УДК 004.056.53:004.7

Козырев Владислав Сергеевич
независимый исследователь

Давыдов Виталий Владимирович
независимый исследователь

МЕТОДИКА СОГЛАСОВАНИЯ КОНТРОЛЯ ДОСТУПА С МИГРАЦИЕЙ QUIC-СОЕДИНЕНИЯ МЕЖДУ СЕТЕВЫМИ АДРЕСАМИ

Аннотация. Рассматривается рассогласование транспортного состояния QUIC и сетевой политики при изменении IP-адреса или UDP-порта клиента. Показано, что проверка нового пути посредством PATH_CHALLENGE и PATH_RESPONSE подтверждает достижимость заявленного транспортного адреса, но не отвечает на вопрос, сохраняется ли право субъекта обращаться к ресурсу из новой сетевой зоны. Использование пяти параметров потока нарушает непрерывность мобильного соединения и создает новые квоты при смене адреса; пассивное связывание по Connection ID ненадежно, поскольку идентификаторы меняются и согласуются в зашифрованных кадрах. Предложены формальный инвариант допуска, конечный автомат миграции и архитектура согласованного контроля на QUIC-терминаторе. Решение объединяет подтвержденный путь, текущую зону, идентичность субъекта, версию политики и стабильный ключ квоты. В вычислительном эксперименте выполнено 400 000 трасс для пяти сценариев и четырех политик. В авторской условной модели предложенная политика сохранила 97,920% легитимных миграций, не допустила успехов в 40 000 трассах смены зоны и отзыва политики и исключила прием запросов сверх единого лимита. Медианная добавленная задержка составила 39,877 мс. Результаты характеризуют архитектурные альтернативы при заданных предположениях и не являются статистикой реальных инцидентов.

Ключевые слова: QUIC, HTTP/3, миграция соединения, NAT rebinding, контроль доступа, Connection ID, Path Validation, сетевая зона, PDP, PEP, ограничение частоты запросов.

ALIGNING ACCESS CONTROL WITH QUIC CONNECTION MIGRATION BETWEEN NETWORK ADDRESSES

Abstract. The paper examines inconsistency between QUIC transport state and network access policy when a client changes its IP address or UDP port. PATH_CHALLENGE and PATH_RESPONSE establish reachability of a claimed transport address, but do not determine whether a subject remains authorized to access a resource from the new network zone. Five-tuple state breaks mobility and creates fresh rate-limit buckets after address changes, while passive Connection ID association is unreliable because identifiers can rotate through encrypted frames. The proposed method introduces a release-independent access invariant, a migration state machine, and a coordinated enforcement architecture at the QUIC terminator. The decision combines validated path state, current zone, subject identity, policy epoch, and a stable quota key. A reproducible computational experiment evaluates 400,000 traces across five scenarios and four policies. Under the stated authorial assumptions, the proposed policy preserved 97.920% of legitimate migrations, observed no unauthorized success in 40,000 forbidden-zone and policy-revocation traces, and rejected all requests above a stable subject/resource limit. Median added delay was 39.877 ms. These results compare architectures and must not be interpreted as measured incident frequencies.

Keywords: QUIC, HTTP/3, connection migration, NAT rebinding, access control, Connection ID, Path Validation, network zone, PDP, PEP, rate limiting.

Введение

Классическая сетевая функция связывает состояние соединения с пятью параметрами: адресом и портом источника, адресом и портом назначения и транспортным протоколом. QUIC отделяет логическое соединение от этого набора: Connection ID позволяет конечной системе продолжать сеанс после NAT rebinding, смены UDP-порта или перехода клиента между интерфейсами [6, 8].

Для мобильного пользователя это повышает непрерывность, но для контроля доступа возникает конфликт жизненных циклов. Транспорт считает соединение прежним, сетевой шлюз видит новый поток, а прикладной компонент может продолжать использовать решение, принятое для первоначального адреса.

Проблема не является предположением о слабости криптографии QUIC. TLS 1.3 интегрирован в протокол, а защищенные пакеты проходят проверку целостности [7]. Адресная проверка предназначена прежде всего для доказательства обратной достижимости и ограничения усиления трафика [6]. Она не подтверждает принадлежность нового адреса доверенной корпоративной зоне, актуальность роли пользователя или остаток общей квоты. HTTP/3 отдельно предупреждает, что реализации, использующие клиентский адрес для журналирования или контроля доступа, должны получать текущий адрес либо явно принять возможность его изменения [9].

Российские публикации рассматривают миграцию как средство сохранения HTTP/3-сеанса при смене сети [5], однако прикладная непрерывность и перенос авторизационного контекста требуют отдельного анализа. Интернет-измерения также показывают неоднородность поддержки миграции у серверов [16]. Следовательно, нельзя считать ни полный запрет мобильности, ни ее прозрачное наследование универсальной политикой.

Цель работы состоит в разработке методики, сохраняющей доступность легитимной QUIC-миграции и одновременно не переносящей без проверки решения, зависящие от текущей сети или версии политики. Для достижения цели решаются четыре задачи: разделяются транспортная и авторизационная семантика пути; строится модель угроз; формулируется инвариант допуска; сравниваются четыре политики в воспроизводимом вычислительном эксперименте. Научная новизна заключается в совместной проверке подтвержденного пути, сетевой зоны, субъекта, эпохи политики и стабильного лимита запросов. В отличие от работ по восстановлению состояния middlebox, объектом является не только принадлежность пакетов соединению, но и допустимость продолжения конкретного доступа после изменения пути.

Нормативная и научная основа

ГОСТ Р ИСО/МЭК 27033-1-2011 рассматривает сетевую безопасность как защиту передаваемой информации, устройств, приложений, услуг и конечных пользователей и связывает архитектуру с идентифицированными рисками [1]. ГОСТ Р ИСО/МЭК 27033-2-2021 требует документировать проектирование и реализацию безопасности сети [2]. Для рассматриваемой задачи это означает необходимость явно описать, где хранится решение, какое событие делает его устаревшим и какой компонент может закрыть путь.

ГОСТ Р ИСО/МЭК 27033-4-2021 связывает шлюзы безопасности с документированной политикой, анализом угроз, мониторингом и проверкой [3]. Однако шифрование QUIC ограничивает пассивному шлюзу доступ к транспортным кадрам. ГОСТ Р ИСО/МЭК 27002-2021 задает риск-ориентированный выбор мер, включая управление доступом, журналирование и сетевую безопасность [4]. Эти документы не предписывают алгоритм обработки QUIC-миграции, но поддерживают принцип: решение должно соответствовать текущему контексту и быть проверяемым.

RFC 9000 определяет Connection ID, NAT rebinding, активную миграцию клиента и Path Validation. При обнаружении нового адреса конечная система должна проверить путь, если он ранее не был подтвержден; намеренная миграция должна использовать новый Connection ID, чтобы уменьшить связываемость трафика [6]. RFC 8999 фиксирует версионно-независимую функцию Connection ID: изменения UDP/IP-адресации не должны доставлять пакет неправильной конечной системе [8]. RFC 9308 уточняет, что Path Validation требует как минимум одного RTT и после миграции сбрасывается состояние управления перегрузкой [10]. QUIC v2 не меняет свойства безопасности и конфиденциальности QUIC v1, поэтому сформулированная задача сохраняется и для второй версии [12].

Видимый Connection ID не является универсальной заменой пяти параметрам потока. RFC 9312 отмечает, что новый идентификатор может быть согласован в зашифрованном кадре, а одинаковые или разные CID не дают

пассивному наблюдателю безусловной связи потоков. Использовать CID как ключ stateful-решения на произвольном промежуточном устройстве не рекомендуется: смена идентификатора может привести к невосстановимой потере состояния [11]. Поэтому предлагаемая методика размещает точку принудительного применения на QUIC-терминаторе или явно координированном ingress-компоненте, имеющем доступ к состоянию соединения.

NIST SP 800-207 разделяет Policy Decision Point и Policy Enforcement Point и не допускает неявного доверия только по сетевому расположению [13]. NIST SP 800-207A переносит гранулярные решения к API-шлюзам и прокси, объединяя идентичность приложения с сетевыми атрибутами [14]. Для QUIC это позволяет не выбирать между «IP решает все» и «IP не учитывается»: сеть выступает одним из атрибутов, который должен быть обновлен после подтверждения нового пути.

Исследования безопасности QUIC выявляют различия зрелости реализаций и необходимость проверять не только текст стандарта, но и поведение конкретных стеков [15]. MIMIQ демонстрирует, что клиент способен намеренно менять адрес внутри одного QUIC-соединения, следовательно, IP-адрес нельзя считать постоянным идентификатором субъекта [18]. SMAQ передает транспортное состояние доверенному middlebox, но прямо оставляет авторизацию, подотчетность и аудит открытыми задачами [17]. QASM исследует нарушение NAT, балансировки и ограничения частоты при миграции и предлагает QUIC-aware-сопоставление потоков [19]. Настоящая работа дополняет эти направления проверяемым условием сохранения права доступа и не требует раскрывать прикладное содержимое пассивному шлюзу.

Семантический разрыв при миграции

Пусть установленное соединение c связано с аутентифицированным субъектом s и ресурсом r. Начальный путь p0 имеет транспортный адрес a0 и классифицирован как корпоративная зона z0. Политика разрешает действие, после чего приложение кэширует решение d0. При NAT rebinding меняется

только порт; при handover могут измениться адрес, интерфейс, оператор и зона. QUIC сопоставляет защищенный пакет с с и инициирует проверку p1, но прикладное решение d0 не получает новую семантику автоматически.

На рисунке 1 разделены три события. Первое — криптографическое распознавание пакета как части с. Второе — подтверждение обратной достижимости p1. Третье — решение о доступе из z1. Только третье сравнивает субъект, ресурс и актуальную политику. Если оно пропущено, соединение может сохранить право, выданное для z0. Если вместо этого шлюз безусловно требует прежний 5-tuple, легитимные NAT rebinding и handover будут блокироваться. Если лимит запросов создается заново для каждого tuple, намеренная смена адресов дает несколько независимых корзин, что экспериментально рассматривается и в QASM [19].

Рисунок 1. Разделение транспортной проверки пути и повторной авторизации

Нарушителем считается аутентифицированный либо скомпрометированный клиент, способный инициировать корректную миграцию и отвечать на PATH_CHALLENGE. Он не получает ключи другого соединения и не подделывает защищенные пакеты. Рассматривается также администратор политики, отзывающий право во время существования сеанса. Не исследуются компрометация QUIC-терминатора, TLS-библиотеки или PDP, анализ трафика и атаки на доступность Initial-пакетами. Такое ограничение отделяет авторизационный дефект от известных атак реализации [15].

Выделены пять сценариев. S1 — смена порта NAT в прежней разрешенной зоне. S2 — переход между корпоративной Wi-Fi и разрешенной мобильной зоной. S3 — продолжение чувствительной операции после перехода в запрещенную публичную зону. S4 — восемь последовательных адресов, используемых одним субъектом для получения новых квот. S5 — отзыв разрешения одновременно с миграцией внутри той же зоны. S1 и S2 проверяют доступность, S3–S5 — безопасность и свежесть решения.

Таблица 1. Сценарии миграции и проверяемые свойства

S	Событие	Переход	Класс	Проверяемое требование
S1	NAT rebinding	corp -> corp	легитимный	непрерывность; не создавать новое право или квоту
S2	Wi-Fi -> mobile	corp -> mobile	легитимный	Path Validation и разрешенная текущая зона
S3	переход в public	corp -> public	нарушитель с действующей сессией	запрет по текущей зоне
S4	8 адресов; 160 запросов	corp -> mobile	обход лимита по адресу	единая квота 100 для субъекта и ресурса
S5	отзыв политики	corp -> corp; epoch меняется	сессия с отмененным правом	проверка Fresh и текущей эпохи

Примечание: сценарии являются условиями авторской сравнительной модели, а не частотами реальных инцидентов.

Формальная модель допуска

Путь p описывается адресом a(p), зоной z(p) и состоянием v(p) ∈ {candidate, validated, failed}. Для соединения известны субъект s(c), ресурс r и подтверждение завершенного handshake H(c). Политика имеет текущую эпоху e(t), увеличиваемую при отзыве или изменении правил. Решение d содержит

время td и использованную эпоху ed. Стабильный ключ квоты не зависит от адреса и CID:

$$k(c, r) = \mathrm{Hash}(\mathrm{tenant} \,\|\, s(c) \,\|\, r \,\|\, e(t)).$$

Свежесть решения определяется равенством эпох и максимальным временем жизни Δd:

$$\mathrm{Fresh}(d, t) = (ed = e(t)) \wedge (t - td \leq \Delta d).$$

Инвариант допуска прикладного запроса q имеет вид:

$$\mathrm{Permit}(c, p, q, t) = H(c) \wedge \mathrm{Validated}(p) \wedge \mathrm{Policy}(s(c), r(q), z(p), e(t)) \wedge \mathrm{Fresh}(d, t) \wedge \mathrm{Budget}(k(c, r), t) > 0.$$

Инвариант различает доказательства. H(c) связывает пакет с криптографическим состоянием соединения; Validated(p) подтверждает обратную достижимость; Policy определяет право субъекта в текущей зоне; Fresh исключает наследование отмененного решения; Budget обеспечивает общий предел независимо от числа адресов и CID. Наличие первых двух условий не влечет истинность остальных.

Для оценки используются три показателя. U — условная доля принятых запросов в S3 и S5; L — доля продолженных легитимных миграций S1 и S2; E — доля принятых запросов сверх единого лимита в S4. Операционная цена выражается ложной блокировкой $F = 1 - L$ и задержкой ΔT между первым пакетом нового пути и решением PEP. Сравнение безопасно интерпретировать только условно по заданному набору сценариев.

$$U(\pi) = \mathrm{Naccept}(S3 \cup S5, \pi) / N(S3 \cup S5).$$

$$L(\pi) = \mathrm{Ncontinue}(S1 \cup S2, \pi) / N(S1 \cup S2).$$

$$E(\pi) = \mathrm{Nexcess\_accept}(S4, \pi) / \mathrm{Nexcess}(S4).$$

Сравниваемые политики и архитектура

Политика P0 отражает несогласованную реализацию: приложение наследует решение начального сеанса, а сетевой ограничитель создает корзину по 5-tuple. P1 получает текущий адрес и повторно проверяет зону, но не ожидает Path Validation и сохраняет квоту по tuple. P2 добавляет обязательное подтверждение пути, однако обновляет решение только при изменении зоны и

также создает адресные квоты. P3 реализует предложенный инвариант: новый путь помещается в карантин, подтверждается, классифицируется доверенным ingress, после чего PDP проверяет изменение зоны или эпохи, а лимит остается связанным с субъектом и ресурсом.

Таблица 2. Сравниваемые политики обработки нового пути

P	**Авторизационное состояние**	**Действие с путем**	**Ключ квоты**	**Ограничение / результат**
P0	кэш решения сеанса	без обязательной проверки	по 5-tuple	устаревшие права и новые квоты
P1	текущий адрес	без ожидания validation	по 5-tuple	видит смену зоны, пропускает epoch
P2	Path Validation + зона	обязательная	по 5-tuple	блокирует S3, пропускает S4/S5
P3	путь + зона + epoch	validation; карантин	субъект + ресурс + epoch	предложенный инвариант допуска

Архитектура P3 показана на рисунке 2. Внешний L4-шлюз выполняет грубую фильтрацию UDP и не пытается восстановить авторизационное состояние по произвольному CID. QUIC-терминатор является PEP и наблюдает подтвержденные транспортные события. Метка зоны поступает от управляемого ingress-интерфейса или подписанного контекста сетевой инфраструктуры; доверять сообщенному клиентом имени зоны нельзя. PDP принимает субъект, ресурс, зону, состояние устройства при наличии и эпоху правил. Единая quota-служба использует стабильный ключ, а журнал записывает старый и новый путь, идентификатор решения и причину разрешения либо запрета.

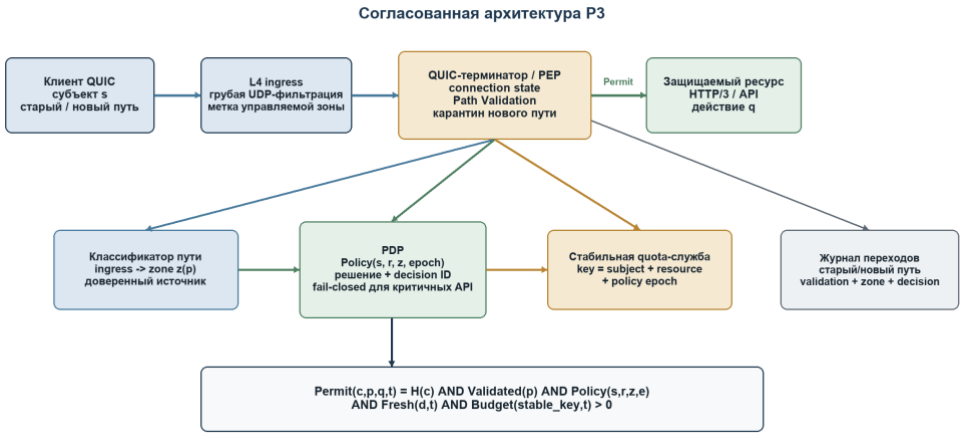

Рисунок 2. Архитектура согласованного контроля доступа при миграции QUIC

Автомат миграции имеет состояния ACTIVE, CANDIDATE, VALIDATING, REAUTH, ACTIVE_NEW и DENIED. Получение защищенного непроверенного пакета создает CANDIDATE, но прикладные действия на новом пути не выпускаются. Успешный PATH_RESPONSE переводит путь в REAUTH; отказ или исчерпание числа попыток — в DENIED при сохранении старого подтвержденного пути, если он еще доступен. При разрешении PDP квота не обнуляется и состояние становится ACTIVE_NEW. При запрете приложение может оставить соединение для нечувствительных ресурсов, закрыть его или потребовать усиленную аутентификацию. Это прикладное решение, а не требование RFC.

Параметр disable_active_migration допустим для сервисов, которым мобильность не нужна, но не заменяет модель: непреднамеренный NAT rebinding остается возможным, а будущий Multipath QUIC предусматривает несколько одновременно управляемых путей [20]. В расширении инвариант применяется отдельно к каждому path ID, тогда как субъект, эпоха политики и квота остаются общими.

Методика вычислительного эксперимента

Эксперимент реализован на Python 3.12.13 и NumPy 2.3.5 с фиксированным seed 20260819. Для каждой пары из пяти сценариев и четырех политик сформировано по 20 000 трасс, всего 400 000. Для U используются 40 000 трасс S3 и S5 на политику, для L — 40 000 трасс S1 и S2. В S4 каждый субъект

выполняет восемь миграций и посылает 160 запросов при едином допустимом лимите 100; 60 запросов считаются сверхлимитными.

RTT задается логнормально с медианами 24, 75, 65, 35 и 40 мс для S1–S5 и параметром формы от 0,40 до 0,55. Доля потерь формируется как 0,12·Beta(1,2; 30). Вероятность полностью непригодного пути принята от 0,004 до 0,015 в зависимости от сценария. Path Validation имеет не более трех попыток; одна попытка успешна при доставке challenge и response. Доступность PDP задана 0,996, классификатора зоны — 0,9995. Его задержка и задержка PDP логнормальны с медианами 0,45 и 2,4 мс. Все значения являются авторскими условными предположениями для сопоставления политик, а не частотами реальных отказов или атак.

Для долей U и L рассчитан 95%-й интервал Уилсона. P0 обрабатывает новый путь без дополнительного ожидания. P1 добавляет классификацию и обращение к PDP при изменении зоны. P2 и P3 включают RTT каждой попытки Path Validation; P3 также проверяет эпоху политики и стабильную квоту. Отказ зависимого компонента трактуется fail-closed. Такая модель намеренно не измеряет производительность конкретной QUIC-библиотеки и не подменяет interop-тестирование.

Отдельно выполнен локальный микробенчмарк четырех функций оценки состояния на Apple M5. Для каждой политики проведено 80 пакетов по 20 000 решений после прогрева. В памяти размещены таблицы соединения, пути, зоны, политики и квоты. Измерение не включает UDP, TLS, сетевой вызов PDP, сериализацию и журналирование, поэтому отражает нижнюю границу вычислительной цены словарных проверок, а не задержку промышленного PEP.

Результаты и обсуждение

Агрегированные результаты приведены в таблице 3. P0 сохранила 98,103% легитимных миграций, но условный U составил 97,950% [97,806–98,084%]: решение исходной зоны продолжало действовать как после перехода в публичную сеть, так и после отзыва политики. P1 блокировала S3 по текущей зоне, поэтому U снизился до 49,110%, однако S5 оставался успешным при

неизменившейся зоне. P2 добавила проверку пути, но без контроля эпохи получила сопоставимые 49,160%. Эти значения являются средним по двум равновзвешенным сценариям и не оценивают их распространенность.

Таблица 3. Агрегированные результаты вычислительного эксперимента

P	U, % [95% ДИ]	L, %	F, %	E, %	ΔT50, мс	ΔT95, мс	Bq, S4	t50, нс
P0	97,950 [97,806-98,084]	98,103	1,898	98,260	0,200	0,328	8	37,576
P1	49,110 [48,620-49,600]	97,735	2,265	97,815	1,330	4,969	8	63,832
P2	49,160 [48,670-49,650]	97,860	2,140	97,900	39,757	125,047	8	72,752
P3	0,000 [0,000-0,0096]	97,920	2,080	0,000	39,877	136,812	1	88,812

Примечание: U — успех несанкционированных S3/S5; L — непрерывность S1/S2; F — ложная блокировка; E — прием сверх единой квоты S4; ΔT — добавленная задержка; Bq — число корзин квоты в S4; t50 — локальный микротест функции решения. Вероятности относятся только к заданной авторской условной модели.

P3 не допустила ни одной успешной трассы в S3 и S5: U = 0 из 40 000, верхняя граница 95%-го интервала Уилсона равна 0,0096%. Нулевое наблюдение не доказывает нулевую вероятность; оно показывает, что при заданной модели инвариант детерминированно закрывает проверяемые пути. Легитимная непрерывность составила 97,920% [97,775–98,055%], ложная блокировка —

2,080%. Таким образом, P3 не получила статистически заметного ухудшения L относительно P2, интервалы политик перекрываются.

В S4 политики P0–P2 приняли соответственно 98,260; 97,815 и 97,900% запросов сверх единого лимита: каждая из восьми адресных корзин вмещала свою долю нагрузки. P3 сохранила одну корзину и не приняла сверхлимитные запросы. Результат не означает запрета сетевых квот: ограничения защиты канала и объемов UDP могут оставаться per-path, тогда как бизнес-лимит операции должен быть связан с устойчивой идентичностью.

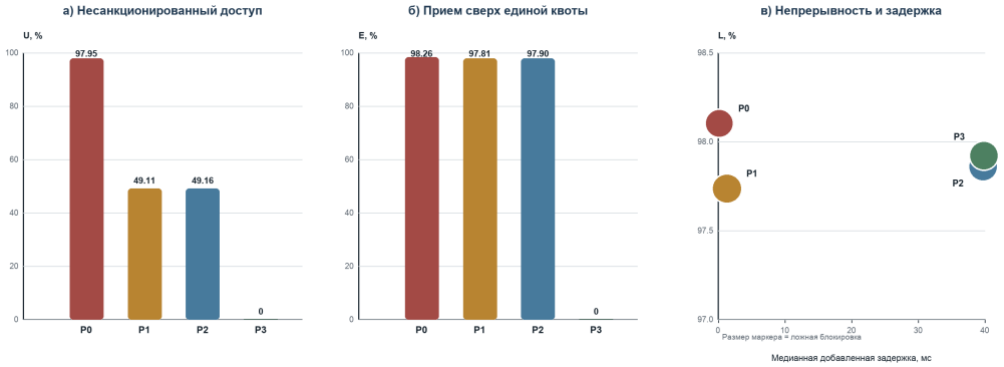

Рисунок 3. Результаты сценарного моделирования и цена согласованной политики

Медианная добавленная задержка P3 составила 39,877 мс, 95-й процентиль — 136,812 мс. Для P2 получены 39,757 и 125,047 мс; основную цену обеих политик формирует RTT проверки пути. P1 имела медиану 1,330 мс, но не обеспечивала транспортный gate. Локальный микробенчмарк дал медианы 37,576; 63,832; 72,752 и 88,812 нс на решение P0–P3. Разница P3 и P0 на данном стенде меньше 0,1 мкс и несопоставима с сетевым RTT; следовательно, оптимизация нескольких локальных lookup не устраняет задержку внешнего PDP.

Результаты согласуются с ограничениями стандартов. RFC 9114 требует учитывать текущий адрес при контроле доступа [9], а RFC 9312 не позволяет считать пассивно наблюдаемый CID надежным ключом произвольного шлюза [11]. NIST переносит решение ближе к ресурсу и объединяет идентичность с контекстом [13, 14]. При этом P3 отличается от QASM: QUIC-aware-сопоставление восстанавливает принадлежность пакетов соединению [19], но

само по себе не отвечает, продолжает ли прежняя авторизация действовать в новой зоне. SMAQ также оставляет авторизацию и аудит будущей работой [17].

Ограничения исследования

Первое ограничение — синтетические сетевые распределения. Они обеспечивают одинаковые условия сравнения, но не воспроизводят конкретного оператора, мобильную сеть или частоту инцидентов. Второе — событийная, а не пакетная модель. В ней не реализованы криптографические кадры QUIC, управление перегрузкой, таймеры потерь и конкретные API получения текущего адреса. Для внедрения необходимы испытания выбранной библиотеки и HTTP/3-сервера, поскольку исследования обнаруживают различия реализаций [15, 16].

Третье ограничение связано с доверием к классификатору зоны. Ошибочная маршрутизация или компрометация ingress способна присвоить публичному пути корпоративную метку. Требуются защищенный канал контекста, минимизация полномочий и независимый аудит. Четвертое — стабильная идентичность субъекта. Для анонимного публичного сервиса ключом квоты может быть выданный сервером privacy-preserving token, но его проектирование выходит за рамки статьи. Пятое — P3 не защищает от компрометации самого клиента: она ограничивает продолжение доступа по политике, но не доказывает добросовестность пользователя.

Микробенчмарк характеризует только локальные операции Python. Он не позволяет утверждать, что промышленный PDP добавит десятки наносекунд. Нулевая доля U и E в P3 обусловлена логикой инварианта и выбранными сценариями; общий корень доверия, ошибочная политика или fail-open реализация создадут другие результаты. Наконец, Multipath QUIC на дату исследования находится в процессе стандартизации [20], поэтому расширение на одновременно активные пути сформулировано архитектурно, но не проверено на совместимых реализациях.

Практическое внедрение

Внедрение начинается с инвентаризации решений, где текущий IP, подсеть, ASN, ingress или географическая зона влияют на доступ. Для каждого

такого правила фиксируются PEP, источник сетевого атрибута, TTL решения и реакция на изменение пути. Отдельно выявляются квоты, ключом которых служит 5-tuple или IP. Запрет всего UDP/443 может упростить контроль, но устраняет свойства HTTP/3 и не является оценкой корректности QUIC-архитектуры.

На QUIC-терминаторе необходим callback нового пути с состояниями candidate и validated. До подтверждения нового пути чувствительные операции помещаются в карантин; объем ответов остается в пределах требований RFC 9000 [6]. После validation терминатор получает зону от управляемого ingress, сравнивает ее с предыдущей, проверяет эпоху и обращается к PDP. При недоступности PDP выбирается заранее документированная политика: fail-closed для критичных ресурсов и ограниченный grace period только для низкорисковых операций.

Квоты разделяются на транспортные и субъектные. Per-path лимит защищает CPU и полосу конкретного ingress. Стабильный subject/resource-лимит предотвращает получение новой бизнес-квоты при смене адреса. Журнал должен содержать connection handle, хэш субъекта, старую и новую зоны, факт Path Validation, policy epoch, decision ID, величину сохраненной квоты и результат. Сырые CID и IP хранятся только в объеме, необходимом для расследования, поскольку миграция и ротация идентификаторов также имеют цели конфиденциальности [6, 18].

Приемочные испытания включают NAT rebinding без смены зоны, handover между разрешенными сетями, переход в запрещенную зону, отзыв политики, ротацию CID и серию миграций при действующей квоте. Положительный критерий состоит не только в сохранении соединения: после каждой миграции должны выполняться формулы Permit и Fresh, а число субъектных корзин не должно расти с числом адресов. Для ресурсов, где сетевое расположение не входит в политику, P3 может переиспользовать свежее решение после validation и тем самым избегать лишнего PDP-вызова.

Заключение

Миграция QUIC создает не криптографическую уязвимость, а границу ответственности между транспортом и контролем доступа. Connection ID сохраняет логическое соединение, Path Validation проверяет достижимость нового адреса, но ни один из механизмов не определяет право субъекта действовать из новой зоны и не переносит корректно адресную квоту. Пассивный шлюз также не может без координации превратить CID в устойчивый ключ состояния.

Предложенная методика связывает допуск с завершенным handshake, подтвержденным путем, текущей зоной, субъектом, ресурсом, эпохой политики и стабильной квотой. В эксперименте P3 сохранила 97,920% легитимных миграций, не допустила успешных трасс S3 и S5 при верхней границе интервала 0,0096%, исключила сверхлимитный прием S4 и добавила медианно 39,877 мс. Практический вывод состоит в размещении PEP на QUIC-терминаторе, повторной оценке только значимых изменений контекста и разделении сетевых и субъектных лимитов. Такая композиция сохраняет мобильность, не приравнивая транспортную непрерывность к непрерывности авторизации.

Список литературы

1. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. М.: Стандартинформ, 2012. URL: https://protect.gost.ru/gost/details/775007f4-c66c-48e3-a0e9-8f0c3bad18b2 (дата обращения: 19.08.2026).

2. ГОСТ Р ИСО/МЭК 27033-2-2021. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сетей. М.: Стандартинформ, 2021. URL: https://protect.gost.ru/gost/details/835bbe29-f2b4-4e51-8eb0-14df14a6b4e5 (дата обращения: 19.08.2026).

3. ГОСТ Р ИСО/МЭК 27033-4-2021. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности. М.: Стандартинформ, 2021. URL: https://protect.gost.ru/gost/details/7cca26f3-1131-479d-8062-d1c4fbb22359 (дата обращения: 19.08.2026).

4. ГОСТ Р ИСО/МЭК 27002-2021. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. М.: Стандартинформ, 2021. URL: https://protect.gost.ru/gost/details/be00167c-6e26-4042-ac31-36be8a9d6b2e (дата обращения: 19.08.2026).

5. Гарифуллин Р. Ш. Внедрение протоколов HTTP/3 и QUIC: повышение безопасности и скорости веб-соединений // Universum: технические науки. 2025. № 4(133). С. 51–54. URL: https://7universum.com/ru/tech/archive/item/19761 (дата обращения: 19.08.2026).

6. Iyengar J., Thomson M. QUIC: A UDP-Based Multiplexed and Secure Transport. RFC 9000. IETF, 2021. DOI: 10.17487/RFC9000. URL: https://www.rfc-editor.org/rfc/rfc9000.html (дата обращения: 19.08.2026).

7. Thomson M., Turner S. Using TLS to Secure QUIC. RFC 9001. IETF, 2021. DOI: 10.17487/RFC9001. URL: https://www.rfc-editor.org/rfc/rfc9001.html (дата обращения: 19.08.2026).

8. Thomson M. Version-Independent Properties of QUIC. RFC 8999. IETF, 2021. DOI: 10.17487/RFC8999. URL: https://www.rfc-editor.org/rfc/rfc8999.html (дата обращения: 19.08.2026).

9. Bishop M. HTTP/3. RFC 9114. IETF, 2022. DOI: 10.17487/RFC9114. URL: https://www.rfc-editor.org/rfc/rfc9114.html (дата обращения: 19.08.2026).

10. Kühlewind M., Trammell B. Applicability of the QUIC Transport Protocol. RFC 9308. IETF, 2022. DOI: 10.17487/RFC9308. URL: https://www.rfc-editor.org/rfc/rfc9308.html (дата обращения: 19.08.2026).

11. Kühlewind M., Trammell B., Gorry Fairhurst et al. Manageability of the QUIC Transport Protocol. RFC 9312. IETF, 2022. DOI: 10.17487/RFC9312. URL: https://www.rfc-editor.org/rfc/rfc9312.html (дата обращения: 19.08.2026).
12. Duke M. QUIC Version 2. RFC 9369. IETF, 2023. DOI: 10.17487/RFC9369. URL: https://www.rfc-editor.org/rfc/rfc9369.html (дата обращения: 19.08.2026).
13. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST SP 800-207. Gaithersburg: NIST, 2020. DOI: 10.6028/NIST.SP.800-207. URL: https://csrc.nist.gov/pubs/sp/800/207/final (дата обращения: 19.08.2026).
14. Chandramouli R., Butcher Z. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments. NIST SP 800-207A. Gaithersburg: NIST, 2023. DOI: 10.6028/NIST.SP.800-207A. URL: https://csrc.nist.gov/pubs/sp/800/207/a/final (дата обращения: 19.08.2026).
15. Chatzoglou E., Kouliaridis V., Karopoulos G., Kambourakis G. Revisiting QUIC Attacks: A Comprehensive Review on QUIC Security and a Hands-on Study // International Journal of Information Security. 2023. Vol. 22. P. 347–365. DOI: 10.1007/s10207-022-00630-6. URL: https://link.springer.com/article/10.1007/s10207-022-00630-6 (дата обращения: 19.08.2026).
16. Buchet A., Pelsser C. An Analysis of QUIC Connection Migration in the Wild. arXiv:2410.06066, 2024. URL: https://arxiv.org/abs/2410.06066 (дата обращения: 19.08.2026).
17. Kosek M., Spies B., Ott J. Secure Middlebox-Assisted QUIC // 2023 IFIP Networking Conference. 2023. URL: https://dl.ifip.org/db/conf/networking2023/networking2023/1570884952.pdf (дата обращения: 19.08.2026).
18. Govil Y., Wang L., Rexford J. MIMIQ: Masking IPs with Migration in QUIC // USENIX Workshop on Free and Open Communications on the Internet. 2020. URL: https://www.usenix.org/system/files/foci20-paper-govil.pdf (дата обращения: 19.08.2026).

19. Selvam H. H. S., Kulkarni S. G. QASM: A Novel Framework for QUIC-Aware Stateful Middleboxes. arXiv:2602.03354, 2026. URL: https://arxiv.org/abs/2602.03354 (дата обращения: 19.08.2026).
20. Liu Y., Ma Y., De Coninck Q. et al. Managing Multiple Paths for a QUIC Connection. draft-ietf-quic-multipath-21. IETF, 2026. URL: https://datatracker.ietf.org/doc/draft-ietf-quic-multipath/21/ (дата обращения: 19.08.2026).