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.

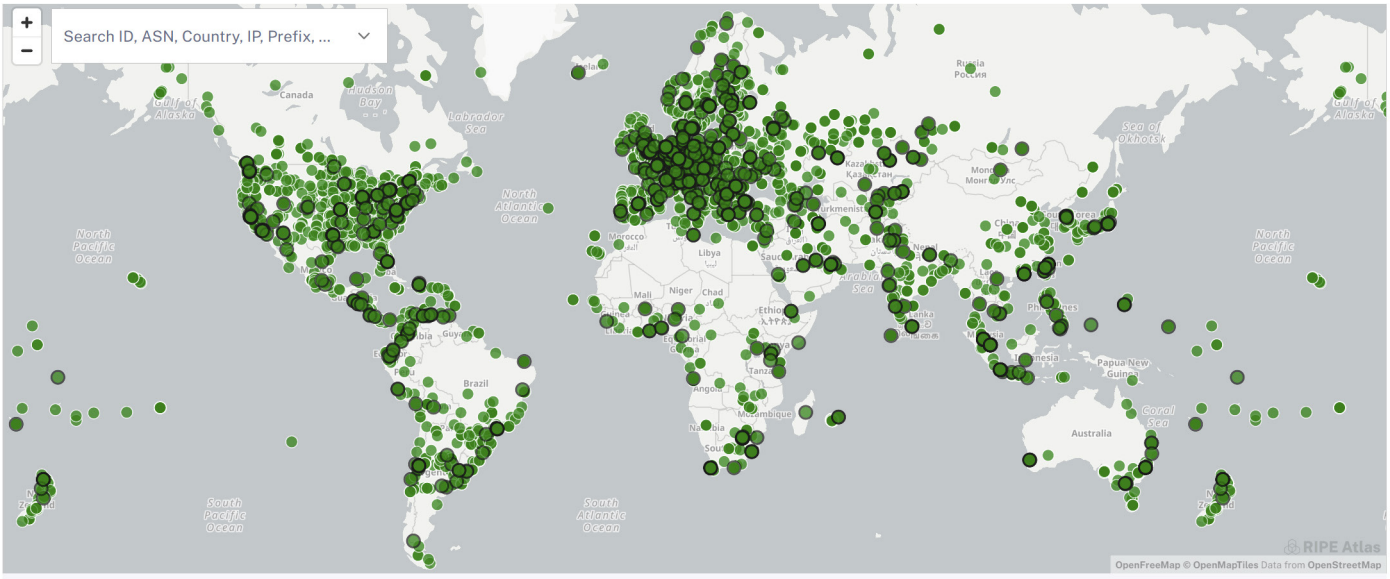

Рис. 1. Географический охват измерительной платформы RIPE Atlas.

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

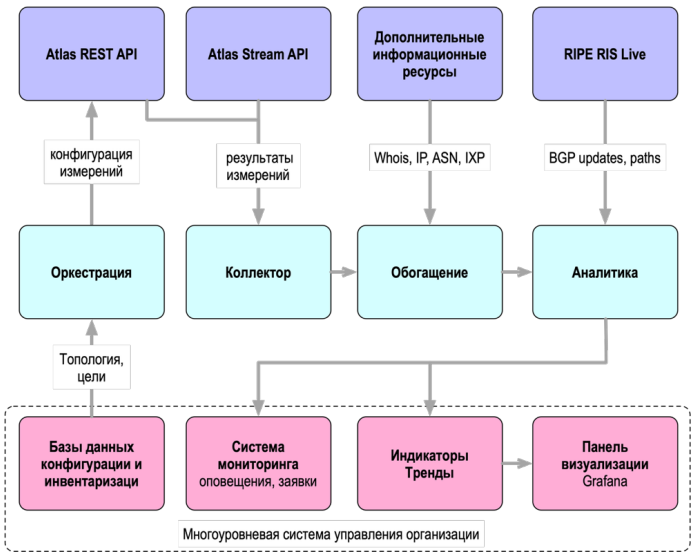

Рис. 2. Пример интеграции платформы RIPE Atlas с системой управления организации.

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