдения также позволяет проверить, используют ли все серверы одну и ту же версию зоны, что подтверждает корректное и согласованное распространение изменений.

Измерения через локальные резолверы превращают RIPE Atlas в инструмент для анализа ландшафта резолверов. Различия в ответах на один и тот же запрос позволяют выявить случаи, когда резолверы подменяют ответы, блокируют домены, подставляют результаты для несуществующих имён или не проходят проверку DNSSEC. Неожиданные ответы, касающиеся доменов самой организации или её поставщиков услуг и возникающие в определённых сетях или странах, могут служить ранним признаком перехвата сообщений DNS (DNS hijacking), отравления кеша или постороннего вмешательства.

Разумеется, здесь также следует учитывать стандартные ограничения и нюансы подобных измерений. Локальные резолверы зондов часто представляют собой пересылающие серверы (форвардеры) на домашних маршрутизаторах, а наличие кеширования означает, что повторные запросы могут вообще не доходить до авторитетных серверов; поэтому при планировании измерений это необходимо учитывать. Географический охват зондов неравномерен. Результаты измерений находятся в открытом доступе, и их анализ может выявить, какие доменные имена важны для той или иной организации. Несмотря на эти ограничения, система RIPE Atlas предоставляет данные, которые сложно получить иным путём: широкую и независимую картину того, как происходит разрешение имён в Интернете и где этот процесс даёт сбой, приводит к расхождениям или подвергается вмешательству.

Мониторинг сертификатов TLS

Зонды RIPE Atlas могут генерировать запросы к любому хосту и порту, выполнять процедуру TLS-рукопожатия (handshake) и фиксировать полученные данные. Сюда входят полная цепочка сертификатов, согласованная версия протокола и временные характеристики процесса установки соединения. Поскольку при запросе можно указать имя сервера (через механизм SNI – Server Name Indication), результаты измерений отражают то, что получил бы реальный клиент, обращающийся к конкретному сайту. Сбор данных одновременно из множества сетей позволяет не просто проверять годность сертификата, но и выяснять, всем ли пользователям в Интернете предъявляется один и тот же сертификат.

Самый очевидный сценарий использования – мониторинг срока действия и согласованности сертификатов. Крупные сервисы часто используют CDN, сети anycast и региональные балансировщики нагрузки. При этом развёртывание или обновление сертификата на отдельных узлах может задержаться или пройти с ошибками. Мониторинг из одной точки позволит увидеть лишь один из вариантов сертификата. Измерения, проводимые с помощью зондов в разных регионах, позволяют выявить устаревшие сертификаты, неполные цепочки или несоответствие имён на отдельных узлах ещё до того, как пользователи в этих сетях столкнутся с ошибками. Аналогичные проверки применимы и к конечным точкам поставщиков услуг, от которых зависит организация, но которые она не контролирует. Периодические измерения также показывают, какие версии протокола поддерживаются, что помогает отслеживать вывод из эксплуатации устаревших версий TLS.

Более важный с точки зрения безопасности аспект – обнаружение перехвата трафика и атак типа «человек посередине» (Man in the Middle, MITM). Если зонды в определённых сетях или странах получают сертификаты от неожиданного центра сертификации, это указывает на перехват TLS-трафика промежуточными устройствами (middleboxes), корпоративными прокси-серверами или системами государственного уровня. Если сертификат внезапно меняется для части точек наблюдения (особенно если новый сертификат является самоподписанным или выдан другим центром сертификации), это может быть признаком перехвата трафика через манипуляции с BGP или DNS, перенаправляющие запросы на сервер злоумышленника. Этот метод отлично дополняет упомянутые ранее инструменты мониторинга маршрутизации и DNS, а также анализ журналов Certificate Transparency (прозрачности сертификатов). Журналы прозрачности показывают, какие сертификаты были выданы для домена, тогда как RIPE Atlas демонстрирует, какие именно сертификаты реально предъявляются пользователям.

RIPE Atlas фиксирует данные о сертификатах, но оставляет их проверку и анализ пользователю, поэтому ценность системы заключается в логике сравнения, выстроенной на основе этих данных. Измерения охватывают только процесс установки соединения (handshake), а не содержимое передаваемых данных. Зонды, находящиеся за корпоративными прокси-серверами, могут фиксировать перехваченные сертификаты, что не всегда является ошибкой, а может быть следствием соответствующей настройки корпоративного прокси-сервера. Кроме того, как и все результаты измерений RIPE Atlas, полученные данные являются общедоступными. В этих рамках система обеспечивает распределённую и независимую проверку одного из ключевых механизмов доверия в Интернете.

Применение RIPE Atlas в исследовании и измерении Интернета

RIPE Atlas стал одним из наиболее широко используемых наборов данных в исследованиях, посвящённых измерениям в сети Интернет. Встроенные измерения, проводимые на постоянной основе, позволяют сформировать исторические базовые показатели, а измерения, настраиваемые пользователями, дают исследователям возможность проверять конкретные гипотезы с использованием тысяч точек наблюдения. Примеры исследований, опубликованные на ресурсе RIPE Labs, охватывают широкий круг тем. Рассмотрим некоторые из них.

Наиболее заметной темой является анализ событий и устойчивости сети Интернет. В случаях обрыва кабелей или сбоев в работе крупных сетей исследователи RIPE NCC используют Atlas для оценки того, что именно происходило с трафиком. Например, в статье «Обходит ли Интернет повреждённые участки?» [2] автор проанализировал сбой в работе точки обмена трафиком AMS-IX, чтобы проверить, действительно ли Интернет перенаправляет трафик в обход повреждённых участков. Ранее при анализе сбоя в сети Time Warner Cable [3] данные о маршрутизации из системы RIS сопоставлялись с результатами измерений Atlas; это выявило показательное расхождение: сбой затронул плоскости передачи данных (data plane) как для IPv4, так и для IPv6, хотя плоскость управления (control plane) IPv6, по-видимому, осталась незатронутой. Это исследование демонстрирует, почему измерения на уровне передачи данных дополняют данные наблюдений за протоколом BGP.

Ещё одной важной темой является поведение и целостность системы DNS. В работе «Пример исследования фильтрации AAAA-записей» [4] исследователи проверяли, блокируют ли интернет-провайдеры или домашние маршрутизаторы DNS-запросы или ответы записей AAAA (предназначенные для получения IPv6-адресов). Лишь 14 из 1810 зондов (0,8%) стабильно не получали ответов на AAAA-запросы, при этом успешно получая ответы на A-запросы; это послужило доказательством отсутствия массовой фильтрации.

Ещё одна популярная тема — топология сети и характеристики путей передачи данных. В рамках исследования «Анализ данных traceroute в RIPE Atlas за 2012–2019 годы» [5] были построены сетевые графы для каждого получасового интервала и разработан алгоритм выявления сбоев узлов или связей, длящихся час и более. Подборка «RIPE Atlas: научные публикации» [6] содержит ссылки на другие научные работы. В их число входят исследования, посвящённые обнаружению «черных дыр» Path MTU, выявлению аномалий маршрутизации и обнаружению сетевых помех.

Важную роль играют и исследования самой платформы, поскольку от её характеристик зависит возможность обобщения полученных результатов. В часто цитируемой работе «Опыт использования платформы RIPE Atlas для проведения измерений» [7] было показано, что распределение зондов по автономным системам (AS) крайне неравномерно, что ограничивает возможности измерений, инициируемых из конкретной исходной AS.

Приведённые в данной статье примеры использования RIPE Atlas показывают, что эта платформа не только незаменима для операционного мониторинга инфраструктуры и услуг организации и её партнеров и провайдеров, но также является ценной инфраструктурой для научно-исследовательской работы. Платформа позволяет реконструировать инциденты постфактум, проверять гипотезы о поведении сети в больших масштабах, а также предоставлять независимые данные для обсуждения вопросов устойчивости Интернета на уровне эксплуатации и выработки политики.

Список литературы:

[1] Day in the Life of RIPE Atlas: Operational Insights and Applications in Network Measurements, https://arxiv.org/html/2511.22474

[2] Does the Internet Route Around Damage? – Edition 2023, https://labs.ripe.net/author/emileaben/does-the-internet-route-around-damage-edition-2023/

[3] Time Warner Cable Outage, https://labs.ripe.net/author/emileaben/time-warner-cable-outage/

[4] RIPE Atlas – A Case Study of AAAA Filtering, https://labs.ripe.net/Members/emileaben/ripe-atlas-case-study-of-aaaa-filtering

[5] Exploring RIPE Atlas Traceroutes from 2012 to 2019, https://labs.ripe.net/author/nevil/exploring-ripe-atlas-traceroutes-from-2012-to-2019/

[6] RIPE Atlas: Scientific Papers, https://labs.ripe.net/author/mirjam/ripe-atlas-scientific-papers/

[7] Lessons Learned From Using the RIPE Atlas Platform for Measurement Research, https://dl.acm.org/doi/10.1145/2805789.2805796

Об авторе:

Юров Андрей Михайлович,
Фонд развития сетевых технологий «ИнДата»



Интернет-измерения: каков вопрос, таков ответ

Павел Храмцов

Аннотация

Измерять в Интернете можно по-разному — всё зависит от того, какую задачу мы решаем.
Если смотреть через призму стека протоколов TCP/IP, то на каждом его уровне можно замерять свои параметры для совершенно разных целей.
Когда говорят о качестве интернет-услуг, обычно имеют в виду соблюдение провайдером условий договора (SLA). Также изучают поведение пользователей, чтобы превратить их технические требования в конкретные задачи для разработчиков.
В последнее время популярность набрали сервисы вроде Downdetector, которые собирают жалобы пользователей на сбои. Это тоже своего рода измерение доступности Интернета, но уже «снизу», глазами обычных людей.
Сейчас много говорят о вкладе Интернета в ВВП и цифровизации экономики. Но на чём основаны эти оценки? Насколько им можно доверять? Как оценить вклад Интернета в традиционные отрасли?
Измерение — это сравнение величины с эталоном для получения точного числа. Но в интернет-измерениях часто сравнивают «тёплое с мягким» — то есть используют некорректные шкалы и метрики. Именно поэтому сегодня мы разберём интернет-измерения через призму теории шкал, чтобы наконец понять: что, с чем и как правильно сравнивать.
.

Ключевые слова:

Интернет-измерения, технометрика, ping, traceroute, tcpdump, whois, RIPE Atlas, RIPE RIS, CAIDA, DNS-OARC, Downdetector

Введение

Само понятие «интернет-измерения» довольно широкое. Можно что-то измерять в рамках стеках протоколов TCP-IP, можно что-то измерять в рамках отдельных приложений, можно измерять «проникновение Интернета», что бы это ни значило, можно измерять физиологические реакции пользователей и составлять различные «тепловые карты», а можно использовать Интернет в качестве социологического опросника.

Можно вообще измерять «мягкое» «тёплым», например, доступность сервиса путём социологического опроса. Собственно, почему нет? Конечному пользователю, в конце концов, важно, чтобы почта ходила и сайт открывался, а не время RTT для утилиты ping.

Измерение, согласно определению Новейшего философского словаря под редакцией Грицанова А.А. [1], — **это процедура присвоения символов наблюдаемым объектам в соответствии с некоторым правилом.**

Китайская модель Qwen 3.7-Plus предлагает рассматривать следующие типы измерений Интернета:

1. **Сетевые и технические измерения:** пропускная способность каналов, задержки, вариации задержек (джиттер), потери пакетов, доступность информационных ресурсов и др.

2. **Веб-аналитику:** количество уникальных посетителей, количество просмотров страниц, глубина просмотра, конверсия и т.п.

3. **SEO-измерения (Search Engine Optimisation — поисковая оптимизация):** позиции в выдаче, индекс цитирования, органический трафик (откуда произошёл переход).

4. **Бизнес-метрики и маркетинг:** стоимость привлечения клиента, пожизненная ценность клиента, окупаемость и возврат затрат на интернет-рекламу, эффективность рекламных объявлений.

Это, конечно, неполный набор. Например, тут есть поисковая оптимизация и нет почтового спама. Опущены измерения информационной безопасности, а также «доля интернет-экономики в ВВП страны». Но в принципе, суть ухвачена верно: Интернет — это инструмент, который нужно калибровать, и которым можно измерять.

Технометрики и технометодики: «от печки»

Самым старым инструментом измерения в Интернете, а точнее, в ARPANET считается утилита ping (1983) [2]. Она появилась через два года после опубликования RFC792 (ICMP-протокол) [3]. Назначение — проверка доступности интернет-адреса. К сожалению там, где протокол ICMP заблокирован, этот старейший инструмент измерений не работает.

Другим старожилом измерений является утилита traceroute, которая была написана в 1987 году [4]. Предназначена для измерения маршрутов и задержек на каждом шлюзе (хопе).

В 1988 году была написана и утилита tcpdump [5] — инструмент для пассивного перехвата и анализа сетевого трафика. Это предтеча Wareshark, который в своей первой версии назывался Etherial и был написан в 1998 году, а в 2008 получил своё современное имя [6].

Заметим, что tcpdump — это не инструмент измерений, а способ получения данных для последующих численных измерений, сопоставлений с образцами, поиска временных последовательностей (измерений в широком философском смысле).

В этом же контексте следует рассматривать и утилиту/сервис whois (протокол и базу данных), который появился в 1982 (RFC812) [7]. Whois для поиска информации о доменных именах, IP-адресах и номерах автономных систем до сих пор является чрезвычайно важным источником данных для «измерений». На основе данных whois строятся, например, кривые внедрения IPv6 или скорость «проникновения Интернета» в национальные экономики.

Хотя появились современные инструменты контроля доступности, перехвата и анализа трафика, мониторинга параметров уровней предоставления услуг, все вышеперечисленные инструменты до сих пор остаются в обойме популярных средств сетевых администраторов. Но это всё же «индивидуальные» средства измерения, которые могут применять сетевые администраторы. Цель таких измерений — поиск неисправностей, контроль состояния среды, решение проблем пользователей и тому подобные задачи, которые возникают в процессе эксплуатации конкретных сетей (локальных, корпоративных, сетей операторов связи).

Однако есть другой предмет изучения — Интернет сам по себе, т.е. глобальные измерения Интернета. И здесь на первый план выходят организации и проекты, которые разрабатывают методики и проводят так называемые глобальные измерения Интернета.

Технометрики и методики: глобальные измерения

Глобальные измерения проводят такие организации, как RIPE NCC, CAIDA, IETF, DNS-OARC, APNIC Labs и различные проекты ICANN.

Наиболее известным проектом RIPE NCC является RIPE Atlas. Официальный запуск проекта RIPE NCC с целью создания крупнейшей сети активных измерений связности сетей был осуществлён в 2010 году. В системе измеряют параметры сетевой связности, доступности и производительности. Измерения опираются на сеть пробников. Пробники проверяют наличие конфигурации под версии протокола IP, собирают данные ping по протоколам IPv4 и IPv6 к двум корневым серверам DNS (k и i) и серверу RIPE, оценивают стабильность измерения к тем же IPv6-адресам, оценивают корректность DNS-резолвинга.

RIPE RIS — это платформа для сбора данных о маршрутизации. Она собирает данные о BGP, протоколе, по которому маршрутизируется трафик между сетями в Интернете. Собирая эти данные, RIS улучшает наше понимание глобальной системы маршрутизации в Интернете.

CAIDA (Center for Applied Internet Data Analysis) — ещё один центр сбора и обработки данных о состоянии глобального Интернета и эффективности используемых в Интернете протоколов и инструментов. Основан в 1997 году при суперкомпьютерном центре в Сан-Диего (США).

CAIDA проводит исследования трафика (на почасовых образцах трафика с магистральных каналов) и таблиц маршрутизации. Результаты своих исследований CAIDA публикует в научной периодике и в материалах научных конференций.

Третьим «столпом» измерений Интернета и исследований на основе этих измерений является APNIC Labs — исследовательское подразделение регионального интернет-реестра APNIC (Asia-Pacific Network Information Centre), которое занимается измерением и анализом развития глобальных интернет-технологий.

Многие свои исследования APNIC Labs проводят в сотрудничестве с Google Research. В частности, различные исследования по внедрению новых DNS-технологий и внедрению

протокола Quick. Основными направлениями исследований являются измерения IPv6; измерения DNS; измерения BGP; измерения использования транспортных протоколов стека TCP/IP; измерения на основе интернет-рекламы.

Все результаты исследований APNIC Labs публикуют в своем блоге. Измерения позволяют оценить скорость внедрения (или «невнедрения») новых стандартов в Интернете, а также выявить причины, по которым происходит торможение внедрения.

Ещё одним независимым исследовательским объединением является DNS-OARC (The DNS Operations, Analysis, and Research Center).

DNS-OARC поддерживает несколько реально больших баз данных DNS-трафика: например, DITL (Day In The Life of the Internet Traces) — двухдневный слепок трафика, который предоставляют участники данного проекта. С 2009 года DNS-OARC является репозитарием файлов зон доменов верхнего уровня (.root, .com, .net, .org, .info, .biz, .name, .asia, .aero, .arpa).

Анализировать данные из баз данных DNS-OARC могут участники объединения, которые платят ежегодные членские взносы (от 1250 долларов США).

Измерения проводятся и в рамках IETF (Internet Engineering Task Force). Если RIPE и CAIDA собирают данные и управляют зондами, то IETF занимается стандартизацией того, как именно нужно измерять Интернет.

Можно выделить несколько групп документов по типам измерений:

- метрики производительности IP (например, RFC2679 [8]);
- протоколы активных измерений (например, RFC8762 [9]);
- протоколы пассивных измерений и терминология (например, RFC5475 [10] и RFC5476 [11]);
- бенчмарки — испытания производительности (например, RFC2544 [12]);
- измерения качества передачи голоса и видео (например, RFC3550 [13]);
- измерения маршрутизации и DNS (например, RFC7854 [14]);
- новые протоколы со встроенными метриками, типа QUIC (например, RFC9000 [15]).

Отдельно существуют документы, которые вводят понятийный аппарат и описания к нему, например, RFC7799 — Active and Passive Metrics and Methods (with Hybrids Types In-Between) [16]. К большому сожалению, на практике эти документы совершенно не знакомы сетевым инженерам, которые относятся к их изучению с определённой долей скепсиса.

ICANN и ее «измерения» находится несколько в стороне от традиционных технометрик и методик. В конечном счёте, все исследования технических комитетов и комиссий ICANN направлены на выработку правил надёжного и безопасного функционирования системы DNS, т.е. на определение параметров уровня предоставления сервиса (SLA), которые затем закладываются в технические требования к контрактам ICANN.

Типичный пример – разработка SLA к контракту по программе new gTDL и требований к системе MoSAPI, которая контролирует/измеряет параметры данного SLA.

Хотя сама математическая модель расчёта доступности сервиса DNS приведена в документе Консультативного комитета системы корневых серверов ICANN (RSSAC047) [17], на практике она применяется и для доменов верхнего уровня. В контрактах ICANN доступность сервиса DNS определена в 100%, что даже жёстче, чем в методике RSSAC047 (99,999% или 5 минут 15 секунд простоя сервиса в год).

Достоверные измерения

Собственно, в этом месте мы приходим к независимой экспертизе приобретаемых услуг, которая опирается на измерения и методики их обработки.

Чтобы экспертиза была признана достоверной, измерения в рамках такой экспертизы должны быть выполнены по общепризнанной методике (см. RFC от IETF, например), и они должны быть выполнены организацией, которой все (в самом общем смысле) или обе стороны контракта доверяют.

Независимый внешний аудит позволяет определить случаи нарушения контрактных обязательств.

Для независимого аудита можно использовать тот же RIPE Atlas, Catchpoint, ThousandEyes (от Cisco), Pingdom (от Solar Wings) или платформу измерений Фонда «ИнДата».

Можно разработать свой инструмент тестирования и согласовать в рамках контракта его использование с исполнителем. ICANN, например, разработала свою методику тестирования инфраструктуры регистратур — Registry System Testing (RST).

Для подтверждения доверия к исполнителю можно воспользоваться результатами проверки на соответствие ISO27001.

Наиболее достоверные данные дают измерения, выполненные непосредственно с рабочих мест конечных пользователей — это системы уровня RUM (Real User Monitoring). Именно такие измерения проводят, например, на JavaScript, который исполняется непосредственно в браузерах пользователей.

К слову сказать, и они могут оказаться недостоверными, если нарушены принципы репрезентативности выборок, на основе которых делаются выводы.

В ряде контрактов заказчик просит исполнителя предоставить логи сервисов для анализа. В этом случае применяются технологии защиты логов — Merkle Tree или BlockChain.

«Пузомерки» — рейтинги

В последнее время термин «Интернет» всё чаще означает не сеть передачи данных, а набор услуг, которые на этой сети нагромождены. Собственно, этот набор услуг саму передачу данных тоже включает.

Каждую услугу или все вместе конечный пользователь хочет получить в заданном качестве и по минимальной цене.

Обычно так формулируются целевая функция и ограничения в этой оптимизационной задаче конечного пользователя массовой услуги. Обратное — получить максимальное качество при фиксированной цене — это госзаказ со всеми рисками такой формулировки задания.

Выбор исполнителя происходит на основе сравнения в рамках рейтинга, например, рейтинга провайдеров мобильного Интернета в заданной географической области.

В основе рейтингов лежат так называемые шкалы, на основе которых и производится измерение, т.е. присвоение некоторого символа некоторому объекту.

Согласно теории шкал Стивенсона существует четыре типа шкал: номинальная (шкала наименований), порядковая (ранговая шкала), интервальная (шкала разностей), отношений (абсолютная шкала).

Приведём ещё несколько примеров номинационных шкал. Например, шкала использования доменных имён (рисунок 1):



Рис. 1. Цели использования доменных имён в национальном домене .ru.

Хотя справа от разноцветной стопки на рисунке 1 и указаны цифры, фактически на рисунке представлен результат раскладывания доменов по корзинкам, т.е. присвоения им метки.

На рисунке 2 представлен другой тип шкалы и её отображения — интервальная шкала.

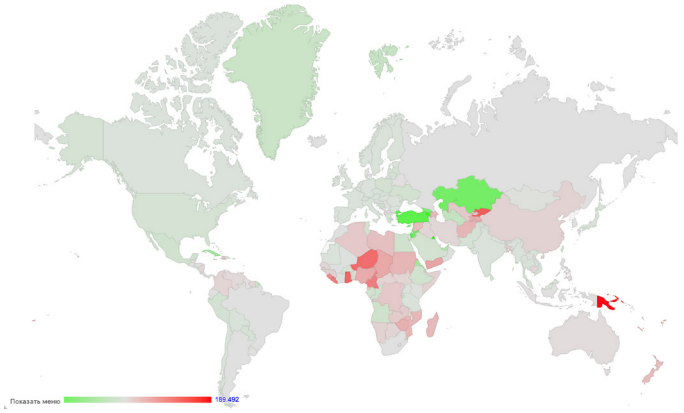


Рис. 2. Скорость RTT в зависимости от протокола IPv4/IPv6 (APNIC labs [18]).

В легенде карты задана непрерывная шкала, которую можно рассматривать как шкалу отношений. Она разбита на равные интервалы, однако у неё нет абсолютного нуля (то есть она не может быть шкалой). Цвет на карте меняется скачком в зависимости от попадания в интервал. Нельзя сказать, что показатели измеряемой величины в Казахстане в два раза лучше, чем в Новой Зеландии.

Есть ещё один нюанс — репрезентативность данных на таких картах и при таких измерениях. В России пробников RIPE Atlas крайне мало, да и те, что есть, нестабильны. О репрезентативности выборок на основе таких измерений говорить не приходится.

Порядковые шкалы — это, собственно, и есть рейтинги. Например, один провайдер услуг доступа в Интернет лучше другого, но вот насколько он лучше, в рамках такой шкалы не определено.

Типичной порядковой шкалой, например, является шкала критичности инцидентов. Пример такой шкалы представлен в таблице 1:

Таблица 1 – Сроки исполнения заявок

Категория заявки	Приоритет заявки	Время реакции, часы	Макс. время исполнения заявки, часы
Инцидент	Критичный	0,5	4
Инцидент	Высокий	0,5	72
Инцидент	Средний	0,5	120
Инцидент	Низкий	0,5	240
Консультация	Не применимо	1 рабочий день	Не применимо

Приоритеты описываются в техническом задании на сервис. Например, приоритет «Критичный» может быть определён как «полное нарушение доступности сервиса продолжительностью более 5 минут. Срок исправления не может превышать четырёх часов».

Очень часто ранговые шкалы используются в качестве маркетинговых инструментов. Например, размещение ссылки на информационный ресурс в выдаче поисковой машины – это измерение, связанное с назначением порядкового номера в выдаче. Поисковая оптимизация — это коммерческая деятельность, которая целенаправленно влияет на значения метрик, которые используются в алгоритме подсчёта рангов. Так, например, американский патент US7058628B1 [19], выданный Lawrence Page в 2001 году, как раз является таким ранжирующим алгоритмом, который применялся в Google при его основании.

Можно привести и другие рейтинги. Например, шкала доступности, которой пользуются сайты типа Downdetector.

В данном случае никаких технических измерений, которые описаны в RFC IETF, никто не проводит. Измеряется количество жалоб конечных пользователей на те или иные сервисы (компании).

Для представления результата используется шкала наименований: «нет проблем», «возможны проблемы», «есть проблемы».

При сборе данных от конечных пользователей учитывается конкретная локация, включающая страну. Не каждая жалоба попадает в расчёт. Существуют фильтры, которые, например, отсекают множественные жалобы за короткий промежуток времени на одну и ту же проблему с одного и того же аккаунта.

Проблемы фиксируются относительно некоторой базы измерений. В конце концов существует некая фоновая величина ошибок сервиса, которые следует исключить из классификации.

Таким образом, доступность сервиса измеряется не в результате измерения, полученного утилитой типа ping, а в результате обработки жалоб конечных пользователей, т.е. буквально «тёплое» измеряется «мягким».

Интернет-экономика: что бы это ни значило

Последнее время стало модно говорить о вкладе Интернета в экономику страны и об интернет-экономике вообще. Коснёмся этой скользкой темы, так как это тоже имеет отношение к измерениям в Интернете.

Цели, задачи, основные измеряемые показатели цифровой экономики приведены в программе «Цифровая экономика Российской федерации» [20] и в её продолжении в виде национального проекта «Экономика данных и цифровая трансформация государства» [21]. Те, кому интересны детали, могут ознакомиться с ними, используя ссылки из списка литературы. Мы же остановимся на измерениях, которые стали основой для оценки влияния физических параметров на финансовые потоки цифровых платформ.

В 2006 году инженер Amazon Грег Линден (Greg Linden) в своём блоге «Geeking with Greg» написал, что 100 мс задержки соответствуют ~1% выручки компании. Эта метрика получила название «правило 100 миллисекунд».

В том же 2006 году Марисса Майер (Marissa Ann Mayer) на конференции Web 2.0 сообщила цифры потерь клиентов при задержке загрузки страниц. Так 0,5 секунды задержки загрузки страницы приводит к потере 20% просмотров страниц, т.е. 0,5 секунды полностью обнуляют удовлетворённость конечного пользователя и приводят к отказу от использования сервиса. Измерения проводились при анализе посещения Google Maps.

Вообще говоря, на основе таких измерений была опубликована таблица пересчёта задержек в потери дохода (таблица 2) [22].

В зависимости от оборота компании указанные проценты могут превратиться в немалые деньги.

Ещё одно интересное исследование на эту тему, «Миллисекунды делают миллионы», — совместное исследование Google и Deloitte [23] — было опубликовано в 2020 году.

Таблица 2. Влияние задержки/ускорения загрузки страницы на доходы компании

Задержка/ Ускорение	**Google (2017)** Падение конверсии при увеличении времени загрузки страницы	**Amazon (2018)** Падение продаж при увеличении времени загрузки страницы	**Walmart (2019)** Увеличение конверсии при сокращении времени загрузки	**HubSpot (2020)** Короткие визиты на сайт (просмотр только одной страницы)
100 мс	1%	1%		
200 мс	4%			
500 мс	12%	20%		
1 с	20%	50%	2%	9%
2 с			8%	38%
3 с			15%	66%
> 3 с				95%

Тип платформы	Примеры	Что измеряют в первую очередь
Транзакционные (Marketplaces)	Amazon, Wildberries, Airbnb, «Яндекс Маркет»	GMV (общий объём товарооборота), Take Rate (комиссия платформы), конверсия воронки покупки.
Инновационные / Технологические	AWS, Yandex Cloud, iOS, Android, Kubernetes	Uptime (99,99%), latency API, количество активных разработчиков, объём потреблённых ресурсов.
Контентные и социальные	YouTube, VK, Telegram, Spotify	DAU (Daily Active Users) и MAU (Monthly Active Users), время сессии (Time Spent), виральность (коэффициент Шарра) — эффективность программ типа «приведи друзей», CPM (стоимость тысячи показов рекламы).
Интеграционные (B2B / Industrial)	Salesforce, «1С:Предприятие», промышленный IoT	Скорость адаптации (onbarding) клиентов, API call success rate, снижение операционных затрат (OPEX) клиентов.

Таблица 3. Цифровые платформы

Измеряли время реальных загрузок страниц мобильных сайтов в секторах ретейла, путешествий (travel), люксовых товаров и лидогенерации. Исследование показало, что улучшение скорости мобильного сайта всего на 0,1 секунды приводило к росту конверсии в ретейле на 8,4% (и росту среднего чека на 9,2%), а в сфере путешествий — на 10,1%.

Поиск зависимости типа «физические параметры -> деньги» не такая простая задача. Например, в таблице 2 все данные, кроме данных Amazon, приведены для зависимости «время -> конверсия», т.е. как влияет задержка или её отсутствие на действия пользователя на сайте. Но это не деньги! Точно так же, как BGP-таблица — это отнюдь не реальный маршрут пакетов.

Для того, чтобы найти зависимость дохода/убытков от временных задержек, нужно «протащить» действия пользователей и, например, рекламные кампании (их идентификаторы) через расчётную систему. В вебе это делается через механизм cookies, а для сведения результатов измерений различных протоколов и данных разных логов, например, веб и DNS, это зачастую делают через так называемые wildcard-домены и выпуск для них TLS-сертификатов.

А теперь вернёмся к цифровым платформам, упомянутым в государственных программах. Именно к ним все приведённые выше измерения задержек имеют прямое отношение. Для классификации платформ можно использовать таблицу 3.

Цифровые платформы — это хорошо и перспективно, но и о доходах провайдеров подключения к интернету (ISP — Internet Service Provider) забывать тоже не стоит.

Одна из популярных моделей биллинга ISP — это модель 95-го перцентиля. Это фактически международный стандарт тарификации интернет-канала для B2B-клиентов (дата-центров, провайдеров, крупных сайтов), который отсекает 5% самых высоких пиков трафика в месяце и выставляет счёт по наибольшему значению из оставшихся 95%.

Провайдер замеряет использование канала каждые 5 минут (288 измерений в сутки, 8640 в месяц), потом отбрасывает 5% самых высоких значений (пиковые всплески). Биллинг идет по оставшемуся максимальному значению.

До сих пор речь, главным образом, шла о доходах. А каковы расходы? Экономия средств достигается за счёт внедрения новых технологий (цифровизация бизнесов, цифровая трансформация и т.п. термины). Но основной статьёй расходов стала информационная безопасность.

Как измеряют страх

Глобально все измерения «страха» сводятся к защищённости трафика (подслушивание и подмена), безопасности маршрутизации, экспозиции уязвимостей и измерению мощности и частоты различных типов атак.

Защищённость трафика — это, в первую очередь, уровень внедрения TLS-сертификатов. Для национальной доменной зоны .ru такую статистику можно посмотреть, например, на сайте «Технического центра Интернет» [24]. Методика измерений и отдельные аспекты статистики использования были представлены в статье Александра Венедюхина «Анализ информации TLS-сертификатов оконечных узлов и меток времени (SCT) для российских логов Certificate Transparency», опубликованной в журнале «Интернет изнутри» № 23 в прошлом году [25].

Безопасность маршрутизации — это внедрение технологии RPKI (Resource Public Key Infrastructure или инфраструктура открытых ключей для интернет-ресурсов). Статистику RPKI можно посмотреть, например, на сайте CloudeFlare (рисунок 3).

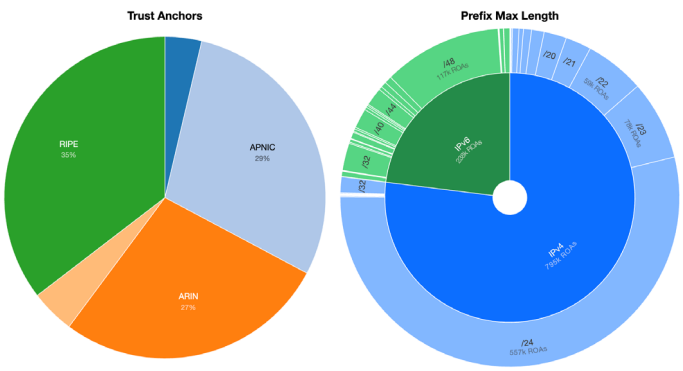


Рис. 3. Статистика RPKI.

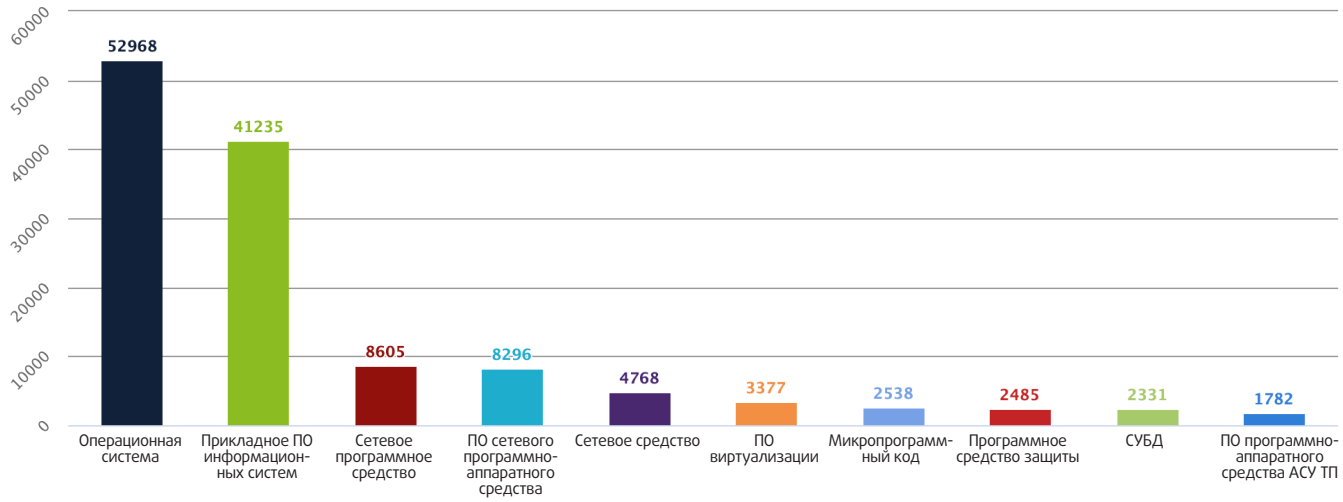


Рис. 4. Распределение уязвимостей по типам программного обеспечения.

Отчёты о сканировании информационных ресурсов Интернета на предмет уязвимостей можно найти на сайтах Национальной базы данных уязвимостей США (NVD) [26] или Банка данных угроз безопасности информации (БДУ ФСТЭК) [27] (рисунок 4).

Динамику количества уязвимостей можно посмотреть на сайте NVD (рисунок 5). Каждая уязвимость помечена числовым кодом CWE (Common Weakness Enumeration).

В доменной индустрии принято выделять не столько безопасность, сколько репутацию доменов (доменных зон). В российских национальных доменных зонах этим вопросам посвящён, например, проект «Нетоскоп» [28]. Он был запущен Координационным центром доменов .RU/.РФ (КЦ — cctld.ru) в 2012 году.

К слову сказать, мировое сообщество в лице ICANN дозрело до аналогичного проекта только в сентябре 2025 (проект Domain Metrica). До этого в 2017 году ICANN запустила исследовательский проект DAAR, но он не содержал «изюминки» «Нетоскопа» — агрегации доменов по признаку принадлежности к одному аккаунту в базах данных регистраторов доменов. В Domain Metrica это свойство появилось, что позволяет проактивно ставить на мониторинг «спящие» домены, которые могут быть задействованы в случае блокировки доменов, уличённых в распространении фишинга, вредоносного ПО, управления ботнетами и (с некоторыми оговорками) спама.

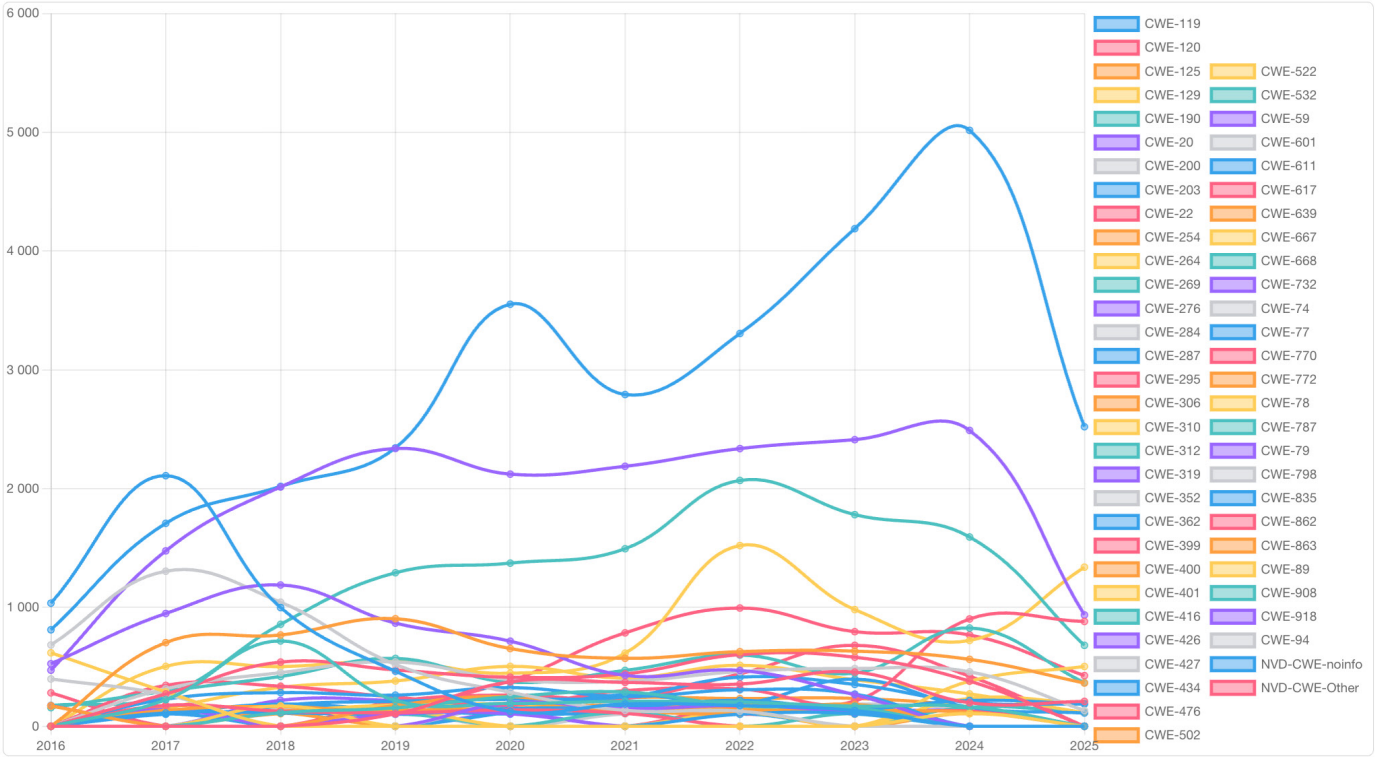


Рис. 5. Динамика обнаружения уязвимостей.

Подводя черту

Интернет как явление можно измерять. Измерять различными способами и различными инструментами. Делать это можно из альтруистических соображений или из меркантильного интереса. Учитывая глубокое проникновение Интернета во все сферы нашей жизни, второй мотив превалирует.

Технические измерения Интернета — это инструмент профессионалов-инженеров. Рейтинги — инструмент маркетинга. Номинационные и интервальные шкалы — инструмент, заложенный в контракты. Анализ трафика — инструмент для обеспечения информационной безопасности. И это далеко не полный перечень различных типов измерений и целей их проведения.

Измерения в Интернете и Интернета — это всегда эксперимент, даже когда эти измерения носят регулярный характер по ранее определённой методике. Каждый раз необходимо повторять стандартные шаги, описанные в теории проведения эксперимента:

1. **Определить цель и вид эксперимента** (цель и вид могут «плыть», т.е. видоизменяться в зависимости от исполнителя и текущей возможности проведения).
2. **Уточнить условия проведения измерений** (например, появление новых блокировок или, наоборот, маршрутов).
3. **Обратить внимание на списки входных и выходных параметров** (возможно, появились новые зависимости или какие-то параметры стали независимыми).
4. **Проверить, сохранилась ли адекватность выбранной математической модели** (на различных этапах жизненного цикла модель может изменяться — исчерпали пространство адресов IPv4, например).
5. **Определиться с точностью измерений** (одно дело — определить годовую тенденцию, а другое — дать прогноз с учётом циклических месячных/недельных/суточных колебаний).
6. **Строго придерживаться плана проведения измерений**, чтобы добиться повторяемости условий проведения — только в этом случае результаты измерений можно будет сравнивать (они должны ложиться в выбранную шкалу).
7. **Выбрать методику обработки результатов**, чтобы они были статистически значимыми (для номинационных шкал это столь же важно, как и для интервальных, например, в случае Downdetector).
8. **В заключении необходимо дать объективную и непредвзятую оценку** (очень часто вину за неполадки списывают на ТСПУ или НСДИ. Например, 11 октября 2026 года была проведена ротация ключей в корневой зоне DNS, и у тех провайдеров, где резолверы не подхватили автоматическую замену ключа и остались на старых ключах, DNSSEC перестал работать. НСДИ и её резолверы в данном случае к самой проблеме валидации DNSSEC отношения не имели).

Всё в первом приближении достаточно просто и одновременно довольно сложно. Но ведь именно этому учит высшая школа.

Список литературы:

[1] Под редакцией Грицанова А.А. Новейший философский словарь. б.м.: Книжный дом, 2003. ISBN 985-428-636-3.

[2] History of Ping. [В Интернете] Joseph Scott, 13 10 2014 г. [Цитировано: 25.10.2026 г.] https://josephscott.org/blog/2014/10/history-of-ping-2/

[3] Postel, J. RFC 792: STD 5: Internet Control Message Protocol. RFC EDITOR. [В Интернете] 9 1981 г. [Цитировано: 25.10.2026 г.] https://www.rfc-editor.org/info/rfc792/

[4] The creation of TRACEROUTE. reddit. [В Интернете] SyberSecWithHaikuInc, 8 2026 г. [Цитировано: 25.10.2026 г.] https://www.reddit.com/r/computerscience/comments/1vok2aj/the_creation_of_traceroute/

[5] Michael Richardson (mcr), Bill Fenner. TCPDUMP&Libpcap. [В Интернете] 1999 г. [Цитировано: 25.10.2026 г.] https://www.tcpdump.org/

[6] A Brief History Of Wireshark. Wireshark.org. [В Интернете] [Цитировано: 25.10.2026 г.] https://www.wireshark.org/docs/wsug_html_chunked/ChIntroHistory.html

[7] Harrestien, Ken. RFC 812: NICNAME/WHOIS. RFC EDITOR. [В Интернете] 1 Март 1982 г. [Цитировано: 25.10.2026 г.] https://www.rfc-editor.org/info/rfc812/

[8] G. Almes, S. Kalidindi, M. Zekauskas. RFC 2679: AOne-way Delay Metric for IPPM. RFC EDITOR. [В Интернете] September 1999 г. [Цитировано: 26.10.2026 г.] https://www.rfc-editor.org/info/rfc2679/

[9] G. Mirsky, G. Jun, H. Nydell, R. Foote. RFC 8762: Simple Two-Way Active Measurement Protocol. RFC EDITOR. [В Интернете] March 2020 г. [Цитировано: 226.10.2026 г.] https://www.rfc-editor.org/info/rfc8762/

[10] T. Zseby, M. Molina, N. Duffield, S. Niccolini, F. Raspall. RFC 5475: Sampling and Filtering Techniques for IP Packet Selection. RFC EDITOR. [В Интернете] March 2009 г. [Цитировано: 26.10.2026 г.] https://www.rfc-editor.org/info/rfc5475/

[11] B. Claise, Ed., A. Johnson, J. Quittek. RFC 5476: Packet Sampling (PSAMP) Protocol Specifications. RFC EDITOR. [В Интернете] March 2009 г. [Цитировано: 26.10.2026 г.] https://www.rfc-editor.org/info/rfc5476/

[12] S. Bradner, J. McQuaid. RFC 2544: Benchmarking Methodology for Network Interconnect Devices. RFC EDITOR. [В Интернете] March 1999 г. [Цитировано: 26.10.2026 г.] https://www.rfc-editor.org/info/rfc2544/

[13] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. RFC 3550: STD

64: RTP: A Transport Protocol for Real-Time Applications. RFC EDITOR. [В Интернете] July 2003 г. [Цитировано: 26.10.2026 г.] https://www.rfc-editor.org/info/rfc3550/

[14] J. Scudder, Ed., R. Fernando, S. Stuart. RFC 7854: BGP Monitoring Protocol (BMP). RFC EDITOR. [В Интернете] June 2016 г. [Цитировано: 26.10.2026 г.] https://www.rfc-editor.org/info/rfc7854/

[15] J. Iyengar, Ed., M. Thomson, Ed. RFC 9000: QUIC: A UDP-Based Multiplexed and Secure Transport. RFC EDITOR. [В Интернете] May 2021 г. [Цитировано: 26.10.2026 г.] https://www.rfc-editor.org/info/rfc9000/

[16] Morton, A. RFC 7799: Active and Passive Metrics and Methods (with Hybrid Types In-Between). RFC EDITOR. [В Интернете] May 2016 г. [Цитировано: 26.10.2026 г.] https://www.rfc-editor.org/info/rfc7799/

[17] Root Server System Advisory Committee (RSSAC). RSSAC047 | RSSAC Advisory on Metrics for the DNS Root Servers and the Root Server System. ICANN.org. [В Интернете] 12 March 2020 г. [Цитировано: 26.10.2026 г.] https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-047-12mar20-en.pdf

[18] APNIC Labs. V6/V4 RTT Comparison by country (ms). Stats.labs.apnic.net. [В Интернете] 26 October 2026 г. [Цитировано: 26.10.2026 г.] https://stats.labs.apnic.net/v6perf

[19] Page, Lawrence. Method for node ranking in a linked database. Google Patents. [В Интернете] 4 September 2001 г. [Цитировано: 26.10.2026 г.] https://patents.google.com/patent/US7058628B1/en

[20] Министерство цифрового развития (Минцифры). Национальная программа «Цифровая экономика Российской Федерации». digital.gov.ru. [В Интернете] 31 Июль 2017 г. [Цитировано: 26.10.2026 г.] https://digital.gov.ru/target/naczionalnaya-programma-czifrovaya-ekonomika-rossijskoj-federaczii

[21] Национальный проект «Экономика данных и цифровая трансформация государства». digital.gov.ru. [В Интернете] 7 Май 2025 г. [Цитировано: 26.10.2026 г.] https://digital.gov.ru/target/naczionalnyj-proekt-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva

[22] Tencent Cloud Community. The Real Impact of Latency on Conversion Rates: Why Every 100ms Matters for Your Business. trancentcloud.com. [В Интернете] [Цитировано: 26.10.2026 г.] https://www.tencentcloud.com/techpedia/143892

[23] Deloitte.Digital. Milliseconds make Millions. Thinkwithgoogle.com. [В Интернете] 2020 г. [Цитировано: 26.10.2026 г.] https://www.thinkwithgoogle.com/_qs/documents/9757/Milliseconds_Make_Millions_report_hQYAbZJ.pdf

[24] Технический Центр Интернет. Статистика TLS. Домены России. [В Интернете] 26 Октябрь 2026 г. [Цитировано: 26.10.2026 г.] https://statdom.ru/tld/ru/report/certscount/#36

[25] Анализ информации TLS-сертификатов оконечных узлов и меток времени (SCT) для российских логов Certificate Transparency. Александр Венедюхин, Павел Якубов. Москва: «Интернет изнутри», Т. 23.

[26] National Institute Of Standards and Technology. National Vulnerability Database. nvd.nist.gov. [В Интернете] 26 October 2026 г. [Цитировано: 26.10.2026 г.] https://nvd.nist.gov/

[27] ФСТЭК России. Банк данных угроз безопасности информации. Банк данных угроз безопасности информации. [В Интернете] 26 Октябрь 2026 г. [Цитировано: 26.10.2026 г.] https://bdu.fstec.ru/charts

[28] Координационный Центр Национального домена Сети Интернет. Нетоскоп. Нетоскоп. [В Интернете] 2013 – 2026 г. [Цитировано: 26.10.2026 г.] https://netoscope.ru/

[29] Postel, J. RFC792. [В Интернете] ISI, 981 г. https://www.rfc-editor.org/info/rfc792/

Об авторе:

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



MSK IX

ПЛАТФОРМА MSK-IX

Сервисы цифровой устойчивости

Для операторов, медиа, облаков, интеграторов и бизнеса.
Нейтральная инфраструктура. Национальный масштаб.

INTERNET EXCHANGE

Прямая сетевая связность

Минимальная задержка (Latency) между участниками IX
Локализация трафика

ANYCAST DNS

DNS-хостинг

Размещение DNS-зон на DNS-узлах трёх континентах, использующих единую IP адресацию. SLA - 99,999%

IX GUARD

Защита от DDoS-атак

Снижение рисков и предотвращение потерь выручки из-за простоя
L3 / L4 / L7 / ПАК

NTP-IX

Сервис точного времени

Единое точное время для всей инфраструктуры

DNS-RESOLVER

Высоконадёжный резолвер

Для быстрого и безопасного доступа к сети Интернет

Узнайте, как MSK-IX усиливает устойчивость вашей сети

1150+ участников экосистемы MSK-IX

Internet Exchange / Instanet / DNSSEC / BGP-аналитика
Защищённые пиринговые группы

msk-ix.ru

Реклама. Рекламодатель АО «ЦВКС «МСК-IX». ИНН: 7733661269

Использование обратного трафика (backscatter) QUIC для анализа конфигураций развёртывания гипергигантов

Йонас Мюкке

Аннотация

В статье рассматривается, как пассивный анализ обратного трафика QUIC может выявить конфигурации его развёртывания у основных поставщиков контента, включая Google, Meta (признана в России экстремистской организацией - ред.) и Cloudflare. Используя данные сетевого телескопа, потоковые записи и активные измерения, исследование показывает, что даже небольшие объёмы нежелательного трафика могут раскрыть поведение повторной передачи и информацию, закодированную в идентификаторах соединений QUIC.

Эти результаты демонстрируют, что защита конфиденциальности QUIC не препятствует идентификации деталей инфраструктуры, включая конфигурации балансировщиков нагрузки и схемы развёртывания в сетях. Такие данные могут помочь в измерении сети и планировании пропускной способности, но также способны раскрыть операционную информацию, которую злоумышленники могут использовать для атаки на конкретные компоненты инфраструктуры.

Ключевые слова:

QUIC, сетевой телескоп, идентификаторы соединений CID, поставщики контента

Протокол QUIC повышает уровень конфиденциальности, однако пассивные измерения всё равно позволяют раскрыть детали его развёртывания. Используя данные сетевого телескопа, мы проанализировали поведение QUIC у крупнейших контент-провайдеров и проверили наши выводы с помощью данных о сетевых потоках (flow data) и активных измерений.

Протокол QUIC (RFC 9000) [1], широко внедряемый крупными контент-провайдерами (так называемыми гипергигантами), обещает низкую задержку в сочетании с шифрованием и улучшенной конфиденциальностью. Несмотря на эти механизмы защиты, мы обнаружили, что пассивные измерения могут раскрыть детальную информацию о конфигурациях развёртывания QUIC у гипергигантов.

Отправной точкой нашего исследования стал простой вопрос: что мы можем узнать о развёртываниях QUIC, просто прослушивая нежелательный трафик? Этот вопрос становится особенно интересным, поскольку QUIC стремится к повышению конфиденциальности путём сокрытия (obfuscation) метаданных.

В нашем исследовании мы использовали сетевой телескоп и потоковые записи QUIC. Сетевые телескопы пассивно регистрируют «фоновое излучение» Интернета (Internet Background Radiation) [2]: трафик от вредоносных и безвредных сканеров, а также ответы на пакеты с поддельным исходным адресом (так называемый обратный трафик, backscatter). Примечательно, что наш анализ использует этот ответный трафик, вероятно, генерируемый злоумышленниками, в безвредных исследовательских целях. Для оценки полноты картины и проверки наших результатов мы также провели активные измерения.

Данные телескопа были предоставлены Калифорнийским университетом в Сан-Диего (UCSD) [3] и охватывали префиксы IPv4 /9 и /10. Мы рассмотрели по одному месяцу пакетов QUIC за каждый год с 2021 по 2025. Чешская национальная исследовательская сеть CESNET [4] предоставила данные о потоках (flow data) за те же месяцы в 2024 и 2025 годах, что позволило нам верифицировать наблюдения телескопа. Каждое свойство, упомянутое в этой статье, было дополнительно проверено по записям сетевых потоков.

Мы проанализировали различные характеристики пакетов QUIC, полученных телескопом. В этой статье мы сосредоточимся на трафике от серверов Cloudflare, Google и Meta*; более подробная информация содержится в нашей полной научной работе.

На рисунке 1 отображены временные интервалы между первым полученным пакетом и последующими обнаруженными повторными передачами в рамках одного соединения. Эти пакеты повторно отправляются серверами QUIC в ответ на поддельный трафик, который серверы воспринимают как исходящий от неотвечающих клиентов. Пики указывают на типичные конфигурации того, когда и как часто эти сообщения отправлялись повторно.

В 2025 году первая повторная передача происходила через 0,1 с в 94% соединений QUIC от Meta*, через 0,3 с в 51% соединений от Google и через 1,0 с в 67% соединений от Cloudflare. За исключением Cloudflare (где в 2022 году 31% соединений имели интервал 0,3 с), это наблюдение оставалось стабильным на протяжении всего периода измерений, хотя доля наиболее частых интервалов варьировалась. На отметке 0,1 мс мы зафиксировали больше повторных передач, чем самих соединений QUIC от

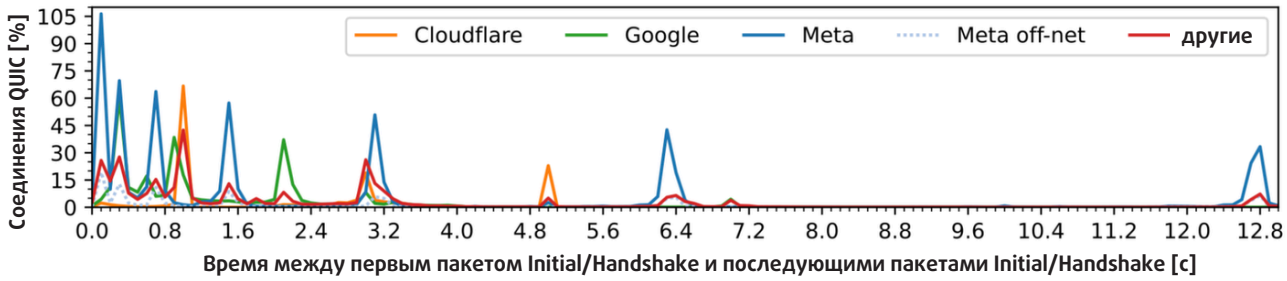


Рис. 1. Конфигурации повторной передачи у серверов QUIC, видимые в обратном трафике (backscatter), когда сервер отвечает на пакеты с поддельным адресом отправителя из диапазона телескопа. Конфигурации серверов Google и Meta остаются неизменными на протяжении всего периода наблюдения (здесь показаны данные за 2025 год). Все гипергиганты используют экспоненциальное увеличение интервала повторных попыток (exponential backoff).

Meta*. Мы выяснили, что в этих соединениях выполнялось две повторные отправки с интервалом ~0,1 мс.

Мы наблюдали экспоненциальное увеличение интервала повторных попыток (exponential backoff) в тайм-аутах повторной передачи от серверов Cloudflare, Meta* и Google. Максимальное количество повторных отправок различалось у гипергигантов, что показывает, что их серверы требуют разных объёмов ресурсов для поддержки соединения.

В целом мы зафиксировали самые короткие тайм-ауты повторной передачи и наибольшее количество повторных передач у Meta*. Это указывает на то, что Meta* быстрее реагирует на потерю пакетов и ожидает более коротких задержек между клиентами и серверами, чем Google и Cloudflare. В сравнении с этим, Google и Cloudflare резервируют меньше ресурсов для обработки ошибок соединений, что снижает их уязвимость к QUIC-флуд-атакам, направленным на переполнение состояний системы.

Пакеты Retry редко используются для защиты от атак типа «отказ в обслуживании» (DoS)

Пакеты QUIC Retry позволяют серверам проверять адрес клиента, требуя, чтобы клиент повторно подключился с использованием токена Retry, выданного сервером. Такие пакеты Retry могут быть эффективны против QUIC-флуд-атак, но добавляют задержку в один RTT. Мы увидели, что такая стратегия защиты применяется относительно редко. Cloudflare начала применять Retry в 2025 году, и 3% её пакетов QUIC были пакетами Retry. Это указывает на то, что при развёртывании приоритет отдаётся соединениям с низкой задержкой, а не смягчению последствий DoS-атак.

Идентификаторы соединений (CID) несут информацию

QUIC использует идентификаторы соединений (Connection ID, CID) для привязки пакетов к конкретным сессиям вместо привычных для TCP и UDP комбинаций IP-адреса и порта. Серверные CID могут стать источником утечки данных, если гипергиганты кодируют в них служебную информацию. Такое кодирование искажает ожидаемое случайное распределение значений серверных CID.

Рисунок 2 визуализирует частоты значений полубайтов (ниббблов) серверных CID (SCID), отслеженные в обратном трафике. Частоты, отклоняющиеся от ожидаемого случайного распределения, показывают, что серверные CID кодируют определённую информацию.

Исключительно пассивным методом мы смогли наблюдать в обратном трафике, что все гипергиганты кодируют информацию в CID. Полученные характерные шаблоны можно использовать для обнаружения развёртываний в чужих сетях (off-net) за пределами автономной системы (AC) гипергиганта. Подробности и точность этого метода обсуждаются далее в нашей полной статье.

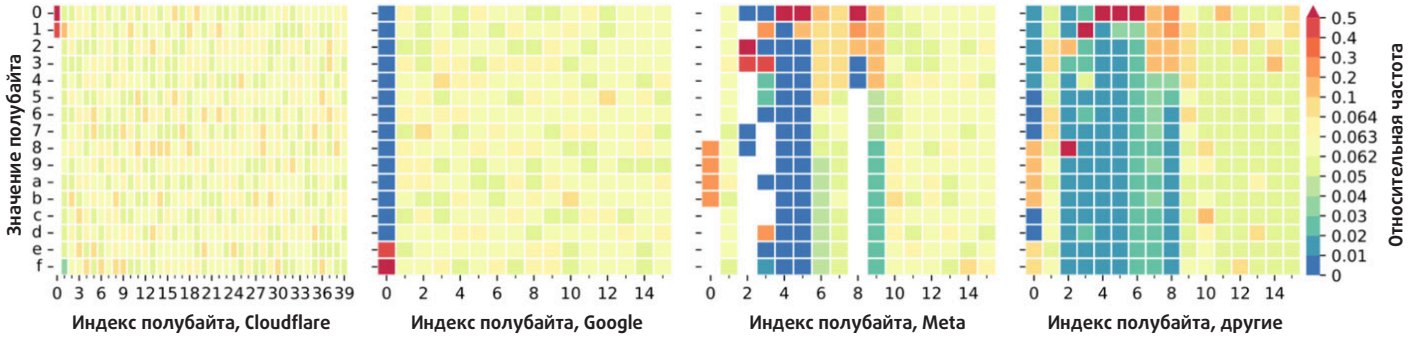


Рис. 2. Относительные частоты значений SCID (серверного CID) в обратном трафике за 2024 год. Неравномерное распределение по столбцам указывает на кодирование информации (например, у Google). Группа «Другие» содержит шаблоны, сходные с шаблонами Meta и Google.

В 2021 и 2022 годах серверные CID от Google имели случайное распределение. Однако в 2023 и 2024 годах конфигурация балансировщика нагрузки изменилась. Мы увидели, что серверные CID начинались с ob11 в 99 % (2023 г.) и с ob111 в 99,9 % (2024 г.) пакетов с длинным заголовком. Согласно драфту IETF «Generating Routable QUIC Connection ID» [6], можно сделать вывод, что Google не кодировал серверные CID информацией для помощи в балансировке нагрузки. Удивительно, но реализация QUIC от Google использует формат этого драфта, но не использует CID для балансировки.

Реализация QUIC от Meta* (mvfst) [7] кодирует детали о хостах, воркерах, процессах и версию этого кодирования внутри серверного CID. Наличие более высокой плотности определённых значений в первых пяти байтах указывает на то, что Meta* в настоящее время кодирует информацию в серверных CID.

Наблюдение за миграцией конфигурации балансировщика нагрузки

Тщательное отслеживание обратного трафика QUIC от Meta* позволило нам зафиксировать миграцию на новую конфигурацию балансировщика нагрузки: переход с версии 1 серверного CID на версию 2 в июле 2023 года (см. рисунок 3).

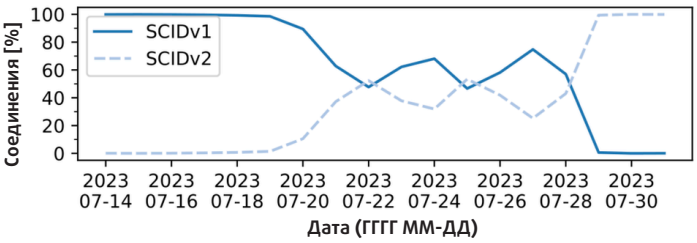


Рис. 3. Версия кодирования SCID в соединениях Meta* в обратном трафике. С 19 по 29 июля 2023 года Meta* перешла на SCIDv2.

Миграция заняла 10 дней, и последующие активные измерения подтвердили эти изменения.

До этой миграции идентификаторы хостов (host ID) обозначали отдельные экземпляры балансировщиков нагрузки. После миграции Meta* стала использовать одни и те же идентификаторы хостов в разных кластерах. Мы подробно описываем наш метод определения кластеров в следующем разделе.

Раскрытие количества балансировщиков нагрузки у Meta*

Обнаружив кодирование информации и даже кодирование конкретных идентификаторов балансировщиков нагрузки в нашем пассивном наборе данных, мы задались вопросом: насколько полным было наше представление и можем ли мы заполнить потенциальные пробелы с помощью активных измерений? С этой целью мы просканировали все IP-адреса QUIC, активные на тот момент (до 7355 адресов в 2025 году) в AC 32934 (Meta*). Для каждого IP-адреса мы выполнили 20 тысяч рукопожатий, последовательно уменьшая порт клиента.

Мы сгруппировали IP-адреса в кластеры, где один и тот же идентификатор хоста использовался несколькими IP-адресами в одном префиксе /24. Мы проверили полученную структуру кластеров с помощью обратного разрешения DNS: международный код IATA, закодированный в PTR-записях DNS всех виртуальных IP-адресов (VIP) кластера, был идентичным, показывая, что кластеры ограничены одним префиксом /24. Этот метод позволил выявить количество балансировщиков нагрузки на кластер.

Мы сравнили количество идентификаторов хостов в обратном трафике с нашими активными измерениями. Если в 2023 году 2366 соединений QUIC позволили обнаружить 93% всех идентификаторов хостов в кластере, то в 2025 году, после перехода на новую структуру, мы достигли 100% покрытия всего с 545 соединениями QUIC. Это связано с меньшим медианным количеством балансировщиков нагрузки на кластер. По сравнению с активными измерениями, обратный трафик зафиксировал наибольшую долю идентификаторов хостов Meta* в 2023 году – 29%.

Рисунок 4 показывает распределение размеров кластеров, наблюдаемых по всему миру. Более подробную информацию о структуре и использовании кластеров можно найти в нашей полной статье.

Почему стоит использовать пассивные измерения?

Наш анализ показал, что:

1. Даже небольшие объёмы обратного трафика раскрывают конфигурации стека QUIC у гипергигантов.

2. Подсчет (enumeration) экземпляров балансировщиков нагрузки возможен с высокой точностью при наличии менее 1000 поддельных соединений QUIC в обратном трафике.

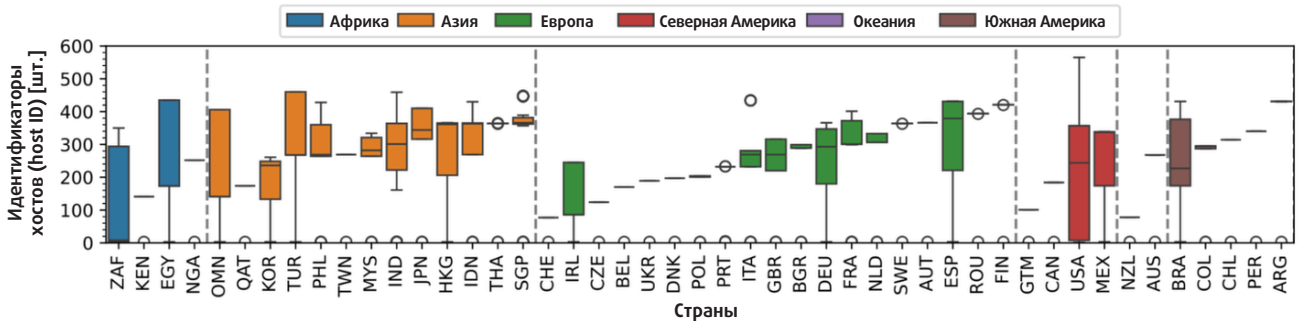


Рис. 4. Балансировщики нагрузки седьмого уровня (L7LB) Meta в разбивке по странам, 2025 год. В точках присутствия (PoP) азиатского региона используется больше L7LB (число идентификаторов хостов, host ID).

Наблюдения из пассивных измерений воспроизводимы с помощью активных, но активные измерения требуют предварительного знания о потенциальных целях, создают дополнительный сетевой трафик и могут спровоцировать срабатывание систем обнаружения вторжений (СОВ). Измерения с помощью телескопа помогают улучшить активные измерения, поскольку они проливают свет на реальное поведение трафика QUIC. Учитывая разнообразие существующих библиотек QUIC, воспроизведение реалистичного поведения для активных измерений представляет собой сложную задачу.

Будет ли расти использование структурированных идентификаторов соединений?

Структурированные CID могут служить отпечатком (fingerprint) конкретных гипергигантов. Мы обнаружили, что Google перешёл на такие CID в 2023 году, и мы увидели характерное кодирование информации в обратном трафике от Akamai, Amazon, Apple, Cloudflare, Fastly, Meta* и Microsoft. Мы полагаем, что использование структурированных CID будет со временем расти, поскольку они упрощают детальную маршрутизацию, контролируемую провайдером.

Однако стандартизация может ограничить уникальность этих идентифицирующих свойств и, как следствие, нашу способность связывать их с конкретными гипергигантами. Более того, расширенные функции QUIC, такие как миграция клиента, требуют кодирования дополнительных данных в таких идентификаторах, чтобы снизить накладные расходы на синхронизацию состояния соединения.

Наш метод обнаружения развёртываний в чужих сетях (off-net) применим и к другим развёртываниям и методам измерений, таким как потоковые записи без эталонных данных из реализаций с открытым исходным кодом. Обнаружение балансировщиков седьмого уровня у Meta*, поскольку только Meta* использует кодирование в открытом виде.

Каковы последствия знания количества балансировщиков нагрузки?

Кодирование целевого балансировщика нагрузки в идентификатор соединения позволяет клиентам направлять трафик на конкретные адреса. Это нежелательное поведение, поскольку злоумышленники могут сфокусировать трафик на одном балансировщике, обойдя механизмы предотвращения единой точки отказа (single point of failure).

Хотя количество экземпляров не раскрывает их реальную пропускную способность и вычислительную мощность, знание их распределения в географическом регионе или размера отдельного кластера можно использовать для оценки нагрузки, необходимой для перегрузки этой точки присутствия (PoP). Эта информация ценна не только для злоумышленников, но и для конкурентов, позволяя им предвидеть бизнес-возможности и локальную конкуренцию, оценивать важность региона и улучшать собственную инфраструктуру.

Почему обнаружение развёртываний в чужих сетях (off-net) важно для сетевых операторов

Понимание и прогнозирование трафика между сетями является сложной, но необходимой задачей для обеспечения стабильных интернет-соединений с низкой задержкой. Получение более подробных сведений об обмене трафиком (например, о типах взаимодействующих серверов) может улучшить планирование ёмкости или позволить обнаружить нежелательный трафик.

Детальная информация об инфраструктуре, встроенная в идентификаторы соединений QUIC, может выявить репликацию кеша между развёртываниями в чужих сетях (off-net) – деятельность, которая обычно тарифицируется принимающими сетями как транзит.

Для получения более подробной информации о конфигурациях развёртывания Akamai, Amazon, Apple, Fastly и Microsoft рекомендуем ознакомиться с нашей полной статьёй «Waiting for QUIC: Passive Measurements to Understand QUIC Deployments» [8], представленной на конференции CoNEXT в декабре 2025 года.

Если вы хотите глубже изучить трафик QUIC, CESNET (один из поставщиков данных для этой работы) публикует набор данных, охватывающий подробные потоки QUIC, записанные на границе сети CESNET за один год: с июня 2024 года по май 2025 года [9].

Список литературы

[1] https://www.rfc-editor.org/rfc/rfc9000.html

[2] https://en.wikipedia.org/wiki/Internet_background_radiation

[3] https://www.caida.org/projects/network_telescope/

[4] https://www.cesnet.cz/

[5] https://dl.acm.org/doi/10.1145/3768988

[6] https://datatracker.ietf.org/doc/draft-ietf-quic-load-balancers/

[7] https://github.com/facebook/mvfst

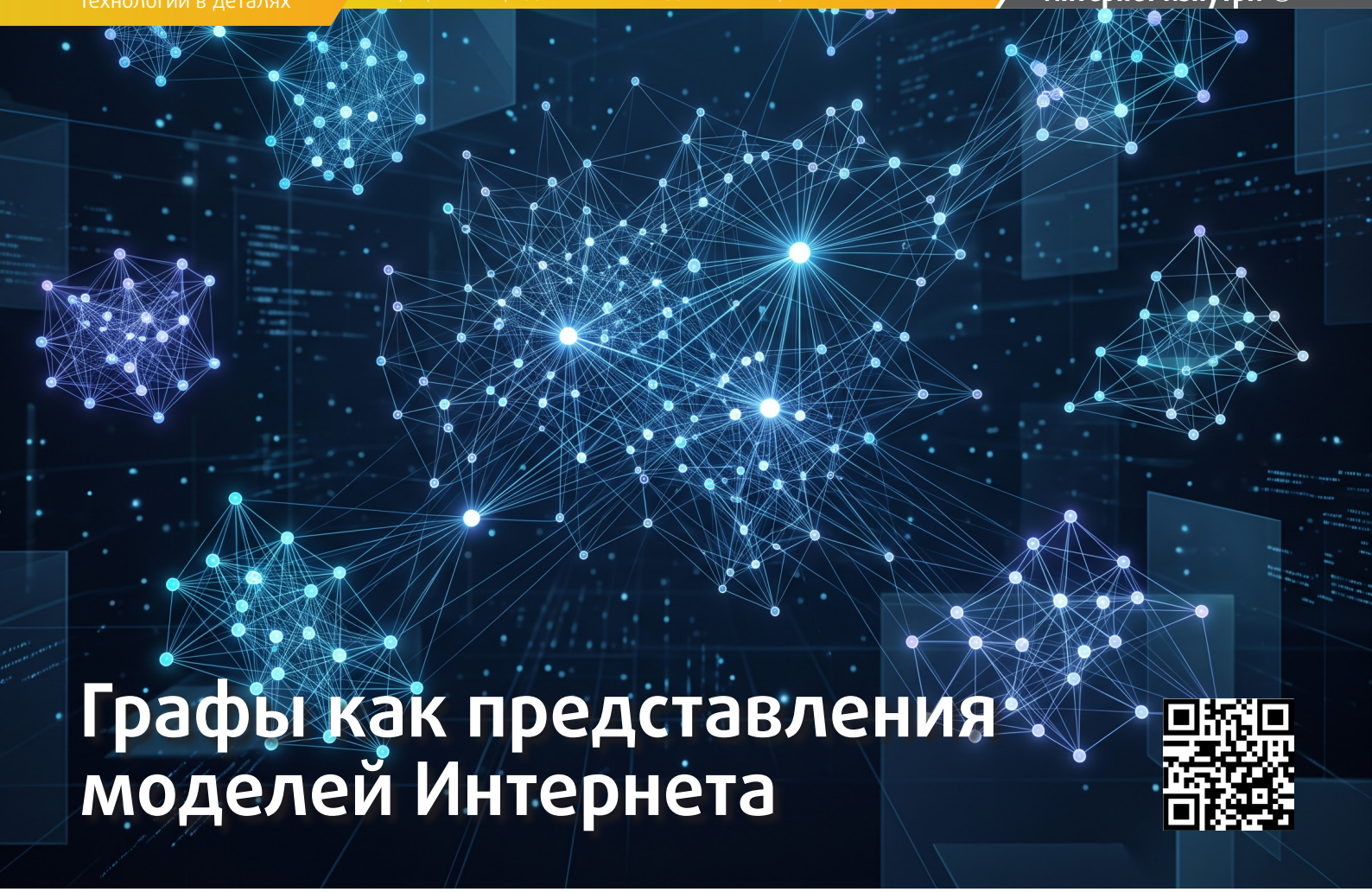
[8] https://dl.acm.org/doi/10.1145/3768988

[9] https://zenodo.org/records/17249078

Об авторе:

Йонас Мюкке – аспирант и научный сотрудник кафедры распределённых и сетевых систем Технического университета Дрездена. Его исследования сосредоточены на активных и пассивных измерениях для лучшего понимания сложных веб-инфраструктур. Он особенно интересуется дополнительными сведениями, которые можно получить благодаря QUIC.

* Meta Platforms Inc. признана экстремистской организацией, и её деятельность запрещена на территории Российской Федерации



Графы как представления моделей Интернета

Александр Венедюхин

Аннотация

Статья рассказывает о роли графов как инструмента визуализации логики взаимодействия элементов вычислительных сетей и как средства исследования моделей Интернета. Граф является естественным воплощением вычислительной сети. С ростом сложности сетей, с появлением концепции межсетевого взаимодействия меняется не только сложность соответствующих графов, но и появляются новые уровни для их применения. Например, ориентированные графы и алгоритмы на графах непосредственно лежат в основе спецификации протокола маршрутизации OSPF, а в практике DNS алгоритмы теории графов непосредственно применяются для обнаружения CNAME-циклов и других «рекурсивных» проблем делегирования в DNS-зонах.

.

Ключевые слова:

визуализация, DNS, граф, BGP, сетевая связность, вычислительные сети, маршрутизация, система доменных имён

Концепция графа как разновидности чертежа сразу же кажется самым логичным инструментом, который нужно применять для анализа вычислительных сетей, поскольку сеть – это граф по определению. С другой стороны, эта концепция достаточно разносторонняя для того, чтобы внутри неё скрывалось немало неочевидных интересных моментов.

Вычислительные сети начинаются с построения линии связи между тремя узлами-компьютерами. Двух – недостаточно. Зато три дают базовый набор элементов для построения содержательного графа, но тут всё банально: вершины – это узлы-компьютеры; а рёбра – линии связи.

Компьютерная сеть – всегда граф. Поэтому она и называется «сетью». Будь то локальная сеть внутри здания или более сложная система, объединяющая несколько университетов.

Сложнее с «большим Интернетом» – это объединение сетей стоит особняком: не бывает одного-единственного «графа Интернета», но Интернет может быть представлен многими различными графами, полученными на основе анализа различных представлений Сети.

Конечно, что касается истории Интернета, тут все помнят знаменитую историческую схему ARPANET, которая, во-первых, граф, а во-вторых, охватывает весь APRANET. Но то ARPANET, а не Интернет. Тем более, не современный Интернет. В современном Интернете добавлено достаточно много нового, чтобы сделать существование единого графа невозможным.

За разными представлениями Интернета скрываются разные графы, плавный переход без потери информации между ними неосуществим.

Рассмотрим, например, таблицы маршрутов, то есть таблицы BGP. Практически всякая непустая таблица – это представление графа: в случае BGP их записывают в таблицу, так как зарисовывать линии и вершины в окне текстового терминала неудобно. Но охватывает ли одна BGP-таблица весь Интернет? Нет, не охватывает. Даже и не приближается: максимально полные варианты, которые принято называть Full View, зависят от точки наблюдения, в которой маршруты получены.

Занимательно, что этот эффект действует даже на крупнейших операторов, которые составляют так называемый Tier 1 Интернета (ядро Backbone). Да, может показаться, что эти операторы, по определению, «видят» всех остальных участников «напрямую», через пользовательские подключения, без «аплинков». Для Tier 1 как бы нет независимых точек сборки BGP, а поэтому и таблицы маршрутов для них должны бы сворачиваться в тот самый «граф Интернета». Однако операторов Tier 1 в современном Интернете несколько, и они всё же обмениваются трафиком между собой, поэтому BGP-граф ни одного из них не является «графом всего Интернета».

Интересным направлением является изучение того, как разные варианты Full View в BGP переходят один в другой при смене точки наблюдения. Заметьте, что такие переходы тоже можно изобразить в виде сложного графа, но этот граф не будет соответствовать ни одному из исходных графов Full View: дело в том, что при переходе от графа к графу будут схлопываться и исчезать некоторые рёбра, потому что в разных Full View одна и та же AS может быть видна по-разному, иметь разных соседей, и это схлопывание происходит так, что уже нельзя признать исходные графы эквивалентными.

Из-за того, что «соседства» различаются, графы становятся несовместимыми; был маршрут <--a<--e<--f; но он поменялся на <--k<--e--f, а так как теперь больше нет ребра a--e, то и графы оказываются «несовместимы». (рисунок 1)

Собственно, из принципов схлопывания рёбер и вырастает спецификация BGP: если бы граф Интернета существовал, то и необходимости в BGP не возникало бы – маршруты были бы известны заранее.

Спецификации многих сетевых протоколов, не обязательно непосредственно определяющих Интернет, но точно лежащих в его фундаменте, прямо используют концепцию графа для того, чтобы протокол определить. Чтобы не раздувать текст, не будем перечислять все такие протоколы, а ограничимся некоторыми узнаваемыми:

- **Spanning Tree** – самый очевидный пример, он противодействует циклам, изымая из графа лишние рёбра; циклы, а точнее, алгебра, связанная с ними, – один из краеугольных камней математического фундамента теории графов;
- **Open Shortest Path First (OSPF)** – прямо использует самый знаменитый алгоритм теории программирования – алгоритм Дейкстры, который работает на графе;
- **Routing Information Protocol (RIP)** – основан на алгоритме Беллмана-Форда поиска путей на графе;
- **IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL)** – обнаружение специальных узлов при помощи представления ориентированного графа.

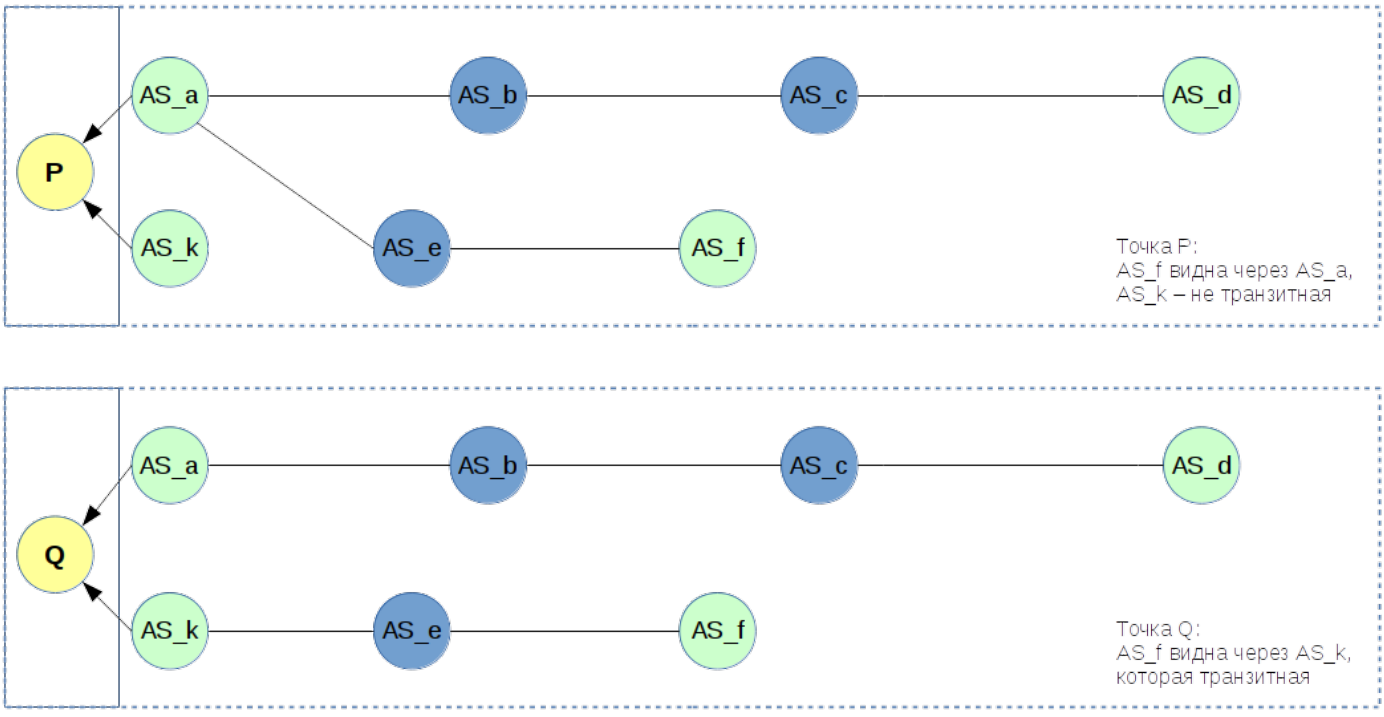


Рис. 1. «Несовместимые» графы BGP-соседств.

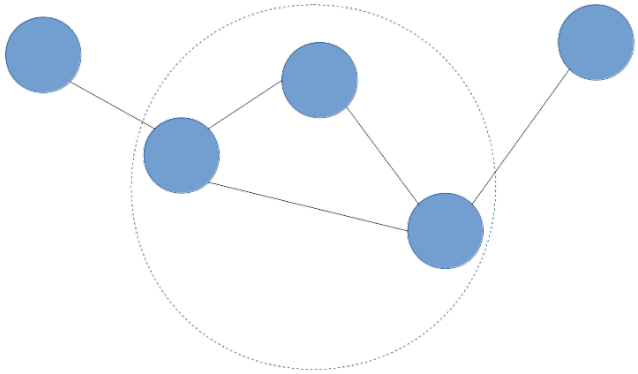


Рис. 2. «Минимальный» содержательный цикл.

Строго говоря, для построения цикла достаточно двух вершин, но для практических вычислительных сред это не работает: требуется три вершины для настоящего цикла и ещё две для задания большей структуры, в которой данный цикл только и виден как проблемный (или ценный?) «элемент». Дело в том, что простейший цикл из двух вершин (узлов), «ссылающихся» друг на друга, не является циклом в смысле вычислительных сетей: это просто два узла, обменивающихся пакетами данных; а вот пять вершин (узлов) уже позволяют построить структуру, в которой пакеты, отправленные из двух крайних, «неполносвязных» узлов, «застревают» в цикле из трёх узлов-коммутаторов. (рисунок 2)

От модели к модели меняется интерпретация. Что считается вершинами, а что – рёбрами? Зависит от модели. Но сам граф как инструмент остаётся всегда. То есть для сетей свойства именно графов имеют универсальное значение, при этом отображаются в разные феномены, связанные с глобальной сетью.

Воплощением графа может быть и набор физических кабелей, и описание правил доставки пакетов в IP-сети, и иерархия доменов в DNS. Графы действуют в каждом воплощении одинаково, а изучение того, как это действие трансформирует подлежащие объекты при переходе между моделями, даёт дополнительную структурную информацию.

Например, дерево DNS можно наложить на граф IP-сети, и это позволит не только выделить соотношения между разными уровнями сетевого транспорта, но и применить инструменты, выстроенные на одном уровне, к анализу данных другого уровня.

Уровни, рёбра и вершины

На уровне физических сетевых соединений вершинами являются сетевые интерфейсы (не обязательно «для проводов»), а рёбрами – кабели различной физической природы и прямые радиоканалы. Это источник интересных примеров, которые, с одной стороны, простейшие, а с другой – отражают сложные физические аспекты построения сетей.

Заметьте, что сейчас, в большинстве случаев, граф физических соединений будет состоять из одного ребра и двух вершин. Этого недостаточно даже с точки зрения синтеза вычислительной сети. Поэтому-то на практике тут, на физическом уровне, возможны и более сложные варианты соединений: кольцо, шина, набор колец, набор шин и т.д. Почему? Во-первых, потому, что сетевой интерфейс – это лишь интерфейс: для того, чтобы ввести сетевое взаимодействие и начать говорить о том, что пакеты ходят между сетевыми интерфейсами, нужно добавить коммутатор, который превратит схему «точка-точка» в сетевую структуру с обработкой адресов участников на выделенном устройстве (на коммутаторе). Внедрение в схему коммутатора приведёт к переходу на новый уровень, где рёбра графа будут разных видов. Во-вторых, с физической точки зрения, кабель, задающий среду распространения сигнала, может совместно использоваться несколькими интерфейсами – и это уже движение в другую сторону: кабель общий, но граф схемы соединений разбивает этот кабель на рёбра.

В предыдущем абзаце мы говорим про сетевые интерфейсы как про устройства с развитой логикой — они могут распознавать формат сетевого пакета, выбирать адреса и так далее. То есть, логически разделять один физический кабель на несколько рёбер графа, которые, тем не менее, соединяют одни и те же вершины. В этом направлении можно спуститься и чуть ниже, на уровень, который нередко называют просто Links и в котором никакой логики интерфейсов уже нет. Тогда рёбра останутся теми же кабелями, а вот вершины станут физическими портами сетевых интерфейсов: «розетками», куда эти кабели подключаются. Обратите внимание, это один из интересных трансформационных примеров: из концепции графа удалили свойства сетевых интерфейсов вычислительных устройств, исчезла сетевая составляющая, осталась только «электрическая» (оптика тут тоже относится к «электрике»).

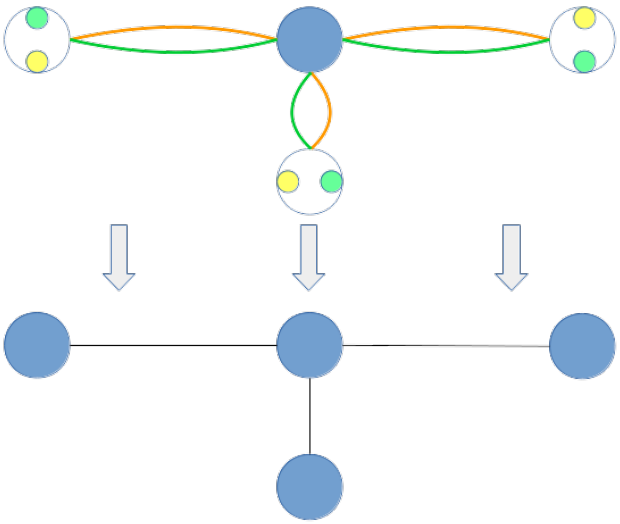


Рис. 3. «Забывание» сетевой логики.

На графе сетевой логики может быть отражено разбиение на подграфы, соответствующие разным логическим сетям (верхний граф), при этом, если ту же сеть рассматривать с чисто «электрической» точки зрения, то рёбра «схлопываются» (нижний граф). (рисунок 3)

На уровне локальной IP-подсети вершины – это узлы с заданным IP-адресом, а рёбра – логические связи между узлами и подсетями. Локальная подсеть IP оказывается полносвязным графом, вне зависимости от того, как именно построена её физическая реализация.

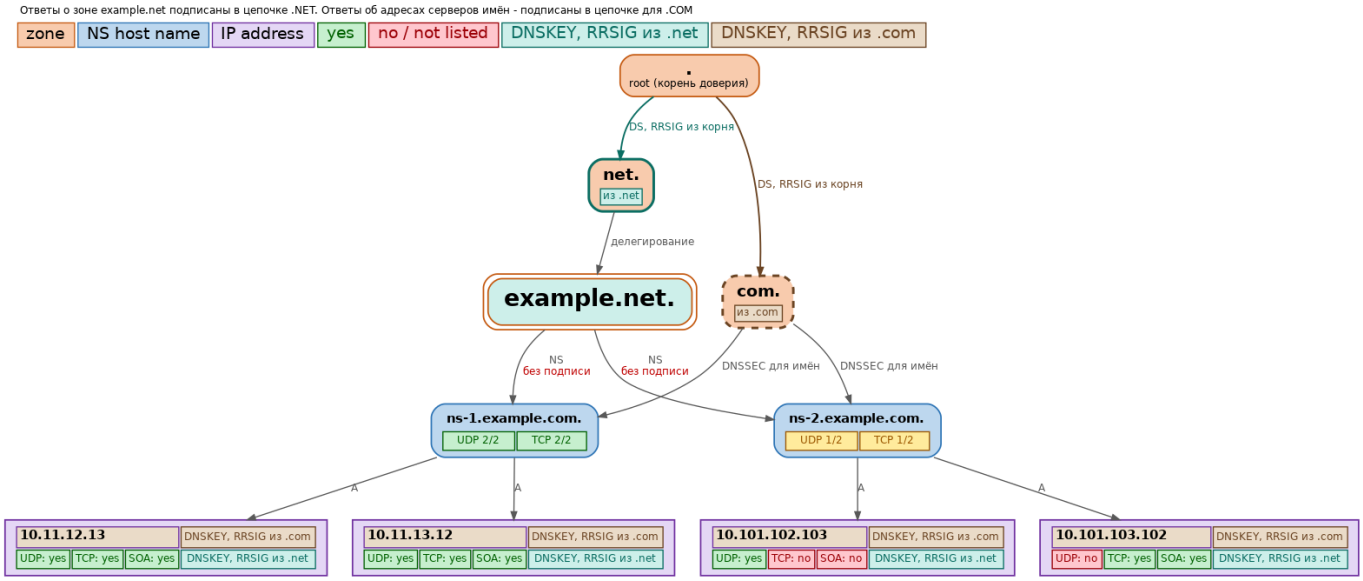


Рис. 4. Разные зоны DNSSEC в одной DNS-зоне.

Переключая модели по узлам и рёбрам, теория графов продвигается через уровни модели OSI. Если узлами являются коммутаторы уровня сетевого протокола с адресацией, то рёбрами становятся логические каналы связи. Примером будет Ethernet. Заметьте, что это ещё далеко не IP. В современном Интернете одни протоколы надстраиваются над другими, далеко не всё сразу видно. Например, эффекты MPLS заметны на уровне ICMP, но MPLS – это совсем другая история, история про наложенные логические структуры.

Свойства наложенных структур – того, что обычно называют «оверлеем», – нередко определяются путём измерений свойств узлов и каналов связи между этими узлами. Так, обнаружить особенности MPLS можно через наблюдение над временем распространения ICMP-пакетов. Но заметьте, что для того, чтобы детально описать происходящие процессы (разные пути пакетов в разных направлениях и пр.), уже потребуется изучить и как-то изобразить свойства узлов и каналов связи. В результате тоже получится граф: например, разные пути «туда» и «обратно» обязательно станут разными рёбрами графа. Предположения о схеме MPLS возникают именно из свойств получившегося графа: здесь скорость соединения соответствует весу путей по графу, количество «хопов» между узлами – промежуточные вершины чётных степеней, разбиение узлов на подмножества – подграфы, сохраняющие чётность степени, эйлеровы пути.

Это работает не только для чисто сетевой инфраструктуры. Так, для DNS граф, связывающий DNS-имена и веб-узлы, основывается на понятии о том, как именно происходит обмен данными в IP-сети при поиске адресов для DNS-имён, то есть при рекурсивном опросе DNS.

Графы и DNS

ФРСТ «ИнДата» в настоящее время заканчивает разработку веб-сервиса отображения DNS-графов. Этот сервис позволит в автоматическом режиме строить графы логических связей в DNS-зоне, заданной пользователем. На уровне DNS графы полезны тогда, когда требуется выяснить то, как влияют на доступность ресурса разные сегменты сетевой инфраструктуры. Например, какие доменные зоны, выглядящие как независимые, используют одну и ту же сетевую инфраструктуру? Что перестанет работать в веб-сервисе, если окажется недоступна какая-то часть доменной инфраструктуры, с ним связанной? Ответы далеко не всегда очевидны, даже несмотря на то, что типовая DNS-схема – это иерархическое дерево, один из относительно простых видов графов.

Прежде всего, DNS-зона практически всегда зависит от других DNS-зон: например, авторитетные серверы имён могут адресоваться записями из совсем другой зоны. Такая зависимость интересно проецируется в область DNSSEC.

Отображение иерархии ключей DNSSEC – та область, где можно эффективно применять графы в роли средства визуализации. Вряд ли DNSSEC вообще возможно внятно визуализировать другим способом. Конечно, существует «табличный» подход (см., например, известный сервис https://dnssec-analyzer.verisignlabs.com/), и он по-своему хорош, но только графы эффективны в отображении свойств, задающих иерархию (см. https://dnsviz.net/).

DNSSEC вносит существенное дополнение в DNS: иерархия в DNSSEC выстраивается по ключам, а не по именам серверов и «вложенности» ответов по делегированию. Делегирование и имена DNS-серверов в DNSSEC являются транспортом для получения набора ключей, а сама доверенная иерархия имён выстраивается уже по этим ключам. Это существенное нововведение. И именно поэтому в DNSSEC не удостоверяется цифровой подписью список делегирования зоны. Естественно, все эти особенности можно описать и «построчно», указывая ключи и их названия. Но визуализация в качестве графа сильно упрощает процесс.

Пример, показывающий, что иерархия ключей DNSSEC создаёт параллельные зависимости на уровне цифровых подписей; здесь example.net делегирована на серверы с именами в зоне example.com, и ответы об адресных записях серверов имён подписываются по независимой цепочке, ведущей к зоне .com, при том, что делегирующий ответ не подписан вовсе. (рисунок 4)

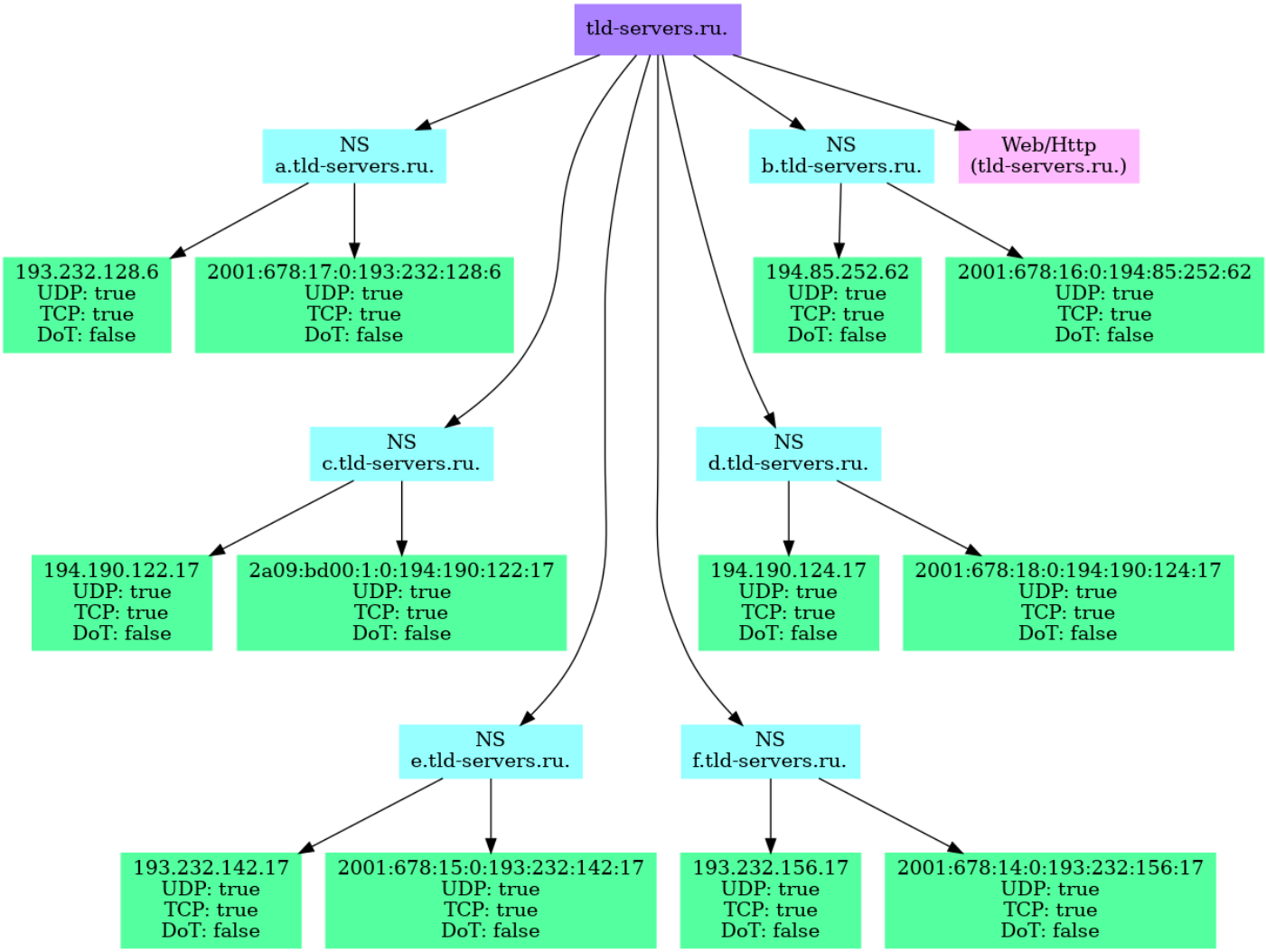


Рис. 5. Граф авторитетных серверов для tld-servers.ru.

Для DNS можно построить графы разных типов. Например:

- привычная иерархия имён зон и имён авторитетных серверов: здесь вершинами являются имена DNS-зон и авторитетных серверов, а рёбра – это факт наличия DNS-зоны в ответе авторитетного сервера; тут есть неочевидные моменты: так, в случае CNAME-записи имени хоста может соответствовать каноническое имя в другой зоне, и наоборот;

- имя авторитетного сервера и соответствующие IP-адреса: вершины – это имена серверов и IP-адреса, а рёбра – «отношение адресации», то есть данный IP-адрес указан в адресной записи для имени авторитетного сервера; здесь уже возникают неочевидные эффекты, например, имён серверов может быть много, но все они указывают на один IP-адрес; есть соотношение «IP-адрес – префикс – оператор», соответственно, ребро графа, ведущее к вершине с IP-адресом, указывает и на префикс конкретного оператора; это позволяет обогащать DNS-графы BGP-информацией.

Веб-сервис отображения DNS-графов, разрабатываемый ФРСТ «ИнДата», позволит в интерактивном режиме получать отображение не только собственно состава авторитетных серверов и их адресов, но и статуса смежных прикладных протоколов, не только относящихся к DNS. Для авторитетных серверов проверяется доступность и по UDP, и по TCP (TCP является необходимым транспортом для DNS), поддержка DNS over TLS (в настоящий момент – очень редко встречается на авторитетных серверах). Проверяются адресные записи для апекса зоны и доступность веб-сервера по соответствующим адресам, также исследуются MX-записи.

DNS-зона tld-servers.ru., в которой размещена часть имён авторитетных серверов зоны ru.; в данном формате, помимо имён серверов и адресов, выводится доступность по UDP/TCP/DoT; показаны IPv4/IPv6-адреса. (рисунок 5)

Национальный домен .ru вместе с зоной зависимости tld-servers.ru.; показаны только IPv4-адреса; одно из имён авторитетных серверов .ru находится в зоне tld-servers.ru., на графе видно, что данная зона используется строго в качестве носителя имени, поскольку авторитетные серверы этой зоны показывают на те же IP-адреса, что и другие имена NS для .ru. (рисунок 6)

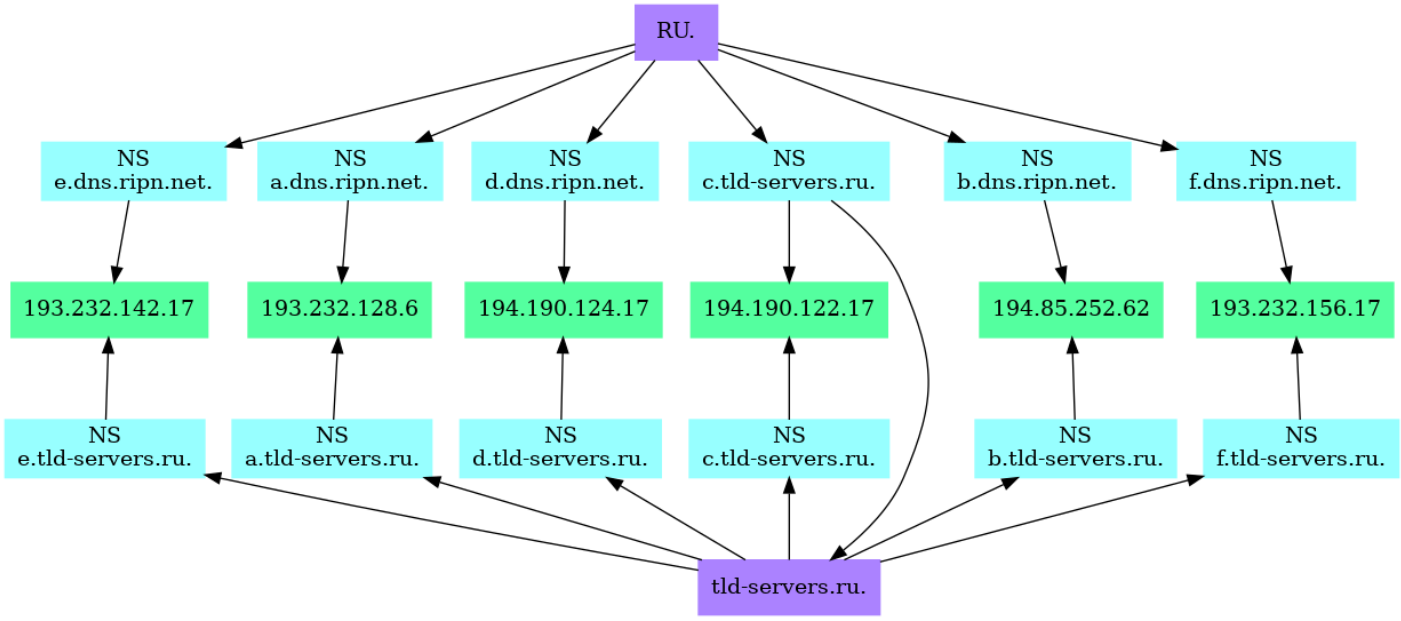


Рис. 6. Граф авторитетных серверов для зоны верхнего уровня .ru.

***

Математика графов является очень развитой областью, которую мы почти не затронули, сосредоточившись на прикладных, технических аспектах. В Интернете структуры, являющиеся графами, тоже возникают не только в DNS. Например, такая структура, известная как хеш-дерево (дерево Меркла), оказывается центральным механизмом, позволяющим применять постквантовые криптосистемы цифровой подписи в TLS и в DNS так, что эффективно экономятся байты интернет-трафика (большинство постквантовых криптосистем цифровой подписи используют очень длинные ключи и большие блоки подписи, что сильно затрудняет прямое их использование, особенно в DNS). То есть наблюдение, что граф – первичен, не выводится только из того, что Интернет – это объединение сетей. Возникновение графов в интернет-технологиях обусловлено геометрией не столько самих сетей, сколько технологий, которые позволяют сети эффективно применять.

Список литературы:

Храмцов П.Б., «Связность и идентификаторы Интернета», «Интернет Изнутри», eISSN: 2949-1967, № 22, 2025.

Венедюхин А.А., «DNS как источник глобальной информации о сети», «Интернет Изнутри», eISSN: 2949-1967, № 12, 2019.

Moy, J., RFC 2328, OSPF Version 2, https://www.rfc-editor.org/info/rfc2328/

Mockapetris P., RFC 1034, https://www.rfc-editor.org/rfc/rfc1034

DNSViz – Monitoring, Analysis, and Visualization, DNS-OARC, Oct. 2013, https://indico.dns-oarc.net/event/1/contributions/41/

GRAPHViz, «Dot language», https://graphviz.org/doc/info/lang.html

Gansner E., Koutsofios E., North S., «Drawing graphs with dot», Jan. 2015, https://graphviz.org/pdf/dotguide.pdf

Gieben M. et al., Go DNS library, https://github.com/miekg/dns

Об авторе:

Александр Анатольевич Венедюхин,
ФРСТ «ИнДата», Россия, Москва.



Matisse: визуализация задержек в Интернете в виде многообразий[1]

Стивен Ясина, Локман Саламатиан, Джошуа Мэтьюз, Скотт Андерсон, Пол Барфорд, Марк Кровелла, Уолтер Уиллинджер

Аннотация

Многообразия – это сложные топологические пространства, которые могут использоваться для представления наборов данных реальных измерений. Визуализация таких многообразий помогает иллюстрировать их топологические характеристики (например, кривизну) и даёт понимание важных свойств исходных данных (например, аномалий в измерениях).

В этой статье описывается новая методология и система для построения и визуализации многообразий, которые выводятся из фактических измерений сетевых задержек в Интернете между разными городами и спроецированы на двумерное евклидово пространство (например, географическую карту). Наш метод использует серию графов, которые фиксируют важную информацию, содержащуюся в данных, включая чётко определённые местоположения для вершин и информацию о кривизне Риччи для рёбер[2] .

Затем наш алгоритм визуализации строит криволинейную поверхность (многообразие), на которой: а) сохраняются географические положения вершин; б) значения кривизны Риччи рёбер графа определяют свойства кривизны многообразия. Итоговое многообразие выделяет области критической связности и определяет экземпляр «пространства интернет-задержек», где измерения задержки отображаются в виде геодезических линий. Мы подробно описываем наш метод и его реализацию в системе Matisse, предназначенной для создания, визуализации и манипулирования многообразиями, спроецированными на базовую карту. Мы проиллюстрируем Matisse двумя кейсами: простым тестовым примером для демонстрации ключевых концепций и визуализацией публичного Интернета США, чтобы показать практическую полезность Matisse.

Ключевые слова:

сеть, измерения Интернета, кривизна, многообразие, визуализация



Введение

При изучении сетей связи, таких как Интернет, часто встречаются наборы измерений, представляющие сеть как граф с различными атрибутами вершин и рёбер. Важный пример – графы, вершины которых вложены в двумерное евклидово пространство (то есть имеют широту и долготу), а атрибуты рёбер представляют собой измерения задержек (то есть время, которое требуется для передачи пакетов между парами узлов в определённый момент времени).

Интерпретация таких одновременно собранных измерений по рёбрам важна для понимания поведения сложной совокупности линий связи, маршрутизаторов и центров обработки данных, образующих Интернет.

Наша работа основана на гипотезе, что такие наборы данных допускают геометрическое представление в виде сложных метрических пространств в форме гладких многообразий, вложенных в трёхмерное пространство. В случае измерений сетевых задержек в Интернете мы называем такое многообразное представление **пространством интернет-задержек** и показываем, что оно открывает новые возможности как для

1 Печатается в сокращении. Оригинальная статья Matisse: Visualizing Measured Internet Latencies as Manifolds, Stephen Jasina, Loqman Salamatian +4 authors, Walter Willinger, Published in IEEE Transactions on Network and Service Management, 9 September 2025, https://arxiv.org/abs/2509.08097

2 Кривизна Риччи – понятие из дифференциальной геометрии, которое позволяет количественно оценить, насколько локально искривлено риманово (или псевдориманово) многообразие. Она тесно связана с тензором Риччи – объектом, который строится на основе тензора кривизны Римана и метрического тензора (прим. редакции).

разработки нового метода визуализации, так и для характеристики различных аспектов исследования измерений интернет-задержек [1], [2].

Многообразное представление измеренных интернет-задержек информативно благодаря контрасту с плоским евклидовым пространством. Если считать, что геопривязанные интернет-узлы приблизительно лежат на плоской двумерной евклидовой поверхности в физическом пространстве, то многообразие может показать тип и величину деформаций этой плоской поверхности, необходимых для отражения измеренных задержек.

Иными словами, можно построить визуализацию так, чтобы кратчайший путь между любыми двумя узлами на многообразии приблизительно отражал измеренную задержку между этими двумя узлами. Тогда, «проходя по многообразию», измеренные интернет-задержки между разными парами узлов могут быть достоверно восстановлены по геодезической длине между соответствующими парами узлов. Например, малые задержки часто соответствуют путям, которые ассоциируются с «прямой видимостью» или «движением по локальной евклидовой плоскости», тогда как большие задержки обычно связаны с более искривлёнными траекториями. В многообразном представлении такого пространства интернет-задержек эти пути должны проходить через «холмы и впадины», возникающие из-за деформаций евклидовой плоскости и проявляющиеся как искривлённые поверхности.

Цель нашей работы – разработать визуализацию, которая: а) вычисляется по известным местоположениям узлов и измеренным задержкам между узлами; б) представлена как многообразие, явно связанное с географией реального мира; в) позволяет макроскопически интерпретировать свойства сети, точно отражая соотношения задержек между отдельными узлами через расстояния на поверхности; г) обрабатывает одновременные измерения задержек между несколькими парами узлов и таким образом интерпретируемо фиксирует базовую структуру соответствующего пространства задержек.

По пути к этой цели мы сталкиваемся с тем, что интернет-задержки возникают в пространстве, скрытом от нас. Оно скрыто, потому что физическая инфраструктура, по которой отдельные пакеты проходят от одного узла к другому, обычно известна лишь частично. Кроме того, география физического пространства, в котором находятся узлы, влияет на структуру измеренных задержек, а точное соотношение между физическим пространством и пространством, задаваемым задержками, неизвестно.

Тем не менее, хотя задержки передачи пакетов в Интернете не обязательно симметричны и могут даже нарушать неравенство треугольника, можно предпринять шаги для решения этих проблем (например, используя в качестве базовой сущности измерения времени прохождения пакета данных в обе стороны, RTT). Поскольку масштаб таких модификаций невелик по сравнению с величинами используемых нами измерений, а их влияние на визуализации минимально, мы можем рассматривать это скрытое пространство как метрическое.

Наш подход к преодолению сложностей, связанных с оценкой задержек в Интернете, опирается на анализ различий между задержками в скрытом пространстве (то есть измеренными интернет-задержками) и задержками в физическом пространстве (то есть основанными на географическом расстоянии по карте). Мы утверждаем, что понимание этих различий даёт представление о природе сетевых измерений и свойствах сетевой инфраструктуры, лежащей в их основе. Основной инструмент, который мы используем для интерпретации этих различий и извлечения смысла, – **кривизна Оливье-Риччи** (далее – кривизна Риччи).

Наша стратегия состоит в том, чтобы использовать кривизну Риччи для построения визуализации, которая отражает как скрытое пространство задержек, так и положение узлов в известном пространстве географической карты. Мы согласуем эти две цели, используя двумерное многообразие, вложенное в трёхмерное пространство, и подбирая локальную кривизну многообразия так, чтобы она соответствовала кривизне, характерной для каждой области измерений задержек.

Полученное многообразие отражает деформацию евклидова пространства, вызванную скрытым пространством задержек; в идеале геодезические линии на многообразии приблизительно кодируют измеренные интернет-задержки.

Наш главный вклад – это **Matisse**, система визуализации, разработанная в соответствии с перечисленными выше критериями. Matisse опирается на: а) создание графов, полученных как от скрытого пространства задержек, так и от базового пространства карты; б) характеристику полученных графов с помощью кривизны Риччи; в) использование полученных значений кривизны Риччи для определения деформации многообразия.

Чтобы проиллюстрировать функциональность, гибкость и практическую пользу Matisse, мы приводим два примера. В первом примере используется упрощённая сеть, в которой не учитывается конкретное географическое расположение узлов. Этот пример приводится для того, чтобы продемонстрировать основные аспекты создания и визуализации многообразий. Второй кейс основан на измерениях задержек пакетов между множеством хостов с известными координатами в общедоступном Интернете США. Полученное многообразие представляет собой отображение предполагаемого пространства интернет-задержек и выделяет интересные области внутри этого топологического пространства.

Наконец, мы используем многообразия, построенные по измеренным интернет-задержкам, чтобы показать, что наш метод создаёт поверхность, правильно отображающую скрытое метрическое пространство. Мы показываем, что геодезические расстояния между вершинами, рассчитанные на поверхности многообразия, более точно отражают измеренные задержки, чем расстояния по прямой. Кривизна полученного многообразия кодирует измеренную интернет-задержку между любыми двумя узлами в виде кратчайшего пути между ними по поверхности многообразия.

Методология

В этом разделе мы представляем нашу методологию создания многообразий скрытых метрических пространств и описываем систему Matisse, реализующую эту методологию. Хотя наш метод и система визуализации являются универсальными в том смысле, что могут применяться к графам, спроецированным на любую евклидову поверхность. Далее мы сосредоточимся на графах, спроецированных на географические поверхности, поскольку они интуитивно понятны и являются наиболее подходящим применением для нашей методики.

Обзор

Первое ключевое наблюдение состоит в том, что пространство интернет-задержек напоминает пространственную карту, где каждое подключённое устройство выступает в роли точки. Эти точки размещаются на основе их физических местоположений и сетевой задержки между ними (латентности).

Латентность пути в обе стороны показывает, сколько времени требуется данным, чтобы дойти от одной точки до другой и вернуться. На него влияют такие факторы, как перегрузка сети, методы маршрутизации и доступность инфраструктуры. В регионах, где инфраструктура отсутствует или недостаточна, связность становится нестабильной, подобно тому, как физический ландшафт может образовывать впадины или складки из-за эрозии.

Это явление создаёт особый эффект в нашем представлении: оно заставляет пространство интернет-задержек изгибаться или искривляться. Эта кривизна, напоминающая описание формы пространства-времени в общей теории относительности, позволяет интуитивно смоделировать искажение между физическим пространством и пространством задержек.

Кривизной Риччи в каждой точке пространства измеряется, насколько пространство отклоняется от плоского. В непрерывном пространстве для описания кривизны в каждой точке используются тензоры, показывающие форму пространства во всех точках: собирается как впадина, простирается как плоскость или скручивается как седло. Основная идея Matisse – использовать эту аналогию с кривизной и многообразиями для создания эффективного метода просмотра и анализа пространства задержек.

Преодоление разрыва между непрерывными и дискретными параметрами имеет решающее значение, особенно при попытке представить непрерывные геометрические характеристики Интернета с помощью дискретных измерений между контрольными точками. В нашем решении используется новый метод определения дискретной кривизны по этим контрольным точкам [1] (описан в подразделе «Входные и выходные данные»), а также применение сеток для преодоления разрыва между дискретными и непрерывными параметрами. Тонко настраивая уровень детализации сетки, можно точнее представлять непрерывные аспекты кривизны. При работе с двумерными поверхностями в трёхмерном пространстве мы заменяем кривизну Риччи эквивалентной гауссовой кривизной, свойства которой более удобны для вычислительных задач. Этот подход позволяет не только представить структуру Интернета через геометрические характеристики, но и оценивать и анализировать сеть способом, согласующимся с нашим пониманием пространства и кривизны в непрерывном мире. В этом разделе мы описываем, как генерируются наши визуализации, применяя подход «снизу вверх» – от необработанных измерений задержек до конечного результата.

Входные и выходные данные

Matisse принимает на вход список геопривязанных контрольных точек (то есть широт и долгот) и набор измеренных значений времени прохождения данных в обе стороны между ними. Вместе они образуют почти полный взвешенный граф (почти полный из-за возможных отсутствующих измерений).

Дополнительные входные данные для Matisse – это управляющие параметры: ε; λ_»smooth» ; r; инициализация; расстояние кластеризации; число вершин в сетке.

Выбор этих гиперпараметров влияет на свойства результирующего многообразия.

Matisse создаёт взвешенный простой граф G=(V,E) как промежуточный результат. Вершины V представляют точки наблюдения, а рёбра E определяются с помощью пороговой обработки. Вес каждого ребра e E равен его кривизне Риччи к_»Ricci» (e). Т.е. алгоритмами пороговой фильтрации и вычисления кривизны формируется этот промежуточный граф.

На выходе Matisse возвращает треугольную сетку, представляющую многообразие, в котором отражены значения к_»Ricci» и каждая вершина v V имеет соответствующее местоположение π(v).

Реализация

Фронтенд приложения Matisse написан на HTML, CSS и JavaScript. Мы используем графическую библиотеку three.js [3] для построения визуализации на основе треугольной сетки. Мы накладываем карту мира на плоскость как текстуру с помощью OpenLayers [4], чтобы получить данные карты.

Бэкенд полностью написан на Python. Мы активно используем стандартные библиотеки: NetworkX, NumPy, scikit-learn и SciPy, – для общих вычислений. Для вычисления кривизны Риччи мы дополнительно используем библиотеку POT [5].

Код Matisse выложен в открытом доступе на GitHub [6].

Matisse в действии

Мы проиллюстрируем работу Matisse и применимость нашей техники визуализации многообразий на примере двух конкретных исследований. В первом из них используются простые графы, чтобы сосредоточиться на ключевых аспектах генерации и уточнения многообразий. Второй кейс касается представления многообразиями наборов измерений интернет-задержек между узлами в публичном Интернете США.

Аналогичные исследования, направленные на изучение частных магистральных инфраструктур трёх крупных сетей облачных провайдеров, описаны в [1].

Тестовая сеть

Наш первый кейс основан на простом графе, показанном на рисунке 1a. Граф имеет три области «плотной» связности, обозначенные рёбрами с положительной кривизной (синими). Области соединены связями с отрицательной кривизной (красными). Граф загружается в Matisse с координатами узлов на простой евклидовой плоскости.

Matisse генерирует многообразие для графа, показанное на рисунке 1b, где граф проецируется на поверхность.

Рисунок 1c показывает эффект, который наложение кривизны оказывает на геодезические линии. Как подсказывает интуиция, геодезические траектории притягиваются к областям отрицательной кривизны. Эти рёбра отрицательной кривизны являются критически важными для сетевой связности. Иными словами, геодезические пути приблизительно совпадают с кратчайшими путями, найденными в сети.

Такие простые примеры очень полезны, потому что позволяют исследовать влияние изменения гиперпараметров на характеристики результирующего многообразия. Например, эксперименты с размером сетки показывают, что слишком грубая сетка не находит искомые особенности, такие как ярко выраженные седловые точки, но, с другой стороны, увеличение детализации может привести к снижению эффективности модели. Конечно, увеличение степени детализации увеличивает и время вычислений. На практике для выбора наиболее грубого уровня детализации, при котором ещё сохраняются желаемые характеристики, зачастую приходится экспериментировать с различными размерами сетки.

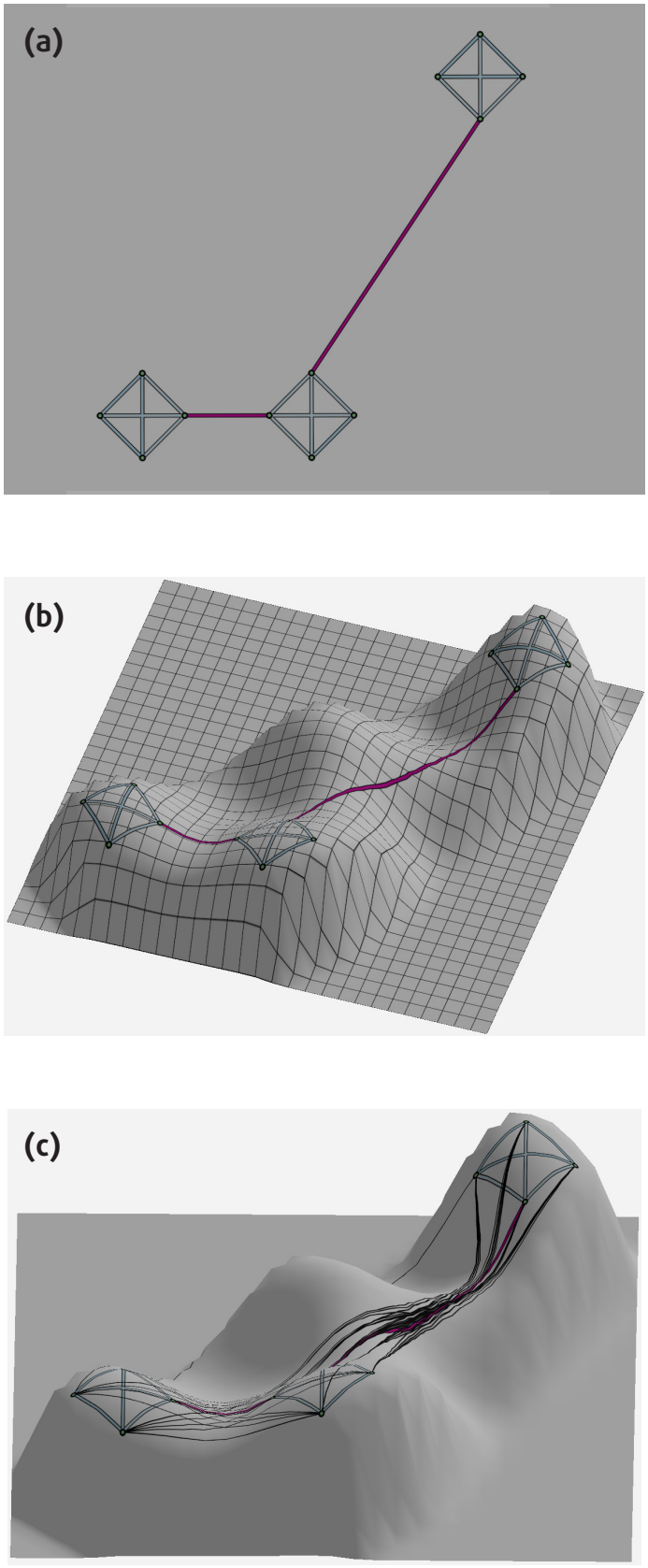


Рис. 1. Тестовая сеть и результирующее многообразие. (a) Сама сеть. Синие связи имеют положительную кривизну; красные связи имеют отрицательную кривизну. (b) Тестовое многообразие. (c) Тестовое многообразие с геодезическими путями, проведёнными чёрным цветом. Обратите внимание на притяжение путей к седловинам.

Измеренное пространство задержек для публичного Интернета США

Структура связности Интернета много лет является предметом интенсивного изучения (например, см. [7], [8] и ссылки в них). Один из способов рассмотрения интернет-связности – построить граф на основе измерений задержки прохожде-

ния пакетов в оба конца между полным набором точек наблюдения, распределённых по всей сети, с использованием стандартного инструмента ping [9]. Эта простая перспектива может дать полезное понимание интернет-связности, которое можно высветить в визуализации многообразия.

Для создания визуализации многообразий пространств интернет-задержек в Matisse мы организуем данные следующим образом. Сначала мы используем инфраструктуру **RIPE Atlas** [10], чтобы собрать измерения RTT в выбранном наборе из 21 точки наблюдения в континентальной части США. Эти точки наблюдения географически распределены по основным крупным городским районам США и физически соединены друг с другом магистральными волоконно-оптическими каналами, которые обычно проложены вдоль основных шоссе и железных дорог [11].

Для Matisse важно, что географические местоположения всех точек наблюдения заранее известны. Это позволяет вычислить большой круг дистанций (GCD) между точками наблюдения. Затем мы вычисляем большой круг задержек (GCL) между двумя точками, деля GCD на 2/3 c, где c – скорость света, а 2/3 c – скорость света в оптическом волокне. Потом мы вычисляем остаточную задержку для каждой пары точек наблюдения. Мы определяем её как минимальную задержку, измеренную за некоторый фиксированный период времени, минус GCL.

Мы генерируем визуализации этого пространства интернет-задержек в Matisse, вводя координаты узлов и значения кривизны Риччи. Мы определяем связность между узлами, выбирая рёбра с остаточными задержками выше указанного порога.

Начиная с небольшого остаточного порога и постепенно увеличивая его, можно создать серию визуализаций многообразий, демонстрирующих различные особенности связности в базовой сети (то есть в Интернете США).

На рисунке 2 показано пространство интернет-задержек в США, сгенерированное Matisse. Базовая карта и граф масштабированы и ориентированы таким образом, чтобы местоположения вершин графа были правильно выровнены по карте. Рисунок 2 показывает многообразие для связности при низком пороге остаточной задержки 10 мс (то есть связи задаются только там, где остаточная задержка близка к GCL). На этом изображении показаны области эффективной связности вдоль Восточного побережья и выделены седловые области с отрицательной кривизной Риччи, которые соответствуют магистралям, пересекающим Средний Запад и Юг. В этих регионах преобладают внутрирегиональные оптоволоконные линии, где соседние узлы обычно непосредственно соединены друг с другом.

Matisse выявляет двойственную природу связности: области, характеризуемые рёбрами с положительной кривизной Риччи, демонстрируют плотно взаимосвязанную инфраструктуру, тогда как отрицательно искривлённые рёбра выделяют географические проблемы и инфраструктурные ограничения. Эти результаты подчёркивают значительное влияние географии на производительность Интернета США.

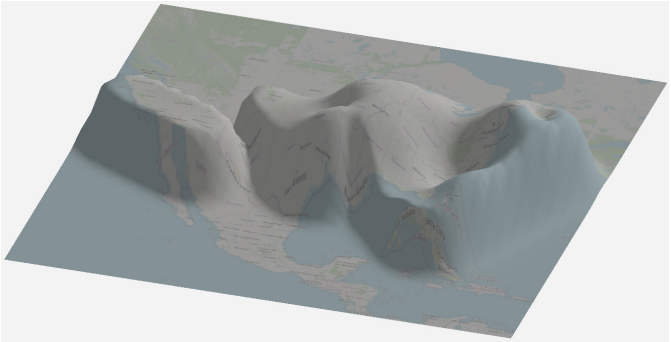


Рис. 2. Визуализация на основе Matisse экземпляра пространства интернет-задержек, публичный Интернет США. Более высокие области на северо-востоке указывают на более плотное соединение с малыми задержками (например, геодезические линии находятся в зоне прямой видимости), а долина, разделяющая страну на две части, указывает на область с редким, но критически важным соединением между восточной и западной частями США, что приводит к увеличенным задержкам (например, геодезические линии находятся далеко от зоны прямой видимости).

Итоги и будущая работа

Визуализации многообразий, полученных на основе данных реальных измерений, могут улучшить наше понимание базовых характеристик этих измерений и выявить важные свойства, такие как аномалии или другие необычные аспекты системы, в которой проводились измерения.

В этой статье мы описали методологию создания многообразных представлений плоских графов, которые включают координаты вершин и значения кривизны Риччи на рёбрах. Наша методология генерирует многообразие с гладкой поверхностью, наследующей характеристики кривизны базового графа и сохраняющей местоположения вершин. Важно, что многообразие позволяет восстанавливать исходные измерения и вычислять расстояния, которые не были включены в исходные данные.

Мы реализовали нашу методологию в системе, которую назвали Matisse. Она генерирует визуализации многообразий и может применяться итеративно для оценки систем в различных топологических конфигурациях. Для демонстрации нашего метода и Matisse мы представили примеры. Они включают тестовую сеть, используемую для иллюстрации основных аспектов функциональности Matisse. Чтобы показать полезность и гибкость инструмента, мы также применили Matisse к графам, полученным на основании измеренных задержек в публичном Интернете США.

В будущей работе мы планируем использовать Matisse для изучения других типов интернет-измерений через их многообразные представления. Мы также намерены исследовать использование Matisse для улучшения понимания других географически распределённых киберфизических критических инфраструктур, таких как транспортные и энергетические сети.

Список литературы:

[1] L. Salamatian, S. Anderson, J. Matthews, P. Barford, W. Willinger, and M. Crovella, «Curvature-based Analysis of Network Connectivity in Private Backbone Infrastructures», in Proc. ACM Meas. Anal. Comput. Syst., 2022.

[2] L. Salamatian, S. Anderson, J. Mathews, P. Barford, W. Willinger, and M. Crovella, «A manifold view of connectivity in the private backbone networks of hyperscalers», Commun. ACM, vol. 66, no. 8, p. 95–103, jul 2023, https://doi.org/10.1145/3604620

[3] Ricardo Cabello (Mr.doob), «three.js», first released in 2010, continuously updated, accessed: 2023-11, https://github.com/mrdoob/three.js/

[4] «Openlayers api», 2021, https://openlayers.org/

[5] R. Flamary, N. Courty, A. Gramfort, M. Z. Alaya, A. Boisbunon, S. Chambon, L. Chapel, A. Corenflos, K. Fatras, N. Fournier, L. Gautheron, N. T. Gayraud, H. Janati, A. Rakotomamonjy, I. Redko, A. Rolet, A. Schutz, V. Seguy, D. J. Sutherland, R. Tavenard, A. Tong, and T. Vayer, «Pot: Python optimal transport», Journal of Machine Learning Research, vol. 22, no. 78, pp. 1–8, 2021, http://jmlr.org/papers/v22/20-451.html

[6] S. Jasina, J. Mathews, and L. Salamatian, August 2025, https://github.com/StephenJasina/linear-geodesic-optimization

[7] W. Willinger and M. Roughan, «Internet topology research redux», Recent Advances in Networking, 2013.

[8] B. Huffaker, D. Plummer, D. Moore, and K. Claffy, «Topology discovery by active probing»,"Proceedings 2002 Symposium on Applications and the Internet (SAINT) Workshops, 2002.

[9] «ping (networking utility)», 2021, https://en.wikipedia.org/wiki/Ping (networking utility)

[10] RIPE Atlas, 2021, https://atlas.ripe.net

[11] R. Durairajan, S. Ghosh, X. Tang, P. Barford, and B. Eriksson, «Internet Atlas: A Geographic Database of the Internet», in Proceedings of the 5th ACM Workshop on HotPlanet. New York, NY, USA: Association for Computing Machinery, 2013.

Приложение. Дополнительные примеры применения в реальном мире

Дополнительные виды измеренного пространства задержек для публичного Интернета США

На рисунке 3 представлена справочная карта опорных точек RIPE Atlas в США.

Одно из важных преимуществ Matisse как инструмента – его интерактивные возможности. Перемещая и вращая камеру, пользователь может избежать проблем, вызванных окклюзией. Из-за ограничений формата документа мы не можем полностью продемонстрировать возможности Matisse здесь. Однако мы предоставляем несколько возможных альтернативных видов на примерах из США – рисунки 2-4.

Рисунки 4b и 4c показывают многообразия для связности при более высоком остаточном пороге (то есть с учётом каналов с остаточными задержками, значительно превышающими GCL). Эти рисунки дают более детальное представление об Интернете США, чем рисунки 1 и 4a, и позволяют увидеть региональные различия внутри единой национальной сети связи. В частности, мы идентифицируем чёткие сёдла в географических областях, таких как Скалистые горы и части юга США (например, дельта Миссисипи), где рельеф местности препятствует развёртыванию обширной физической инфраструктуры и ограничивает маршруты ВОЛС небольшим числом каналов, обычно пролегающих вдоль немногих существующих автомагистралей между штатами или железнодорожных путей.

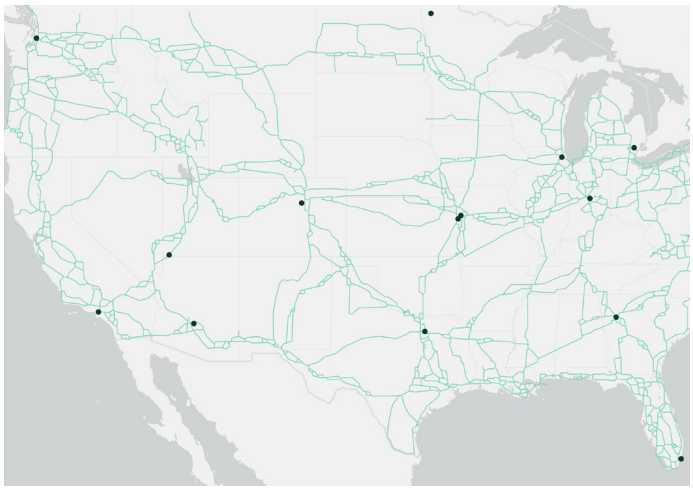


Рис. 3. Географическая карта якорей RIPE Atlas и магистральной волоконно-оптической сети в США.

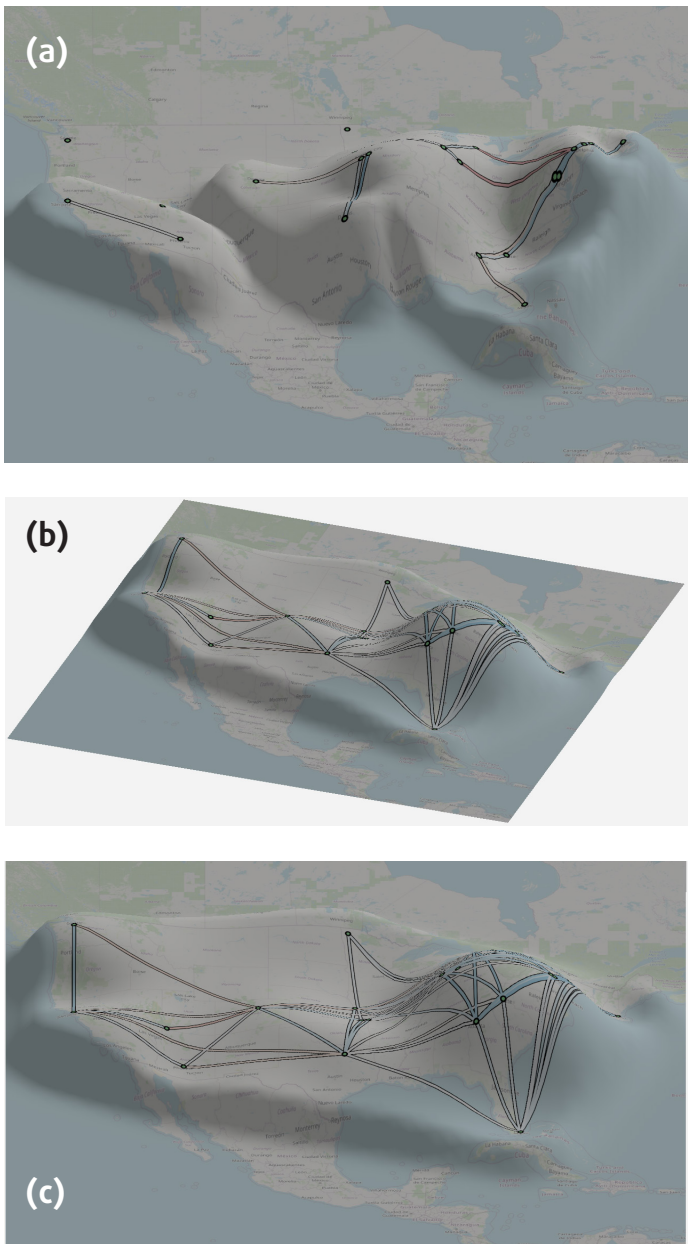


Рис. 4. Многообразные представления публичного Интернета США при разных порогах остаточной задержки. (a) Пространство интернет-задержек США при низком пороге остаточной задержки. (b) Пространство интернет-задержек США при высоком пороге остаточной задержки. (c) Альтернативный вид пространства интернет-задержек США при высоком пороге остаточной задержки.

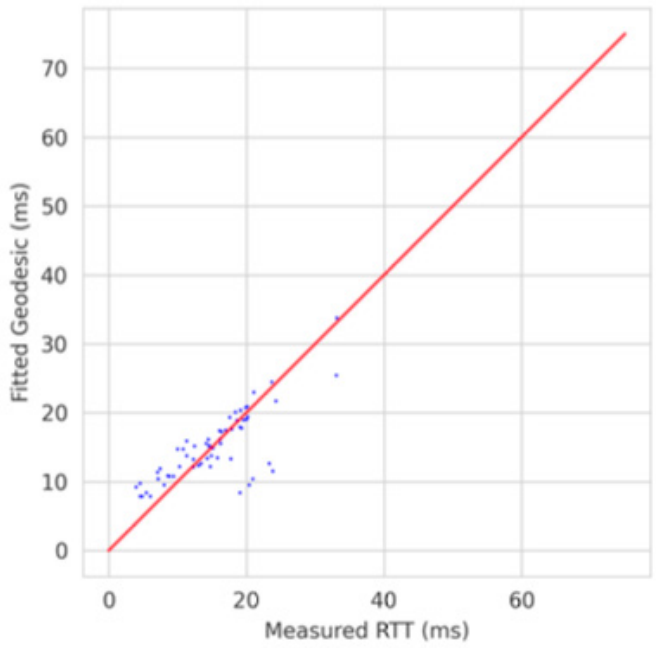


Рис. 5. Сопоставление вычисленных геодезических с измеренными задержками для данных США с порогом задержки 10 миллисекунд.

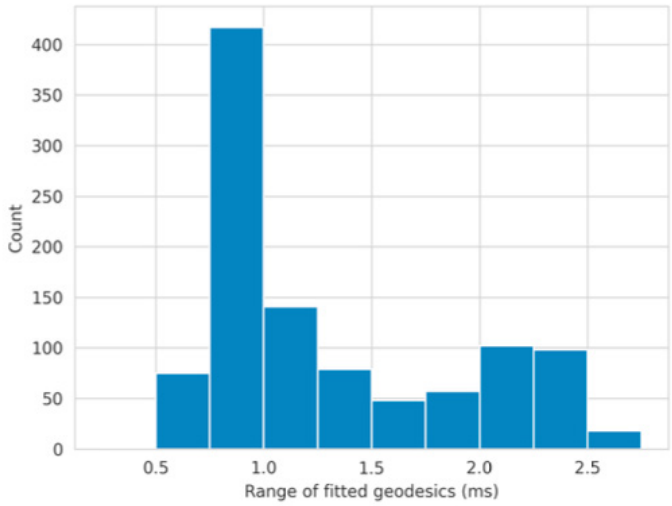


Рис. 6. Диапазоны вычисленных геодезических задержек в миллисекундах для фиксированных пар городов за две недели. Данные из набора США с порогом задержки 22 миллисекунды.

Графическое сравнение RTT и геодезических расстояний

Рисунок 5 показывает, что геодезические расстояния, полученные из нашего многообразия, в целом отражают измеренные RTT. Рисунок 6 отображает стабильность геодезических расстояний на промежутке нескольких недель.

Измеренное пространство задержек для публичного Интернета Европы

В другом примере мы рассматриваем публичный европейский Интернет. Как и в нашем исследовании публичного Интернета США, мы используем данные RIPE Atlas для построения графа связности и генерации многообразий с помощью Matisse.

На рисунке 7 показаны многообразия с уменьшенным и увеличенным масштабом для среднего порога остаточной задержки (5 мс) с использованием кластеризованной входной сети. При таком пороге мы видим небольшие островки связности в пределах крупных городских агломераций, а также

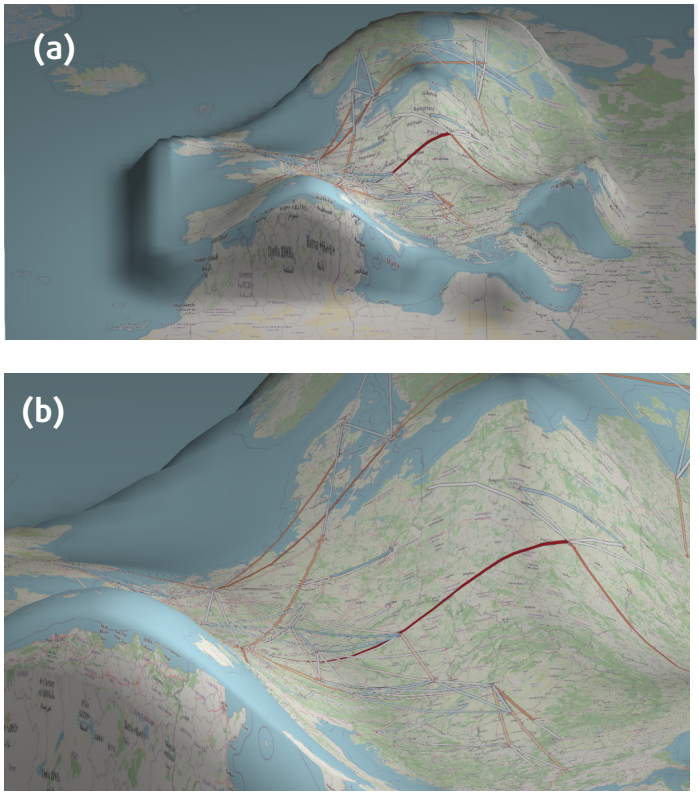


Рис. 7. Многообразные представления европейского публичного Интернета при среднем пороге остаточной задержки (5 мс) с использованием кластеризованной входной сети. (a) Пространство интернет-задержек Европы. (b) Увеличенный участок пространства интернет-задержек Европы.

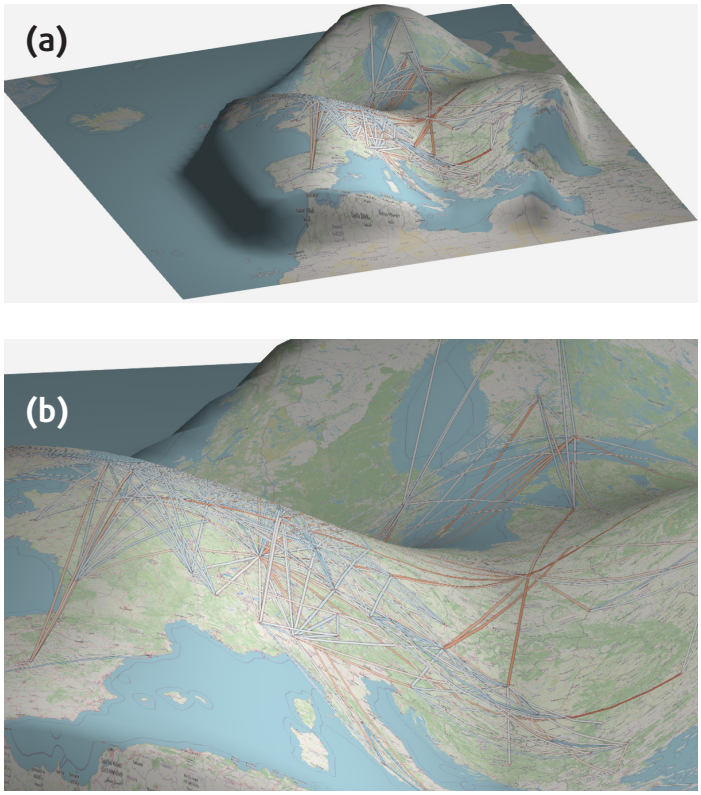


Рис. 8. Многообразные представления европейского публичного Интернета при высоком пороге остаточной задержки (8 мс) с использованием кластеризованной входной сети. (a) Пространство интернет-задержек Европы. (b) Увеличенный участок пространства интернет-задержек Европы.

рёбра с отрицательной кривизной, которые служат мостами связности между этими агломерациями. Эти рёбра интуитивно представляют физические каналы, связывающие разные сетевые кластеры, и представляют «важные» связи в сети.

Рисунок 8 показывает уменьшенный и увеличенный виды публичного Интернета Европы, сгенерированные при относительно высоком пороге остаточной задержки (8 мс) с использованием кластеризованной входной сети. Благодаря выбранному порогу результирующий граф является относительно плотным с точки зрения связности.

Визуализация многообразия показывает, насколько плотно связаны регионы, соответствующие Западной Европе и Скандинавии, что проявляется большими холмами, отражающими положительную кривизну Риччи на графе. Визуализация также подчёркивает относительно недостаточную связность в Восточной Европе, о чём свидетельствует седловидная форма в этом регионе.

Разнообразные визуализации на рисунках 7 и 8 подчёркивают разные аспекты связности в Европе. Matisse был специально разработан для облегчения изучения и анализа этого при различных уровнях детализации, как объясняется в [1].

Об авторах:

Стивен Ясина, Университет Висконсин-Мэдисон, США -
Stephen Jasina, University of Wisconsin-Madison

Локман Саламатиан, Колумбийский университет, США -
Loqman Salamatian, Columbia University

Джошуа Мэтьюз Университет Карнеги-Меллон, США -
Joshua Mathews, Carnegie Mellon University

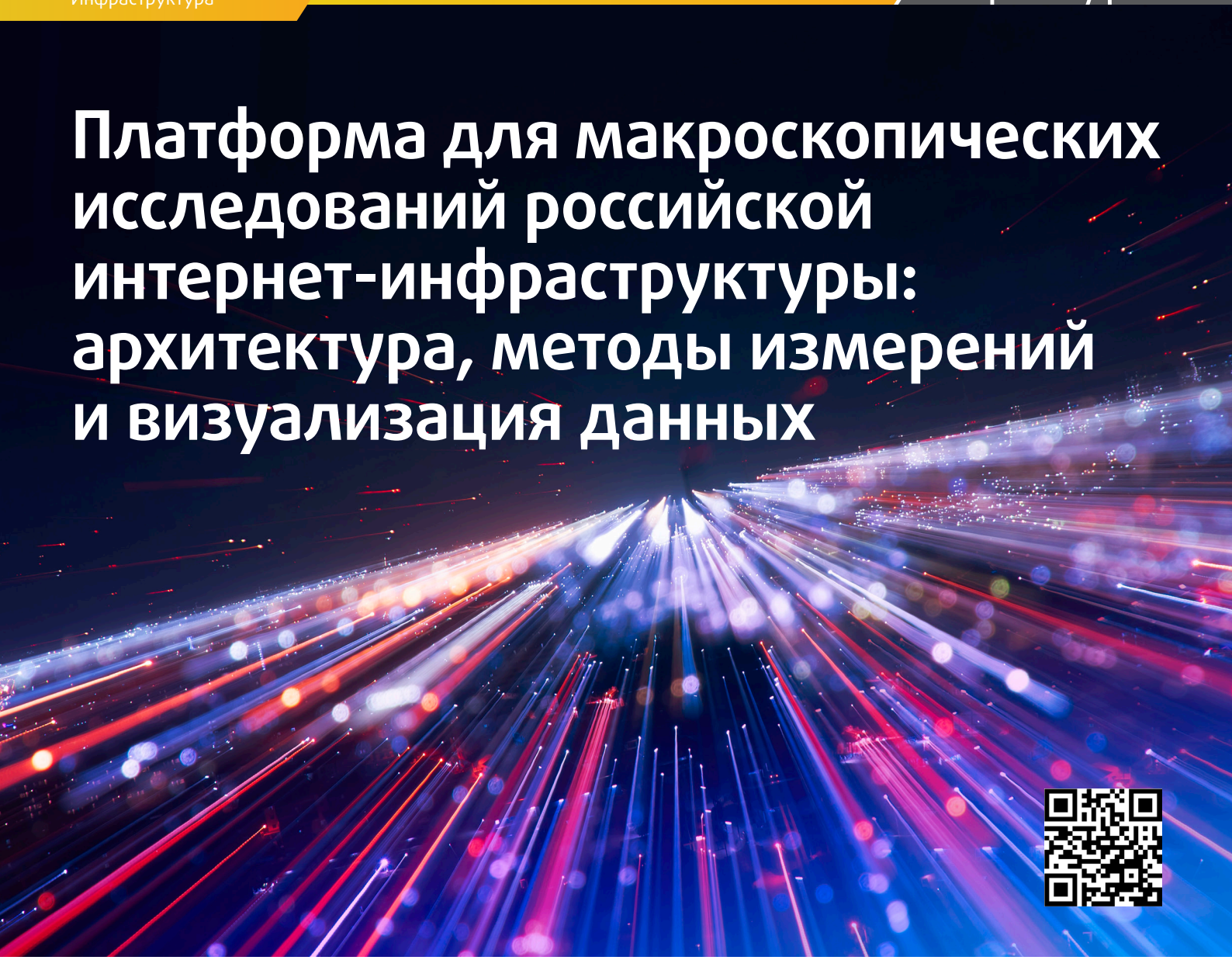
Скотт Андерсон Университет Висконсин-Мэдисон, США -
Scott Anderson, University of Wisconsin-Madison

Пол Барфорд, Университет Висконсин-Мэдисон, США -
Paul Barford, University of Wisconsin-Madison

Марк Кровелла, Бостонский университет, США -
Mark Crovella, Boston University

Уолтер Уиллинджер, NIKSUN Inc. , США -
Walter Willinger, NIKSUN Inc.

Платформа для макроскопических исследований российской интернет-инфраструктуры: архитектура, методы измерений и визуализация данных



Николай Гавриченко

Аннотация

В статье представлена исследовательская платформа Фонда развития сетевых технологий «ИнДата», предназначенная для макроскопического исследования связности и качества взаимодействия в российском сегменте сети Интернет. Платформа объединяет распределённые пробники активных измерений, сбор и анализ BGP-данных, экспертную геолокацию IP-ресурсов, мониторинг веб-сервисов и интерактивную визуализацию. Показана измерительная модель, в которой HTTP, ping, traceroute, DNS-разрешение и данные маршрутизации рассматриваются как взаимодополняющие плоскости наблюдения. Анализ эксплуатационной выгрузки 17–21 сентября 2026 года включает восемь публично доступных консолей управления облачных провайдеров и государственных платформ, наблюдавшихся одновременно из 60 пробников в 12 городах РФ. Показано, что при высокой доле успешных HTTP-ответов (96,2% для кодов 200/301/302) ICMP-доступность большинства целевых узлов ограничена политиками фильтрации на стороне сервисов – вплоть до 100% таймаутов у отдельных узлов при сохранении успешного HTTPS-отклика; это делает непригодным бинарный мониторинг доступности на базе ICMP для admin-консолей. Установлено, что все восемь целевых сервисов используют статический круговой алгоритм DNS без GeoDNS: один и тот же набор IP-адресов наблюдался всеми 60 пробниками в течение всего периода. Зафиксированы устойчивые пространственные и операторские различия в задержке отклика. Обсуждаются ограничения активного зондирования, интерпретации HTTP RTT и DNS-метрик, а также требования к воспроизводимости. Сделан вывод о том, что наибольшая исследовательская ценность платформы связана с возможностью объединения прикладных, сетевых и маршрутизационных наблюдений в едином аналитическом контуре.

Ключевые слова:

активные измерения, интернет-инфраструктура, BGP, AS, HTTP, RTT, traceroute, DNS, IP-геолокация, распределённые пробники, мониторинг связности

1. Введение

Интернет представляет собой распределённую систему, в которой состояние сети определяется взаимодействием автономных систем, сетевых операторов, точек обмена трафиком, магистральных линий и политик междоменной маршрутизации [1]. В отличие от традиционной телекоммуникационной инфраструктуры, единая точка наблюдения для Интернета отсутствует: один и тот же ресурс может иметь существенно различное сетевое и прикладное поведение в зависимости от расположения источника измерения, оператора доступа, выбранного маршрута и текущего состояния промежуточных узлов.

Особенно сложной является задача макроскопического исследования национального сегмента. Глобальные платформы активных измерений дают широкое покрытие, однако для анализа внутрироссийской структуры важно иметь точки наблюдения непосредственно внутри рассматриваемой сети и одновременно учитывать внутреннюю маршрутизацию, региональную неоднородность и особенности локальной инфраструктуры. В этом контексте особую ценность приобретает сочетание распределённых пробников с данными BGP, поскольку активное измерение показывает фактический результат прохождения конкретного трафика, а BGP — логическую структуру маршрутизации и достижимости префиксов [2].

Важным методологическим следствием этого является отказ от бинарного представления доступности. HTTP-код успешного ответа не означает малого времени отклика, а отсутствие ответа на ICMP-запрос не является достаточным доказательством недоступности прикладного сервиса. Аналогично, изменение BGP-маршрута само по себе не означает деградации пользовательского доступа: оно описывает состояние контрольной плоскости и должно сопоставляться с результатами активных измерений.

Платформа Фонда «ИнДата» создаётся для формирования распределённой исследовательской инфраструктуры, позволяющей изучать связность, доступность и качество взаимодействия с сетевыми ресурсами из различных регионов и сетей доступа российского сегмента Интернета. Её развитие предполагает объединение активных измерений, данных маршрутизации и геолокационной информации в единой среде анализа. В рамках этой задачи настоящее исследование направлено на проверку возможностей платформы на эксплуатационных данных, выявление пространственных и операторских различий, а также оценку информативности различных типов измерений.

2. Платформа как измерительная среда

Платформа спроектирована как модульная измерительная среда. В ней функционально разделены запуск активных измерений, хранение временных рядов и геоданных, визуализация и экспертная работа с геолокацией. Такое разделение позволяет расширять набор измерений и число точек наблюдения без перестройки основной логики системы.

Контур активных измерений поддерживает несколько типов задач.

Ping используется для оценки базовой сетевой задержки и потерь пакетов. Получаемый показатель круговой задержки RTT является совокупной характеристикой пути в прямом и обратном направлениях и не позволяет разделить вклад этих направлений. Поэтому ping рассматривается как базовый сетевой уровень сравнения, а не как полная характеристика качества сервиса.

Traceroute используется для выявления промежуточных узлов и анализа изменений маршрута во времени. Длина маршрута оценивается по числу хопов (hop) — переходов между сетевыми узлами на пути от источника до целевого узла. Этот показатель характеризует количество переходов, а не физическую протяжённость маршрута.

Kdig используется для DNS-запросов с возможностью разрешения через системный резолвер пробника.

HTTP GET используется как стандартизированная прикладная проверка. Измеряемый HTTP RTT включает сетевую задержку, TLS и время обработки запроса конечной точкой, поэтому не является чистой сетевой метрикой.

Хранилище реализовано на PostgreSQL, программный стек включает Python и JavaScript

3. Экспериментальные данные

Экспериментальная выборка охватывает 12 городов: Москву, Санкт-Петербург, Ростов-на-Дону, Ставрополь, Самару, Уфу, Екатеринбург, Пермь, Новосибирск, Красноярск, Иркутск и Хабаровск. Пробники размещены на сетях восьми российских операторов.

Каждый пробник представляет собой точку входа в сеть конкретного оператора доступа; в одной географической точке могут одновременно присутствовать пробники нескольких операторов, что позволяет разделять пространственный и операторский факторы при интерпретации результатов.

Измерения проводились в течение 96 часов (17–21 сентября 2026 года) с соблюдением единого расписания по всем пробникам и целевым ресурсам. Общее количество наблюдений составило 1 592 756 записей.

Таблица 1. Состав измерительных задач

Тип задачи	Наблюдений	Пар (probe × target)	Периодичность
ping (L3 ICMP)	564 734	1495	15 мин
HTTP (L7 HTTPS GET)	380 647	476	15 мин
kdig (DNS A / AAAA)	365 009	960	15 мин
traceroute	282 366	1494	30 мин
Итого	1 592 756		

Ping-задачи выполнялись по списку из 25 уникальных IP-адресов, сформированных на этапе первичного DNS-разрешения доменных имён. HTTP-задачи выполнялись в варианте «конкретный IP-адрес + URL», что позволяет однозначно сопоставить прикладной отклик и целевой сетевой адрес и разделить эффекты балансировки DNS и прикладной инфраструктуры. Задачи kdig выполнялись с параметром, при котором разрешение доменного имени производится системным резолвером пробника.

Для основной статистики исключались технические исходы и наблюдения без числового RTT. Значения RTT > 3000 мс рассматривались отдельно как подозрительный хвост распределения.

Для пространственного сравнения используются медианы по городу и оператору. Статусы HTTP не сводятся к бинарной переменной. Код 200 означает успешный ответ сервера, 301 и 302 – корректное перенаправление, а специальные значения -1, timeout, connection_error и error фиксируют иные исходы. Эти состояния не включаются в числовые показатели RTT.

В эксперименте исследовались восемь публично доступных адресов, объединяющих консоли управления крупных облачных провайдеров РФ и государственные платформы электронного голосования:

1. auth.mws.ru – MWS (MTC Web Services);
2. www.cloud.rt.ru – «Ростелеком Облако»;
3. console.yandex.cloud – Yandex Cloud;
4. my.selectel.ru – Selectel;
5. cloud.ru – Cloud.ru;
6. mcs.mail.ru – VK Cloud;
7. vybory.gov.ru – Дистанционное электронное голосование;
8. elec.mos.ru – Система электронного голосования Москвы.

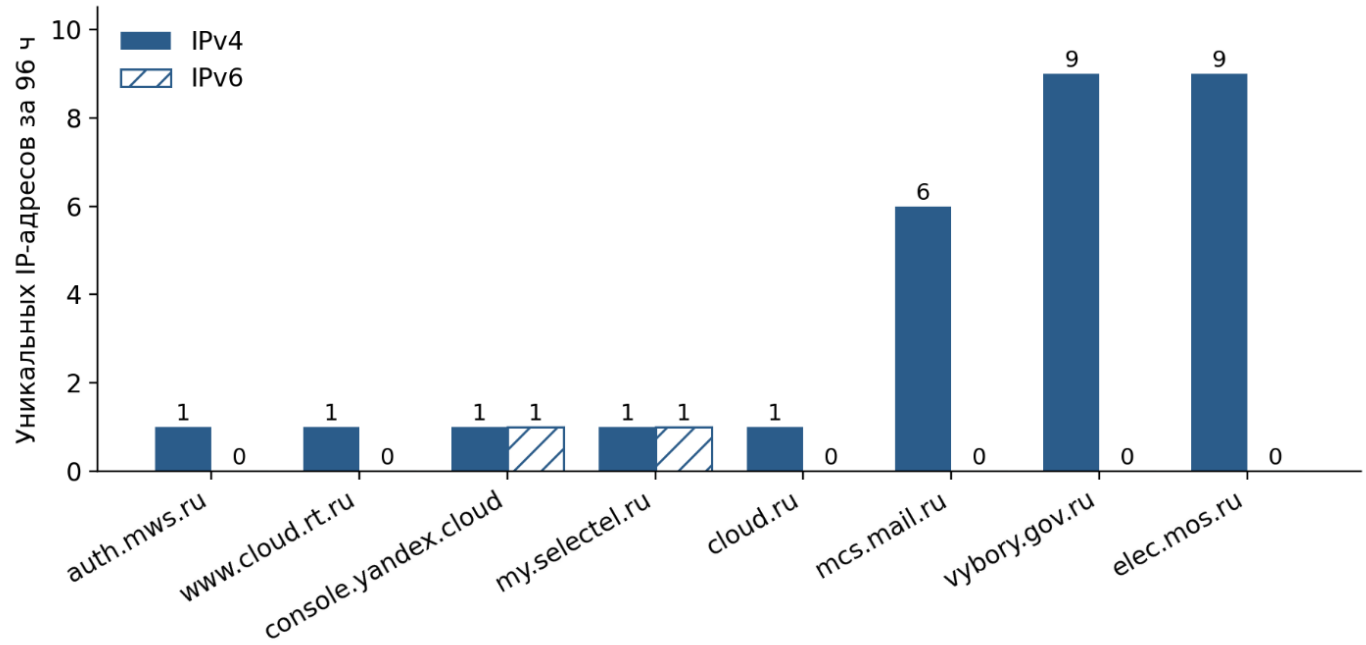
Полученные значения характеризуют время ответа выбранных URL и доступность соответствующих сетевых узлов из конкретных сетей доступа и не являются прямой оценкой всей инфраструктуры соответствующих компаний или операторов. Замеры выполнены в B2B-сегменте; B2C-трафик и прямой M2M-трафик к API-узлам в эксперимент не входили.

4. Результаты эксперимента

4.1. Архитектура DNS и распределение целевых IP

За 96 часов наблюдения ни у одного из восьми сервисов не зафиксировано изменения состава IP-адресов во времени.

Рис. 1. Уникальные IP-адреса целевых доменов за 96 часов.



Каждый уникальный IP был замечен всеми 60 пробниками, независимо от города и оператора доступа.

Отсутствие пространственной вариативности DNS указывает на использование статического кругового алгоритма из единого пула адресов, а не GeoDNS распределения (технология распределения сетевого трафика на основе географического местоположения пользователей). Этот результат важен для корректной атрибуции причин: даже у сервисов, инфраструктура которых географически распределена, балансировка на уровне DNS по региону не производится; прикладная маршрутизация, по-видимому, реализуется другими механизмами.

Поддержка IPv6 зафиксирована только у двух сервисов из восьми — console.yandex.cloud и my.selectel.ru. У остальных шести доменов AAAA-записи не обнаружены.

ASN-атрибуция IP-адресов выполнена по данным ididb.ru (таблица 2).

Таблица 2. ASN и BGP-префиксы целевых IP

Сервис	Префикс	ASN	Holder
MWS	188.93.55.0/24	AS44677	MTS-NGCLOUD MTS PJSC
«Ростелеком»	213.59.197.0/24; 188.254.0.0/17; 82.196.128.0/19	AS12389	Rostelecom PJSC
Yandex Cloud	185.206.164.0/22; 2a0d:d6c1::/32	AS200350	YandexCloud LLC
Selectel (v4)	85.119.149.0/24	AS50340	SELECTEL-MSK JSC
Selectel (v6)	2a00:ab00::/32	AS49505	SELECTEL JSC
Cloud.ru	185.71.64.0/24	AS43298	StormNetworks LLC
VK Cloud	95.163.248.0/21	AS47764	VK-AS LLC
elec.mos.ru	212.11.153.0/24; 212.11.157.0/24; 212.11.158.0/24	AS8901	GKU Mosgortelecom
ДЭГ (vybory.gov.ru)	188.254.0.0/17; 82.196.128.0/19	AS12389	Rostelecom PJSC

4.2. Пространственная неоднородность и операторские различия

Наиболее содержательными с точки зрения пространственного покрытия являются результаты серии HTTP-измерений для сервиса mcs.mail.ru. Медианные значения RTT по городам (мс) приведены на рисунке 2.

Разница между московскими и дальневосточными измерениями достигает двух раз. Пространственный градиент устойчиво воспроизводится и на L3-измерениях: для ICMP-доступных узлов (185.206.167.35 Yandex Cloud, 213.59.197.32 «Ростелеком», 185.71.64.201 Cloud.ru, 85.119.149.4 Selectel) медианный RTT растёт от 2–7 мс в Москве до 97–105 мс в Хабаровске, что пропорционально физическому расстоянию и соответствует ожидаемому поведению магистральных сетей.

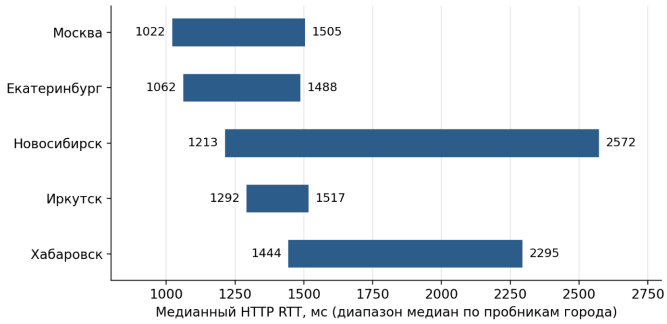


Рис. 2. Медианный HTTP RTT по городам для mcs.mail.ru, мс.

Особое наблюдение связано с elec.mos.ru. Из 378 HTTP-запросов доля исходов timeout варьируется от 64 до 239. Это единственный сервис в выборке, где доля таймаутов стабильно превышает 15% и в отдельных пробниках достигает 63%. Для остальных семи сервисов доля timeout и connection_error в сумме не превышает 5%. Причины столь высокой доли таймаутов могут быть связаны как с защитой от автоматизированных запросов на уровне сервиса, так и со спецификой обработки на промежуточных прокси; окончательная интерпретация требует дополнительного анализа TLS.

Операторские различия проявляются внутри одной географической точки. Для mcs.mail.ru медианы HTTP RTT между операторами различаются на десятки процентов. Однако эти различия нельзя трактовать как прямое доказательство преимущества одного оператора: HTTP RTT зависит также от маршрутизации и конечной инфраструктуры сервиса

4.3. ICMP-фильтрация и интерпретация L3-метрик

Наиболее важное методологическое наблюдение эксперимента связано с L3 ICMP. Из 564 734 ping-измерений 249 377 (44%) завершились таймаутом. Это не потеря пакетов в сети: сопоставление с L7-измерениями показывает, что те же узлы успешно отвечали на HTTPS-запросы в тот же период. Наблюдаемый эффект вызван политикой фильтрации ICMP на стороне целевых сервисов.

Различия носят системный характер и отражают политику защиты инфраструктуры, а не состояние сети. Практический вывод: измерение доступности admin-консолей не может строиться на ICMP. Все выводы о доступности должны опираться на L7-метрики; ICMP имеет смысл использовать только как индикатор состояния пути для тех узлов, где он не фильтруется.

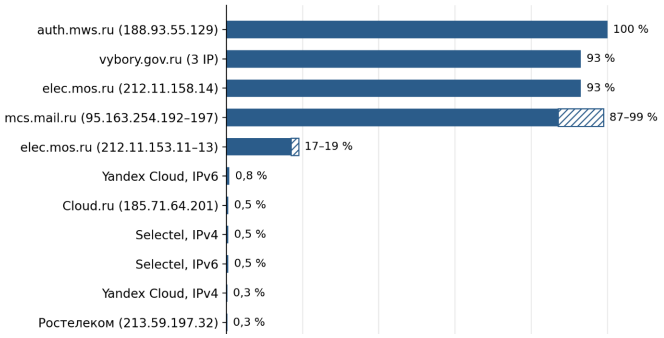


Рис. 3. Доля ICMP-таймаутов для целевых узлов.

4.4. DNS-резолвинг через пробники и операторские особенности

Всего за период наблюдения платформа зафиксировала 17 уникальных DNS-резолверов, использовавшихся 60 пробниками. Из них три являются публичными (1.1.1.1, 8.8.4.4 и 9.9.9.9), остальные используются в сетях восьми операторов связи, в которых размещены пробники Фонда «ИнДата».

Особый интерес представляет распределение DNS-ошибок – запросов, на которые резолвер не вернул ответ за отведённое время. Все 12 пробников одного из операторов показывают аномально высокий процент таких ошибок.

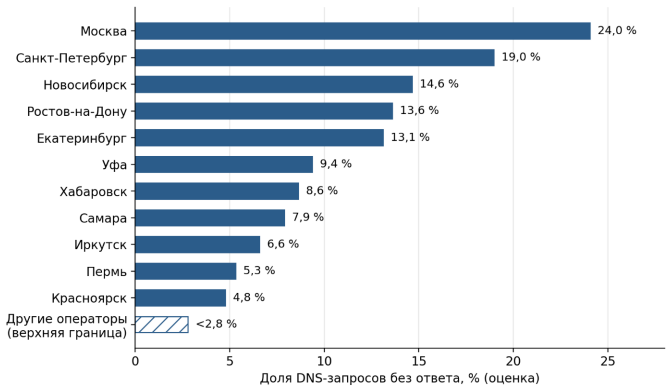


Рис. 4. DNS-ошибки по пробникам (запросы без ответа).

На пробниках других операторов зафиксированы единицы–десятки ошибок. Это устойчивая операторская особенность, которая заслуживает отдельного анализа инфраструктуры DNS сети и не может быть объяснена только нагрузкой или географией.

4.5. Traceroute и топология целевых сервисов

Распределение длины маршрутов по всей выгрузке характеризуется следующими перцентилями: p50 = 10 хопов, p90 = 14,06 хопа, p95 = 15,72 хопа. Перцентиль p50 соответствует медиане: 50% наблюдений имеют значение не выше этого уровня. Перцентили p90 и p95 показывают уровни, ниже или на которых находятся соответственно 90% и 95% наблюдений.

Между сервисами наблюдаются качественные различия. Для Yandex Cloud (185.206.167.35) длина маршрута из Хабаровска составляет 6 хопов, тогда как до MWS (188.93.55.129) — 15 хопов, а до VK Cloud (95.163.254.192) — 13 хопов. Это соответствует гипотезе о наличии у Yandex Cloud локальных edge-узлов или anycast-анонсов в Дальневосточном регионе, что снижает как сетевую задержку, так и чувствительность к состоянию транзитных маршрутов.

Для elec.mos.ru наблюдается обратная картина: короткие маршруты из Хабаровска (в среднем 7,6 хопа по отдельным IP) при относительно высоком HTTP RTT (715–1212 мс). Это указывает на то, что сетевой путь заканчивается на узле-терминаторе в регионе, но прикладная обработка (TLS-сессия, серверная логика, редиректы) происходит на стороне московской инфраструктуры. Данное наблюдение требует дополнительного анализа на уровне TLS-handshake и HTTP-timing, чтобы разделить вклад сетевого и прикладного компонентов.

4.6. BGP и геолокация

BGP-контур платформы расширяет объект наблюдения за пределы результатов активного зондирования. Ping, traceroute и HTTP показывают результат конкретного измерения из конкретного источника, тогда как BGP описывает состояние контрольной плоскости: видимость префиксов, последовательность автономных систем и изменения анонсов [2]. В настоящем эксперименте BGP и промежуточные хопы traceroute не использованы для количественной проверки причин пространственных и операторских различий: промежуточные IP-адреса не обогащались номерами AS, поэтому выводы о конкретных транзитных автономных системах в рамках данного эксперимента не делаются.

ASN-атрибуция выполнена только для целевых IP-адресов и достаточна для привязки сервисов к автономным системам, но не для анализа маршрутизации между источником и целью.

5. Обсуждение, ограничения и направления дальнейших исследований

Полученные результаты позволяют сделать несколько общих выводов.

ICMP-фильтрация на стороне admin-консолей является системным явлением. Из 564 734 ping-измерений 44% завершились таймаутом, причём у отдельных узлов доля таймаутов достигает 100% (auth.mws.ru). При этом те же узлы в тот же период успешно отвечали на HTTPS-запросы. Это означает, что для сервисов класса «консоль управления» ICMP непригоден как канал измерения доступности, а системы мониторинга, построенные на ping, будут систематически давать ложно-негативный результат. Все выводы о доступности должны опираться на L7-метрики; ICMP сохраняет цен-

ность только как индикатор состояния пути для узлов, где он не фильтруется.

ASN-структура российских облачных сервисов неоднородна. Yandex Cloud, Cloud.ru, MWS используют отдельные автономные системы, не совпадающие с ASN головных структур. Это важно для BGP-мониторинга: привязка сервиса к «головному» ASN будет некорректной.

IPv6-поддержка целевых сервисов слабая. Только два из восьми доменов имеют AAAA-записи, что ограничивает переход на IPv6-only и сужает наблюдаемое пространство IPv6-связности в российском сегменте.

Активные измерения требуют осторожности. ICMP может обрабатываться с иным приоритетом, HTTP RTT зависит от сервера и прикладного стека, traceroute может содержать артефакты (скрытые или незаполненные хопы из-за ограничения скорости и фильтрации ICMP TTL-exceeded на маршрутизаторах; смешение путей при балансировке нагрузки ECMP; невидимые MPLS-туннели; адреса интерфейсов, не совпадающие с реальным путём прямого и обратного трафика), а DNS-разрешение на пробнике отражает состояние конкретной сети доступа, а не абстрактной «глобальной DNS». Именно объединение нескольких наблюдательных плоскостей является сильной стороной платформы Фонда «ИнДата».

Сравнительно с универсальными платформами измерений, описанный подход ориентирован на более плотную работу с российской географией и локальными источниками BGP. Его отличие состоит не только в количестве пробников, но и в объединении измерительной, маршрутизационной и геолокационной плоскостей в одном исследовательском контуре. При этом прямое количественное сравнение с другими системами требует отдельного эксперимента, поскольку охват, состав пробников и политика доступа к результатам различаются.

Исследование ограничено 96-часовым периодом, 12 городами и отсутствием ASN-атрибуции промежуточных хопов traceroute. TLS-параметры также не фиксировались, что ограничивает интерпретацию прикладной составляющей HTTP RTT. Поэтому полученные результаты не могут быть распространены на всю инфраструктуру России.

6. Заключение

Проведённый эксперимент показал, что распределённая платформа активных измерений Фонда «ИнДата» может использоваться для исследования пространственной и прикладной неоднородности доступа к сетевым ресурсам. Существенным результатом является возможность совместного анализа нескольких измерительных уровней, а не отдельных показателей RTT.

Одним из основных направлений дальнейшего развития является расширение сети измерительных точек. Увеличение числа стационарных пробников повысит пространственное разрешение и снизит зависимость результатов от отдельных точек наблюдения, особенно в регионах с ограниченным покрытием. Дополнение сети мобильными пробниками позволит исследовать локальную неоднородность сетей доступа, выявлять зоны деградации качества и сравнивать характеристики маршрутов в различных точках подключения.

Важным направлением является интеграция с внешними источниками данных. Сопоставление активных измерений с маршрутной информацией, данными об IP-пространстве и автономных системах, внешними измерительными платформами и специализированными наборами данных позволит повысить полноту интерпретации сложных сетевых событий.

Перспективным является и применение методов машинного обучения к накопленным данным. Временные ряды RTT, результаты HTTP- и DNS-проверок, сведения о маршрутах и географии могут использоваться для автоматического обнаружения аномалий, выделения периодов деградации и классификации типовых событий. При этом автоматические методы должны дополнять измерительную методологию и сопровождаться контрольными выборками и экспертной проверкой результатов.

Отдельное значение имеет развитие открытого API платформы. Программный интерфейс позволит автоматизировать получение результатов измерений, интегрировать их с внешними системами анализа, создавать специализированные исследовательские приложения и воспроизводить эксперименты. Это позволит перейти от платформы визуализации и локального анализа к исследовательской инфраструктуре, доступной более широкому сообществу.

Совокупность этих направлений развития должна обеспечить переход от фиксации отдельных измерительных показателей к формированию воспроизводимой картины состояния и поведения российской интернет-инфраструктуры.

Интерфейс платформы доступен для ознакомления и тестирования по адресу: https://ms.ididb.ru/

Список литературы:

[1] Claffy K., Hyun Y., Keys K., Fomenkov M., Krioukov D. Internet Mapping: From Art to Science. Cybersecurity Applications & Technology Conference, 2009.

[2] Rekhter Y., Li T., Hares S. A Border Gateway Protocol 4 (BGP-4). RFC 4271, 2006.

Об авторе:

Николай Егорович Гавриченко, координатор разработки продуктов Фонда развития сетевых технологий «ИнДата», ассистент кафедры интеллектуальных систем и теплофизики ИИР НГУ.



Измерение DNS поверх IPv6

Джефф Хьюстон

Аннотация

В статье рассматривается готовность системы DNS к работе с протоколом IPv6 – в частности, возможность разрешения доменных имён через авторитетные DNS-серверы, доступные исключительно по IPv6. Опираясь на данные измерений APNIC, Джефф Хьюстон предлагает метод тестирования, ориентированный именно на DNS и дополняющий измерения, проводимые через веб-среду.

Результаты показывают, что около 75% пользователей Интернета способны выполнять DNS-запросы по протоколу IPv6. При этом расхождения в данных, полученных с помощью разных методов измерения, подчёркивают сложность оценки готовности к IPv6, а также трудности, связанные с переходом на DNS-инфраструктуру, функционирующую исключительно на базе IPv6.

Ключевые слова:

DNS, IPv6, резолвер

Теоретически, архитектура IPv6 была спроектирована так, что транспортные протоколы сквозной передачи данных верхнего уровня, а именно TCP и UDP, не должны были знать о том, какой IP-протокол используется на сетевом уровне. Ведь мы должны иметь возможность использовать IPv4 и IPv6 в системе DNS взаимозаменяемо, верно?

Эта тема рассматривалась в документе серии BCP (Best Common Practice, «лучшая современная практика»), опубликованном в 2004 году под номером RFC 3901, «DNS IPv6 Transport Operational Guidelines» («Рекомендации по использованию транспорта IPv6 для DNS»). В документе содержались две основные рекомендации:

- во-первых, каждый рекурсивный сервер имён должен быть либо с поддержкой только IPv4, либо с двойным стеком (dual-stack);
- во-вторых, каждая зона DNS должна обслуживаться как минимум одним доступным сервером имён, использующим IPv4.

По сути, это был призыв «Пока не отказывайтесь от IPv4!», что на то время было вполне разумным советом.

В начале 2026 года планируется опубликовать обновлённую версию этого документа под названием RFC 3901bis, в которой предлагается несколько иной набор рекомендаций (прим. редакции – эта версия была опубликована в августе 2026 года под номером RFC10001). Согласно этому документу, как минимум два сервера имён для каждой зоны должны поддерживать двойной стек, то есть каждый сервер имён будет доступен по IPv6. Этот документ даёт следующую практическую рекомендацию по поддержке IPv6 в DNS: «Пришло время отнестись к IPv6 всерьез!» Предположение, лежащее в основе документа RFC 3901bis, заключается в том, что IPv6 теперь является зрелой и хорошо изученной технологией, а использование IPv6 в качестве транспорта для DNS столь же эффективно и быстро, как и использование IPv4.

Но можно ли считать этот совет разумным? Основная проблема, связанная с отказами в обслуживании DNS, заключалась в адаптации к нагрузкам при передаче больших объёмов данных через сети с ограничением размера паке-

тов. IPv6 лишил маршрутизаторы возможности выполнять «фрагментацию на лету», и это повлияло на работу DNS при больших нагрузках с использованием UDP поверх IPv6.

За последние несколько лет я неоднократно рассматривал этот сценарий, в том числе в статьях «Adding IPv6-only to DNS and Truncation in UDP», «IPv6, the DNS and Happy Eyeballs», «IPv6 and the DNS». При попытке передать по протоколу IPv6 большие ответы, требующие фрагментации пакетов, DNS сталкивается с примерно 40% отказов.

Что, если мы ограничим рассмотрение типичным случаем DNS, когда запросы и ответы свободно помещаются в размере максимального нефрагментированного пакета IPv6 в 1280 байт? Какая часть пользователей Интернета сможет получить надёжный доступ к DNS-серверу, доступ к которому возможен только по протоколу IPv6?

Чтобы ответить на такой вопрос, нам нужно было бы провести широкомасштабное исследование среди пользователей Интернета и проверить их способность «резолвить» (разрешать в адрес IP) DNS-имя, доступ к которому возможен только по IPv6. Эта тема степени готовности конечных пользователей использовать IPv6 для доступа ко всем формам интернет-сервисов уже много лет вызывала значительный интерес в рамках более масштабной задачи перевода всего Интернета на IPv6.

Вопрос, который я хотел бы здесь рассмотреть, касается степени поддержки пользовательскими DNS-резолверами протокола DNS поверх IPv6. Другими словами, если бы мы разместили авторитетный сервер на платформе, поддерживающей только IPv6, какая часть пользователей Интернета смогла бы разрезолвить имя, доступное таким образом?

Измерение DNS

Во-первых, несколько слов предостережения. При измерении DNS всё не так просто, как кажется. Когда мы говорим о DNS в этом контексте, мы на самом деле говорим о функции резолвинга имён. И центральным в этом является концепция «DNS-резолвера».

Резолверы

Итак, давайте зададим вопрос: «Что такое DNS-резолвер?»

Как ни странно, прямого ответа не существует. Мы на самом деле не до конца понимаем, что такое «DNS-резолвер». Это может быть единая платформа, на которой запущен экземпляр кода DNS-резолвера, или это может быть набор серверных DNS-систем с каким-либо фронтенд-распределителем нагрузки, или это может быть гибридная совокупность серверов с набором частично синхронизированных кешей, чтобы они эмулировали общий кеш и использовали этот общий кеш в работе каждого серверного движка.

Мы грубо классифицировали DNS-резолверы на stub-резолверы (локальные резолверы), которые находятся близко к конечному пользователю на его устройстве, рекурсивные резолверы, которые предназначены для навигации по распределённой базе данных DNS для резолвинга запрашиваемых имён, и перенаправляющие (forwarding) резолверы, которые передают свои запросы другим резолверам, а не отвечают на них сами. Существуют и более сложные формы гибридного поведения, которые могут быть распределены между множеством различных систем резолвинга. Все они называются резолверами.

Не все резолверы одинаковы и не все одинаково важны. У резолвера может быть всего один клиент, как у DNS-резолвера в моей локальной сети, а может быть и несколько миллионов, если не сотен миллионов клиентов, как в случае с некоторыми крупными открытыми DNS-резолверами, или любое промежуточное значение. Поэтому, когда мы говорим о DNS-резолверах, на самом деле довольно сложно понять, о чём именно идёт речь. Получение статистического показателя в виде некоторого процента DNS-резолверов, поддерживающих запросы по IPv6, не имеет смысла с точки зрения оценки полезности IPv6 в DNS. Вот почему, когда мы говорим об уровне поддержки IPv6 в DNS-резолвинге, метрикой, которую мы будем использовать, будет не количество самих DNS-резолверов, а количество пользователей в процентном соотношении от общего числа пользователей.

Запросы

Конечно, если вы думали, что это был сложный вопрос о DNS, то вот вам еще один: «Что такое запрос?»

Вопрос может показаться глупым, но в нём есть смысл. Процесс резолвинга, используемый DNS для навигации по структурам данных DNS, вызывает веерный (fan-out) запрос, где один начальный запрос к рекурсивному резолверу заставляет этот резолвер запускать последовательность поисковых запросов, в попытках понять, где может находиться запрашиваемая информация в рамках распределённой базы данных DNS.

Связанная с этим проблема заключается в том, что по умолчанию DNS использует UDP в качестве транспорта. UDP не обеспечивает никаких гарантий доставки, поэтому отправитель должен некоторое время ждать ответа, и если ответ не поступает за это время, у него нет другого выхода, кроме как повторить запрос. Резолверы не ведут себя единообразно, в разных реализациях используются разные значения таймеров для определения времени повторного запроса. Выбор таймера представляет собой компромисс между стремлением ответить как можно быстрее на исходный DNS-запрос и предотвращением флуда(перегрузки) DNS излишними запросами.

DNS-запросы не имеют счётчика переходов – «хопов» (hop count), поэтому, если запрос перенаправляется от одного резолвера к другому, к нему не прикрепляется история того, откуда пришёл запрос, и нет кода причины, почему запрос был перенаправлен. В DNS нет контекста, который позволил бы нам определить причину любого конкретного запроса,

нет счётчика хопов для выявления зацикливания и нет TTL (time-to-live) – «времени жизни» для обнаружения и удаления «устаревших» запросов. В результате DNS-резолвинг склонен грешить избыточностью в генерации запросов. Наши измерения, проведённые на авторитетном DNS-сервере, показывают, что от 25% до 30% отдельных запросов повторяются внутри DNS (рисунок 1).

Я подозреваю, что одна из причин такого расточительного повторения запросов внутри DNS кроется в выборе UDP в качестве транспортного протокола по умолчанию. Резолвер не знает, когда запрос был отброшен, и лучшая стратегия для резолвера – разослать поток запросов на другие авторитетные серверы, а в случае локального резолвера – на другие рекурсивные резолверы, чтобы компенсировать непредсказуемое время отклика UDP.

Измерения APNIC

Наконец, давайте посмотрим на собственную измерительную установку APNIC, которая используется для проведения подобных измерений.

Мы используем рекламную сеть Google для генерации DNS-запросов внутри рекламных онлайн-кампаний и используем параметры в рекламной кампании, чтобы получить как можно более широкое распространение рекламы. Каждое объявление содержит список URL-адресов и управляющий скрипт, который ставит браузеру задачу запрашивать каждый URL-адрес, а затем сообщает об успешном (или неуспешном) выполнении каждой попытки запроса. DNS-имена, входящие в состав каждого URL, содержат компонент имени, уникальный для каждого отдельного пользователя, получившего рекламу. Таким образом, рекурсивные DNS-резолверы не имеют кешированных данных и вынуждены отправлять запросы авторитетному DNS-серверу для резолвинга предоставленного имени. Мы отслеживаем эти запросы от рекурсивных к авторитетным серверам инструментами нашего авторитетного сервера и сопоставляем эти запросы с записями о размещении рекламы на экспериментальной платформе.

Измерение DNS поверх IPv6 с помощью Web Fetch

Для выполнения этого измерения мы написали скрипт для рекламы, который включает URL, использующий уникальное DNS-имя, и настроили авторитетный сервер для этого DNS-имени так, чтобы он был доступен только по IPv6.

Пользователь может резолвить DNS-имя и, следовательно, загрузить веб-объект, только если его настройка резолвера имён поддерживает DNS-запросы по IPv6. Хотя резолвинг

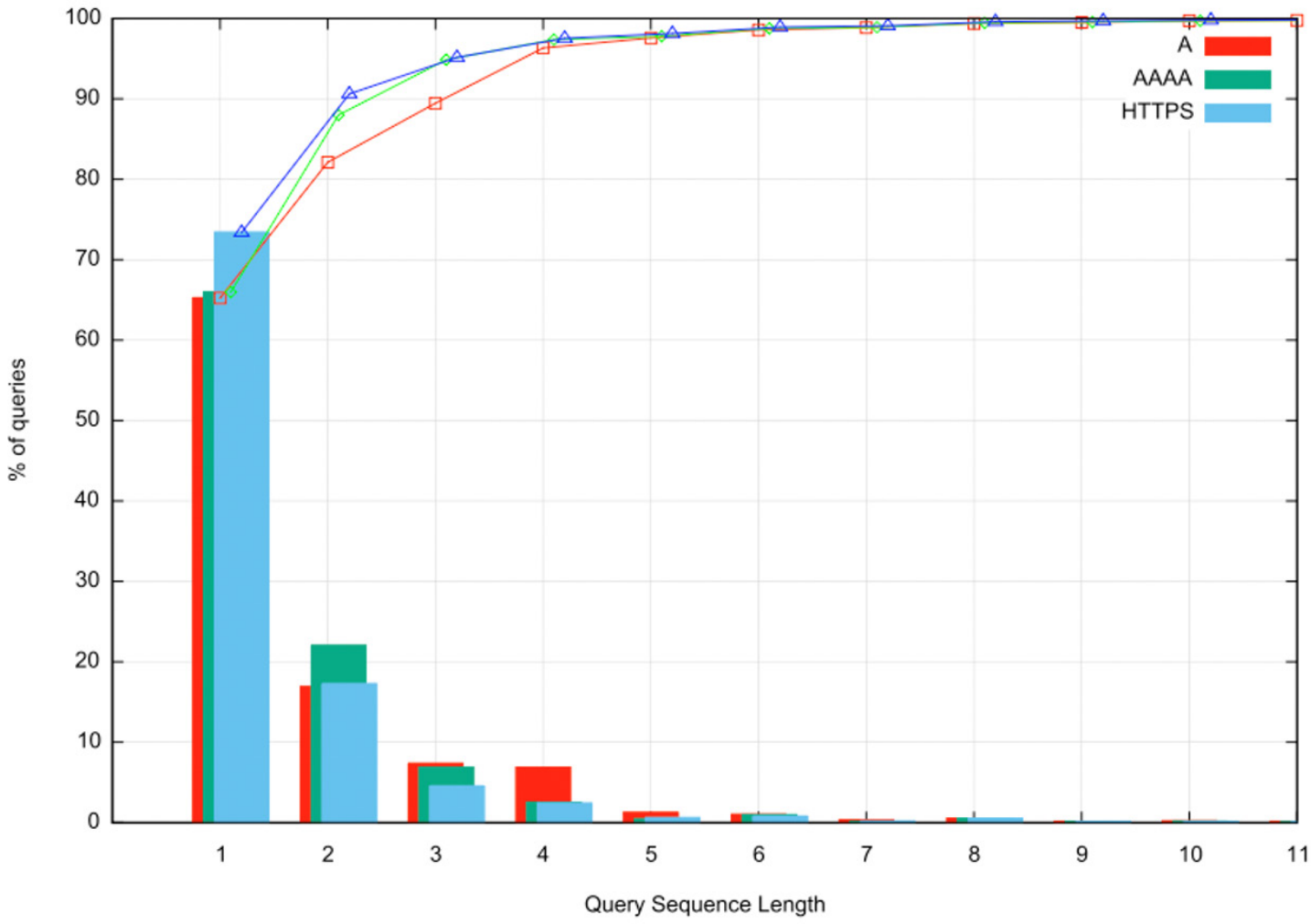


Рис. 1. Профиль повторения DNS-запросов.

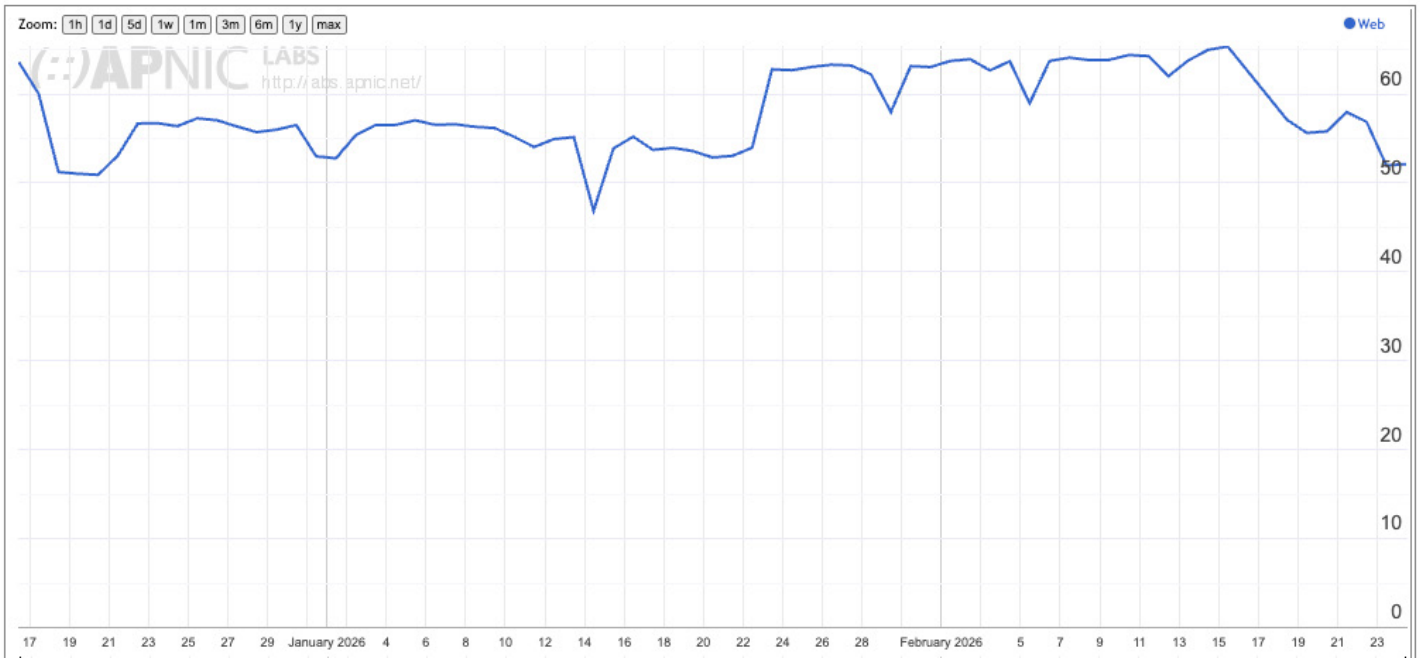


Рис. 2. Веб-измерение способности DNS-резолвинга с использованием IPv6.

DNS-имени опирается на IPv6, само имя может быть преобразовано как в IPv4 (A), так и в IPv6 (AAAA) записи.

Таким образом, провести измерение довольно просто. Мы считаем записи о размещении рекламы и долю тех записей, где пользователь успешно выполняет загрузку веб-объекта DNS поверх IPv6. Таким образом, доля успешных обращений – это показатель способности пользователей по всему Интернету выполнять резолвинг DNS с использованием IPv6. Эти данные показаны на рисунке 2.

Кажется, это разумное измерение. Результат, а именно то, что от 50% до 65% пользователей демонстрируют свою способность резолвить DNS-имя, требующее использования DNS поверх IPv6.

Мы закончили, да?

Ну, возможно, нет. Видите ли, внутри браузера пользователя происходит пара действий, о которых нам нужно знать. Браузер получает задачу загрузить веб-объект. Ему сообщают его имя, DNS-имя, которое он сначала должен резолвить. Только когда DNS разрезолвит это имя, браузер сможет выполнить загрузку. Но что, если выполнение скрипта рекламы будет прервано до завершения скрипта? Задача DNS, которая, возможно, уже была передана резолверу, будет выполняться до завершения, но когда результат будет передан обратно в браузер, последующей веб-загрузки не произойдёт. Возможно, этот результат не будет учтён.

Есть ли другой способ выполнить это измерение способности IPv6 в DNS, используя только DNS? Если бы это было возможно, то после передачи задачи в DNS процесс резолвинга имени продолжался бы до завершения и не прерывался бы досрочно, если бы управляющий скрипт рекламы был завершён.

Измерение DNS поверх IPv6 с помощью DNS

Ответ на этот вопрос заключается в том, что такое измерение можно провести полностью в рамках DNS. Мы используем метод «делегирования без привязки» (glueless delegation) в DNS.

Когда рекурсивный резолвер спрашивает авторитетный сервер об имени, которое не существует в обслуживаемой зоне, но находится в делегированной зоне, сервер вернёт ответ с перенаправлением (referral response).

При делегировании в DNS указывается имя делегированной зоны и имена серверов, которые являются авторитетными для этой зоны. Когда авторитетный сервер запрашивают об имени, которое находится в делегированной зоне, он генерирует ответ с перенаправлением, в секции Authority которого содержатся записи о серверах DNS, а в секции Additional – IP-адреса этих серверов («склеивающие записи», glue records). Если эти имена серверов указаны в делегированной зоне, то эти склеивающие записи необходимы, так как нет другого способа для рекурсивного резолвера преобразовать эти имена в их IP-адреса. Однако когда имена определены в другой зоне, не связанной с запрашиваемой зоной, эти склеивающие записи не являются необходимыми для резолвинга. Если склеивающие записи отсутствуют в ответе-перенаправлении, то рекурсивному резолверу потребуется приостановить основную задачу преобразования исходного имени и поработать над подзадачей резолвинга имени сервера DNS. После этого он сможет использовать полученные IP-адреса для возобновления резолвинга исходного имени.

Таким образом, это даёт основу для проверки поддержки IPv6 в DNS, как показано на рисунке 3.

```
Zone: example.com
...
a IN NS ns1.some.other.zone.
...


Zone: some.other.zone
...
. IN NS nso.some.other.zone.
nso IN AAAA 2001:db8::1
...
ns1 IN AAAA 2001:db8::2
...


Zone: a.example.com
...
. IN NS ns1.some.other.zone.
. IN A 192.0.2.3
IN AAAA 2001:db8::3
```

Рис. 3. Пример делегирования без склеивающих записей.

В этом случае рекурсивный резолвер, пытающийся преобразовать имя a.example.com, получит ответ с перенаправлением на имя сервера ns1.some.other.zone без склеивающих записей. После этого ему нужно будет приостановить процесс резолвинга a.example.com и начать процесс резолвинга имени сервера ns1.some.other.zone. После завершения этого процесса (с получением IPv6-адреса 2001:db8::2) он сможет вернуться к исходной задаче и запросить у этого IPv6-адреса IP-адреса a.example.com. Однако, поскольку сервер some.other.zone поддерживает только IPv6, рекурсивный резолвер может отправить этот запрос только в том случае, если он поддерживает DNS-запросы по протоколу IPv6 и может получить DNS-ответ только по протоколу IPv6.

Мы можем провести оба измерения с использованием DNS по IPv6 в рамках одного рекламного скрипта, протестировав DNS-среду пользователя обоими способами. Мы ожидаем, что результаты измерений будут достаточно хорошо коррелировать, при этом измерение с использованием DNS даст чуть более высокий результат. Именно это мы и наблюдаем (см. рисунок 4). Приблизительно на 10% более низкий результат при использовании веб-запроса можно объяснить «потерями» при переходе от резолвинга DNS к завершению веб-запроса.

Есть ли у нас основания для такого предположения?

Аномалии измерений

В ряде африканских стран наблюдается стабильное, хотя и аномальное поведение при измерении этого показателя, когда значение, полученное с помощью веб-измерений, значительно выше значения, полученного с помощью DNS. Хороший пример — Алжир (рисунок 5), хотя аналогичная ситуация наблюдается в Ливии, Египте, Мавритании, Либерии и ряде других преимущественно африканских стран (см. https://stats.labs.apnic.net/v6odns).

Есть и страны с противоположным аномальным результатом: в них показатель DNS выше веб-показателя значительно больше, чем на 10%. Хорошим примером такого противоположного аномального результата является Эфиопия (рисунок 6).

Стоит отметить ещё один результат, который можно увидеть на примере Германии, где ежедневные измерения на основе веб-запросов и DNS-запросов очень хорошо коррелируют друг с другом. Уровень «потери веб-трафика», когда DNS-запрос не преобразуется в видимый веб-запрос, крайне низок для всей выборки в этой стране (рисунок 7).

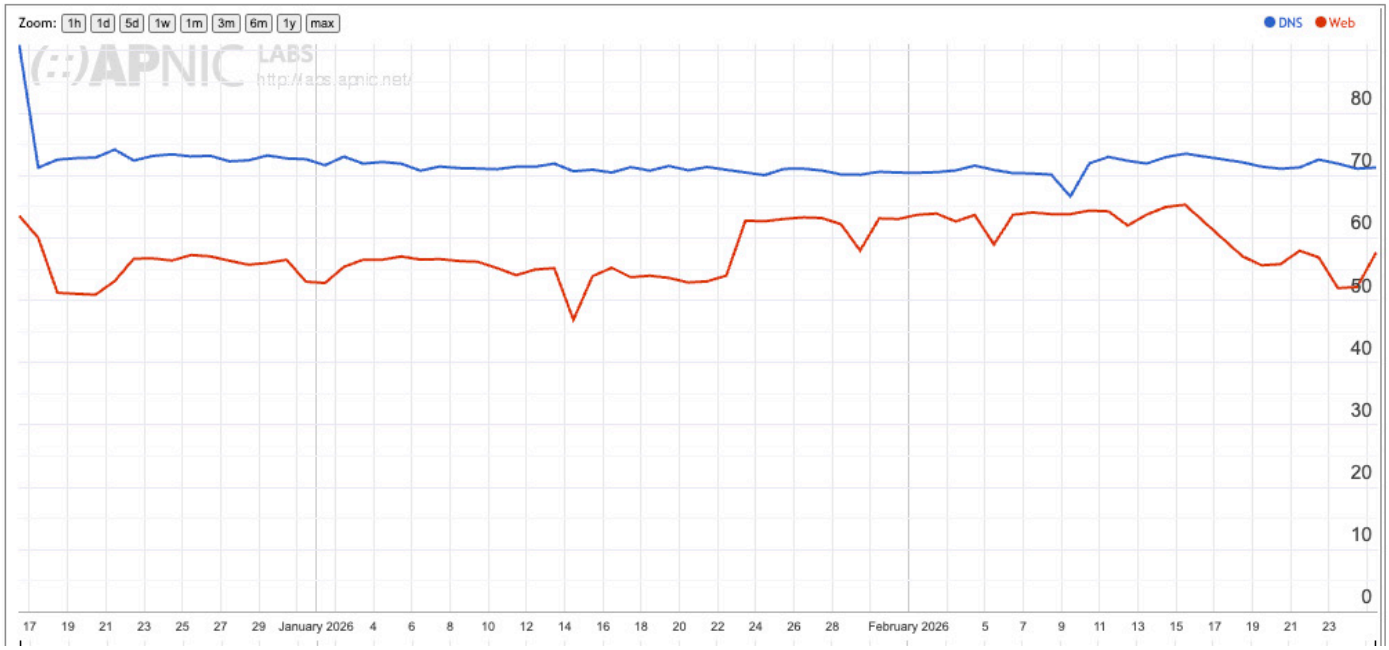


Рис. 4. Измерение способности резолвинга DNS поверх IPv6 с помощью DNS и веб-измерений.

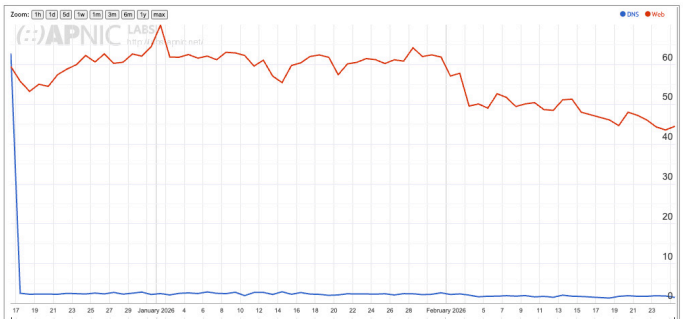


Рис. 5. Измерение способности резолвинга DNS поверх IPv6 на основе данных DNS и веб-измерений в Алжире.

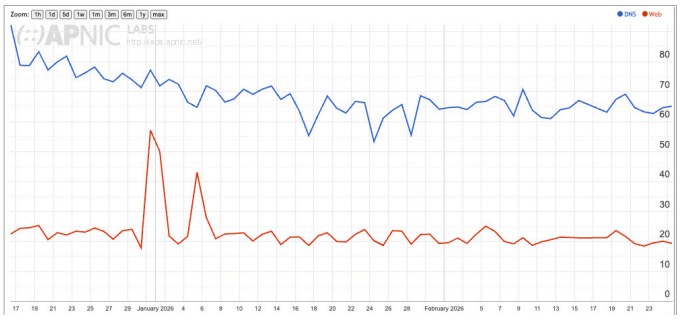


Рис. 6. Измерение способности резолвинга DNS поверх IPv6 на основе измерений DNS и веб-трафика в Эфиопии.

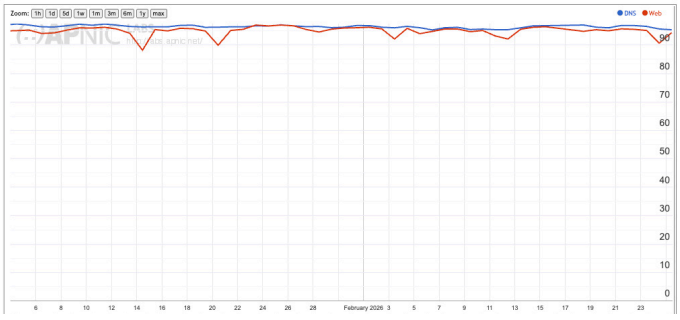


Рис. 7. Измерение способности резолвинга DNS поверх IPv6 на основе данных DNS и веб-измерений в Германии.

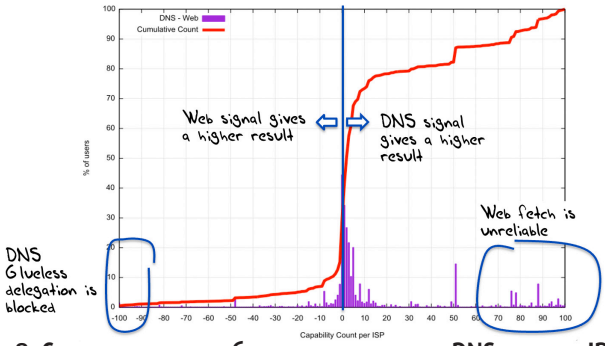


Рис. 8. Сравнение способности резолвинга DNS поверх IPv6, DNS и веб.

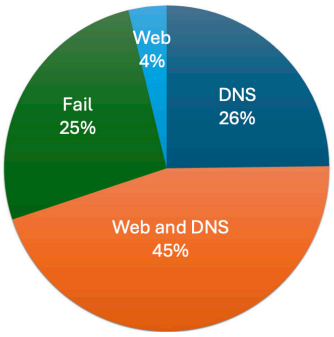


Рис. 9. Разбивка результатов измерений веб-трафика и DNS.

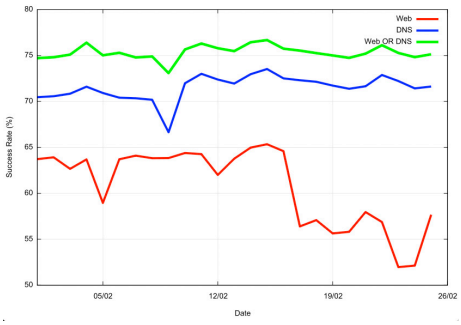


Рис. 10. Серия результатов по дням.

Эти результаты сложно объяснить в рамках традиционной модели инфраструктуры DNS, поскольку в обоих случаях измеряется одно и то же поведение одних и тех же пользователей, тестирующих одни и те же DNS-резолверы.

Один из способов сравнить эти два подхода — проанализировать каждую сеть и сопоставить результаты измерений DNS- и веб-трафика. Такое сравнение показано на рисунке 8.

Менее чем для 8% измеренных конечных точек значение, полученное при измерении с помощью DNS, было более чем на 10% меньше значения, полученного при измерении с помощью интернет-трафика, в то время как для 30% измеренных конечных точек наблюдалась обратная ситуация. Для оставшихся 62% измерений разница между двумя показателями не превышала 10%.

На рисунках 9 и 10 представлена разбивка результатов измерений с помощью трафика Интернет и с помощью DNS по дням. В 4% случаев при измерении с помощью трафика Интернет был получен положительный результат, указывающий на поддержку DNS поверх IPv6, в то время как при измерении с помощью DNS результат был отрицательным. В 26% случаев при измерении через DNS был получен положительный результат, а при измерении с помощью трафика Интернет — отрицательный. В 45% случаев и при измерении с помощью трафика Интернет, и при измерении с помощью DNS результат был положительным.

Результаты, безусловно, интересны. Измерение только с помощью DNS более показательно, поскольку мы видим, что DNS работает через делегирование без «склеивания» более надёжным образом. Однако есть сети, в которых происходит блокировка резолвинга доменных имён при отсутствии «склеивающих» записей (в основном в Северной Африке), и эта блокировка затрагивает около 3% от общего числа пользователей.

Таким образом, мы видим, что около 75% пользователей могут использовать DNS через IPv6.

Примечание

Приведённые выше взгляды не обязательно отражают точку зрения Азиатско-Тихоокеанского сетевого информационного центра.

Об авторе:

Джефф Хьюстон (Geoff Huston), AM B.Sc., M.Sc., является главным научным сотрудником Азиатско-Тихоокеанского сетевого информационного центра (APNIC), регионального интернет-регистратора, обслуживающего Азиатско-Тихоокеанский регион.

Контроль качества инфраструктуры Интернета – ICANN SLAM

Дмитрий Коваленко

Аннотация

Как ICANN контролирует стабильность Интернета в миллисекундах? Разбираем устройство системы SLAM (Service Level Agreement Monitoring) — невидимого арбитра, который непрерывно тестирует сотни доменных зон верхнего уровня через сеть из 40 глобальных пробников. Внутри статьи — технические критерии Спецификации № 10 для gTLD, особенности добровольного мониторинга для национальных доменов (ccTLD) и принципы получения данных через API (MoSAPI).

Ключевые слова:

ICANN SLAM, MosAPI, распределённая сеть мониторинга, gTLD, ccTLD, DNS, RDAP, SRS

Введение

Доменная индустрия является важной частью цифровой инфраструктуры и влияет на развитие технологий, бизнеса и общества в целом. ICANN (Internet Corporation for Assigned Name and Numbers) является ключевой некоммерческой организацией в доменной индустрии на глобальном уровне. Одной из важнейших задач в обеспечении бесперебойного функционирования доменов верхнего уровня (TLD) является контроль за соблюдением технических требований к инфраструктуре, обеспечивающей работоспособность TLD. Важными частями этой инфраструктуры являются несколько сервисов: широко известный сервис DNS и менее известные сервисы SRS и RDAP. В частности, при регистрации домена второго уровня регистратор отправляет команду по протоколу EPP в систему регистрации доменов (SRS) реестра TLD. Впоследствии информация о домене из реестра попадает в DNS — домен делегируется на соответствующие серверы имён, а данные о владельце домена становятся доступны через RDAP, являющимся преемником устаревшего протокола WHOIS. Главным инструментом контроля работы основных сервисов TLD выступает система SLAM (Service Level Agreement Monitoring) [1].

В этой статье мы разберём, как устроена система SLAM, из каких географических точек планеты производятся замеры и как эту систему можно использовать для мониторинга сервисов национальных доменов верхнего уровня (ccTLD).

Зачем ICANN контролирует регистратуры TLD

Когда ICANN делегирует новую доменную зону верхнего уровня (например, .tech, .online или .tatar), она подписывает с регистратурой — организацией, которая отвечает за функционирование TLD — базовое соглашение (Base gTLD Registry

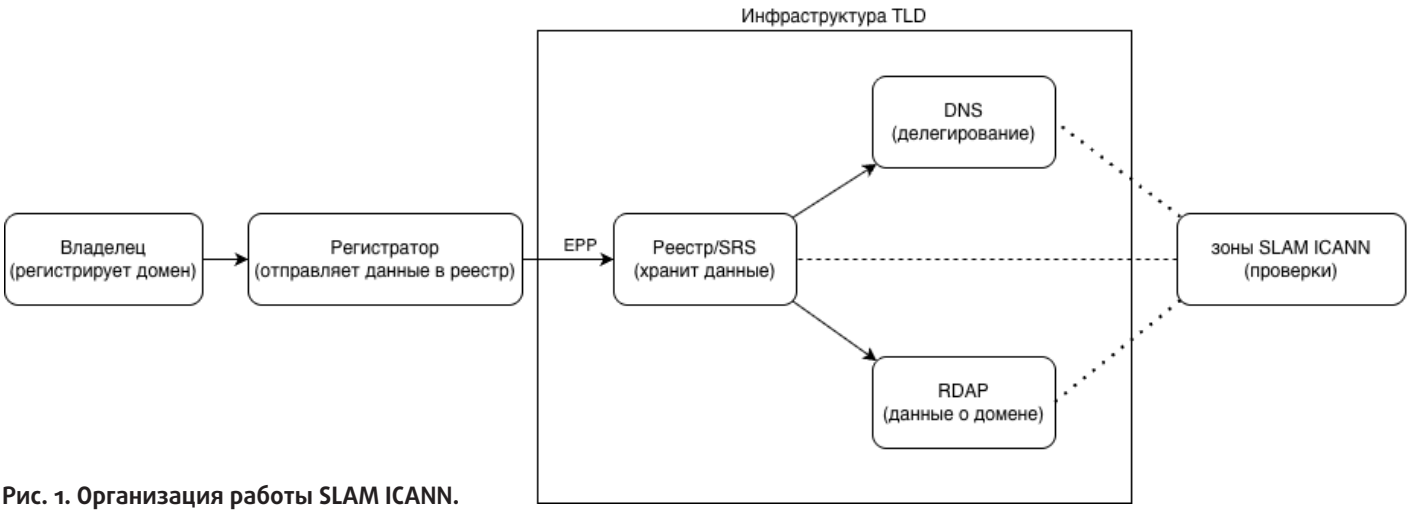


Рис. 1. Организация работы SLAM ICANN.

Agreement). В Спецификации № 10 (Specification 10) этого соглашения прописаны требования к качеству, доступности и скорости работы критически важных сервисов. Система SLAM создана именно для того, чтобы проверять, выполняют ли регистратуры эти обязательства.

При этом важно понимать, что зона юридической ответственности разделена в зависимости от типа регистратуры.

- Регистратуры gTLD (такие как .shop, .tech, .moscow) связаны с ICANN договорами. Они обязаны строго соблюдать все параметры Спецификации № 10, иначе рискуют потерять право на управление зоной.

- Регистратуры исторических gTLD (legacy gTLDs — таких как .com, .net или .org) имеют свои индивидуальные контракты с ICANN, в которые изначально не входила Спецификация № 10. Однако в процессе продления договоров ICANN планомерно унифицирует технические требования, например, на базовое соглашение перешли .org, .info и .biz. Исключение составляют лишь домены верхнего уровня .gov, .edu, .mil, которые регулируются отдельными внутренними регламентами США.

- Регистратуры страновых доменов ccTLD (такие как .uk, .de, .jp или .ru) находятся в совершенно иных условиях. Они представляют собой национальные структуры, работают по национальным правилам и не подпадают под прямое административное регулирование со стороны ICANN. Соответственно, они не обязаны выполнять требования Спецификации № 10. Тем не менее, ccTLD могут добровольно подключаться к системе SLAM, чтобы использовать её инструменты для анализа собственных сервисов.

Что именно измеряет SLAM: критерии Спецификации № 10

В Спецификации № 10 описаны проверки конкретных технических параметров по трём главным китам доменной инфраструктуры: DNS, RDDS/RDAP и SRS/EPP. Но в настоящее время мониторинг проводится только для служб DNS и RDDS/RDAP, а для SRS/EPP не проводится [2]. Замеры контролируют две ключевые метрики: доступность (availability) — процент времени стабильной работы — и время ответа (Round-Trip Time, RTT) — скорость реакции сервиса. Если показатели падают ниже требуемых значений, SLAM автоматически открывает инцидент.

Критерии проверки DNS

- Доступность DNS-сервиса: 100% (0 минут простоя в месяц). Сервис считается доступным, если в конкретный момент времени хотя бы два делегированных DNS-сервера из всех прописанных для зоны IP-адресов успешно отвечают на запросы зондов SLAM. Это самый критичный компонент инфраструктуры. Сбой в доступности DNS-сервиса означает, что домены в зоне по истечении TTL закешированных записей станут недоступны по всему миру. Поэтому здесь самое строгое требование к доступности, и падение сервиса — это триггер для немедленного вмешательства ICANN.

- Валидация DNSSEC: SLAM проверяет корректность цепочки доверия и правильность отдачи DNSSEC-записей. Любая техническая ошибка в подписях зон приравнивается к падению DNS.

- Доступность конкретного DNS-сервера: ≥ 99% (допускается не более 432 минут простоя в месяц для каждого отдельного IP-адреса). SLAM индивидуально проверяет каждый зарегистрированный IPv4- и IPv6-адрес каждого DNS-сервера зоны. Здесь требования мягче, что позволяет проводить техническое обслуживание инфраструктуры отдельных DNS-серверов без инцидентов в SLAM.

- Время ответа (RTT) для UDP: ≤ 500 мс для не менее 95% запросов. Тестовые пакеты DNS из сети зондов SLAM должны получить ответы по протоколу UDP от DNS-сервера быстрее, чем за полсекунды, а 5% ответов, превышающих порог, SLAM проигнорирует при подсчёте.

- Время ответа (RTT) для TCP: ≤ 1500 мс для не менее 95% запросов. Для тестовых пакетов DNS из сети зондов SLAM по протоколу TCP порог выше, так как необходимо дополнительное время для установки TCP-сессии.

- Время обновления DNS: ≤ 60 минут для не менее 95% зондов. Эта метрика считает время с момента, когда регистратор получил от системы регистрации (SRS) подтверждение об изменении данных по домену (например, смена NS-записей или добавление новых), до момента, когда зонды SLAM начнут получать от DNS-серверов новые данные. По сути, это жёсткий лимит на генерацию и дистрибуцию файлов доменной зоны, но на момент написания статьи эта метрика не контролировалась SLAM.

Критерии проверки RDDS/RDAP

- Доступность RDDS-сервиса: 98% (допускается не более 864 минут простоя в месяц). Сервисы WHOIS, классический — Port 43 и Web-WHOIS, предоставляющие информацию о владельцах доменов. Хотя они напрямую не влияют на открытие сайтов, ICANN считает их критически важными для безопасности и борьбы с фишингом.

- Время ответа RDDS (RTT): ≤ 2000 мс для не менее 95% запросов. Для запроса, отправленного на конкретный IP-адрес одного из серверов одной из служб RDDS, считается время от момента начала TCP-соединения и до его завершения. В зависимости от выбранной службы анализируется либо ответ WHOIS (для Port 43), либо HTTP-ответ (для Web-WHOIS).

- Время обновления RDDS: ≤ 60 минут для не менее 95% зондов. Эта метрика считает время с момента, когда регистратор получил от системы регистрации (SRS) подтверждение об изменении данных по домену (например, смена контакта), до момента, когда зонды SLAM начинают получать от RDDS-серверов новые данные. По сути, это лимит на синхронизацию данных между базой данных реестра и

её внешними публичными сервисами RDDS, но на момент написания статьи эта метрика не контролировалась SLAM.

С января 2025 года RDAP стал основным источником информации о регистрации доменных имен в gTLD, и ICANN перешла к полноценному контролю RDAP через систему SLAM. С этого момента проблемы с RDAP подлежат таким же процедурам эскалации, как и у старого протокола WHOIS [3]:

- доступность RDAP-сервиса: 98% (допускается не более 864 минут простоя в месяц);
- время ответа (RTT) для RDAP: ≤ 2000 мс для не менее 95% запросов. Для этой проверки появляется обязательное требование – использование протокола HTTPS;
- время обновления RDAP: ≤ 60 минут для не менее 95% зондов.

Критерии проверки SRS

- Доступность EPP-сервиса: 98% (допускается не более 864 минут простоя в месяц). Служба считается доступной, если зонды SLAM успешно устанавливают TCP-соединения со службой и получают корректные ответы на базовые команды. SRS/EPP — важная часть распределённой системы регистрации, через которую аккредитованные регистраторы отправляют XML-команды по протоколу EPP на регистрацию, продление или изменение доменов. Сбои этой системы не ломают текущий DNS, но полностью парализуют продажи и управление доменами.

SLAM разделяет команды EPP на три категории по уровню нагрузки и замеряет их RTT раздельно:

- команды EPP-сессии (RTT): ≤ 2000 мс для не менее 95% транзакций. Сюда входят служебные команды управления сессией: <login> (авторизация) и <logout> (завершение сессии). Зонды имитируют реальное поведение регистратора: устанавливают защищённое TLS-соединение, проходят авторизацию, выполняют серию тестовых запросов/изменений и корректно закрывают сессию. Если на этапе «рукопожатия» или логина происходят задержки — это сразу отразится на данной метрике;
- EPP-команды чтения (RTT): ≤ 2000 мс для не менее 95% транзакций. К этой категории относятся команды чтения данных, такие как <check> (проверить доступность домена) и <info> (получить данные объекта);
- EPP-команды записи (RTT): ≤ 4000 мс для не менее 95% транзакций. Это команды, которые меняют состояние базы данных реестра: <create> (регистрация), <update> (обновление данных), <delete> (удаление) и <renew> (продление).

Задекларировано, что метрики времени ответа для EPP-команд чтения и записи выполняются только над реально существующими в реестре объектами и учитывают интервал между отправкой одной команды и получением ответа на неё. Накладные расходы, такие как открытие/закрытие TCP- и EPP-сессий, из этих замеров исключены, но на момент написания статьи эти метрики SRS/EPP не контролировались SLAM.



Рис. 2. География размещения зондов ICANN.

При взгляде на метрики RTT невольно появляется вопрос, почему используются такие высокие пороги. Для сетевого инженера задержка в 500 миллисекунд на DNS-ответ кажется огромной, ведь в пределах одной небольшой страны или города DNS-сервер отвечает за 2—10 мс. Ответ на этот вопрос раскрою в следующем разделе.

Географическая архитектура SLAM: глобальная сеть зондов

Чтобы круглосуточно контролировать «пульс» инфраструктуры доменов верхнего уровня, ICANN развернула глобальную сеть из 40 измерительных зондов, охватывающих все регионы. Списки IP-адресов этих зондов периодически обновляются и доступны регистратурам через RRI (Registration Reporting Interfaces).

Для обеспечения максимальной объективности ICANN арендует мощности в крупнейших дата-центрах мировых магистральных провайдеров и облачных гигантов. Зонды не сконцентрированы в одной локации, а буквально «опоясывают» земной шар.

География SLAM заставляет ICANN закладывать огромный буфер на физические ограничения сети:

- скорость света в оптоволокне конечна: запрос от зонда из Австралии или Южной Африки до узла в Европе, проходя через трансокеанские подводные кабели и десятки стыков, в идеальных условиях тратит 150—250 мс только на путь туда и обратно;
- магистральный Интернет постоянно «дышит»: перестроение таблиц маршрутизации и временные перегрузки на стыках операторов связи могут поднять RTT.

Высокие пороги гарантируют, что SLAM зафиксирует реальную деградацию важных инфраструктурных сервисов, а не зафиксирует нарушение SLA из-за того, что где-то посреди Атлантического океана оператор связи перенаправил трафик по резервному маршруту. Кроме этого, зонды не размещают за каналами связи с большой задержкой распространения сигнала, такими как спутниковые каналы.

Как SLAM проверяет аварии: правило консенсуса 51%

Система SLAM спроектирована так, чтобы исключить ложные срабатывания, вызванные проблемами с Интернетом у самого измерительного зонда. Система работает по следующему алгоритму консенсуса:

- цикл проверок: тесты запускаются каждую минуту для DNS и каждые пять минут — для RDDS/RDAP;
- консенсус (51%): чтобы зафиксировать сбой службы (например, падение DNS), система должна получить подтверждение как минимум от 51% всех активных зондов в рамках цикла проверки. Если только один зонд в Лондоне не получает ответа от сервера, а остальные 39 успешно получают ответы — инцидент не откроется, проблема признается локальной для сети этого зонда;
- правило нескольких циклов: инцидент в SLAM откроется только тогда, когда сбой, подтверждённый 51% зондов, держится три цикла подряд для DNS и два цикла — для RDDS/RDAP, и закроется, если восстановление подтверждено аналогичным образом. Такая логика делает SLAM надёжным арбитром: если была зафиксирована авария, значит, у регистратуры действительно начались серьёзные проблемы на инфраструктуре.

Что происходит при нарушении SLA: механизм эскалации и запуск EBERO

Система SLAM это не просто пассивный счётчик миллисекунд. Как только фиксируется, что показатели доступности или времени ответа вышли за рамки Спецификации № 10, ICANN запускает регламентированный процесс. В зависимости от характера сбоя события развиваются по двум сценариям: юридическому (Compliance Escalation) или экстренному техническому (программа Emergency Back-end Registry Operator — EBERO), где бюрократические процедуры откладываются.

Сценарий 1. Юридический

Этот путь активируется, если регистратура систематически нарушает взятые на себя обязательства. За дело берётся департамент ICANN Contractual Compliance, который осуществляет проактивный мониторинг для обеспечения соблюдения договорными сторонами условий соглашений и публикует отчёты о своей работе на ежемесячной основе [4], касательно регистратуры этот сценарий можно структурировать следующим образом:

- запрос разъяснений (Inquiry Notice): регистратуре высылается запрос, на который она обязана оперативно отреагировать, объяснить причины деградации критического сервиса и отчитаться о принятых мерах. Здесь может быть несколько итераций, в зависимости от качества ответов регистратуры;
- уведомление о нарушении (Notice of Breach): если сбои повторяются или регистратура не может исправить ситуацию, ICANN выносит официальное предупреждение. С этого момента регистратуре даётся ограниченный временной лимит на исправление проблем. Статус этих уведомлений является публичным. С текущим списком можно ознакомиться на сайте ICANN [5];
- расторжение контракта (Termination): ICANN запускает процесс расторжения контракта (Termination by ICANN), на завершающем этапе этого процесса ICANN официально уведомляет о расторжении контракта, тем самым аннулируя права регистратуры на gTLD.

Сценарий 2. Экстренное спасение — EBERO

Если инфраструктурный сбой носит необратимый характер и влияет на работу владельцев доменов в этом gTLD, например, технический бэкенд-оператор расторг контракт с регистратурой и отключил критические сервисы, отвечающие за gTLD, как это было с gTLD .nowruz, то ICANN официально инициирует экстренную процедуру спасения gTLD.

Как это работает: ICANN имеет долгосрочные контракты с опытными бэкенд-операторами (такими как CIRA, Nominet и CNNIC), которые действуют в соответствии с детально проработанной процедурой реагирования на чрезвычайные ситуации, называемой «Общий порядок перехода» (Common Transition Process — CTP).

Час «X»: если регистратура не может обеспечить работу критически важных сервисов, управление зоной в принудительном порядке переключается на одного из операторов EBERO.

Что спасают: перехватив управление, EBERO поднимает пять критических сервисов: DNS, DNSSEC, WHOIS/RDAP, SRS/EPP и выгрузку данных реестра в Escrow.

Что не спасают: бэкенд-оператор EBERO не предоставляет никаких дополнительных услуг, которые регистратура gTLD могла предоставлять своим пользователям, например, услуги хостинга.

Реальные прецеденты уже были; например, в 2024 году из-за критических проблем с WHOIS/RDAP под экстренное управление EBERO были принудительно переведены gTLD .nowruz, .pars, .shia, .tci и .xn--mgbt3dhd, за которые отвечала регистратура AGIT. В декабре 2024 ICANN расторгла с AGIT контракты на поддержку этих gTLD [6]. На текущий момент число gTLD, которые поддерживаются по программе EBERO, равно семи. Все эти домены поддерживаются бэкенд-оператором Nominet [7] и ждут своей дальнейшей участи.

Как устроен сбор данных: Архитектура MoSAPI

Все метрики, которые собирает распределённая сеть зондов SLAM, не остаются вещью в себе. ICANN предоставляет регистраторам gTLD, аккредитованным регистраторам и участвующим регистратурам ccTLD доступ к специальному программному интерфейсу — MoSAPI (Monitoring System API). Это защищённый REST API, работающий по протоколу HTTPS. Взаимодействие с MoSAPI подчиняется нескольким правилам:

- на транспортном уровне: поддерживается только протокол TLS версии 1.3, а также осуществляется фильтрация по IP;
- на сессионном уровне: для одного аккаунта разрешена только одна активная сессия, срок действия сессии не более 15 минут, кроме этого, разрешено открывать только одну сессию на один аккаунт не чаще чем раз в 5 минут, и новая сессия автоматически закроет старую.

Ключевые возможности

Через запросы к API можно собирать следующие сущности:

- текущий статус сервисов: общий статус сервисов (DNS, DNSSEC, RDDS, RDAP) по домену верхнего уровня;
- статус оповещений: информация о том, есть ли в данный момент предупреждение по какому-либо сервису;
- счётчик downtime: возвращает общее количество минут простоя сервиса за скользящую неделю (rolling week), что позволяет видеть, насколько близко сервис подошёл к критической отметке;
- логи инцидентов: полная выгрузка истории открытых и закрытых инцидентов по конкретной службе;
- логи измерений: детализация конкретных тестов, привязанная к временным меткам;
- сетевая диагностика: детализация сетевой связности для исследования сетевых инцидентов — когда зонд фиксирует ошибку подключения к anycast IP-адресу, то с помощью сохранённой диагностики утилиты MTR можно понять, на каком участке сети произошёл сбой.

Для технических специалистов работа системы SLAM приносит несколько ключевых особенностей:

- прозрачность: благодаря интерфейсу MoSAPI ICANN предоставляет сторонний взгляд на ключевую инфраструктуру TLD. Выгрузка сырых логов из распределённой сети 40 глобальных зондов позволяет объективно оценить, как критически важные сервисы выглядят в глазах пользователей из Москвы, Сан-Паулу или Токио;
- необходимость локальной аналитики: ограниченное хранение исторических данных (365 дней) в MoSAPI и отсутствие интерфейса для аналитиков заставляют строить собственные отказоустойчивые системы сбора и визуализации данных, которые позволяют сохранять многолетнюю историю системы SLAM для глубокого ретроспективного анализа.

Интерфейс MoSAPI не является статичным, с момента выпуска первой публичной версии 2.5 в 2017 году спецификация прошла через более чем 15 крупных итераций и дополнений. А внедрение тестового полигона на базе домена .test для отладки создаваемых интеграций информационных систем регистратур с MoSAPI говорит о высокой востребованности интерфейса.

Заключение

Система мониторинга ICANN SLAM — это важный элемент обеспечения стабильности современного Интернета. С её помощью ICANN поддерживает стабильность, предсказуемость и безопасность работы глобальной адресной системы для миллионов пользователей по всему миру. Для доменной индустрии существование такой независимой системы мониторинга даёт несколько важных преимуществ:

- глобальный стандарт качества;
- прозрачность взаимодействия;
- приоритет интересов пользователей.

SLAM демонстрирует, как автоматизированный аудит и чёткие правила игры помогают координировать сложнейшую распределённую инфраструктуру и сохранять Интернет единым и связанным пространством.

Для регистратуры ccTLD лучшей практикой для контроля инфраструктуры является гибридный подход:

- использование внешнего мониторинга ICANN SLAM через добровольное подключение позволяет получать объективный трансграничный взгляд на доступность важных сервисов ccTLD;
- развёртывание собственной распределённой системы мониторинга, спроектированной и построенной с учётом лучшего международного опыта эксплуатации критических систем. Собственная сеть измерительных зондов позволяет контролировать внутреннюю связность, гибко настраивать уведомления под локальную специфику и повышать суверенитет и отказоустойчивость национальной доменной зоны в любых условиях.

Глоссарий:

DNS (Domain Name System) — система доменных имён.

DNSSEC (Domain Name System Security Extensions) — набор расширений к протоколу DNS, который повышает его безопасность за счёт криптографической проверки подлинности и целостности данных, передаваемых через систему доменных имён.

EBERO (Emergency Back-end Registry Operator) — комплекс мер по поддержке работоспособности доменов в случаях нарушения регистратором правил функционирования в соответствии с контрактом ICANN.

Escrow — депозит данных реестра TLD.

gTLD (generic Top-Level Domain) — общий домен верхнего уровня.

ccTLD (Country Code Top Level Domain) — страновой домен верхнего уровня.

MosAPI — Monitoring System API в ICANN.

NS-запись (Name Server) — тип ресурсной записи в системе DNS, который указывает, какие DNS-серверы являются авторитетными для конкретного домена.

REST API (Representational State Transfer Application Programming Interface) — архитектурный стиль взаимодействия между клиентом и сервером.

RDDS (Registration Data Directory Services) /RDAP (Registration Data Access Protocol) — сервис, позволяющий третьим лицам получать доступ к данным регистрации доменных имён.

RTT (Round-Trip Time, RTT) — скорость ответа сервиса.

RRI (Registration Reporting Interfaces) — набор интерфейсов, предоставляемых организацией ICANN регистратурам и аккредитованным регистраторам для предоставления необходимой отчётности.

SRS (Shared Registration System) — распределённая система регистрации доменов.

SRS/EPP (Extensible Provisioning Protocol) — протокол, который работает внутри SRS и задаёт правила обмена данными.

TTL (Time to Live) — механизм, который ограничивает время жизни данных.

WHOIS (от англ. who is — «кто это») — сетевой протокол прикладного уровня, базирующийся на протоколе TCP (порт 43). Основное применение — получение регистрационных данных о владельцах доменных имён. В настоящее время заменен на RDAP.

Список литературы:

[1] https://www.icann.org/en/system/files/files/presentation-slam-13may17-en.pdf

[2] https://www.icann.org/en/system/files/files/mosapi-specification-26may26-en.pdf, page 7

[3] https://itp.cdn.icann.org/en/files/contracted-parties-communications/escalations-sla-failures-rdap-15jan25-en.pdf

[4] https://www.icann.org/resources/pages/contractual-compliance-monthly-reports-2025-09-15-en

[5] https://www.icann.org/compliance/notices

[6] https://www.icann.org/en/contracted-parties/registry-operators/services/registry-agreement-termination-service

[7] https://nominet.uk/blog/emergency-rescue-whats-an-ebero/

Об авторе:

Дмитрий Юрьевич Коваленко, архитектор DNS-решений — начальник отдела в MSK-IX.



Эпоха цифровой прозрачности: как меняется регулирование российских национальных доменов в зонах .ru, .рф и .su

Ирина Пыжова

Аннотация

С 1 сентября 2026 года меняется регулирование доменов .ru, .рф и .su. Правила теперь утверждает правительство РФ. В статье рассказывается о главных нововведениях: обязательной идентификации администраторов через ЕСИА, бессрочной регистрации доменных имён с ежегодной верификацией и создании спецрегистраторов для госсектора.

Ключевые слова:

домены, ЕСИА, регулирование Интернета, идентификация администраторов, цифровая прозрачность, Координационный центр доменов .RU/.РФ, РосНИИРОС

С 1 сентября 2026 года в российском сегменте Интернета начался новый этап регулирования. Масштабные изменения затрагивают правила регистрации, делегирования и администрирования более семи миллионов доменов в национальных зонах .ru, .рф и .su.

Новые нормы направлены на повышение кибербезопасности, искоренение анонимности в доменной зоне и усиление государственного контроля над российским доменным пространством.

Разбираем три ключевых нововведения, которые изменят правила игры для бизнеса, госорганов и обычных пользователей.

Государственный вектор: правила утверждает правительство РФ

До недавнего времени основные правила регистрации доменов формировались Координационным центром доменов .RU/.РФ (для доменов .ru и .рф) и Российский Научно-Исследовательский Институт Развития Общественных Сетей (РосНИИРОС) (для домена .su), а также отраслевыми соглашениями при участии регуляторов.

Повышение статуса норм: Перевод Правил регистрации доменных имён на уровень правительственных постановлений означает, что они станут неотъемлемой частью государственной политики в сфере информационного суверенитета.

Единые стандарты: Новая система опирается на федеральные законы № 560-ФЗ, № 569-ФЗ и № 210-ФЗ, а также постановления правительства РФ № 1119 и № 1120. Если закон определяет принципы, то постановления регламентируют конкретные правила, исполнение которых обеспечивают Координационный центр доменов .RU/.РФ, Российский НИИ развития общественных сетей (РосНИИРОС) и «Технический центр Интернет». Это позволит синхронизировать доменное регулирование с другими законами, сделав правоприменение более однозначным.

При этом сам Координационный центр подчёркивает, что ужесточение регулирования не отменяет важности горизонтальных связей в отрасли. Директор Координационного центра доменов .RU/.РФ Андрей Воробьев отмечает:

«Важно понимать, что жёсткое регулирование Интернета попросту невозможно по самой природе сети: даже в национальных доменах существует огромное количество горизонтальных связей, что, к примеру, помогает оперативно решать вопросы, связанные с кибербезопасностью, и быстро реагировать на инциденты».

Конец анонимности: идентификация администраторов только через ЕСИА

Одним из самых заметных изменений для рынка станет полный переход на идентификацию администраторов доменных имён через Единую систему идентификации и аутентификации (ЕСИА).

Если ранее для регистрации домена физическому лицу достаточно было предоставить паспортные данные, а юридическому — карточку предприятия, то теперь связка «домен — личность» будет проходить через портал госуслуг (ЕПГУ).

При этом меняется и жизненный цикл доменных имён. Регистрация переходит в статус бессрочной функции (понятие ежегодного продления уходит в прошлое), однако главным условием владения становится обязательная ежегодная идентификация администратора через ЕСИА (ЕПГУ).

Что это значит: Все ключевые операции – регистрация, смена администратора, передача домена между регистраторами и управление DNS – теперь жёстко привязаны к верификации и невозможны без подтвержденной учётной записи ЕСИА. Обязанность по аннулированию доменов при непрохождении идентификации возложена на регистраторов. Это существенно снизит использование поддельных паспортов, «дропов» и номинальных администраторов.

Зачем это нужно: Государство получает надёжный инструмент для быстрого выявления владельцев ресурсов, распространяющих противоправный контент, фишинговые сайты и мошеннические платформы. Для добросовестных пользователей это упростит процедуру восстановления доступа к домену в случае утери паролей или споров о праве на доменное имя.

Чтобы избежать коллапса, одномоментный ввод жёстких требований был заменён мягким переходным периодом: действие текущих соглашений с регистраторами продлено до 18 января 2027 года – это и есть финальный дедлайн для обязательной ЕСИА-идентификации.

Российские изменения вписываются в общемировой тренд на повышение прозрачности и достоверности данных об администраторах доменных имён. Аналогичные меры в последние годы активно внедряются и за рубежом. Так, в странах Евросоюза с октября 2024 года действует директива NIS2, обязывающая национальные регистратуры вести точные и полные базы данных WHOIS и обеспечивать верификацию сведений о владельцах доменов. В Германии оператор национального домена .de (DENIC) с 2023 года ужесточил требования к проверке контактных данных администраторов доменных имён, в Великобритании Nominet проводит обязательную верификацию для доменов .uk, а в Австралии с 2022 года регистрация в зоне .au

возможна только при подтверждённой связи заявителя со страной и прохождении процедуры идентификации. На глобальном уровне аналогичные требования к проверке данных администраторов закреплены в правилах ICANN для доменов верхнего уровня.

Таким образом, переход на идентификацию через ЕСИА не изолирует российский доменный рынок, а, напротив, синхронизирует его с международной практикой. Достоверные сведения об администраторах становятся стандартом ответственного управления интернет-пространством: это повышает доверие к национальным доменам со стороны пользователей, бизнеса и международных партнёров, а также создаёт равные условия для борьбы с киберпреступностью, фишингом и распространением противоправного контента вне зависимости от юрисдикции.

«В мире национальных доменов (ccTLD), таких как .ru и .рф, правила регистрации доменных имён и управление этими доменами являются исключительной прерогативой государства, с которым они ассоциированы. Соответственно, безопасность здесь обеспечивается государственными органами: правоохранительными структурами, национальными CERT (группами реагирования на компьютерные инциденты) и судами. При этом важную роль играет и экспертное сообщество. Ярким примером такого синергетического подхода в России является «Доменный патруль», где коммерческие компании, обладающие глубокой технической экспертизой, помогают оперативно выявлять и блокировать зловредные домены».

Защита госсектора: институт специальных регистраторов

Отдельный блок реформы касается обеспечения безопасности сайтов государственных и муниципальных организаций. Для работы с госсектором на координаторов возлагается обязанность по регистрации специальных доменных имён.

Кто такие координаторы: Это назначенные правительством РФ компании, которые получают исключительное право на регистрацию и обслуживание доменов для органов государственной власти, бюджетных учреждений и государственных корпораций. Сегодня такой статус имеют Координационный центр доменов .RU/.РФ для доменов .ru и .рф и Российский НИИ развития общественных сетей (РосНИИРОС) для домена .su.

Требования к регистраторам доменов для госорганов: Они обязаны соответствовать жёстким требованиям по финансовой устойчивости, технической защищённости и кадровому обеспечению.

Цель внедрения: Защита государственных сайтов от перехвата управления (угон доменов) и несанкционированного изменения DNS-записей. Координаторы станут «цифровым щитом» для госсектора, обеспечивая бесперебойную работу порталов госуслуг, министерств и ведомств.

Именно в работе с национальными доменами уже сегодня отрабатывается модель, которую Андрей Воробьев называет образцовой:

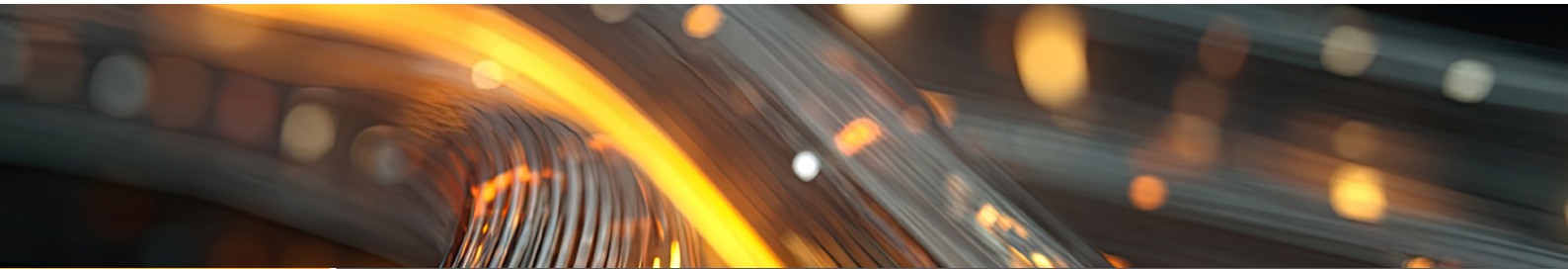
Исторический контекст: путь Координационного центра

Чтобы понять масштаб реформы, важно вспомнить, как формировалась сама доменная индустрия России. История национальных доменов неразрывно связана с эволюцией Координационного центра доменов .RU/.РФ, а до его появления – Координационной группы при РосНИИРОС – первой регистратуры домена .ru

Домен .ru был делегирован в апреле 1994 года, и первоначально его администрированием занимался РосНИИРОС. По мере роста Интернета и коммерциализации сети стало очевидно, что управление зоной требует отдельной профессиональной структуры. Так, в 2001 году был создан Координационный центр домена .RU – некоммерческая организация, объединяющая представителей интернет-сообщества, бизнеса и государства.

В 2010 году Россия стала одной из первых стран, получивших кириллический домен .рф, оператором которого также стал КЦ. С тех пор центр обеспечивает техническую стабильность обеих зон, развивает инфраструктуру, взаимодействует с регистраторами и участвует в международных дискуссиях об управлении Интернетом.

За четверть века КЦ прошёл путь от отраслевого саморегулирования к тесному партнёрству с государством. Именно этот опыт – баланс между технической гибкостью и государственной ответственностью – сегодня ложится в основу новой модели регулирования.



Гибридная модель как российский ответ на глобальные вызовы

Новые правила с 1 сентября 2026 года – это не просто ужесточение, а формирование принципиально новой архитектуры. На Глобальном цифровом форуме Андрей Воробьев выделил три мировые модели управления Интернетом: мультистейкхолдерную (с равноправным участием всех сторон), мультилатеральную (исключительно между государствами или наделёнными государством определёнными полномочиями специальными организациями) и гибридную, где государство обладает расширенными возможностями влияния, но сохраняет взаимодействие с отраслью.

Россия делает ставку именно на гибридную модель. И, как показывает опыт КЦ, она справляется с современными вызовами:

«Опыт доменной индустрии показывает, что гибридная модель уже работает на практике и может стать ориентиром для более широких решений на межгосударственном уровне».

Что в итоге?

Изменения с 1 сентября 2026 года знаменуют собой окончательный переход российской доменной индустрии в статус регулируемой государственной инфраструктуры.

Для государства это создание прозрачного, безопасного и управляемого контура национального Интернета. Для бизнеса и IT-отрасли – необходимость выстраивания новых бизнес-процессов с учётом жестких compliance-требований и работы в экосистеме ЕСИА. Для пользователей – повышение общего уровня доверия к сайтам в зонах .ru, .рф и .su, ведь за каждым доменом теперь будет стоять верифицированный и установленный законом владелец.

А для самой доменной индустрии – новый этап зрелости, когда 25-летний опыт Координационного центра становится фундаментом для построения суверенной, безопасной и технологически современной цифровой среды.



Об авторе:

Пыжова Ирина Борисовна – руководитель пресс-службы и главный редактор сайтов Координационного центра доменов .RU/.РФ, выпускающий редактор журнала «Интернет изнутри».

Исследование российского рынка фиксированной связи: от агрегированных оценок к анализу отдельных операторов и регионов

Алексей Леонтьев, Дмитрий Петров

Аннотация

В статье представлены результаты исследования российского рынка фиксированной связи на основе данных Роскомнадзора и ФНС о деятельности региональных операторов. Оценены объём и структура рынка, доли федеральных и региональных компаний, динамика их развития и финансовые показатели. Особое внимание уделено региональным различиям и роли небольших операторов в обеспечении инфраструктуры связи.

Ключевые слова:

Мобильная связь, фиксированная связь, рынок связи, Минцифры России

Введение

Необходимость более детального исследования российского рынка связи стала особенно очевидной в 2025 году. Несмотря на значительный объём отраслевой статистики, существующие оценки плохо отвечают на достаточно простой вопрос: как в действительности устроен рынок фиксированной связи и какую его часть занимают федеральные и региональные операторы.

В рамках настоящего исследования рынок связи рассматривается как совокупность двух крупных сегментов — мобильной и фиксированной связи. Мобильный сегмент представлен четырьмя федеральными операторами сотовой связи, тогда как фиксированный рынок значительно более фрагментирован и включает как федеральных, так и несколько тысяч региональных и локальных операторов.

При этом на протяжении многих лет воспроизводится приблизительное представление о соотношении федеральных и региональных операторов как 70 к 30, хотя происхождение этой пропорции не всегда очевидно, а сам рынок существенно изменился.

Различаются и оценки его общего объёма. По данным за 2024 год, TMT Consulting оценивает рынок примерно в 2,05 триллиона рублей, Минцифры — в 2,12 триллиона рублей, Росстат в части телекоммуникационных услуг — приблизительно в 2,31 триллиона рублей. Ещё заметнее различается внутренняя структура этих оценок: мобильный сегмент TMT Consulting оценивает примерно в 1,24 триллиона рублей, тогда как соответствующий показатель Минцифры составляет около 0,98 триллиона рублей.

Само наличие разных оценок не означает ошибочности какой-либо из них. Скорее речь идёт о различных способах наблюдения за одним рынком. Методики, в значительной степени опирающиеся на отчётность и опросы крупнейших компаний, хорошо отражают деятельность федеральных игроков, но потенциально хуже учитывают несколько тысяч небольших операторов. Росстат охватывает более широкий круг хозяйствующих субъектов, однако его данные сложнее использовать для разделения рынка по типам операторов и сегментам.

Это поставило перед исследованием основной методологический вопрос: возможно ли построить независимую модель рынка на уровне отдельных компаний и сопоставить полученный результат с существующими оценками?

Построение модели рынка

Исходной точкой стали открытые данные Роскомнадзора о лицензиях связи. Первоначальный массив включал порядка восьми тысяч лицензиатов, однако наличие лицензии само по себе не означает, что организация является оператором связи, работающим на конкурентном рынке. Среди лицензиатов присутствуют промышленные предприятия, университеты, вещательные организации, компании с собственными технологическими сетями и другие категории.

Поэтому лицензиаты первоначально были разделены примерно на 15 групп по типам лицензий и предполагаемому профилю деятельности. Около 4,5 тысячи компаний по набору лицензий потенциально могли быть отнесены к операторам передачи данных и доступа в Интернет, более 1,5 тысячи — преимущественно к сфере теле- и радиовещания.



Рис. 1. Операционная эффективность операторов связи.

Затем сведения Роскомнадзора были объединены с открытыми данными Федеральной налоговой службы. Для каждой компании сопоставлялись наименование и ИНН, место регистрации, виды и территория действия лицензий, выручка, финансовый результат и численность работников.

После объединения массивов проводились дополнительная фильтрация и ручная проверка. Исключались организации, для которых связь являлась вспомогательной деятельностью, а также дочерние общества федеральных групп, если их показатели уже учитывались в консолидированной отчётности. При существенной неопределённости применялся консервативный принцип: спорную компанию лучше исключить, чем искусственно увеличить рынок за счёт выручки, которую невозможно надёжно отнести к услугам связи.

Отдельным ограничением стали индивидуальные предприниматели: сопоставимые финансовые данные ФНС по ним отсутствуют, поэтому эта часть малого регионального рынка практически не учитывается. Следовательно, используемый подход скорее создаёт риск некоторого недоучёта малого сегмента, чем его завышения.

В рамках исследования под региональным оператором понимается компания, обладающая необходимыми лицензиями и фактически оказывающая услуги фиксированной связи физическим лицам, организациям или другим операторам, но имеющая существенно меньший географический масштаб деятельности по сравнению с федеральными операторами. К федеральным отнесены крупнейшие операторские группы, оказывающие аналогичные услуги практически во всех субъектах Российской Федерации. Таким образом, понятие «региональный оператор» определяется не размером выручки, а прежде всего масштабом географии деятельности: в эту группу входят и небольшие локальные компании, и крупные операторы, работающие в нескольких субъектах, но не имеющие общенационального охвата.

После классификации, объединения данных, фильтрации и ручной проверки была сформирована итоговая группа примерно из 4,7 тысячи региональных операторов связи. Полученный массив позволил анализировать не только совокупную выручку, но и финансовые показатели, численность работников, размер компаний и географию их деятельности.

Объём и структура рынка

После объединения данных региональных компаний с показателями крупнейших федеральных операторов общий объём российского рынка связи по построенной модели составил около 2,2 триллиона рублей. Эта величина оказалась достаточно близка к оценке Росстата. Само совпадение не доказывает абсолютную точность модели, однако является важной внешней проверкой порядка полученной величины.

Отдельно был оценён мобильный сегмент — приблизительно в 1,24 триллиона рублей, что практически совпадает с оценкой TMT Consulting. После его выделения объём рынка фиксированной связи в рамках модели составил около 960 миллиардов рублей.

Из примерно 960 миллиардов рублей фиксированного рынка около 560 миллиардов рублей, или 58%, приходится на федеральных операторов, а около 400 миллиардов рублей, или 42%, — на региональные компании. Полученное соотношение существенно отличается от традиционной пропорции 70/30.

Для оценки распределения рынка по клиентским сегментам дополнительно был проведён опрос 20 крупнейших региональных операторов, специализирующихся на работе в сегментах B2B (Business-to-Business, «бизнес для бизнеса») и B2O (Business-to-Operator, «бизнес для оператора») и непосредственно конкурирующих в них с федеральными компаниями. Полученные данные использовались при сопоставлении федерального и регионального сегментов по основным категориям клиентов. Поскольку эта часть исследования основана на выборочном обследовании, результаты приводятся в виде диапазонов, а не точечных значений.

Структура заметно различается по клиентским сегментам. В B2G (Business-to-Government, «бизнес для государства») доля федеральных компаний оценивается примерно в 80–85%, в B2O — 65–70%, в B2B — 60–70%. На массовом B2C-рынке (Business-to-Consumer, «бизнес для потребителя») картина обратная: совокупная доля региональных операторов превышает 55%.

Таким образом, федеральные компании особенно сильны в работе с государственными заказчиками, крупным бизнесом и другими операторами, тогда как региональные занимают наиболее значимые позиции на массовом рынке домашнего фиксированного доступа.

Масштаб и эффективность операторов

Данные на уровне отдельных компаний позволяют сравнить некоторые характеристики операторов разного размера. Одной из наиболее доступных метрик является отношение выручки к численности работников.

У крупнейших федеральных компаний выручка на одного сотрудника составляет приблизительно 5–7 миллионов рублей в год: около 6,7 миллиона рублей у «Ростелекома», 7,1 миллиона рублей у «ЭР-Телекома» и 5,4 миллиона рублей у ТТК.

У региональных операторов разброс значительно выше и зависит от модели бизнеса. В B2O показатель достигает примерно 22–25 миллионов рублей на сотрудника, в B2B — 10–13 миллионов рублей, в массовом B2C — приблизительно 2,5–7,5 миллиона рублей. Последний сегмент более трудоёмок из-за необходимости обслуживания большого количества физических подключений и разветвлённой сетевой инфраструктуры.

Если усреднить показатели всех региональных операторов с годовой выручкой от 20 миллионов рублей, выручка на одного работника составляет около 8 миллионов рублей в год, то есть как минимум сопоставима с показателями крупнейших федеральных компаний. Эта метрика не учитывает рентабельность, долговую нагрузку и капиталоёмкость бизнеса, однако результат не подтверждает предположение, что меньший масштаб регионального оператора автоматически означает меньшую производительность.

Рентабельность и финансовая устойчивость

Дополнительную картину даёт анализ финансовых результатов операторов различных размеров. Для неоднородного массива компаний в качестве основного показателя использовалась медианная рентабельность.

Рис. 2. Темпы роста операторов связи в 2024-2025 гг.



годовая выручка компаний (млн руб)	компаний в группе	выручка группы 2024 (млрд руб)	выручка группы 2025 (млрд руб)	прирост 2024-2025
< 1	610	0,1	2,7	-
1 - 5	600	1,7	2,7	-
5 - 10	505	3,8	4,5	**18,4%**
10 - 20	640	9,4	11,7	**24,5%**
20 - 50	940	31	35,8	**15,5%**
50 - 100	630	43,8	50,1	**14,4%**
100 - 150	270	34,5	37,6	**9%**
150 - 200	170	28,8	32,5	**12,8%**
200 - 500	225	65,1	71,3	**9,5%**
500 - 1 000	55	36,2	40,4	**11,6%**
1 000 - 5 000	45	88,6	94,2	**6,3%**
> 5 000	7	55	62,5	**13,6%**
все	**4697**	**396**	**446**	**12,6%**

У небольших операторов рентабельность и абсолютный размер прибыли закономерно ниже. В группе 50–100 миллионов рублей медианная рентабельность составляет около 7%, медианная прибыль — порядка 4,9 миллиона рублей. Наиболее заметное изменение происходит при переходе к диапазону 100–200 миллионов рублей: медианная рентабельность достигает около 10,5%, а медианная прибыль — порядка 15 миллионов рублей. После достижения этого масштаба относительная прибыльность стабилизируется: у операторов с выручкой 200–500 миллионов рублей она находится примерно на уровне 10%, а у более крупных компаний — около 9–10%.

Таким образом, наиболее уязвимыми оказываются самые небольшие компании: они располагают не только меньшей абсолютной прибылью, но и меньшим финансовым запасом. По мере роста до 100–200 миллионов рублей финансовая модель оператора становится заметно устойчивее, после чего относительная прибыльность меняется уже значительно меньше. При этом больший масштаб сам по себе не гарантирует более высокой чистой рентабельности.

Динамика регионального сегмента

Особенно важные результаты дало сопоставление одного и того же верифицированного массива компаний за 2024 и 2025 годы.

Совокупная выручка региональных операторов за 2025 год выросла примерно на 12,5%. Для сравнения, крупнейшие федеральные операторы фиксированной связи росли приблизительно на 6,5–7%. Таким образом, в рассматриваемом периоде региональный сегмент развивался почти вдвое быстрее федерального.

Это существенно меняет представление о региональных операторах как о статичной совокупности небольших компаний, занимающих постоянную нишу рядом с федеральными игроками. Перед нами самостоятельный растущий сегмент, экономический вес которого меняется.

Одним из возможных факторов такой динамики остаётся спрос на развитие фиксированной инфраструктуры, в том числе в индивидуальной жилой застройке, небольших населённых пунктах и на территориях, где строительство сети требует локального присутствия. Дополнительным фактором последних лет могли стать периодические ограничения мобильной передачи данных, повышающие значение фиксированного доступа как независимого канала связи. Однако независимо от объяснения причин сам наблюдаемый результат очевиден: в рассматриваемом периоде региональный сегмент рос существенно быстрее крупнейших федеральных операторов.

Поэтому традиционная пропорция 70/30 проблематична не только как оценка текущего состояния рынка. Если федеральный и региональный сегменты развиваются разными темпами, использование неизменного соотношения из года в год будет всё сильнее расходиться с фактической структурой отрасли.

Ещё нагляднее изменение структуры видно по переходу компаний между размерными группами. В 2024 году в группу региональных операторов с годовой выручкой 1–5 миллиардов рублей входили 43 компании, а в 2025 году — уже 56. Число операторов с выручкой 500 миллионов – 1 миллиард рублей выросло с 50 до 55, а в группе 200–500 миллионов рублей — с 225 до 285.

Следовательно, рост регионального сегмента сопровождается не только увеличением выручки существующих лидеров, но и расширением самой группы средних и крупных региональных операторов. Понятие «региональный оператор» объединяет принципиально разные компании — от небольших локальных сетей до предприятий с миллиардной выручкой, способных превращаться в крупных межрегиональных игроков.

Региональная структура рынка

Ещё одной важной возможностью модели стал анализ отдельных субъектов Российской Федерации.

Для распределения региональных операторов по субъектам использовались два последовательно применяемых критерия: территория действия лицензии и место нахождения головного офиса. Основным критерием являлась территория лицензии Роскомнадзора. Для значительной части небольших операторов, особенно компаний с годовой выручкой до 200 миллионов рублей, лицензия выдана на один субъект, а в ряде случаев территория деятельности ограничена отдельными районами. Такие компании непосредственно относились к соответствующему субъекту.

Если оператор имел лицензии на несколько регионов, его выручка относилась к субъекту по месту нахождения головного офиса. В исключительных случаях, когда компания была зарегистрирована в одном регионе, но лицензия предусматривала деятельность только в другом, приоритет отдавался территории действия лицензии.

Дополнительная проверка на основе опроса крупнейших региональных операторов показала, что такой способ даёт практически точное территориальное отнесение операторов с годовой выручкой до 100 миллионов рублей и корректно определяет основной регион деятельности абсолютного большинства компаний с выручкой до 200 миллионов рублей. Погрешность возрастает по мере увеличения масштаба бизнеса. Среди операторов с годовой выручкой от 500 миллионов рублей встречаются компании, фактически работающие сразу в нескольких субъектах; по результатам проверки такие случаи составляют менее 20% операторов этой размерной группы.

Поскольку открытая финансовая отчётность формируется по юридическому лицу в целом и не позволяет точно разделить выручку между территориями, вся выручка такого оператора относится к региону головного офиса.

Проведённая проверка позволяет оценить связанное с этим возможное отклонение для большинства субъектов в пределах примерно 10% объёма регионального рынка.

Существенным исключением является Республика Башкортостан. Зарегистрированный в республике «Уфанет» — крупнейший по выручке региональный оператор исследуемой группы — ведёт значительную деятельность и в соседних субъектах. Отнесение всей его выручки к Башкортостану существенно завышает оценку рынка республики; по экспертной оценке, величина завышения может достигать примерно трёх раз. Поэтому показатели Башкортостана требуют отдельной оговорки при межрегиональных сравнениях.

Региональный анализ показал чрезвычайно неравномерную структуру рынка. На Москву и Московскую область приходится почти 40% совокупной выручки региональных операторов России, на Санкт-Петербург и Ленинградскую область — еще около 10%. Таким образом, два крупнейших рынка формируют около половины выручки всего регионального сегмента.

Однако наиболее важный результат связан не с крупнейшими агломерациями. Во многих субъектах практически весь выявленный региональный рынок фиксированной связи сформирован компаниями с годовой выручкой до 200 миллионов рублей. В 35 субъектах Российской Федерации такие операторы обеспечивают более 70% либо практически весь региональный сегмент, а в 26 субъектах формируют практически весь выявленный региональный рынок.

Роль небольшой компании здесь принципиально отличается от роли аналогичного по размеру оператора в Москве или Санкт-Петербурге. В крупнейшей агломерации это один из многочисленных участников конкурентного рынка. В небольшом городе, районном центре или группе населённых пунктов компания аналогичного размера может обеспечивать значительную часть локальной инфраструктуры фиксированного доступа.

Подобная структура во многом объясняется экономикой строительства сети. Оператор может последовательно развиваться внутри своего города или района, тогда как выход на соседнюю территорию требует строительства транспортной инфраструктуры при относительно небольшом количестве новых абонентов. Для компании с выручкой в несколько десятков миллионов рублей такие инвестиции могут оказаться непропорционально велики. Поэтому в ряде субъектов формируется система множества небольших локальных сетей.

На противоположном полюсе находятся территории, где сформировались сильные региональные лидеры. В Москве, Санкт-Петербурге и ряде крупнейших регионов региональные компании способны конкурировать с федеральными операторами не только стоимостью, но и качеством услуг, клиентским сервисом, скоростью развития сети и дополнительными продуктами.

Таким образом, общероссийское соотношение 58/42 является лишь первым уровнем описания. За ним скрываются принципиально разные региональные модели. Один из важнейших результатов исследования состоит в том, что экономический размер оператора и его инфраструктурное значение не всегда совпадают: компания с выручкой менее 200 миллионов рублей практически незаметна в масштабах российского рынка, но может быть одним из

Рис. 3. Новый баланс рынка фиксированной связи.



ключевых поставщиков фиксированной связи для конкретной территории.

Региональная структура и темпы роста

Сопоставление структуры региональных рынков с изменением выручки за 2024–2025 годы выявило ещё одну закономерность. Территории, где уже сформировались относительно крупные региональные операторы и развитая конкурентная среда, демонстрируют достаточно высокие темпы роста.

В Санкт-Петербурге и Ленинградской области совокупная выручка региональных операторов увеличилась примерно на 20%, в Свердловской области — на 22%, в Москве и Московской области — приблизительно на 15%. Все три рынка росли быстрее среднего показателя по региональному сегменту — 12,5%. В Краснодарском крае прирост составил около 10%, а в ряде территорий с особенно высокой долей операторов минимального размера — порядка 6–7%.

Двухлетнего наблюдения недостаточно для доказательства причинной зависимости, поэтому это наблюдение носит разведочный характер. Тем не менее, результат позволяет выдвинуть гипотезу, что наличие сильных региональных игроков может быть одним из факторов развития локального рынка фиксированной связи.

Речь необязательно идёт о многомиллиардных компаниях. Существенную роль способны играть операторы с выручкой в несколько сотен миллионов рублей: у них появляется больший ресурс для строительства инфраструктуры, освоения соседних территорий и развития дополнительных услуг. Поэтому переход оператора в диапазон 200–500 миллионов рублей, а затем 500 миллионов – 1 миллиард рублей может иметь значение уже для всего регионального рынка.

Обсуждение и выводы

Полученные результаты показывают, что включение в анализ нескольких тысяч небольших и средних компаний меняет представление не только о размере, но и о механизмах развития российского рынка фиксированной связи.

Региональный сегмент представляет собой не периферийную часть федерального рынка, а самостоятельную и неоднородную среду — от небольших локальных сетей до формирующихся региональных лидеров. При этом его развитие может существенно отличаться от динамики крупнейших федеральных телекоммуникационных групп, бизнес которых сегодня включает не только классические услуги связи, но и IT-сервисы, ЦОДы, цифровые платформы и другие направления.

Особенно существенен вывод о соотношении экономического размера компании и её инфраструктурной роли. Небольшой оператор, практически незаметный в общероссийской статистике, может обеспечивать значительную часть фиксированной инфраструктуры отдельного города, района или группы населённых пунктов.

Полученные результаты позволяют дополнить традиционный взгляд на цифровое неравенство ещё одним измерением — структурой и экономической устойчивостью операторов, обеспечивающих доступ. В одних регионах существуют сильные компании, развитая конкуренция и возможности территориального расширения; в других инфраструктура распределена между небольшими локальными сетями с существенно меньшими возможностями для масштабирования.

Такой подход важен и для оценки последствий регулирования. Одинаковое фиксированное требование имеет принципиально разный экономический вес для компании с многомиллиардной выручкой и для оператора, годовая прибыль которого составляет несколько миллионов рублей. Если небольшой оператор одновременно играет значимую роль в инфраструктуре конкретной территории, последствия изменения условий его деятельности определяются уже не его долей в общероссийском рынке, а локальным значением.

Об авторах:

Леонтьев Алексей Владимирович, директор Ассоциации Телекоммуникационных Операторов

Петров Дмитрий Андреевич, генеральный директор ООО «Комфортел»

Интернет-наука и образование

Ведущий рубрики: Марат Биктимиров



Уважаемые читатели!

Мы продолжаем публиковать студенческие работы, выполняющиеся в Фонде развития сетевых технологий «ИнДата» в рамках совместных с вузами-партнёрами мероприятий, направленных на профессиональную подготовку будущих специалистов отрасли.

Напомним также, что все студенческие проекты осуществляются при поддержке ведущих сотрудников Фонда «ИнДата».

В представленной статье коллектив авторов из МГТУ им. Н.Э. Баумана предлагает практическую методику оценки качества радиоканала LoRa в помещениях со сложной топологией. На базе разработанного измерительного стенда исследователи провели серию экспериментов в главном корпусе университета, количественно оценив ключевой компромисс между скоростью передачи данных и надежностью их доставки.

Работа наглядно демонстрирует, что снижение скорости до минимальных значений позволяет успешно принимать пакеты даже при уровне сигнала ниже уровня шума. Полученные результаты станут ценной основой для проектирования стабильных и отказоустойчивых IoT-сетей в реальных условиях эксплуатации.

Методика измерений и оценка компромисса параметров передачи данных телеметрии IoT-устройств в помещениях по радиоканалу LoRa

Денис Кочетков, Богдан Бондарев, Андрей Никитин, Данила Посевин

Аннотация
В статье рассматриваются теоретические основы измерений и методология оценки качества передачи данных телеметрии по радиоканалу LoRa в помещении со сложной топологией. Основное внимание уделяется методологии проведения эксперимента на базе доступных электронных компонентов, обеспечивающих обмен информацией в туннелях и коридорах зданий. Предложена реализация измерительного стенда, описаны способы измерения дальности и достоверности передачи информации на основе существующих подходов. Приведён сравнительный анализ экспериментальных данных.

Ключевые слова:
LoRa, беспроводные компьютерные сети, измерения, оценка качества радиоканала, Интернет вещей

LoRa (англ. Long Range) — современная технология модуляции радиосигнала, которая позволяет передавать данные на значительные расстояния при мощности сигнала, значительно меньшей уровня шума, сохраняя при этом энергоэффективность. Выигрыш в мощности и, соответственно, в дальности радиосвязи достигается за счёт уменьшения пропускной способности радиоканала до нескольких кбит/с, что недостаточно для проектирования стабильной мультимедийной связи, но оказывается достаточной для передачи коротких текстовых сообщений или данных телеметрии. Поэтому LoRa-модуляция получила особую популярность для реализации устройств Интернета вещей (англ. Internet of Things, IoT), особенно для стационарных датчиков [5].

Применение LoRa-модуляции на практике связано с трудностями при определении возможности радиосвязи в более сложных условиях, чем на открытой местности: внутри зданий, на лесных территориях, в сельской и городской местности, а также в тоннелях [5]. Поэтому в качестве цели данной работы было выбрано исследование возможности применения LoRa-модуляции в сложных условиях радиосвязи для передачи различных видов информации. Для достижения поставленной цели необходимо выполнить общий обзор технологии LoRa-модуляции, исследовать существующие методы определения дальности радиопередачи в различных условиях, сконструировать экспериментальный стенд на основе выполненного теоретического анализа, определить план испытаний, провести эксперименты и проанализировать полученные результаты.

Основные параметры LoRa-модуляции

LoRa-модуляция является одной из частных реализаций модуляции Chirp Spread Spectrum (далее — CSS). CSS-модуляция использует M ортогональных «чирпов» — сигналов, частота которых меняется плавно по определённой форме [4]. Значение M определяет число уникальных сигналов и часто выражается по формуле M»\=» 2^SF, где SF (англ. Spreading Factor) — число бит на сигнал. Кроме того, CSS-модуляция определяется несущей частотой f_0 и шириной полосы радиопередачи BW (англ. Bandwidth). В LoRa реализуется CSS со строго линейными «чирпами»; в общем случае форма сигнала CSS не фиксирована.

Для передачи данных на практике поверх LoRa-модуляции используется помехоустойчивое кодирование, например, циклический код Хэмминга [2], поэтому во многих LoRa-ра-

диопередатчиках кроме уже описанных параметров модуляции также используется значение степени кодирования CR (англ. Code Rate). Использование помехоустойчивого кодирования значительно увеличивает расстояние передачи данных с помощью механизма восстановления потерь, а также позволяет уменьшить число ложных приёмов данных из-за радиошума, но линейно увеличивает количество передаваемых данных.

Основными критериями качества радиоканала являются доля ошибок в доставленных данных и скорость передачи данных. Для LoRa-радиоканала доля ошибок может быть описана в терминах вероятности битовой ошибки и вероятности пакетной ошибки.

Вероятность битовой ошибки описывает вероятность инвертирования бита в принятом сообщении. При вероятности битовой ошибки, равной 0, гарантируется, что сообщение дойдёт без изменений; при вероятности 0,5 нельзя определить, какое сообщение было изначально. Для определения доли битовой ошибки существует большое количество моделей, но в значительной степени эти модели опираются на отношение сигнал/шум на приёмнике и на характер шума в среде. Однако битовая ошибка обладает малой наглядностью для реального LoRa-радиопередатчика, так как реальные модули используют помехоустойчивое кодирование, а также систему отбрасывания пакетов данных при невозможности восстановления исходного пакета.

Более наглядной является вероятность пакетной ошибки. Вероятность пакетной ошибки характеризует долю пакетов, потерянных при передаче данных из-за высокой степени ошибок. Вероятность пакетной ошибки определяется по величине битовой ошибки и зависит от режима кодирования [1]. В силу невозможности непосредственного измерения битовой ошибки на реальном устройстве в работе будет рассмотрена величина пакетной ошибки.

Скорость передачи данных ADR либо определяется производителем модуля и указывается в документации, либо рассчитывается через параметры передачи данных:

$$ADR = \frac{CR \cdot BW \cdot SF}{2^{SF}}$$

Описание идеи измерения потерь

Задача эксперимента — количественно оценить надёжность канала связи LoRa в условиях закрытого помещения. Измеряются две величины: доля пакетов, не дошедших до приёмника (вероятность пакетной ошибки), и мощность, с которой приняты дошедшие пакеты (уровень сигнала). Стенд состоит из двух одинаковых узлов: микроконтроллер ESP8266 и радиомодуль E220-900T22D [3]. Модуляцию, помехоустойчивое кодирование и контроль целостности данных в эфире реализует радиомодуль; микроконтроллер отвечает за его настройку и обмен данными по последовательному интерфейсу (UART).

Описание тестового кадра

Тестовым кадром в настоящей работе называется служебное сообщение фиксированной длины (64 байта), которое передатчик формирует и отправляет с периодом 1 с для оценки качества канала. Модуль разделяет на пакеты данных сообщения длиннее 200 байт, поэтому кадр всегда передаётся одним пакетом и его потеря тождественна потере пакета. Длина всех кадров выбрана одинаковой, поскольку она определяет время нахождения пакета в эфире и вероятность его искажения. Содержимое кадра не влияет на результаты измерений: байты кадра передаются в эфир последовательно. Структура кадра приведена в таблице 1.

Таблица 1. Структура тестового кадра

Поле	Байт	Назначение
magic	2	Сигнатура 0x544C («LT»)
version	1	Версия формата кадра
config_hash	1	Хеш настроек (должен совпадать на обеих платах)
boot_id	2	Случайный идентификатор включения передатчика
air_rate	2	Скорость передачи в эфире, бит/с
seq	4	Сквозной номер кадра с момента включения
block	4	Номер блока
pos	2	Номер слота внутри блока (0…29)
send_offset_ms	4	Момент отправки от начала блока, мс
prev_tx_busy_ms	2	Служебное: время передачи кадра в модуль, мс
payload	38	Заполнитель: фрагмент строки, состоящей из последовательности чисел вида «012345678…997998999» без разделителей
crc	2	Контрольная сумма CRC-16/CCITT
Итого	**64**	

Временная структура передачи кадров

Передача кадров осуществляется по фиксированному расписанию, отсчёт которого ведётся от момента включения передатчика. Время передачи разделено на последовательные блоки по 32 секунды: 2 секунды паузы, во время

которой приёмник измеряет фоновый шум, и 30 слотов по 1 секунде, в каждом — ровно один кадр. Скорость передачи в течение опыта постоянна (допустимы значения от 2400 до 62 500 бит/с). Мощность передатчика во всех опытах постоянна — 22 дБм, частота — 850,125 МГц. Главное свойство расписания: приёмник заранее знает, сколько кадров должно прийти, и учитывает потери, даже когда не пришло ничего.

Синхронизация приёмника и проверка кадров

Приёмнику заранее неизвестен момент включения передатчика, однако он восстанавливается по первому принятому кадру: по номеру блока, смещению момента отправки и моменту приёма t_пр приёмник вычисляет начало расписания передатчика по своим часам:

$$t_0 = t_{\text{пр}} - (n \cdot T_{\text{бл}} + \Delta t_{\text{отп}}), \qquad (1)$$

где n — номер блока (поле block); $T_{бл}$ = 32 000 мс — длительность блока; $\Delta t_{отп}$ — смещение момента отправки кадра относительно начала блока, мс (поле send_offset_ms).

Далее оценка t_0 уточняется по каждому вновь принятому кадру. После паузы длительностью более 15 мс принятый пакет передаётся на микроконтроллер единой посылкой в 65 байт — кадр и байт уровня сигнала. Затем кадр проходит проверки:

- сигнатура и CRC-16 — ошибка означает сбой на проводах между модулем и платой (испорченные в эфире пакеты отбрасывает сам LoRa); такие случаи считаются отдельно (bad);
- версия и хеш настроек — при несовпадении кадр игнорируется;
- boot_id — если он изменился, передатчик перезагружался, и приёмник синхронизируется заново.

Методика расчёта потерь

Для каждого блока приёмник ведёт битовую карту из 30 ячеек — по одной на слот — и отмечает принятые кадры по полю pos, не учитывая повторы; потери соответствуют незаполненным ячейкам, и по завершении блока их доля равна

$$P_{\text{пот}} = \frac{N_{\text{ож}} - N_{\text{пр}}}{N_{\text{ож}}} \cdot 100\%, \qquad (2)$$

где $N_{ож}$ — число ожидаемых кадров (30 для полного блока), $N_{пр}$ — число уникальных принятых кадров. Дополнительно фиксируется самая длинная серия подряд потерянных кадров (max_burst).

Для исключения ложных потерь в статистику не включаются блоки, приём которых начат с середины, а завершённый блок засчитывается лишь после повторного приёма того же передатчика (с тем же boot_id): так, пустой блок считается 100% потерь, только если передатчик заведомо работал. При отсутствии кадров дольше трёх блоков синхронизация сбрасывается. Итоговая доля потерь для каждой скорости передачи вычисляется по совокупности полных блоков.

Метод измерения мощности сигнала

Мощность принятого сигнала оценивается по показателю RSSI (англ. Received Signal Strength Indicator). Модуль E220 вычисляет его самостоятельно и добавляет одним байтом к каждому принятому пакету; в децибел-милливатты значение пересчитывается по формуле

$$RSSI = v - 256, \text{ дБм}, \qquad (3)$$

где v — значение байта уровня сигнала (от 0 до 255), передаваемого модулем вместе с кадром.

Помимо сигнала, приёмник измеряет фоновый шум — мощность, регистрируемую на входе приёмника в отсутствие полезной передачи. Для этого он запрашивает у модуля значение регистра шума в моменты, заведомо свободные от передачи: через 20 мс после приёма кадра и в начале паузы каждого блока. Разность

$$\text{Запас} = RSSI - \text{Шум}, \text{ дБ} \qquad (4)$$

показывает, насколько сигнал превышает фон, — это грубая оценка отношения сигнал/шум. Благодаря использованию модуляции с расширением спектра технология LoRa обеспечивает приём пакетов при уровне сигнала ниже уровня шума.

Методика измерений

С использованием описанного программно-аппаратного комплекса 23 сентября 2026 года с 13:20 до 16:20 были проведены испытания в главном корпусе МГТУ им. Н.Э. Баумана. Передатчик был размещён в одной из аудиторий южного крыла университета. Такое расположение позволило оценить ослабление сигнала на максимальном расстоянии в пределах корпуса — между его противоположными крыльями, — а также передачу на большое расстояние по открытому пространству между окнами закруглённых крыльев здания («циркулей»).

В ходе испытаний передатчик оставался неподвижным и автоматически передавал пакеты данных, а приёмник был подключён к ноутбуку, на котором велась непрерывная запись принятых пакетов с точными отметками времени.

Для каждой из трёх выбранных скоростей передачи был проведён отдельный эксперимент. В ходе каждого эксперимента приёмник перемещался по маршруту, охва-

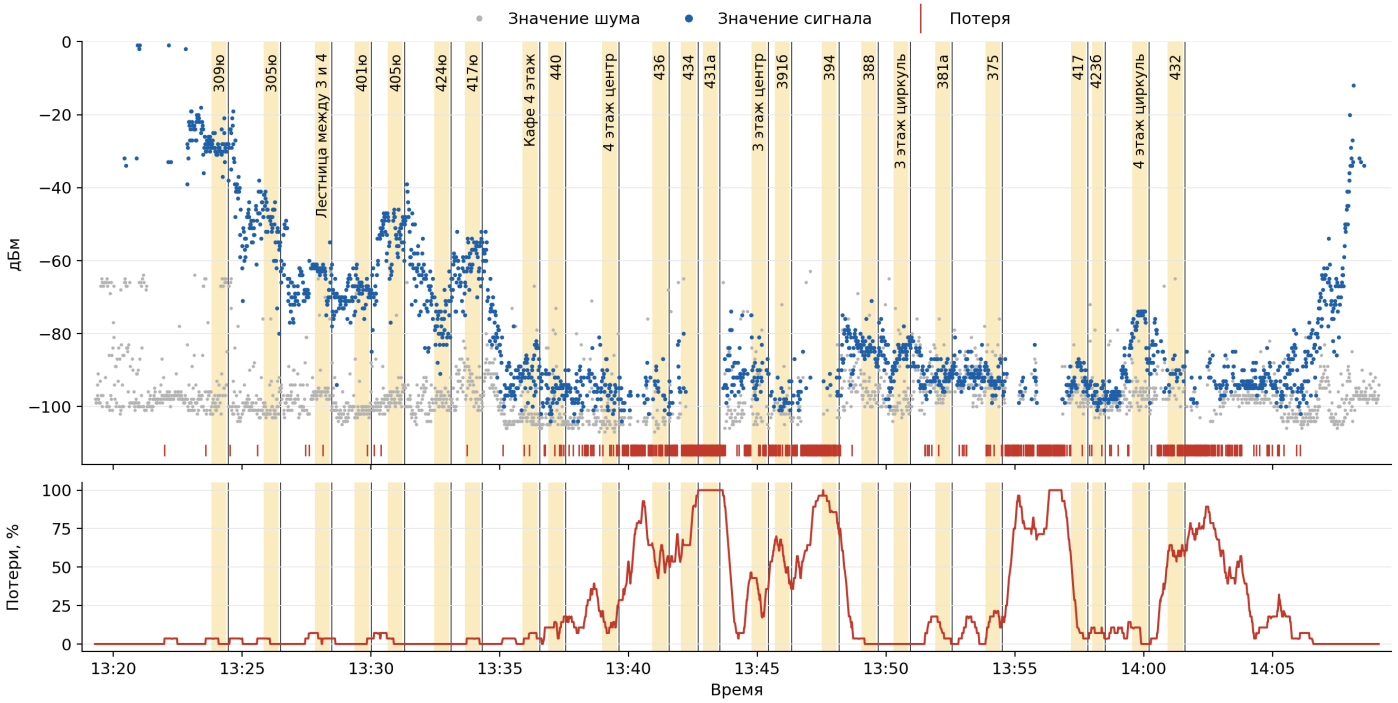


Рис. 1. Уровни сигнала и шума, потери пакетов и доля потерь во времени (эксперимент на скорости 2,4 кбит/с); закрашенными полосами отмечены точки измерений.

тывающему бо льшую часть помещений университета, в которых принимался сигнал. Пример данных, записанных в ходе эксперимента на скорости 2,4 кбит/с, приведён на рисунке 1.

Для привязки записанных данных к местоположению приёмника параллельно вёлся протокол испытаний, в который вручную заносились приближённые результаты измерений с привязкой к аудиториям и другим ориентирам в здании университета. В точках, где уровень сигнала, уровень шума или доля доставленных пакетов заметно отличались от значений в предыдущей точке, приёмник фиксировался на некоторое время, а в протокол заносились ориентир (аудитория), точное время и оценочные значения показателей. По этим записям из общего массива выделялись данные для точек с известным местоположением. В точках, где сигнал не принимался вовсе, опыты, как правило, не проводились; этим объясняется меньшее количество опытов на более высоких скоростях передачи. В качестве основных точек измерений были выбраны аудитории центральной части, южного и северного крыльев и центральной «башни» университета (последнее только для скорости 2,4 кбит/с).

Диаграммы визуального распределения качества сигнала и доли потерь для всех скоростей представлены на рисунках 2–4.

По полученным результатам наблюдается снижение качества сигнала с увеличением расстояния до передатчика и количества стен на пути распространения сигнала, причём на более высоких скоростях передачи это снижение происходит быстрее. На минимальной скорости пакеты принимались практически во всех частях университета, тогда как на максимальной скорости потери возникали уже при выходе из прямой видимости или при переходе на другой этаж. Существенное влияние количества стен между передатчиком и приёмником подтверждается тем, что сигнал стабильно принимался в северном «циркуле», связь с которым осуществляется через открытое пространство, но не во всех точках центральной части здания, хотя она расположена ближе к передатчику. Кроме того, с увеличением высоты расположения приёмника в башне качество сигнала улучшалось: при переходе с 5-го на 12-й этаж медианный уровень сигнала увеличился на 20 дБ.

Зависимость доли доставленных пакетов от расстояния до передатчика и от медианного уровня сигнала приведена на рисунке 5. При уровне сигнала выше −85 дБм доля доставленных пакетов составляет в среднем 94,5%, тогда как при более слабом сигнале она резко снижается (рисунок 5, б): медианная доля доставленных пакетов для скоростей 19,2 и 62,5 кбит/с составляет 24–25%, для скорости 2,4 кбит/с — 82%. Аналогичная закономерность наблюдается и для расстояния (рисунок 5, а): на расстояниях более 85 м стабильный приём обеспечивается только на скорости 2,4 кбит/с, для которой медианная доля доставленных пакетов составляет 88% против 24–25% для остальных скоростей.

Аппроксимация зависимости медианного уровня сигнала от расстояния (рисунок 6) логарифмической моделью даёт убывание, пропорциональное третьей степени расстояния, а не второй (последнее присуще свободному пространству), что объясняется дополнительным затуханием в стенах и на поворотах коридоров здания.

Преимущество минимальной скорости при передаче на большие расстояния проявляется и в статистике приёма пакетов с низким уровнем сигнала (рисунок 7). На ско-

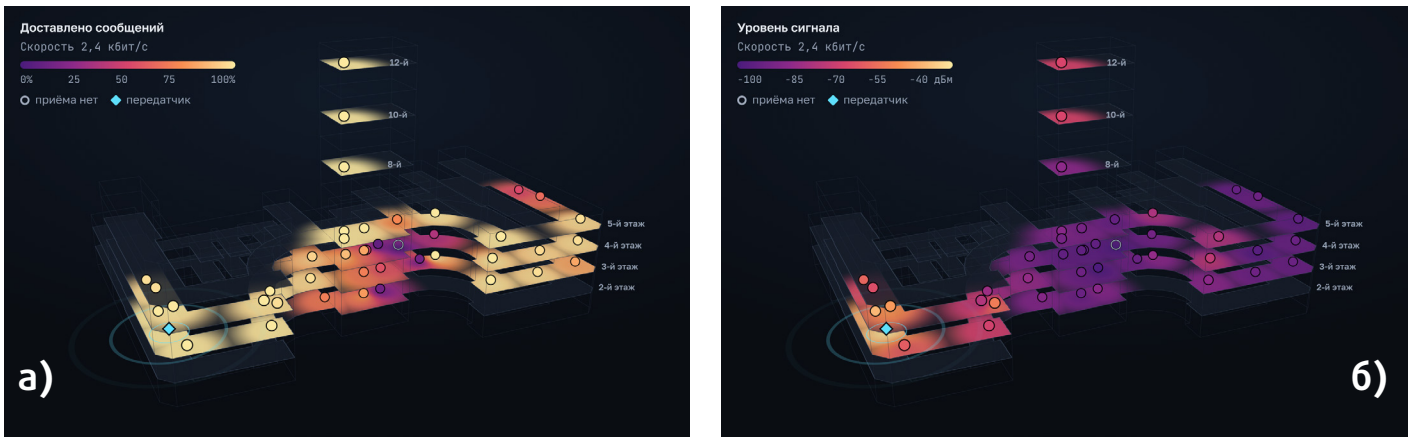


Рис. 2. Распределение показателей приёма по точкам университета при скорости 2,4 кбит/с: а) доля доставленных пакетов; б) уровень сигнала.

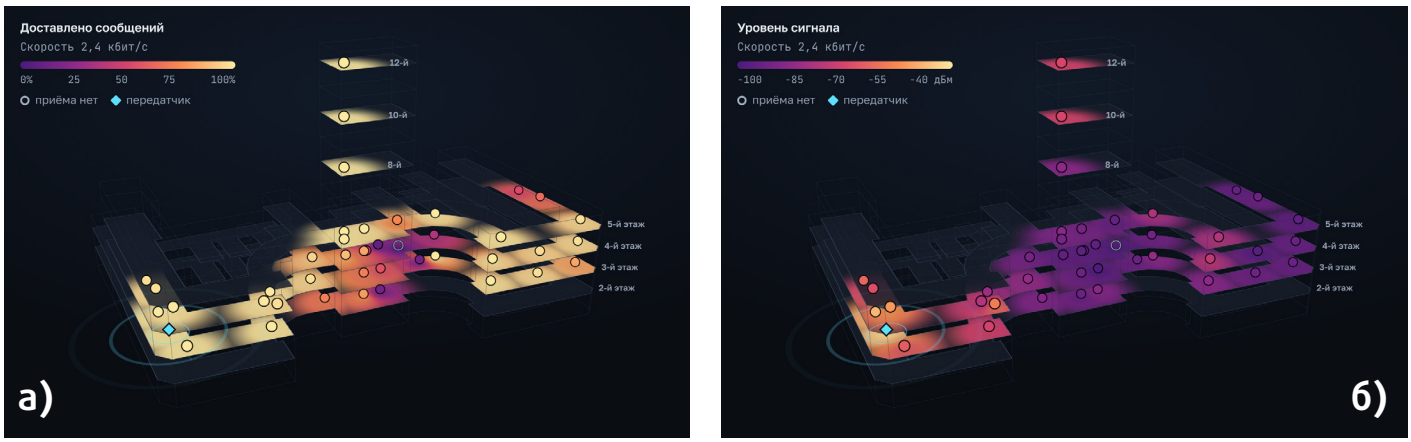


Рис. 3. Распределение показателей приёма по точкам университета при скорости 19,2 кбит/с: а) доля доставленных пакетов; б) уровень сигнала.

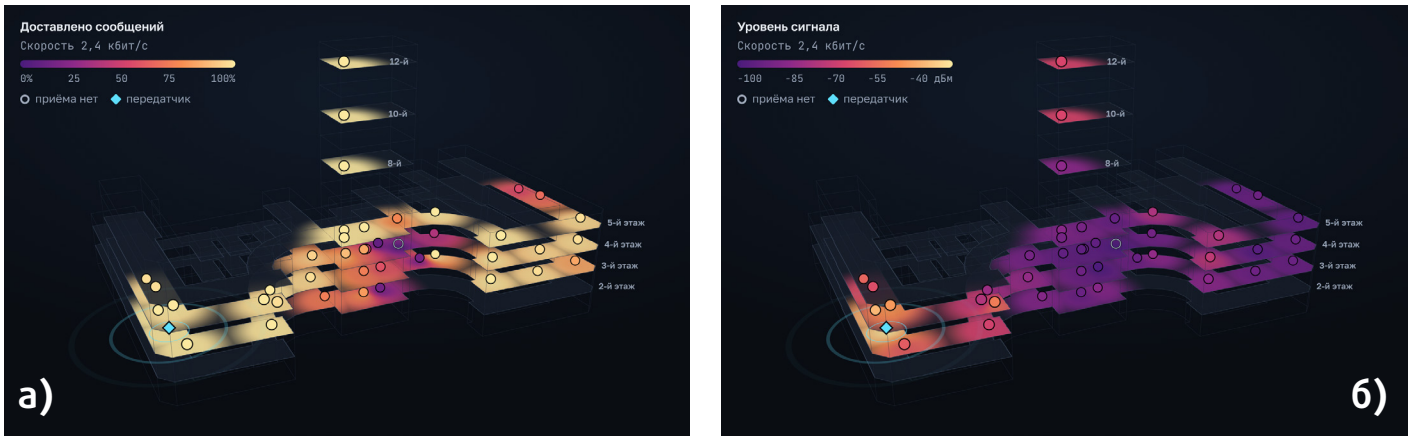


Рис. 4. Распределение показателей приёма по точкам университета при скорости 62,5 кбит/с: а) доля доставленных пакетов; б) уровень сигнала.

рости 2,4 кбит/с приёмник чаще принимал такие пакеты (рисунок 7, а): минимальный уровень сигнала принятого пакета составил −104 дБм против −102 дБм для скорости 19,2 кбит/с и −98 дБм для скорости 62,5 кбит/с. Кроме того, на этой скорости чаще принимались пакеты с уровнем сигнала ниже уровня шума (рисунок 7, б): 8,5% всех принятых пакетов против 2,3% для скорости 19,2 кбит/с и 1,9% для скорости 62,5 кбит/с.

Заключение

В ходе работы были проанализированы методы и параметры оценки качества радиоканала и существующие модели выделенных параметров радиоканала LoRa. Был спроектирован и разработан испытательный стенд для проверки данных параметров на практике.

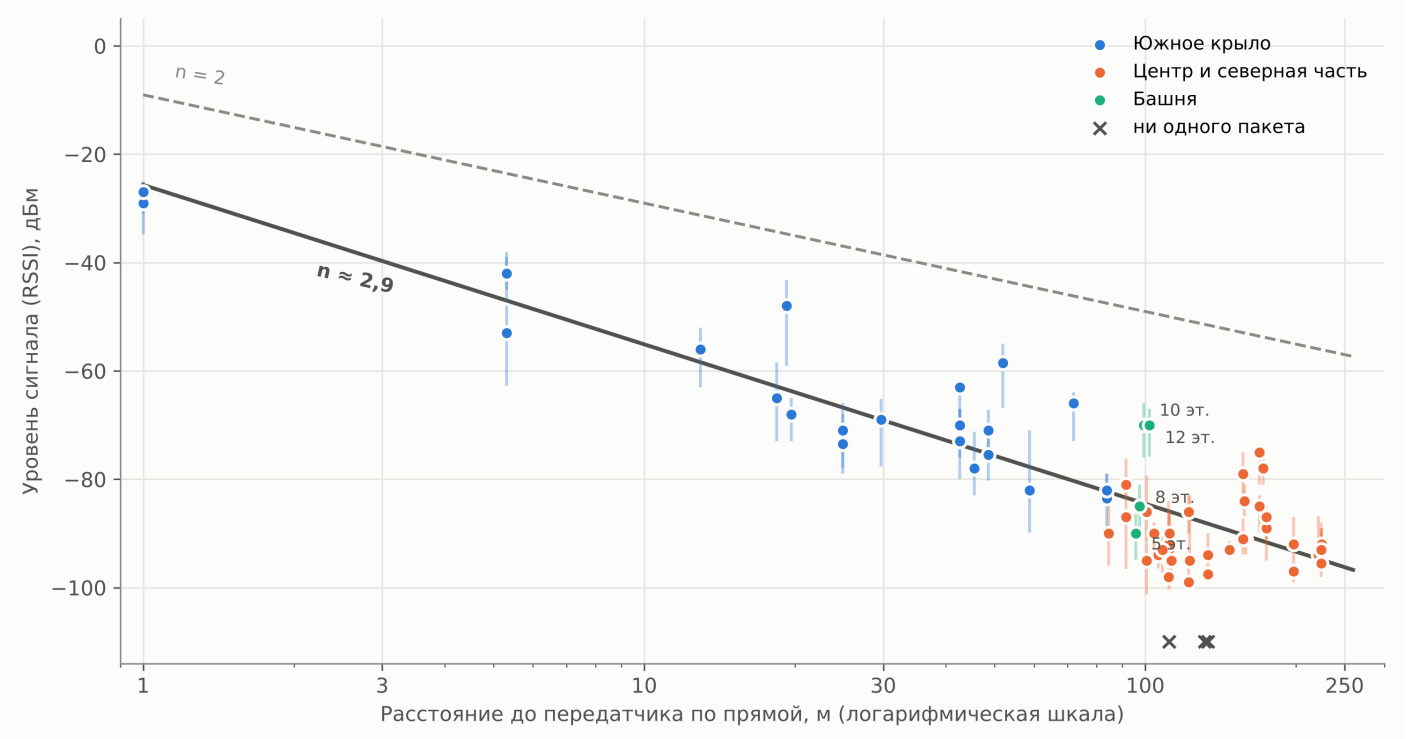


Рис. 5. Доля доставленных пакетов в зависимости: а) от расстояния до передатчика; б) от медианного уровня сигнала принятых пакетов.

Была проведена серия экспериментов для оценки качества радиоканала внутри зданий на примере главного корпуса МГТУ им. Н.Э. Баумана. По результатам проведения испытаний была доказана возможность использования LoRa-радиоканалов для передачи данных от автономных IoT-датчиков на примере главного корпуса МГТУ им. Н.Э. Баумана. Но были доказаны значительные ограничения модуляции LoRa по скорости передачи данных. Экспериментально было показано, что при передаче данных со скоростью, превышающей минимальную для модуля E220-900T22D, потери сигнала фиксировались при нахождении любой преграды на прямой радиоканала.

В дальнейших планах рассматривается оценка возможности передачи по LoRa сжатых изображений и звуковых сигналов при автономном питании.

Рис. 6. Зависимость медианного уровня сигнала от расстояния до передатчика (вертикальные отрезки — разброс значений между 10-м и 90-м перцентилями).



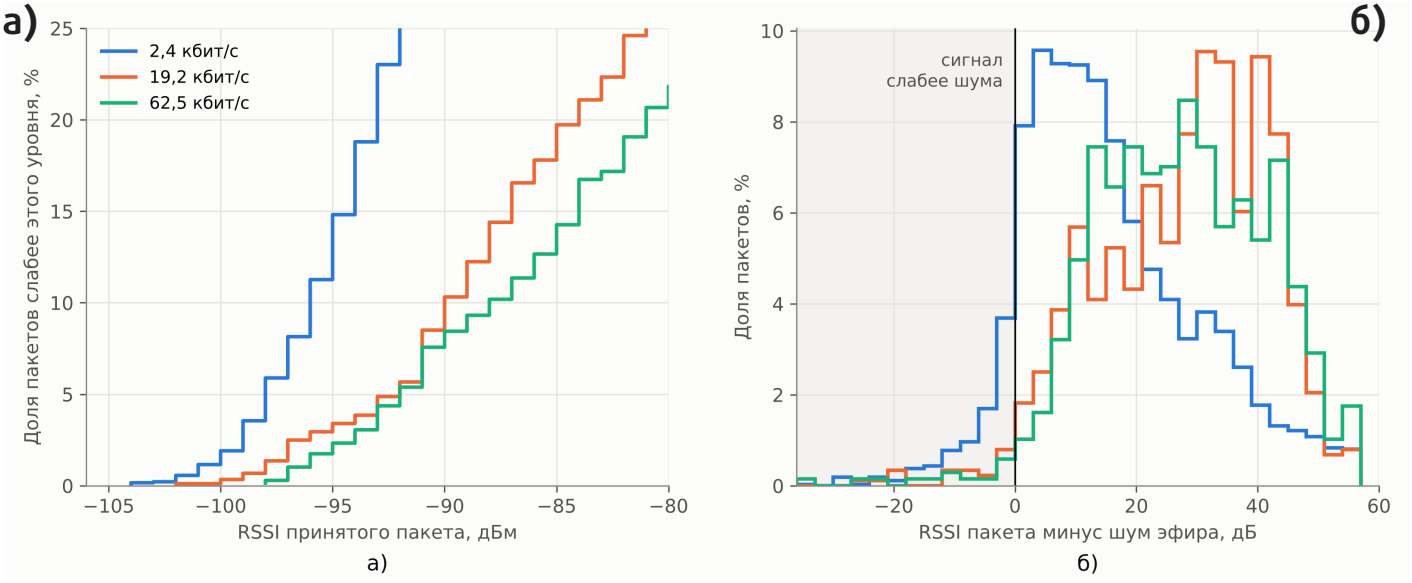


Рис. 7. Статистика приёма пакетов с низким уровнем сигнала: а) интегральное распределение уровня сигнала принятых пакетов; б) распределение превышения уровня сигнала над уровнем шума.

Список литературы:

[1] Afisiadis, O. Coded LoRa frame error rate analysis [Текст] / O. Afisiadis, A. Burg, A. Balatsoukas-Stimming // ICC 2020 – 2020 IEEE International Conference on Communications (ICC). – Piscataway: IEEE, 2020.

[2] Baruffa, G. Error probability performance of chirp modulation in uncoded and coded LoRa systems [Текст] / G. Baruffa [et al.] // Digital Signal Processing. – 2020. – Vol. 106. – Art. 102828.

[3] E220-900T22D User Manual: 868/915MHz 22dBm LoRa Wireless Module. – Version 1.0. – Chengdu: Chengdu Ebyte Electronic Technology Co., Ltd., 2020. – 22 p. – URL: https://www.cdebyte.com/products/E220-900T22D (дата обращения: 01.10.2026) – Текст: электронный.

[4] Maleki, A. A tutorial on chirp spread spectrum modulation for LoRaWAN: Basics and key advances [Текст] / A. Maleki, H. H. Nguyen, E. Bedeer, R. Barton // IEEE Open Journal of the Communications Society. – 2024. – Vol. 5. – P. 4578–4612.

[5] Pramanik, J. A comprehensive systematic review of progressive applications of LoRa and LoRaWAN networks in the Internet of Things [Текст] / J. Pramanik [et al.] // International Journal of Internet Manufacturing and Services. – 2025. – Vol. 11, no. 1. – P. 1–22.

Об авторах:

Кочетков Денис Игоревич, бакалавр, 4074-5575, инженер, НУК «Информатика и системы управления», РУНЦ «Безопасность», лаборатория «Мультиспектральных информационных систем», МГТУ им. Н.Э. Баумана.

Бондарев Богдан Андреевич, студент учебной группы ИУ9-51Б, МГТУ им. Н.Э. Баумана.

Никитин Андрей Владимирович, студент учебной группы ИУ9-51Б, МГТУ им. Н.Э. Баумана.

Посевин Данила Павлович, к. т. н., доцент кафедры ИУ-9, МГТУ им. Н.Э. Баумана.



Понятие и специфика исследований измерений Интернета

Мадина Касенова

Аннотация
Автор рассматривает специфику ландшафта интернет-измерений через призму многомерности Интернета и его эволюционного развития. С учётом масштабного и разнообразного состава вовлечённых в интернет-измерения субъектов в статье отмечены складывающиеся международные организационные механизмы, а также в общем плане рассмотрен ряд документов, предметно затрагивающих интернет-измерения.

Ключевык слова:
измерения Интернета, RFC 1262, стейкхолдеры, эмерджентность, IETF, Конференция по измерениям в Интернете, Internet-Drafts

Исследования, предметно относящиеся к проблематике измерений Интернета (Internet Measurement), иначе – «измерения в Интернете», «измерение параметров Интернета», «мероприятия по измерению Интернета» и т.д. (далее – «интернет-измерения»), – проводятся несколько десятилетий. Спектр исследований интернет-измерений многообразен и контекстно затрагивает как теоретические, так и практические аспекты, анализируя среди прочего технологические параметры функционирования инфраструктуры Интернета, включая её фундаментальные принципы и свойства; углубляют понимание перспектив дальнейшего развития Интернета как глобальной «сети сетей» [1]; рассматривают вопросы планирования будущего интернет-технологий с учётом масштабов их роста, сложности и роли в современных реалиях цифровой трансформации и т.д. Едва ли можно подвергнуть сомнению, что сам Интернет как таковой, включая эволюционное развитие форматов его использования, по сути, объективно и всецело обусловливают интернет-измерения (их формат, контекст, параметры, средства, методы и проч.).

Здесь целесообразно обратить внимание на 1983 год, т.е. на тот период, с которого исторически принято отсчиты-

вать появление Интернета, функционирующего в качестве открытой и доступной всем технологически-горизонтальной «сети сетей», универсальность которой изначально зиждилась на трансграничном децентрализованном администрировании её использования (Internet Governance) с опорой на «саморегулирование» (Self-Regulation). Между тем, ретроспективный взгляд позволяет обозначить 90-е годы XX века – т.н. эпохи интернет-классицизма – как временной срок начала проведения интернет-измерений, и аргументировать сказанное можно соображениями следующего порядка.

Отметим, что именно к 90-м годам минувшего века Интернет превратился в важный инфраструктурный ресурс, а часть его компонентов и технологических элементов получила применение в экспериментах, обеспечивающих и поддерживающих технологии иных сетевых инфраструктур. В то же время интернет-технологии стали использоваться в деятельности широкого круга осуществляющих интернет-измерения стейкхолдеров, охватывая в т.ч. масштабное число технических специалистов, операторов-компьютерщиков, инженеров, представителей бизнес-кругов, академического и гражданского сообщества и т.д. Помимо этого, в рассматриваемый временной период вниманию широкого интернет-сообщества были адресованы первые документы, касающиеся проведения интернет-измерений, и в их числе: «Этика и Интернет» (Ethics and the Internet, 1987) [2], «Руководство относительно мероприятий по измерению Интернета» (Guidelines for Internet Measurement Activities, 1991) [3]. Критическая значимость упоминаемых документов во многом вытекает из факта их закрепления в статусе документов RFC (Request for Comments) [4]. Так, первый из названных документов был выпущен в формате документа RFC 1087, а второй – RFC 1262. Отрицать решающую регуляторную авторитетность положений, закреплённых документами в статусе RFC для обеспечения функционирования технологической инфраструктуры Интернета, невозможно, поэтому также следует отметить немаловажное обстоятельство «отсутствия сроков действия» названных документов RFC.

Вышеизложенное позволяет утверждать, что к настоящему моменту интернет-измерения преодолели de facto 35-летний рубеж, вместе с тем, за такой относительно длительный срок ландшафт исследований интернет-измерений устойчиво продолжает сохранять свою специфику. Такая специфика, наряду с прочим, неразрывно связана с двумя объективно существующими факторами, которые дополняют друг друга, взаимосвязаны, взаимообусловлены и, по сути, равным образом определяют как содержание, так и параметры проводимых интернет-измерений.

Во-первых, уместно повторить, что сам Интернет per se объективно обусловливает интернет-измерения, а имманентные свойства его горизонтально-сетевой технологической инфраструктуры и эволюционное развитие форматов использования Интернета также существенным образом определяют специфику проведения соответствующих исследований. Примечательно, что в целом ряде специализированных исследований обращалось внимание на решающее свойство горизонтально-сетевой инфраструктуры Интернета, выражающееся в «эмерджентности» (или «эмергентности», от англ. слова – emergent), которое означает наличие у системы качества, не присущего составляющим её компонентам по отдельности, а также несводимость качеств системы к сумме свойств её компонентов [5]. Необходимость учёта качества эмерджентности инфраструктуры Интернета, с одной стороны, выступает основой проведения измерений любого технологического компонента Интернета, однако, с другой стороны, эмерджентность усложняет получение актуальных и достоверных данных о сетевой инфраструктурной функциональности в глобальном масштабе и, среди прочего, затрудняет репрезентативность понимания показателей производительности Интернета в целом, а также оценки его сетевых настроек, конфигураций и так далее [6].

Нельзя обойти вниманием также то, что специфические особенности ландшафта интернет-измерений сопряжены с эволюционными этапами развития использования Интернета. В этом контексте можно, в частности, обратиться к авторитетному исследованию группы специалистов «Общества Интернета» (ISOC), представивших обобщённые модели-этапы хронологически последовательного развития Интернета: так называемая классическая эпоха; время развития периферийной инфраструктуры по региональному принципу («начало освоения кеш-памяти»); максимальное приближение такой инфраструктуры к пользователю («гипермасшабирование»); переход на оказание услуг по модели телекоммуникационных операторов («расслоение Интернета») [7]. Этапы эволюционного развития Интернета соответственно определяют ландшафт интернет-измерений, когда тематика и направленность исследований не только диверсифицируется, но и выражается в усложнении применяемых средств и экспериментальных методов и т.д. Например, по мере того как Интернет превращался в объект критически важной инфраструктуры, насущной необходимостью становилась потребность в изучении актуальных угроз кибербезопасности, оценке степени внедрения соответствующих средств защиты и анализе эффективности мер по снижению рисков. С использованием разнообразных методов измерения параметров Интернета в контексте кибербезопасности — от угроз в конкретных прикладных областях до анализа самих угроз — исследования измерений параметров Интернета, связанных с кибербезопасностью, предложено классифицировать через призму двух измерений: (i) охватывая различные вертикальные уровни (и компоненты) экосистемы Интернета; (ii) противопоставляя нормальное внутреннее функционирование системы и негативное воздействие внешних субъектов как в цифровом, так и в физическом пространстве [8].

Во-вторых, объективно существующим фактором специфики ландшафта интернет-измерений является то, что его контуры неизменно формируются разнообразным и масштабным кругом стейкхолдеров (представители технического и инженерного сообщества, бизнес-сферы, академических кругов, гражданского общества), которые осуществляют свою деятельность на принципах «саморегулирования» и децентрализованного управления использованием Интернета. При такой множественности и разнообразии стейкхолдеров важно не упустить из виду принципиально важный момент, связанный с правовым

статусом вовлечённых субъектов и их принадлежностью к различным правовым системам. Конкретно речь идёт как о субъектах системы национального права, так и о субъектах системы международного права. Сказанное можно подтвердить некоторыми примерами.

Так, многообразные сферы широкого круга исследовательских тем интернет-измерений с охватом теоретических и практических аспектов рассматриваются в рамках Инженерного совета Интернета (Internet Engineering Task Force, IETF), а конкретные исследования осуществляются проектными исследовательскими лабораториями и создаваемыми рабочими группами (Internet Measurement Research Group, IMRG), которые, в т.ч. выступают площадками для: (i) обсуждения вопросов измерения интернет-параметров в контексте содействия координации различных исследовательских проектов; (ii) оценки и разработки новых методов и средств интернет-измерений; (iii) расширения взаимодействия между операторами, разработчиками инструментов и методов измерения и исследователями, анализирующими и моделирующими динамику Интернета; (iv) анализа всех видов измерения сетевых параметров (активные методы, пассивный мониторинг, зондирование конечных точек, внутрисетевые методы, сетевой уровень, транспортный уровень, прикладной уровень и т.д.), а также полученных результатов сетевых измерений [9].

Проблематика интернет-измерений систематически исследуется на международном уровне, охватывая как деятельность международных организаций, так и проведение мероприятий разнообразного международного формата. Интерес в этой связи представляет определение понятия «Измерение Интернета», разработанное Организацией экономического сотрудничества и развития (ОЭСР) и означающее многомерную систему для оценки функционирования Интернета в технологическом, социальном и экономическом плане, в т.ч. с использованием стандартизированных индикаторов, определяющих возможности широкополосного доступа, уровень подключения домохозяйств и предприятий, производительности сетей, а также вклада цифровизации в обобщённо-совокупный рост добавочной стоимости [10].

Серьёзное развитие получает многолетняя серия регулярных международных мероприятий по проблематике интернет-измерений, и в их ряду значительная роль принадлежит широкомасштабной Конференции по измерениям в Интернете (Internet Measurement Conference, IMC). Первая Конференция по измерениям в Интернете (далее – «Конференция ACM IMC») прошла в 2001 году (США, г. Сан-Франциско) [11]. Она была организована по инициативе Специализированной группы по вопросам передачи данных Ассоциации вычислительной техники (Association for Computing Machinery's Special Interest Group on Data Communications, SIGCOMM ACM) [12]. С этого года Конференция ACM IMC стала проводится в ежегодном формате, способствуя международному многостороннему обмену новейшими методологиями, инструментами и результатами исследований интернет-измерений. Если обобщить, то на Конференции ACM IMC рассматриваются вопросы текущего состояния и будущего функционирования «сетевого взаимодействия», основанного на фундаментальных принципах интернет-инфраструктуры; анализируются модели, свойства и характеристики параметров развития интернет-технологий; обсуждаются проекты документов, рабочие материалы и результаты работ, углубляющие понимание методов сбора и анализа обмена данными в современных условиях т.н. гибридного Интернета, «расслоения Интернета» и т.д. В 2025 году Конференция ACM IMC (Висконсин, США) отметила свой двадцатипятилетний, «серебряный» юбилей. Труды 25 конференций опубликованы и охватывают более 160 работ по конкретным исследованиям интернет-измерений [13]. В октябре 2026 года Конференция ACM IMC проводится в двадцать шестой раз – в г. Карлсруэ (Германия) – и предлагает более масштабную программу, чем обычно [14]. Безусловно, итоги Конференции ACM IMC 2026 ещё предстоит проанализировать, но не вызывает сомнений, что она придаст новый импульс и динамику исследованиям интернет-измерений как на национальном, так и на международном уровне.

В свете представленных выше положений логично обратиться к ряду документов, которые не только выступают ориентиром для исследователей и практиков интернет-сообщества при реализации конкретных мероприятий интернет-измерений разной направленности, но также потенциально могут оказать влияние на дальнейшее формирование возможной нормативной основы проведения интернет-измерений. Значение названных документов невозможно игнорировать, хотя все они носят рекомендательный характер и не устанавливают интернет-стандарты. В числе таких документов следует бегло рассмотреть «Руководство относительно мероприятий по измерению Интернета»; «Руководство по безопасному проведению измерений в Интернете»; «Рекомендации (факторы и условия) безопасного проведения измерений в Интернете».

«Руководство относительно мероприятий по измерению Интернета» получило своё закрепление в формате RFC 1262, о чём говорилось в начале настоящей статьи. В 1991 году под редакцией Винта Серфа (Vinton G. Cerf) был опубликован RFC 1262, адресованный исследователям, рассматривающим возможность проведения экспериментов по измерениям в Интернете [15]. В RFC 1262 указывалось, что данный RFC не является интернет-стандартом, но вместе с тем пользователям Интернета настоятельно рекомендовалось следовать положениям RFC 1262 «...из уважения к интернет-сообществу и профессиональных соображений». Заслуживает внимание тот факт, что временной срок действия RFC 1262 не определен.

Согласно RFC 1262, осуществляющие интернет-измерения лица должны обеспечить соблюдение следующих условий:

- собранные данные не должны нарушать конфиденциальность, безопасность или правила допустимого использования;
- если агрегированные данные потенциально могут нарушать конфиденциальность, исследователь должен защитить конфиденциальность;
- если деятельность по сбору данных может быть истол-

кована как нарушение безопасности, исследователям настоятельно рекомендуется заранее уведомить CERT;

- сбор данных не должен создавать чрезмерной нагрузки или иным образом мешать работе сети или подключённых устройств, соответственно, следует в первую очередь проводить неинвазивные измерения (пассивный мониторинг);
- необходимо связаться с поставщиками услуг, когда возникает влияние на работу системы;
- должны быть широко доступны цели исследования, методология и планы;
- необходимо получить предварительное разрешение, когда интернет-измерения создают чрезмерную нагрузку на удалённое устройство или сеть.

Помимо основных рекомендаций для исследователей интернет-измерений, в RFC 1262 затронут общий контекст безопасности проведения измерений, в частности, проблемы, связанные с потенциально возможной путаницей между плановыми измерениями (активными/пассивным) и vice versa враждебными атаками на безопасность.

В отношении трёх далее рассматриваемых документов, принятых в последние два года (2025-2026), принципиально важно оговорить следующие моменты. Первый момент касается формального статуса этих документов, поскольку все они являются «предварительными документами» (Internet-Drafts) [16], которые действуют не более шести месяцев и в любой момент могут быть обновлены, заменены или признаны устаревшими в связи с появлением иных подобных документов. Второй момент относится к тому, что в настоящей статье документы формата Internet-Drafts использованы в качестве справочных материалов и исключительно с рекомендованной ссылкой – «рабочие материалы»/«незавершённая разработка». Третий момент связан с тем, что нижеуказанные документы предметно сфокусированы на проблематике безопасности интернет-измерений, конфиденциальности и безопасности пользователей. Четвёртый момент определяется тем, что объём рассматриваемых ниже документов позволяет затронуть лишь некоторые их положения.

«Руководство по безопасному проведению измерений в Интернете» (Guidelines for Performing Safe Measurement on the Internet) [17] принято в марте 2025 года со сроком действия до 19.09.2025 года. Данный документ (далее – «Guidelines 2025») соответствует положениям IETF Trust [18] и BCP 78 [19]. В Guidelines 2025 отмечается важность интернет-измерений для широкого круга пользователей, но поскольку их проведение нередко создаёт риски для конфиденциальности и безопасности пользователей, документ содержит рекомендации, которые актуальны для проектов, связанных с генерацией, сбором и/или анализом трафика, создаваемого людьми.

Несмотря на тот факт, что Guidelines 2025 утратил своё действие, представляется интересным обратить внимание на закрепление ряда ключевых понятий, с учётом существующих рисков для конфиденциальности и безопасности пользователей, а именно:

- модель угроз (Threat model): угроза — это потенциальная возможность нарушения безопасности, возникающая при наличии обстоятельств, возможностей, действий или событий, способных привести к нарушению безопасности и причинению ущерба (RFC 4949) [20];
- пользователь (User): в контексте Guidelines 2025 интернет-пользователем считается физическое лицо или организация, чьи данные используются при обмене информацией через Интернет, или, в более широком смысле, любой субъект, использующий Интернет для коммуникации;
- активные измерения (Active Measurement): активные измерения предполагают генерацию или модификацию трафика;
- пассивные измерения (Passive Measurement): пассивные измерения заключаются в наблюдении за существующим трафиком без активного вмешательства;
- измерения на пути следования трафика (On-path): измерения, которые выполняются непосредственно в сети;
- измерения вне пути следования трафика (Off-path): измерения, указывающие на активность, осуществляемую через побочный канал, в оконечной точке или в иных местах, где возможен доступ к пользователю, его соединению или данным;
- односторонние измерения (One-ended): измерения, подобные зондированию или трассировке;
- двусторонние измерения/измерения с двусторонним управлением (Two-ended): измерения, требующие взаимодействия обеих оконечных точек; при этом сеть также может выступать в качестве одной из таких точек, если она является объектом измерения.

«Рекомендации (факторы и условия) безопасного проведения измерений в Интернете» (Considerations for Performing Safe Measurement on the Internet draft-irtf-pearg-safe-internet-measurement-13) [21]. Данный документ (далее – «Considerations 13») принят в июле 2025 года со сроком действия 26.01.2026, соответствует положениям BCP 78 и BCP 79, т.е. Considerations 13 исчерпал срок своего действия [22].

По сути, Considerations 13 являлся обновлённой версией предыдущего документа – Guidelines 2025, соответственно, положения Considerations 13 de facto также направлены на определение рисков для конечных пользователей и инфраструктуры третьих сторон в ходе активных или пассивных интернет-измерений, включая как научные исследования, так и прикладные. Вместе с тем, в Considerations 13 особое внимание уделено рискам, сопряжённым с обеспечением безопасности пользователей при проведении интернет-измерений, и необходимости получения согласия пользователей и сбора данных. Отмечается важность учёта того, что даже если риск нарушения конфиденци-

альности не очевиден или не может быть реализован в текущий момент, рост вычислительных мощностей в будущем может сделать это возможным. В Considerations 13 отмечается, что любое проведение интернет-измерений может повлиять на безопасность пользователей, в частности, измерение генерируемого трафика может косвенно дать также представление о трафике других пользователей.

В ходе интернет-измерений потенциально возможными вариантами воздействия на пользователей могут быть:

- нарушение конфиденциальности (Breach of Privacy). На этапе сбора данных первого уровня (например, имя) возможно идентифицировать конкретного человека; данные второго уровня (например, IP-адрес) могут использоваться для отслеживания поведения. Риск нарушения конфиденциальности также связан с передачей данных пользователя третьим лицам в объёме, превышающем тот, на который пользователь дал согласие; это может произойти в результате случайного или преднамеренного разглашения либо принудительного раскрытия информации. Нарушение конфиденциальности также может касаться риска повторной идентификации или деанонимизации зашифрованных или замаскированных данных пользователей;

- недостаточная защита данных (Inadequate Data Protection). Передаваемые и хранящиеся данные недостаточно защищены от разглашения, и возникает возможность риска несанкционированного доступа к данным, либо отсутствия надлежащего контроля доступа (т.е. когда доступ к пользовательским данным имеют лица, которым он не требуется);

- генерация трафика (Traffic Generation). Генерируемый интернет- трафик – избыточен;

- подмена лица, иначе – имперсонация (Impersonation). В ходе интернет-измерений осуществляется имитация действий пользователя или выдача себя за него;

- правовые аспекты (Legal). Пользователи и поставщики услуг обязаны соблюдать широкий спектр политик и нормативных правил (условия и порядок предоставления услуг, законодательные акты и проч.), применяющихся в зависимости от контекста и юрисдикции. Интернет-измерения способны нарушать такие правила и нормы, а последствия нарушений могут быть серьёзными, и по запросу государственных органов или судов может потребоваться раскрытие конфиденциальных данных;

- недоступность (Unavailability). Пользователи или иные субъекты могут зависеть от информации или систем, задействованных в интернет-измерениях, а неожиданная или запланированная недоступность такой информации или систем может нанести ущерб пользователю;

- нарушение целостности системы или данных (System or Data Corruption). Сгенерированный или модифицированный трафик может привести к нарушению работы системы, что охватывает случаи потери или повреждения данных пользователя, а также ситуации, когда в результате этого нарушается доступ пользователя к системе;

- эмоциональная травма (Emotional Trauma). Проведение интернет-измерений определённых показателей, либо воздействие контента, либо моделей поведения – наносит пользователю эмоциональный или психологический вред.

«Рекомендации (факторы и условия) безопасного проведения измерений в Интернете» (Considerations for Performing Safe Measurement on the Internet draft-irtf-pearg-safe-internet-measurement-14) [23]. Этот документ (далее – «Considerations 14») принят в январе 2026 года со сроком действия 29.07.2026, и соответствует положениям BCP 78 и IETF Trust [24]. В отношении Considerations 14 также следует сказать об исчерпании сроков действия этого документа, равно как и то, что он выступает в качестве обновлённой версии предыдущего документа – Considerations 13. В связи с активным развитием интернет-измерений, проведение исследований в реальной среде Интернета, в отличие от использования изолированных экспериментальных стендов или платформ для моделирования, означает, что эксперименты сосуществуют в одном пространстве с другими сервисами и конечными пользователями. С учётом множественности вовлечённых в интернет-измерения исследователей, Considerations 14 предлагает для них рекомендации, призванные помочь им снизить риски для безопасности конечных пользователей и других сервисов. Нельзя не заметить, что структурно и содержательно Considerations 14 коррелирует ключевым положениям Considerations 13, включая применяемый понятийно-терминологический аппарат, а также потенциально параметры воздействия на пользователей в ходе проведения интернет-измерений [25].

Вполне закономерно и логично было бы в статье не упоминать отдельно каждый из вышерассмотренных документов, принимая во внимание, что и Guidelines 2025, и Considerations 13, и Considerations 14 предметно относятся к безопасности интернет-измерений, являясь «последующими обновлёнными» связанными версиями. Однако рассмотрение исключительно последней версии – Considerations 14, – как представляется, ограничило бы восприятие самого факта самостоятельного значения безопасности проведения интернет-измерений, а также не способствовало бы пониманию важности документального закрепления содержательных границ соответствующих конструируемых понятий, включая определение объёма таких понятий.

***

Принимая во внимание масштаб, разнообразие и стремительно расширяющееся развитие исследований в области интернет-измерений, едва ли можно избежать фрагмен-

тарности и беглости изложения в рамках одной статьи. Однако любое обращение к проблематике интернет-измерений представляется важным в силу того, что такого рода исследования затрагивают не только компоненты Интернета, но и представляют интерес для каждого из нас как пользователей Интернета.

Список литературы:

[1] См, например, D. Karrenberg. Measuring Root Server Performance Internet Way of Networking, https://circleid.com/posts/20120217_measuring_root_server_performance; W.Lehr. Measuring the Internet: The Data Challenge. https://ideas.repec.org/p/oec/stiaab/194-en.html; Агафонов А.С. Цифровая суверенность государства: анализ зарубежных подходов // Российский юридический журнал. 2025. N 3. С. 7 – 15, http://www.consultant.ru/

[2] Ethics and the Internet (RFC 1087, January 1989), https://datatracker.ietf.org/doc/html/rfc1087

[3] Guidelines for Internet Measurement Activities. Vinton G. Cerf (RFC 1262, October 1991), https://datatracker.ietf.org/doc/html/rfc1262

[4] Request for Comments, https://www.ietf.org/process/rfcs/. Подробнее об RFC см. также А. Робачевский. Интернет изнутри: Архитектура экосистемы Интернета. 3-е изд. перераб. и дополн. – М.:Серпантин Эджензи, 2024. С. 15.

[5] О сути концепции эмерджентости см., например, А. Себрант, От Аристотеля до Альтмана: почему «эмерджентность» – ключевой термин для понимания ИИ. https://www.forbes.ru/mneniya/522204-ot-aristotela-do-al-tmana-pocemu-emerdzentnost-klucevoj-termin-dla-ponimania-ii

[6] A. Dayekh. The Illusion of Digital Sovereignty (Part II) – Emergence, Sovereign AI Ecosystem, the RIR System, Number Resources, https://circleid.com/posts/the-illusion-of-digital-sovereignty-part-ii

[7] О. Колкман, А. Робачевский, К. Габерг, Х. Бодран. Влияние развития периферийных сетевых вычислений Интернета // Интернет изнутри (апрель). 2025. – N 22. С.2-8.

[8] M. Safaei Pour, C. Nader, K. Friday, E.Bou-Harb. A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security, https://www.sciencedirect.com/science/article/pii/S0167404823000330

[9] Internet Measurement Research Group (IMRG), https://www.icir.org/imrg/

[10] См., например, Measuring the Internet, https://www.oecd.org/en/publications/measuring-the-internet_5k9bhk5fzvzx-en.html

[11] Internet Measurement Conference, https://dl.acm.org/doi/proceedings/10.1145/3730567; и https://www.sigcomm.org/events/imc-conference

[12] Группа ACM SIGCOMM, https://www.sigcomm.org/about

[13] IMC'25 Proceedings of the 2025 ACM Internet Measurement Conference, https://dl.acm.org/action/showFmPdf?doi=10.1145%2F3730567

[14] ACM Internet Measurement Conference 2026, https://conferences.sigcomm.org/imc/2026/

[15] https://www.iab.org/about/

[16] https://en.wikipedia.org/wiki/Internet_Draft

[17] Guidelines for Performing Safe Measurement on the Internet, https://www.ietf.org/archive/id/draft-irtf-pearg-safe-internet-measurement-12.html

[18] Legal Provisions Relating to IETF Documents, TLD, https://trustee.ietf.org/documents/trust-legal-provisions/

[19] BCP 78 – это документ «Наилучшей текущей практики» в рамках IETF, который определяет практику предоставления прав авторами в отношении их вкладов (Contributions) в IETF, https://www.rfc-editor.org/info/bcp78/ https://www.rfc-ditor.org/info/bcp78/

[20] RFC 4949 (Internet Security Glossary, Version 2), https://datatracker.ietf.org/doc/html/rfc4949

[21] Considerations for Performing Safe Measurement on the Internet, https://datatracker.ietf.org/doc/draft-irtf-pearg-safe-internet-measurement/13/

[22] BCP 78, BCP 79, https://www.rfc-editor.org/info/bcp78/ и https://www.rfc-ditor.org/info/bcp79/

[23] Considerations for Performing Safe Measurement on the Internet, https://www.ietf.org/archive/id/draft-irtf-pearg-safe-internet-measurement-14.html

[24] См ссылки 16 и 18.

[25] M. Fayed. The tricky science of Internet measurement, https://blog.cloudflare.com/tricky-internet-measurement/

Об авторе:

Касенова Мадина Балташевна, д.ю.н, юридическая фирма «Лиджист» (научно-консультативный совет).

От секундомера до микросекунды: эволюция и технологии хронометража в лёгкой атлетике



Александр Бабаев

Аннотация

Статья посвящена истории и применяемым современным технологиям хронометража в лёгкой атлетике — одном из самых точных и технологически оснащённых видов спорта. Статья состоит из двух связанных частей.

Первая часть представляет собой хронологический обзор развития систем измерения времени на Олимпийских играх и чемпионатах мира по лёгкой атлетике с 1932 года до наших дней. Рассматриваются ключевые этапы: с Олимпийских игр в 1932 году, когда швейцарская компания Omega получила статус официального хронометриста Олимпийских игр и впервые была применена фотофинишная камера Кирби, до современных цифровых фотофинишей Scan'O'Vision и Seiko Slit Video System вкупе с современным хронометражем с точностью до 1 миллионной секунды.

Вторая часть содержит обзор технологий, применяемых на крупнейших легкоатлетических турнирах: электронные стартовые пистолеты и датчики фальстарта, фотофинишные камеры с частотой сканирования до 40 тысяч строк в секунду, лазерные дальномеры для технических видов, RFID-системы для марафона и системы трекинга спортсменов в реальном времени, а также новейших разработок — датчиков в обуви для спортивной ходьбы и систем компьютерного зрения.

..

Ключевые слова:

хронометраж, рекорды, олимпийские игры, лёгкая атлетика, секунды

Введение

Лёгкая атлетика – спорт, в котором судьбу медали решают порой сотые и даже тысячные доли секунды. За этой точностью стоит более чем вековая история совершенствования измерительных систем: от механических секундомеров с погрешностью в пятую долю секунды до современных фотофинишных камер, способных делать десятки тысяч снимков в секунду, и таймеров с точностью до микросекунды. Эта статья состоит из двух частей: первая прослеживает хронологию развития хронометража на Олимпийских играх и чемпионатах мира по лёгкой атлетике, вторая – даёт краткий обзор технологий, которые определяют результаты крупнейших соревнований сегодня.

Часть I. Хронологическая справка: от ручного секундомера до цифровой эпохи

1896–1928: Эра ручного хронометража

Первые современные Олимпийские игры в Афинах (1896) обходились самым простым инструментарием: судьи использовали механические карманные секундомеры, которые запускались и останавливались вручную. Точность таких измерений составляла примерно 1/5 секунды (0,2 с), а результаты фиксировались с округлением до десятых. О погрешности, связанной с человеческой реакцией (в среднем 0,15–0,25 с), тогда задумывались мало – разрывы между спортсменами были достаточно велики, и спорные ситуации возникали нечасто. Занимательная история в хронометраже на марафоне в 1896 году: так как старт и финиш были в разных местах, секундомер вёз судья на велосипеде на протяжении всей дистанции.

На Играх 1900 года в Париже и 1904 года в Сент-Луисе случались и другие курьёзы: разные судьи с секундомерами показывали разные результаты для одного и того же забега, и итоговое время определялось усреднением или голосованием. Это наглядно демонстрировало ненадёжность ручного метода.

На Играх 1912 года в Стокгольме впервые были опробованы полуавтоматические электрические секундомеры, запускавшиеся выстрелом стартового пистолета. Однако останавливались они по-прежнему вручную, что лишь частично решало проблему. Именно на этих Играх впервые был применён фотофиниш, который позволил зафиксировать разрыв между вторым и третьим местом в 0,1 секунды на дистанции 1500 м.

1932: Выход на сцену Omega и первый фотофиниш

Олимпийские игры 1932 года в Лос-Анджелесе стали поворотным моментом. Швейцарская компания Omega впервые получила статус официального хронометриста Олимпийских игр. На Игры были доставлены 30 высокоточных секундомеров с точностью до 1/10 секунды и один квалифицированный часовщик – весь штат хронометристов состоял из одного человека.

Но подлинной революцией стало применение фотофинишной камеры Кирби, разработанной Густавусом Кирби. В финале 100-метровки американцы Эдди Толан и Ральф Меткалф пересекли финишную черту практически одновременно. Ручные секундомеры зафиксировали одинаковое время – 10,3 с. Однако фотофинишная плёнка недвусмысленно показала, что Толан коснулся финишной линии первым. Это был один из первых в истории спорта случаев, когда фотографическое доказательство разрешило спор, который без него остался бы неразрешимым.

1936–1948: От Берлина к «Волшебному глазу»

На Олимпийских играх 1936 года в Берлине хронометраж сделал ещё один шаг вперёд – использовалось уже 185 хронографов, и на месте была организована специальная ремонтная мастерская. Немецкие инженеры представили усовершенствованную фотофинишную систему, а в забеге на 100 метров с результатом 10,3 секунды триумфатором стал американец Джесси Оуэнс.

После войны, на Играх 1948 года в Лондоне, произошла настоящая революция. Олимпийская хронометражная система Racend Omega Timer, известная также как «Волшебный глаз» (Magic Eye), впервые была развёрнута в полном объёме. В отличие от предыдущих камер, делавших один снимок в момент финиша, эта система использовала щелевую съёмку: плёнка непрерывно двигалась за узкой щелью, направленной точно на финишную линию. Результатом было не обычное фото, а развёртка времени, где по горизонтали откладывалось время, а по вертикали – положение на финишной линии. Этот принцип лежит в основе всех современных фотофинишных систем.

1960: Римский урок

Финал 100-метровки на Олимпийских играх 1960 года в Риме стал ещё одним мощным аргументом в пользу электроники. Немец Армин Хари и американец Дэйв Сайм финишировали в исключительно плотной борьбе. Ручные секундомеры всех судей показали 10,2 с для обоих. Однако фотофиниш чётко зафиксировал победу Хари. Этот случай окончательно убедил спортивное сообщество в том, что ручной хронометраж на спринтерских дистанциях более не может считаться достаточным. Также на этой олимпиаде появились крупные электронные табло, позволявшие зрителям в режиме реального времени видеть предварительные и итоговые результаты соревнований.

1964–1968: Электронная революция

Олимпийские игры 1964 года в Токио стали первыми, на которых была развёрнута полностью электронная система хронометража. Официальным хронометристом на этих Олимпийских играх была японская фирма Seiko.

Параллельно с этим фирма Omega представила Omegascope – систему, которая в реальном времени накладывала электронное время на телевизионную картинку. Зрители у экра-

нов впервые могли видеть бегущие цифры секунд прямо во время трансляции соревнования. Это произвело колоссальное впечатление и навсегда изменило восприятие спорта телеаудиторией.

Олимпийские игры 1968 года в Мехико закрепили электронную революцию: электронное время впервые стало официальным результатом, заменив ручной хронометраж. Именно здесь Джим Хайнс пробежал 100 метров за 9,95 с – первый в истории официальный результат из 10 секунд, зафиксированный электроникой. Примечательно, что по ручному хронометражу его результат составил бы 9,9 с, но новая система показала более точную картину. На этих же Играх Боб Бимон совершил «прыжок века» в длину – 8,90 м, и результат был зафиксирован с точностью до сантиметра благодаря специальному оптическому маркеру, перемещавшемуся по направляющему рельсу вдоль прыжковой ямы.

1972–1988: Стандартизация и рост точности

На Играх 1972 года в Мюнхене точность до 1/100 секунды окончательно утвердилась как стандарт для спринтерских и средних дистанций в лёгкой атлетике. Результаты стали фиксироваться с двумя знаками после запятой.

В этот период Omega продолжала совершенствовать фотофинишные системы, увеличивая скорость съёмки и улучшая разрешение. На Играх 1976 года в Монреале были внедрены системы резервирования данных – на случай отказа основной аппаратуры. На Играх 1980 года в Москве, проходивших в условиях бойкота, советские специалисты, тем не менее, работали в тесном контакте с Omega, что позволило отечественным инженерам получить уникальный опыт в области спортивного хронометража.

На Играх 1984 года в Лос-Анджелесе были представлены новые электронные табло и улучшенные системы обработки данных. В это же время в лёгкой атлетике произошли важные изменения в правилах фальстарта: если раньше спортсмен имел право на один фальстарт без дисквалификации, то с 1990-х годов правила ужесточались, и к 2010 году было введено правило «нулевой толерантности» – любой фальстарт означает немедленную дисквалификацию. Это стало возможным только благодаря появлению датчиков давления в стартовых блоках, объективно фиксирующих момент начала движения, которые впервые появились на Играх 1984 года.

Параллельно развивался и другой важный фронт: чемпионаты мира по лёгкой атлетике. Первый чемпионат мира состоялся в 1983 году в Хельсинки. С 1985 года официальным хронометристом World Athletics (тогда – IAAF) стала японская компания Seiko, которая и по сей день обеспечивает хронометраж на всех чемпионатах мира. Это создало интересную ситуацию: на Олимпийских играх хронометраж обеспечивает Omega, а на чемпионатах мира – Seiko, и обе компании соревнуются в технологическом совершенстве.

1992: Scan'O'Vision и цифровая эра

Зимние Олимпийские игры 1992 года ознаменовались появлением системы Scan'O'Vision – первого полностью цифрового фотофиниша, показывающего время финиша с точностью до тысячных долей секунды. Вместо плёнки использовалась цифровая матрица, что позволило мгновенно получать, обрабатывать и транслировать результаты. Время от финиша до появления официального результата на табло сократилось с минут до секунд. Позже эта технология перенеслась и на летние Олимпийские игры.

На Играх 1996 года в Атланте система Scan'O'Vision сыграла ключевую роль в финале 100-метровки у женщин, где результат был определён с точностью до тысячных долей секунды.

2008–2012: К микросекундам

Олимпийские игры 2008 года в Пекине запомнились не только феноменальным мировым рекордом Усэйна Болта (9,69 с на 100 м), но и внедрением высокоскоростных камер с разрешением, позволяющим определять разницу в тысячные доли секунды. Любопытно, что Болт на последних метрах дистанции замедлился, празднуя победу, и аналитики позже подсчитали, что без этого замедления его результат мог составить около 9,55–9,60 с. Именно здесь впервые была применена система «виртуального рекорда» – на телевизионной графике зрители могли видеть линию, соответствующую времени мирового рекорда, и сравнивать с ней бегущего спортсмена. А вес всего привезённого хронометрического оборудования на Олимпийские игры составил 420 тонн.

На Играх 2012 года в Лондоне Omega представила Quantum Timer – хронометр с разрешением до одной микросекунды (одна миллионная секунды). Хотя результаты в лёгкой атлетике по-прежнему округляются до сотых, такая точность критически важна для внутренней обработки данных, определения порядка финишировавших и разрешения спорных ситуаций. На этих же Играх впервые были массово применены системы RFID-транспондеров для марафона и спортивной ходьбы, что позволило точно отслеживать прохождение каждого спортсмена через все контрольные точки на трассе.

2016–2024: Эра сверхвысоких скоростей и интеллектуальной аналитики

На Играх 2016 года в Рио-де-Жанейро была представлена камера Scan'O'Vision Myria, способная делать до 10 тысяч кадров в секунду. На Играх 2020 года в Токио (прошедших в 2021 году) системы трекинга в реальном времени позволили показывать телезрителям скорость спортсменов, их позиции на дистанции и отставание от лидеров прямо во время забега. Именно в Токио впервые были применены системы компьютерного зрения для автоматического определения нарушений в спортивной ходьбе – потери контакта с землёй и сгибания опорной ноги в колене.

Олимпийские игры 2024 года в Париже стали демонстрацией комплексного подхода: Omega развернула более 350 тонн оборудования, задействовала более 550 профессиональных хронометристов и около 500 обученных добровольцев. В финале 100 м у мужчин Ной Лайлс опередил Кинани Уэйтмана всего на 0,005 секунды – один из самых плотных финишей в истории Олимпийских игр. Впервые на Играх были широко применены системы компьютерного зрения и искусственного интеллекта для автоматического анализа техники бега,

прыжков и метаний. В спортивной ходьбе были использованы инновационные датчики в обуви спортсменов, передававшие данные о контакте с землёй в режиме реального времени.

На чемпионатах мира Seiko также не отставала: на ЧМ 2022 года в Юджине и ЧМ 2023 года в Будапеште использовались новейшие фотофинишные системы, лазерные дальномеры нового поколения и расширенные системы трекинга спортсменов на дистанции. На ЧМ 2023 года впервые была применена система автоматического измерения скорости снаряда в метаниях с помощью радаров, что позволило телезрителям видеть скорость вылета ядра или копья в реальном времени.

Часть II. Современные технологии хронометража: как это устроено сегодня

Современная система хронометража на Олимпийских играх или чемпионате мира по лёгкой атлетике – это сложный комплекс взаимосвязанных технологий, охватывающий старт, дистанцию, финиш и обработку данных. Рассмотрим ключевые компоненты.

1. Старт: электронный пистолет и датчики фальстарта

Электронный стартовый пистолет давно заменил традиционный огнестрельный. Он не производит настоящего выстрела: вместо этого он генерирует звуковой сигнал, который одновременно подаётся через динамики, встроенные в стартовые блоки каждого спортсмена. Это устраняет проблему, при которой бегуны на дальних дорожках слышали выстрел на доли секунды позже, чем на ближних (скорость звука – 343 м/с, и на девятой дорожке задержка может составлять до 0,03 секунды).

Стартовые блоки оснащены высокочувствительными датчиками давления, которые непрерывно измеряют силу, с которой спортсмен давит на педали. Система фиксирует момент, когда давление начинает нарастать (начало реакции), и сравнивает его с моментом стартового сигнала. Если это время составляет менее 0,100 секунды, фиксируется фальстарт. Порог в 100 мс основан на научных данных: считается, что человек физиологически не способен обработать звуковой сигнал и начать мышечное движение быстрее, чем за эту долю секунды. Реакция быстрее 0,100 с трактуется как предвосхищение сигнала, а не реакция на него.

Современные стартовые блоки также измеряют распределение силы между левой и правой ногой, что используется для биомеханического анализа старта. Данные со всех блоков синхронизируются с центральным таймером с точностью до микросекунды.

Именно эта технология привела к одному из самых громких инцидентов в истории лёгкой атлетики: на чемпионате мира 2011 года в Тэгу Усэйн Болт был дисквалифицирован за фальстарт в финале 100 м. Датчики зафиксировали, что его реакция составила менее 0,100 с, что автоматически означало фальстарт. Этот случай наглядно продемонстрировал, что даже величайшие спортсмены не застрахованы от ошибок, и что технология хронометража стала неотъемлемой частью справедливости соревнований.

2. Финиш: фотофинишные камеры

Сердце любой системы хронометража – фотофинишная камера, установленная строго на продолжении финишной линии. Принцип, заложенный ещё в 1948 году, остаётся неизменным: это щелевая (сканирующая) съёмка. Камера не делает «фотографии» в привычном смысле – она непрерывно сканирует узкую вертикальную полосу, совпадающую с финишной линией, с чрезвычайно высокой частотой.

Физика процесса такова: оптическая система камеры фокусируется на вертикальной щели шириной в несколько миллиметров, направленной строго на финишную линию. Свет от этой щели попадает на линейку светочувствительных элементов (матрицу), которая считывает изображение с частотой от 10 тысяч до 40 тысяч строк в секунду. Каждая строка содержит информацию о том, какие объекты находились на финишной линии в данный момент. Из этих строк компьютер формирует изображение, где горизонтальная ось представляет время, а вертикальная – пространство (позицию на финишной линии).

Результат: на итоговом изображении чётко видно, какой спортсмен пересёк линию первым, с точностью, позволяющей различить разницу в тысячные доли секунды (а при использовании Quantum Timer – и в микросекунды). Характерная «размазанность» изображения на таких фотографиях – не дефект, а следствие принципа съёмки: быстро движущиеся части тела занимают на изображении меньше пикселей по горизонтали, чем движущиеся медленно.

На Олимпийских играх 2024 года в Париже использовалась камера Omega Scan'O'Vision Ultimate, способная делать до 40 тысяч сканирований в секунду. Это в четыре раза больше, чем у предыдущего поколения (10 тысяч кадров в секунду у модели Scan'O'Vision Myria). Именно эта камера зафиксировала финиш Ноя Лайлса в финале 100 м с преимуществом всего в 0,005 секунды.

На чемпионатах мира Seiko использует систему Slit Video System, которая работает со скоростью до 10 тысяч кадров в секунду в высоком разрешении.

Важно понимать: хотя внутренние системы работают с точностью до микросекунд, официальные результаты в лёгкой атлетике по правилам World Athletics округляются до 1/100 секунды на дистанциях до 10 тысяч метров включительно. Однако при определении порядка финишировавших (кто был первым, вторым и т.д.) используются полные данные без округления.

3. Лазерные дальномеры и системы измерения в технических видах

В прыжках в длину, тройном прыжке и метаниях (ядро,

диск, молот, копьё) ручные рулетки давно уступили место электронным дальномерам (EDM – Electronic Distance Measurement). Это лазерные тахеометры, установленные на штативах в секторе, которые с точностью до миллиметра измеряют расстояние от точки приземления снаряда или отпечатка в песке до заданной контрольной точки.

В прыжках в длину и тройном прыжке дополнительно используются системы видеоконтроля заступа. Высокоскоростная камера направлена на планку отталкивания и фиксирует, не переступил ли спортсмен линию заступа. Это дополняет, но не полностью заменяет традиционную пластилиновую индикаторную доску, на которой остаётся отпечаток стопы при заступе. Современные системы видеоконтроля способны анализировать положение стопы с точностью до миллиметра в реальном времени, автоматически сигнализируя о заступе.

В прыжках в высоту и с шестом лазерные системы используются для точной установки и контроля высоты планки. На крупных соревнованиях применяются специальные лазерные нивелиры, которые исключают человеческий фактор при измерении высоты – погрешность составляет менее миллиметра.

В метаниях всё чаще применяются радарные системы, измеряющие скорость вылета снаряда и траекторию его полёта. Это позволяет не только фиксировать результат, но и предоставлять телезрителям дополнительную аналитику: скорость, угол вылета, расчётную дальность полёта.

4. RFID-транспондеры для марафона и спортивной ходьбы

В дисциплинах, проходящих на шоссе (марафон, полумарафон, спортивная ходьба), невозможно использовать фотофинишную камеру на протяжении всей трассы. Вместо этого каждый спортсмен получает RFID-чип (обычно встроенный в нагрудный номер или закреплённый на обуви). На трассе через определённые промежутки (обычно каждые 5 км, а также на отметках 10, 15, 20, 25, 30, 35, 40 км и на финише) установлены антенны-считыватели. Когда спортсмен пробегает над антенной, чип фиксируется, и система записывает его промежуточное время.

Современные RFID-системы работают на частоте 13,56 МГц (HF) или 860–960 МГц (UHF). UHF-системы обеспечивают большую дальность считывания (до 10 метров) и высокую скорость опроса – до нескольких сотен чипов в секунду, что критично важно на старте массовых марафонов, где одновременно на трассу выходят десятки тысяч участников.

Эта технология позволяет не только фиксировать итоговый результат, но и отслеживать динамику гонки: темп каждого спортсмена, моменты отрывов и отставаний. Данные в реальном времени передаются в телевизионную графику и на информационные табло.

Для определения официального времени в марафоне используются два показателя: «время от выстрела» (gun time) и «чистое время» (net time) – от момента пересечения стартовой линии до финиша. Официальным результатом считается время от выстрела, но чистое время также публикуется и важно для массовых забегов.

5. Системы трекинга и аналитики в реальном времени

Одно из самых заметных нововведений последних лет – системы позиционирования спортсменов в реальном времени. На Олимпийских играх Omega и на чемпионатах мира Seiko используют различные технологии для отслеживания позиции каждого спортсмена на беговой дорожке с частотой обновления в десятки раз в секунду.

Это позволяет в режиме реального времени вычислять и отображать:

- мгновенную скорость каждого спортсмена;
- позицию в забеге и отставание от лидера;
- пройденную дистанцию с точностью до метра;
- сравнение темпа с мировым рекордом (визуализируемое в виде «линии рекорда» на экране).

Для телезрителей это означает совершенно новый уровень понимания происходящего: можно видеть, что на отметке 60 м Болт уже набрал максимальную скорость 44,72 км/ч, или что на последнем круге забега на 10 тысяч метров темп лидера составляет 58 секунд на круг.

6. Новейшие разработки: датчики в обуви и компьютерное зрение

Особого внимания заслуживают новейшие системы, внедрённые в последние годы. В спортивной ходьбе с 2023 года World Athletics разрешила использование специальных датчиков в обуви, которые фиксируют момент потери контакта стопы с землёй. Эти датчики, разработанные совместно с производителями спортивной обуви, передают данные на центральный блок обработки в режиме реального времени. Если система фиксирует потерю контакта, она подаёт сигнал судьям, которые принимают окончательное решение о дисквалификации. Это решение было принято после многочисленных скандалов на крупных турнирах, когда судьи физически не успевали фиксировать все нарушения невооружённым глазом.

В технических видах всё активнее применяется компьютерное зрение. Камеры, установленные в секторах, автоматически анализируют технику спортсменов: угол вылета снаряда, положение тела в фазе отталкивания, траекторию полёта. Эти данные используются не только для телевизионной графики, но и для тренировки спортсменов – тренеры получают детальную биомеханическую картину каждого выступления.

7. Обработка данных, интеграция и ТВ-графика

Все перечисленные системы объединены в единую информационную платформу, которая в реальном времени соби-

рает, обрабатывает и распределяет данные. Результаты автоматически поступают:

- на электронные табло стадиона;
- в систему информирования (комментаторы, судьи, тренеры, журналисты);
- в телевизионную графику (наложенные на картинку титры, таблицы, анимации);
- в официальные базы данных World Athletics и МОК;
- в мобильные приложения и на веб-сайты.

Скорость обработки такова, что предварительный результат забега на 100 метров появляется на табло стадиона через менее чем 15 секунд после финиша, а официальный (после проверки фотофиниша) – в течение одной-двух минут. Современные системы используют алгоритмы машинного обучения для автоматической проверки результатов на аномалии: если время спортсмена значительно отличается от его персональных рекордов или от ожидаемого, система автоматически помечает результат для дополнительной проверки судьёй.

8. Анемометры и контроль условий

Хотя это не хронометраж в прямом смысле, для легитимности результатов в спринте и прыжках критически важно измерение скорости ветра. Электронные анемометры, установленные рядом с беговой дорожкой и сектором прыжков, непрерывно фиксируют скорость и направление ветра. Если попутный ветер превышает 2,0 м/с, результат не может быть признан рекордом (хотя засчитывается для определения мест в данном соревновании). Данные анемометра автоматически привязываются к результату каждого забега.

Современные анемометры используют ультразвуковые датчики, не имеющие движущихся частей, что повышает их надёжность и точность. Измерения проводятся на высоте 1,22 м над уровнем беговой дорожки – именно на этой высоте, по мнению специалистов, ветер оказывает наибольшее влияние на бегунов.

9. Будущее: искусственный интеллект

Искусственный интеллект всё активнее внедряется в системы хронометража. Нейросети обучаются распознавать типичные ошибки в измерениях, автоматически калибровать оборудование, предсказывать возможные отказы аппаратуры. В перспективе ИИ сможет полностью автоматически определять победителя забега по данным фотофиниша, исключая необходимость ручной проверки оператором.

Развиваются и носимые сенсоры, которые в будущем могут быть интегрированы в экипировку спортсменов и передавать в реальном времени данные о пульсе, частоте дыхания, мышечной активности, температуре тела. Это откроет новые возможности для анализа производительности и предотвращения травм.

10. Сопоставимость результатов

Стандартизация условий проведения соревнований – ключевой фактор, обеспечивающий сопоставимость результатов, полученных на разных турнирах. Все соревнования, на которых фиксируются официальные результаты, должны соответствовать требованиям World Athletics: сертифицированные беговые дорожки и сектора, электронный хронометраж с точностью до сотых долей секунды, контроль скорости ветра (не более 2,0 м/с для спринта и прыжков). Благодаря этим требованиям результат, показанный на чемпионате мира в Будапеште, может быть напрямую сопоставлен с результатом, показанным на Олимпийских играх в Париже или на национальном чемпионате любой страны, – все они вносятся в единую глобальную базу данных World Athletics и признаются во всём мире.

Для сравнения достижений в принципиально разных дисциплинах (например, бег на 100 метров и метание копья) World Athletics использует систему таблиц очков (World Athletics Scoring Tables). В основе лежат математические формулы, которые переводят результат в любой дисциплине в числовое значение. Именно благодаря этой системе в многоборьях (десятиборье, семиборье) результаты в разных видах складываются в общую сумму очков, а также определяются рейтинги спортсменов и лучшие атлеты года, что позволяет объективно сравнивать несравнимое.

Заключение

Путь от карманного секундомера с погрешностью в пятую долю секунды до квантового таймера с разрешением в одну микросекунду занял чуть более ста лет. За это время хронометраж превратился из вспомогательной судейской функции в высокотехнологичную индустрию, в которой задействованы сотни тонн оборудования, передовые достижения оптики, электроники, информатики и телекоммуникаций.

Но суть осталась прежней: обеспечить справедливый и точный результат. Каждый раз, когда мы видим на экране, что спортсмен выиграл с преимуществом в 0,01 секунды, за этим стоит невидимая работа сложнейших систем, которые начинали свой путь с одного часовщика и тридцати секундомеров на Играх 1932 года в Лос-Анджелесе. И можно не сомневаться, что технологии хронометража продолжат развиваться – ведь спорт не перестаёт ставить новые задачи на грани человеческих возможностей.

Об авторе:

Бабаев Александр Сергеевич, мастер спорта по лёгкой атлетике, многократный чемпион России в беге на 100 км.

Новости науки и техники

Система HERMES: новый инструмент мониторинга Интернета

Оценивая состояния Интернета, исследователи и операторы прежде всего проверяют доступность сети: могут ли пакеты данных попасть из одной точки в другую. Такие системы мониторинга, как Cloudflare Radar или IODA Технологического института Джорджии, достаточно эффективно обнаруживают отключения сетей и блокировки Интернета. Однако само наличие соединения ещё не означает, что Интернет работает нормально. Например, задержка при передаче данных может внезапно увеличиться на несколько сотен миллисекунд. Пакеты по-прежнему достигают адресата, поэтому формально сеть остаётся доступной. Но для пользователя видеоигры, видеосвязи или другого чувствительного к задержкам приложения качество соединения резко ухудшается, при том, что традиционные системы мониторинга могут вообще не заметить такой сбой.

Исследователи разработали систему HERMES, позволяющую обнаруживать подобные ситуации с помощью данных обычных тестов скорости Интернета. Такие тесты каждый день проводят миллионы пользователей. Одна из крупнейших открытых измерительных платформ Measurement Lab (M-Lab) собирает результаты миллионов измерений, в том числе выполняемых через интерфейс поиска Google.

Разумеется, любой отдельно взятый тест почти ничего не говорит о состоянии Интернета в целом: он показывает лишь качество соединения конкретного пользователя с конкретным сервером в определённый момент. Однако миллионы таких измерений позволяют обнаруживать закономерности, одновременно возникающие у пользователей в разных географических точках и сетях. При этом существует важная проблема: тесты скорости изначально предназначены не для научного мониторинга, а для диагностики соединения самими пользователями. Люди запускают их неравномерно и особенно часто тогда, когда уже подозревают неполадки. Кроме того, скорость зависит от технологии доступа и возможностей конкретного подключения. Поэтому HERMES не пытается определить, является ли отдельный результат «хорошим» или «плохим». Система ищет устойчивое изменение обычных показателей сразу у множества пользователей.

Затем эти данные сопоставляются с маршрутами прохождения интернет-трафика. Если соединения пользователей, одновременно столкнувшихся с ухудшением качества, проходят через одни и те же элементы сетевой инфраструктуры, это позволяет локализовать возможный источник проблемы. Для анализа используются как traceroute, так и reverse traceroute – измерения маршрута в обоих направлениях.

В ходе исследования система HERMES проанализировала около четырёх миллиардов тестов скорости, собранных за пять месяцев. Система выявила примерно 65 тысяч случаев ухудшения производительности, затронувших группы пользователей в 16 тысячах городов, 9710 сетях и 166 странах. Показательный случай произошёл в сети Cogent в Чикаго. Задержка у пользователей внезапно выросла более чем на 200 миллисекунд, хотя сеть оставалась полностью доступной. Выяснилось, что причиной стал необычный маршрут: в одном направлении трафик проходил относительно обычным путём через Даллас, а в обратном отправлялся через Сан-Хосе и Сингапур и лишь затем возвращался в Чикаго. Пользователи активно обсуждали проблему, однако системы, ориентированные на обнаружение потери связности, её практически не видели.

Авторы HERMES считают, что мониторинг Интернета должен отвечать не только на вопрос, доступна ли сеть, но и на вопрос, насколько хорошо она работает для пользователей. Миллионы разрозненных тестов скорости в сочетании с информацией о маршрутах трафика фактически могут превратиться в распределённую систему датчиков, способную обнаруживать проблемы, остающиеся незаметными для традиционных средств мониторинга.

Источник: https://pulse.internetsociety.org/en/blog/2026/09/the-internet-can-fail-without-going-down-how-can-millions-of-speed-tests-help-us-see-performance-problems/

Больше измерителей не равнозначны большей точности измерений

Для масштабного мониторинга Интернета обычно используются специальные устройства – измерительные зонды (probes), установленные в домах пользователей, в офисах, на предприятиях и т.д. в различных городах и странах. Они регулярно измеряют задержку – время, необходимое данным для передачи до сервера и обратно. На первый взгляд кажется очевидным: чем больше таких устройств, тем больше информации можно получить. Однако исследование, проведённое учёными Чикагского университета, показало, что значительная часть измерений фактически дублирует друг друга.

Учёные проанализировали четыре месяца высокочастотных измерений задержки, полученных с 99 зондов, размещённых в разных районах Чикаго. Выяснилось, что многие аномалии, зарегистрированные разными устройствами, были проявлениями одного и того же события — например, одновременного ухудшения качества соединения у абонентов одного интернет-провайдера. Иными словами, 99 зондов вовсе не давали исследователям 99 независимых представлений о состоянии сети. Значительная часть собранных ими данных была избыточной.

Авторы исследования разработали набор методов, позволяющих определить, какие устройства действительно обнаруживают новую информацию, а какие лишь подтверждают уже зафиксированные другими зондами проблемы. Результат оказался неожиданным: для обнаружения 95% совокупного воздействия сетевых аномалий оказалось достаточно всего 44

из 99 устройств. При этом предложенный алгоритм выявлял более чем вдвое больше различных аномалий, чем случайный выбор примерно такого же количества зондов.

Однако ещё более интересными оказались географические результаты. Сокращая количество используемых устройств более чем наполовину, алгоритм сохранил по крайней мере один зонд в 17 из 21 районов Чикаго. При этом географическое разнообразие не было специально заложено в критерии отбора: система просто выбирала устройства, предоставлявшие наиболее уникальную информацию. Особенно выделился один район на юге Чикаго. Именно оттуда в сокращённый набор попало больше всего зондов, и там же было обнаружено наибольшее число уникальных аномалий. По мнению исследователей, это указывает на то, что качество интернет-соединений в этом районе отличается большей нестабильностью и вариативностью по сравнению с другими частями города. Простой метод равномерного или случайного размещения измерительных устройств мог бы эту особенность не обнаружить.

Полученные результаты могут быть использованы крупными проектами интернет-мониторинга, включая Measuring Broadband America Федеральной комиссии по связи США, RIPE Atlas и Measurement Lab. Предложенный подход позволяет уменьшить избыточность уже существующей измерительной инфраструктуры без установки дополнительного оборудования.

Авторы также обращают внимание на недостаток современной интернет-статистики. Многие платформы фиксируют скорость и задержку в конкретный момент, но значительно реже учитывают продолжительность и масштаб ухудшения соединения. Исследователи предлагают систематически регистрировать не только средние показатели, но также амплитуду и длительность аномалий задержки.

Это позволило бы оценивать не только формальную доступность широкополосного Интернета, но и его реальное качество. Два домохозяйства могут считаться одинаково подключёнными к Интернету, однако качество связи у них способно существенно различаться. Поэтому задача интернет-измерений заключается не обязательно в увеличении количества датчиков, а прежде всего в правильном выборе точек наблюдения и понимании характера обнаруженных ими аномалий.

Источник: https://pulse.internetsociety.org/en/blog/2026/07/why-more-measurement-probes-dont-mean-better-internet-data/

Боты генерируют уже более трети веб-трафика

Доля автоматизированного трафика в Интернете продолжает расти. По данным Cloudflare Radar, в третьем квартале 2026 года боты генерировали 35,49% всех HTTP-запросов, проходивших через инфраструктуру Cloudflare. Годом ранее их доля составляла 30,13%, а во втором квартале нынешнего года – 33,21%. Эти показатели не следует воспринимать как измерение всего мирового интернет-трафика: компания Cloudflare анализирует запросы, проходящие через её собственную сеть. Однако благодаря огромному масштабу инфраструктуры компании эти данные позволяют отслеживать заметные изменения в структуре веб-трафика.

В категорию автоматизированного трафика входят поисковые роботы, различные служебные системы, вредоносные боты и множество других программ. На инструменты искусственного интеллекта в третьем квартале приходилось 22,12% всего трафика ботов. Поэтому периодически встречающиеся утверждения о том, что едва ли не половина интернет-трафика уже создаётся искусственным интеллектом, данные Cloudflare не подтверждают.

Рост автоматизированного трафика влияет в том числе и на статистику используемых устройств. Доля запросов, классифицированных как поступающие с настольных компьютеров, достигла 60,41% против 54,26% годом ранее. Однако это вовсе не означает массового возвращения пользователей от смартфонов к настольным компьютерам. Существенную часть этого роста обеспечивает именно активность ботов. В результате обычная статистика распределения трафика между мобильными и настольными устройствами может давать искажённое представление о поведении людей, если автоматические запросы не отделять от пользовательских.

Другие показатели демонстрируют дальнейшее распространение современных технологий защиты соединений. В третьем квартале HTTPS использовался в 95,1% HTTP-запросов, а TLS 1.3 и QUIC вместе обеспечивали 93,89% наблюдаемого веб-трафика. Одновременно произошло неожиданное снижение доли HTTP/3. В третьем квартале 2025 года этот протокол использовался для 22,98% запросов, а год спустя – только для 20,17%. В сентябре показатель опустился до 19,83%. Таким образом, распространение новейшей версии HTTP пока не демонстрирует устойчивого роста. Несколько снизилась и доля IPv6 в HTTP-запросах: с 31,25% в третьем квартале прошлого года до 29,54% в нынешнем.

Одним из самых заметных изменений стало распространение постквантового шифрования. Если в третьем квартале 2025 года оно применялось примерно в 32% наблюдавшихся запросов, то год спустя – уже в 57,3%. Только с января по сентябрь 2026 года показатель увеличился почти на 10 процентных пунктов.

Авторы исследования обращают внимание на важную проблему интернет-статистики: изменение цифр не всегда означает изменение самого Интернета. Cloudflare периодически корректирует методы классификации трафика и состав анализируемых данных. Например, изменения категорий ИИ-ботов затрудняют прямое сравнение некоторых показателей за разные годы, а резкое падение доли скомпрометированных попыток входа оказалось связано прежде всего с изменением состава анализируемого трафика.

Поэтому измерение современного Интернета становится не только задачей сбора огромных объёмов данных. Не менее важно понимать, что именно измеряется, каким способом получены результаты и не вызвано ли наблюдаемое изменение новой методикой подсчёта, а не реальным изменением сети.

Источник: https://technologychecker.io/blog/web-traffic-statistics

Новости доменной индустрии

Опубликован отчёт IDN Implementation and UA Adoption Report 2026

Корпорация ICANN опубликовала на своём официальном сайте отчёт о работе по внедрению интернационализированных доменов и достижению универсального принятия IDN Implementation and UA Adoption Report 2026. Он фиксирует прогресс в создании более многоязычного и инклюзивного Интернета.

Интернационализированные домены (IDN) дают возможность пользователям всего мира использовать доменные имена на предпочитаемых ими языках и в привычных системах письменности. По состоянию на июнь 2026 года был делегирован 151 интернационализированный домен верхнего уровня, представляющий 37 языков и 23 системы письменности. Число зарегистрированных интернационализированных доменных имён второго уровня оценивается примерно в 4,3 миллиона.

Более широкое использование IDN зависит от дальнейшего внедрения универсального принятия (Universal Acceptance — UA), которое должно обеспечить корректное принятие, проверку, обработку, хранение и отображение всех действительных доменных имён и адресов электронной почты во всех подключённых к Интернету приложениях, устройствах и системах. Хотя поддержка UA расширяется, в отчёте отмечается, что проблемы сохраняются и работа в этом направлении должна продолжаться.

Вектор усилий интернет-сообщества всё более смещается с повышения осведомлённости о UA к его практическому внедрению и распространению. В рамках UA Day 2026 состоялось 33 мероприятия на 15 языках в 30 странах и территориях. Практическому внедрению универсального принятия способствуют инициативы университетов, местных языковых сообществ, технологических компаний и международных организаций, в том числе проект Координационного центра доменов .RU/.РФ «Поддерживаю.РФ».

В отчёте также рассматриваются изменения в политике и практике внедрения IDN, а также работа, связанная с новым этапом программы новых общих доменов верхнего уровня. Достижение универсального принятия — общая задача всех участников интернет-экосистемы. Свою роль в этом процессе должны играть разработчики технологических решений и программного обеспечения, научное и образовательное сообщество, операторы реестров и регистраторы доменных имён, поставщики услуг электронной почты и хостинга, а также разработчики государственной и отраслевой политики.

Источник: https://www.icann.org/en/announcements/details/new-icann-report-highlights-global-progress-on-idns-and-universal-acceptance-22-09-2026-en

Национальный домен Словении показал рекордный рост

В воскресенье 27 сентября в национальном домене Словении .si было зарегистрировано 4311 доменных имён. Это превосходит число регистраций за весь август, составившее 3515. Причиной удивительного роста стал президент США Дональд Трамп: 22 сентября, выступая на заседании ООН, он заявил, что правительство Соединенных Штатов впредь откажется от формулировки «искусственный интеллект» (artificial intelligence) и будет вместо неё использовать термин «сверхинтеллект» (super intelligence).

Решение Трамп обосновал тем, что слово «искусственный» содержит смысловой оттенок, подразумевающий «ненастоящесть», «фейковость». А это способно сеять сомнения и недоверие в отношении ИИ и его возможностей. При этом президента США, очевидно, не смутило то, что термин «сверхинтеллект» уже существует и используется для обозначения гипотетической стадии развития искусственного интеллекта, на которой он будет способен освоить и превзойти когнитивные способности человека в подавляющем большинстве областей.

Слова Дональда Трампа прозвучали для доменных инвесторов сигналом стартового пистолета. Аббревиатура от Super Intelligence — SI — полностью совпадает с кодом национального домена Словении. По данным оператора доменной зоны Register.si, на 4 сентября в словенском национальном домене было зарегистрировано 190 тысяч имён. А по состоянию на утро 29 сентября — 219 тысяч. Таким образом, за неполный месяц доменная зона выросла более чем на 15%.

Есть вероятность, что домен Словении может хотя бы отчасти повторить успех национального домена Ангильи .ai, который уже несколько лет демонстрирует бурный рост и собирает щедрые дивиденды на волне популярности искусственного интеллекта (Artificial intelligence, AI). Впрочем, ресурс Domain Name Wire, сообщая эту новость, отмечает, что с финансовой точки зрения словенский домен находится в не столь выгодном положении: годовая регистрация доменного имени стоит здесь порядка 10 евро (против 70 долларов и минимального срока регистрации в два года в .ai). Что же касается роста, то он будет зависеть прежде всего от того, придёт ли в голову кому-то, кроме Дональда Трампа, официально переименовать искусственный интеллект в сверхинтеллект.

Источник: https://cctld.ru/media/news/industry/41126/

От принципов к метрикам: на TLDCON 2026 обсудили создание системы индикаторов универсального принятия на базе МСЭ



21 сентября в рамках 19-й Международной конференции администраторов и регистраторов национальных доменов верхнего уровня стран Восточной Европы и Центральной Азии TLDCON 2026 в Ташкенте состоялась сессия «Разработка и внедрение индикаторов поддержки универсального принятия доменных имён и адресов электронной почты на базе Международного союза электросвязи (МСЭ)».

Мероприятие прошло в формате расширенного заседания с элементами круглого стола и объединило экспертов Регионального содружества в области связи (РСС), Координационного центра доменов .RU/.РФ, Межгосударственного статистического комитета СНГ, Совместной группы экспертов по статистике в области ИКТ (СГЭ-ИКТ) РСС, Региональной координационной группы по универсальному принятию стран СНГ и Восточной Европы, Российской группы по универсальному принятию, а также представителей национальных регистратур региона.

Универсальное принятие (Universal Acceptance, UA) является фундаментальным условием для построения действительно многоязычного и инклюзивного Интернета. Несмотря на то, что принцип универсального принятия и поддержка интернационализированных доменных имён закреплены в итоговых документах ВВУИО (ВВУИО+10 и ВВУИО+20) и резолюциях МСЭ, главной проблемой остаётся отсутствие стандартизированных подходов к их внедрению и единых измеримых метрик прогресса.

В ходе дискуссии заместитель генерального директора РСС Мария Большакова и председатель СГЭ-ИКТ Арсений Плосский подчеркнули, что продвижение универсального принятия должно опираться не на общие декларации, а на конкретные, измеримые метрики. В ответ на инициативу ICANN по созданию новой группы индикаторов на базе Международного союза электросвязи, эксперты региона предложили структурировать будущие показатели по трём ключевым направлениям: регуляторные аспекты, фактическое внедрение в государственные и коммерческие сервисы, а также технические требования. Особый акцент был сделан на том, что методология сбора данных должна быть прозрачной и не создавать чрезмерной административной или финансовой нагрузки на национальные статистические службы.

Для реализации этой задачи РСС планирует выступить с консолидированной позицией на ближайших заседаниях профильных рабочих органов МСЭ. Стратегия региона заключается в интеграции индикаторов универсального принятия в уже существующие системы оценки, такие как Индекс развития ИКТ (IDI). Это позволит странам СНГ и Восточной Европы не только объективно отслеживать собственный прогресс в цифровизации местных языков, но и принимать непосредственное участие в формировании глобальных стандартов многоязычного Интернета.

Главный аналитик Координационного центра доменов .RU/.РФ Мария Колесникова представила практический опыт регистратуры российских национальных доменов в этой сфере. Она подробно рассказала о масштабных исследованиях КЦ по поддержке интернационализированных адресов электронной почты (EAI) и доменных имён (IDN) в зонах .ru и .рф. Особое внимание было уделено успешным кейсам: крупные российские платформы, такие как Ozon, «Российская газета», Apteka.ru и Litres.ru, уже успешно принимают и отправляют письма на кириллические почтовые адреса.

«С 2026 года мы начали региональную работу по внедрению индикаторов универсального принятия в глобальную систему мониторинга Международного союза электросвязи. Наш опыт показывает, что синхронизация технических усилий с государственными инициативами даёт мощный импульс для цифровизации национальных языков», – отметила Колесникова.

По итогам дискуссии участники согласовали дальнейший план совместных действий. Согласно этому плану, СГЭ-ИКТ продолжит работу над формализацией предложений для включения в повестку рабочих органов МСЭ. Региональное сообщество (страны СНГ и Восточной Европы) выступит с консолидированной позицией на ближайших собраниях профильных групп МСЭ (EGTI), продвигая идею создания нового рабочего пункта по формированию показателей UA. Также будет продолжен обмен методологиями сбора данных между национальными статистическими службами и техническими специалистами регистратур интернационализированных доменов для обеспечения сопоставимости результатов.

Проведение этой секции на TLDCON 2026 подтвердило, что регион Восточной Европы и Центральной Азии не только активно внедряет принципы многоязычия, но и готов взять на себя лидирующую роль в формировании глобальных стандартов их оценки.

Источник: https://cctld.ru/media/news/kc/41124/


Интернет изнутри
БЕСПЛАТНЫЙ ЭКЗЕМПЛЯР