Безопасность интернет-инфраструктуры в Центральной Азии

Авторы: Анастасия Пак, Касим Лоан, Алекс Семеняка, Ваан Овсепян

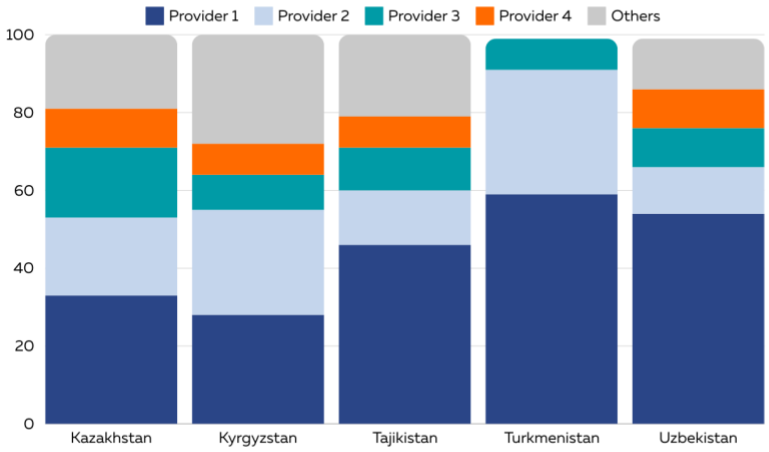
Третий Центральноазиатский Форум по пирингу и связанности (CAPIF 3) пройдет в Бишкеке, Кыргызстан, 24-25 сентября 2024 года. Мероприятие соберет экспертов из Центральной Азии, Ирана и соседних регионов для укрепления региональной интернет инфраструктуры и содействия цифровому развитию. В этой статье мы рассмотрели ключевые области в сфере интернет технологий, которые могут существенно повлиять на безопасность, масштабируемость и готовность интернет сетей в странах Центральной Азии к будущим вызовам. В этом контексте мы выделили две важные технологии: Инфраструктура открытых ключей ресурсов (RPKI) и Протокол Интернета версии 6 (IPv6).

Центральная Азия — это регион с богатой общей историей, не имеющий выхода к морю, с населением почти 80 миллионов человек (по состоянию на 2024 год). В последние несколько лет регион продемонстрировал значительный социально-экономический рост, который, по прогнозам ЕБРР, к концу 2024 года превысит 5%. Наряду с этим регион переживает стремительную цифровизацию, с более чем 65 миллионами интернет-пользователей (в 2023 году). Однако доступность интернета и его подключение по-прежнему представляют собой вызов в некоторых областях.

В этой статье мы анализируем внедрение RPKI и переход на IPv6 в Центральной Азии, подчеркивая возможности для укрепления интернет-инфраструктуры региона и поддержки его дальнейшего цифрового роста.

При анализе развития интернет-рынка в каждой из стран Центральной Азии можно заметить общую тенденцию к концентрации рынка. Несмотря на то, что это может ограничивать конкуренцию, данный тренд также представляет уникальные возможности для технологического прогресса. В среднем четыре крупнейшие автономные системы (AS) в каждой стране региона обслуживают около 80% населения, что означает, что несколько ключевых игроков способны инициировать значительные изменения во внедрении важных интернет технологий во всем регионе.

Число интернет пользователей в Центральной Азии



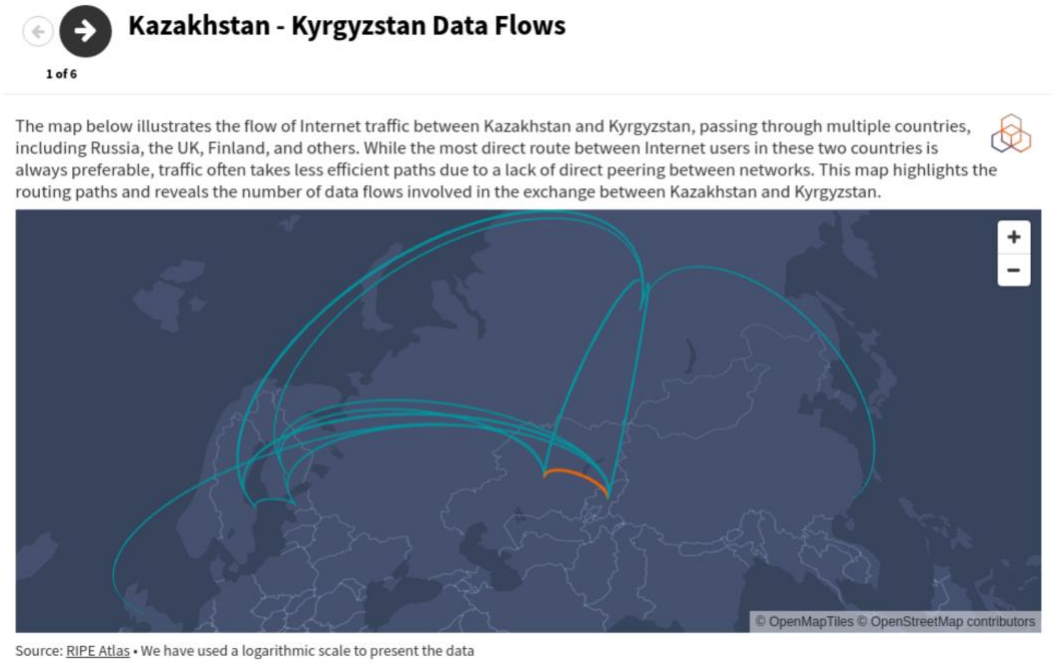
Этот график показывает примерное число пользователей каждой автономной системы (АС) в Центральной Азии, согласно данным APNIC. Мы определили долю 4-х самых крупных АС (провайдеров) в каждой из стран. Доля крупнейшего провайдера в регионе значительна и варьируется от 30% до 60%.

Источник: APNIC

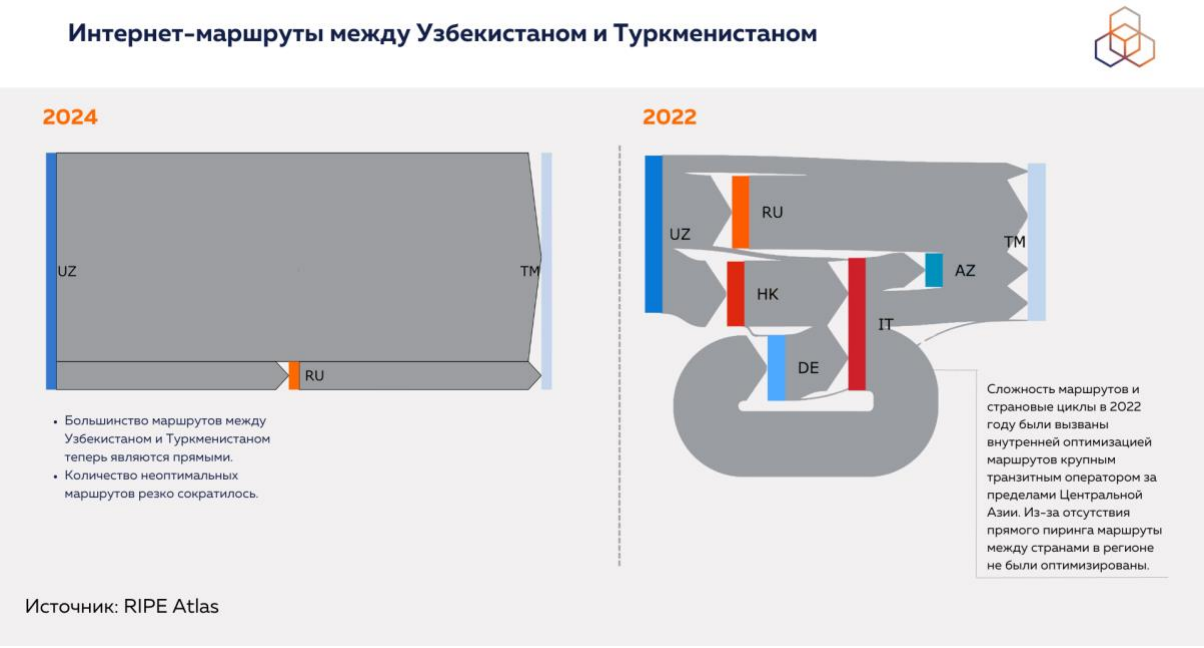
Межсетевое взаимодействие в Центральной Азии

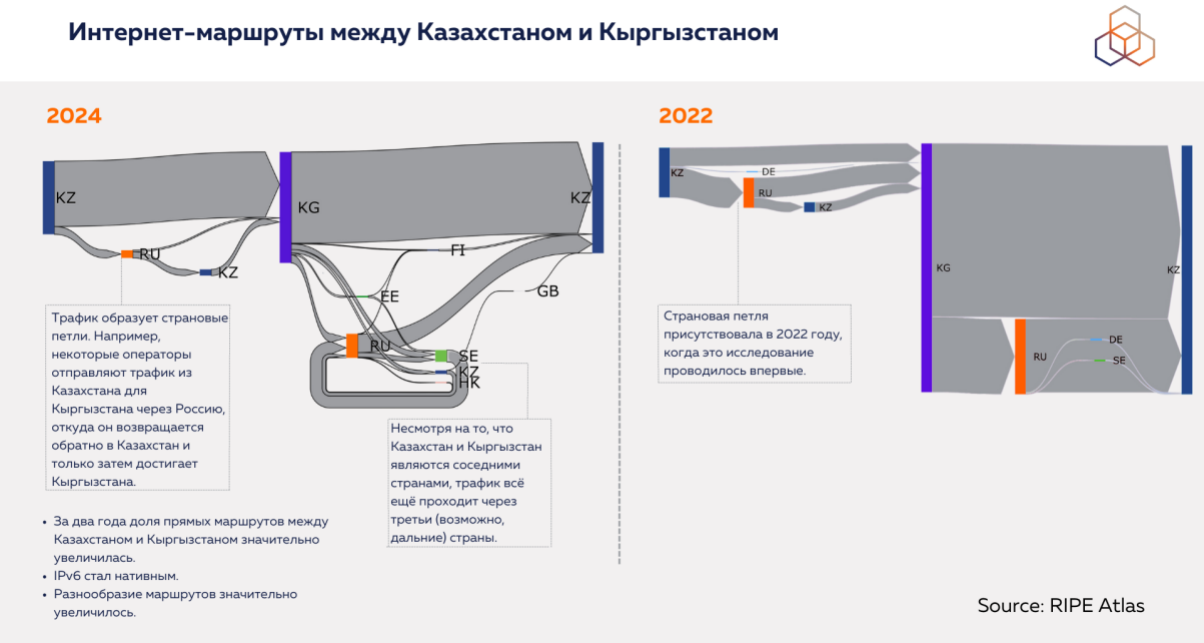
По мере усиления внутри регионального сотрудничества в Центральной Азии, включая рост торговли, инвестиций и туризма, мы изучили региональные сети с точки зрения маршрутизации, используя данные RIPE Atlas. Все точки RIPE Atlas в странах Центральной Азии были использованы в качестве исходных и конечных пунктов. В Туркменистане, где отсутствуют подключенные пробы, использовались дополнительные хосты. Это исследование было проведено два года назад и представлено на CAPIF 1, поэтому в этот раз мы смогли увидеть изменения с 2022 года.

На данной карте показаны потоки данных интернет-трафика между Казахстаном и Кыргызстаном, а также между Казахстаном и Таджикистаном, проходящие через несколько стран. Хотя наиболее предпочтительным является прямой маршрут между пользователями Интернета в этих странах, трафик часто проходит через менее эффективные пути из-за отсутствия прямого пиринга.



По сравнению с 2022 годом, значительные улучшения произошли в маршрутах между Узбекистаном и Туркменистаном, в то время как основные маршруты между Казахстаном и Кыргызстаном все еще нуждаются в улучшении (см. графики ниже).





В целом виден прогресс в локализации трафика в регионе и диверсификации маршрутов по странам. Однако субоптимальные маршруты транзита трафика все еще присутствуют в регионе. Внедрение более эффективных пиринговых политик и соглашений может стать важным шагом на пути к улучшению межсетевого взаимодействия в регионе.

CAPIF 3 предоставляет возможность укрепить и наладить новые пиринговые отношения с участниками мероприятия. В рамках CAPIF 3 будет выделен час для проведения двухсторонних встреч по пирингу. Ознакомьтесь с этой страницей, чтобы запланировать свои встречи на мероприятии.

Обратите внимание, что эти данные основаны на пробах RIPE Atlas, и нам все еще необходимо увеличить количество проб в регионе. Свяжитесь с командой RIPE Atlas, если вы хотите разместить физическую или виртуальную (software) пробу.

Защита сетевой маршрутизации в Центральной Азии

Безопасность маршрутизации (routing security) является основополагающим аспектом сетевой безопасности, который обеспечивает целостность и устойчивость глобального интернет-трафика. По мере усложнения сетей увеличиваются риски угонов маршрутов, утечек префиксов и ошибок в настройке BGP. Эти инциденты могут привести к значительным сбоям, перехвату данных и даже крупномасштабным нарушениям в работе сервисов.

Для решения этих проблем была разработана Инфраструктура открытых ключей ресурсов (RPKI), которая стала критически важной системой безопасности, помогающей операторам связи принимать более обоснованные и безопасные решения по маршрутизации. Благодаря криптографической проверке легитимности объявлений о маршрутах, RPKI позволяет администраторам сетей предотвращать

злонамеренные или случайные ошибки в маршрутизации, повышая как безопасность, так и операционную стабильность интернет-инфраструктуры.

Два ключевых компонента RPKI:

- **Авторизация источника маршрута (ROA)** — это электронно подписанный документ, который определяет, какие автономные системы (AS) уполномочены объявлять конкретные IP-префиксы. ROA выступают в качестве доверительного якоря, позволяя операторам сетей проверять происхождение информации о маршрутизации.
- **Проверка происхождения маршрута (ROV)** — это процесс использования ROA для проверки действительности объявлений о маршрутах. Он классифицирует маршруты BGP на три состояния: «действительные», «недействительные» или «не найдены» в зависимости от наличия и содержания соответствующих ROA.

Влияние RPKI на интернет-безопасность

До внедрения RPKI система маршрутизации Интернета была особенно уязвима как для случайных ошибок конфигурации, так и для злонамеренных атак. Один из примечательных инцидентов произошел в 2008 году, когда компания Pakistan Telecom (PTCL) случайно захватила IP-адреса YouTube, что привело к глобальному сбою работы видеоплатформы почти на два часа. Этот случай продемонстрировал хрупкость глобальной системы маршрутизации и необходимость более надежных мер безопасности. В последующие годы множество других инцидентов, связанных с крупными телекоммуникационными компаниями и технологическими гигантами, подчеркивали важность устранения уязвимостей BGP.

После внедрения RPKI инциденты с маршрутизацией все же продолжают происходить, но их последствия можно значительно уменьшить. Например, инцидент с Cloudflare 1.1.1.1, произошедший 27 июня 2024 года, был вызван ошибочной маршрутизацией, что привело к сбоям в работе сервисов. Валидация происхождения маршрута (ROV) могла бы предотвратить распространение этого ошибочного маршрута, тем самым смягчив последствия инцидента.

Другой реальный случай, когда ROV "спас ситуацию", произошел в июле 2023 года, когда правительство Ирака пыталось заблокировать приложение Telegram. Ошибочное объявление BGP маршрута привело к блокировке значительной части глобального интернет-трафика. Сети, в которых ROV была внедрена, отклонили эти неправильные маршруты, сохранив доступность сервисов для своих пользователей. Telegram создал ROA для своих маршрутов, что позволило автономным системам (AS) за пределами Ирака автоматически отклонять попытки угона маршрутов.

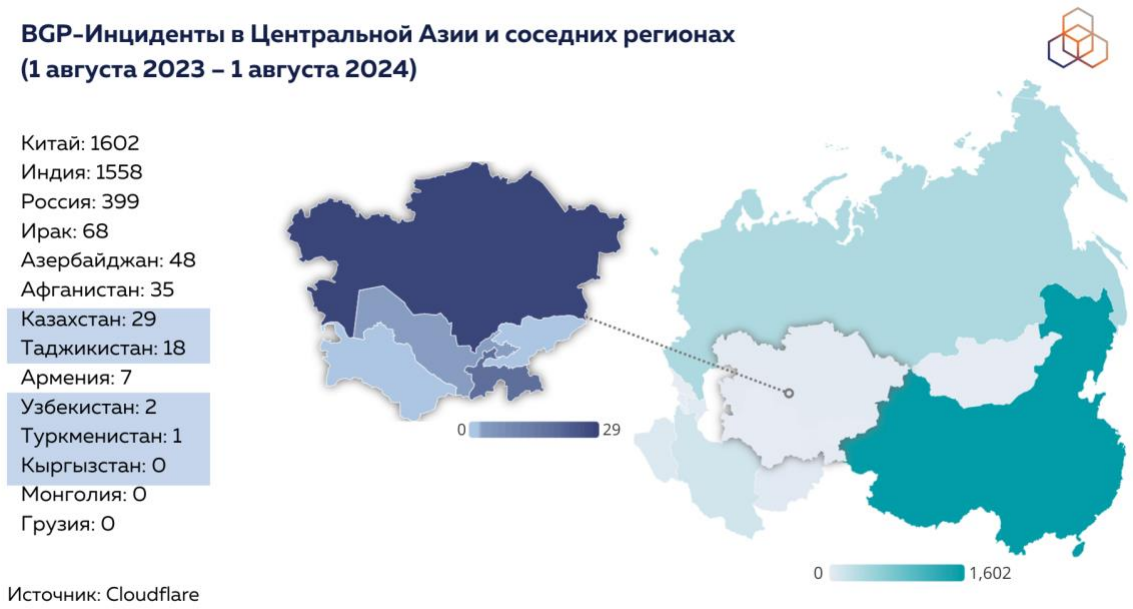
Эти примеры подчеркивают важность внедрения RPKI для защиты от случайных и преднамеренных ошибок в маршрутизации, обеспечивая бесперебойный доступ к интернету.

BGP Инциденты в Центральной Азии

Инциденты с протоколом пограничного шлюза (BGP), в частности угоны маршрутов, были зафиксированы в Центральной Азии и соседних регионах. Эти инциденты могут возникать как в результате ошибок конфигурации, так и в результате злонамеренных действий, что потенциально приводит к перенаправлению интернет-трафика.

Анализ данных Cloudflare по инцидентам с BGP выявляет интересные закономерности в этом регионе. Представленные данные включают информацию о захваченных префиксах, количестве злоумышленников и общем числе инцидентов.

На карте ниже можно увидеть, что например в Китае и Индии, наблюдается большое количество инцидентов, в то время как их количество достаточно небольшое в странах Центральной Азии. Хотя количество BGP инцидентов в регионе меньше, они все же могут привести к значительным сбоям в интернет-инфраструктуре региона. Важно понимать, что даже один случай угона префикса, будь то из-за ошибки конфигурации или злонамеренных действий, может вызвать серьезные сбои или потерю связи.



Глобальный и взаимосвязанный характер маршрутизации Интернета подчеркивает важность усиления BGP безопасности. Проактивные меры необходимы не только для защиты от локальных ошибок конфигурации, но и для смягчения потенциальных последствий инцидентов, происходящих в соседних регионах с более высоким уровнем инцидентов. Чтобы лучше понять состояние безопасности маршрутизации в регионе, мы проанализировали покрытие сетей ROA, а затем внедрение ROV в Центральной Азии.

Уровень внедрения авторизации источника маршрута (ROA Coverage) в Центральной Азии

Внедрение ROA набирает значительную популярность во всем мире. Недавно мировое интернет-сообщество достигло важного рубежа: по данным NIST RPKI Monitor, более 50% глобального адресного пространства IPv4 теперь покрыто ROA. Это знаменует собой поворотный момент в усилиях по обеспечению глобальной безопасности маршрутизации, отражая растущее осознание операторами сетей важности RPKI в предотвращении угонов маршрутов BGP и ошибок конфигурации.

В контексте Центральной Азии охват ROA демонстрирует неоднородную картину. Уровни внедрения в странах региона варьируются от 10% до почти 100% как для адресного пространства IPv4, так и для IPv6. Такая большая вариативность говорит о том, что в то время как некоторые сети в Центральной Азии находятся на передовой внедрения этих мер безопасности, другие все еще находятся на начальных этапах реализации.

Значительная часть охвата, который мы видим в Кыргызстане и Туркменистане, была достигнута за последние два года. В Кыргызстане компания Mega-line внедрила ROA в свое IPv4 пространство в марте и декабре 2022 года, а Kyrgyztelecom завершил внедрение ROA в мае того же года. В Туркменистане Turkmentelecom завершил внедрение ROA в непокрытое адресное пространства в мае 2023 года, что привело к почти 100% охвату пространства IPv4 (см. график).

В Узбекистане уровень охвата ROA увеличился в апреле 2019 года, когда Sarkor Telecom внедрил ROA. Следующий скачок произошел в мае 2024 года, когда компания Turon Media также внедрила ROA. В Таджикистане, уровень внедрения увеличился на 10%, когда Zet Mobile (ранее известная как Tacom) добавила ROA в свое IP пространство.

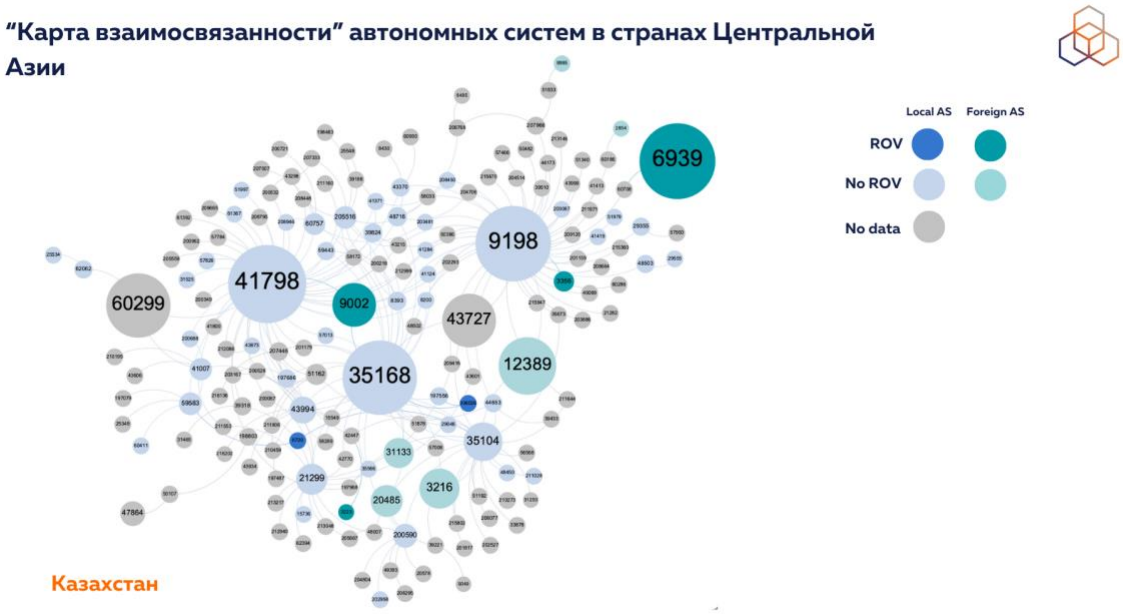
Проверка происхождения маршрута (ROV) и взаимодействие автономных систем

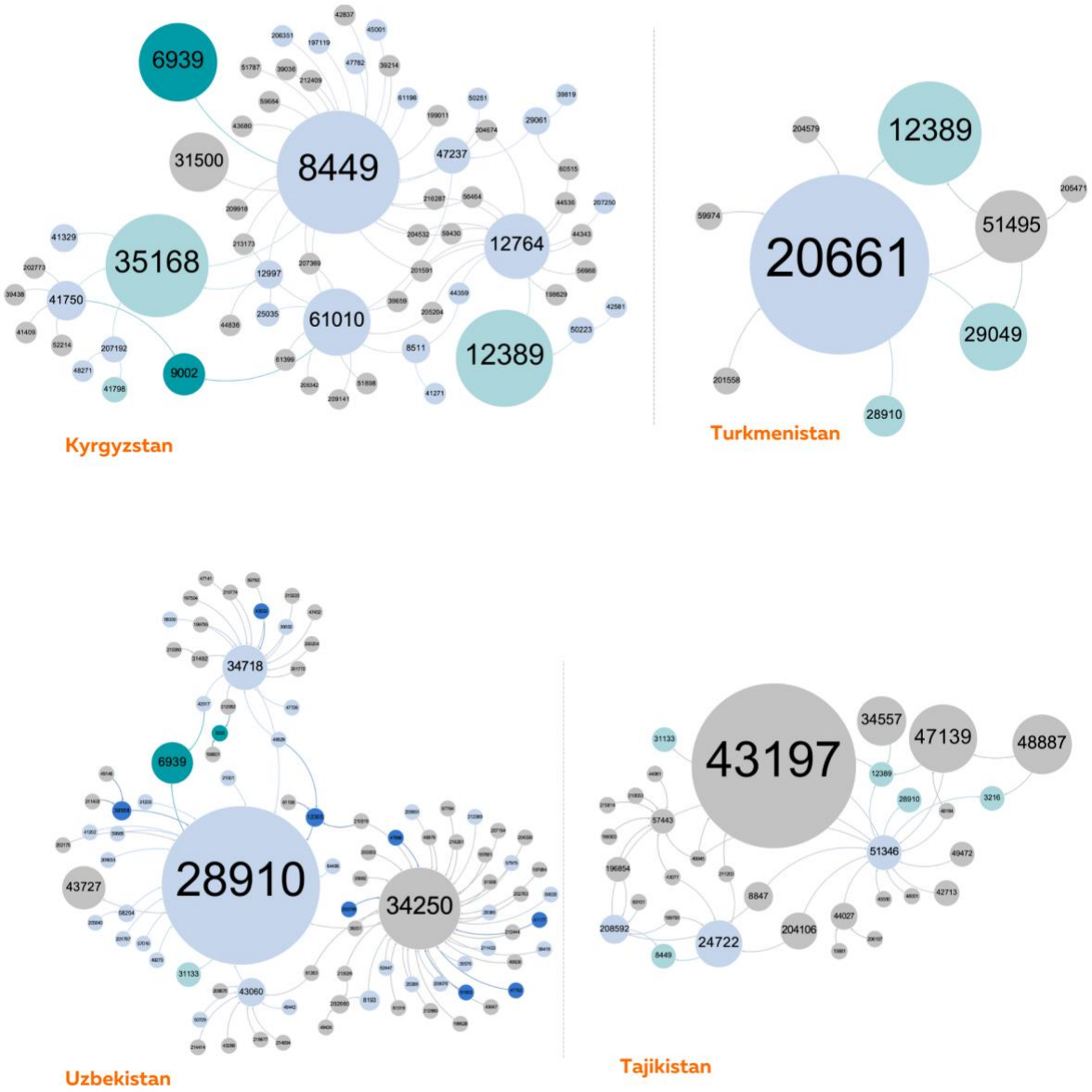
Как «второй шаг» в обеспечении безопасности маршрутизации через систему RPKI, ROV проверяет, соответствуют ли объявления о маршрутах авторизациям, указанным в ROA.

Мы проанализировали внедрение ROV в регионе с помощью инструмента RoVISTA, который рассчитывает оценки на основе количества недействительных префиксов RPKI, которые может достичь автономная система (AS).

Мы оценили влияние ROV с точки зрения центральности сети, используя методологию AS Hegemony для измерения центральности автономных систем в пределах страны. Результаты визуализированы таким образом, что размер каждой AS указывает на то, насколько центральную роль эта сеть играет в маршрутизации Интернета:

На графиках ниже можно увидеть, что относительно небольшая группа автономных систем (AS) в регионе играет особенно важную роль в ландшафте маршрутизации. Внедрение ROV особенно важно для таких сетей. Оно не только помогает защитить их собственных клиентов, но и, когда крупные AS внедряют ROV, они автоматически защищают меньшие, напрямую подключенные сети от угроз маршрутизации. Этот побочный эффект подчеркивает важность принятия ROV крупными операторами связи для улучшения общей экосистемы безопасности межсетевых взаимодействий.





Однако визуализации также показывают, что большинство центральных сетей в Центральной Азии пока не внедрили ROV, даже в тех странах, где уровень внедрения ROA уже достаточно высокий. Это может быть связано с нехваткой знаний о внедрении ROV, как указали респонденты последнего опроса RIPE NCC (опро был проведен среди членов RIPE NCC в Европе, Ближнем Востоке и Центральной Азии в 2023 году).

Инициативы по внедрению RPKI на государственном уровне

Принятие RPKI, включая реализацию ROA и ROV, все больше признается как критически важное не только сетевыми инженерами, но и на уровне правительств.

Политики играют значительную роль в ускорении внедрения этих мер безопасности и усилении общей устойчивости интернет-инфраструктуры.

В соединенных Штатах например, Белый дом выпустил дорожную карту, в которой RPKI рассматривается как зрелое решение для устранения уязвимостей, связанных с BGP. Этот всеобъемлющий план описывает действия для всех поставщиков сетевых услуг, включая тех, кто управляет корпоративными сетями или владеет IP-ресурсами.

Кроме того, Федеральная комиссия по связи США (FCC) ранее рекомендовала поставщикам интернет услуг разработать и ежегодно обновлять дорожную карту по управления рисками связаннами с BGP безопасностью. Эти планы должны включать стратегии для внедрения ROA и ROV.

Эти действия подчеркивают роль правительств в усилении безопасности маршрутизации. Внедряя аналогичные инициативы, правительства региона могут предпринять несколько важных шагов, таких как установление четких руководящих принципов и сроков для принятия RPKI среди интернет-провайдеров и других сетевых операторов.

Развитие IPv6 в регионе

С быстрым экономическим ростом в Центральной Азии операторам важно инвестировать в решения, ориентированные на будущее. Помимо стратегий безопасности, необходимо расширять мощности для поддержки большего числа пользователей, где ключевую роль играет IPv6. Переход на IPv6 — решение для долгосрочного роста интернета, учитывая ограниченность IPv4 ресурсов.

Мы изучили способность и и уровень внедрения IPv6 в регионе. В среднем процент автономных систем (ASNs), поддерживающих IPv6 (определяемых как процент ASNs, маршрутизирующих хотя бы один префикс IPv6), остается низким в Центральной Азии — около 18%. Для сравнения, в странах ЕС этот показатель составляет около 39%, что подчеркивает значительный разрыв в готовности к внедрению IPv6. Небольшой рост способности использования IPv6 был отмечен в Казахстане, Таджикистане и Узбекистане по сравнению с предыдущим годом, что свидетельствует о некоторых улучшениях.

Хотя способность использования IPv6 показывает, объявляются ли выделенные префиксы IPv6 в глобальных таблицах маршрутизации, внедрение IPv6 отражает, действительно ли пользователи используют IPv6 в своих сетях. Это различие важно для определния реального уровн внедрения IPv6.

Данные крупных контент-провайдеров (CDN) показывают разные уровни внедрения IPv6 в странах Центральной Азии и соседних регионах. Казахстан лидирует в регионе с показателями внедрения в диапазоне от 13% (Facebook) до 17% (Cloudflare и Google), что отражает различия между сетями внутри страны. В Кыргызстане эта цифра составляет около 4%, а в Узбекистане — примерно 3%. Обе страны демонстрируют более низкие уровни внедрения по сравнению с Казахстаном.

Интересно, что соседний Иран, демонстрирует значительно более высокие, но непоследовательные показатели внедрения IPv6: 76% (Facebook), 22,6% (Cloudflare) и 16% (Google). Эти значительные расхождения подчеркивают важность понимания методологий измерения, используемых различными CDN. Cloudflare рассчитывает процент использования IPv6 как (запросы IPv6 / запросы для контента с двойной стековой структурой), предоставляя специфическую метрику использования IPv6 среди клиентов, способных использовать как IPv4, так и IPv6. Что касается Google и Facebook, их методология расчета показателей внедрения менее прозрачна, что может способствовать вариациям в представленных данных.

Несмотря на различия в методах измерения, в среднем показатели внедрения IPv6 в Центральной Азии довольно низкие.

Согласно опросу RIPE NCC 2023, ниже представлены некоторые факторы, влияющие на медленное внедрение IPv6 среди респондентов из Европы, Ближнего Востока и Центральной Азии.

- Обеспечение функционального паритета между IPv4 и IPv6 является основной проблемой при внедрении IPv6 для 46% респондентов, причем эта цифра увеличивается до более чем половины в Центральной Европе (54%) и Евразии (56%).
- 41% респондентов отметили, что им необходимо изменить мышление в отношении IPv4 в своих организациях, особенно в Германии (56%) и Польше (61%).
- Около 40% респондентов отметили трудности с получением знаний о конкретных внедрениях, что говорит о необходимости в дополнительной информации и/или обучении.

Эти данные подчеркивают сложную картину внедрения IPv6 не только в Центральной Азии, но и в других регионах. Внедрение данной технологии требует скоординированных усилий через политические инициативы, инвестиции в инфраструктуру и повышение осведомленности.

Если вы хотите повысить свои знания о IPv6 и RPKI, ознакомьтесь с курсами в RIPE NCC Academy. Мы также опубликовали курс по основам IPv6 на русском языке и проведем тренинги, связанные с IPv6, в Бишкеке сразу после мероприятия — зарегистрируйтесь здесь.

Заключение

Внедрение ключевых технологий, таких как RPKI и IPv6, является важным шагом для обеспечения безопасного и стабильного интернета в Центральной Азии. По мере того как регион переживает быстрый цифровой рост, решение проблем маршрутизации через ROV и увеличение использования IPv6 становятся необходимыми шагами. Хотя прогресс был достигнут в реализации ROA, особенно в таких странах, как Кыргызстан и Туркменистан, остаются проблемы, такие как недостаток знаний и опасения по поводу ROV. Уделяя приоритетное внимание этим улучшениям, сети Центральной Азии смогут лучше подготовиться к угрозам маршрутизации и обеспечить долгосрочную цифровую устойчивость.

Мы будем рады услышать ваше мнение об этих исследованиях — пообщайтесь с нами на CAPIF 3. Это исследование представит главный исследователь RIPE NCC Касим Лоан во вторник, 24 сентября.

**перевод данной статьи был сделан с помощью ChatGPT*