CAPIF 4: Развитие интернет-технологий в Центральной Азии

В преддверии CAPIF 4 мы вновь решили изучить последние достижения в цифровой трансформации Центральной Азии. На фоне углубления регионального сотрудничества мы отслеживаем улучшения в безопасности маршрутизации и внедрении IPv6, а также исследуем модели взаимосвязи на основе данных K-root.

Возвращаясь в Казахстан на четвёртый Центральноазиатский форум по пирингу и связанности RIPE NCC (CAPIF 4), мы находим регион с углубляющимися связями и сильным осознанием своей роли в качестве важного цифрового перекрёстка. Региональное сотрудничество продвинулось за прошедший год благодаря пограничным соглашениям и торговым договорённостям, а международное взаимодействие продолжается через такие платформы, как ШОС, C5+1 и СНГ.

Быстрое развитие местного интернета продолжается ускоренными темпами, с явными признаками того, что регион настроен на формирование архитектуры своего собственного цифрового будущего. В своём недавнем Послании народу президент Казахстана Касым-Жомарт Токаев изложил планы по превращению Казахстана в «полностью цифровую нацию» в течение трёх лет, указав на серьёзный стратегический фокус на внедрении ИИ. Тем временем стратегия «Узбекистан-2030» ставит целью превращение страны в региональный IT-хаб, при этом, по оценкам, в этот сектор уже инвестировано около 3 миллиардов долларов в последние годы.

Цель нашего исследования — вновь наметить новый набор данных для отслеживания траектории цифровой трансформации Центральной Азии. Мы будем искать улучшения в безопасности маршрутизации — особенно с точки зрения развёртывания ROA и ROV — и внедрения IPv6 со времён CAPIF 3. Мы изучим правительственную инфраструктуру и внедрение RPKI в правительственных доменах. И мы будем изучать распределение DNS-

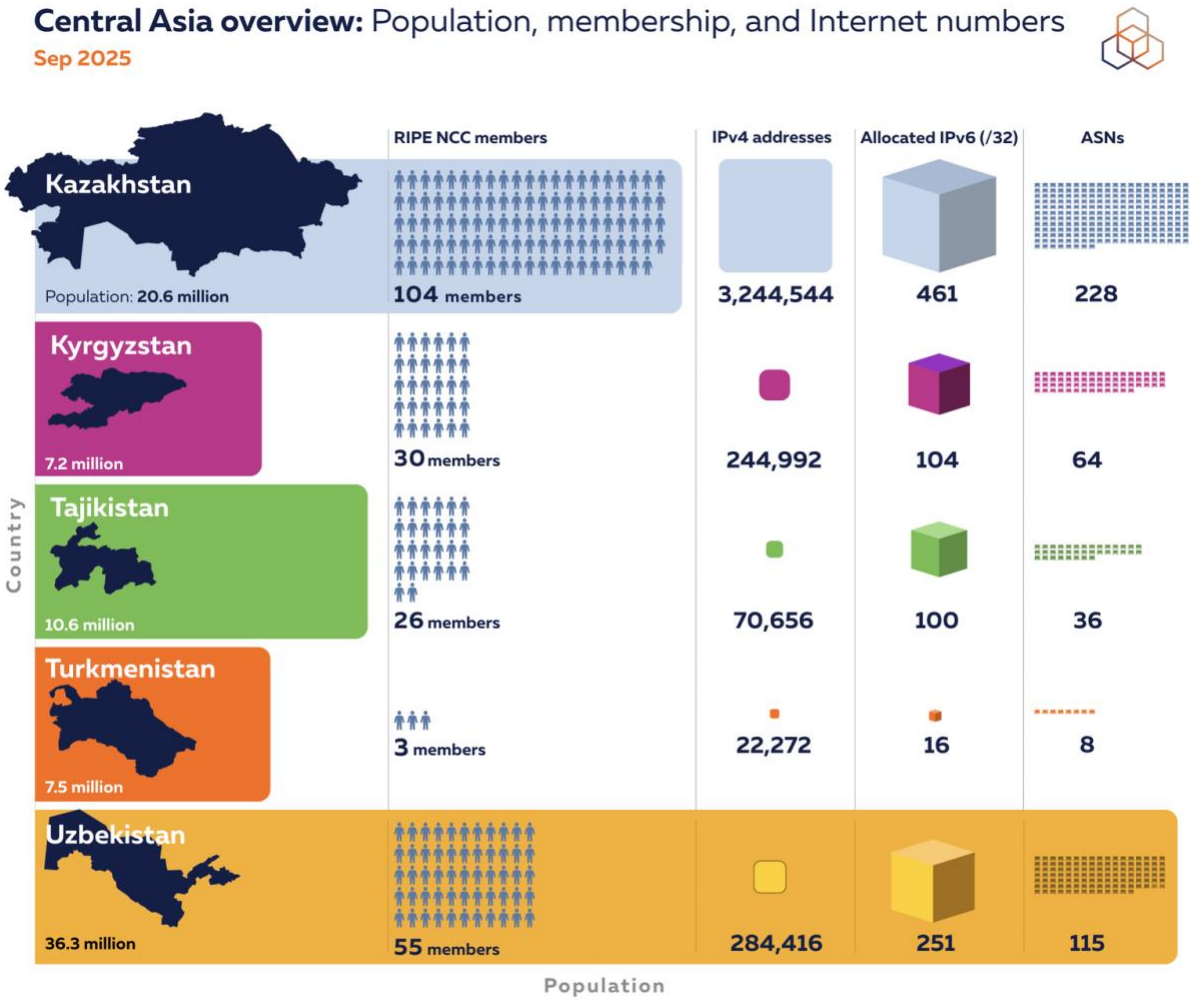
запросов по сети K-root anycast для картирования основных предпочтений BGP-маршрутизации региона и локализации трафика. Как и в предыдущих отчётах, мы также будем отслеживать аналогичные разработки в Иране — активном участнике CAPIF с самого начала, чья география позиционирует его как шлюз, связывающий не имеющую выхода к морю Центральную Азию с Ближним Востоком и Европой, что делает его ключевым заинтересованным лицом в устойчивой взаимосвязи в регионе.

Обзор ресурсов в Центральной Азии

IP-адреса являются критически важными элементами нашего связанного мира, служа необходимыми уникальными идентификаторами для каждого устройства, подключённого к интернету.

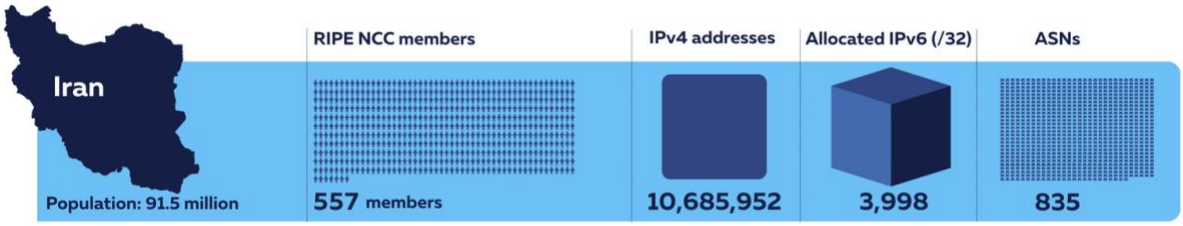
В условиях ускоряющегося цифрового роста Центральной Азии доступность ресурсов как IPv4, так и IPv6 становится всё более важной для удовлетворения растущего спроса. Исчерпание IPv4 (подробнее об этом здесь) делает переход на IPv6 необходимым для обеспечения будущего роста.

Анализ распределения ресурсов выявляет значительные региональные диспропорции. Казахстан показывает самое высокое соотношение членов RIPE NCC к населению в регионе, за ним следует Кыргызстан. Напротив, Узбекистан, несмотря на большее население, демонстрирует более низкое соотношение членов к населению и меньше выделенных IPv4-адресов на душу населения. Однако его выделение IPv6 на одного члена сопоставимо с соседями, что указывает на готовность к будущему расширению сети.



Source: RIPE NCC Inernet Registry data as of September 2025; Population figures from World Bank, 2024; visualisations created with Flourish Studio.

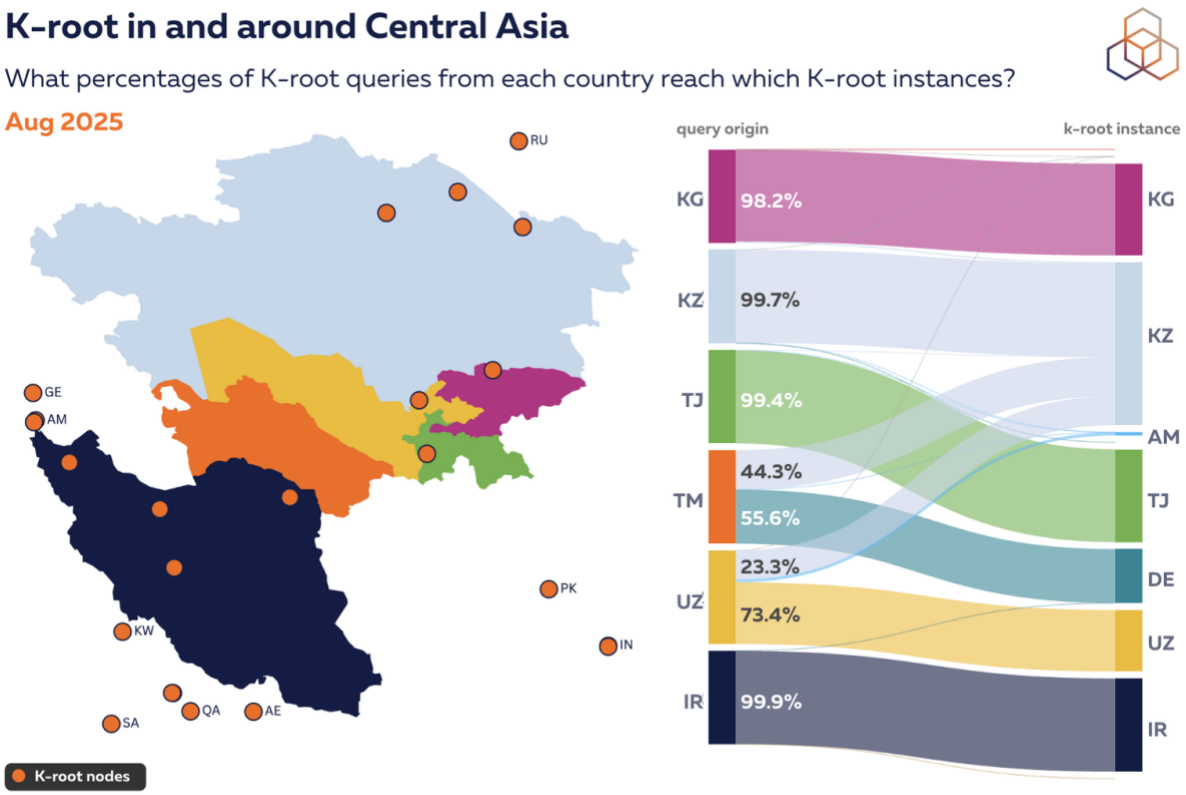
В другом масштабе сетевой ландшафт Ирана значительно больше. Он владеет значительно большим адресным пространством IPv4 и IPv6 и обладает большим количеством активных номеров автономных систем (ASN). Это отражает более зрелую и плотно взаимосвязанную интернет-экосистему по сравнению с центральноазиатскими странами.



K-root и взаимосвязанность

DNS сопоставляет человекочитаемые доменные имена с машиночитаемыми IP-адресами. RIPE NCC управляет K-root, одним из 13 авторитетных корневых серверов для корневой зоны DNS.

Чтобы понять интернет-связность, мы изучили DNS-запросы, отправленные от резолверов каждой страны в глобальную anycast-сеть K-root. K-root, управляемый RIPE NCC, является фундаментальной частью инфраструктуры интернета, его серверы отвечают за первый шаг в разрешении большинства доменных имён. Наблюдая, какой конкретный экземпляр сервера K-root отвечает на запрос, мы можем картировать основные предпочтения BGP-маршрутизации страны, выявляя, локализован ли её интернет-трафик или распределён по различным региональным и международным хабам.



Source: RIPE NCC K-root data: https://www.ripe.net/analyse/dns/k-root/; visualisations created with Flourish Studio.

По всей Центральной Азии и в соседних странах, которые размещают свои собственные сервера K-root, таких как Иран, Казахстан и Таджикистан, паттерны трафика весьма однородны на 1 августа 2025 года. График показывает распределение запросов от IP-адресов

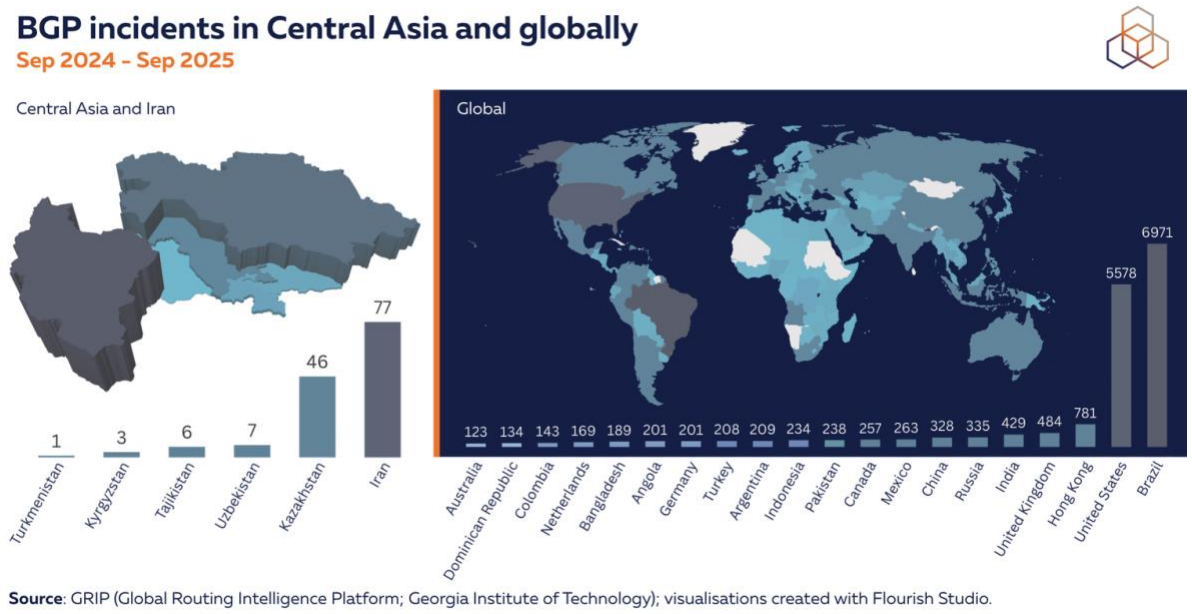
резолверов, геолоцированных с помощью IPinfo, к экземплярам K-root, которые обрабатывают их трафик. В этих странах подавляющее большинство запросов обслуживается местным экземпляром, что отражает сильные внутренние зоны охвата.

Узбекистан выделяется: на ту же дату примерно две трети запросов достигли экземпляра в UZ, в то время как около трети обслуживались экземпляром в Казахстане, с меньшей долей, направленной в Армению. Туркменистан, напротив, не имеет местного экземпляра, и его трафик разделён между экземплярами в Казахстане и Германии. Наш анализ, основанный на IP-адресах резолверов, а не на прямом трафике конечных пользователей, подчёркивает заметный контраст с соседними странами. Хотя геолокация на основе IP может вносить некоторую неопределённость, различия в поведении зон охвата остаются поразительными. Мы более подробно рассмотрим потенциальные движущие силы этих паттернов во время презентации. *Чтобы узнать больше, посмотрите презентацию Джеймса Кауи 25 сентября на CAPIF 4.*

Безопасность маршрутизации

RPKI позволяет держателям адресного пространства IP публиковать авторизации происхождения маршрутов (ROA), которые указывают, какие AS авторизованы для оригинирования их префиксов. Через валидацию происхождения маршрута (ROV) сети проверяют BGP-анонсы против опубликованных ROA, позволяя им отклонять анонсы с неавторизованными AS происхождения и тем самым смягчать захваты префиксов и определённые неправильные конфигурации происхождения.

RPKI предоставляет криптографическую структуру, которая позволяет операторам проверять, соответствуют ли BGP-анонсы авторизациям происхождения, опубликованным держателями префиксов. Ниже мы показываем инциденты происхождения BGP-маршрутов в Центральной Азии и соседних странах, как их видит Глобальная платформа маршрутной разведки (GRIP). Каждый инцидент учитывается один раз на страну, используя уникальный ID события GRIP вместе с набором вовлечённых ASN (как оригинирующих, так и покрытых/затронутых).



GRIP обеспечивает наблюдаемость в режиме, близком к реальному времени, за подозрительными событиями BGP-маршрутизации, включая:

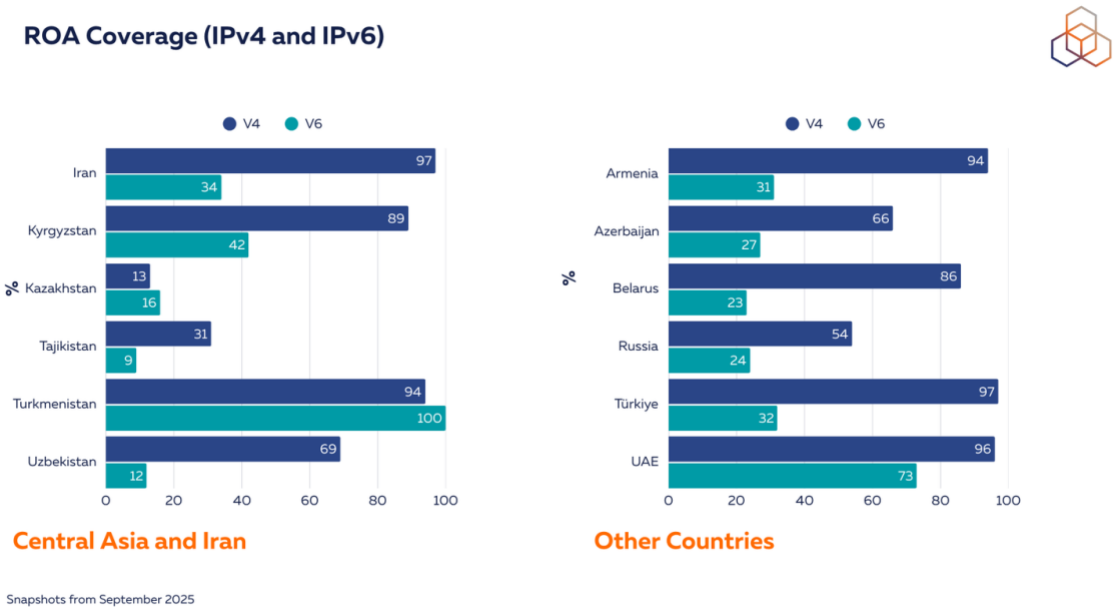
- MOAS (Multiple Origin AS): когда один и тот же префикс анонсируется более чем одной AS
- Sub-MOAS: событие, при котором AS анонсирует более специфический префикс, который находится внутри покрывающего префикса, анонсированного другой AS

Наш анализ фокусируется на событиях MOAS и Sub-MOAS, поскольку они могут быть смягчены с помощью RPKI, когда обнаруживаются недействительные происхождения, ограничивая их распространение в сетях, которые применяют валидацию происхождения маршрута. Для добавления географического контекста каждый вовлечённый ASN аннотируется страной его регистрации, как записано в базе данных RIPE. Мы отмечаем, что страна регистрации не обязательно отражает, где AS работает.

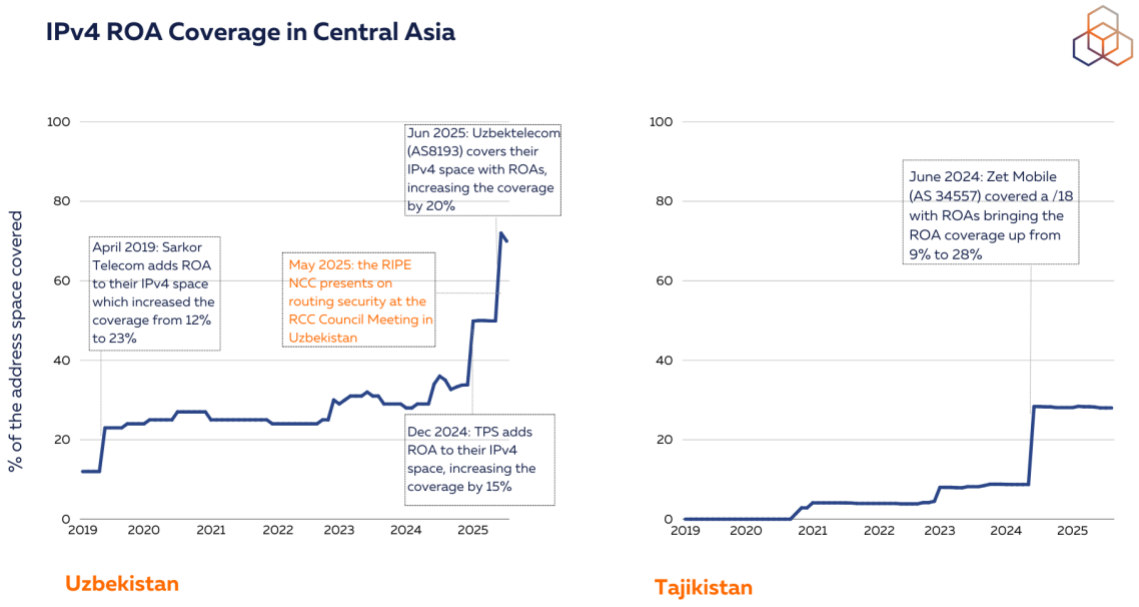
Хотя количество инцидентов в Центральной Азии и Иране относительно невелико по сравнению с глобальными показателями, принятие правильных решений по безопасности маршрутизации сейчас поможет обеспечить стабильную экосистему маршрутизации по мере взросления интернета региона.

Покрытие ROA

В настоящее время покрытие ROA в регионе варьируется по странам, с очень небольшими изменениями с нашего последнего отчёта.



Однако были заметные улучшения в покрытии IPv4 ROA Узбекистана, которое выросло с менее чем 40% в прошлом году до примерно 70% в этом году. В мае 2025 года RIPE NCC провёл взаимодействие по безопасности маршрутизации с узбекским Министерством цифровых технологий и выступил на заседании Совета операторов RCC, которое проходило в Ташкенте.



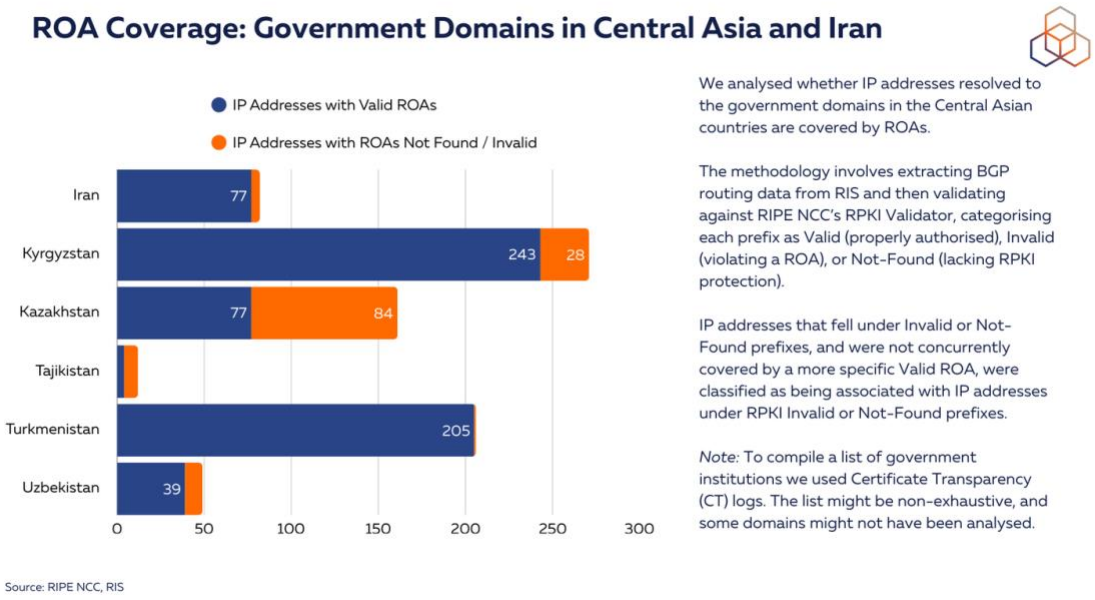
Туркменистан, Кыргызстан и Иран имеют очень высокий уровень покрытия ROA для своего адресного пространства IPv4. Тем временем для Казахстана и Таджикистана это остаётся низким. Важно отметить, что мы измеряем покрытие в % адресного пространства, поэтому цифры относительны к ресурсам, зарегистрированным в каждой стране.

Защита цифровой инфраструктуры для правительственных доменов

По мере того как страны региона ускоряют свои цифровые повестки во всех секторах, от электронного правительства до основных услуг, становится критически важным, чтобы правительственная инфраструктура была как устойчивой, так и безопасной. Большинство правительственных веб-сайтов в Центральной Азии зарегистрированы под национальными доменами второго уровня '.gov' (например: .gov.kg; .gov.uz). В этом году в Узбекистане было объявлено, что с 1 марта все официальные веб-сайты государственных органов в Узбекистане начали работать исключительно на Правительственном портале (gov.uz) в рамках более широких реформ по цифровизации и безопасности. Это может помочь обеспечить более последовательный и централизованный подход к безопасности, предоставляя единую точку контроля для мониторинга, аудита и применения политики. Чтобы оценить безопасность этих доменов, мы хотели изучить их покрытие ROA. Для этого мы извлекли соответствующие данные BGP-маршрутизации из RIS, а затем провели валидацию с помощью валидатора RPKI RIPE NCC, категоризируя каждый префикс как Valid (правильно авторизованный), Invalid (нарушающий ROA) или Not-Found (отсутствующий защиту RPKI). IP-адреса, которые разрешались в эти домены и попадали под префиксы RPKI Invalid или Not-Found - и не были одновременно покрыты более специфичным Valid ROA - были классифицированы как принадлежащие к префиксам RPKI Invalid или Not-Found (чтобы увидеть, как мы составили список правительственных доменов, см. примечание внизу этой статьи).

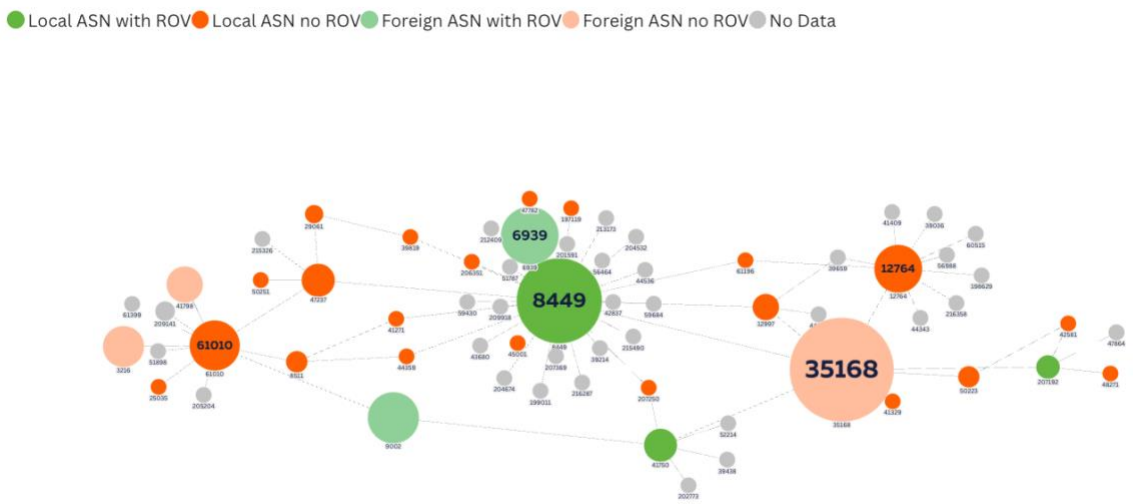
График ниже показывает количество IP-адресов за идентифицированными доменами, которые покрыты и не покрыты ROA. Результаты указывают на различные уровни принятия ROA среди правительственных доменов в проанализированных странах.

Например, в Иране из 114 протестированных доменов и поддоменов (82 IP-адреса) только 5 не были покрыты ROA. В Казахстане из 420 протестированных доменов и поддоменов (271 IP-адрес) 238 (84 IP-адреса) не были покрыты.



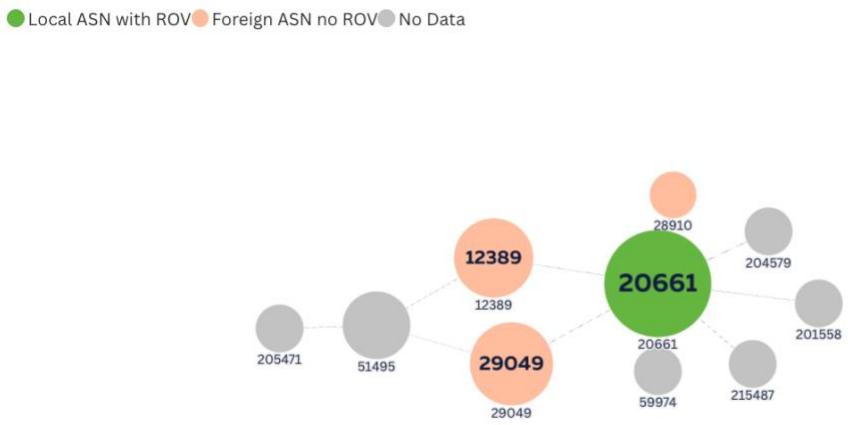
ROV: От авторизации к валидации

Для анализа развёртывания и влияния ROV в регионе мы объединили данные из RoVISTA с представлением о централизованности сети, полученным из методологии AS Hegemony, подхода, который даёт нам меру централизованности автономных систем внутри страны.
На основе того, что мы видим в данных RoVISTA, кажется, произошли позитивные изменения как в Кыргызстане, так и в Туркменистане. В Кыргызстане сети, такие как ElCat (AS8449) и Megaline (AS41750) — или их апстримы — похоже, развёртывают ROV. Elcat также имеет особенно высокий показатель гегемонии, что предполагает, что он играет значительную роль для взаимосвязи в стране. Развёртывая ROV (сами или через своих апстримов), они создают существенные сопутствующие выгоды, повышая безопасность маршрутизации для своих даунстрим-сетей, будь то от злонамеренных захватов происхождения префикса или случайных неправильных конфигураций.



Карта взаимосвязанности Кыргызстана

Согласно RoVista, ROV теперь виден в путях, включающих Turkmentelecom в Туркменистане, что предполагает, что недействительные анонсы фильтруются либо самим Turkmentelecom, либо одним из его апстрим-провайдеров. Однако важно отметить, что данные ROV могут иметь искажения, так как показатель может значительно варьироваться изо дня в день.



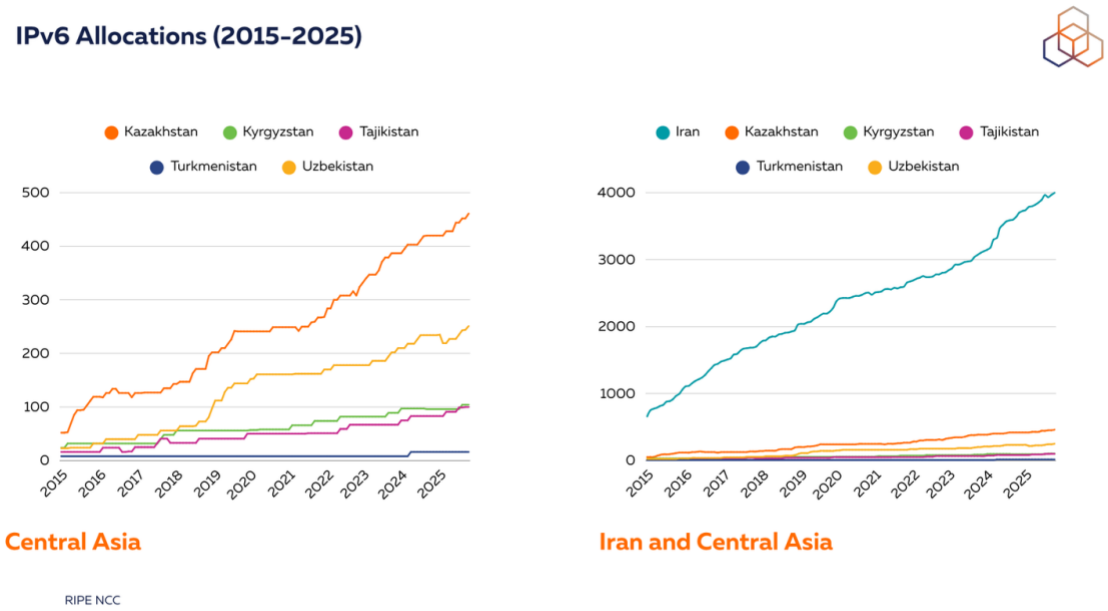
Карта взаимосвязанности Туркменистана

Чтобы помочь вам изучить эти данные дальше, посмотрите на эту интерактивную версию вышеприведённой визуализации в Flourish Studio.

Улучшение безопасности маршрутизации в Центральной Азии — это общая ответственность. Сетевые операторы играют центральную роль, но правительства и отраслевые органы могут поддерживать прогресс через политику, обучение и информационную работу. По мере того как цифровая инфраструктура в регионе продолжает расширяться, последовательная реализация мер безопасности маршрутов, таких как RPKI, будет необходима для поддержания стабильности и доверия в глобальной системе маршрутизации.

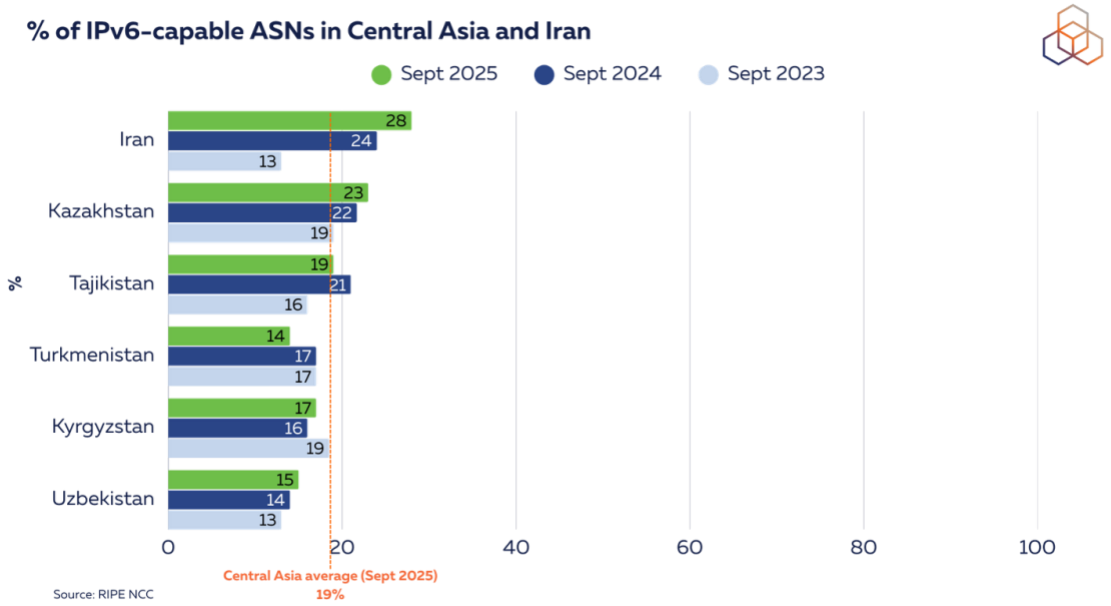
Внедрение IPv6

Выделения IPv6 неуклонно росли в регионе в последние годы. Иран имеет значительно больше выделений IPv6, чем пять центральноазиатских республик (см. график ниже для сравнения), подчёркивая как масштаб его интернет-рынка, так и более сильное стремление к развёртыванию IPv6 его операторами. Однако устойчивый рост по всей Центральной Азии предполагает растущую готовность к принятию IPv6 и будущей интеграции в глобальную интернет-экосистему.

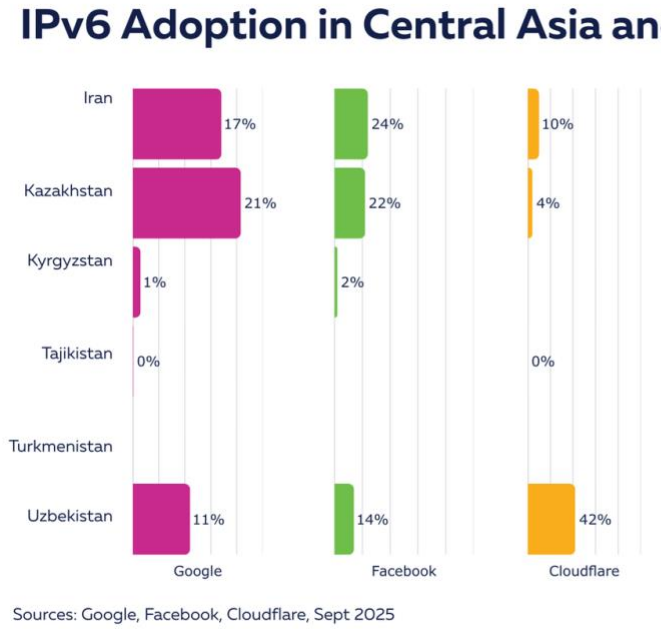


Возможность IPv6 по странам, определяемая как процент ASN, маршрутизирующих хотя бы один префикс IPv6

Со времён CAPIF 3 не было поразительных изменений в возможностях IPv6. Иран по-прежнему лидирует с 28%, за ним следует Казахстан с 23% и Таджикистан с 19%. Средняя возможность по региону увеличилась всего на 1% в этом году до 19%.



Хотя возможность IPv6 указывает на готовность сетей использовать IPv6, фактическое внедрение нелегко измерить. Мы изучили измерения, сообщённые некоторыми крупными сетями доставки контента (CDN) о внедрении IPv6 в регионе. Недавние данные выявляют различные уровни внедрения IPv6 в Центральной Азии и Иране. Казахстан и Иран лидируют во внедрении IPv6 с различными уровнями, сообщаемыми Google, Facebook и Cloudflare. Ускорение IPv6 в последнем в основном обусловлено Советом IPv6, национальным органом, продвигающим лучшие практики для развёртывания IPv6. В Узбекистане внедрение IPv6 составляло 0% по состоянию на сентябрь 2024 года, хотя усилия в этом направлении были официально запущены в предыдущем году через сотрудничество между RIPE NCC и национальным телекоммуникационным оператором Uzbektelecom. По состоянию на сентябрь 2025 года уровень внедрения значительно вырос до 14%, отражая реальный прогресс в развёртывании.



К устойчивому и безопасному интернету Центральной Азии

Интернет Центральной Азии быстро развивается, формируемый как сильными национальными амбициями, так и растущим региональным сотрудничеством. Прогресс в безопасности маршрутизации — через более широкое покрытие ROA и начальные шаги в развёртывании ROV в Туркменистане и Кыргызстане — подчёркивает укрепляющуюся приверженность устойчивости. Быстрый рост Узбекистана во внедрении IPv6 и улучшения в безопасности маршрутизации по всему региону отражают растущую приверженность со стороны правительств, операторов и международных партнёров. Конечно, проблемы остаются. Но импульс очевиден: Центральная Азия позиционирует себя как активного игрока в формировании безопасного, связанного и готового к будущему цифрового ландшафта.

Присоединяйтесь к нам на четвёртом издании Центральноазиатского форума пиринга и взаимосвязи (CAPIF 4), чтобы стать частью дискуссии о будущей устойчивости и взаимосвязи в Центральной Азии.

Примечание о методологии

Для составления списка правительственных доменов мы использовали журналы прозрачности сертификатов (CT), которые являются общедоступными записями всех выданных SSL/TLS-сертификатов. Основным инструментом для этого является crt.sh, веб-интерфейс, который позволяет искать в этих обширных журналах. Методология включает запрос crt.sh с поиском по шаблону для конкретного правительственного домена верхнего уровня, например %.gov.xx. Этот начальный запрос извлекает все сертификаты, выданные для поддоменов под этим родительским доменом. Необработанные данные из этих сертификатов, включая общие имена и альтернативные имена субъектов, затем систематически извлекаются и нормализуются. Это включает очистку данных путём удаления префиксов с подстановочными знаками (например, преобразование *.example.gov в example.gov), разделение записей, содержащих несколько доменных имён, и стандартизацию текста для создания чистого, дедуплицированного списка уникальных правительственных имён хостов.