Эволюция связности в эпоху нулевого доверия

Константин Чумаченко

Аннотация

Интернет сегодня — это не только «сеть сетей», но и основа для множества сервисов. В статье исследуется, как развитие прикладных применений Интернета влияло на способность сети передавать данные и меняло значение термина «связность».

Ключевые слова:

маршрутизация, облачные платформы, CDN, DDoS-атаки, концепция Zero Trust, фрагментация Интернета.

Введение

Я пишу этот текст в онлайн-редакторе, даже не задумываясь о том, какие потоки информации порождает каждое нажатие клавиши. В это время через сетевой интерфейс моего ноутбука проходит череда интернет-соединений: десятки запросов к серверам по всему миру — авторизация, загрузка шрифтов, обновление счётчиков, работа трекеров. Всё это происходит автоматически, без моего участия, и обретает форму в окне браузера. Если что-то пойдёт не так, мне будет непросто найти причину, хотя я работаю в сфере интернет-технологий не первый год.

Когда-то Интернет был другим. Чтобы открыть файл на удалённом компьютере или прочитать новости, требовалось вручную установить соединение. Возможных результатов было всего два: успех либо ошибка, отображавшаяся в командной строке.

На протяжении десятилетий мы используем IP-протокол, обеспечивающий «связность» — способность устройств, сетей и систем взаимодействовать через Интернет. Инфраструктура сети неоднократно менялась под влиянием технологий, новых моделей поведения пользователей, требований бизнеса и политических процессов. Сегодня «связность» стала сложным, многогранным понятием, охватывающим широкий спектр технологий, и даже профессионалы порой затрудняются дать ей точное определение.

Давайте проследим, как развитие прикладных применений Интернета придало термину «связность» новые значения. Для этого обратимся к ключевым этапам этой эволюции, которые, накатываясь друг на друга, как волны, сформировали современный Интернет.

Первый бум доткомов

С появлением в конце 1990-х годов таких компаний, как Amazon, eBay и Yahoo!, люди открыли для себя новые возможности: от покупок без походов в магазин до мгновенного доступа к информации и общению. Спрос на подключение резко вырос, Интернет перестал быть инструментом для избранных и стал быстро расширяться.

Рост операторских сетей и пользовательских подключений

Интернет-провайдеры начали активно расширять свои сети и улучшать качество доступа. К 2000 году число интернет-пользователей в мире достигло 400 миллионов (в 1995 году — всего 16 миллионов). Этот рост был вызван не только удобством новых сервисов, но и снижением стоимости подключения. Количество автономных сетей (AS) выросло с пяти тысяч в 1995 году до десяти тысяч в 2000 году [1].

Владельцы сетей ищут альтернативы транзиту

Этот период также ознаменовался появлением первых точек обмена интернет-трафиком, IXP (Internet eXchange Points), которые помогли улучшить маршрутизацию и снизить затраты на передачу данных между автономными сетями провайдеров [2]. В 1995–1998 годах были созданы AMS-IX (Амстердам), DE-CIX (Франкфурт), LINX (Лондон) и MSK-IX (Москва), впоследствии ставшие крупнейшими центрами концентрации пирингового трафика в мире.

Что изменилось?

Бурный рост интернет-инфраструктуры в 1990-х годах заложил основу для современного цифрового мира, в котором связность стала базовой потребностью человека.

Видеоконтент приходит в сеть

Широкое использование мультимедиа и интерактивных элементов в вебе обострило проблему доставки «тяжёлого» контента (видео, изображений, анимации) через перегруженные межоператорские соединения. Это привело к появлению в конце 1990-х годов сетей доставки контента (CDN, Content Delivery Networks), которые оптимизировали маршруты трафика, кешируя данные на распределённой сети серверов ближе к пользователям. Пионером индустрии стала компания Akamai, основанная в 1998 году.

Внедрение CDN сразу улучшило время отклика сайтов для пользователей, но настоящая революция в интернет-инфраструктуре произошла в период 2005–2015 годов из-за стремительного роста потребления видео. Видео стало доминирующей формой интернет-трафика благодаря YouTube, Netflix, TikTok, сервисам прямой трансляции и пиратскому контенту, распространяемому через P2P-сети. С 2005 года ежегодный отчёт Cisco Visual Networking Index фиксировал кратный рост IP-трафика, а к 2016 году объёмы годового трафика превысили 1 зеттабайт (миллиард терабайтов) [3].

CDN принесли с собой важные перемены в структуре потоков данных:

1. **Глобальное распределение трафика.** CDN используют сложные алгоритмы для балансировки нагрузки между своими узлами по всему миру. Эти алгоритмы могут учитывать состояние серверов, сетевые задержки, загрузку межоператорских соединений и даже стоимость размещения в конкретных дата-центрах. Перенаправление пользовательских запросов осуществляется средствами прикладных протоколов DNS и HTTP. Алгоритмы балансировки CDN стали новой формой маршрутизации данных.
2. **Локализация трафика.** Чтобы сократить маршруты доставки контента, CDN размещают кеширующие узлы непосредственно в сетях интернет-провайдеров (ISP), активно участвуют в приватных пиринговых соглашениях и присутствуют на точках обмена трафиком (IXP). Такая локализация трафика позволяет избежать длинных маршрутов через множество межоператорских стыков и значительно снижает вероятность потерь при доставке контента.

Что изменилось?

По мере аккумулирования «контрольного пакета» в 60–80% сетевого трафика интересы владельцев CDN — провайдеров услуг и видеосервисов — стали определять пути контента к пользователю. На одной из интернет-конференций я наблюдал горячую дискуссию: операторы, вынужденные справляться с непредсказуемыми всплесками трафика на стыках с CDN, активно выражали недовольство. Тем не менее, благодаря CDN задержки и буферизация перестали быть проблемой для любителей 4K-видео на больших экранах.

Интернет связывает IT-ландшафт предприятий

Бизнес быстро осознал преимущества удалённого доступа к программам и вычислительным ресурсам через Интернет. В 1999 году компания Salesforce представила онлайн-сервис управления продажами, на долгие годы заняв лидирующие позиции в сегменте SaaS (Software-as-a-Service). В 2006 году Amazon Web Services дала старт эпохе облачных инфраструктурных сервисов, позволив компаниям арендовать серверные мощности без владения физическим оборудованием.

Популярность облачных сервисов, появление компаний со множеством филиалов, а также тренд на удалённую и мобильную работу стимулировали развитие новых технологий управления маршрутизацией и доступом пользователей.

Централизация управления маршрутами

Компаниям потребовалась связность с критически важными приложениями с гарантированной пропускной способностью и низкой задержкой. Изначально основой для распределённых корпоративных сетей служили каналы магистральных операторов. Однако растущие потребности в гибкости привели к появлению в начале 2010-х годов технологии SD-WAN (Software-Defined Wide Area Network) [4]. SD-WAN позволяет централизованно управлять подключениями головного офиса и филиалов, абстрагируясь от типа соединения (Ethernet, Wi-Fi, LTE и др.) Единый контроллер обеспечивает гибкую сегментацию сети, настройку политик безопасности и оптимизацию передачи данных. Это позволяет создавать сложные системы «туннелей» для различных типов трафика и приложений, обеспечивая высокую производительность и безопасность.

Гранулярный контроль доступа пользователей

С внедрением облачных сервисов и веб-приложений границы корпоративных сетей стали размываться, а принцип доверенного периметра устарел. Предприятиям потребовались гарантии, что доступ к приложениям получают только авторизованные пользователи и устройства, независимо от их местоположения. В популярной концепции Zero Trust [5] идентичность и права пользователя проверяются при каждом обращении к ресурсу. Следующие ей современные решения, такие как Secure Access Service Edge (SASE) [6], объединяют компоненты безопасности в сетях и в облачных платформах, интегрируя политики доступа с маршрутизацией.

Что изменилось?

Сегодня каждая транзакция — будь то доступ к почте или загрузка файлов в облако — проверяется на соответствие политикам доступа. Например, сотрудник, подключающийся к VPN, должен пройти двухфакторную аутентификацию, а его устройство — соответствовать требованиям безопасности, иметь актуальные обновления и антивирус. Политики доступа влияют на сетевые маршруты, например, трафик из офиса к облачному серверу может быть перенаправлен через защищённый канал, чтобы минимизировать риски утечки данных.

Таким образом, современные сети компаний стали не просто «трубами» для передачи данных, а интеллектуальными системами, поведение которых определяется целями безопасности и контроля доступа.

Сети и облака против кибератак

На фоне стремительного развития интернет-сервисов сетевая безопасность долгое время оставалась второстепенной задачей. Однако с ростом значимости веб-сайтов, приложений и облачных платформ ущерб от кибератак стало невозможно игнорировать. Большой ущерб стали наносить атаки типа Distributed Denial of Service (DDoS), в которых злоумыш-

ленники использовали множество заражённых устройств для генерации огромных объёмов вредоносного трафика.

DDoS-атаки быстро эволюционировали, эксплуатируя слабые пароли устройств (например, IoT-ботнет Mirai), уязвимости протоколов (NTP amplification) и программного обеспечения (Memcached, CLDAP reflection), а также ошибки в логике CPU (Meltdown, Spectre). Мощность атаки ботнета Mirai в 2016 году превысила 1 Тбит/с, а в 2024 году его вариация породила атаку в 5,6 Тбит/с [7].

Как показала практика, эффективно противостоять таким атакам могут только системы сопоставимого масштаба.

Фильтрация DDoS-атак в операторских сетях

Рост вычислительных мощностей сетевого оборудования и развитие технологий анализа данных сделали возможным появление интеллектуальных механизмов анализа IP-пакетов и TCP-соединений. Большинство крупных интернет-провайдеров (ISP) внедрили системы очистки трафика на основе Deep Packet Inspection (DPI), которые интегрированы с машинным обучением и внутрисетевой маршрутизацией. Такие системы позволяют выявлять аномалии на сетевом и транспортном уровнях и блокировать вредоносный трафик ещё до его попадания в сеть клиента.

Облачные платформы защищают от атак на уровне приложений

Сегодня большинство кибератак осуществляется на уровне приложений. Для таких атак DPI-анализ неэффективен в связи с повсеместным применением шифрования трафика протоколов HTTP и DNS. Ситуация усугубляется тем, что многие атаки на уровне приложений не создают аномального сетевого трафика и выглядят для операторов как обычная пользовательская активность, за которой скрывается эксплуатация уязвимостей веб-ресурсов.

Для эффективного устранения таких угроз необходим анализ запросов к веб-ресурсам с раскрытием TLS/SSL-соединений. Эту возможность реализовали компании Akamai и Cloudflare, подобные сервисы разработаны также в России, в частности, в компании NGENIX, где работаю я. Архитектура распределённых облачных платформ, в которые эволюционировали CDN, эффективно масштабируется как для обработки всплесков легитимного трафика, так и для отражения масштабных атак. Анализ HTTP- и DNS-запросов позволяет выявлять источники вредоносной активности с точностью до конкретного устройства и снизить долю false positives — ошибочных блокировок легитимных запросов.

Что изменилось?

Кибератаки наглядно показали, что всеобщая связность в Интернете — это не только благо, но и источник рисков. Количество потенциально уязвимых сетевых устройств уже невозможно подсчитать, поэтому потребность в защите растёт. Системы фильтрации вредоносного трафика на базе операторских сетей и распределённых облачных платформ стали неотъемлемой частью интернет-инфраструктуры, обеспечивая стабильность и безопасность цифровых сервисов.

Фрагментация Интернета вокруг якорей доверия

Якорь доверия (trust anchor) — это критически важный объект или механизм, который служит основой для установления доверия в ходе цифровых транзакций. Вот некоторые примеры якорей доверия в Интернете:

1. **Корневые DNS-серверы.** Система доменных имён (DNS) полагается на корневые серверы как на якоря доверия для преобразования доменных имён в IP-адреса [8]. В управлении и обеспечении работы корня DNS принимают участие различные организации: ICANN, Verisign, а также организации-операторы корневых серверов. Кроме того, с внедрением DNSSEC появился ещё один якорь — ключ корневой зоны. Эта система управляется ICANN (IANA) и Verisign под надзором международной общественности (Trusted Community Representatives). С 2021 года якорем доверия для российских национальных доменов .ru и .рф является Национальная система доменных имён (НСДИ).
2. **Удостоверяющие центры (Certificate Authorities, CAs).** Корневые удостоверяющие центры (УЦ) являются якорями доверия в системах цифрового обмена с использованием открытых ключей (Public Key Infrastructure, PKI). Они выпускают подписанные цифровые сертификаты, которые используются для подтверждения идентичности нижестоящих УЦ, веб-сайтов, устройств и отдельных лиц. Например, для проверки подлинности веб-сайта браузер проверяет, что SSL/TLS-сертификат сайта может быть удостоверен корневым удостоверяющим центром напрямую или через цепочку промежуточных сертификатов. При успешной проверке пользователь видит замочек в адресной строке браузера. Статус корневого УЦ для систем PKI может устанавливаться законодательно, быть результатом отраслевого соглашения или определяться единолично владельцем системы. Примерами корневых УЦ в мире являются организации GlobalSign и Let's Encrypt, для юридически значимого обмена в России эту функцию выполняют Минцифры и ФНС.
3. **Серверы точного времени.** В системе серверов точного времени, поддерживающих протокол NTP, роль якорей доверия играют серверы, получающие сигнал непосредственно от спутниковых систем, таких как GPS, ГЛОНАСС или китайской Beidou. Эти серверы выступают в качестве источника точного времени для NTP-серверов нижестоящих уровней.

В широком контексте управления Интернетом роль якорей доверия могут выполнять технологические стандарты (например, шифрование в соответствии с ГОСТ [9]), а также нормативные акты. Например, законы ФЗ-152 в России и GDPR в странах ЕС устанавливают требования к обработке персо-

нальных данных в соответствующих юрисдикциях и вводят ограничения на их трансграничную передачу.

Что изменилось?

Интернет стал неотъемлемой частью сложных общественно-политических отношений. Фрагментация Интернета вокруг различных якорей доверия, ограничения трансграничных потоков данных, блокировки противоправного контента обусловлены соображениями контроля и безопасности, которые превалируют в сегодняшнем мире.

От IP к AI и дальше

Как видно из примеров выше, хотя протокол IP сохраняет глобальную совместимость устройств, на связность — возможность обмена данными — влияет множество факторов:

1. **Техническая возможность подключения и качество соединения.** Потери пакетов, задержки, джиттер и другие параметры, определяющие качество связи.
2. **Масштабируемость и устойчивость сетей.** Способность операторов справляться с растущим трафиком и обеспечивать стабильность работы.
3. **Межоператорское взаимодействие.** Условия пиринга и транзита между сетями.
4. **Балансировка и оптимизация нагрузки.** Распределение трафика умными алгоритмами при доступе к веб-ресурсам и приложениям.
5. **Политики маршрутизации и управления доступом.** Особенности работы корпоративных сетей и облачных платформ.
6. **Защита от DDoS-атак и вредоносной активности.** Системы фильтрации, обеспечивающие безопасность и доступность сервисов.
7. **Доверие и безопасность.** Выбор якорей доверия (например, корневых сертификатов) для проверки подлинности транзакций, определение источников доверенной информации и правил обработки данных.

Этот список далеко не исчерпывающий. Например, применение рекомендательных алгоритмов, определяющих, какие видеоролики показывать пользователям, или антифрод-систем, дающих красный или зелёный свет финансовым транзакциям, также можно считать факторами, влияющими на связность.

Можно быть уверенным, что перспективные технологии, старт которых мы наблюдаем сегодня, в очередной раз изменят потоки данных и создадут новые формы связности в сети.

1. **5G и спутниковые сети.** Операторы мобильных сетей и спутниковых группировок (например, Starlink и Qianfan) обещают повсеместный высокоскоростной доступ для пользователей и IoT-устройств, устраняя «белые пятна» в покрытии.
2. **Децентрализованные архитектуры.** Технологии, такие как блокчейн и децентрализованные вычисления, могут снизить зависимость от облачных провайдеров, вернув нас к эпохе одноранговых сетей.
3. **Периферийные вычисления (Edge Computing).** Облачные провайдеры развёртывают инфраструктуру ближе к пользователям, чтобы снизить задержки и улучшить производительность SaaS-приложений.
4. **Искусственный интеллект (AI).** Как прогнозирует Сатья Наделла из Microsoft, SaaS скоро прекратит своё существование, уступив место веб-интерфейсам для AI-агентов [10]. Это сделает связность с AI-платформами критически важной для веб-приложений.

Связность Интернета продолжает развиваться благодаря накоплению знаний и потребности решать с помощью сети всё более сложные задачи. В биологии эволюция часто ведёт к усложнению организмов. Будем надеяться, что Интернет, как «цифровой организм», сможет адаптироваться к изменениям среды и успешно справиться с вызовами завтрашнего дня.

Список литературы:

[1] G. Houston, The 32-bit AS Number Report, https://www.potaroo.net/tools/asn32, дата обращения: март 2025.

[2] I. Castro, Shaping the Internet: History and Impact of IXP Growth, 2019, https://labs.ripe.net/author/ignacio_castro/shaping-the-internet-history-and-impact-of-ixp-growth, дата обращения: март 2025.

[3] Cisco, Press Release Cisco Visual Networking Index, 2014, https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2014/m06/cisco-visual-networking-index-predicts-annual-internet-traffic-to-grow-more-than-20-percent-reaching-1-6-zettabytes-by-2018.html, дата обращения: март 2025.

[4] Palo Alto Networks, What Is SD-WAN?, https://www.paloaltonetworks.com/cyberpedia/what-is-sd-wan, дата обращения: март 2025.

[5] J. Kindervag, Build Security Into Your Network's DNA: The Zero Trust Network Architecture, Forrester Research, 2010, https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf, дата обращения: март 2025.

[6] Palo Alto Networks, What is SASE?, https://www.paloaltonetworks.com/cyberpedia/what-is-sase, дата обращения: март 2025.

[7] The Cloudflare Blog, Record-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4, 2025, https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/, дата обращения: март 2025.

[8] IANA, Root Zone Management, https://www.iana.org/domains/root, дата обращения: март 2025.

[9] ТЦИ, «Веб-серверы и ГОСТ-криптография», 2023, https://tcinet.ru/press-centre/articles/7759, дата обращения: март 2025.

[10] Satya Nadella on the Future of SaaS, 2025, https://www.youtube.com/watch?v=GuqAUv4UKXo, дата обращения: март 2025.

Об авторе:

Чумаченко Константин Викторович,
генеральный директор компании NGENIX