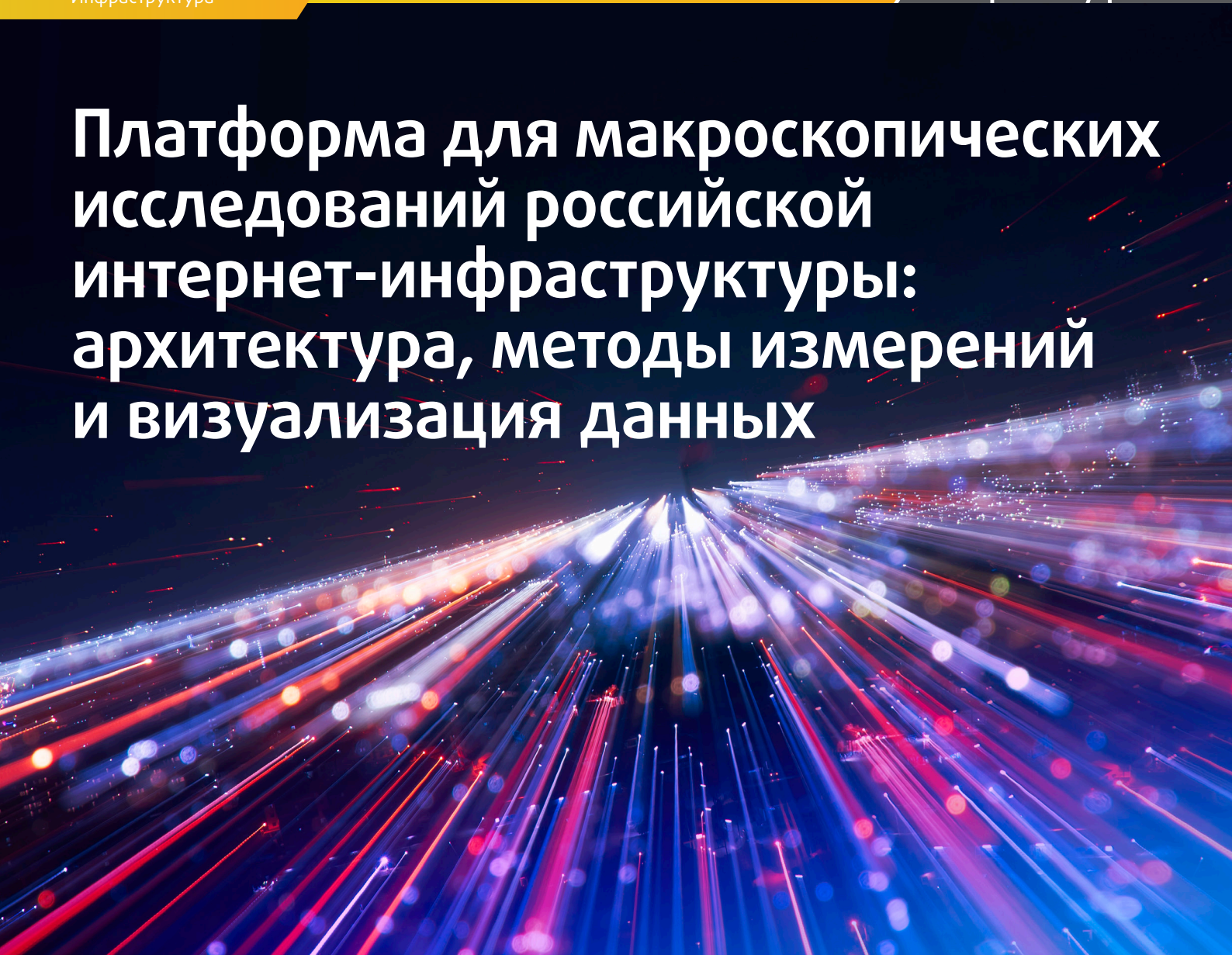
Платформа для макроскопических исследований российской интернет-инфраструктуры: архитектура, методы измерений и визуализация данных



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.

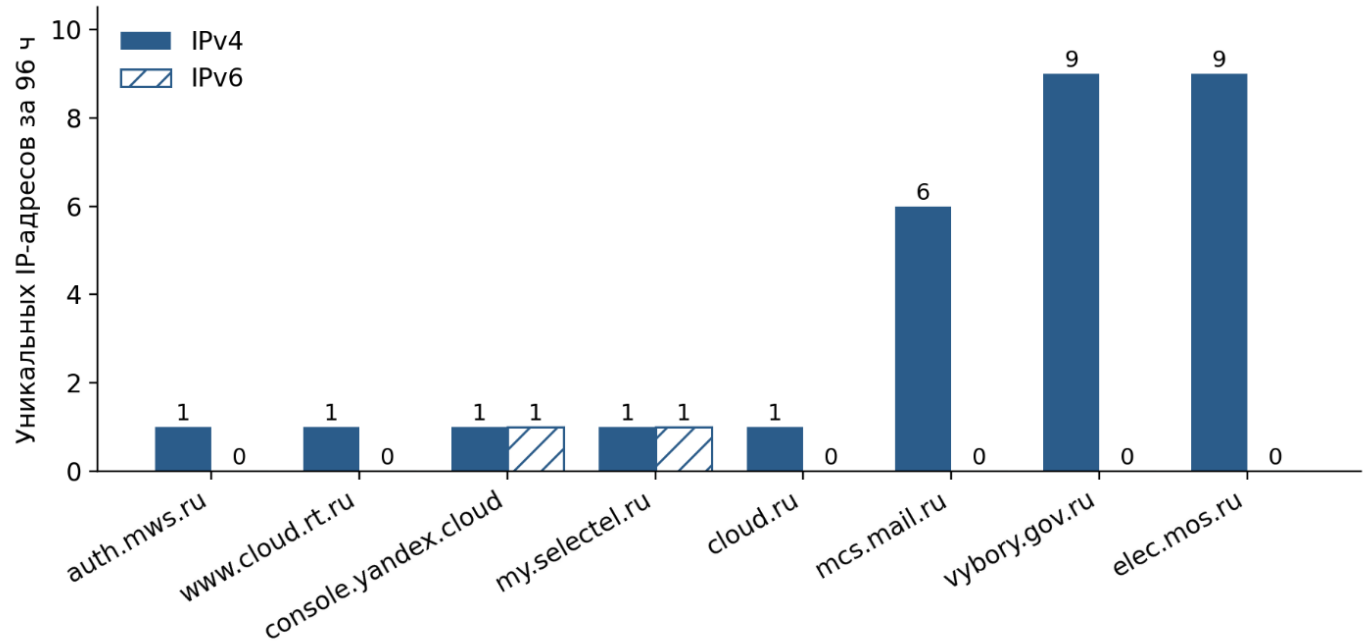
Полученные значения характеризуют время ответа выбранных URL и доступность соответствующих сетевых узлов из конкретных сетей доступа и не являются прямой оценкой всей инфраструктуры соответствующих компаний или операторов. Замеры выполнены в B2B-сегменте; B2C-трафик и прямой M2M-трафик к API-узлам в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

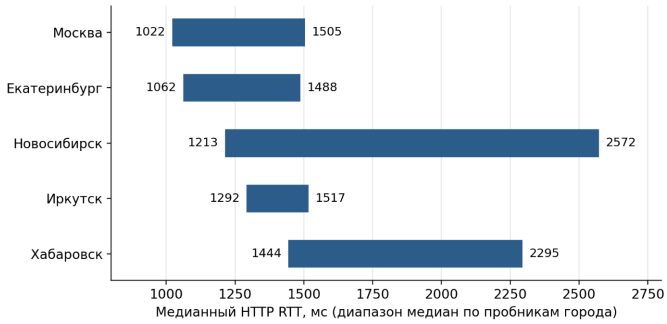


Рис. 2. Медианный HTTP RTT по городам для mcs.mail.ru, мс.

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.

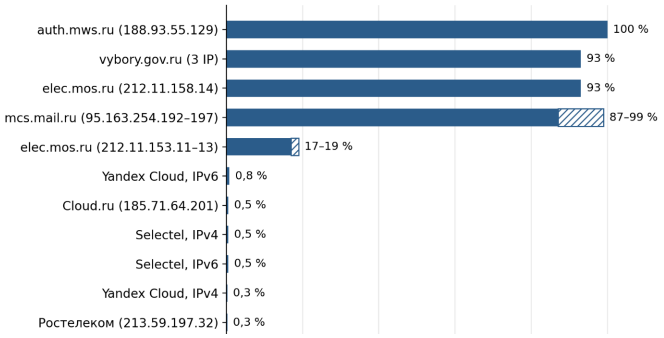


Рис. 3. Доля ICMP-таймаутов для целевых узлов.

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.

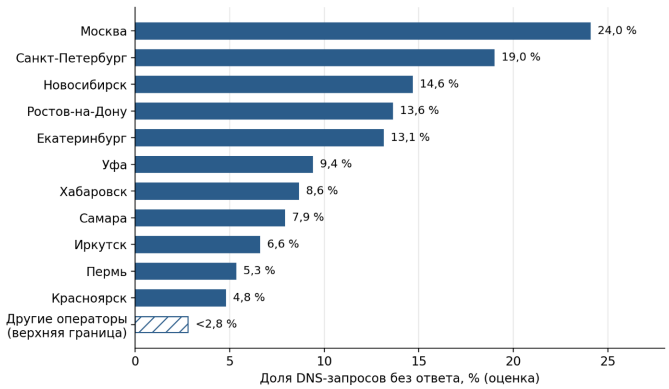


Рис. 4. DNS-ошибки по пробникам (запросы без ответа).

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.