№17
Декабрь 2022

MSK IX

Интернет изнутри

ИНТЕРНЕТ: БОЛЬШЕ БЫСТРЕЕ ДЕШЕВЛЕ

Движущие силы Интернета
50 лет эволюции сетевой инфраструктуры

С. 2

Спутниковый Интернет - очарование низких орбит

Конкуренция между разными видами спутниковой связи стала еще острее

С. 11

ЦОДы будущего: основные тенденции развития

В каком направлении движутся сегодня центры обработки данных

С. 18

Биометрия в Интернете и современные цифровые платформы

Вопросы безопасности биометрии в контексте её использования для идентификации пользователя

С. 23

DNS: от технологии к сервису

Из истории DNS и SLA

С. 43

Содержание:

Журнал
«Интернет изнутри»

info@internetinside.ru

Выпуск №17, дата выхода:
Декабрь 2022 г.

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Регистрационный номер:
ПИ № ФС77-71202 от 27.09.2017

Публикуется при поддержке АНО «ЦВКС «МСК-IX»

Редакционная коллегия:
Марат Биктимиров
Елена Воронина
Алексей Платонов

Выпускающий редактор:
Ирина Пыжова

Продакшн:
Алексей Гончаров

Дизайн и вёрстка:
Дмитрий Ивлянов

Корректор:
Наталья Рябова

Обложка разработана с использованием ресурсов сайта Freepik.com

MSK IX

DNS

DNS-RESOLVER MSK-IX для ISP

Получите быстрый и безопасный доступ к информационным ресурсам сети Интернет

Скорость
Максимально быстрый ответ на DNS-запрос за счёт использования технологии Anycast

Надёжный
Обеспечивает доступность сервиса на уровне выше 99,98%

Высокопроизводительный
Обрабатывает 200 000+ (UDP) запросов в секунду

Безопасный
Поддерживает протоколы безопасности: DNSSEC, DoT, DoH

ANYCAST DNS

Удобный и эффективный сервис по размещению DNS-зон на нескольких DNS-узлах, использующих единую IP адресацию.

Скорость – максимально быстрый ответ на DNS-запрос за счёт использования технологии Anycast

Безопасность – поддержка DNSSEC как средства минимизации атак, связанных с подменой IP-адреса

Надёжность – работоспособность сервиса не зависит от работоспособности отдельного узла Anycast

Технологичность – постоянный мониторинг оказываемых услуг и оборудования, а также техническая поддержка заказчиков

Удобство – редактор DNS-зон с массовым созданием списка зон для списка доменов и загрузкой из внешних источников

Статусность - возможность именования сервиса DNS собственными доменными именами (white-label)

MSK-IX.RU

Больше, быстрее, дешевле!

Дорогой читатель,
Эти наречия как нельзя лучше характеризуют Интернет и его эволюцию. Согласно отчету МСЭ «Цифровое развитие. Факты и цифры 2021» (https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf), число пользователей Интернета в 2021 году достигло почти пяти миллиардов, или 63% мирового населения, и продолжает неуклонно расти. Согласно тому же отчету, мировой международный трафик в 2021 году достиг 932 Тбит/с по сравнению с 719 Тбит/с в 2020 году. Это увеличение на 30%, и оно следует за увеличением, аналогичным увеличению в предыдущем году.

Интернет растет и в плане доступных услуг, приложений и контента. Почти четыре тысячи новых приложений ежедневно добавляется на платформе Google Play к существующим 3,55 миллиона программ! За последние три года трафик крупнейшей сети доставки контента (CDN) Akamai вырос в три раза, достигнув 250 Тбит/с.

Стоимость подключения, особенно в расчёте на мегабит пропускной способности, постоянно снижается. Правда, наблюдается существенное различие между развитыми и развивающимися странами. В то время как, согласно МСЭ, для европейских стран стоимость стандартного подключения составляет в районе 1% ВВП на душу населения, для Африки эта цифра достигает 18,6%.

К сожалению, рост Интернета сопровождается и ростом вредоносных факторов. В июле 2022 года компания Akamai противостояла крупнейшей DDoS-атаке, когда-либо проводившейся против европейского клиента на платформе Prolexic, при этом глобально распределенный трафик атаки достиг пиковой скорости 853,7 Гбит/с и 659,6 миллиона пакетов в секунду на протяжении 14 часов (https://www.akamai.com/blog/security/largest-european-ddos-attack-ever). В ноябре 2021 года клиенты Microsoft Azure стали целью DDoS-атаки с пропускной способностью 3,45 Тбит/с и скоростью передачи пакетов 340 миллионов пакетов в секунду, что считается крупнейшей DDoS-атакой из когда-либо зарегистрированных (https://www.zdnet.com/article/microsoft-heres-how-we-stopped-the-biggest-ever-ddos-attack/).

Чем же обусловлено это необыкновенное развитие, какие силы обеспечивают этот невероятный рост? Над этим вопросом размышляет Джеф Хьюстон в свой статье «Движущие силы Интернета».

Интернет как глобальная универсальная коммуникационная среда открывает громадные возможности для инновации и внедрения новых технологий. В этом выпуске номера мы познакомим вас с технологиями низкоорбитальной спутниковой коммуникации и тенденциями в развитии центров обработки данных.

Вопросы защищенности приложений и услуг, безопасности их использования стоят как никогда остро на повестке как разработчиков, так и политиков. В этом номере мы рассмотри оба аспекта в статьях о биометрии в современных приложениях и европейской модели обеспечения безопасности Интернета вещей.

Не обойдем мы вниманием и инфраструктуру Интернета. В своей статье «DNS: от технологии к сервису» Павел Храмцов расскажет о 40-летней истории развития этой услуги и технологии.

Как всегда, нам очень интересно и важно знать ваше мнение. Что понравилось и что можно улучшить? Какие темы вы хотели бы увидеть в следующих выпусках? Пишите нам по адресу info@internetinside.ru.

Движущие силы Интернета

Джефф Хьюстон (Geoff Huston)

Давайте вернемся на 50 лет назад и представим мир, существовавший в 1972 году, а также технологии и телекоммуникации того времени. Это был мир огромных и дорогих универсальных компьютеров («мейнфреймов»), круглосуточно обслуживаемых операторами и специальными программистами, обученными разбираться в том «тарабарском» наборе символов, который использовался для управления заданиями на этих машинах. При этом самым сложным бытовым прибором, с которым сталкивался средний потребитель, был радиоприемник или телевизор. Наши часы все еще были механическими. Тем не менее, изменения набирали ход. Пилотируемые космические полеты с их невероятными технологическими достижениями стали не только предметом восхищения целого поколения, но и помогли заглянуть в тот мир высоких технологий, который завладел нашими умами сегодня.

В течение всех этих 50 лет в информатике царствовал вездесущий закон Мура (https://en.wikipedia.org/wiki/Moore %27s_law). Универсальные компьютеры становились все более мощными, быстрыми и дешевыми. Одновременно появились компьютеры, которые не обязательно отличались более высокой скоростью или мощностью, но при этом были меньше и дешевле. Благодаря неуклонному уменьшению размеров и себестоимости, а также повышению удобства использования, они постепенно превратились в персональные компьютеры. В 1990-х годах появление рынка персональных компьютеров как потребительского товара оказало сильное влияние на архитектуру технологической среды. Появилось разделение между мейнфреймами и окружающим их созвездием персональных компьютеров. Кроме того, это разделение проникло в сети обмена компьютерными данными. Эти сети, в отличие от телефонных сетей, обращающихся одинаково со всеми подписчиками (по сути, это была истинная «одноранговая» сеть), начали внедрять сетевую архитектуру, которая проводила фундаментальное различие между клиентами и серверами. Компьютерные сети начали объединять и совершенствовать некоторые жизненно важные сетевые функции, такие как сервис общих имен и система маршрутизации, в рамках укрупненной концепции сети. При этом клиенты становились потребителями предоставляемых сетью сервисов. В некотором смысле 1990-е годы стали эпохой трансформации компьютерных сетей от парадигмы телефонии к концепции, которая была ближе к широковещательному телевидению.

Однако такое изменение модели сетевого взаимодействия клиент-серверных систем привело к появлению более фундаментального набора проблем в рамках сетевой среды. В вертикально связанном мире телефонии емкость сети в основном определялась количеством подключенных телефонных аппаратов. Поэтому обеспечение сети было детерминированным процессом, который полностью контролировался оператором телефонной сети. В несвязанном мире, построенном на основе новой клиент-серверной модели 1990-х, требования к пропускной способности сети определялись событиями на потребительском рынке. В результате объединение потребительского спроса и сетевого обслуживания стало функцией самого рынка Интернета. К началу 2000-х это привело к судорожным попыткам увеличить масштаб сервисов, предоставляемых серверной частью сети. Ненасытный спрос на потребительские устройства не был уравновешен соизмеримым уровнем инвестиций в масштабирование сервисной инфраструктуры и пропускную способность соединяющих сетей. При этом перестали существовать ценовые сигналы, а появление фиксированных тарифов на доступ к сетевым услугам еще больше усугубило проблему. Повышение потребительского спроса не сопровождалось увеличением выручки, что, в свою очередь, привело к тому, что все большая часть инфраструктуры финансировалась за счет повышения задолженности поставщиков услуг и инфраструктуры. Телекоммуникационная инфраструктура отошла от связанной модели, в рамках которой рост использования напрямую транслировался в дополнительные доходы для поставщиков, что, соответственно, позволяло получить дополнительный капитал для расширения инфраструктуры. При новой несвязанной экономической модели дополнительную выручку генерировали только новые пользователи, а увеличение уровня использования могло финансироваться лишь за счет наращивания инфраструктуры, вызванного привлечением дополнительных пользователей с предположительно низкой интенсивностью потребления. Если, по вашему мнению, эта картина похожа на огромную финансовую пирамиду, то вы недалеки от истины. Именно так выглядела индустрия поставщиков телекоммуникационных услуг (ISP) во второй половине 1990-х годов!

Такая среда привела к созданию петли обратной связи, которая усиливала спрос на сервисную инфраструктуру, и в состоянии стресса оказались не только финансовые модели: высокие темпы роста привели к сильному напряжению и технологических моделей. Огромную перегрузку испытывали популярные сервисы, развернутые в рамках единой платформы, кроме того, не справлялась с нагрузками сетевая инфраструктура, соединяющая эти сервисы. Решение проблемы заключалось в смене технологии сервисной инфраструктуры, в рамках которой произошел переход к фермам серверов и дата-центрам, коммутаторам и шлюзам, а также к иерархическому структурированию поставщиков услуг по «уровням». Снова стали проводиться эксперименты с виртуальными схемами в виде MPLS и VPN, а также в форме разделения

сети на фрагменты. Поскольку такие усилия по наращиванию мощности сервисов обычно отставали от спроса, это вело к другим экспериментам с различными формами «качества обслуживания», которые позволяли нормировать потребление самых дефицитных сетевых ресурсов.

Возможно, самым существенным изменением 2000-х стало появление сетей распределения контента. Вместо того, чтобы соединять всех клиентов с единой точкой предоставления услуги (вспоминается ситуация, когда компания Microsoft пыталась распространять все онлайновые обновления Windows со своей расположенной в Сиэтле фермы серверов, что создавало серьезные проблемы как с вычислительной, так и телекоммуникационной точек зрения), произошел переход к модели репликации услуги вблизи от ее клиентов. В результате запросы клиентов передавались только внутри сетей доступа, тогда как внутренние ресурсы сетей использовались для подачи обновлений на пограничные центры обслуживания. По сути, Интернет открыл для себя пограничные механизмы распределения, которые приблизили сервисы к пользователям. Предыдущая телекоммуникационная модель старалась приблизить пользователей к сервисам.

И произошло это очень своевременно, учитывая громадный сдвиг кривой спроса, который совпал с появлением на рынке смартфонов Apple iPhone в 2007 году. Отрасли пришлось справляться с увеличением спроса на пропускную способность, который на три или четыре порядка превзошел аналогичный показатель для эпохи подключаемых персональных компьютеров. Никого уже не удовлетворяли килобиты в секунду. Заказчикам требовались соединения с пропускной способностью порядка нескольких мегабит в секунду для погружения в иммерсивную среду, созданную на их мобильных устройствах.

За последние 50 лет произошла стремительная эволюция сетевой инфраструктуры. Основанная на передаче пакетов данных сетевая модель, которая использовалась локальными сетями Ethernet, была втиснута в высокоскоростную инфраструктуру дальней связи. Уже десятилетия, как мы перестали строить системы синхронной передачи SDH, и сегодня пакетные коммутаторы Интернета непосредственно подключены к коммуникационной (физической) среде. Однако несмотря на все эти изменения, мы по-прежнему используем IP-протокол для передачи пакетов.

Как и почему это произошло? С моей точки зрения, гениальность IP заключается в отделении среды приложений и контентных услуг от характеристик основообразующей коммутирующей платформы. Каждый раз, когда изобретается новая технология передачи данных, достаточно отобразить на нее IP-протокол, после чего вся база установленных IP-устройств получает возможность безболезненно использовать эту технологию. Начиная с появления двухточечных последовательных соединений, систем Ethernet с общей шиной и до возникновения таких кольцевых технологий связи, как FDDI и DQDB, а также радиосистем, каждый раз происходила стремительная интеграция этих технологий на уровне IP без внесения каких-либо изменений в прикладную или сервисную среду. Это позволяло не только сохранить инвестиции, которые вкладывались в целый спектр следующих друг за другом телекоммуникационных технологий, но и повысить их ценность при каждом расширении базы интернет-пользователей и объема использования ресурсов.

Все это дает нам возможность представить следующие 50 лет развития телекоммуникационных технологий. Как мы уже убедились, 50 лет – это довольно большой срок, но во многих отношениях он не столь уж продолжителен. Изменения, происходящие на протяжении нескольких столетий, часто сопровождаются отбрасыванием всех аспектов прежнего состояния и внедрением абсолютно «новой» среды. Но я не думаю, что это справедливо для прогнозов на 50 лет. Большую часть современного мира можно было представить в 1971 году или даже еще раньше. Превращение мобильных телефонов в «умные» (смарт) устройства была очевидной тенденцией еще в начале 1970-х. Трансформация вычислительных машин в связи с поступательным совершенствованием технологий обработки кремния, которая позволила создавать процессоры с миллиардами транзисторных затворов, невероятно низким энергопотреблением и чрезвычайно высокой тактовой частотой, не привела к фундаментальному переосмыслению внутренней природы компьютеров. Произошла резкая миниатюризация, но компьютерная логика осталась, в основном, неизменной. Суть в том, что семена тех «плодов», которые стали доминировать спустя 50 лет, были ясно видны еще в 1971 году. То же самое применимо и к семенам будущего, которые уже, вероятно, существуют в современной телекоммуникационной среде и которые будут доминировать в нашем мире через 50 лет. Возможно, главная проблема заключается не в идентификации существующих зародышей идей будущего, а в попытке отличить значимые идеи от отвлекающих.

В связи с этим, скорее всего, не имеют никакого смысла попытки нарисовать детальную картину компьютерной телекоммуникационной среды через 50 лет. Однако если не вдаваться в детали, то можно взглянуть на формирующие будущее движущие факторы и выбрать из них самые важные на основе тех сил, которые формируют современный мир.

Каковы движущие факторы современных изменений?

Крупнее

Когда закончилось время вертикально-интегрированных провайдеров и произошел переход на рыночное балансирование спроса и предложения, мы стали свидетелями огромных волн увеличения спроса. В свое время телефония довольствовалась пропускной способностью, измеряемой килобитами в секунду. Сегодня телефонный обмен данными уже требует даже не мегабит или гигабит в секунду, а измеряется в терабитах в секунду. Например, анонсированный в марте 2021 года кабель Google Echo, который свяжет США с Сингапуром и будет проложен по дну Тихого океана, будет включать 12 оптоволоконных пар, проектная пропускная способность каждой из которых составляет 12 Тбит/с. И это соответствует совокупной пропускной способности кабеля в 144 Тбит/с. В настоящее время строятся все более крупные телекоммуникационные системы на базе фотоэлектронных усилителей, средств мультиплексирования длины волны и фазовой/амплитудной/поляризационной модуляции, которые позволяют добиться существенного повышения пропускной способности кабелей.

Возможно, Мур и открыл в свое время экстраординарный закон, но, положа руку на сердце, рост индустрии потребительских устройств намного превышает даже предсказанные им значения. В одном лишь 2020 году было продано примерно 1,4 миллиарда мобильных интернет-устройств, и мы наблюдаем подобный объем потребления и даже выше, начиная с 2015. Огромное количество устройств и широчайшая пропускная способность стимулируют появление все более иммерсивного контента и услуг. Так каким же образом происходит доставка контента всем этим клиентским устройствам? Мы стали экспертами в агрегировании серверов и контента, сегодня существуют выделенные сети распределения контента, которые обслуживают все эти клиентские устройства со скоростью и в масштабах, соответствующих пропускной способности сетей доступа «последней мили».

Когда мы говорим о том, что инфраструктура становится крупнее, то критически важное значение имеет не только использование сетей человеком. Компьютерные сети являются «пакетными», и их, в том числе, использует динамично развивающийся мир так называемого Интернета вещей. Если взглянуть на этот новый мир, то сразу возникают два вопроса, на которые невозможно точно ответить. Сколько таких «вещей» уже используют Интернет сегодня? И сколько их будет использовать Интернет завтра?

В настоящее время существуют разные оценки количества подключенных к Интернету устройств (https://techjury.net/blog/how-many-iot-devices-are-there/#gref). По общему мнению, их количество находится в диапазоне от 20 до 50 миллиардов устройств, но это результат довольно грубых оценок, а не надежного аналитического измерения. Объемы производства микропроцессоров измеряются миллиардами в год, поэтому в этом отношении существует крайняя неопределенность в сочетании с ожиданиями чрезвычайно высоких темпов роста. Пятилетние прогнозы темпов роста для этого сегмента рынка начинаются в районе 50 миллиардов устройств, но постоянно пересматриваются в сторону увеличения.

За всем этим кроется наблюдение за тем, как по мере роста Интернета больше не отслеживается количество использующих его людей и уровень использования ими сетевых ресурсов - рост Интернета более не зависит от этих показателей. Эта сеть переходит к обслуживанию набора компьютерных устройств, чье использование основано на избыточной модели: избыточные мощности обработки, избыточные средства хранения и избыточные сетевые ресурсы. Мы на самом деле не понимаем, что означает «крупнее» в контексте спроса. Лучшее, что мы можем сделать, это продолжать стратегию последних двух десятилетий: вкладывать капитал, экспертные знания и ресурсы сразу же, как только они становятся доступными. Похоже, мы по-прежнему пытаемся угнаться за спросом, и, независимо от размера получившейся сети, модель ее использования способна с лихвой это переварить.

Быстрее

Одновременно со строительством более крупных сетей, имея в виду как количество подключенных устройств и клиентов, так и объем перемещаемых по сетям данных, мы стремимся сделать так, чтобы эти данные проходили через сеть как можно быстрее.

Происходит развертывание мобильных сетей доступа высокой пропускной способности, и сегодня для многих потребителей даже скорости передачи данных стандарта 3G являются неприемлемо низкими. Отрасль побуждают развертывать системы 5G, которые способны передавать данные в конечные точки с хваленой пиковой скоростью 20 Гбит/с. Возможно, такая скорость достижима в условиях «стремительного спуска с горы, когда ветер дует в спину», однако ожидания потребителей, что мобильные сети способны обеспечивать пропускную способность, измеряемую сотнями мегабит в секунду, для подключенных устройств, выглядят вполне оправданными. В современном мире использование проводных DSL-технологий и более общих форм передачи цифрового сигнала через кабельные системы прошлого поколения, состоящие из витых медных пар, в основном уже является неактуальным, а само использование технологий доступа на базе инфраструктуры медных кабелей продолжает убывать. Происходит переоснащение нашей проводной среды за счет прокладки оптоволоконных кабелей, а единицей измерения пропускной способности становятся уже не мегабиты, а гигабиты в секунду.

Однако скорость – это не только пропускная способность систем обмена данных, но и сама скорость передачи. Здесь вступают в силу непреложные законы физики, которые подразумевают неизбежную задержку распространения сигнала, передаваемого от отправителя получателю. Если под понятием «быстрее» понимать не только объем брутто передаваемых данных, но и быстроту реагирования системы на запросы клиента, то пользователь заинтересован в обеих характеристиках. Ему необходима как низкая задержка, так и высокая пропускная способность, и единственный способ этого добиться заключается в уменьшении «пакетных миль» для каждой транзакции. При передаче контента и предоставлении доступа к услугам в рамках сетей доступа можно резко снизить неизбежную задержку между двумя сторонами (отправителем и получателем). В результате благодаря более быстрому обмену данными протокола система становится более «отзывчивой».

Однако сделать сети быстрее можно не только за счет перемещения услуг ближе к клиентским устройствам. Специалисты стараются повысить эффективность протоколов, что позволит осуществлять транзакции при меньшем количестве обменов запросами между клиентом и сервером. Все это приводит к повышению «отзывчивости» сети, которую пользователь ощущает как увеличение скорости ее работы.

Понятие «быстрее» включает в себя:

- увеличение пропускной способности сетей доступа «последней мили»;
- перевод всех видов контента и доставки услуг в сети распределения контента с высоким уровнем репликации;
- повышение плотности точек распределения контента с целью перемещения серверов и сервисов ближе к пользователю;
- опережающее предоставление контента, позволяющее выполнять всю сервисную транзакцию в сети доступа «последней мили»;
- проектирование прикладной среды с учетом повышения скорости ее реакции;
- улучшение характеристик транспортных протоколов.

Цель заключается в том, чтобы удалить из сетевых транзакций этап передачи данных на дальнее расстояние. Благодаря прогнозированию потребностей и предварительному перемещению контента в точки доставки дата-центров можно избавиться от неизбежных узких мест, которые связаны с дистанционной передачей данных. В сетевых технологиях понятие «ближе» неизменно означает «быстрее».

Лучше

Это понятие имеет более абстрактный смысл, однако если «лучше» значит «более надежно» и «аутентично», то мы движемся в правильном направлении в рамках решения данной наиболее сложной задачи.

В современной среде веб-услуг протокол HTTPS или сеансы передачи зашифрованного и аутентифицированного контента применяются практически повсеместно. В настоящее время специалисты работают над закрытием последней щели в протоколе TLS за счет указания имени сервера (SNI) в сообщении TLS Client Hello. При этом технологии продвинулись еще на один шаг вперед благодаря подходам, предложенным в рамках Oblivious DNS и Oblivious HTTPS, которые предоставляют средства для изоляции любой стороны, даже оператора услуги, от информации о комбинации идентификации клиента и выполняемой транзакции. Это означает, что за исключением клиента никто не будет обладать априорными знаниями о сочетании идентификации и транзакции.

Все разработчики, занимающиеся созданием контента, приложений и платформ, с энтузиазмом развивают разнообразные аспекты конфиденциальности и аутентичности, а вопрос того, до какой степени сетям можно потенциально доверять, больше не стоит на повестке дня. Если сеть не способна извлекать привилегированную информацию, то проблема того, стоит ли ей доверять такую информацию, больше не актуальна. Вопрос доверия включает аспекты передаваемых полезных данных, транзакционных метаданных, например, запросов DNS и даже параметров управления транспортным протоколом. В современных сетях «лучший» результат для пользователей и выбираемых ими услуг достигается в том случае, если мы относимся ко всей сетевой инфраструктуре как к не заслуживающей доверия!

У меня есть подозрение, что произошел безвозвратный переход, и ранее существовавшие уровни предполагаемого доверия между сервисами, приложениями и контентом, с одной стороны, и базовой платформой и сетевой оболочкой, с другой стороны, навсегда исчезли. После того, как было продемонстрировано, что данный уровень доверия подвергается самым разным видам злоупотреблений, среда приложений и услуг принимает все необходимые ответные меры для блокировки каждой точки потенциального риска и утечки данных.

И из этой ситуации нет пути назад. Сегодня концепция внутренней паранойи захватила все уровни стека протоколов. В рамках этой концепции каждый уровень стека открывает другим слоям доступ лишь к функционально минимальному набору позиций информации, который необходим для выполнения запрошенной транзакции, защищая все остальные данные. В настоящее время эта концепция твердо укоренилась в операционной модели сетевого проектирования и эксплуатации, а также в разработке приложений.

Дешевле

Судя по всему, происходит переход в среду избыточных телекоммуникационных и вычислительных ресурсов. Вместе с тем, такие системы характеризуются значительной экономией за счет масштаба. Например, совершенствование систем передачи данных, сопровождавшееся увеличением пропускной способности кабельных систем в миллионы раз, не привело к соразмерному повышению цены кабельных систем, а в некоторых случаях капитальные и эксплуатационные издержки более крупных систем в течение ряда лет фактически понизились. В результате удельные расходы на передачу бита информации на единицу расстояния резко упали.

Избыточность также привела к уходу от тарифов на транзакцию. Плата в один пенни за отправку письма по почте или поминутный тариф для телефонных звонков имели когда-то экономический смысл, но единичная стоимость сетевой транзакции обычно столь мала, что внедрение для цифровых услуг модели стоимостного транзакционного тарифа представляется неосуществимой задачей.

Вместе с тем, произошло «съеживание» сети, которое привело к переводу сервисных транзакций на локальный уровень. Как мы это уже наблюдали, рост использования модели сетей распределения контента (content distribution network, CDN) изменил Интернет. Благодаря предварительной доставке контента в окрестности каждой пограничной точки, последующая запрашиваемая транзакция от сервера к клиенту реализуется на очень малом расстоянии. Однако уменьшение расстояния приводит не только к ускорению сервисной транзакции, но и к снижению расходов на строительство и эксплуатацию инфраструктуры. Уменьшение расстояния означает снижение энергопотребления и улучшение соотношения сигнал/шум. Такое повышение эффективности передачи данных также транслируется в снижение издержек.

В то же время, помимо уменьшения издержек, это влечет за собой и дополнительные выгоды. Некоторые услуги финансируются косвенным образом и, с точки зрения потребителя, пользователь не несет за них никаких видимых расходов. Например, поисковые запросы Google выполняются без взимания с пользователя какой-либо платы - эта услуга косвенно финансируется за счет доходов от рекламы. Такие рекламные поступления стали возможны благодаря тому, что компания Google обладает богатой информацией о профилях своих пользователей и продает эту информацию рекламодателям через средства по управлению рекламными кампаниями. Что интересно, если я в качестве пользователя попытаюсь продать рекламодателям собственный индивидуальный профиль, у меня ничего не получится. На индивидуальном уровне я не являюсь жизнеспособным рынком. Однако если мой профиль агрегировать с несколькими миллиардами профилей других пользователей Интернета, то в совокупности мы будем представлять собой очень ценный рынок. Настолько прибыльный, что он способен полностью финансировать инфраструктуру поиска Google и при этом зарабатывать еще немало денег.

Можно сказать, что значительная часть сервисной среды финансируется провайдерами услуг, которые используют агрегированные активы, недоступные индивидуальным пользователям. Результат получается на качественно ином уровне,

особенно если бывшая дорогая услуга, ранее доступная только ограниченной аудитории, которая могла позволить себе собрать команду специальных исследователей, трансформировалась в услугу массового спроса, доступную для всех. Причем такая услуга предлагается не просто по доступной цене. Во многих случаях она становится полностью бесплатной.

Крупнее, быстрее, лучше и дешевле

Часто выражается мнение о том, что невозможно в рамках сетевых технологий добиться одновременного выполнения всех перечисленных выше целей. Однако цифровые сервисные платформы Интернета каким-то образом умудряются этого достичь. Как им это удается?

Подход, на основе которого строятся сервисные платформы, способные справляться с непрерывно растущими нагрузками и обеспечивать постоянное сокращение издержек, заключается не просто в создании более крупных сетей, но и в изменении способа, с помощью которого клиентские устройства получают доступ к этим сервисам. Практически полностью прекратилась передача контента и транзакционной информации через всю сеть и произошел переход к обслуживанию с пограничных точек.

Обслуживание с пограничных точек позволяет уменьшить преодолеваемое пакетами расстояние, что, в свою очередь, снижает сетевые издержки и время реакции, обеспечивая повышение скорости. Похоже, именно эти факторы будут определять следующие несколько десятилетий.

Это не обязательно означает, что сеть становится более «затейливой», функциональной или интеллектуальной. И это точно не вычурно украшенная сеть «New IP» или нечто подобное. На самом деле, я могу утверждать, что все эти факторы являются полной противоположностью перечисленным характеристикам! Развитие Интернета следует той же логике, что и эволюция предшествующих телефонных сетей. Благодаря вытеснению различных функций за пределы сети мы избавляемся от части общих затрат, перекладывая их на подключенные устройства. А компьютерная индустрия отвечает на это созданием более мощных устройств, которые с готовностью берут на себя эти функции. Перемещая сервисы к пограничным точкам сети, мы все больше маргинализируем роль совместно используемой сети в деле предоставления цифровых услуг.

С моей точки зрения, именно эти движущие факторы будут определять следующие 50 лет эволюции компьютерных коммуникаций и цифровых услуг.

Вопросы к размышлению

Если мы правильно идентифицировали важные движущие силы, которые привели нас к сегодняшнему дню, то кажется совершенно разумным считать, что они будут продолжать действовать и в будущем, оказывая влияние на направления развития Интернета и цифровой среды. Весьма вероятно, что будет продолжаться дальнейшее усовершенствование телекоммуникационной инфраструктуры в плане создания более крупных, быстрых, совершенных и дешевых сетевых систем.

Однако я подозреваю, что в современной телекоммуникационной среде существует несколько «зародышей», которые в предстоящие годы поставят перед нами ряд интересных вопросов. Давайте рассмотрим часть таких родственных тем.

Адреса

Прежде всего обратимся к природе «адресации». Интернет позаимствовал ее у телефонных сетей, в которых каждая конечная точка была уникально пронумерована и идентифицирована. Проблема, с которой столкнулся Интернет, заключалась в том, что первоначальные оценки потребностей, равные четырем миллиардам уникальных адресов, оказались неадекватными, и нам пришлось начать затянувшийся на 20 лет, дорогостоящий и все еще не законченный переход на новую версию протокола с гораздо большим адресным пространством - на протокол IPv6. Тот факт, что этот переход еще не завершен и даже не приближается к окончанию, а также наблюдение за тем, что в нем по-прежнему не ощущается никакой острой необходимости, поднимает вопрос, почему мы считаем важным его завершение.

Является ли эта концепция универсальной идентификации конечных точек через протокольную адресацию устаревшей идеей из 1980-х, чье время уже истекло? Является ли эта абсолютная адресация свойством сетевой инфраструктуры, которая не способна угнаться за спросом на все более крупные сети? Должны ли мы отказаться от абсолютной адресации конечных точек и продолжить движение по пути использования трансляторов сетевых адресов и протоколов, более гибких в отношении адресации, как, например, QUIC? И обращаться с такими сетевыми адресами как с кратковременными сеансовыми идентификаторами, которые лишь позволяют сети избавиться от неоднозначности при направлении трафика между двумя параллельными активными сеансами и ничего больше? В то же время по-прежнему существует необходимость в уникальной идентификации услуг и точек доставки услуг, но обязательно ли это должна быть функция сети, или этим может заниматься само сервисное приложение?

Имена

Для того, чтобы компенсировать недостатки адресного пространства IPv4, мы перегружаем пространство имен. В контексте Интернета о DNS думают как о синониме адресов, которые позволяют человеку находить адресата в сети. При этом в систему имен загружают дополнительную информацию и хотят использовать DNS в качестве функции для рандеву сервисов - вместо простого отображения имени в IP-адрес. И DNS теперь не только сообщает нам IP-адрес, на который требуется отправлять IP-пакеты, но и рассказывает о том, какой транспортный протокол следует использовать и какие реквизиты шифрования услуг необходимо задействовать.

Изменение заключается в том, что DNS превращается из общего атрибута сети в набор зависящих от сервиса функций, который способен сообщить каждому клиентскому устройству, каким образом можно получить доступ к названному сервису. Если перефразировать это в более понятных терминах, то являются ли «имена» общим атрибутом сетевой инфраструктуры? Или они стали динамическими и относительными атрибутами сервиса, который разрешает клиентским устройствам «встречаться» с собой?

Ссылки

Второй аспект, связанный с именами, приводит нас к ссылочным оболочкам. Каким образом клиент идентифицирует услугу? Каким образом клиент передает эту идентичность другим участникам в виде ссылки? Критически важное семантическое различие заключается в том, что для индивидуального клиента достаточно идентифицировать услугу в показателях, которые являются авторефернтными, однако для ее независимого от клиента использования требуется дополнительный контекст. (Например, я могу найти свой местный магазин по следующей фразе: «повернуть от моего дома налево и идти до следующего перекрестка». Однако другому человеку такой алгоритм принесет мало пользы.)

Для сети с густо реплицированными точками доставки услуг имеется целый ряд дополнительных соображений. Каким образом клиент встречается с «наилучшим» экземпляром точки доставки услуги? Может ли сам клиент определить, какой из альтернативных экземпляров точки доставки является «наилучшим»? Или этот выбор должна взять на себя сеть? Либо это решение необходимо принимать самому сервису? Должна ли ссылка быть абсолютной, но решение о том, куда ведет ссылка и при каком наборе параметров выполняется сервисная транзакция, будет зависеть от клиента? Кто реализует функцию такого решения? Сеть? Или сам сервис?

Двусторонние транзакции

И наконец, если сомнению подвергают основы сетевой инфраструктуры имен и адресов, то что можно сказать о механизме транзакций? Имеет ли смысл по-прежнему представлять себе модель транзакций в виде двустороннего, синхронного обмена данными? В каком контексте имеют смысл многосторонние транзакции? Двусторонние синхронизированные транзакции подходят для многих видов коммуникации между людьми, но являются ли они наилучшим шаблоном для обмена данными между компьютерами?

Очевидно, что сегодня на все эти вопросы нет ясного ответа. Однако я думаю, что такие базовые вопросы о роли и функциях имен, адресов и ссылок представляют собой важнейшую часть эволюции архитектуры компьютерных сетей.

Тренды более длительного времени

Куда это все нас приводит? Похоже, что для построения более крупных, быстрых, совершенных и дешевых сетей нам придется передавать все больше и больше сетевых функций внутренним элементам сети, реплицировать и перемещать их ближе к границам в те места, в которых они окажутся поблизости от клиентских устройств. Кроме того, произошла трансформация мощностей для передачи данных и вычислений из дефицитного и дорогого ресурса в избыточный и дешевый товар. А это означает, что совместное использование объединенных в общий пул ресурсов больше не является неотъемлемой частью доставки услуг. Мы накопили столько ресурсов для передачи данных, вычислений и хранения, что пропала всякая мотивация использовать общую сеть для подключения клиентов к дистанционным точкам доставки услуг. Вместо этого происходит переход этих услуг к предварительному предоставлению контента для клиентов «на всякий случай», а внутренние сети теперь используются для поддержки репликации услуг с целью синхронизации всех пограничных точек доставки.

Это, в свою очередь, предвещает более значительное изменение, в рамках которого приложение перестанет быть окном доступа к дистанционно управляемой услуге, а само превратится в сервис. Я полагаю, что стремление разместить услугу как можно ближе к клиенту закончится тем, что возникнет идея напрямую предоставлять услугу на клиентском устройстве.

Все это приводит нас к финальной паре вопросов, которые я хочу поставить в связи с прогнозом на следующие 50 лет в сфере телекоммуникаций.

По итогам всего обсуждения, будут ли по-прежнему актуальны совместно используемые сети?

В настоящее время мы наблюдаем тренд на лишение сети функций и сокращение расходов на нее с переносом всего этого на конечные устройства. Это позволило добиться снижения издержек, повышения скорости и отзывчивости при предоставлении услуг. Так когда же мы остановимся? Что случится, когда все это будет перенесено на пограничные устройства? Что останется от сети и ее роли?

А как насчет самого «Интернета»?

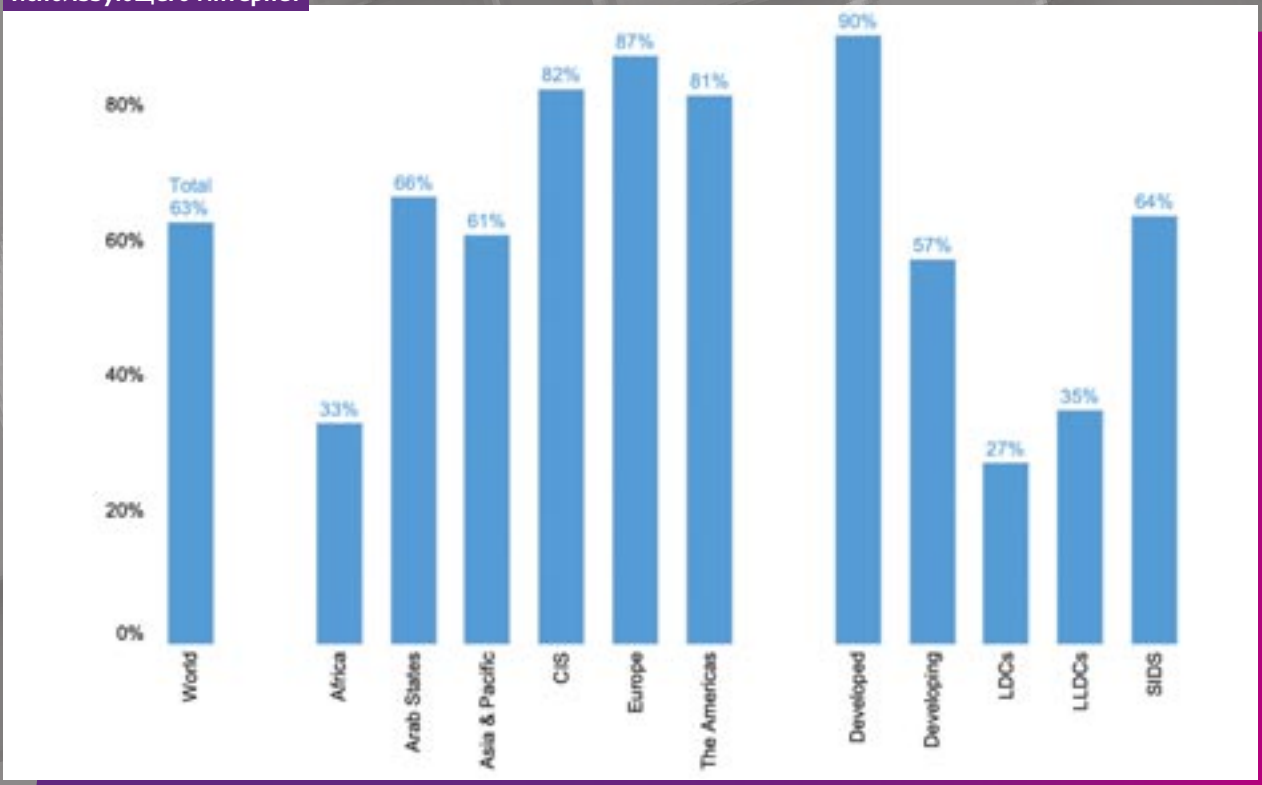
Что во всем этом определяет «Интернет»?

Мы привыкли к тому, что «Интернет» – это общая сеть, общий протокол и общий пул адресов. Любое подключенное устройство может отправить IP-пакет любому другому подключенному устройству. Таким был Интернет. Если вы используете адреса из пула адресов Интернета, то сами являетесь его частью. Этот общий пул адресов, по сути, и определял Интернет.

Сегодня это уже не так, и если продолжится дробление сети, оболочки протоколов, адресного пространства и даже пространства имен, то что останется от определения «Интернета»? Возможно, все, что останется от «Интернета» в качестве унифицирующей концепции, – это некая аморфная характеристика разнородного набора услуг, использующих общие ссылочные механизмы.

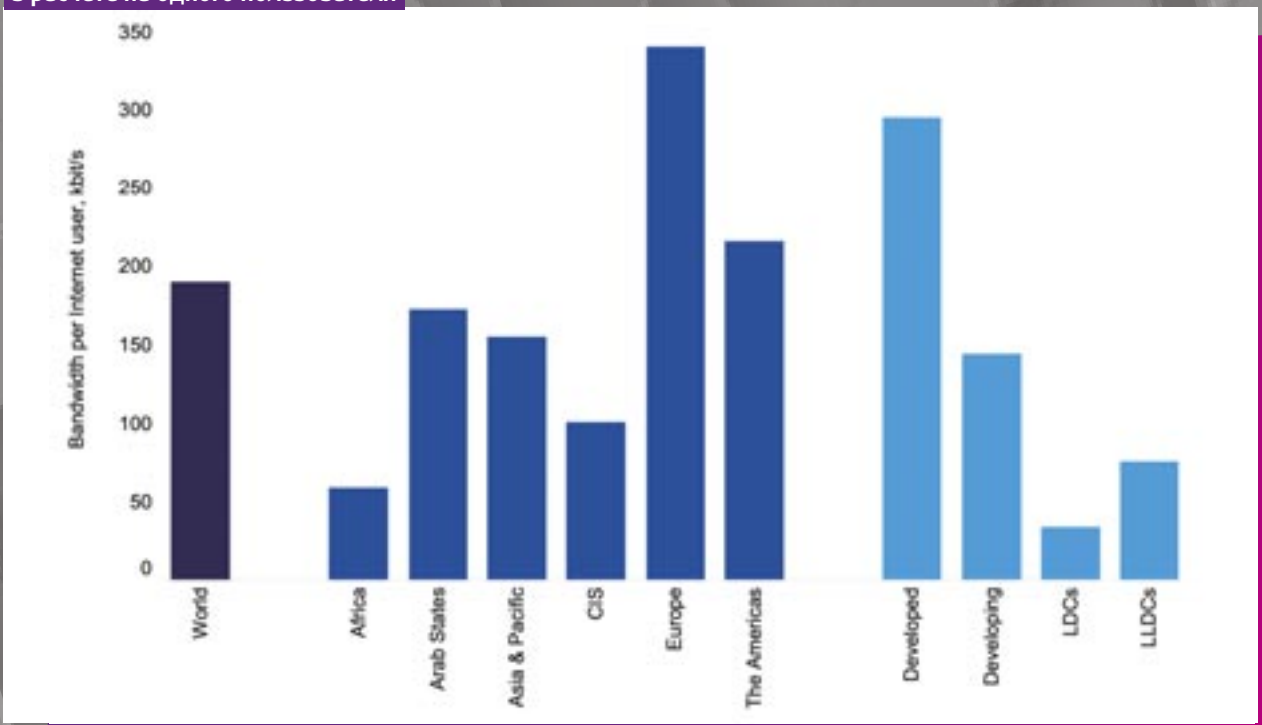
Однако в течение следующих 50 лет я хочу, чтобы сохранилась одна особенность предыдущего 50-летнего периода. Это была сумасшедшая гонка. Нам многократно удавалось подвергать сомнению все, что мы раньше понимали под возможностями этой технологии, сделав по пути несколько удивительных технических открытий. Я бы хотел, чтобы в течение следующих 50 лет мы достигли не меньшего!

Процент населения, использующего Интернет



Источник:
МСЭ, https://www.itu.int/itu-d/reports/statistics/facts-figures-2021/

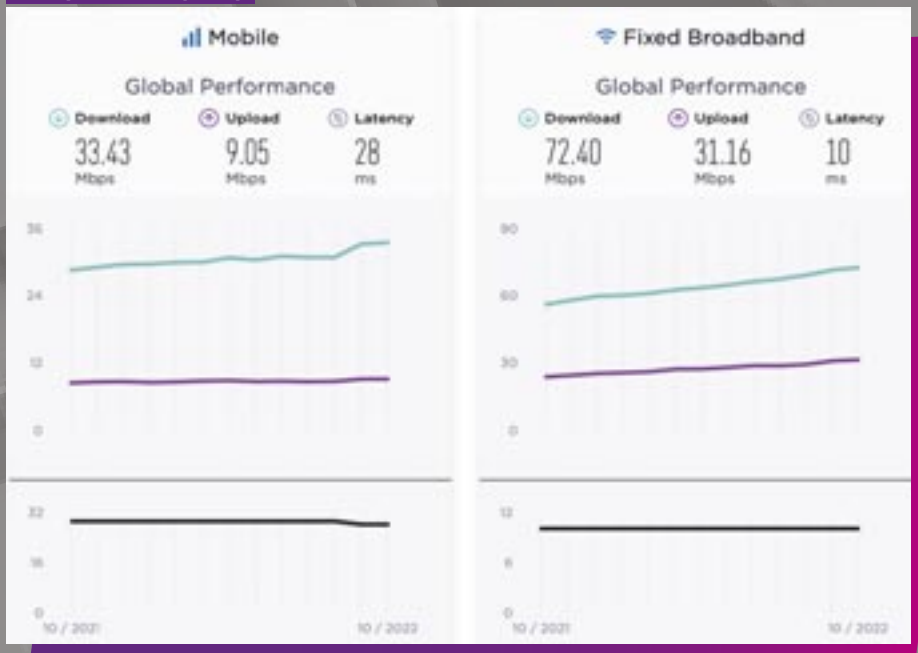
Международный трафик в расчете на одного пользователя



Источник:
МСЭ, https://www.itu.int/itu-d/reports/statistics/facts-figures-2021/

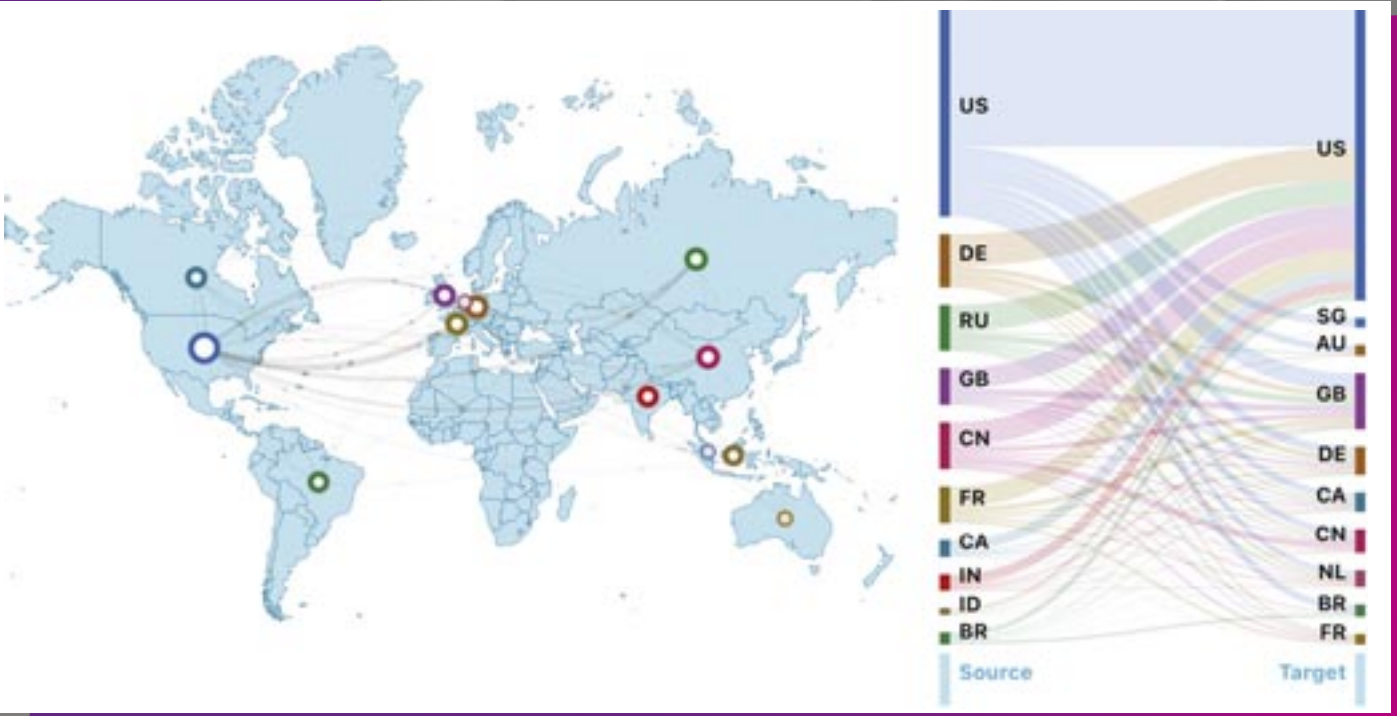
LDCs—Least Developed Countries, наименее развитые страны
LLDCs — Landlocked Developing Countries, развивающиеся страны, не имеющие выхода к морю
SIDS — Small Island Developing States, малые островные развивающиеся государства

Среднемировые скорости доступа к Интернету



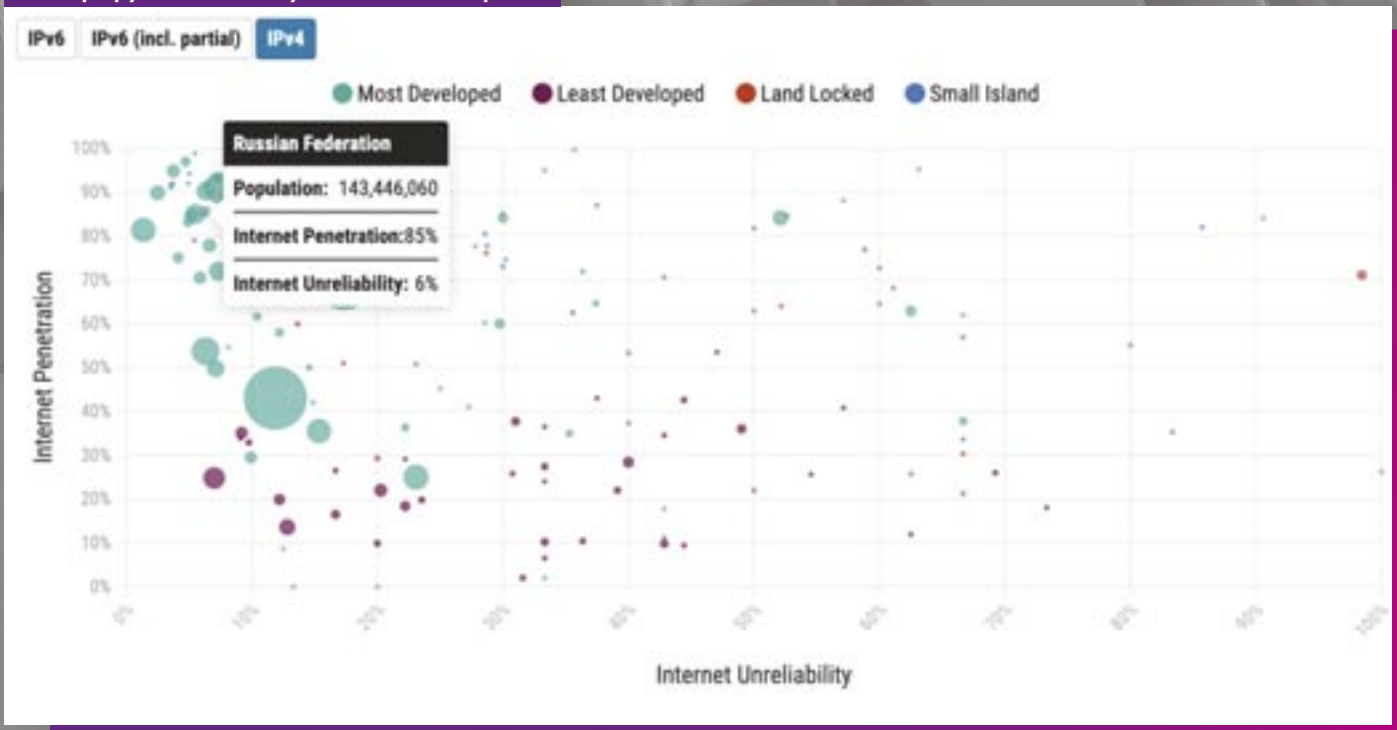
Источник:
https://www.speedtest.net/global-index

Атаки уровня приложений: Источник (Source) – Цель (Target)



Источник:
https://radar.cloudflare.com/security-and-attacks

**Индекс ненадежности Интернета.
Размер круга соответствует населению страны.**



Источник:
https://pulse.internetsociety.org/blog/internet-unreliability-around-the-world,
Данные: Qrator Labs, UN, World Bank

Цветовая кодировка:
- Наиболее развитые,
- Наименее развитые,
- Без выхода к морю,
- Островные государства

Спутниковый Интернет — очарование низких орбит

Владимир Глебский

Развитие низкоорбитальных систем спутникового Интернета является, наверное, самой злободневной темой для спутниковой связи, которая сегодня переживает один из острейших периодов своей трансформации. В прошлые десятилетия большинство услуг этой сферы было прочно связано со спутниками, базировавшимися на геостационарной орбите (ГСО) – уникальной по своим характеристикам круговой линии, расположенной в плоскости экватора Земли на расстоянии 35 786 км, где каждый спутник, вращаясь с угловой скоростью, равной угловой скорости нашей планеты, постоянно находится над одной и той же частью земной поверхности.

Использование спутников на этой орбите дает ряд неоспоримых преимуществ:

- с одной точки на орбите можно обслуживать территории целых государств в режиме 24/7;
- средний срок службы спутника на геостационарной орбите достигает 10-20 лет и зависит исключительно от надежности его аппаратуры и запасов топлива для периодической коррекции орбиты (удержания спутника в точке);
- для работы со спутником на ГСО наземные станции связи и пользовательские антенны не нуждаются в системах слежения за спутником (автосопровождением), т.к. постоянно «видят» его в одном и том же месте на «небосводе».

Указанные особенности делают системы связи на ГСО исключительно интересными для оказания услуг спутникового телевидения и радиовещания, а также организации магистральных каналов связи и передачи данных. Долгий срок службы всех элементов системы, простота и дешевизна абонентских комплектов длительное время позволяли ГСО удерживать пальму первенства в этом секторе услуг. К примеру, разместив на ГСО спутник непосредственного телевизионного вещания (СНТВ) с зоной обслуживания всей центральной части России, вы даете возможность любому жителю этой территории получить внушительный пакет ТВ-каналов, купив и установив недорогой комплект оборудования. Соответственно, битвы на полях Международного союза электросвязи (МСЭ) за приобретение и сохранение каждой точки на гео-

Рисунок 1. Плотное размещение спутников на ГСО (источник – МСЭ).

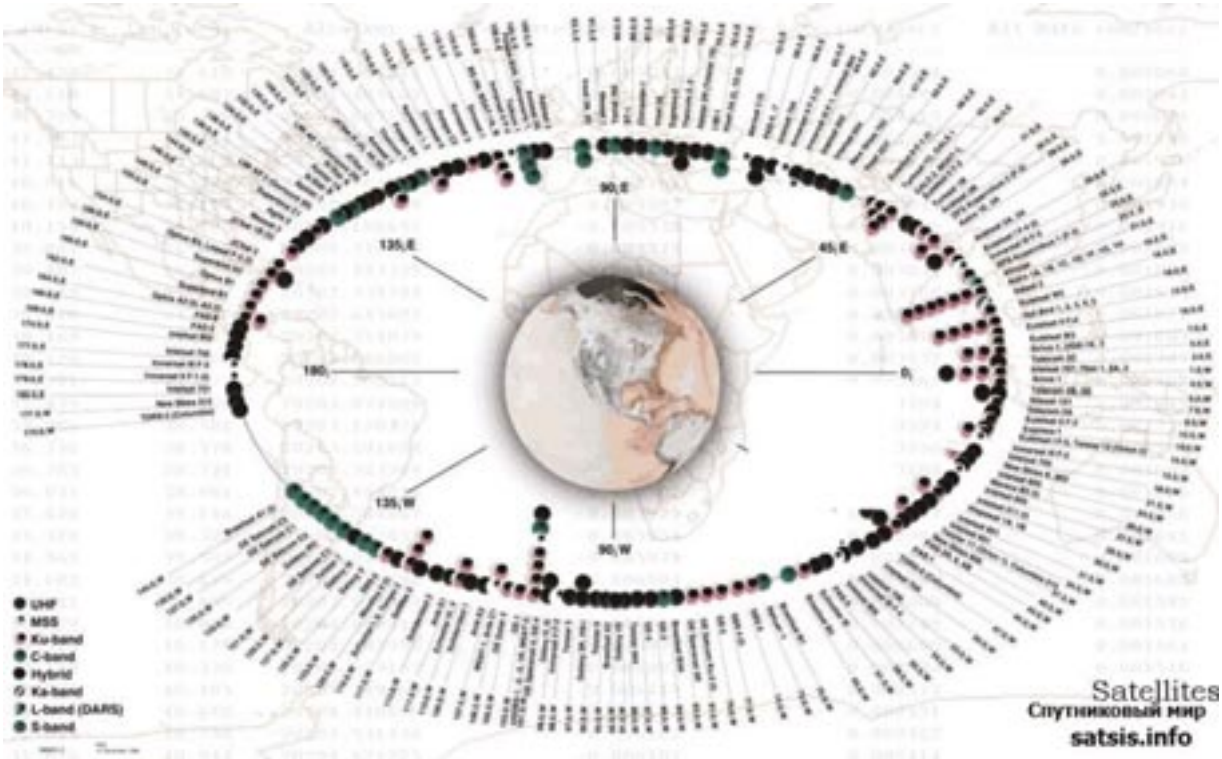


Рисунок 2. Пример зоны обслуживания спутником, расположенным на ГСО.

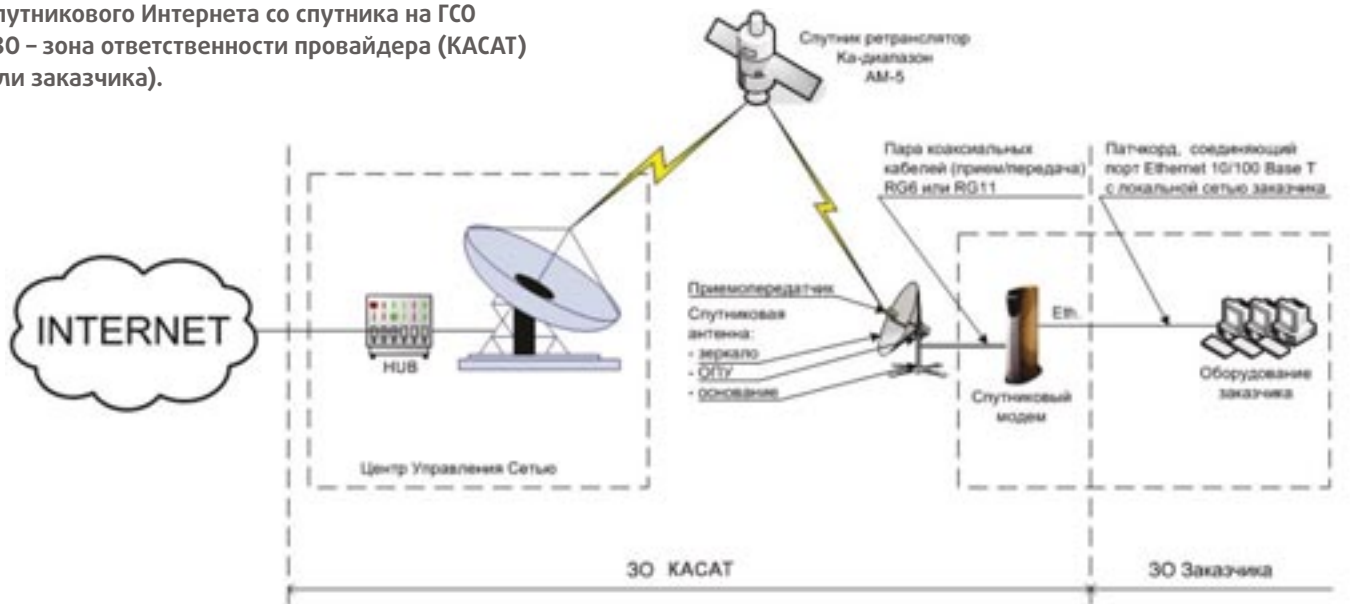
стационарной орбите (т.н. орбитальной позиции), включающее в себя право использовать в ней те или иные радиочастоты под определенные виды услуг, длительное время были одной из главных забот операторов спутниковых систем связи.

Вы спросите: «Ну а при чем же тут Интернет? Где он тут вообще?» Вот в нем-то как раз вся и загвоздка!

Интернет как технология, позволяющая передачу больших потоков разнородных цифровых данных, стал ключевым фактором ускоренного развития оптоволоконных и целого ряда беспроводных (в первую очередь сотовых) технологий. Любой спутник связи является для Интернета всего лишь каналом распространения - «трубой», по которой текут потоки цифровых данных Интернета. Эти «трубы» могут быть «широкими», «узкими», «длинными», «гладкими», «шершавыми», обладать разной «герметичностью», содержать различного вида «переходники», «разветвители» и «преобразователи», но главная их суть неизменна – доставить цифровой поток Интернета от источника к потребителю в целости и сохранности, в нужное время и без потерь. Цена и качество каждой из этих «труб» и определяет их востребованность для «монтажа» в общую «водопроводную» систему Интернета. Если данный вид «трубы» не обеспечивает необходимую пропускную способность, недостаточно «герметичен» или слишком дорог, то он остается лежать на складе.

Примерно так и произошло с традиционными спутниками на ГСО – их «трубы» оказались хоть и гладкими, но слишком длинными, узкими и дорогими по сравнению с другими вариантами. Они по-прежнему остаются привлекательными для услуг СНТВ, но неконкурентоспособны по отношению к каналам оптоволоконной или мобильной связи. «Труба» спутника на ГСО длиной в 72 000 км (2х36 000 км – расстояние, которое должен пройти сигнал от источника сигнала до спутника на орбите и обратно к потребителю, длина канала), даже при том, что она одна из самых «гладких» - скорость распространения радиосигналов в пространстве равна скорости света, что позволяет «цифровой жидкости» течь максимально быстро, - дает задержку почти в половину секунды, что для достаточно большого числа интернет-приложений неприемлемо (управление транспортом, беспилотниками, игровыми программами и т.д.). К этому еще добавились ограниченные и, в силу этого, весьма дорогие полосы частот на традиционных ГСО-спутниках, шириной от 27 до 108 МГц на один частотный канал (ствол), через эти «узкие» (в сравнении с возможностями других технологий) каналы можно было организовать потоки Интернета со скоростью не более 200 Мбит/с в стволе, а пропускная способность всего спутника ограничивалась единицами Гигабит /с. Даже с учетом коэффициентов загруженности и разновременного использования канала различными клиентами, общее число абонентов такого спутникового Интернета могло достигать максимум 20-30 тысяч на спутник, со стоимостью ежемесячной подписки от 2000 рублей за канал и с

Рисунок 3. Классическая схема организации канала спутникового Интернета со спутника на ГСО (ЗО – зона ответственности провайдера (КАСАТ) или заказчика).



негарантированной скоростью до 20 Мбит/с. Надо сказать, что в странах со значительно более дорогой, чем в России, мобильной связью (например, в США) такой спутниковый Интернет сумел получить развитие, но в России, как и в большинстве других государств мира, он оказался неконкурентоспособен. Для сравнения, число абонентов одного спутника СНТВ может достигать нескольких миллионов пользователей.

Таким образом, традиционные спутники на ГСО оказались не приспособлены к «прокачке» через себя больших потоков данных Интернета и приложений, приносящих старым и новым отраслям и направлениям услуг все большие деньги. Наметилась тенденция стагнации рынка спутниковой связи, что подтолкнуло его участников к активному поиску вариантов выживания. И к концу первого десятилетия текущего века сформировался запрос на новые спутниковые технологии, лишенные недостатков предыдущих поколений.

И вот тут, для многих неожиданно, вышли на передний план проекты орбитальных спутниковых группировок на низких орбитах. Почему неожиданно? Да потому что примеры попыток создания подобных группировок уже имели место в течение десятилетий, но практически все закончились неудачно. Взять, к примеру, нашумевший случай с банкротством системы мобильной связи «Иридиум», в которой тоже предусмотрена организация каналов Интернета (в самой последней модификации Iridium Next со скоростью всего лишь до 1,7 Мбит/с).

Все эти проекты были либо свернуты, либо прошли через «очистительную» процедуру банкротства, означающую потерю первоначальными инвесторами огромных денег. Поэтому на начальном этапе возрождения проектов на низких орбитах против голосов горстки энтузиастов зазвучал внушительный хор скептиков: системы из тысяч спутников никогда не окупятся, потому что:

- группировки спутников слишком велики, сложны и дороги в управлении;
- спутники не могут быть дешевыми, а для этих систем нужны тысячи аппаратов;
- вы разоритесь на их запусках: нужны сотни ракет;
- вы не сможете скоординировать их работу с другими системами: они будут создавать помехи;
- эти системы с глобальным охватом поверхности Земли, они в основном будут расходовать энергию на «нагрев мирового океана»;
- вас не пустят на локальные рынки целых стран и регионов по политическим и прочим другим причинам;
- и т.д. и т.п.

Нужно сказать, здравого смысла в этих замечаниях было, да и остается, немало – пока ни одна из низкоорбитальных группировок на окупаемость не вышла, интрига в самом разгаре!

Однако со временем голоса скептиков стали тише, более того, ряд скептиков быстро «перековался» и начал сам активно поддерживать эти проекты. По одной простой причине: всем нужны развитие и деньги, а на прежних технологиях, как уже было написано выше, «въехать в рай Интернета» у спутниковых операторов никак не получалось, им оставалось только смотреть, как Интернет растекается по оптоволокну, сотовым и Wi-Fi-сетям и т.д.

Рисунок 4. Громкий провал первого этапа создания низкоорбитальной системы «Иридиум»: вложившие в нее 6 миллиардов долларов США инвесторы были вынуждены продать «Иридиум» за 25 миллионов долларов.

Глобальная система спутниковой связи Iridium (США)

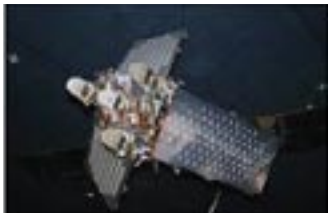
Оператор системы	Iridium Satellite LLC
Зона обслуживания	Глобальная
Число ИСЗ (орбита)	66 6+7
Параметры орбиты	H=781 км, i=86,4* (резервные спутника - на H=650 км), 6 плоскостей
Срок службы ИСЗ	7 лет
Мощность солнечных батарей	1430 Вт
Масса спутника	680 кг
Рабочий диапазон частот:	Телефон - спутник (L-диапазон) 1626,5 МГц Спутник - наземная станция (K-диапазон) 19,4-19, ГГц Наземная станция - спутник (K- диапазон) 29,1-29,3 ГГц
Число лучей	48 лучей (6 АФАР по 8 лучей)
Пропускная способность ИЗС	Скорость передачи цифрового потока в L-диапазоне при телефонной связи составляет 4800 бит/с, при передаче данных - 2400 бит/с.
Межспутниковая радиолиния:	
Рабочий диапазон частот	Ка-диапазон: 23,18-23,38 ГГц
Пропускная способность	10Мбит/с
Стоимость системы	6 млрд. долл.

Система Iridium была введена в эксплуатацию 1 ноября 1998 года. Группировка КА состояла из 66 основных и 6 резервных спутников. Однако через 9 месяцев - 13 августа 1999 года - компания Iridium Communications начала процедуру банкротства.

Сервис был снова запущен в 2001 году вновь созданной компанией Iridium Satellite LLC, принадлежавшей группе частных инвесторов. Несмотря на оценку спутников, оборудования и собственности Iridium в 6 млрд. долл. Инвесторы приобрели компанию за 25 млн. долл.

Сигнал, поступивший с телефонной трубки на ближайший спутник, передается на наземную базовую станцию, которая проверяет право использования услуг системы и вновь направляет сигнал на ближайший спутник Iridium.

Сегмент управления системой включает три основных элемента: четыре узла телеметрии, слежения и управления (ТТАС), расположенные в Аризоне и на Аляске (США) и в Икалуите (Канада), сеть эксплуатационной поддержки и оперативный центр спутниковой сети (SNOC), расположенный в Вирджинии (США) со шлюзами в Аризоне и на Гавайях.



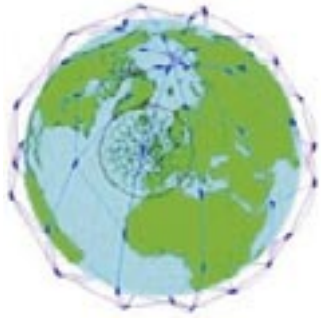
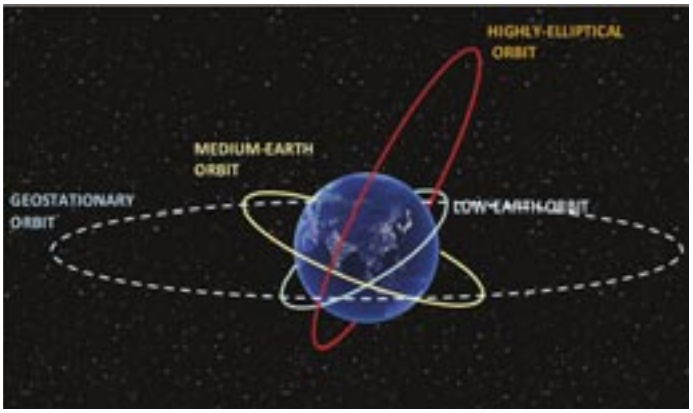


Рисунок 5. Наиболее распространенные типы спутниковых орбит для создания систем связи по классификации МСЭ: низкие (500-2000 км), средние (8000-20 000 км), геостационарная орбита (35 786 км), высокоэллиптические орбиты (до 40 000 км в апогее).



Наземная инфраструктура связи и раньше была слабым местом спутниковых операторов. Спутник всегда приходил первым, т.к. ему не нужно ничего, кроме электричества, которое можно обеспечить генераторами, солнечными батареями и т.д. По существу, появление спутникового покрытия давало толчок развитию новых мест, способствовало их заселению, развитию бизнеса, организации местного производства, давало связь и обеспечивало каналы продаж на «большую землю». Но как только новый «объект» разрастался до внушительных размеров, которые делали рентабельным прокладку до него того же оптоволокна, – «на обетованное место» приходили наземные линии связи и мгновенно «убивали» каналы спутникового оператора более дешевыми тарифами. Естественно, без всякого «спасибо». В лучшем случае спутниковые каналы сохранялись в качестве резервных на случай аварий.

В не лучшем положении оказались и инвесторы, которые специализировались на спутниковых проектах: нет проектов — некуда вкладывать! Нужно менять многолетнюю квалификацию и уходить в другие сегменты, вступать в борьбу с хорошо окопавшимися там конкурентами.

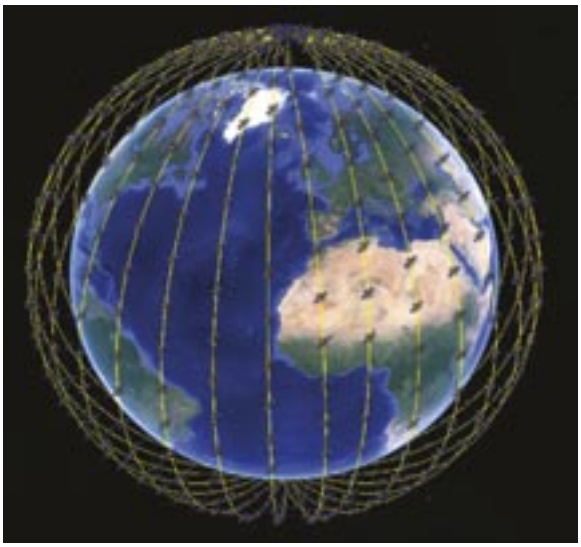
Таким образом, брошенные зерна многотысячных спутниковых проектов на низких и других негеостационарных орбитах (НГСО), обещающие огромные вложения и невероятные барыши, упали на благодатную почву: они сулили страждущим столь желанное для них будущее развитие и новые горизонты бизнеса. Трудно объяснить чем-либо иным желание инвесторов вливать огромное количество средств в проекты, которые зачастую не могли представить даже детализированных бизнес-планов. Энтузиастами этих проектов в большинстве своем стали специалисты, еще вчера трудившиеся в операторских компаниях, радевших за спутники на ГСО. Теперь они столь же активно агитировали за новые прорывные технологии на НГСО.

Чем же так привлекательны системы спутникового Интернета на низких, средних и других НГСО по сравнению с прежними решениями на ГСО?

Во-первых, степень заполнения спутниками ГСО близка к своему пределу, ГСО - это всего лишь круговая линия, на которой невозможно разместить бесконечное число спутников. Интерференция с соседними аппаратами в большинстве случаев начинает ощущаться при угловом расстоянии около 1 градуса, а этих градусов у круга всего 360. Несмотря на то, что уже давно активно используются методы установки спутников в коллокации (несколько спутников висят «гирляндой» в одной и той же орбитальной позиции, но во избежание интерференции работают в разных диапазонах частот и поляризациях), диапазоны частот для их работы тоже ограничены. Соответственно, освоение новых орбит открывает новый простор «для творчества», хотя он тоже сопряжен с процессами частотной координации новых систем со старыми, в частности, одним из решений является требование выключения низкоорбитальных спутников при пересечении ими зон работы геостационарных систем из-за угрозы интерференции сигналов. Это требование усложняет и без того непростую математику управления НГСО-

Рисунок 6. Бум заявок, подаваемых в МСЕ на координацию НГСО-систем с уже работающими системами на ГСО.

ADM	System	Sats	Orbit	Bands
CAN	CANPOL-2	51	LEO/HEO	Ka
	COMMSTELLATION	891	LEO	Ka
CHN	TXIN	60	LEO	Ka
CYP	ANDROMEDA-A	48	LEO	Ka
D	COURIER-3	72	LEO	Ka
F	AST-NG-C-1	797	LEO/MEO	Ka
	AST-NG-C-2	4872	LEO	Ka
	ES-SAT-2	1428	LEO/MEO	MEO
	MCSAT LEO	774	LEO	Ka
	MCSAT-2 HEO	312	MEO	Ka
	MCSAT-2 HEO-1	36	HEO	Ka/Ku
	MCSAT-2 LEO-1	72576	LEO	Ku
	MCSAT-2 LEO-2	2772	LEO	Ka
	MCSAT-2 MEO-1	1104	MEO	Ku
	MCSAT-2 MEO-2	744	MEO	Ka/Ku
G	L5	2892	LEO	Ka/Ku
	O3B-A/B	24	MEO	Ka/Ku
	O3B-C	840	LEO/MEO	Ka/Ku
LIE	3ECOM-1	288	LEO	Ka/Ku
	3ECOM-3	288	LEO	Ka/Ku
LUX	CLEOSAT	80	LEO	Ka
NOR	ASK-1	7	HEO	Ka/Ku
	NORSAT-H1	4	HEO	Ka/Ku
	STEAM-1	3993	LEO	Ku
	STEAM-2	3993	LEO	Ka
RUS	SKY-F	24	MEO	Ka



группировкой, состоящей из сотен и тысяч космических аппаратов. Тем не менее, НГСО – это целый пласт для новых миллиардных проектов, которые ни при каких условиях нельзя реализовать на ГСО.

Во-вторых, следует помнить, что главными конкурентами спутникового Интернета являются наземные проводные и беспроводные сети, в которых временные задержки меньше на один-два порядка (десятки и единицы миллисекунд по сравнению с почти 500 млс в сетях с ГСО). Переход на НГСО позволяет снизить задержки на порядок, что для многих интернет-приложений имеет принципиальное значение.

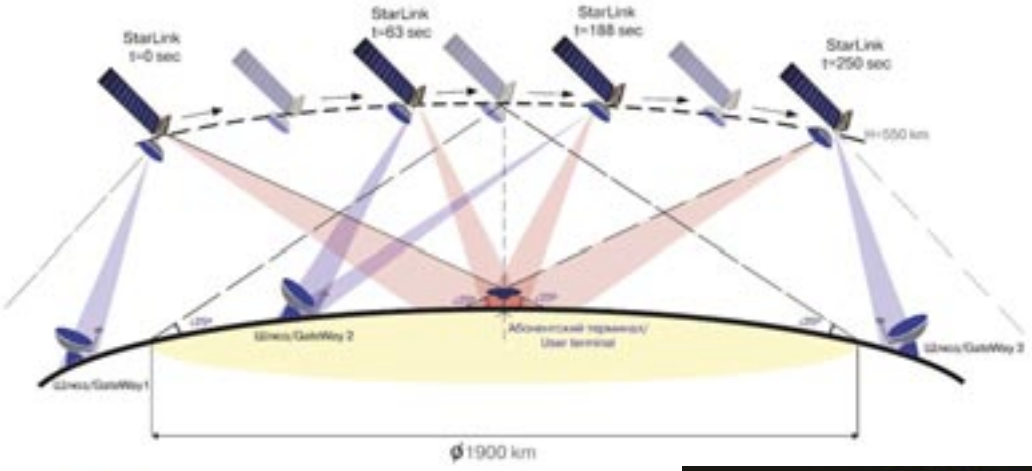
В-третьих, за счет перемещения НГСО-спутников по орбите их работа с наземным терминалом осуществляется, когда спутник «пролетает над головой». За какой бы естественной преградой (дерево, гора и т.п.) на открытой местности ни находился абонентский терминал, в большинстве случаев он видит нужное для получения информации количество спутников. Тогда как для спутника на ГСО необходимо подбирать подходящее для терминала место, с которого он увидит геостационарный аппарат.

В-четвертых, немалую роль в продвижении проектов на НГСО сыграло развитие спутниковых технологий, совершивших за последние два десятка лет революционный скачок по целому ряду направлений.

Этому способствовали:

- развитие электроники и программного обеспечения для создания программно управляемых полезных нагрузок космических аппаратов с программно-электронными системами формирования и управления лучами и многолучевыми системами;
- развитие технологий многократного использования радиочастот, которые активно стали применяться как на спутниках, так и в наземных системах связи;
- развитие технологий повторного использования компонентов и систем запуска спутников на орбиту (произошло удешевление запусков космических аппаратов за счет применения многоразовых элементов и блоков);
- развитие технологий массового (поточного, конвейерного) производства однотипных малых и средних спутников из унифицированных блоков и систем;
- расширение спектра ракетоносителей и технологий массового (пакетного) выведения спутников на орбиту;
- развитие технологий «плоских антенн» (антенных фазированных решеток) с программно-электронным управлением для работы наземных терминалов связи с космическими аппаратами связи на различных орбитах;
- развитие технологий межспутниковых радио- и оптических линий.

Рисунок 7. Сравнение схем организации передачи трафика Интернета в геостационарной и низкоорбитальной (StarLink) системах.



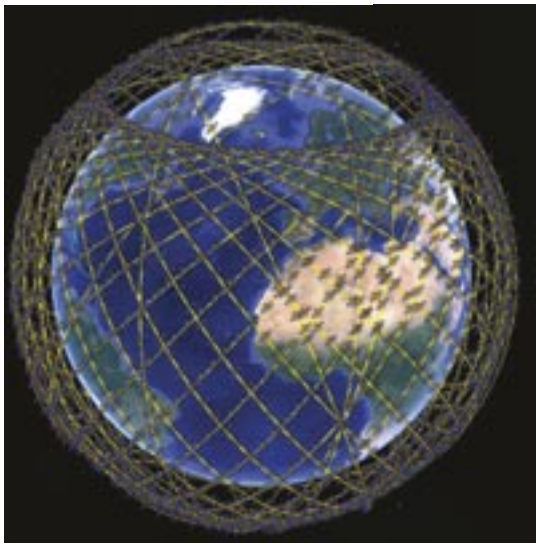
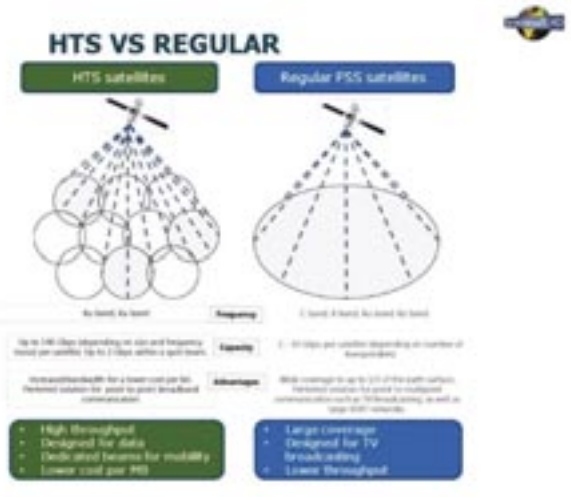
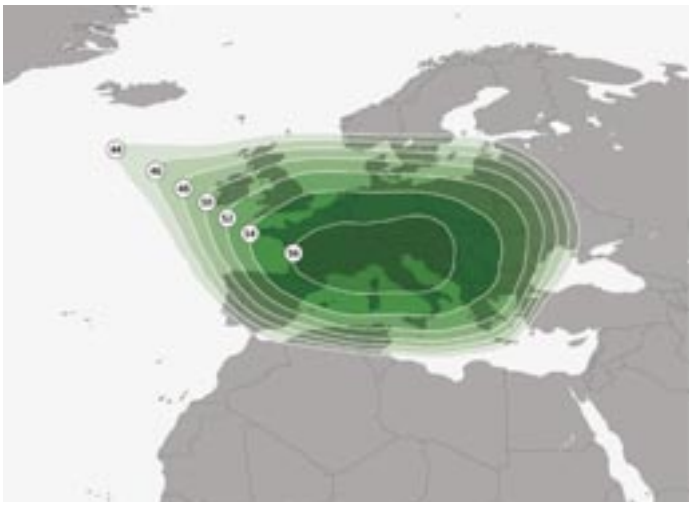
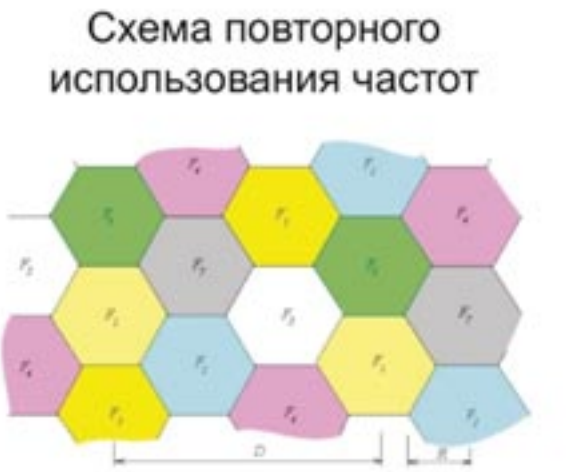
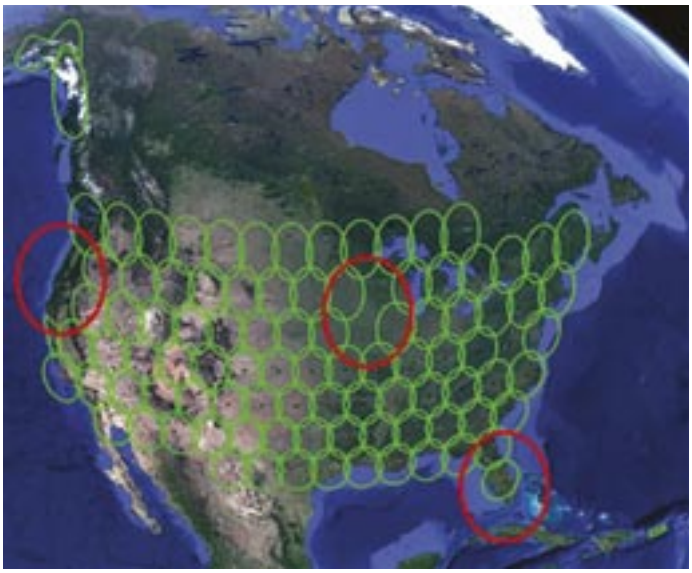


Рисунок 8. Трансформация спутников на ГСО из «традиционных» в спутники высокой и сверхвысокой пропускной способности (HTS и VHTS).







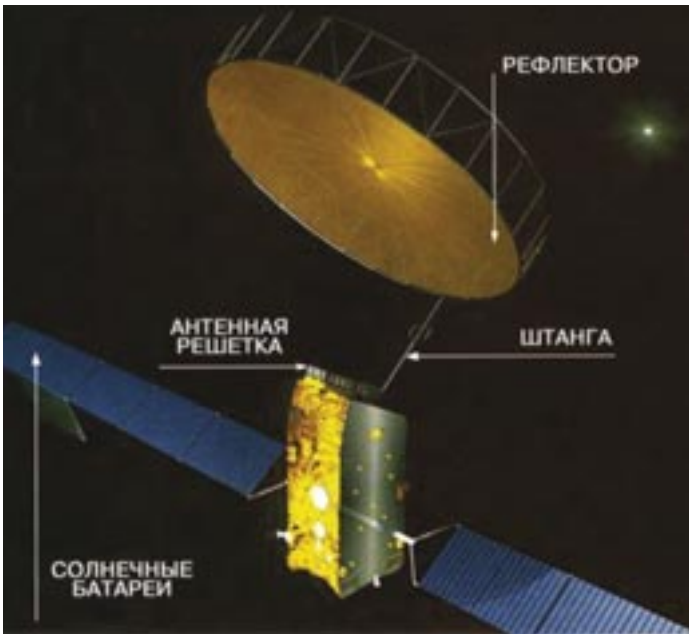


Этот технологический рывок сделал физически возможной реализацию многоспутниковых проектов на НГСО.

Однако интрига выбора между геостационарными и негеостационарными системами сохраняется.

Дело в том, что технологический скачок коснулся всех спутниковых систем, не только негеостационарных. Геостационарные системы тоже получили новые варианты развития, существенно укрепляющие их позиции на рынке, и при этом сохранили характерные для них преимущества, такие как простота и относительная дешевизна абонентских терминалов, значительно более простая система управления спутниками и трафиком, длительные сроки эксплуатации аппаратов на орбите. Геостационарную орбиту начали заполнять спутники высокой производительности (High throughput satellites, HTS), которые вместо нескольких Гбит/с, как это было ранее, получили пропускную способность в несколько сотен Гбит/с и даже Тбит/с за счет применения технологий многократного использования частот, к которым также добавляются гибкие полезные нагрузки, позволяющие эффективно управлять трафиком во всей системе и перераспределять мощность в зонах обслуживания, подстраивая конфигурацию сети под нужды заказчиков.

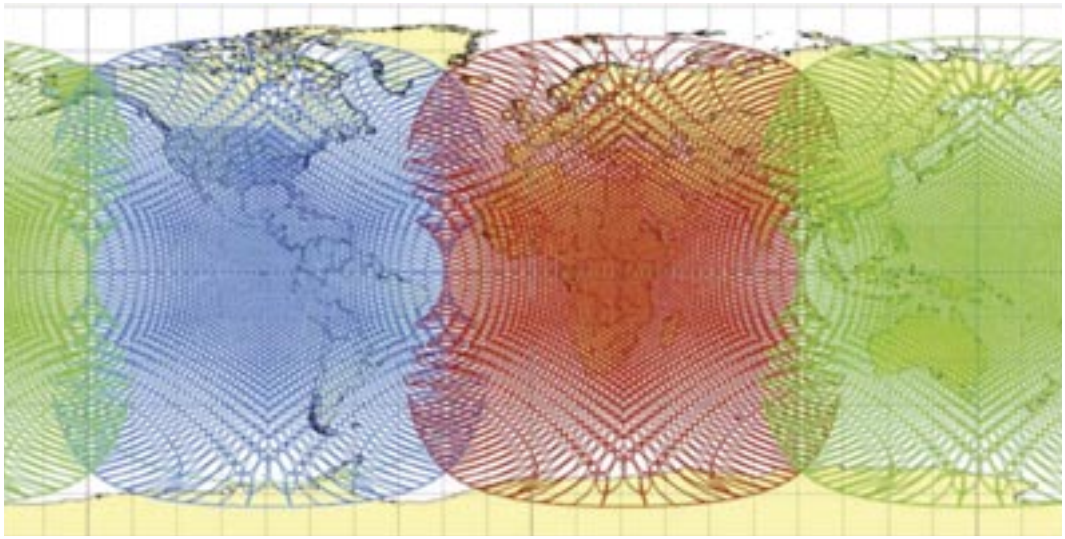
Рисунок 9. Внешний вид и компоновка основных элементов спутника HTS.



Из наиболее продвинутых в этом плане сегодня можно выделить спутник VHTS ViaSat-3 одноименной компании-оператора ViaSat, пропускная способность которого достигает 1 Тбит/с.

При этом сравнивать пропускную способность системы из трех VHTS-спутников ViaSat-3 и, к примеру, всей системы из четырех тысяч спутников StarLink, где для каждого спутника заявляется пропускная способность примерно в 20 Гбит/с, а тем более оценивать их экономическую составляющую - дело довольно сложное. В организации канала Интернета StarLink участвует целая группа N пролетающих мимо абонента спутников, тогда как в системе ViaSat-3 это один и тот же канал, т.е. пропускную способность StarLink надо делить на N - и это не единственный нюанс! 70% территории Земли покрыто океанами, где кроме одиночных кораблей нет потребителей, а значит, пролетающие над ними спутники НГСО будут просто «греть воду». Срок службы спутников на низкой орбите составляет в среднем около пяти лет, что в 3-4 раза меньше, чем у спутников на ГСО, следовательно, систему надо постоянно обновлять. Кроме того, система управления трафиком требует строительства гораздо большего числа шлюзовых станций, сложной математики. Значительно усложняются и сами абонентские терминалы – они должны быть следящими, вовремя переключаться на спутники низкоорбитальной системы и иметь соответствующую математику и служебную информацию. Мало того, существуют политические, нормативные и другие барьеры, которые приводят к тому, что услуги этих систем могут и вовсе оказаться невостребованными в целом ряде государств. А поскольку системы эти фактически строятся и модернизуются буквально на ходу, однозначно оценить перспективы этого направления сейчас невозможно. Добавляют интриги и разработки спутникового 5G последних лет, обещающие дать Интернет непосредственно со спутника на смартфон. Увлекательнейший сериал о соревновании разных видов спутникового Интернета продолжается, смотрите новые серии!

Рисунок 10. Спутник сверхвысокой пропускной способности (VHTS) ViaSat-3 и многолучевая зона глобального покрытия Земли, формируемая системой из трех таких аппаратов.



ЦОДы будущего: основные тенденции развития

Николай Носов

Современную жизнь уже невозможно представить без цифровых технологий. И это только начало. Большие данные, искусственный интеллект, электронное правительство, автономные автомобили, умные города… Информационные технологии стремительно развиваются, оцифровывается все что можно, объемы данных стремительно растут, а для их хранения и обработки нужны дата-центры, которые в условиях построения цифровой экономики становятся ключевым элементом цифровой инфраструктуры как отдельных предприятий, так и страны в целом. Попробуем разобраться, в каких направлениях развиваются современные дата-центры, или центры обработки данных (ЦОД), какие используются технологии и архитектуры.

Что такое ЦОД?

На законодательном уровне определением понятия ЦОД занялись совсем недавно. В мае этого года в принятых Госдумой РФ в первом чтении поправках к закону «О связи» дается следующая формулировка: «ЦОД – сооружение связи с комплексом систем инженерно-технического обеспечения, спроектированное и используемое для размещения оборудования, обеспечивающего обработку и (или) хранение данных, и соответствующее утвержденной классификации». Проще говоря – здание или группа зданий для размещения компьютеров, телекоммуникационных систем и систем хранения данных.

По большому счету – не обязательно здание, IT-нагрузку можно размещать в различного рода контейнерах, причем не только на поверхности земли, но и в пещерах, под водой и даже в космосе. Главное – создать условия для надежной бесперебойной работы вычислительного оборудования. Для этого ЦОД должен обеспечить надежную инфраструктуру электроснабжения, отвода тепла и каналов передачи данных. Оборудование должно быть защищено от пожаров и других негативных внешних воздействий, от несанкционированного доступа посетителей и персонала.

В настоящее время стандартный ЦОД – это, как правило, специально построенное (модель greenfield) или реконструированное (brownfield) здание для обеспечения наилучших условий размещения IT-оборудования, рассчитанное на 200-1000 стоек. Классифицируя по размерам, можно выделить микроЦОДы – шкафы с одной стойкой, миниЦОДы – контейнеры с несколькими (как правило, от двух до 10) стойками, малые ЦОДы до 200 стоек и мегаЦОДы – более 1000 стоек. Самая высокая стоимость одной стойки – в микроЦОДе. Самая низкая – в мегаЦОДе, что достигается за счет масштаба, более эффективного использования технических средств и сокращения расходов на администрирование.

По конструкции ЦОДы можно разделить на контейнерные, размещающиеся в одном или нескольких контейнерах, как правило, стандартного размера, модульные – собираемые из изготовленных в заводских условиях крупных блоков – и стационарные, когда ЦОД строится на месте.

По модели использования ЦОДы делят на коммерческие, когда оператор ЦОДа предоставляет его клиентам по сервисной модели, например, для размещения стоек со своим оборудованием (модель colocation), и корпоративные – создаваемые предприятием для своих нужд.

МегаЦОД Сбербанка в «Сколково». Фото Николая Носова

Возвращаясь к российскому определению, вспомним про требование соответствия утвержденной классификации. Классификация пока не разработана, но на практике большинство ориентируется на классификацию по уровню надежности Uptime Institute (https://uptimeinstitute.com/tier-certification). Соответствующий уровню Tier I дата-центр имеет базовую инженерную инфраструктуру (источники бесперебойного питания, системы охлаждения), но ее элементы не зарезервированы, и выход из строя важного узла приведет к нарушению работы или даже остановке объекта. Самый надежный, соответствующий уровню Tier IV ЦОД имеет полное дублирование инженерной инфраструктуры и без проблем переживет поломку любого узла. Но и стоит такой ЦОД немало.

Впрочем, иногда можно использовать ЦОДы, которые не соответствуют даже нижнему уровню надежности – например, для обеспечения отказоустойчивости на уровне архитектуры или дублирования ЦОДов, как это делает компания Yandex. Такой подход возможен и в случае, когда остановка дата-центра не критична для выполняемых задач, как в случае использования оборудования для майнинга. Но и здесь нужно заниматься инженерной инфраструктурой, ведь в противном случае дорогое IT-оборудование может выйти из строя или даже сгореть.

Эффективность

Бизнес – это про деньги, а затраты на электричество – основная статья операционных расходов. Не удивительно, что главное направление развития ЦОДов – повышение энергоэффективности. Для ее оценки используется показатель PUE (Power Utilization Efficiency), который определяется как соотношение полной электрической энергии, потребляемой ЦОДом, к энергии, которая расходуется непосредственно IT-оборудованием.

Чем ниже PUE, тем лучше. В идеале – единица, и к этому значению уже приближаются лучшие дата-центры.

Перспективным выглядит концепция OCP (Open Compute Project, https://www.opencompute.org/) – повышение энергоэффективности, снижение стоимости владения оборудованием и ускорение развертывания путем использования специализированных серверов, блоков питания, серверных стоек и систем резервного питания. В соответствии с требованиями стандарта в новых стойках питание серверов стандартизовано и осуществляется с помощью вертикальной шины постоянного тока, которая проходит по всей высоте стойки. Для подачи питания используются силовые полки, что уменьшает количество промежуточных преобразований электроэнергии по пути, повышая общую энергоэффективность ЦОДа.

Значительно снизить энергопотребление системы охлаждения дата-центра можно, используя технологию фрикулинга (свободного охлаждения). Самые эффективные системы охлаждения – с прямым фрикулингом, но они требуют, чтобы температура уличного воздуха даже в летний период была ниже температуры в компьютерном зале. Таких мест немного. Новая технология – «холодные стены», которые за счет большой площади теплообмена позволяют обеспечить выход на режим фрикулинга при более высоких температурах наружного воздуха. При этом снижение нагрузки на компрессор увеличивает его срок службы.

Самая распространенная на сегодня реализация технологии фрикулинга в мире – чиллеры с системой динамического фрикулинга и турбокомпрессорами. При внешней температуре ниже +15°C такие системы работают в режиме фрикулинга, используя холод уличного воздуха, а выше этой температуры включаются чиллеры. Если учесть, что по статистике 82% времени в году в средней полосе России температура не поднимается выше +15°C, то экономия электроэнергии может оказаться весьма внушительной, достигая 45% по сравнению с обычными фреоновыми DX-системами охлаждения.

Ну и конечно много усилий уходит на повышение энергоэффективности самих чиллеров и другого используемого в ЦОДе инженерного оборудования.

Перспективный подход к повышению энергоэффективности – комбинация решений. Например, российская компания ITK вывела на рынок новую линейку систем охлаждения, в которую входят и нетрадиционные решения, так называемые гибридные. Это совокупность жидкостного охлаждения самых важных узлов сервера, таких как центральный и графический процессор, и воздушного охлаждения менее нагруженных компонентов.

Холодный коридор в ЦОДе «Миран» в Санкт-Петербурге.
Фото Николая Носова

Чем выше допустимая температура в компьютерном зале, тем меньше нужно электроэнергии на его охлаждение. Значительной экономии электричества можно добиться, используя «теплолюбивые» серверы, работающие при температуре окружающей среды выше 40°C. Правда, как указывают эксперты, при повышении температуры воздуха срок эксплуатации жестких дисков сокращается, а при динамично меняющейся вычислительной нагрузке необходимо будет устранять локальные перегревы в стойках.

Рекордно низкого PUE можно достичь, применяя жидкостное охлаждение. При погружном (иммерсионном) способе вычислительную систему помещают в диэлектрические жидкости, как правило, минеральные или синтетические масла. При контактном – подводят к охлаждающей материнскую плату пластине трубочки с теплоносителем – водой или водяными растворами. Оба подхода используются при высокопроизводительных вычислениях (суперкомпьютеры, HPC), а иммерсионный – еще и при майнинге.

Окупаемость ЦОДа сильно зависит от эффективности использования площади компьютерного зала. Один из трендов – увеличение нагрузки на стойку. И если совсем недавно стандартом были стойки по 5 кВт, то сейчас все чаще 8-10 кВт. Для высокопроизводительных вычислений (High Perfomance Computing, HPC) нагрузка на стойку может достигать 30 кВт.

Наиболее распространенная система охлаждения – с изоляцией холодных и горячих коридоров. Циркуляция воздуха организуется таким образом, чтобы горячие и холодные потоки не пересекались и не смешивались. Смешиванию препятствует размещение стоек плотно в два ряда, разделенных коридором, установка заглушек и изоляционных панелей. Как правило, холодный воздух подается в коридор – сбоку внутрирядными кондиционерами или снизу через перфорированный фальшпол шкафными кондиционерами, он охлаждает IT-оборудование и возвращается в компьютерный зал. Повышение энергоэффективности и снижение занимаемой в компьютерном зале площади внутрирядных и шкафных кондиционеров – одно из направлений работы проектировщиков ЦОД.

Минимизировать площадь, занимаемую в компьютерном зале инженерным оборудованием, позволяет и использование других подходов к охлаждению, например, уже упомянутых выше «холодных стен».

Экологичность

Напряженная геополитическая обстановка многих заставила забыть о «зеленой повестке», но проблемы загрязнения окружающей среды и глобального потепления никуда не делись. И ЦОДы, особенно мегаЦОДы, должны прилагать усилия для снижения своего негативного влияния на будущее планеты.

Прежде всего – снижать электропотребление, задача, во многом совпадающая с задачей повышения энергоэффективности. Чем ниже PUE, тем меньше энергии расходуется напрасно. Еще лучше – не выводить тепло в атмосферу, а использовать в полезных целях, например, для отопления домов, что уже применяется в одном из дата-центров Хельсинки.

Другая проблема связана с теплоносителями. Применяемый в чиллерах фреон разрушает озоновый слой и способствует образованию «озоновых дыр». Уже есть решения по замене его на аммиак, имеющий нулевой потенциал разрушения озона (ODP = 0) и нулевой потенциал глобального потепления (GWP = 0). Такая технология используется в Schwarz IT Data Center. Но еще лучше, если условия позволяют, совсем отказаться от чиллеров и перейти на фрикулинг. Например, охлаждать оборудование испаряющейся естественным путем водой, как это сделано в ЦОДе Inoventica во Владимирской области, где используется вода из старицы Клязьмы.

Возобновляемыми источниками энергии – ветром и водой – обеспечен норвежский дата-центр, открытый в 2017 году в выработанной шахте на глубине 150 метров близ фьорда Лефдаль. Серверные стойки IBM находятся в контейнерах. Естественным теплоотводом служит сам фьорд, глубина которого составляет более 560 метров.

«Зеленые» технологии дошли и до систем пожаротушения дата-центров. Вместо вредного для людей хладона в последнее время стали применять «сухую воду» – разработанное американской компанией 3M пожаротушащее вещество Novec 1230 или более дешевый российский аналог «Инерген».

Любой пожар можно потушить ложкой воды, только нужно знать, где и когда ее вылить. Альтернативный вариант – защита ЦОДа установками пожаротушения тонкораспыленной водой HI-FOG, когда водяным облаком окутывается не весь компьютерный зал, а лишь место возгорания. Да и вода, даже дистиллированная, намного дешевле хладона. В России такая система пожаротушения уже используется в дата-центрах Moscow One и Moscow Two компании Ixcellerate.

Автоматизация и искусственный интеллект

Эпидемия COVID-19 и последующие ограничения еще раз продемонстрировали, что человек является слабым звеном в системе эксплуатации дата-центра. Мало того, что сотрудник может заболеть, заразить коллег и вывести из строя целую смену, он еще и не в состоянии переварить огромное количество данных, собираемых в процессе эксплуатации ЦОДа.

В диспетчерской ЦОДа Selectel в Санкт-Петербурге.
Фото Николая Носова

Инженеры проверяют серверы и систему охлаждения Project Natick. ЦОД имеет примерно те же размеры, что и стандартный грузовой контейнер.
Фото: Франк Бетермин. Источник: https://news.microsoft.com/ru-ru/features/project-natick/

Размещение дата-центров под водой снимает массу вопросов по строительству, аренде и коммуникациям на чужой территории. Кроме того, морская вода используется для охлаждения, что дешево и экологично.

Запускать быстрее

Чем быстрее ЦОД будет введен в строй, тем быстрее начнут окупаться вложенные в него инвестиции. Скорость возведения дата-центров постоянно растет.

Службам эксплуатации помогают многочисленные автоматизированные системы, обрабатывающие сигналы и выводящие информацию в адаптированном для человека виде. Но идеальный вариант – «темный ЦОД», когда в компьютерном зале не надо даже включать свет (еще один небольшой вклад в энергоэффективность), так как в нем нет обслуживающего персонала. IT-оборудованием и так управляют удаленно, а вмешательства человека в работу инженерных систем не требуется.

К этому идут, перекладывая все больше функций человека на «умное» оборудование, проводящее самодиагностику и выбирающее оптимальный режим работы. Системы предиктивной аналитики предсказывают выход оборудования из строя и дают сигнал о необходимости его замены. Автоматизированные системы DCIM (Data Center Infrastructure Management) моделируют влияние изменений на воздушные потоки между горячим и холодным коридором, нагрев отдельных зон компьютерного зала и подсказывают, как оптимально разместить оборудование и какие изменения стоит произвести в инженерной инфраструктуре.

Системы с искусственным интеллектом уже используются в ЦОДах и с развитием технологий будут использоваться еще шире. Но пока без человека в большом ЦОДе не обойтись – по крайней мере, он нужен для демонтажа вышедшего из строя инженерного оборудования и установки нового. Уж не говоря о вычислительной технике – серверы в стойку роботы еще не ставят.

А вот «темный» контейнерный ЦОД уже реальность. Летом 2018 года в рамках второй фазы испытаний проекта Natick по производству и эксплуатации экологичных и автономных сетевых систем команда Microsoft опустила на морское дно на глубину 35 метров в прибрежных водах Шотландии контейнер с небольшим дата-центром внутри. К суше он подключался силовым и оптоволоконным кабелем, вместо воздуха в контейнер закачали азот, что исключило возможность пожара. Через два года компания подняла ЦОД и отчиталась об успехе проекта — за это время вышло из строя в восемь раз меньше серверов, чем в аналогичной конфигурации на суше.

В этом тоже помогают цифровые технологии, планирующие и распараллеливающие работы на строительной площадке. Моделирование ЦОДа позволяет не только заранее получить цифровой двойник объекта, но и предотвратить опасные ситуации, например, когда силовой кабель прокладывается по сильно нагревающемуся коробу.

Значительно ускоряет строительство использование модулей, собранных и протестированных в заводских условиях. Такой подход повышает качество сборки. Модульные ЦОДы легко масштабируются и возводятся быстрее стационарных.

Еще быстрее запускаются контейнерные ЦОДы. Они полностью готовятся в заводских условиях – их достаточно привезти на место и подключить к электропитанию и каналам связи. Можно забросить на удаленный объект в любую глухомань вертолетом. Когда в ЦОДе отпадет надобность – вывезти обратно. А масштабирование достигается установкой дополнительных контейнеров.

Практически не требует времени на развертывание мобильный ЦОД, представляющий из себя специализированный контейнер, поставленный на колеса. Он изначально подключен к каналам связи и оснащен комплексом информационной, телекоммуникационной и инженерной инфраструктуры.

Ближе к данным

МегаЦОДы снижают стоимость услуг, но в любом месте их не построишь — не хватит достаточной для окупаемости проекта вычислительной нагрузки. С другой стороны, многие данные выгодней не гонять по каналам связи, а обрабатывать на месте в периферийных или edge-ЦОДах. Особенно это становится заметным, если каналы дорогие и медленные, а расчеты надо проводить быстро, иногда в режиме реального времени – тогда в большой ЦОД отправляются только агрегированные и обработанные данные, которые собирают для сводной аналитики с периферии.

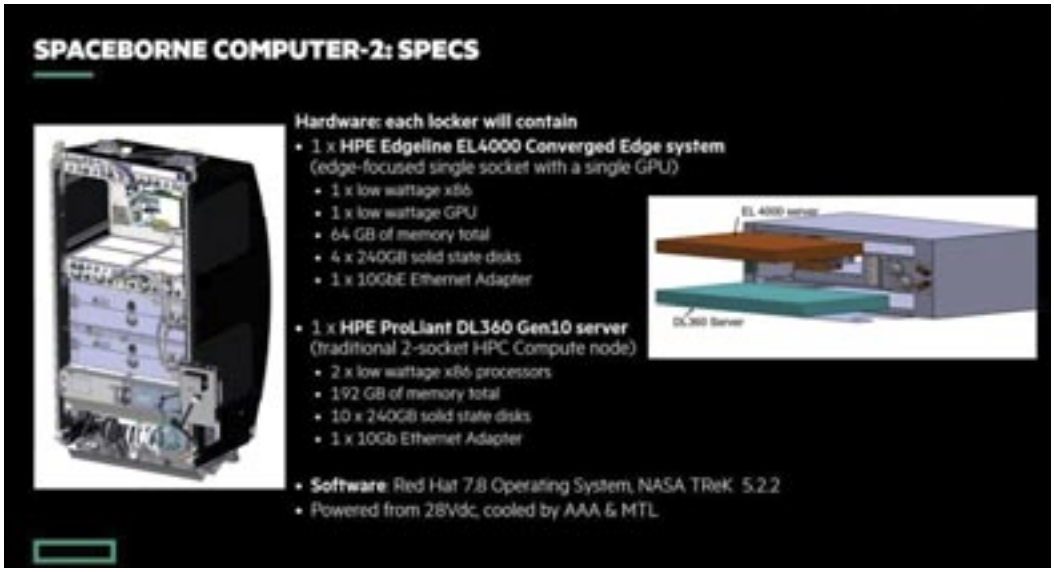
Еще одним важным преимуществом edge-ЦОДов является автономность, то есть возможность работы при разрывах

связи с облаком центрального ЦОДа. Когда связь восстановится — накопленные обработанные данные передадут в центр.

Типичный пример – edge-ЦОД на буровой на земле или даже на море. Вся оперативная информация нефтяников оперативно обрабатывается на месте. И только самая важная отправляется через спутниковый канал в ЦОД на материк.

Edge-ЦОДы активно используются на предприятиях и заводах с распределенной структурой. В цехе с вредным производством в качестве edge-ЦОДа может выступать микроЦОД с повышенным уровнем защиты корпуса, например, от пыли или влаги. В большом филиале – миниЦОД, в тайге – контейнерный.

Spaceborne Computer-2. Фото: hardwareluxx.ru



Термин edge – связывающий узел на границе сетей – появился в телекоме. В качестве пограничного часто рассматривают и микроЦОД базовой станции. Тем более, что в современной концепции Mobile Edge Computing (MEC) в нем можно проводить компьютерные и облачные вычисления. По сути MEC – это программная платформа для запуска приложений, развернутая на инфраструктуре виртуализации NFV (Network Functions Virtualization) микроЦОДа, который вынесен в радиосеть, например, на базовую станцию. Таким образом операторы мобильной связи могут выступать в роли провайдеров услуг периферийных вычислений.

ЦОДы в космосе

В феврале 2021 Hewlett Packard Enterprise в партнерстве с NASA развернула на Международной космической станции (МКС) edge-ЦОД, доступ к которому можно получить через облако Microsoft Azure. Spaceborne Computer 2 представляет собой ящик с контейнерами, в каждом из которых установлен сервер HPE Proliant DL360 Gen10 для высокопроизводительных вычислений и оснащенная графическим процессором конвергентная edge-система Edgeline EL4000.

Расположенные на борту МКС датчики собирают огромные объемы информации, для дальнейшей обработки которой требуется мощный канал связи с Землей. Edge-ЦОД на борту МКС разгружает каналы связи, обрабатывая первичные данные с датчиков, приемников и камер непосредственно на месте, в космосе. Это позволяет вести в режиме реального времени мониторинг состояния здоровья космонавтов и на основе анализа физиологических параметров устанавливать диагнозы. Можно анализировать данные об атмосфере и посылать на Землю информацию для прогнозов погоды или выявления вредных выбросов, следить за движущимися в космосе и в атмосфере объектами, фиксировать запуски ракет.

Графические процессоры помогут в решении задач машинного обучения и искусственного интеллекта, обработки изображений с высоким разрешением, например, фотографий полярных ледяных шапок на Земле или медицинских рентгеновских снимков космонавтов.

Принимавшая участие в работах на МКС компания Lonestar Data Holdings Inc. из Санкт-Петербурга (St.Peterburg), правда, не российского, а из американской Флориды, в апреле 2022 года объявила, что запускает серию центров обработки данных на лунной поверхности. Компания заключила контракт на первых два полета на Луну и сборку на ней первого дата-центра. Lonestar занимается разработкой сервера, а за проект спускаемого аппарата Nova-C и планирование его посадки отвечает компания Intuitive Machines.

Lonestar рассматривает Луну как идеальное место для обслуживания премиум-сегмента глобальной индустрии хранения данных стоимостью 200 миллиардов долларов. Пилотный «лунный ЦОД», который планируется доставить на поверхность нашего спутника и разместить вблизи холмов Мариус в океане Процелларум в вырытой роботами шахте до конца 2024 года, не подразумевает активный обмен данными, а будет служить в качестве бэкапа для наиболее важной и неизменяемой информации.

При удачном исходе эксперимента следующие экспедиции доставят на Луну более мощные серверы, а роботы наладят полноценный обмен информацией между Луной и Землей. К концу 2026 года планируется довести этот показатель до 15 гигабит в секунду.

Дата-центры прочно вошли в нашу жизнь. ЦОДы постоянно улучшаются, становятся все более надежными, эффективными, безопасными и экологичными. Они разные – большие и маленькие, умные и не очень, сухопутные, подводные и космические. Пусть расцветают все цветы – будущее за сетью разных по размерам и используемым технологиям ЦОДов, наиболее соответствующих стоящим перед ними задачами.

Биометрия в Интернете и современные цифровые платформы

Н. С. Коннова, П. В. Мизинов

Биометрия настолько незаметно и глубоко вошла в нашу повседневную жизнь, что стала совершенно неотъемлемой её частью. Разработчики внедряют данную технологию практически везде: от мобильного телефона до автомобильного иммобилайзера, - ведь биометрия подкупила всех простотой своего использования. В век цифровой экономики биометрия стала ключом для входа в новый цифровой мир, где есть доступ и к банковским счетам, и к данным о состоянии здоровья конкретной личности, и к другой персональной информации. Но насколько можно доверять биометрическим методам? В данной статье мы рассматриваем вопросы безопасности биометрии в контексте её использования для идентификации пользователя в цифровых платформах и сервисах.

Сегодня никого не удивишь возможностью оплатить покупки в магазине одним взглядом или открыть турникет в метро, посмотрев в объектив камеры, разблокировать ноутбук, приложив к датчику палец, или авторизоваться в удалённой системе, проговорив несколько контрольных фраз цифровому помощнику. Всё это — удачный симбиоз биометрии и цифровых сервисов, стремительно проникших в нашу повседневную жизнь в последние десять лет и ставших её неотъемлемой частью.

Вернитесь мысленно на десять лет назад и вспомните процесс оплаты выставленного финансового счёта, да и вообще процесс получения финансовых услуг в любой кредитной организации. Приходилось получать талон, вставать в очередь, дожидаться вызова в соответствующее окно, долго объяснять работнику банка, какая операция вам требуется, чтобы узнать, что «вам в соседнее окно», стоять в очереди повторно, предъявлять, как минимум, паспорт, а то и СНИЛС, оплачивать наличными, получать подтверждающие оплату документы и, с чувством выполненного долга, через час-полтора покинуть помещение банка. Знакомая ситуация? Лично мне — да. Вспоминаю, как приходилось занимать очередь в банке в субботу утром, чтобы хотя бы за час совершить ежемесячный платёж по ипотеке, так как в будний день этот процесс занимал минимум два часа.

«Лучом света» в то время стала возможность получать банковские услуги онлайн. Да, были и значительные проблемы в работе банковских сайтов, и ошибки в проведении операций, и неудобство авторизации при помощи одноразовых паролей (которые можно было получить только в банкомате или терминале), но «всепоглощающим» плюсом, перекрывающим все недостатки первых платформ, являлось отсутствие самой необходимости личного посещения кредитной организации.

С появления первых цифровых платформ, предоставляющих финансовые услуги, берёт своё начало масштабная цифровая трансформация деятельности и бизнес-процессов государственных и частных организаций в России. Была запущена цепочка принципиальных изменений подходов к работе, преобразивших сам механизм функционирования всех участников процесса. Начался переход на новую ступень развития в предоставлении услуг и управлении организацией, получивший название «цифровизация».

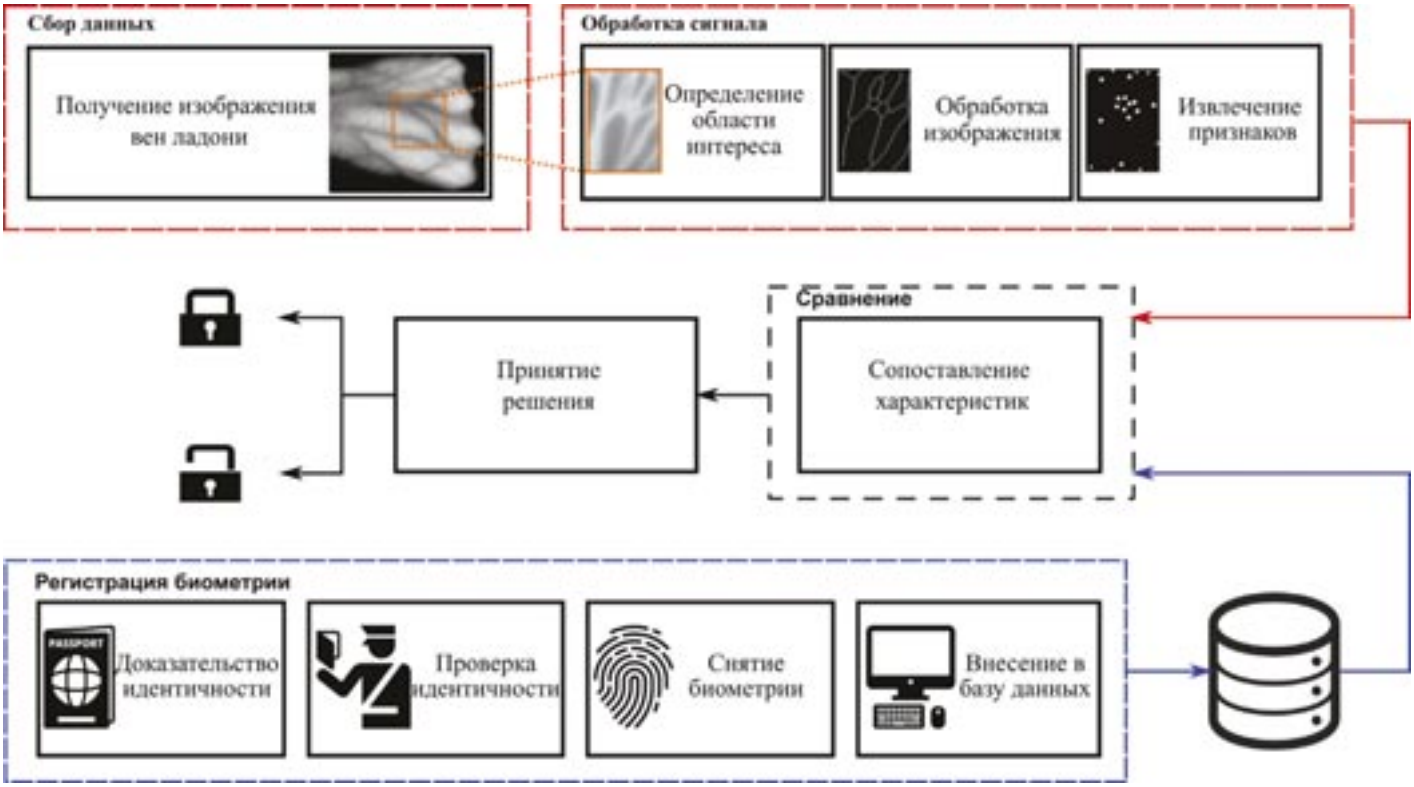
Если сильно упрощать, цифровизация — это переход основной деятельности компании в цифровую среду. Предоставляемые услуги компании трансформируются в цифровые сервисы. Например, компания «Рога и копыта» специализировалась на выдаче условных справок и заключений. После цифровизации деятельности эти два документа стало возможным получить в электронном (цифровом) виде, т.е. теперь компания предоставляет два цифровых сервиса: первый — получение справки, второй — заключения, а сайт, через который можно заказать данные услуги (и справку, и заключение), будем условно называть цифровой платформой. Теперь электронные услуги компании «Рога и копыта» можно получить из любого места, в любое время через цифровую платформу компании. Данный подход позволяет потенциальному потребителю получать услуги по принципу «в один клик»: практически мгновенно и без личного посещения организации.

Сегодня в России через различные цифровые платформы в сети Интернет предоставляется несколько сотен разновидностей цифровых услуг, и их спектр постоянно расширяется. Крупнейшей цифровой платформой для получения государственных услуг в РФ является Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)» (Госуслуги), насчитывавшая на 01 апреля 2022 года 96,4 миллиона пользователей[1] и удовлетворяющая до 40 миллионов обращений за государственными электронными услугами ежемесячно.

Чтобы цифровизация стала возможна, государству пришлось адаптировать, видоизменить, а также принять большое количество законов и подзаконных актов. Необходимо было

[1] https://ria.ru/20220405/gosuslugi-1781833741.html

Рисунок 1. Обобщённое схематическое изображение процесса аутентификации по рисунку вен ладони.



не только решить данный вопрос юридически (например, уравнение в правах «бумажных» и электронных копий, придание правового статуса электронно-цифровой подписи и т.д.), но и заняться очень сложной технической задачей: от организации дата-центров для хранения данных до максимального покрытия регионов России сетями с доступом в Интернет. Причём последнее играет, пожалуй, важнейшую роль. Ведь основной смысл цифровизации — доступ к услугам и сервисам для любого гражданина или бизнеса в любом месте и в любое время. Для этого необходимо соблюдение трёх условий: наличие доступа к Интернету, наличие зарегистрированной учётной записи на цифровой платформе, а также наличие оборудования для взаимодействия с цифровой платформой (стационарный ПК, мобильный телефон или планшет).

В контексте информационной безопасности вопрос защищённости учётной записи пользователя цифровых услуг является наиболее приоритетным. Потеря управляемости идентификационными и аутентификационными данными (логином и паролем) верифицированной учётной записи, например, тех же Госуслуг, влечёт за собой риски раскрытия конфиденциальной информации о гражданине: с указанными учётными данными возможно авторизоваться и на платформе mos.ru (там получить сведения о состоянии здоровья клиента через систему ЕМИАС[2]), а также в личном кабинете Федеральной налоговой службы. Такие же неприемлемые риски грозят и физическому лицу – индивидуальному предпринимателю.

Учитывая, что подавляющее число платформ, предоставляющих цифровые услуги в Интернете, авторизуют пользователя по стандартной связке «логин-пароль», а до 38% среднестатистических пользователей используют одинаковый пароль для всех сайтов и приложений[3], угроза компрометации идентификационных данных и раскрытия личной конфиденциальной информации более чем актуальна. Кроме этого, почти треть пользователей (31%[4]) хранит свои пароли в виде записи в блокноте или на листке бумаги, что значительно упрощает возможность их получения злоумышленником. При таких обстоятельствах использовать аутентификацию на цифровых платформах по связке «логин-пароль» – это добровольно подвергать себя риску утраты конфиденциальной информации.

В сложившейся ситуации необходимо использовать такие методы аутентификации, риск «взлома» которых маловероятен или экономически не целесообразен для злоумышленника. К ним, прежде всего, принято относить биометрические технологии, позволяющие идентифицировать пользователя системы по его физиологическим (отпечаток пальца, особенности радужной оболочки глаза, венозный рисунок или форма лица), поведенческим (звук голоса, походка) характеристикам или их комбинации (мультимодальные[5] биометрические технологии).

Идентификация личности по его биометрическим характеристикам (вне контекста автоматизированных систем) использовалась социумом веками. Мы узнаём людей по звуку их голоса, по чертам лица, по поведенческим характеристикам, бессознательно понимая, что определённые параметры присущи только единственному человеку, т.е. уникальны (точнее, обладают высокой степенью репрезентативности). Именно

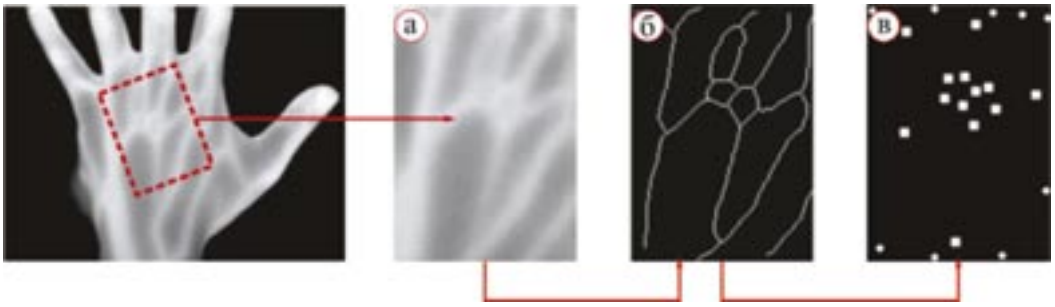
[2] Единая медицинская информационно-аналитическая система

[3] https://safe.cnews.ru/news/line/2022-05-05_issledovanie_odnoklassnikov

[4] https://safe.cnews.ru/news/line/2022-05-05_issledovanie_odnoklassnikov

[5] Модальностью называют разновидность биометрических характеристик

Рисунок 2. Этапы получения биометрических параметров по рисунку вен ладони:
а) выделение области интереса,
б) бинаризация и скелетизация изображения,
в) извлечение биометрических параметров.



знания об уникальности антропометрических характеристик помогли создать первые неавтоматизированные системы идентификации личности.

Методы применения различных биометрических характеристик (или модальностей) для однозначного подтверждения личности применяются по меньшей мере более двух тысяч лет: считается, что ещё древние ассирийцы и вавилоняне имели представление об уникальности папиллярного узора и активно использовали это знание. Применяли биометрию и в Древнем Китае: отпечаток пальца использовался в качестве подписи на торговых договорах и соглашениях наряду с традиционными печатями[6].

На сегодняшний день идентифицировать человека возможно на основании более 20 модальностей (начиная от венозного рисунка вены пальца и заканчивая схемой ДНК), а также поведенческих характеристик.

Применяемые модальности условно делятся на два класса: динамические и статические. К первым относят модальности, заметно претерпевающие изменения с течением времени: например, звучание голоса, рукописный почерк, походка. Ко вторым — мало меняющиеся со временем модальности, такие как рисунок венозной сети (глазного яблока, дорсальной/вентральной стороны ладони, пальца или запястья), рисунок радужной оболочки глаза, геометрия частей тела и прочее, либо не изменяющиеся совсем: например, ДНК.

Процесс аутентификации личности, как правило, состоит из четырёх этапов: получение цифрового изображения, содержащего биометрический образ, его предварительная обработка, извлечение биометрических параметров (признаков) и непосредственно аутентификация по полученным признакам (сопоставление) (см. рисунок 1).

После получения биометрического образа изображение подвергается предварительной обработке путём позиционирования, улучшения посредством наложения фильтров, выделения области интереса и его сегментации. Затем происходит процесс извлечения биометрических параметров, количество и качество которых зависят от производителя оборудования, и, наконец, данные параметры сохраняются в базе данных в качестве биометрического контрольного шаблона. В конечном итоге происходит процесс сравнения полученных биометрических признаков с заложенным в системе эталоном и принятие системой решения о подтверждении личности пользователя. В качестве иллюстрации схематично продемонстрируем извлечение биометрических параметров из узора сосудистого русла кисти руки (см. рисунок 2).

Биометрические методы идентификации обладают рядом неоспоримых преимуществ. Любая используемая модальность является «универсальным идентификатором», которую в отличие от классических smart-cart, ibutton или token практически невозможно потерять и изменить (исключения составляют видоизменения вследствие возраста, болезней, травм или хирургического вмешательства).

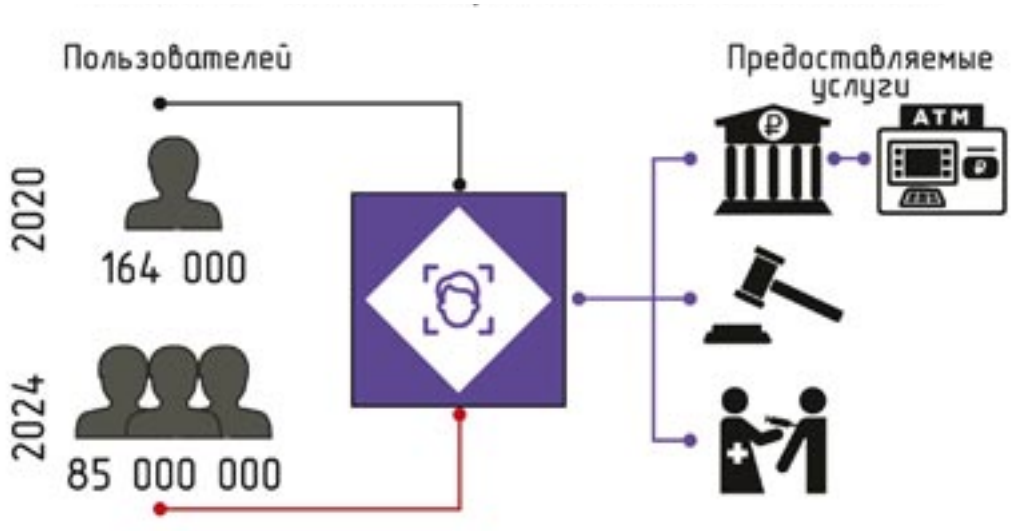
Большинство модальностей демонстрируют высокую защищённость идентификационных данных. Например, поскольку вены защищены кожным покровом, венозный рисунок возможно рассмотреть только в ближнем инфракрасном диапазоне, в обычных условиях негласно получить биометрические характеристики (особенно вентральной поверхности ладони) представляется весьма затруднительным.

Биометрия по геометрии лица, руки либо по венозному рисунку дает возможность считывания биометрических параметров бесконтактным методом, что в современных

Рисунок 3. Упрощённая схема работы биометрической системы.

[6] https://laowai.ru/malenkaya-krasnaya-pechat-bolshoj-kitajskij-tysyacheletnij-lajfxak/

Рисунок 4. Единая биометрическая система: перспектива развития.



условиях возможных пандемий обеспечивает высокий уровень гигиены и позволяет избежать распространения инфекции.

Однако, как и у любого другого вида идентификации, у биометрии имеются и отрицательные стороны. Основной недостаток — уязвимость биометрических систем на основе распознавания лица, радужной оболочки глаза, отпечатка пальца и геометрии руки к атакам на биометрическое предъявление, подразумевающим предъявление биометрическому датчику артефакта — искусственно созданной копии модальности. То есть злоумышленнику необходимо изготовить такую копию биометрических параметров пользователя, чтобы, пройдя все этапы обработки, биотермическая система опознала самозванца в качестве зарегистрированного пользователя. Основные этапы работы биометрической системы и схематическое изображение атаки на биометрическое предъявление представлено на рисунке 3.

Из всех перечисленных модальностей наибольший интерес представляют идентификация по звуку голоса, геометрии лица и венозному рисунку кисти руки. Дело в том, что данные модальности задействованы[7] (или планируются к внедрению) в качестве идентификационных данных в Единой биометрической системе (ЕБС) — государственном информационном ресурсе (цифровой платформе), направленном на сбор биометрической информации и её использование для идентификации (аутентификации) пользователей финансовых услуг (см. рисунок 4).

В настоящее время ЕБС используется в качестве средства аутентификации для финансовых цифровых сервисов и банковских услуг. А возможным это стало благодаря принятому в 2018 году закону (482-ФЗ), по которому биометрические образцы стали юридически значимыми для идентификации личности (приравнены к паспорту гражданина РФ). На этом основании уже сегодня отечественные банки представляют возможность открыть счёт или оставить заявку на кредит, идентифицируя пользователя по его биометрическим характеристикам. С января 2021 года через ЕБС возможно получение и страховых услуг[8]. А с декабря текущего года разработчики обещают интеграцию ЕБС и портала госуслуг[9]. Таким образом, ЕБС становится универсальным ключом к подавляющему большинству государственных, финансовых и банковских цифровых услуг. И устойчивость используемых в системе модальностей к атаке на биометрическое предъявление является критическим условием при их использовании в качестве идентификатора на цифровых платформах.

Сегодня ЕБС — мультимодальная биометрическая система, действующая на основе модальностей геометрии лица и звука голоса. Данная комбинация модальностей позиционируется разработчиками надёжной, однако данные в научной литературе показывают, что обе используемые модальности (по геометрии лица [1–14] и по звуку голоса [15–19]) уязвимы к различным видам подделок или спуфинг-атак.

Мы не будем приводить сотни рецептов по изготовлению дорогостоящих 3D-масок для обмана биометрического сканера или попыток имитации голоса, повсеместное распространение нейронных сетей делают процесс подделки двух перечисленных модальностей практически беззатратным для атакующего. Эти инструменты атаки получили название deepfake («deep» — глубокий, от метода изготовления — глубокого обучения нейросети, «fake» — подделка).

В случае с deepfake модальности геометрии лица нейронной сети «скармливают» сотни доступных в социальных сетях эталонных фотографий и видео, содержащих изображения легитимного пользователя, чтобы научить сеть генерировать анимированную «маску» лица. Далее эта «маска» «накладывается» на лицо атакующего во время процесса идентификации системой в режиме реального времени.

Для атаки не требуется экзотическое дорогостоящее оборудование или программное обеспечение: программные продукты с открытым исходным кодом способны генерировать высококачественную «маску», обучившись на датасете из двухсот фотографий.

Последние версии такого программного обеспечения позволяют проходить сложные тесты коммерческих биометрических систем непосредственно в реальном времени, задержка в работе с «маской» составляет 1-5 миллисекунд.

[7] https://bio.rt.ru/about/

[8] https://www.kommersant.ru/doc/4721686

[9] https://www.cnews.ru/news/top/2022-01-18_ne_sdavshim_biometriyu_rossiyanam

Компанией Sensity в мае 2022 проводилось тестирование на проникновение десяти биометрических систем, используемых для доступа к личному кабинету в десяти европейских банках. Согласно их отчёту[10], девять из десяти систем уязвимы для атаки на биометрическое предъявление при помощи deepfake, сгенерированных открытым программным обеспечением.

Аналогичная ситуация и с модальностью звука голоса. Если ранее злоумышленнику приходилось записывать образцы голоса жертвы длительностью по несколько часов, чтобы потом «нарезать» из них контрольные фразы системы, то при помощи нейросети возможно создать deepfake, используя аудиофайл с записью голоса потенциальной жертвы длительностью всего 3 (!) секунды[11].

Данное программное обеспечение позволяет воспроизвести набранный на клавиатуре текст голосом легитимного пользователя. Да, открытый инструмент слишком «медленный» для использования в атаке в режиме реального времени, но злоумышленник может заранее создать вероятные фразы, а затем воспроизводить их по мере необходимости.

Идеальным сценарием для злоумышленника было бы говорить, а не печатать и преобразовывать свою речь в клонированный голос. И, похоже, что и в этой технологии наметился прогресс. В настоящее время уже представлен прототип вокодера (кодировщика голоса)[12], который, как утверждается, способен выполнять преобразование аудиосигнала с задержкой всего в 10 миллисекунд.

Иначе говоря, deepfake-атака на модальность голоса в реальном времени может стать достижимой в ближайшем будущем — если уже не стала.

Таким образом, обе используемые в ЕБС модальности потенциально уязвимы перед deepfake-атаками.

В конце 2021 года разработчик заявил о намерении дополнить ЕБС рисунком вен ладони в качестве дополнительной биометрической модальности[13]. Связано это с предоставлением равных возможностей для клиентов, испытывающих сложности при использовании устной речи, в том числе с проблемами слуха и речи.

Выбор разработчиками ЕБС данной модальности обуславливается несколькими факторами:

- прежде всего, универсальностью, поскольку венозный рисунок кисти руки присущ большинству индивидуумов;
- высокая степень репрезентативности данной модальности позволяет использовать венозный рисунок в качестве уникального идентификатора;
- данная модальность постоянна, так как принято считать, что рисунок вен с течением времени меняется незначительно;

кроме того, данную модальность можно считать бесконтактным методом, что обеспечит высокий уровень гигиены в период возможных пандемий.

Одним из основных достоинств биометрии по сосудистому руслу руки заслуженно считают недоступность идентификационных данных пользователя. Действительно, венозная сеть защищена кожным покровом, плохо различима при естественном освещении, качественно визуализируется только в условиях ближнего инфракрасного света, что затрудняет негласное получение биометрических характеристик злоумышленником.

Однако последние работы, посвящённые визуализации сосудов из изображений, полученных в видимом спектре [20–22], делают дискуссионным вопрос о невозможности получения сосудистого рисунка вне ИК-освещения.

Также из открытых источников и научной литературы известно несколько примеров [23–26] успешного проведения атак на биометрическое предъявление на основе модальности рассматриваемого типа, где в качестве инструмента атаки на биометрическое предъявление выступало изображение пальца [24] и кисти руки [23, 25, 26], полученное в инфракрасном диапазоне.

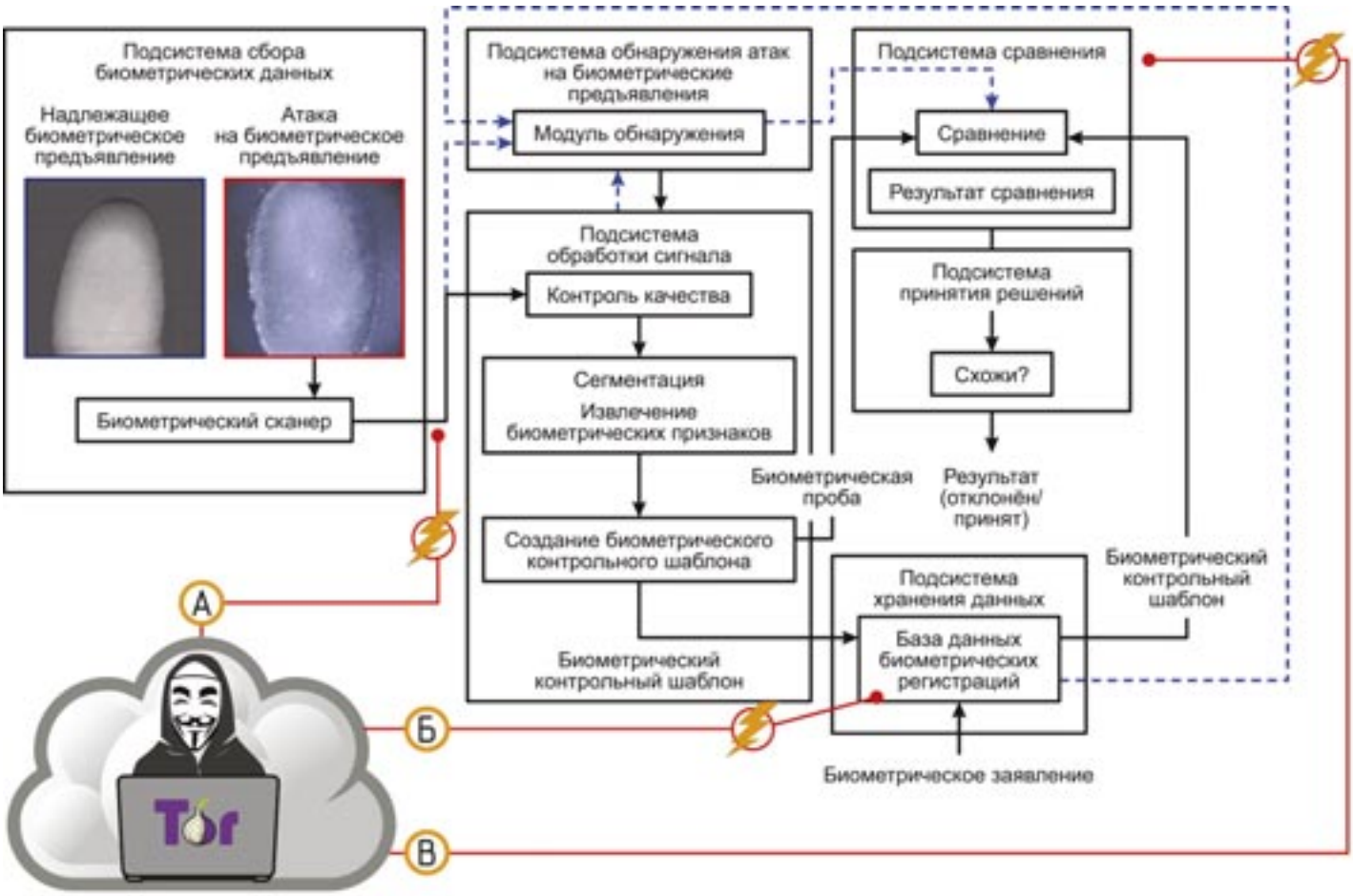
Кроме этого, авторами [27] проведено исследование возможности получения венозного изображения кисти руки вне ИК-диапазона доступным оборудованием – камерой мобильного телефона. Полученные данные позволяют сделать предварительный вывод о возможности получения венозного рисунка без применения специальных технических средств, достаточного (после предварительной обработки) для использования в качестве инструмента атаки на биометрические системы на основе модальности вены руки.

Таким образом, модальность венозного рисунка руки также потенциально уязвима перед атакой на биометрическое предъявление.

Утверждение, что некоторые виды биометрических образов (рисунок вен, кардиограмма, ДНК) невозможно подделать, вовсе не означает, что невозможно скомпрометировать систему в целом. Производителями оборудования при демонстрации преимуществ их продукта делается упор именно на невозможность предъявления артефакта в качестве идентификатора, т.е. надёжность системы оценивается по этапу сбора данных. Примеры успешных атак, описанных выше, также проведены на этом этапе. Однако работа любой биометрической системы состоит из минимального набора следующих шагов: сбор данных, обработка сигнала, сравнение параметров с образом из базы, принятие решения о допуске и этап верификации в приложении. На каждом из этих этапов возможно провести атаку, позволяющую скомпрометировать систему без изготовления муляжей рук, фальшивых отпечатков, фотографии сетчатки глаза. Например, дополнить базу данных системы «нужным» биометрическим образом либо изменить логику работы

[10] https://sensity.ai/reports/
[11] https://soundcloud.com/protocol-443256612/demo-of-deepfake-phone-scam-fictitious
[12] https://jmvalin.ca/demo/lpcnet_codec/
[13] https://iz.ru/1231860/2021-10-06/v-edinuiu-biometricheskuiu-sistemu-mogut-dobavit-risunok-ven-ladoni

Рисунок 5. Схема типовой биометрической системы (обозначены возможные векторы для атаки).



сопутствующего программного обеспечения, заставляя принимать «нужные» решения при любом предъявленном идентификаторе. Исследователи в области информационной безопасности насчитывают до 13 возможных векторов атаки на биометрические системы (см. рисунок 5).

Подводя итог, отметим, что любые виды биометрии имеют свои достоинства и недостатки. Безусловно, решения на основе распознавания рисунка вен, звука голоса и геометрии лица, используемые в ЕБС, являются наиболее современными и надёжными. Однако анализ упомянутых в работе подходов показал уязвимость используемых методов к атакам на биометрическое предъявление. Таким образом, применение биометрии в качестве метода аутентификации на цифровых платформах должно быть основано на тщательнейшем анализе и оценке рисков. Как показал анализ литературы, интенсивное развитие нейросетей и алгоритмов deepfake в ближайшем будущем позволит создавать артефакты, практически неотличимые от биометрических показателей легального пользователя.

Также пользователь не застрахован от утери биометрических идентификационных данных вследствие компрометации базы данных «центра биометрической авторизации», в роли которого выступает ЕБС. Ярчайший пример — «взлом»[14] в 2018 году AADHAAR — индийской идентификационной системы, содержащей данные более чем 1,3 миллиарда человек и являющейся крупнейшей базой биометрических данных в мире.

Злоумышленники получили полный доступ к уникальным 12-значным номерам граждан Индии, привязанным к биометрическим (фотографии лица, отпечатки 10 пальцев рук и два скана радужной оболочки глаза) и персональным (ФИО, адрес регистрации, дата рождения, пол, номер телефона и адрес электронной почты) данным владельца.

После успешной атаки хакеры предоставляли заинтересованным лицам полный доступ к скомпрометированному ресурсу всего за 500 рупий (~500 руб.), кроме этого, за 300 рупий (~300 руб.) предлагалось программное обеспечение, позволяющее изготовить оригинальный Aadhaar card (аналог паспорта).

Как и ЕБС, AADHAAR была создана в качестве «центра биометрической авторизации» при реализации различных государственных программ на цифровых платформах.

Поэтому для повышения защищённости систем авторы рекомендуют использовать биометрию только в качестве идентификатора, применяя в дополнение факторы знания (пароли) и владения (токены, смарт-карты и т.д.).

[14] https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361

Литература.

1. R. Shao, X. Lan, P.C. Yuen, Joint discriminative learning of deep dynamic textures for 3d mask face anti-spoofing. IEEE Transactions on Information Forensics and Security 14(4), 923–938 (2019). https://doi.org/10.1109/tifs.2018.2868230
2. A. George, Z. Mostaani, D. Geissenbuhler, O. Nikisins, A. Anjos, S. Marcel, Biometric face presentation attack detection with multi-channel convolutional neural network. IEEE Transactions on Information Forensics and Security 15, 42–55 (2020). https://doi.org/10.1109/tifs.2019.2916652
3. H. Chen, G. Hu, Z. Lei, Y. Chen, N.M. Robertson, S.Z. Li, Attention-based two-stream convolutional networks for face spoofing detection. IEEE Transactions on Information Forensics and Security 15, 578–593 (2020). https://doi.org/10.1109/tifs.2019.2922241
4. J.C. Neves, R. Tolosana, R. Vera-Rodriguez, V. Lopes, H. Proenca, J. Fierrez, GAN-printR: Improved fakes and evaluation of the state of the art in face manipulation detec-tion. IEEE Journal of Selected Topics in Signal Processing 14(5), 1038–1048 (2020). https://doi.org/10.1109/jstsp.2020.3007250
5. S. Zhang, A. Liu, J. Wan, Y. Liang, G. Guo, S. Escalera, H.J. Escalante, S.Z. Li, CASIA-SURF: A large-scale multi-modal benchmark for face anti-spoofing. IEEE Transactions on Biometrics, Behavior, and Identity Science 2(2), 182–193 (2020). https://doi.org/10.1109/tbiom.2020.2973001
6. W. Sun, Y. Song, C. Chen, J. Huang, A.C. Kot, Face spoofing detection based on local ternary label supervision in fully convolutional networks. IEEE Transactions on Information Forensics and Security 15, 3181–3196 (2020). https://doi.org/10.1109/tifs.2020.2985530
7. Z. Yu, J. Wan, Y. Qin, X. Li, S.Z. Li, G. Zhao, NAS-FAS: Static-dynamic central difference network search for face anti-spoofing. IEEE Transactions on Pattern Analysis and Machine Intelligence 43(9), 3005–3023 (2021). https://doi.org/10.1109/tpami.2020.3036338
8. G. Wang, H. Han, S. Shan, X. Chen, Unsupervised adversarial domain adaptation for cross-domain face presentation attack detection. IEEE Transactions on Information Forensics and Security 16, 56–69 (2021). https://doi.org/10.1109/tifs.2020.3002390
9. A. George, S. Marcel, Learning one class representations for face presentation attack detection using multi-channel convolutional neural networks. IEEE Transactions on Information Forensics and Security 16, 361–375 (2021). https://doi.org/10.1109/tifs.2020.3013214
10. R. Cai, H. Li, S. Wang, C. Chen, A.C. Kot, DRL-FAS: A novel framework based on deep reinforcement learning for face anti-spoofing. IEEE Transactions on Information Forensics and Security 16, 937–951 (2021). https://doi.org/10.1109/tifs.2020.3026553
11. D. Deb, A.K. Jain, Look locally infer globally: A generalizable face anti-spoofing approach. IEEE Transactions on Information Forensics and Security 16, 1143–1157 (2021). https://doi.org/10.1109/tifs.2020.3029879
12. A. Liu, Z. Tan, J. Wan, Y. Liang, Z. Lei, G. Guo, S.Z. Li, Face anti-spoofing via adversarial cross-modality translation. IEEE Transactions on Information Forensics and Security 16, 2759–2772 (2021). https://doi.org/10.1109/tifs.2021.3065495
13. R. Cai, Z. Li, R. Wan, H. Li, Y. Hu, A.C. Kot, Learning meta pattern for face anti-spoofing. IEEE Transactions on Information Forensics and Security 17, 1201–1213 (2022). https://doi.org/10.1109/tifs.2022.3158551
14. A. Liu, C. Zhao, Z. Yu, J. Wan, A. Su, X. Liu, Z. Tan, S. Escalera, J. Xing, Y. Liang, G. Guo, Z. Lei, S.Z. Li, D. Zhang, Contrastive context-aware learning for 3d high-fidelity mask face presentation attack detection. IEEE Transactions on Information Forensics and Security 17, 2497–2507 (2022). https://doi.org/10.1109/tifs.2022.3188149
15. S. Saleem, A. Dilawari, M.U.G. Khan, M. Husnain, in 2019 International Conference on Robotics and Automation in Industry (ICRAI) (IEEE, 2019), pp. 1–6. https://doi.org/10.1109/icrai47710.2019.8967385
16. H. Malik, in 2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR) (IEEE, 2019), pp. 512–517. https://doi.org/10.1109/mipr.2019.00104
17. K. Phapatanaburi, L. Wang, S. Nakagawa, M. Iwahashi, Replay attack detection using linear prediction analysis-based relative phase features. IEEE Access 7, 183,614–183,625 (2019). https://doi.org/10.1109/access.2019.2960369
18. I. Himawan, S. Madikeri, P. Motlicek, M. Cernak, S. Sridharan, C. Fookes, in Handbook of Biometric Anti-Spoofing (Springer International Publishing, 2019), pp. 391–415. https://doi.org/10.1007/978-3-319-92627-8_17
19. A. Chintha, B. Thai, S.J. Sohrawardi, K. Bhatt, A. Hickerson, M. Wright, R. Ptucha, Recurrent convolutional structures for audio spoof and video deepfake detection. IEEE Journal of Selected Topics in Signal Processing 14(5), 1024–1037 (2020). https://doi.org/10.1109/jstsp.2020.2999185
20. C. Sungchul, O. Beom-Seok, T. Kar-Ann,L. Zhiping, Extraction and cross-matching of palm-vein and palmprint from the RGB and the NIR spectrums for identity verification. IEEE Access 8, 4005–4021 (2020). https://doi.org/10.1109/access.2019.2963078
21. C. Tang, Y. Yuan, S. Xia, G. Ma, B. Wang, Visualizing veins from color skin images using convolutional neural networks. Journal of Innovative Optical Health Sciences 13(04), 2050,020 (2020). https://doi.org/10.1142/ s1793545820500200
22. C. Sungchul, O. Beom-Seok, K. Donghyun, T. Kar-Ann, Palm-vein verification using images from the visible spectrum. IEEE Access 9, 86,914–86,927 (2021). https://doi.org/10.1109/access.2021.3089484
23. FIDIS (Future of Identity in the Information Age). D6.1 Forensic Implications of Identity Management Systems. — 2006. — Режим доступа: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf (дата обращения: 30.06.2021).
24. Tome Pedro, Vanoni Matthias, Marcel Sébastien. On the vulnerability of finger vein recognition to spoofing // 2014 International Conference of the Biometrics Special Interest Group (BIOSIG). — 2014. — P. 1–10.
25. Tome Pedro, Marcel Sebastien. On the vulnerability of palm vein recognition to spoofing attacks // Proceedings of 2015 International Conference on Biometrics, ICB 2015. — IEEE, 2015. DOI: 10.1109/icb.2015.7139056.
26. Patil Ishan, Bhilare Shruti, Kanhangad Vivek. Assessing vulnerability of dorsal hand-vein verification system to spoofing attacks using smartphone camera // 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA). — IEEE, 2016. — P. 1–6. DOI: 10.1109/isba.2016.7477232.
27. Коннова Н. С., Мизинов П. В. Анализ надежности методов аутентификации на основе васкулярного сканирования // Физические основы приборостроения. 2021. Т. 10. С. 52–63.

Авторы статьи – сотрудники Московского государственного технического университета им. Н. Э. Баумана: к.т.н, доцент кафедры «Информационная безопасности» Н. С. Коннова (nkonnova@bmstu.ru), аспирант кафедры «Информационная безопасности» П. В. Мизинов (paul.mizinov@gmail.com).

Европейская модель обеспечения безопасности Интернета вещей

Мадина Касенова

Физические объекты («вещи»), подключенные к Интернету и иным коммуникационным сетям, иначе – Интернет вещей (Internet of Things, IoT), получают широкомасштабное применение, а современная парадигма IoT приобретает первостепенную значимость в силу ее многоплановости, которая охватывает бытовую технику, промышленность, секторы здравоохранения, энергетики, транспортные системы и т.д. Интернет вещей как некое слияние цифрового и физического мира в последнее десятилетие стал одной из фундаментальных и определяющих тенденций цифровой трансформации экономики, бизнеса, социальных отношений. По показателям некоторых статистических данных количество инсталлированных устройств IoT стремительно увеличивается, и к 2025 году прогнозируется их рост до 75,44 миллиарда, тогда как в 2015 году их насчитывалось 15,41 миллиарда[1].

Посредством датчиков и электронных преобразователей технология IoT агрегирует, обрабатывает, хранит на устройствах, операционных системах, платформах облачных сервисов, а также распределяет и передает огромные объемы данных. Вместе с тем становится все более очевидным, что устройства Интернета вещей не всегда устойчивы к уязвимостям, подвержены взлому и другим видам атак, что создает существенные проблемы кибербезопасности, включая обеспечение конфиденциальности данных. Принимая во внимание взаимосвязанность и взаимообусловленность пространства Интернета вещей, любой киберинцидент, например, с подключенным устройством, способен оказать негативное влияние не только на само устройство, но также на целую зависимую систему в трансграничном масштабе.

Сказанное объясняет сфокусированность современных государств на принятии разнообразных законодательных и нормативных актов, направленных на решение сложных проблем стандартизации безопасности Интернета вещей, что обеспечит защиту всех, кто использует устройства IoT, а также определит специальные требования кибербезопасности к изготовителям, поставщикам и пользователям цифровой продукции.

Стандартизация безопасности является существенным инструментом, обеспечивающим универсализацию спецификаций, сертификатов и протоколов для целей совместимости устройств и приложений технологии Интернета вещей. В этой связи следует отметить, что нормативный регуляторный формат Интернета вещей зиждется на комплексе международных (универсальных и региональных) технических стандартов, куда прежде всего входят стандарты ISO/IEC, стандарты Европейского института телекоммуникационных стандартов (ETSI)[2], используемые в Европе, а также принимаемые де-факто Европейской комиссией (далее – Еврокомиссия) в качестве технической основы для директив и регламентов Европейского Союза (далее – Евросоюз или ЕС). Нелишне обратить внимание, в частности, на тот факт, что на международном стандарте ISO/IEC 30141:2018 «Информационные технологии – Интернет вещей (IoT) – Эталонная архитектура»[3] основывается действующий национальный стандарт Российской Федерации, утвержденный приказом Росстандарта (23.07.2020 № 29-пнст) и введенный в действие на период с 01.01.2021 по 01.01.2024[4]. Стандарты ETSI стали основой системы маркировки для устройств Интернета вещей (Labeling Scheme for IoT Devices), которую Финляндия ввела в действие с 2019 года для смарт-телевизоров, смартфонов, игрушек. Стандарты ETSI и ISO/IEC явились базой потребительской маркировки безопасности (Consumer Security Label) в Германии (2021) для широкополосных маршрутизаторов, смарт-телевизоров, камер, динамиков, игрушек, уборочных и садовых роботов.

Несмотря на значимость принимаемых на национальном уровне законодательных и нормативных актов, направленных на обеспечение безопасности Интернета вещей, они фрагментарны и лишь частично решают существующие проблемы кибербезопасности цифровой продукции, а это не только создает риски нормативно-правовой неопределенности как для продавцов, так и для пользователей такой продукции, но также обременяет субъекты экономической деятельности необходимостью соблюдать многочисленные требования и обязательства. Немаловажным обстоятельством, подлежащим учету, выступает так называемое трансграничное измерение кибербезопасности Интернета вещей, поскольку цифровая продукция, произве-

1 10 IoT Trends for 2022/2023: Latest Predictions According To Expert. URL: https://financesonline.com/iot-trends/

2 European Telecommunications Standards Institute. URL: https://www.gartner.com/en/information-technology/glossary/etsi-european-telecommunications-standards-institute.

3 ISO/IEC 30141:2018 «Information technology - Internet of Things (IoT) - Reference architecture», MOD). URL:https://www.iso.org/obp/ui/#iso:std:iso-iec:30141:ed-1:v1:en

4 «Предварительный национальный стандарт Российской Федерации. Информационные технологии. Интернет вещей промышленный. Типовая архитектура» (утв. и введен в действие Приказом Росстандарта от 23.07.2020 N 29-пнст) // СПС КонсультантПлюс

денная в одной стране, зачастую используется лицами (физическими и юридическими) в других странах, соответственно, возникающие киберинциденты могут одновременно затрагивать не только физические и юридические лица, но и целые секторальные сферы нескольких государств.

Палитра системно развивающейся нормативно-правовой базы Евросоюза, обеспечивающая защиту киберпространства единого внутреннего рынка ЕС и транспарантную регламентацию функционирования его цифрового сектора, пополнилась новой законодательной инициативой. Речь идет о том, что 15 сентября 2022 года Еврокомиссия представила на рассмотрение Европейского парламента и Совета Предложение о принятии Регламента 2022/0272 (COD) относительно горизонтальных требований по кибербезопасности для продукции с цифровыми элементами, а также внесении изменений в Регламент (ЕС) 2019/1020[5]. Контекстный аспект данного регламента, кратко именуемого «Акт о киберустойчивости» (Cyber Resilience Act, CRA), сопряжен с тем, что кибербезопасность большей части аппаратного и программного обеспечения в Евросоюзе не регулируется общими правовыми актами ЕС, несмотря на то, что существующее законодательство ЕС регламентирует отдельные аспекты применения цифровой продукции. Предлагая к принятию названный регламент, Еврокомиссия исходила из следующих принципиальных моментов.

Во-первых, действующие законодательные акты Евросоюза не затрагивают ряд вопросов кибербезопасности невстроенного программного обеспечения, даже если кибератаки все чаще нацелены на уязвимости в этих изделиях, а это приводит к значительным социальным и экономическим издержкам. Во-вторых, глобальный характер рынков цифровой продукции и трансграничный масштаб ее применения порождают в государствах-членах ЕС риски, независимо от того, в каком государстве эта продукция используется. В-третьих, попытки регулирования рынка цифровой продукции на уровне государств-членов ЕС приводят к возникновению потенциально разных систем национальных нормативных правил, что способствует фрагментации регулирования и не содействует созданию открытого и конкурентоспособного единого рынка цифровой продукции. В-четвертых, повысить уровень доверия пользователей и привлекательность цифровой продукции в Евросоюзе можно лишь совместными действиями на уровне ЕС, усилив его роль в противодействии угрозам кибербезопасности, что принесет пользу единому внутреннему рынку ЕС, обеспечит правовую определенность, а также создаст равные условия для продавцов и потребителей цифровой продукции.

Надлежит отметить, что Акт киберустойчивости 2022 предложен Еврокомиссией в формате принятия не директивы, а регламента, т.е. общеправового законодательного акта прямого действия, подлежащего обязательному непосредственному применению в полном объеме как на уровне ЕС, так и в правопорядках всех государств-членов ЕС. Выбор такого типа регуляторного инструментария – регламента – можно объяснить тем, что законодательная форма директивы оставляет значительную меру усмотрения на национальном уровне, что потенциально может привести к отсутствию единообразного применения существенно значимых требований кибербезопасности, создаст правовую неопределенность и дальнейшую фрагментацию регулирования или породит дискриминационные ситуации в трансграничном масштабе, даже с учетом того, что охватываемая цифровая продукция может иметь различное предназначение или использование, а изготовители могут размещать на рынке разнообразные категории цифровой продукции.

Немаловажно также, что в силу прямого указания, имеющегося в Акте киберустойчивости 2022, сфера его действия распространяется на европейское экономическое простран-

[5] Proposal for a Regulation of the European Parliament and Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454

ство (European Economic Area, EEA)[6], а это расширяет рамки применения нормативных положений данного акта на правопорядки стран-членов ЕЕА, т.е. на Исландию, Лихтенштейн, Норвегию. Помимо этого, следует обратить внимание на «опосредованное» расширение сферы охвата Акта киберустойчивости 2022, поскольку пунктом (67) его Преамбулы предусмотрено использование широкого спектра правовых инструментов, таких как билатеральные межправительственные соглашения о взаимном признании (Mutual Recognition Agreements, MRAs). Названные соглашения заключаются между Евросоюзом и третьими странами, которые находятся на сопоставимом уровне технического развития, в частности, со странами Европейской ассоциации свободной торговли (European Free Trade Association, EFTA), членами которой являются как страны-члены ЕЕА, так и Великобритания, Швейцария[7]. Соглашения о взаимном признании не только способствуют торговле товарами между ЕС и странами-членами указанных организаций, равно как и с другими странами[8], облегчая взаимный доступ на рынки, но и базируются на взаимном признании сертификатов (certificates), знаков соответствия (marks of conformity), протоколов испытаний (test reports), выданных органами по оценке соответствия одной из сторон, согласно законодательству другой стороны. По смыслу положений упомянутого выше пункта (67) Акта киберустойчивости 2022, сотрудничество со странами-партнерами повышает киберустойчивость в глобальном масштабе, а в долгосрочной перспективе способствует укреплению системных рамок кибербезопасности как в рамках Евросоюза, так и за его пределами.

Предлагаемый Акт киберустойчивости 2022 тесно встраивается в регуляторные рамки как действующих законодательных актов, так и актов, находящихся в стадии разработки и принятия. Это гармонизирует и упорядочивает нормативно-правовую базу ЕС в части соблюдения вводимых требований кибербезопасности для цифровой продукции, в т.ч. исключая дублирование требований, вытекающих из разнообразных законодательных актов ЕС. В этой связи целесообразно отметить, что Акт киберустойчивости 2022 предполагает его системное взаимодействие с такими ключевыми действующими законодательными актами Евросоюза, как:

- Директива 2013/40/ЕС об атаках на информационные системы (12.8.2013)[9];
- Директива (ЕС) 2016/1148 о мерах по обеспечению высокого общего уровня безопасности сетевых и информационных систем в рамках Евросоюза (6.7.2016), именуемая Директивой NIS1[10];
- Регламент (ЕС) 2019/881 от 17.4.2019 об Агентстве Европейского союза по кибербезопасности (ENISA) и о сертификации кибербезопасности информационно-коммуникационных технологий, а также отмене Регламента (ЕС) 526/2013 (Акт о кибербезопасности)[11];
- Регламент (ЕС) 2019/1020 от 20.6.2019 о надзоре за рынком и соблюдении требований к продуктам, изменяющий Директиву 2004/42/ЕС и Регламенты (ЕС) 765/2008 и (ЕС) 305/2011[12].

Примечательно, что Акт киберустойчивости 2022 опирается на ряд законодательных актов, которые в настоящее время находятся в стадии принятия, и в их числе следует назвать Предложение по замене Директивы NIS и принятию Директивы NIS2, предварительное соглашение по тексту которой было достигнуто 13 мая 2022 года[13]; Предложение по принятию Регламента (21.04.2021) в отношении установления гармонизированных нормативных правил об искусственном интеллекте, а также внесении изменений в ряд законодательных актов Евросоюза, именуемый «Актом об искусственном интеллекте» (Artificial Intelligence Act, AI Act)[14].

Значительный объем Акта киберустойчивости 2022 позволяет в формате настоящей статьи лишь кратко обозначить его структуру, которая охватывает 71 пункт Преамбулы и семь глав: Общие положения (I); Обязательства для субъектов экономической деятельности (II); Соответствие продукции с цифровыми элементами (III); Нотификация органов по оценке соответствия (IV); Надзор за рынком и правоприменение (V); Делегированные полномочия и процедуры работы

6 О Европейском экономическом пространстве, именуемого также Европейской экономической Зоной, см. подробнее, например, URL: Legal Aspects of the EEA Agreement. https://www.efta.int/eea/eea-agreement#, а также: The basic features of the EEA Agreement. URL: http://www.efta.int/eea/eea-agreement/eea-basic-features.aspx and the EFTA website http://www.efta.int.

7 European Free Trade Association, EFTA. URL: https://www.efta.int/Free-Trade/news/EEA-EFTA-States-sign-free-trade-agreement-UK-524641

8 Европейские компании, экспортирующие свою продукцию в Австралию, Канаду, Японию, Новую Зеландию, США, Израиль, обязаны соблюдать действующие Соглашения о взаимном признании (MRAs), а также взаимодействовать с соответствующими назначенными органами по оценке соответствия (Conformity Assessment Bodies, CABs). URL:https://single-market-economy.ec.europa.eu/single-market/goods/international-aspects-single-market/mutual-recognition-agreements_en

9 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Официальный Журнал ЕС. Право. 218, 14.8.2013, с. 8–14.

10 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Официальный Журнал ЕС. Право. 194/1, 19.7.2016, с.1)

11 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Официальный Журнал ЕС. Право. 151, 7.6.2019, с. 15

12 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011. Официальный Журнал ЕС. Право. 169/1, 25.6.2019, с. 1

13 Directive NIS2. URL: https://www.nis-2-directive.com/

14 Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts of 21 April 2021, COM (2021) 206 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

комитетов (VI); Конфиденциальность и взыскания (VII). Кроме того, Акт киберустойчивости 2022 содержит четыре приложения, соответственно, (I) детализирует существенно значимые требования кибербезопасности; (II) определяет информацию и инструкции для пользователей; (III) содержит классификацию критически значимой цифровой продукции; (IV) определяет содержание Декларации ЕС о соответствии; (V) детализирует содержание технической документации; (VI) описывает процедуру оценки соответствия.

В содержательном плане нормативные положения Акта киберустойчивости 2022 распространяются на всю цифровую продукцию, предполагаемое и разумно прогнозируемое использование которой связывается с прямым или косвенным, логическим или физическим подключением данных к устройству или сети, что охватывает как аппаратное, так и программное обеспечение. Установленные Актом киберустойчивости 2022 общие правила и требования кибербезопасности затрагивают обязательства разработчиков, изготовителей, дистрибьюторов цифровых продуктов (в т.ч. их представителей) и связываются с реализацией конкретных задач: (1) изготовителям следует обеспечивать безопасность цифровой продукции с момента ее проектирования и разработки, а также на протяжении всего жизненного цикла продукции; (2) производители оборудования и программного обеспечения должны предпринимать согласованные действия по соблюдению требований кибербезопасности; (3) размещаемые на рынке ЕС подключенные устройства, продукция и ПО должны отвечать требованиям кибербезопасности и быть устойчивыми к уязвимостям; (4) изготовители цифровой продукции и разработчики ПО, а также их представители должны нести ответственность за нарушение кибербезопасности продукции на протяжении всего ее жизненного цикла; (5) потребители должны обладать возможностью безопасно использовать цифровую продукцию, а также быть проинформированы надлежащим образом о кибербезопасности приобретаемой или используемой ими цифровой продукции.

Следует обратить внимание, что согласно рассматриваемому акту, изготовители цифровой продукции должны соблюдать установленные требования независимо от того, производятся ли эти продукты в ЕС или нет. Обязательным требованием для цифровой продукции является необходимость маркировки «CE», подтверждающей ее соответствие минимальному уровню проверки кибербезопасности. За нарушение установленных требований предусмотрены меры взыскания, включая штрафные санкции – штрафы в размере до 15 миллионов евро или 2,5% от мирового оборота, в зависимости от того, какая сумма больше.

* * *

Обозначенная в начале статьи широкая сфера действия Акта киберустойчивости 2022, а также его краткая структурно-содержательная характеристика, как представляется, дает основание сделать выводы обобщающего свойства.

Предложенный к принятию Акт киберустойчивости 2022 дополняет и обогащает широкую палитру нормативного регуляторного механизма защиты киберпространства единого внутреннего рынка ЕС, одновременно содействуя прозрачной регламентации функционирования цифрового сектора и ИКТ-пространства в масштабе Европы в целом.

Отнюдь не безосновательно Еврокомиссия полагает, что данный акт способен стать неким «международным» эталоном соответствия цифровой продукции требованиям кибербезопасности, повторив регуляторный успех системы маркировки Евросоюза «CE» и Регламента GDPR.

Текущий момент рассмотрения предлагаемого Акта киберустойчивости 2022 сопрягается с процедурой экспертного согласования, а также определения соразмерности и пропорциональности на уровне общих институциональных механизмов Евросоюза. Вместе с тем не вызывает сомнений, что в концептуальном, содержательном и регуляторном плане Акт киберустойчивости 2022 вряд ли претерпит существенные изменения.

Где находится .ru? Анализ воздействия конфликта на российскую доменную инфраструктуру

Mattijs Jonker, Roland van Rijswijk-Deij — Университет Твенте

Alessio Botta, Antonia Affinito — Неаполитанский университет

Gautam Akiwate, Geoffrey M. Voelker, Stefan Savage — Калифорнийский университет в Сан-Диего

kc Claffy — Центр прикладного анализа данных Интернета (CAIDA) / Калифорнийский университет в Сан-Диего

Военные действия на Украине привели к возведению беспрецедентных экономических барьеров вокруг России – как по инициативе третьих стран, так и по ее собственной. В Интернете эти барьеры выражены в форме влияния на российские сайты со стороны государства, побуждающего их к переносу необходимой для их функционирования инфраструктуры (такой, как служба имен и хостинг) в Россию, а также давления извне со стороны западных провайдеров, отказывающихся вести бизнес с российскими клиентами. Хотя на эту тему уже существует немало публикаций – как освещающих политику провайдеров, так и описывающих личный опыт, – мы решили подойти к вопросу эмпирически и напрямую измерить долгосрочные изменения в географическом расположении серверов имен, хостинга и удостоверяющих центров для доменов Российской Федерации.

1. ВВЕДЕНИЕ

24 февраля 2022 года начался вооруженный конфликт России и Украины, что привело к крупнейшему гуманитарному кризису в Европе со времен Второй мировой войны. Действия России, в отличие от присоединения Крыма в 2014 году и неизменной поддержки новообразованных республик на востоке Украины, вызвали резкую реакцию со стороны мирового сообщества, в первую очередь западных стран. Помимо военной и финансовой помощи Украине, страны Запада объявили широкомасштабные экономические санкции против лиц и организаций, связанных с Россией, включая Центробанк РФ, внедрили ограничения экспорта, чтобы лишить Россию доступа к стратегическим материалам, конфисковали или заморозили российское имущество и активы за рубежом, закрыли небо для российских авиакомпаний и въезд для многих категорий российских граждан. Помимо этих мер, принятых на государственном уровне, около тысячи частных компаний приняли решение полностью или частично уйти с российского рынка [16].

Не избежал этого конфликта и Интернет. Например, Управление США по контролю над иностранными активами (US Office of Foreign Asset Control, OFAC) внесло ряд веб-сайтов российских компаний в свой санкционный список Specially Designated Nationals (SDN) [17]. Независимо от этих конкретных санкций, многие западные поставщики интернет-сервисов приняли решение — будь то по морально-этическим соображениям или исходя из репутационных рисков и/или угроз экономической стабильности — решительно оборвать связи с российским рынком. Некоторые из них, такие как Amazon, Microsoft, Google [13] или GoDaddy [6], просто остановили продажи российским заказчикам, а другие, такие как Cogent, прекратили оказывать России вообще любые услуги [20]. Украина эти действия не только поддерживала, но и призывала к ним – вплоть до того, что ее вице-премьер в открытом письме руководству ICANN от 1 марта 2022 года формально потребовал от этой организации упразднить домены .ru, .рф и .su, поддержать отзыв всех сертификатов TLS и отключить корневые серверы DNS на территории Российской Федерации [5].

В результате в России еще более усилились давнишние опасения угроз «суверенитету в Интернете», а потому правительство решило действовать на опережение и перенести ключевые сервисы на свою территорию. В марте 2022 года российские власти предписали всем государственным сайтам и сервисам использовать только российских интернет-провайдеров, операторов системы доменных имен (DNS), а также российский хостинг [23]. Кроме того, Минцифры РФ объявило о создании независимого государственного удостоверяющего центра, чей корневой сертификат будет доверенным для российских браузеров (VK Atom и Yandex.Browser)[1]. Частные российские операторы также стали опасаться демаршей сторонних поставщиков услуг: в частности, RU-CENTER, ведущий российский регистратор и хостинг-провайдер, рекомендовал клиентам, «ведущим деятельность в секторах, подверженных иностранным санкциям», «приобретать сертификаты от GlobalSign, японского удостоверяющего центра» [22].

Действия российского правительства, вкупе с риском того, что западные провайдеры и дальше будут свертывать сотрудничество, создают беспрецедентную атмосферу для российских операторов и их корпоративных клиентов. Было бы логично предположить, что происходящие процессы стимулируют уход российских сайтов из нероссийской инфраструктуры.

В настоящей статье мы попытаемся подойти к изучению этого вопроса эмпирически. В частности, мы исследуем долгосрочные изменения в геолокации инфраструктуры для российских сайтов – в первую очередь это DNS, хостинг и выдача сертификатов TLS – до и после начала российско-украинского конфликта. Наш анализ охватывает пять лет ежедневных наблюдений за доменами .ru и .рф, включая активные актуальные измерения и ретроспективные данные о выдаче сертификатов. Мы рассмотрим, в какой степени для этих сайтов имеет место перенос инфраструктуры в РФ из-за границы, и (в той мере, в которой он имеет место) объясняется ли он действиями провайдеров вне РФ или упреждающими мерами самих российских операторов.

2. НАБОРЫ ДАННЫХ

Мы оперируем данными измерений DNS по всем доменным именам, зарегистрированным в российских национальных доменах верхнего уровня .ru и .рф[2] за период в 1803 дня (чуть меньше пяти лет). Точные даты начала и конца изучаемого периода – с 18 июня 2017 по 25 мая 2022 года, т.е. массив данных охватывает несколько лет до начала конфликта (24 февраля 2022 года) и 90 дней после.

Измерения DNS предоставлены проектом OpenINTEL, который использует ежедневные снапшоты файлов зон в качестве стартовых точек для активного опроса всех зарегистрированных доменных имен в рамках одного домена верхнего уровня (TLD) по выборке записей ресурсов DNS [21][3]. Собранные данные включают записи NS внутри каждого домена (по ним можно установить, делегируется ли служба имен за пределы доменов .ru и .рф), а также разрешение записи A для серверов имен и для их корневых доменов. Мы осуществляем геолокацию каждого из полученных IP-адресов, используя результаты на соответствующий момент из сервиса IP2location [9], получая на выходе прокси для физического хостинга инфраструктуры DNS и веб-сайта каждого домена соответственно[4]. Наш набор данных содержит 11,7 миллиона уникальных российских доменных имен, 13,3 тысячи уникальных сетей (номеров автономных систем – AS), в которых находятся корневые домены, и 9,5 тысячи сетей, в которых расположены авторитетные серверы DNS. Кроме того, мы собрали долгосрочные данные по сертификатам для доменов .ru и .рф как по историческим логам прозрачности сертификатов, так и по активным сканам веб-сайтов за время исследования, выполненным Censys [2][5]. И, наконец, мы выделили 107 уникальных доменов в отдельную группу санкционных, поскольку они представлены в санкционных списках США (US OFAC SDN) [17] или Великобритании [7][6].

3. ВОЗДЕЙСТВИЕ НА ЭКОСИСТЕМУ DNS

В этом разделе мы сначала предоставим исторический контекст для инфраструктуры DNS, поддерживающей домены .ru и .рф, а затем перейдем к рассмотрению ситуации с российскими доменами вообще и санкционными российскими доменами в частности, а также действий, предпринятых крупнейшими западными провайдерами.

3.1 Исторический контекст

Для описания исторического контекста мы классифицировали российские домены, попавшие в нашу выборку данных, по долгосрочному расположению их хостинга и инфраструктуры DNS за период с 18 июня 2017 года по 25 мая 2022 года. Назовем хостинг домена полностью российским, если все его записи A геолоцированы на территории Российской Федерации; частично российским, если в РФ находится лишь часть таких записей; и нероссийским, если все такие записи расположены вне РФ. Аналогично назовем полностью, частично или нероссийской службу DNS – по месту геолокации авторитетных серверов имен для этого домена.

---

1 Судя по дате, толчком к этому мог послужить шаг DigiCert, отозвавшего TLS-сертификат у банка ВТБ – предположительно, в ответ на включение банка в санкционный список США.

2 .рф – кириллический национальный домен верхнего уровня Российской Федерации. Международное доменное имя для него – .xn--p1ai.

3 https://openintel.nl/coverage/

4 Отметим, что в отношении геолокации на уровне стран имеется небольшая неопределенность, наводящая на мысль, что релокация может «запаздывать» – в частности, когда IP-адрес (или адресное пространство) хостинга или инфраструктуры DNS переносится, а не меняется.

5 Мы квалифицируем сертификат как «match», если в его поле CN (Common Name) или SAN (Subject Alternative Name) содержится доменное имя в домене верхнего уровня .ru или .рф.

6 Впоследствии Управление США по контролю над иностранными активами опубликовало 24 апреля 2022 года список исключений для ряда интернет-сервисов [24], но мы не наблюдали заметных изменений в практике выдачи сертификатов в ответ на это изменение политики.

Рисунок 1.
Географическое распределение инфраструктуры DNS для доменных имен .ru и .рф. Полностью российские означает, что серверы имен полностью расположены на территории РФ. Нероссийские означает, что ни один из серверов имен не находится на территории РФ. Частично российские означает частичное нахождение на территории РФ.

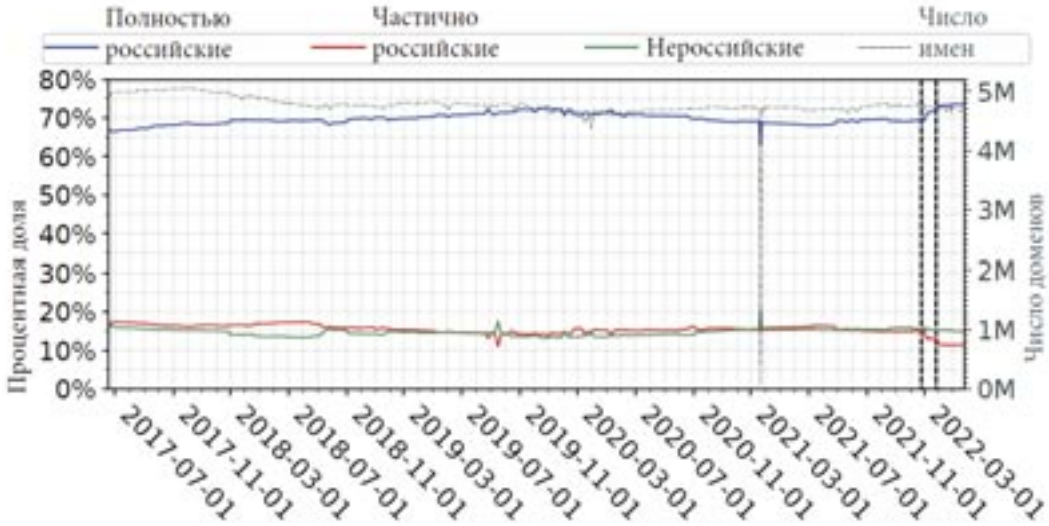
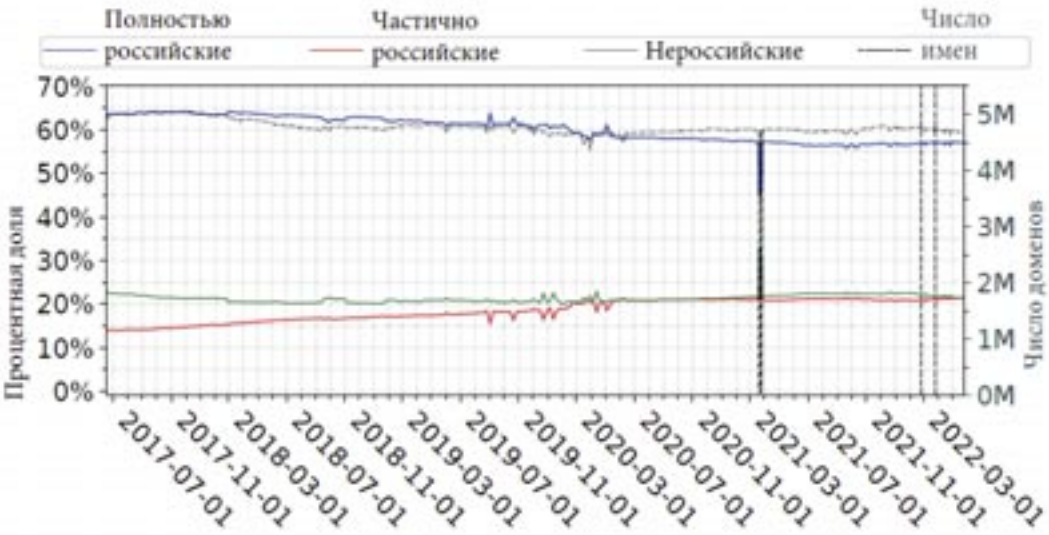


Рисунок 2.
Географическое распределение TLD-зависимости для авторитетных серверов доменных имен .ru и .рф. Полностью российские означает, что серверы имен полностью расположены на территории РФ. Нероссийские означает, что ни один из серверов имен не находится на территории РФ. Частично российские означает частичное нахождение на территории РФ.



В исторической перспективе доля доменов, расположенных в сетях на территории РФ, не претерпевала значительных изменений за изучаемый период. Например, на 18 июня 2017 года полностью расположены в России были 71,0% всех имен .ru и .рф, еще 0,19% были частично российскими, а 28,81% – нероссийскими. Это распределение не претерпело существенных изменений вплоть до начала конфликта в феврале 2022 года. После этого мы наблюдаем небольшой рост доли как полностью, так и частично российских доменов, вызванный «утеканием» доменных имен из США и других западных стран в Россию и Нидерланды.

Инфраструктура серверов имен для российских доменов также обнаружила относительную стабильность за долгий период времени, но с начала конфликта появились более выраженные изменения. На рис. 1 подробно показано долгосрочное распределение геолокации серверов имен. Для всех доменных имен в зонах .ru и .рф показано, расположены ли их серверы имен в России полностью, частично или нет[7]. Черной кривой показано общее количество российских доменов (штрихи справа). Для наглядности ситуации за последние месяцы мы выделили три периода: до начала конфликта (до 24 февраля 2022), после введения санкций (после 26 марта 2022) и до введения санкций (период между этими датами). На графике эти периоды отчеркнуты вертикальными пунктирными линиями.

На 18 июня 2017 года существовало чуть меньше пяти миллионов зарегистрированных доменов, 67,0% из которых пользовались серверами имен, полностью расположенными в России. Это распределение (как и почти идентичное количество частично российских и нероссийских доменов) остается более-менее стабильным с течением времени – это наводит на мысль, что в период, предшествовавший конфликту в 2022 году, внутреннее давление с целью переноса инфраструктуры в Россию большого эффекта не имело. А в феврале 2022 года появляются существенные изменения – многие домены, чьи серверы имен находились частично вне РФ, становятся полностью российскими. Однако в историческом контексте эти изменения невелики. По нашим последним данным, полностью российскими являются 73,9% имен – за пятилетний период изменение составило всего 6,9%.

У российской доменной инфраструктуры есть один аспект, который с течением времени становится все менее ориентирован на Россию: это принадлежность серверов имен к российским или иностранным доменным зонам. Назовем этот аспект для краткости TLD-зависимостью. Мы определили домен верхнего уровня (TLD) для каждого сервера имен, которому делегируют обслуживание доменные имена в зонах .ru и .рф. Если все серверы имен домена зарегистрированы исключительно в доменах верхнего уровня, относящихся к Российской Федерации, мы считаем TLD-зависимость полностью российской. Аналогично

[7] Провал 22 марта 2021 года вызван сбоем в работе измерительного оборудования.

Рисунок 3.
Пять крупнейших TLD, используемых авторитетными серверами имен для доменных имен .ru и .рф. На долю каждого из остальных 265 TLD (не показаны) приходится менее 1%.

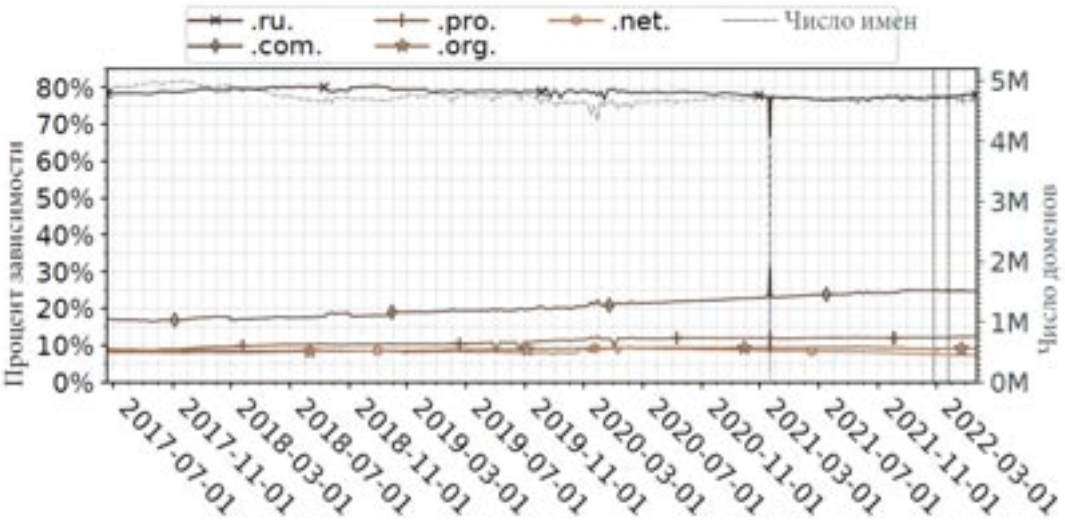
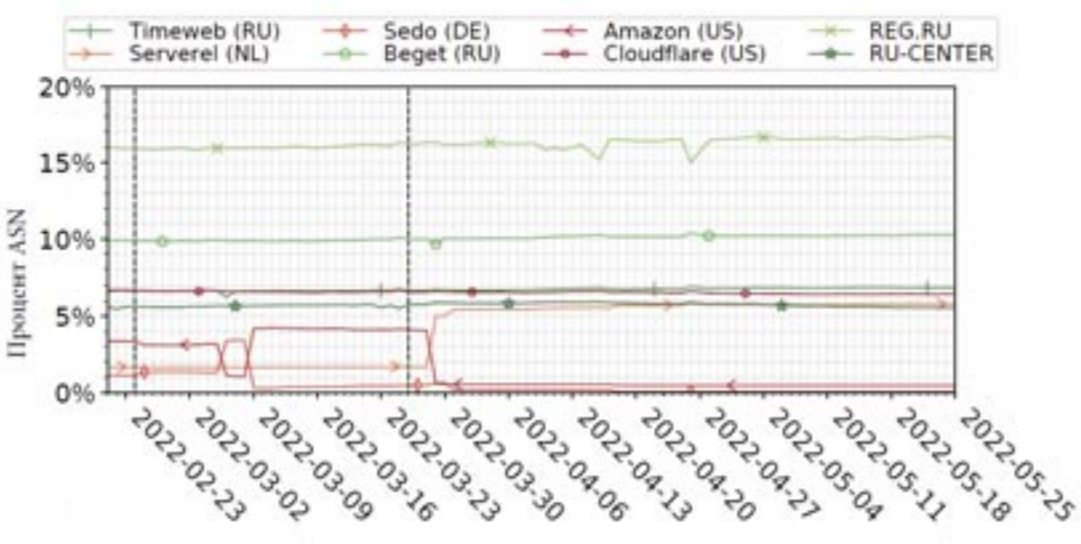


Рисунок 4.
Хостинговые сети доменных имен .ru и .рф (крупнейшие ASN). Для каждой хостинговой сети показана приходящаяся на нее доля российских доменных имен.



предыдущим определениям, если только часть TLD являются российскими, то TLD-зависимость частично российская, а если их нет вообще – то нероссийская.

На рис. 2 показан исторический тренд TLD-зависимости за время наблюдения. Возможно, это несколько неожиданно, но доля полностью российской TLD-зависимости несколько снижается (чистое уменьшение от максимума до минимума 6,3%), а доля частично российской растет (чистый рост 7,9%). Со временем все больше российских доменов используют серверы имен в нероссийских доменах верхнего уровня, неявно увеличивая свою зависимость от внешней инфраструктуры, которая может попасть под западные санкции. На рис. 3 показано долгосрочное распределение долей различных TLD, в которых зарегистрированы авторитетные серверы российских доменов. Из 270 доменов на рисунке изображены только пять крупнейших. Лидирует в этом списке (что и неудивительно) домен .ru: на него приходится 78,3% всех серверов имен на 25 мая 2022 года. Вторым является домен .com, на который приходится 24,7% российских доменов (чистый рост на 7,5% за пять лет). Дальше по убыванию идут .pro (чья доля выросла с 8,8% до 12,4%), .org (его доля выросла с 8,2% до 9,2%) и .net (его доля снизилась с 9,1% до 7,3%). Ни один из остальных TLD не преодолел однопроцентный барьер (по состоянию на 25 мая).

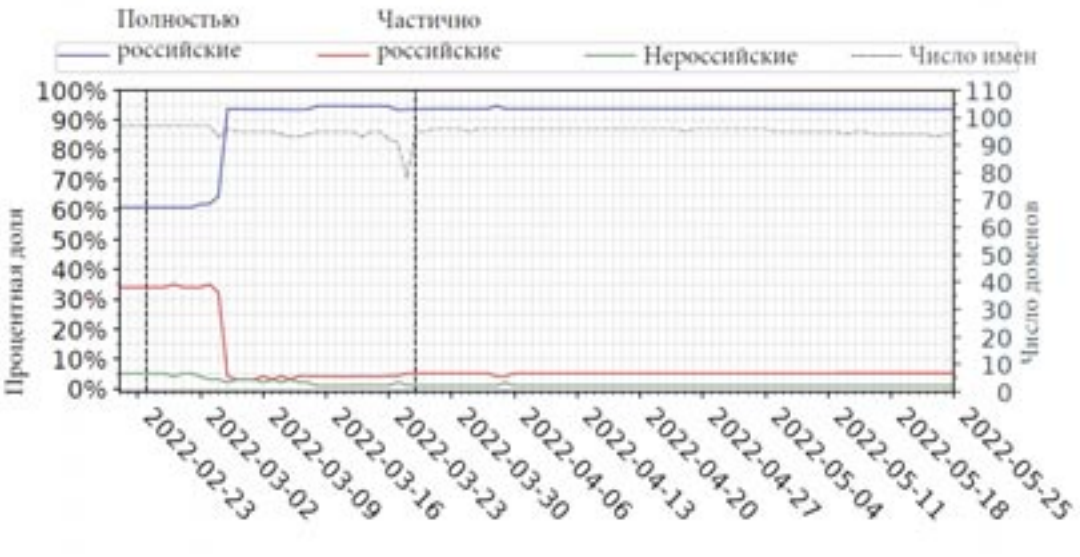
Тренды TLD-зависимости также изменились с началом конфликта. Доля полностью и частично российской TLD-зависимости доменов (см. рис. 2) очень незначительно увеличилась (соответственно на 0,2% и 0,5%). В результате крошечная доля российских доменов, для которых TLD-зависимость перестала быть нероссийской, стала менее уязвима к потенциальному влиянию Запада. Оставшиеся домены могут стать недоступными, если авторитетные серверы перестанут их обслуживать, или если Россия сама отключит себя от глобального Интернета.

3.2 Недавняя активность

С начала вооружённого конфликта многие российские домены сменили хостинг, но в подавляющем большинстве случаев они «переехали» из одной зарубежной хостинговой сети в другую. На рис. 4 показана статистика по нескольким провайдерским сетям, хостящим доменные имена .ru и .рф. У российских ASN, если рассматривать их в совокупности, клиентская база осталась стабильной, практически не изменившись – все вместе они хостили 38% российских доменов в начале наблюдения и 39% в конце. Еще одна стабильная кривая – это Cloudflare, на который приходится почти 7% российских доменов за весь период. Наблюдается и переток доменов .ru и .рф между тремя крупными провайдерами: сначала российские клиенты спешно выбирают между американским Amazon и германским Sedo, а затем уходят к нидерландскому Serverel. Эта динамика частично была вызвана реакцией бизнеса на конфликт, мы обсудим этот аспект в разделе 3.4.

Также произошли изменения и в части того, где хостится инфраструктура DNS российских доменов: здесь существенные подвижки начались до введения санкций и продолжились после их введения. В частности, значительные изменения коснулись шведского DNS-провайдера Netnod и RU-CENTER, крупного российского регистратора доменных имен и (бывшего) клиента Netnod. После реконфигурации IP-адресов 3 марта 2022 года Netnod перестал обслуживать 76 тысяч российских

Рисунок 5.
Распределение геолокации авторитетной инфраструктуры DNS по странам для санкционных российских доменов: полностью в России, частично в России и за рубежом.



доменов, которые быстро переехали из частично российского сегмента по инфраструктуре DNS в полностью российский (рис. 1). В конце марта произошел еще ряд крупных подвижек, связанных с миграцией доменов из сетей Hetzner (Германия) и Linode (США). С другой стороны, у еще одного крупного хостера DNS-инфраструктуры для российских доменов, Cloudflare, изменений с начала конфликта практически нет.

3.3 Санкционные доменные имена

Теперь мы вплотную рассмотрим доменные имена, явно связанные с российскими структурами, подпавшими под санкции США и Великобритании.

Отметим, что тут потенциал каких-то подвижек крайне мал, т.к. 101 из 107 санкционных доменов (94,4%) на 24 февраля 2022 года уже размещались исключительно в российских ASN. К 25 мая 2022 года полностью российскими стали еще три[8], а три оставшихся остались нероссийскими – их хостинг целиком расположен в Германии, Чешской Республике и Эстонии.

Однако инфраструктура имен доменов для этих санкционных доменов претерпела существенные изменения. На рис. 5 показано распределение геолокации авторитетной инфраструктуры DNS для этих доменов в разные периоды времени. Опять же, три цветные кривые показывают полностью российскую, частично российскую и нероссийскую части, а черная кривая – общее количество за день.

На 24 февраля 2022 года 34,0% всех санкционных доменов были частично российскими, а 5,2% – нероссийскими. К 4 марта 2022 года ситуация в корне изменилась: у подавляющего большинства (93,8%) санкционных доменов инфраструктура DNS теперь целиком располагается в России. Отметим, что почти у всех санкционных доменов к 4 марта превратившихся из частично российских в полностью российские, хостером авторитетных серверов имен до релокации в Россию был шведский Netnod.

[8] Ранее хостинг этих трех доменов осуществлялся исключительно в Германии или Польше.

3.4 Действия провайдеров

Ряд западных провайдеров публично заявили о своих действиях в ответ на возникший конфликт – будь то в качестве добровольного протеста или в соответствии с санкциями. Анализируя наши данные по DNS, мы попробуем определить масштаб и последствия действий, предпринятых четырьмя крупнейшими западными провайдерами.

Amazon: 8 марта 2022 года Amazon заявил, что прекращает регистрацию новых учетных записей AWS для клиентов из России и Беларуси [1]. С этого момента мы видим существенные изменения для доменов .ru и .рф, разрешающихся в ASN компании Amazon (AS16509) – в том числе и появление новых доменов из этих зон, что стало для нас некоторой неожиданностью.

На рис. 6 показана динамика российских доменов, которые на 8 марта 2022 года относились к ASN компании Amazon. К 25 мая 2022 года больше половины этих доменов перебрались в другие ASN – но произошло ли это по инициативе Amazon или по собственному решению клиентов, мы сказать не можем. Чуть меньше половины доменов (43%) осталось в Amazon, но при этом 574 домена из этого числа ранее не существовали и были зарегистрированы только что (данные подтверждены с помощью API Whois Domain от Cisco), а еще 988 переехали в Amazon из других ASN.

Рисунок 6.
Динамика российских доменных имен в ASN AS16509 компании Amazon (сравнение 08.03.2022 и 25.05.2022).

Рисунок 7.
Динамика российских доменных имен в ASN AS47846 компании Sedo (сравнение 08.03.2022 и 25.05.2022).

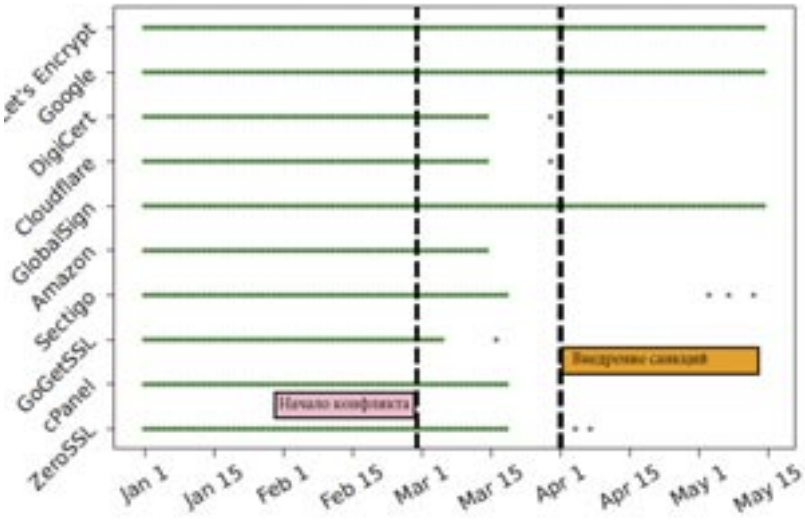
Таблица 1.
Выпуск сертификатов удостоверяющими центрами за три периода 2022 года

До начала конфликта			До введения санкций			После введения санкций		
УЦ	Число серт.	(%)	УЦ	Число серт.	(%)	УЦ	Число серт.	(%)
Let's Encrypt	6586K	91,58%	Let's Encrypt	3285K	98,06%	Let's Encrypt	5458K	99,23%
DigiCert	244K	3,40%	GlobalSign	25K	0,76%	GlobalSign	28K	0,52%
cPanel	153K	2,13%	cPanel	11K	0,34%	Google	13K	0,24%
Прочие УЦ	207K	2,89%	Прочие УЦ	28K	0,84%	Прочие УЦ	422	0,01%

Таблица 2.
Отзыв сертификатов пятью УЦ, на которые приходится большая часть отзывов

	Домены .ru и .рф		Санкционные домены	
УЦ	Выдано	Отозвано	Выдано	Отозвано
Let's Encrypt	15 млн	10K (0,06%)	16K	196 (1,19%)
DigiCert	247K	2,1K (0,80%)	308	308 (100%)
GlobalSign	95K	1,6K (1,68%)	905	23 (2,54%)
Sectigo	96K	5,1K (5,15%)	164	164 (100%)
ZeroSSL	56K	165 (0,30%)	82	2 (2,43%)

Рисунок 8.
Временной график выпуска новых сертификатов для доменов .ru и .рф удостоверяющими центрами. Зеленая точка означает, что УЦ выпустил в этот день хотя бы один сертификат.



Появление 1,5 тысяч новых доменных имен .ru и .рф на первый взгляд противоречит заявлениям Amazon, но не исключено, что эти домены принадлежат уже существующим клиентам[9].

Sedo: 9 марта 2022 года в прессе появились сообщения о том, что Sedo «перекрывает кислород» российским доменам [15]. Слова у Sedo не разошлись с делами, хотя «кислород» был перекрыт все-таки не полностью. На рис. 7 видно, что изменения для доменов .ru и .рф в сети Sedo AS47846 были весьма существенными. На 8 марта 2022 года в сеть Sedo (AS47846) разрешалось 164 тысячи доменов .ru и .рф. К 25 мая 2022 160 тысяч доменов (98%) переехали в другие ASN, 2,7 тысячи (1,6%) осталось, а 311 доменов переместились в Sedo извне.

Cloudflare: 7 марта 2022 года Cloudflare опубликовала статью, в которой заявляла о том, что будет соблюдать санкции [18]. Также фирма заявила, что, проконсультировавшись с госорганами и экспертами по гражданскому обществу, она приняла решение не прекращать оказание услуг Cloudflare на территории Российской Федерации. Разрешения доменов подтверждают, что существенных изменений и не произошло. На 7 марта 2022 года в сеть AS13335 разрешалось почти 315 тысяч имен из доменных зон .ru и .рф. На 25 мая 2022 в AS-сети Cloudflare из них осталось 296 тысяч (94% первоначального списка), а также добавились 34 тысячи новых российских доменов. Такая картина коррелирует с заявлением руководителя Cloudflare Мэтью Принса о том, что «России нужно больше доступа к Интернету, а не меньше» [18].

Google: 10 марта 2022 года пресса сообщила, что, по словам представителя Google, компания перестанет принимать новых клиентов из России [11]. О том, как Google поступит с имеющимися облачными клиентами из РФ, представитель умолчал. На 10 марта 2022 в сеть Google (AS15169) разрешалось 17,7 тысячи доменов .ru и .рф. К 25 мая 2022 года 57,1 тысячи доменов (10,1%) переехали в другие ASN, но большинство из них (75,2%) остались в Google, просто перебазировавшись в другую его сеть (AS396982)[10]. За этот период в Google также переехало небольшое количество доменов извне (187) и вновь зарегистрированных доменов (184). Возможно, эти домены, как и в случае Amazon, принадлежат уже существующим клиентам.

[9] Используя API Whois Domain от Cisco, мы нашли сведения о том, на кого зарегистрирована часть этих доменов (около 1/6 от общего количества). Проверив эти имена вручную, мы выяснили, что часть вновь зарегистрированных доменов принадлежит существующим клиентам Amazon, никак не связанным с Россией, и была создана в рамках обычной бизнес-практики или для защиты интеллектуальной собственности (например, Disney зарегистрировала целый ряд доменов с такими именами, как thorloveandthunder.ru или blackpantherwakandaforever.ru).

[10] Используя данные измерений DNS по нероссийским доменным именам, предоставленные OpenINTEL, мы обнаружили, что существенная миграция из сети AS15169 в AS396982 имела место и для имен из других TLD (это случилось примерно 16 марта). Поэтому можно предположить, что эта «внутригугловская» релокация произошла не потому, что 8,5 тысяч (75,2% от общего числа в 10,1 тыс.) затронутых доменов являлись российскими.

4. ВОЗДЕЙСТВИЕ НА ЭКОСИСТЕМУ WEBPKI

В современной веб-экосистеме сертификаты TLS являются жизненно важными инфраструктурными элементами для обеспечения безопасности доменов. В этом разделе мы рассмотрим реакцию различных удостоверяющих центров (УЦ) на конфликт и санкции в плане выдачи сертификатов российским доменам.

С одной стороны, конфликт и санкции не оказали существенного влияния на число сертификатов, выдаваемых глобальными УЦ российским доменам. За три рассматриваемых периода в 2022 году УЦ выдавали до конфликта в среднем по 130 тысяч сертификатов в день, до введения санкций – по 115 тысяч, после введения санкций – те же 115 тысяч. Однако различные УЦ отреагировали на конфликт очень по-разному, и в этом разделе мы обсудим действия глобальных УЦ, выдающих и отзывающих сертификаты, а также эффект появления нового российского доверенного корневого сертификата.

4.1 Изменения в выдаче сертификатов

Мы использовали журналы прозрачности сертификатов (Certificate Transparency, CT), индексированные Censys [2], чтобы получить сертификаты TLS для доменов .ru и .рф с 1 января 2022 года по 15 мая 2022. Для каждого сертификата мы извлекли фрагмент Issuer Organization из поля Issuer DN, чтобы установить, какой удостоверяющий центр выдал сертификат.

На рис. 8 показаны тренды выдачи новых сертификатов российским доменам для десяти крупнейших УЦ. Зеленая точка означает, что УЦ выпустил в этот день хотя бы один сертификат для домена .ru или .рф. Шесть из десяти крупнейших УЦ, обслуживавших российские домены, после начала конфликта или введения санкций перестали выдавать сертификаты совсем. Оставшиеся три УЦ на сегодняшний момент являются единственными крупными УЦ, обслуживающими домены .ru и .рф. Поскольку УЦ обычно выдают сертификаты с разными значениями CN (Common Name) (так, например, DigiCert использует RapidSSL и GeoTrust), мы подозреваем, что изолированные точки, скорее всего, вызваны тем, что данный УЦ не прекратил выпуск сертификатов под менее известными своими CN.

В таблице 1 показано количество выданных сертификатов за каждый из трех периодов по трем наиболее активным УЦ за соответствующий период. В целом можно сказать, что в результате конфликта выдача сертификатов еще более централизовалась, сосредоточившись в трех УЦ. Let's Encrypt и до конфликта доминировал на рынке, а после его начала он увеличил свою долю более чем до 99%. До конфликта сертификаты российским доменам выдавало множество УЦ, но после начала боевых войсковых действий сколько-то заметную деятельность в этой сфере ведут только три.

4.2 Отзыв сертификатов

Выдача сертификатов – это лишь одна сторона медали: некоторые УЦ не просто прекратили выдавать сертификаты, но и отозвали все ранее выданные сертификаты у санкционных доменов. Используя списки отзыва сертификатов (CRL) и состояние протокола OCSP (Online Certificate Status Protocol), индексированные Censys, мы подсчитали число отзывов сертификатов для доменов .ru и .рф по всем удостоверяющим центрам после 25 февраля 2022 года.

В таблице 2 приведена статистика выдачи и отзыва сертификатов пятью УЦ, на которые приходится большая часть отзывов. Стоит отметить, что DigiCert и Sectigo отозвали ранее выданные сертификаты у всех санкционных доменов – видимо, чтобы свести к нулю любой риск. Хотя мы не владеем информацией о политиках различных УЦ, можно отметить, что у всех УЦ существенно больше процент отзывов для санкционных доменов по сравнению с общей массой доменов .ru и .рф. Мы также подозреваем, что часть сертификатов могла быть отозвана по инициативе самих санкционных доменов, которые приспосабливались к санкциям, пробуя различные УЦ.

4.3 Сертификат Головного УЦ Минцифры России

Создание Головного удостоверяющего центра в Минцифры России привлекло к себе значительное внимание в момент объявления. Во-первых, это государственный УЦ, во-вторых, он не регистрирует выданные сертификаты в журналах CT, а в-третьих, не является доверенным для большинства браузеров[11]. Для оценки первоначального воздействия российского УЦ мы использовали набор данных CUIDS (Censys Universal Internet Data Set), который выполняет ежедневное сканирование IP по всему Интернету и индексирует все сертификаты TLS, возвращаемые опрошенными IP-адресами[12]. На основе этих результатов мы идентифицировали все сертификаты TLS, содержащие российский УЦ в своей цепочке сертификатов, с момента его учреждения до 15 мая 2022 года.

Сканы сертификатов позволяют выявить два тренда. Во-первых, очень мало сайтов используют сертификаты российского УЦ: в данных CUIDS обнаружилось всего лишь 170 уникальных сертификатов от Минцифры РФ. Для полноты картины заметим, что все остальные УЦ за то же время выпустили более 800 тысяч сертификатов для российских доменов. Хотя эти метрики нельзя сравнивать – выдается сертификатов гораздо больше, чем активно используется – скромное количество активных сертификатов от российского УЦ показывает, что он еще не успел оказать значительного влияния на общую экосистему российского Интернета. Во-вторых, как и ожидалось, все обнаружившиеся сертификаты российского УЦ выданы доменам организаций, связанных с Россией, а большинство из них относится к санкционным доменам. Из 170 сертификатов 130 приходятся на домен .ru, два – на домен .рф, а остальные рассредоточены по связанным с Россией доменам из длинного списка других TLD. По датам выдачи видно, что сертификаты выдавались в течение нескольких недель. Из 170 сертификатов 36 выданы санкционным доменам (34% всего списка санкционных доменов).

[11] Российским гражданам рекомендуется настроить свой браузер на доверие новому УЦ или же использовать браузер, одобренный госорганами.

[12] Поскольку активные сканы сертификатов, скорее всего, являются лишь подмножеством выданных сертификатов, сканы представляют собой нижнюю границу.

5. ДРУГИЕ РАБОТЫ В ЭТОЙ ОБЛАСТИ

Взаимосвязь между коммуникацией в Интернете и политическими интересами государств в последнее время стала важной темой для исследования: от анализа государственной цензуры на глобальном уровне [8, 25] до работ, посвященных цифровым методам борьбы с оппозицией – блокировкам, DoS-атакам и масштабным отключениям доступа в Интернет [3, 10]. Применительно к России, работа Moyakine и др. [14] посвящена принятому в 2015 году контртеррористическому «закону Яровой», налагающему на российских телекоммуникационных провайдеров обширные обязательства по мониторингу клиентов, и его воздействию на коммуникацию в уязвимых группах населения. Работа Epifanova and Dietrich [4] посвящена стремлению РФ к «цифровому суверенитету» – как для контроля над коммуникациями в стране, так и для большей независимости от зарубежных IT-сервисов. Эта цель ясно прослеживается в эмпирических исследованиях Zembruzki и др. [26] и Liu и др. [12], выявивших централизацию служб хостинга и электронной почты у очень маленькой группы западных провайдеров, но обнаруживших, что Россия противостоит этому тренду, демонстрируя сильную централизацию всей своей инфраструктуры. Ramesh и др. [19] анализируют централизованную политику блокировок Роскомнадзора, описывая блокировки контента в России и различие ситуации для индивидуальных и корпоративных заказчиков.

6. ОБСУЖДЕНИЕ

Усилия российского правительства по созданию «суверенного Интернета» включают в себя ряд нормативных требований к провайдерам, включая требование хранить данные о российских гражданах на российской территории, использование контролируемых Россией корневых серверов DNS, а также активное стимулирование в пользу выбора отечественных служб информационных и коммуникационных технологий (ICT) [4]. Возможно, самым ярким примером является (уже апробированная?) способность России жить в условиях отключения страны от глобального Интернета. Таким образом, Россия, вступая в конфликт с Украиной, несомненно, отдавала себе отчет, что Интернет может быть потенциальной уязвимостью, через которую на страну можно осуществлять давление.

В самом деле, мы видим четкие эмпирические подтверждения тому, что такое давление существует: тысячи российских сайтов потеряли доступ к ряду западных провайдеров, например, DNS-хостеру Netnod, хостеру сайтов Sedo, удостоверяющим центрам DigiCert и Sectigo. Однако эти проблемы далеко не судьбоносны. Во-первых, уровень отечественной локализации сервисов в России изначально был очень высок. Еще задолго до начала конфликта подавляющее большинство российских сайтов (70%) хостились полностью на российских сайтах и делегировали службу имен полностью отечественным серверам DNS[13]. Поэтому, пусть мы и наблюдаем изменения в размере нескольких процентов, их эффект по сравнению со всем российским Интернетом незначителен. Во-вторых, те российские сайты, которые пользуются зарубежной инфраструктурой, могут выбирать из множества провайдеров, которые не отказались от российских клиентов – как на территории РФ, так и за рубежом. Поэтому выход крупных западных провайдеров с российского рынка привел лишь к тому, что практически все пострадавшие сайты быстро нашли новых провайдеров. Мало того, мы практически не видим случаев спонтанной или упреждающей релокации в Россию у операторов российских доменов, которых к этому не принудили. В завершение следует отметить, что единственной уязвимой точкой для России является выдача сертификатов. Практически полный контроль Let's Encrypt над безопасностью в доменах .ru и .рф ошеломляет. Пускай Let's Encrypt и видит своей миссией бесплатную выдачу сертификатов для всех желающих во имя общественного блага – но это все равно американское учреждение, подчиняющееся американским законам и экспортным ограничениям. Мало того, Россия не предотвратила эту проблему, создав отечественный УЦ с аналогичными возможностями и, что еще важнее, установив доверительные отношения такого УЦ с распространенными браузерами.

7. ЭТИКА

В настоящей статье мы постарались предоставить ситуативный контекст изменений в инфраструктуре доменов .ru и .рф в результате воздействия противоборствующих сил (изнутри и извне России) и идей «киберсуверенитета». Хотя этот тип анализа – идентификация трендов в инфраструктуре – не вызывает этических возражений, мы осознаем, что ситуация вокруг конфликта является весьма деликатной, а влияние санкций на глобальный Интернет может вызывать тревогу. Понимая и признавая эти соображения, мы тем не менее убеждены, что прозрачность поможет их разрешить.

8. БЛАГОДАРНОСТИ

Мы благодарим анонимных рецензентов IMC за содержательную обратную связь и рекомендации. Настоящая работа осуществлена при частичной поддержке проекта EC H2020 CONCORDIA (830927), гранта Национального научного фонда США CNS-1705050, кафедры информации и компьютерных наук имени Ирвина Марка и Джоан Клейн Джейкобс в Калифорнийском университете в Сан-Диего, а также при операционной поддержке Центра сетевых систем Калифорнийского университета в Сан-Диего. Настоящее исследование стало возможным благодаря OpenINTEL, совместному проекту Университета Твенте, SURF, SIDN и NLnet Labs.

[13] Самые ранние из наших данных датированы 2017 годом, поэтому мы ничего не можем сказать о том, является ли такая централизация интернет-сервисов на территории РФ типичной для России за более продолжительный период.

СПИСОК ЛИТЕРАТУРЫ

1. Amazon. 2022. Updates to Amazon's retail, entertainment, and AWS businesses in Russia and Belarus. https://www.aboutamazon.com/news/aws/updates-to-amazons-retail-entertainment-and-aws-businesses-in-russia-and-belarus aboutamazon (март 2022 г.) Дата обращения: май 2022 г.
2. Censys. 2022. Censys Bulk Data Access. https://censys.io/data.
3. Alberto Dainotti, Claudio Squarcella, Emile Aben, Kimberly C. Claffy, Marco Chiesa, Michele Russo, and Antonio Pescapé. 2014. Analysis of Country-Wide Internet Outages Caused by Censorship. IEEE/ACM Transactions on Networking 22, 6 (декабрь 2014 г.), 1964–1977.
4. Alena Epifanova and Philipp Dietrich. 2022. Russia's Quest for Digital Sovereignty: Ambitions, Realities and Its Place in the World. German Council on Foreign Relations 1 (2022).
5. Mykhailo Fedorov. 2022. Letter to Goran Marby, President and CEO of ICANN. https://eump.org/media/2022/Goran-Marby.pdf. Дата обращения: июнь 2022 г.
6. GoDaddy. 2022. How GoDaddy is Supporting Ukrainian Customers. https://aboutus.godaddy.net/newsroom/company-news/news-details/2022/How-GoDaddy-is-Supporting-Ukrainian - Customers/default.aspx. Дата обращения: май 2022 г.
7. UK Government. 2020. The UK Sanctions List. https://www.gov.uk/government/ publications/the-uk-sanctions-list. Дата обращения: 14.04.2022.
8. James Griffiths. 2021. The great firewall of China: How to build and control an alternative version of the internet. Bloomsbury Publishing.
9. IP2Location. n.d. IP2Location IP Address Geolocation Database. https://www. ip2location.com/database/ip2location/. Дата обращения: май 2022 г.
10. [10] Lukas Kawerau, Nils B. Weidmann, and Alberto Dainotti. 2022. Attack or Block? Repertoires of Digital Censorship in Autocracies. Journal of Information Technology & Politics 0, 0 (2022), 1–14. https://doi.org/10.1080/19331681.2022.2037118
11. [11] Rebecca Klar. 2022. Google Cloud to stop accepting new customers in Russia. https://www.msn.com/en-us/news/politics/google-cloud-to-stop-accepting-new-customers-in-russia/ar-AAUTGK4. msn (2022). Дата обращения: май 2022 г.
12. Enze Liu, Gautam Akiwate, Mattijs Jonker, Ariana Mirian, Stefan Savage, and Geoffrey M. Voelker. 2021. Who's Got Your Mail? Characterizing Mail Service Provider Usage. В составе сборника: Proceedings of the 21st ACM Internet Measurement Conference (Virtual Event) (IMC '21). Association for Computing Machinery, New York, NY, USA, 122–136.
13. Ron Miller. 2022. Amazon, Microsoft and Google Have Suspended Cloud Sales in Russia. https://techcrunch.com/2022/03/10/amazon-microsoft-and-google-have- suspended-cloud-sales-in-russia. TechCrunch (2022). Дата обращения: май 2022 г.
14. E. Moyakine and A. Tabachnik. 2021. Struggling to strike the right balance between interests at stake: The 'Yarovaya', 'Fake news' and 'Disrespect' laws as examples of ill-conceived legislation in the age of modern technology. Computer Law & Security Review 40 (2021), 105512.
15. Kevin Murphy. 2022. Now Sedo Pulls the Plug on Russians. https://domainincite.com/27630-now-sedo-pulls-the-plug-on-russians. 2022. Дата обращения: май 2022 г.
16. Yale School of Management. 2022. Almost 1,000 Companies Have Curtailed Operations in Russia — But Some Remain. https://som.yale.edu/story/2022/almost- 1000-companies-have - curtailed-operations-russia-some-remain. Дата обращения: май 2022 г.
17. US Department of Treasury. 2022. Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists. https://home.treasury.gov/policy- issues/financial-sanctions/specially- designated-nationals-and-blocked-persons-list-sdn-human-readable-lists. Дата обращения: 14.04.
18. Matthew Prince. 2022. Steps We've Taken Around Cloudflare's Services in Ukraine, Belarus and Russia. https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/. Дата обращения: май 2022 г.
19. Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi. 2020. Decentralized Control: A Case Study of Russia. В составе сборника: Network and Distributed System Security. The Internet Society. https://www.ndss-symposium.org/wp-content/uploads/2020/02/23098.pdf
20. Reuters. 2022. U.S. firm Cogent cutting internet service to Russia. https://www.reuters.com/technology/us-firm-cogent- cutting-internet-service-russia-2022-03-04/. Дата обращения: май 2022 г.
21. Roland van Rijswijk-Deij, Mattijs Jonker, Anna Sperotto, and Aiko Pras. 2016. A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements. IEEE journal on selected areas in communications (JSAC) 34, 6 (июнь 2016 г.), 1877–1888. https://doi.org/10.1109/JSAC.2016.2558918
22. RU-Center. 2022. Recommended SSL certificates. https://www.nic.ru/en/catalog/ssl/recommended-ssl. Дата обращения: 14.05.
23. Юлия Тишина, Анастасия Гаврилюк, Венера Петрова, Никита Королев. 2022. Власти изолируют сети. https://www.kommersant.ru/doc/5249500. «Коммерсант» (2022). Дата обращения: май 2022 г.
24. [24] Department Of The Treasury. 2022. GENERAL LICENSE NO. 25 Authorizing Transactions Related to Telecommunications and Certain Internet-Based Communications. https://home.treasury.gov/system/files/126/russia_gl25.pdf.
25. Barney Warf. 2011. Geographies of global Internet censorship. GeoJournal 76, 1 (2011), 1–23.
26. Luciano Zembruzki, Raffaele Sommese, Lisandro Zambenedetti Granville, Arthur Selle Jacobs, Mattijs Jonker, and Giovane C. M. Moura. 2022. Hosting Industry Centralization and Consolidation. В составе сборника: NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. IEEE, 1–9.

DNS — от технологии к сервису

Павел Храмцов

Из истории DNS и SLA

В далеком 1971 году Пегги Карп (Peggy Karp) решила, что запоминать номера компьютеров в сети сложно, а потому им нужно дать символьные обозначения. В результате появился документ RFC-226 (STANDARDIZATION OF HOST MNEUMONICS) и широко известный атрибут каталога /etc в Unix-системах и не только – файл HOSTS (в ранних версиях NIC SRI[1] - HOSTS.TXT).

Содержание файла было небольшим – 20 хостов с номерами и именами (см. таблицу 1).

Таблица 1. Содержание файла HOSTS.TXT из документа RFC-226

HOST #	DESIGNATOR
1	UCLA
65	UCLA36
2	SRIARC
66	SRIAI
3	UCSB
4	UTAH
6	MULTCS
70	MITDM
7	RAND
8	SDC
9	HARV
10	LNCTX2
74	LNC360
11	STAN
12	ILL
69	BBN
133	BBNB
144	AMES
145	MITRE
158	TIP

Документ был опубликован 20 сентября 1971 года. До 3 ноября принимались возражения, дополнения, замечания, а с 8 ноября предполагалось, как бы пафосно это ни звучало, внедрение этого новшества.

К слову сказать, 12 октября того же года вышел обновленный документ. В нем было уже 44 хоста, уточнялся формат файла и разъяснялся механизм конструирования имен. Первая дистрибуция файла HOSTS состоялась в 1972 году.

Основной мотив использования HOSTS был обусловлен не большим количеством хостов в сети, которые невозможно было запомнить, а наличием «зоопарка» подобных файлов на компьютерах, подключенных в сеть.

К этому моменту, кстати, еще не появились протоколы стека TCP/IP, и имена вводились для использования в программе удаленного доступа (терминала) Telnet, а не для записи имен хостов в адресах электронной почты, как в последующих документах. Тем не менее, с этого момента в именовании компьютеров будущего Интернета появилась централизация.

А еще в неявном виде появилась услуга, которой до этого времени не было – ведение централизованной базы доменных имен. Файл HOSTS.TXT по существу является предтечей современных реестров доменных имен.

Раз появилась услуга, то появился и ее поставщик в лице Пегги Карп и ее коллективный потребитель в лице администраторов хостов.

Сначала для дистрибуции файла HOSTS.TXT использовали BBS (Bulletin Board System) Tenex. Затем файл стали получать по ftp из архива NIC SRI. Обновления в файл вносили один или два раза в неделю. Довольно часто изменения запаздывали, содержание было неактуальным, что вызывало нарекания[2].

Здесь мы подходим к еще одному аспекту, который важен в контексте данной статьи – управление услугой, а точнее, качеством предоставляемой услуги. Очевидно, что NIC SRI тут оказался не на высоте. Но сеть ARPA была небольшой и бесплатной для конечных пользователей. Заниматься оптимизацией за счет управления доходами и расходами никому даже в голову не приходило, и решение стали искать в новом технологическом подходе - системе DNS, благо работы финансировались за государственный счет.

В сфере телекоммуникаций первые SLA (Service Level Agreement, дословно переводится как «Соглашение об уровне обслуживания (оказания услуги)») появились в конце 1980-х. Их стали включать в сервисные контракты операторы фиксированной связи.

SLA, в первую очередь, – это соглашение между поставщиком и потребителем услуги. Оно, с одной стороны, предоставляет потребителю сервис заданного качества (качество определяется числовыми параметрами сервиса, определенными в SLA), а с другой, защищает поставщика услуги от необоснованных требований и претензий потребителя. К слову сказать, кто тут в большем выигрыше – это большой вопрос. Обычно сервис, предоставляемый по договору, частью которого является SLA, стОит гораздо дороже аналогичного, у которого в договоре на его предоставление раздела SLA нет.

Кроме того, в SLA указываются не только технические параметры услуги, но и прочие параметры обслуживания, например, время реакции клиентских служб на запросы клиентов или/и время устранения неисправностей. Также услуга может относиться к категории высокой доступности, когда время плановых профилактических работ (ППР) включено в учет доступности услуги, или, наоборот, существует согласованный

[1] Network Information Center of Stanford Research Institute

[2] https://iconia.com/before_the_dns.txt

график таких работ и время ППР в расчет доступности не включено.

Но вернемся к сервису DNS. Соглашения об уровне обслуживания не было в 1980-е годы даже на уровне сервиса реестра доменных имен. Собственно, его и не могло быть, т.к. поставщика услуги и потребителя услуги в коммерческом понимании тогда не существовало, как, впрочем, и самого Интернета и системы доменных имен в привычном смысле.

Система доменных имен (Domain Name System – DNS) как понятие, спецификация и пробная реализация этой спецификации была разработана по контракту с DARPA в 1983 году[3]. Она пришла на смену HOSTS.TXT. Сделано это было в рамках проекта ARPANET Полом Мокапетрисом (Paul Mockapetris) под руководством Джона Постела (Jon Postel).

По воспоминаниям Мокапетриса[4], Постел поручил ему несколько иную задачу – свести пять различных предложений по улучшению работы с HOSTS.TXT к некоторому компромиссу. Среди них было как минимум три готовые системы: IEN116, Xerox Reepvine и Clearinghouse systems.

Но вместо компромисса (как это часто случается, когда изучают чужой опыт) получилась новая спецификация распределенной иерархической информационной системы. В ней Мокапетрис использовал свой предыдущий опыт разработки распределенной файловой системы для малых компьютеров. Возможно, именно по этой причине DNS оказалась такой «живучей» и масштабируемой на широкий круг задач.

Первое программное обеспечение DNS появилось в 1983 году. Это был сервер «Jeeves» (отсылка к персонажу новелл сэра Пелама Гренвилла Вудхауса[5]), написанный Полом Мокапетрисом. Позже был написан DNS-сервер для Unix-машин, The Berkeley Internet Name Domain (BIND) package.

С 1983 по 1987 год ARPANET была тестовой площадкой для новой технологии. В 1987 году появились классические стандарты DNS - RFC-1034 (Domain Names-Concepts and Facilities) и RFC-1035 (Domain Names-Implementation and Specification), которыми разработчики ПО для сервиса DNS пользуются до сих пор.

Наличие контрактов с DARPA, а позже с NSF (National Scientific Foundation) не подразумевали каких-либо соглашений об уровне предоставления услуг. Это были исследовательские контракты, в которых главным результатом была разработка технологий. Собственно, в это время и начались трения между «заказчиком» и «исполнителем». Дух исследования преобладал над качеством, которое и определяется соглашением об уровне предоставления услуги.

Все должна была изменить приватизация Интернета. 30 апреля 1995 была отключена магистраль NSF, что поставило точку в приватизации инфраструктуры. Но оставалась еще система доменных имен, а точнее, порядок управления этой частью информационной инфраструктуры.

Для того, чтобы оценить, насколько DNS была скорее исследовательским проектом, чем коммерческим предприятием, следует вспомнить историю «тестовой смены» корня, которая произошла в 1998 году[6].

К тому времени уже вовсю шли баталии вокруг коммерциализации доменных имен. Регистрация имен по $100 за имя в Network Solution Inc многим, в первую очередь, в США, не давала покоя. Администрация Клинтона была озабочена экономическим рывком за счет интернет-технологий. Уже готовилась реформа, в результате которой появится ICANN. И вот на фоне этой суеты Джон Постел решил провести «тест».

К тому времени primary DNS корневой зоны управлялся NSI[7] (A сервер). Остальные авторитативные серверы корневой зоны (Secondary DNS) копировали с него эту зону и далее отвечали на запросы кэширующих серверов, тем самым поддерживали процедуру разрешения доменных имен в Интернете.

Джон Постел в январе 1998 года попросил Джима Кода и Пола Викси (Paul Vixie) развернуть реплику primary DNS в ISI[8]. 28 января 1998 года Джон Постел направил администраторам восьми авторитативных серверов корневой зоны, которые не были в зоне прямого контроля администрации США, письмо с указаниями получения корневой зоны не с A-сервера NSI, а с B-сервера ISI.

Айра Магазайнер (Ira Magaziner), который отвечал в администрации президента Клинтона за реорганизацию Интернета, после переключения серверов был довольно быстро извещен службой безопасности о том, что авторитативные серверы DNS перенаправлены[9] с A-сервера на B-сервер. Он связался с Постелом и руководством USC и пообещал проблемы не только Джону Постелу, но и университету в целом, если Постел не вернет все в исходное положение.

Это была рекомендация, которую Джон Постел не мог не выполнить. Считается, что определение действий Постела администрацией президента США как «тест» системы DNS было способом «сохранить лицо» в данной ситуации для такого гуру Интернета как Джон Постел.

Возможно, что демарш Постела был реакцией на действия администрации президента США, которые привели к тому, что 18 сентября 1998 года была учреждена ICANN (Internet Corporation for Assigned Names and Numbers), и ее устав был зарегистрирован 30 сентября 1998 года[10].

[3] https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/mockapetris88.pdf

[4] https://historyofnetworking.s3.amazonaws.com/Paul+Mockapetris+-+Origins+Of+DNS.mp3

[5] «Just like Wodehouse's Jeeves guarding access to his master, there is a who;e my of digital doorkeepers patiently and continuously wathching over the internet (unless the are on strike).» The Server: A Media History from the Present to the Baroque Авторы: Markus Krajewski

[6] https://www.icann.org/en/system/files/files/rssac-023-17jun20-en.pdf

[7] Network Solution Inc

[8] USC Information Sciences Institute (ISI)

[9] https://www.youtube.com/watch?v=yoCfWcd_dFM&t=1813s

[10] https://www.icann.org/en/system/files/files/articles-incorporation-30sep98-en.pdf

С момента появления ICANN в системе доменных имен появились «хозяйствующие субъекты» (business entities): регистратуры, независимые регистраторы, операторы реестров, операторы DNS-инфраструктуры, депозитарии и резервные операторы регистратур.

Т.е. появились коммерческие услуги и компании, которые эти услуги оказывают. И с этого момента начался отсчет формирования соглашений об уровне предоставления этих услуг. Давайте же совершим краткий исторический экскурс в историю управления IT-услугами. Точнее, мы остановимся только на одном аспекте этого управления, а именно на соглашении об уровне предоставления сервиса или Service evel Agreement (SLA).

Корневая зона и домены верхнего уровня и SLA

Требования к параметрам сервиса DNS для доменов верхнего уровня и корневой зоны появились далеко не сразу. Первый документ на эту тему был разработан в виде RFC-2010[11] в 1996 году, т.е. до появления ICANN.

Чем примечателен этот документ? В нем определены основные технические параметры и требования к времени реакции технического персонала (администратора сервера DNS) на запросы, т.е. типичный набор требований SLA уже наличествует.

Производительность сервера определялась в 1200 запросов в секунду (qps), что по современным меркам довольно скромно, а вот время ответа на запрос должно было быть не более 5 ms, что и по современным меркам очень хорошо. Современный SLA для new gTLD, например, требует время отклика для транспорта UDP не более 500 ms.

В документе, правда, по поводу времени отклика есть оговорка, что сеть растет быстро и требование производительности может быть увеличено до 2000 qps, но при этом желательно сохранять задержку с ответом в 5 ms.

Интересно, что требование 5 ms на ответ в 1996 году характеризует размер сети, в которой такое время отклика было достижимо: это норма для локальной сети, но не для сети, распределенной по всем континентам.

При этом время реагирования администратора по электронной почте на запросы, связанные с проблемами функционирования сервера, не должно было превышать 24 часов.

Позже, уже в 2000 году, по рекомендациям RSSAC (Root Server System Advisory Committee) требования RFC-2010 были заменены на требования RFC-2870[12]. Из документа убрали производительность и время отклика и ввели требование поддержки DNSSEC и регламенты проведения плановых профилактических работ (ППР), а также сняли требование применения ПО, рекомендованного командой primary DNS.

В 2014 году RSSAC опубликовали проект документа «Servers Expectation of Root Servers»[13]. В этом документе появилось понятие «доступность сервиса», но у него еще отсутствовали конкретные параметры. В основном речь шла только о регламентах, которые должны соблюдаться командами root-серверов. Параллельно был опубликован проект документа «Measurements of the Root Server System», который ввел список измеряемых параметров. Документы были приняты в 2015 году и с тех пор регулярно обновляются.

В 2020 году в этих документах появилась новация, связанная со временем распространения корневой зоны по root-серверам. За время распространения стали считать время, за которое новую редакцию корневой зоны начинают поддерживать 95% экземпляров root-серверов.

Здесь имеет смысл сделать пояснение, что формально мы имеем 13 корневых серверов по количеству IPv4-адресов и Ipv6-адресов. Но реальных физических и виртуальных экземпляров DNS-серверов, которые выполняют функции корневых серверов (авторитативных серверов корневой зоны), гораздо больше. Каждый адрес – это Anycast-облако географически и типологически распределенных хостов.

В 2022 году RSSAC выпустил документ RSSAC047v2: RSSAC Advisory on Metrics for the DNS Root Servers and the Root Server System[14].

Этот документ замечателен тем, что в нем появилась методика расчета доступности сервиса DNS для корневой зоны. В основу методики исследования надежности была положена довольно распространённая модель системы «k из n».

RSSAC рекомендовал использовать для определения необходимого числа root-серверов формулу [1]:

[1] K = [2/3(n-1)];

Где n – общее количество авторитативных серверов корневой зоны;
K – требуемое для надежной работы количество серверов корневой зоны.

В настоящее время n равно 13 и, соответственное, K равно 8.

Рекомендованный порог надежности (доступности) для одного root-сервера (IPv4- или IPv6-адрес) установлен в 96%, соответственно, общая доступность сервиса при таком допущении при расчете по формуле [2]:

$$[2]\ A=\sum_{i=k}^{n}\binom{n}{i}a^{i}(1-a)^{(n-i)};$$

Где n=13, k=8, a=96, будет равна, соответственно, A=99,999% (пять девяток), что в области телекоммуникаций в последнее время принято считать стандартным уровнем доступности сервиса, который прописывается в SLA.

[11] https://datatracker.ietf.org/doc/html/rfc2010
[12] https://datatracker.ietf.org/doc/html/rfc2870
[13] https://www.icann.org/en/system/files/files/rssac-001-draft-02may13-en.pdf
[14] https://www.icann.org/en/system/files/files/rssac-047-03feb22-en.pdf

В этом же документе установлен и порог для времени ответа на запросы root-сервером (IPv4- или IPv6-адрес):

- для UDP этот порог равен 250 ms;
- для TCP этот порог равен 500 ms.

Авторы документа отмечают, что обычно доступно более восьми серверов, следовательно, в этом случае доступность сервиса стремится к 100%, а порог для времени отклика всего сервиса может быть снижен.

Рекомендации по порогам для сервиса системы корневых серверов (Root server system, RSS) RSSAC сформулированы следующим образом:

Таблица 2. Рекомендованные параметры уровня сервиса для сервиса авторитетных серверов корневой зоны DNS

Metrics	Name(s)	Threshold(s)
6.1 RSS Availability	IPv4 UDP Availability IPv4 TCP Availability IPv6 UDP Availability IPv6 TCP Availability	99.999% 99.999% 99.999% 99.999%
6.2 RSS Response Latency	IPv4 UDP Response Latency IPv4 TCP Response Latency IPv6 UDP Response Latency IPv6 TCP Response Latency	150 milliseconds 300 milliseconds 150 milliseconds 300 milliseconds
6.3 RSS Correctness	Correctness	100%
6.4 RSS Publication Latency	Publication Latency	35 minutes

RSS Availability – доступность сервиса;
RSS Response Latency - время отклика на DNS-запрос;
RSS Correctness – корректность сервиса (корректность ответов);
RSS Publication Latency – задержка при распространении зоны по серверам.

Однако считать этот документ SLA оснований нет. Это скорее OLA, т.е. соглашение об уровне эксплуатации, т.к. коммерческих договоров у ICANN или PTI[15] с операторами корневых (root) серверов нет.

Приведенный выше подход применяется в программе new gTLD[16]. В спецификации 10, разделе 2 к договору перечислены следующие технические SLA-параметры:

Таблица 3. Service Level Agreement Matrix

	Параметры	SLR (ежемесячно)
DNS	Доступность сервиса DNS	0 минут простоя = 1 00% доступность
	Доступность сервера DNS	432 минуты простоя (99%)
	Время отклика по протоколу T CP для сервиса DNS	1500 миллисекунд, как минимум для 95% запросов
	Время отклика по протоколу UDP для сервиса DNS	500 миллисекунд, как минимум для 95% запросов
	Время обновления зоны после внесения изменений на серверах DNS	60 минут, как минимум для 95% тестовых запросов

[15] https://pti.icann.org/
[16] https://newgtlds.icann.org/en/

Конечно, время отклика на DNS-запрос в исторически первом RFC, посвященном этому вопросу, выглядит гораздо привлекательнее для пользователей DNS, но Интернет большой, и гарантировать ответ в 5 ms на любой DNS-запрос сейчас уже не решаются даже в ICANN. Тем не менее, такие требования от операторов связи поступают время от времени, и современные сервисы публичных DNS-резолверов постоянно к этому стремятся, но это уже тема следующего раздела нашей статьи.

Коммерческие услуги DNS и SLA

Долгое время сервис DNS своим клиентам предоставляли провайдеры подключения к сети Интернет (интернет-сервис провайдеры – Internet Service Provider, ISP). В первую очередь речь идет о предоставлении клиенту DNS-резолвера, т.е. программы, которая выполняет в Интернете поиск соответствия между доменными именами и адресами (классический случай). Адрес резолвера, как и адрес устройства пользователя, автоматически настраивается при подключении к сети провайдера. Именно резолвер имеют в виду в руководстве конечного пользователя ISP, когда ведут речь о сервере доменных имен.

В договоре на оказание услуг подключения к Интернету у российских ISP упоминания о DNS нет совсем. Соответственно, нет и SLA для этого сервиса. Единственным исключением является «Билайн», и то только потому, что «Билайн», хоть и формально, является регистратором доменных имен. Однако и здесь конкретных исчисляемых параметров, а также дисконтов при нарушении условий SLA не указано. В конце концов основная услуга ISP не DNS.

Если раньше (до Google DNS) кто-то регистрировал собственный домен, то найти DNS-провайдера было проблематично. Обычно либо поднимался собственный авторитативный сервер для своих доменов, либо использовались услуги DNS-сервиса хостинга. При наличии собственного сервера главной задачей было найти второй сервер для доменов второго уровня в .su и .ru.

Провайдеры хостинга предоставляют SLA на услугу хостинга, и для российских компаний значение доступности DNS сейчас находится где-то в диапазоне от 99,5[17] до 99,9[18].

Но есть в мире компании, которые специализируются на оказании услуг DNS - DNS дорос до того, чтобы стать коммерческой услугой. Как здесь обстоят дела с SLA? Насколько зрелой можно считать эту услугу?

В таблице 4 приведен сводный список параметров SLA ведущих DNS-провайдеров.

[17] https://www.1gb.ru/services_premium_plan_sla.php
[18] https://timeweb.com/ru/services/hosting/sla/

Таблица 4. Параметры SLA ведущих DNS-провайдеров

№ п/п	Сервис	Доступность (%)	Определение параметра доступности	Дисконт* (% от месячного платежа)				DNSPef
				<100	<99,99	<99,5	<95	
1	Azure	100	Время простоя – это общее количество минут, в течение которых доступ к DNS-зоне заказчика не предоставлялся. Зона считается недоступной, если на валидный запрос нет ответа в течение 2 секунд. Запрос направляется ко всем авторитетным серверам этой зоны. В случае отсутствия ответа в течение 2 секунд повторные запросы направляются в течение последующих 60 секунд Monthly Uptime % = (Maximum Available Minutes – Downtime) / Maximum Available Minutes X100	10	25	100		99,81
2	Google	100	Невозможность получить ответ со всех авторитетных серверов Cloud DNS зоны. «Время недоступности» означает период в 60 последовательных секунд, когда сервис недоступен. Любой период времени меньше, чем 60 секунд, когда сервис был недоступен, не входит во время недоступности.	10	10	25	50	99,86
3	Alibaba	100 (n HA)	«Время недоступности» означает период в 60 последовательных секунд, когда сервис недоступен. Любой период времени меньше, чем 60 секунд, когда сервис был недоступен, не входит во время недоступности.	15	30	100		
4	Amazon 53	100	Зона считается недоступной, если в течение минуты все 4 виртуальных имени авторитетных имен не способны ответить на все DNS-запросы в течение минуты.	10	25	100		99,98
5	CloudFlare	100 (n HA)	Для каждого периода недоступности в течение отчетного месяца дисконт при нарушении SLA считается, как: Service Credit = (Outage Period minutes * Affected Customer Ratio) ÷ Scheduled Availability minutes Affected Client Ratio= (Количество уникальных источников запросов (IP-адресов) затронутых отказом в обслуживании/ Общее количество уникальных источников запросов (IP-адресов)					99,98
6	Dyn (Oracle)	100	Для каждого периода недоступности в течение отчетного месяца дисконт при нарушении SLA считается, как: Service Credit = (Outage Period minutes * Affected Customer Ratio) ÷ Scheduled Availability minutes Affected Client Ratio= (Количество уникальных источников запросов (IP-адресов) затронутых отказом в обслуживании/Общее количество уникальных источников запросов (IP-адресов)					99,95
7	F5	99,9 (n HA)	Кредиты выписываются поминутно + учитывается время реакция на инцидент	> 60 секунд	> 60 минут	> суток		
8	Godaddy	99,9						99,98
9	UltraDNS (neustar)	100	Не более 55 млрд запросов в сутки (на 30 узлов)	Дисконта нет				99,99

*Дисконт – это скидки провайдера сервиса для клиентов в соответствии с фактической доступностью сервиса.

В этом сводном списке контролируемых параметров услуги DNS следует обратить внимание на несколько моментов:

- во-первых, в отличие от DNS SLA для доменов верхнего уровня, здесь не обозначены ограничения на время отклика для конечного клиента или специального пробника, который измеряет доступность сервиса;
- во-вторых, не определена методика проверки доступности, а сам расчет является классическим расчетом времени доступности сервиса;
- в-третьих, сервис считается доступным, если получен ответ хотя бы от одного из авторитетных серверов зоны клиента.

Стоит обратить внимание на последнюю колонку (таблица 4). Это измерения доступности сервиса независимой службой DNSperf[19] на момент написания статьи.

Любопытно, что все компании, кроме Godaddy, не соблюдают свой SLA и должны предоставлять дисконт от ежемесячного платежа. Т.е., видимо, сбои в обслуживании клиентов есть, но так как «бодаться» с клиентами накладно, то проще предоставить дисконт на минимальную сумму при появлении рекламации, чем идти в суд. Это полезно и для маркетинга услуги: таким образом можно управлять скидками без ущерба имиджу компании.

С точки зрения зрелости сервиса эти «недостижимые» 100% доступности говорят о высокой технологичности, осознанном риске и соответствии стандартам других услуг сектора услуг телекоммуникаций, где доступность сервиса в последнее время обычно определяют в 99,999%

- технологический триггер (англ. technology trigger) — появление инновации, первые публикации о новой технологии;
- пик чрезмерных ожиданий (Peak of Inflated Expectation) — от новой технологии ожидают революционных свойств, технология, благодаря новизне, становится популярной и предметом широкого обсуждения в сообществе;
- избавление от иллюзий (Trough of Disillusionment) — выявляются недостатки технологии, а утеря новизны не способствует восторженным публикациям, в сообществе отмечается разочарование новой технологией;
- преодоление недостатков (Slope of Enlightenment) — устраняются основные недостатки, интерес к технологии медленно возвращается, технология начинает внедряться в коммерческих проектах;
- плато продуктивности (Plateau of Productivity) — наступление зрелости технологии, сообщество воспринимает технологию как данность, осознавая её достоинства и ограничения.

Рисунок 1. Кривая зрелости IT-технологии Гартнера.

Вместо заключения

В 2023 году технологии DNS исполнится 40 лет. Она родилась тогда, когда Интернета не было не только в виде сети вебсайтов, но в виде социальных сетей. Даже технология TCP/IP не была внедрена.

Сейчас на базе DNS предоставляется целый спектр коммерческих услуг, как традиционных для этой технологии, так и новых. Наличие подробных соглашений об уровне предоставления этих услуг говорит о технологической и коммерческой зрелости DNS.

В диаграмме «Хайпа» Гартнера (Кривая Гартнера, Gartner Hype Cycle[20], рисунок 1), которая описывает цикл зрелости IT-технологии, выделяют несколько этапов[21]:

Кривая Гартнера – это руководство по вкладыванию или сворачиванию инвестиций в те или иные IT-направления.

В 1983 году DNS как технология и услуга находилась в области технологического триггера. Пик популярности пришелся на период с 1995 по 2000 годы. Скандалы вокруг Network Solution Inc, образование ICANN, пузырь доткомов пришлись на этот период. Пик популярности порождает поиск уязвимостей и их устранение, разработку и внедрение DNSSEC, применение DNS в областях, которые раньше в этом не нуждались, например, в мобильной связи. Таким образом, к 2010 году DNS выходит на «склон просвещения» («Slope of Enlightenment» на рис.1).

За 40 лет своей истории технология DNS прошла все стадии зрелости и сейчас находится на «плато продуктивности». Согласно Гартнеру, это означает, что технология широко внедрена, ее место на рынке и области применения хорошо известны. И это также означает, что DNS сегодня не только и не столько технология, сколько зрелый сервис с определенными соглашениями об уровне его предоставления – хотя ряд важных параметров пока еще остаются «за скобками» SLA.

[19] https://www.dnsperf.com
[20] https://www.gartner.com/en/research/methodologies/gartner-hype-cycle
[21] https://ru.wikipedia.org/wiki/Gartner

Новости науки и техники

1,84 петабайта в секунду – уже не фантастика

Группа исследователей университетов Дании и Швеции сообщила об успешном проведении эксперимента, в ходе которого была достигнута рекордная скорость передачи данных. Используя оптоволоконный кабель и лазерный чип особой конструкции, ученые смогли осуществить передачу примерно 1,84 петабайта данных в секунду. Результат является абсолютным рекордом: он почти вдвое превосходит объем данных, передаваемый за 1 секунду всей глобальной сетью (порядка 1 петабайта).

Задействованный в эксперименте чип использовал лазер для создания оптической частотной гребенки – набора синхронно колеблющихся оптических линий, каждая из которых служит для передачи данных. В результате была достигнута скорость, для которой в нормальных условиях потребовалось бы около 1000 лазеров.

Пока разработка находится в экспериментальной стадии и ее коммерциализация может занять годы. Однако результат выглядит чрезвычайно перспективным. Технология потенциально позволит существенно повысить скорость передачи данных и компьютерных вычислений. Не менее важно и то, что метод скандинавских исследователей предполагает заметное сокращение энергозатрат на передачу данных. Это особенно актуально, если учесть, что уже сегодня Интернет потребляет примерно 10% всей вырабатываемой в мире электроэнергии.

Источник:
https://www.washingtonpost.com/technology/2022/10/27/laser-powered-chip-internet-data-transfer/

Можно ли «отрезать» Европу от мировых линий связи?

Недавние аварии на газопроводе «Северный поток», признанные экспертами диверсиями, породили немало разговоров о том, что такие же диверсии могут быть совершены и на проложенных по океанскому дну оптоволоконных кабелях, оставив Европу без интернет-соединения с остальным миром. Этой теме посвятил свой комментарий Алан Молдин (Alan Mauldin), директор исследовательских проектов TeleGeography. Он констатирует, что подводные кабели действительно играют ключевую роль в телекоммуникациях: объем проходящих по ним данных просто несопоставим с пропускной способностью наземных и спутниковых линий связи.

Также Молдин признает, что проложенные по океанскому дну кабели достаточно уязвимы: даже без всяких диверсий в мире повреждаются в среднем 2-4 подводных кабеля в неделю. Но есть и хорошие новости. Прежде всего, индустрия знает об уязвимости, поэтому кабели прокладываются в наиболее защищенных от повреждений местах, а в крупных портах по всему миру ежедневно дежурят десятки специальных судов, готовых в любой момент отправиться к месту аварии для ее ликвидации.

Кроме того, Европу связывает с остальным миром весьма значительное число кабелей. Львиная доля трафика приходится на Северную Америку: в 2021 году 75% всей пропускной способности межрегиональных европейских линий связи занимал обмен данными с США и Канадой. Соответственно, и число трансатлантических кабелей достаточно велико: в данный момент их насчитывается 17, пропускная способность новейшего их них оценивается в 352 Тб/с.

Еще более двух десятков кабельных линий связывают Европу с Северной и Западной Африкой и Южной Америкой, кроме того, в ближайшие годы в эксплуатацию планируется ввести еще несколько новых кабельных линий. При этом сама Европа играет роль телекоммуникационного хаба для других регионов: согласно статистике прошлого года, на Европу было завязано около 97% всей пропускной способности межрегиональных сетей Африканского континента, а для Ближнего Востока эта доля составляет порядка 90%. Таким образом, заключает Алан Молдин, гипотетическое отключение Европы от мировых коммуникаций ощутимо ударит не только по самой Европе, но и по Африке и Ближнему Востоку. Однако само такое отключение представляется весьма трудно осуществимой задачей.

Источник:
https://blog.telegeography.com/cutting-off-europe-a-look-at-how-the-continent-connects-to-the-world

Организация Web3 Domain Alliance попытается установить «правила игры» для блокчейн-доменов

Компания Unstoppable Domains при поддержке нескольких более мелких игроков рынка объявила о создании организации Web3 Domain Alliance. Инициаторы проекта ставят перед собой две основные цели: предотвращение конфликтов имен в блокчейн доменных зонах и выработка механизмов защиты авторских прав в таких доменах. Обе задачи настолько же важны, насколько и труднодостижимы, отмечает ресурс Domain Name Wire, сообщая эту новость.

В настоящее время никаких механизмов регулирования альтернативных доменных зон просто не существует. Компания Unstoppable Domains ратует за то, чтобы структура, первой выведшая на рынок тот или иной блокчейн-домен, получала эксклюзивные права на него. Демонстрируя приверженность этому принципу, компания уже подала в суд на компанию Handshake, запустившую свой блокчейн-домен .wallet – позже, чем это сделала сама Unstoppable Domains. Одновременно она отказалась от домена .coin, узнав, что ранее он уже был выведен на рынок другой компанией. Также Unstoppable Domains пыталась добиться от властей США права регистрировать блокчейн-домены как торговые марки. Успеха, впрочем, это не принесло, по-

скольку в Соединенных Штатах даже традиционные общие домены верхнего уровня не рассматриваются как торговые марки.

Заявленным целям Web3 Domain Alliance препятствует прежде всего сама природа блокчейн-доменов как децентрализованных и часто анонимных. Многие из них управляются множеством различных структур и частных лиц, не всегда известных. По этой причине достичь консенсуса в вопросах управления и соблюдения правил – уже весьма сложное дело. Кроме того, каждое доменное имя в блокчейн-доменах является собственностью владельца, что делает исключительно сложным и контроль за соблюдением авторских прав. Однако решать эту проблему необходимо, поскольку правообладатели являются одними из самых влиятельных игроков на доменном рынке и без их благосклонности блокчейн-домены вряд ли могут рассчитывать на широкое признание.

В каком-то смысле формирование Web3 Domain Alliance можно рассматривать как попытку создания аналога корпорации ICANN для альтернативных доменных зон. Насколько успешной окажется эта попытка, покажет время.

Источник:
https://domainnamewire.com/2022/11/03/web3-domain-alliance-launches-to-try-to-bring-order-to-blockchain-domains/

Контент- и сервис-провайдеры стимулируют рост пропускной способности

Запрос на пропускную способность глобальных сетей растет стремительными темпами. Об этом свидетельствуют данные сервиса изучения глобальной пропускной способности TeleGeography. Так, только за период с 2019 по 2021 год международная пропускная способность сетей удвоилась, достигнув 2,900 Тб/с. При этом существенно изменилась структура рынка. Если ранее основной запрос исходил от операторов связи, то в последние годы безусловными лидерами стали несколько крупнейших контент- и сервис-провайдеров. Конкретно речь идет о таких компаниях, как Google, Meta (признана в России экстремистской организацией), Amazon и Microsoft. В 2021 году на их долю пришлось 69% всей задействованной международной пропускной способности сетей.

Интересно отметить, что запрос контент- и сервис-провайдеров в значительной степени зависит от географии. В том же 2021 году на их долю пришлось 92% всей использованной пропускной способности трансатлантических линий связи, соединяющих Европу и Северную Америку. Тогда как для линий между Европой и Юго-Восточной Азией эта доля составила лишь 21%. Так или иначе, во всех регионах планеты запрос контент- и сервис-провайдеров на пропускную способность сетей рос в период с 2017 по 2021 год совокупными темпами не ниже 51%. Для всех остальных участников рынка, включая и операторов связи, этот темп не превышал 45%.

Источник:
https://blog.telegeography.com/content-providers-binge-on-global-bandwidth

Красный Крест призывает создать цифровой эквивалент своих символов для кибервойн

Международный комитет Красного Креста выступил с инициативой создания цифровых аналогов своих символов – Красного Креста и Красного Полумесяца. Эти цифровые эмблемы должны служить для маркировки медицинских и гуманитарных цифровых ресурсов, защищая их от атак в ходе возможной кибервойны. «Более 150 лет защитные эмблемы, подобные Красному Кресту, служат, чтобы донести простое сообщение: люди, объекты и строения, несущие на себе эти символы, подлежат защите в ситуации вооруженных конфликтов. Обязанность конфликтующих сторон уважать и защищать медицинские и гуманитарные миссии в той же мере распространяется и на онлайн-пространство», - сказано в заявлении организации.

В настоящее время рассматриваются три возможных варианта создания таких символов. Первый предполагает использование системы DNS – например, путем выделения специального общего домена верхнего уровня, доступного лишь для медицинских учреждений и гуманитарных организаций. В этом случае любому человеку должно быть достаточно одного взгляда на доменное имя, чтобы понять, что речь идет об организации, которая подлежит защите.

Второй вариант подразумевает создание «символов» на базе IP-адресов. Это может быть особая последовательность цифр в IP-адресе, которая будет указывать системам на защищенные от посягательств цифровые ресурсы и их сообщения. Наконец, третий путь – разработка аутентифицирующей цифровой эмблемы (Authenticated Digital Emblem – ADEM). В данном случае речь о выработке цепочки цифровых сертификатов, которые будут сигнализировать о необходимости защиты.

Красный Крест совместно с несколькими исследовательскими центрами уже начал работу над выработкой оптимального решения. Сроки создания цифровой эмблемы не называются, но генеральный директор Международного комитета Красного Креста Роберт Мардини (Robert Mardini) уверен, что это задача, не терпящая отлагательств, поскольку наступательные кибероперации уже стали полноправной частью тактики современных войн.

Источник:
https://www.theregister.com/2022/11/07/red_cross_digital_emblem/

ТЦИ запустил Центр сертификации, выпускающий TLS-сертификаты

В июле 2022 года Технический центр Интернет осуществил запуск Центра сертификации, предоставляющего услуги по выпуску TLS-сертификатов для веб-ресурсов. Это один из первых подобных сервисов в России.

Главной его особенностью является то, что он поддерживает сертификаты как с распространённой криптосистемой ECDSA, так и с российской криптосистемой семейства ГОСТ 34.10. Помимо этого, многие процессы в Центре сертификации ТЦИ автоматизированы, что позволяет сократить

время выпуска сертификата до нескольких минут. Выпуск сертификатов осуществляется через личный кабинет, в котором также можно отслеживать выполнение сформированных заказов и срок действия уже выпущенных сертификатов.

В октябре в Центре сертификации ТЦИ была реализована поддержка логов Certificate Transparency «Яндекса» и VK. Теперь TLS-сертификаты, выпущенные Центром сертификации ТЦИ, содержат в себе криптографические метки, подтверждающие включение сведений о сертификате в лог.

Также в октябре была добавлена возможность выпуска сертификатов для электронной почты (S/MIME). Доступен выпуск сертификатов сроком на 90 и 365 дней. Получить S/MIME-сертификат можно в личном кабинете Центра сертификации, его выпуск займет всего несколько минут.

Источник:
https://tcinet.ru/press-centre/news/

Новости доменной индустрии

12 декабря 2022 года вступает в силу новая редакция Правил регистрации доменных имен в доменах .ru и .рф.

Внесение изменений в Правила было инициировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в целях пресечения неправомерного использования персональных данных третьих лиц при регистрации доменных имен.

Изменения касаются пункта 5.5 Правил, регулирующего прекращение делегирования доменных имен регистратором. Теперь делегирование домена может быть прекращено регистратором, в том числе, на основании мотивированного требования руководителя (заместителя руководителя или иного уполномоченного должностного лица) Роскомнадзора в случае регистрации доменного имени с использованием персональных данных третьих лиц без их согласия или если данный интернет-ресурс содержит информацию, доступ к которой должен быть ограничен на территории Российской Федерации в соответствии с положениями федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Источник:
https://cctld.ru/media/news/kc/33385/

Регистратура Identity Digital начала публиковать отчеты о противоправном использовании доменов в своих доменных зонах

Компания Identity Digital (ранее Donuts) объявила о том, что будет ежеквартально публиковать отчеты о полученных жалобах на противоправную активность доменных имен в доменных зонах под ее управлением. Первый отчет уже опубликован и подводит итоги второго квартала нынешнего года. Согласно его данным, за это время регистратура получила 3007 сообщений о различных видах противоправного использования системы DNS. Сообщения касались в общей сложности 3816 уникальных доменных имен, что составляет лишь 0,024% от всех доменных имен, находящихся под управлением компании.

Ресурс Domain Incite, сообщая эту новость, обращает внимание на то, что львиную долю всех жалоб – почти 93% – составили жалобы на фишинговую активность. А вот число случаев интеллектуального пиратства и нарушения авторских прав, вопреки ожиданиям, оказалось крайне низким. Так, по запросам Американской ассоциации кинопроизводителей за минувшие три месяца были заблокированы лишь шесть доменных имен.

Отметим, что Координационный центр доменов .RU/.РФ публикует такие отчеты ежемесячно: это результат взаимодействия аккредитованных регистраторов доменных имен в доменах .ru и .рф с компетентными организациями – компаниями, которые предоставляют Координационному центру и аккредитованным регистраторам информацию о ресурсах с противоправным контентом, о случаях фишинга, распространения вредоносных программ и других нарушений с использованием доменных имен в доменах .ru и .рф. Если суммировать данные за третий квартал 2022 года, то результаты будут практически аналогичны полученным регистратурой Identity Digital: из 4234 обращений, полученных за этот период российским регистраторами, 4069 или 96% составили жалобы на фишинг. Все отчеты и другая информация, касающаяся безопасности российских доменных зон .ru и .рф, публикуются на сайте доменный-патруль.рф.

Кроме того, на сайте проекта «Нетоскоп» (нетоскоп.рф) ежеквартально публикуются отчеты об обнаруженных участниками проекта вредоносных ресурсах в сети Интернет. Так, за третий квартал 2022 года в базу данных проекта было добавлено 5590 новых доменов, 5318 которых относятся к категории «фишинг».

Источник:
https://domainincite.com/28319-identity-digital-publishes-treasure-trove-of-abuse-data

Корпорация ICANN официально утвердила Политику по выводу национальных доменов верхнего уровня из эксплуатации

Правление корпорации ICANN утвердило порядок вывода национальных доменов верхнего уровня из эксплуатации, разработанный и предложенный организацией поддержки национальных доменов ccNSO. Официальное решение было принято на заседании правления в Куала-Лумпуре, состоявшемся в последний день работы конференции ICANN 75, 22 сентября, сообщает ресурс Domain Incite.

Политика предусматривает, что корпорация ICANN и регистратура национального домена согласовывают план удаления. Это происходит в случае, если двухбуквенный код государства или территории удаляется из реестров Международной организации по стандартизации (ISO), что может случиться, например, если государство, которому был делегирован домен, прекращает свое существование вследствие распада либо переименования. Предполагается, что домен подлежит удалению из корневой зоны через пять лет после того, как код государства удален из реестров ISO. Однако этот срок может быть продлен по запросу регистратуры и с согласия ICANN.

Источник:
https://domainincite.com/28297-icann-approves-cctld-killer-policy

Об особенностях внедрения поддержки почтовой адресации на русском языке рассказали на конференции Saint HighLoad++ 2022

Консультант Координационного центра доменов .RU/.РФ по инфраструктуре Вадим Михайлов выступил на конференции разработчиков высоконагруженных систем Saint HighLoad++ 2022, которая прошла 22-23 сентября в Санкт-Петербурге. В докладе «Глобальный переход на Unicode: как обеспечить готовность почтовых систем к адресации на русском языке» он рассказал об истории интернационализации интернет-идентификаторов, текущей работе экспертных сообществ в ракурсе разработанных ими отраслевых стандартов интернационализации интернет-идентификаторов, а также о практических особенностях внедрения поддержки интернационализированных доменных имен и адресов электронной почты.

Он отметил, что глобальная интернационализация Интернета, вызванная увеличением числа интернет-пользователей из разных стран, привела к появлению большого числа многоязычных онлайн-платформ, сервисов и других программных решений. Одним из поворотных событий в системе доменной адресации стало появление интернационализированных доменных имен (IDN), состоящих из non-ASCII символов, а за ними и адресов электронной почты с использованием таких доменов (EAI). «Развитие IDN и EAI продолжается, и возрастает необходимость в реализации правильной работы с такими идентификаторами во всех интернет-ориентированных системах, приложениях и устройствах. В связи с этим в своем докладе я рассказал о последних достижениях в этом вопросе и о том, как не оказаться за бортом с устаревшими подходами при работе с новыми реалиями многоязычной экосистемы глобальной сети», – пояснил Вадим Михайлов.

Источник:
https://cctld.ru/media/news/kc/32859/

Объявлено о создании единого сервиса защиты торговых марок в доменных зонах

На крупнейшей конференции доменного бизнеса NamesCon, которая прошла в конце августа – начале сентября в городе Остин, штат Техас (США), объявлено о создании сервиса NameBlock AS. Он призван помочь правообладателям защитить наименования своих торговых марок в доменном пространстве. Это весьма серьезная проблема, поскольку случаи киберсквоттинга и мошенничества с использованием доменов, имена которых чрезвычайно сходны или совпадают с наименованиями известных брендов, к сожалению, совсем не редкость.

Некоторые регистратуры предлагают правообладателям услуги блокировки имен, совпадающих с наименованиями брендов в доменных зонах, которыми управляют. Но этот сервис есть не у всех регистратур, а число общих доменов верхнего уровня давно уже превышает тысячу, что делает задачу защиты наименований торговых марок в доменном пространстве весьма непростой. Облегчить ее и призван сервис NameBlock AS. Он позиционируется как своего рода «маркетплейс» для блокировки наименований брендов. Сервис предлагает регистратурам возможность создания собственных механизмов блокировки, а правообладателям – своего рода «услугу одного окна» для защиты своих брендов сразу во множестве доменных зон.

Разумеется, успех проекта будет прямо зависеть от того, сколько регистратур сочтут нужным к нему присоединиться. Но, как сообщает ресурс Domain Name Wire, за созданием сервиса стоит Рольф Ларсен (Rolf Larsen) – специалист с огромным опытом работы в доменном бизнесе и отличной репутацией. Ранее он был в числе руководителей регистратуры CloudNames, управлявшей новым общим доменом верхнего уровня .global. Также Ларсен создал сервис защиты брендов IQ Global. Таким образом, он обладает и необходимым опытом, и связями в доменном бизнесе, что позволяет экспертам оценивать перспективы NameBlock AS весьма оптимистично.

Источник:
https://domainnamewire.com/2022/08/31/nameblock-launches-to-make-domain-blocking-easier/