№24
Апрель 2026

indata
ФОНД РАЗВИТИЯ СЕТЕВЫХ ТЕХНОЛОГИЙ «ИНДАТА»

Интернет изнутри

ИНТЕРНЕТ И ВРЕМЯ

В поисках потерянной микросекунды: как Интернет договаривается о времени

Временная синхронизация в современных распределённых телекоммуникационных системах играет критическую роль

с. 6

Время и протокол сетевого времени

Эволюция измерения времени – от астрономических наблюдений и механических часов до современных атомных стандартов

с. 14

Альтернативные способы частотно-временного обеспечения

Все крупные страны ведут разработку альтернативных способов распределения эталонных сигналов времени и частоты, поскольку отказ глобальной навигационной спутниковой системы нарушит функционирование критически важной инфраструктуры

с. 36

Роль времени в спутниковых сетях Интернета

Спутниковые интернет-сети становятся важной и неотъемлемой частью новой гибридной архитектуры Интернета, рождающейся буквально на наших глазах.

с. 42

«У меня есть часы, но нет времени...»

Что такое проблема 2038 года?

с. 52

Нормативная определённость измеримости времени

Одним из самых устойчивых стремлений человечества является измерение такой универсальной константы как время

с. 82

Содержание:

Сетевое издание
Журнал **«Интернет изнутри»**
info@internetinside.ru

Выпуск №24,
дата выхода:
Апрель 2026 г.

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Регистрационный номер:
ЭЛ № ФС 77 – 85232 от 25.04.2023 ISSN: 2949-1967

Все статьи размещаются и индексируются в НЭБ «e-Library»

Издатель: **Фонд развития сетевых технологий «ИнДата»**

Главный редактор:
Алексей Платонов

Выпускающий редактор:
Ирина Пыжова

Редакционная коллегия:
Елена Воронина
Марат Биктимиров
Алексей Платонов

Продакшн:
Алексей Гончаров

Дизайн и вёрстка:
Антон Иванов

Корректор:
Наталья Рябова

Обложка разработана с использованием ресурсов сайта Freepik.com

Часами измеряется время...

Дорогой читатель,

Время — одна из тех невидимых основ, на которых держится Интернет. Оно определяет порядок событий, синхронизирует процессы и обеспечивает согласованность распределённых систем, разбросанных по всему миру. Мы редко задумываемся о том, насколько хрупка и одновременно критична эта основа: от корректной работы протоколов времени зависят безопасность соединений, устойчивость сервисов и доверие к цифровой среде в целом.

В этом номере мы предлагаем взглянуть на Интернет через призму времени как технической категории и как источника рисков. Проблемы синхронизации, уязвимости протоколов, такие как накопленные эффекты переполнения счётчиков или атаки на инфраструктуру времени, всё чаще выходят за рамки узкоспециализированных обсуждений и становятся фактором, способным повлиять на бизнес и общество. В условиях растущей зависимости от распределённых систем даже небольшие сбои во времени могут приводить к масштабным последствиям.

Мы надеемся, что материалы этого выпуска помогут читателям по-новому оценить значение времени в Интернете — не только как абстрактного параметра, но как важного элемента устойчивости и безопасности цифрового мира.

Открывает журнал статья Александра Ильина «В поисках потерянной микросекунды: как Интернет договаривается о времени». В ней подробно рассмотрена система синхронизации времени в Интернете, включая основные протоколы, инструменты сетевых инженеров и специфику внедрения в сетях. Статья наглядно показывает, к чему могут привести ошибки этой системы, и предлагает практические рекомендации по построению отказоустойчивой иерархии серверов времени.

За ней следует ряд интересных статей, рассматривающих различные аспекты времени и его синхронизации в разных системах – от национальной инфраструктуры синхронизации времени до синхронизации в беспроводных сенсорных сетях. Особое внимание уделено подробному рассмотрению различных протоколов, обеспечивающих временную синхронизацию, и областей их применения.

Однако забираясь в дебри протоколов и технологий, нельзя забывать, что время пронизывает всё наше существование и важно не только для компьютерных систем, но и для специалистов, которые их разрабатывают и обслуживают. Об этом напоминает нам Алевтина Мокиевская в своей статье о роли циркадных ритмов как ключевого механизма синхронизации функций организма и клинических последствиях их нерегулярности, характерной для IT-специалистов.

Конечно, мы продолжаем поддерживать наши традиционные разделы. В разделе «Образование и Наука» мы познакомим вас с системой мониторинга сетевых соединений протокола потоковой передачи аудио и видео. В разделе «Технология и Право» Мадина Касенова рассказывает о нормативно-правовых требованиях синхронизации времени, что ещё раз подчёркивает критическую важность времени в цифровом сообществе. А в «Новостях» мы познакомим вас с интересными фактами об Интернете и доменной индустрии.

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**.

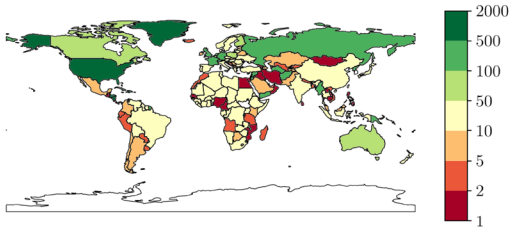
Редакция журнала

Интернет в цифрах

Распределение по странам автономных систем (AS) – поставщиков точного времени из NTP Pool

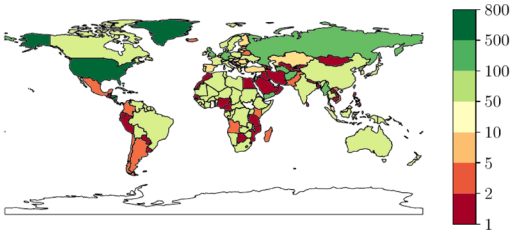
В составе NTP Pool более 4700 серверов, доступных пользователям из разных стран (экономик) мира. Но их распределение оказывается сильно неравномерным и, соответственно, может считаться несправедливым по отношению к пользователям.

Количество NTP-серверов, доступных пользователям в разных странах (экономиках) мира



Наиболее острая проблема состоит в том, что пользователи из 27 стран, в которых проживает 767 миллионов человек и 465 миллионов интернет-пользователей, обслуживаются всего одной автономной системой (AS) в качестве поставщика времени при использовании NTP Pool, даже несмотря на то, что в пуле указано более 4700 серверов. Эти страны выделены на рисунке красным цветом.

Количество автономных систем (поставщиков точного времени), обслуживающих разные страны (экономики) мира

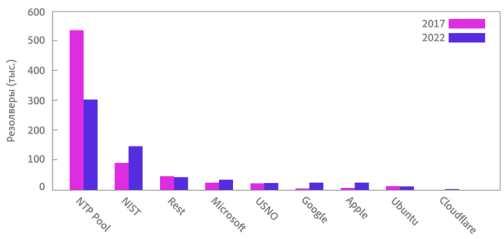


Источник: NTP Pool: The Internet timekeeper https://blog.apnic.net/2024/03/15/ntp-pool-the-internet-timekeeper/

Наиболее популярные в Интернете службы точного времени

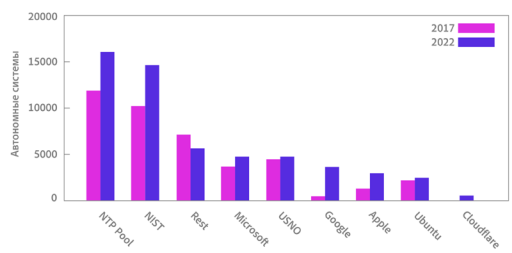
Анализ количества IP-адресов (DNS-резолверов), отправлявших запросы для каждого из наиболее часто используемых сервисов времени к корневым DNS-серверам, показал, что NTP Pool является самым популярным сервисом времени с большим отрывом — он популярнее, чем NIST и крупные облачные и контент-провайдеры, как в данных за 2017 год, так и за 2022 год.

Количество резолверов для каждого сервера времени в наборах данных DITL Root DNS



Анализ количества автономных систем (AS), отправлявших запросы для каждого из наиболее часто используемых сервисов времени к корневым DNS-серверам за 2017 и 2022 годы, подтвердил, что популярность NTP Pool наблюдается не только среди отдельных DNS-резолверов, но и в более широком масштабе — на уровне сетевых операторов и интернет-провайдеров.

Количество автономных систем (AS) для каждого сервера времени в наборах данных DITL Root DNS

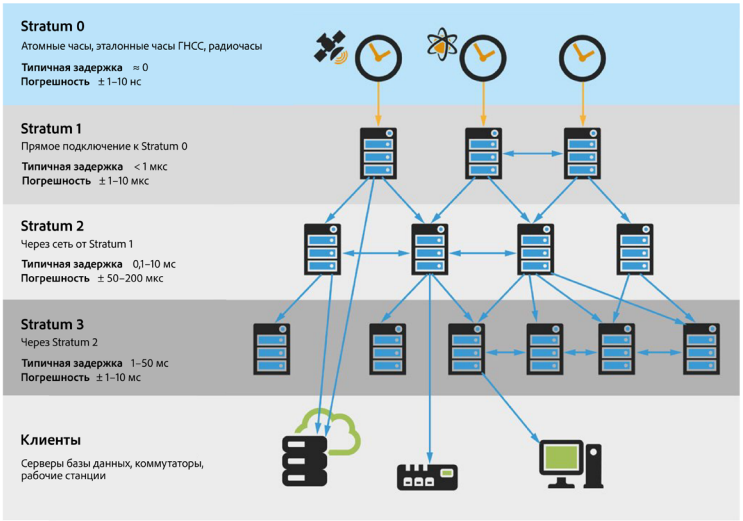


Источник: NTP Pool: The Internet timekeeper https://blog.apnic.net/2024/03/15/ntp-pool-the-internet-timekeeper/

Иерархия временной синхронизации NTP

Точное время в Интернете поддерживается благодаря специальным протоколам, таким как NTP (Network Time Protocol), и работе серверов точного времени. NTP работает по иерархической структуре, передавая время от авторитетных источников и спутников через различные слои серверов точного времени (Stratum) к конечным пользователям.

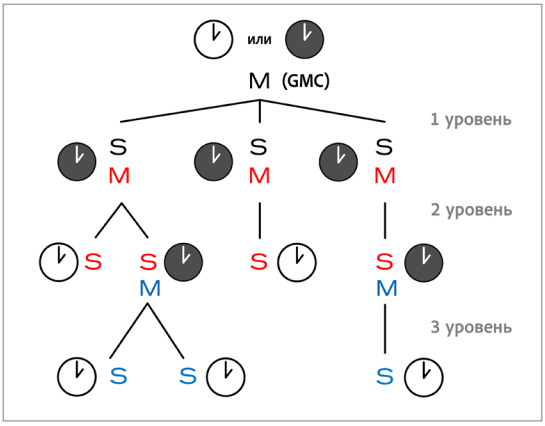
Удалённость Stratum от авторитетного источника времени позволяет определять относительную точность в иерархии источников времени в сети. Накапливающиеся задержки, возникающие при синхронизации устройств с серверами точного времени от Stratum к Stratum, снижают точность времени. Поэтому, чем меньше номер Stratum, тем точнее источник времени.



Источник: NTP TIME, https://www.ntp-zeit.de/index-en.htm?utm_source=chatgpt.com

Иерархия временной синхронизации PTP

PTP (протокол точного времени) обеспечивает высокоточную синхронизацию за счёт использования аппаратных меток времени и точных расчётов часов. Это делает его подходящим для приложений, критичных ко времени, где требуется точность на уровне миллисекунд. PTP работает по принципу синхронизации часов в сети путём обмена пакетами с метками времени. Он использует архитектуру «главный-подчинённый», где одно устройство действует как главные часы, а другие синхронизируют с ним своё время. Преимуществом PTP является его способность учитывать переменные задержки в сети, что обеспечивает точную синхронизацию даже в динамических средах.



Обычные часы (Ordinary Clock) - устройство с одним портом, которое может быть ведущими часами или ведомыми часами

Граничные часы (Boundary Clock) - устройство с несколькими портами, которое может быть ведущими часами или ведомыми часами, т.е. эти часы могут синхронизироваться от вышестоящих ведущих часов и синхронизировать нижестоящие ведомые часы

M Ведущие часы (Master-State) - являются источником точного времени, по которому синхронизируются другие часы

S Ведомые часы (Slave-State) - конечное устройство, которое синхронизируется от ведущих часов

GMC Гроссмейстерские часы (Grandmaster clock) - основной источник точного времени. Часто оснащаются интерфейсом для подключения GPS

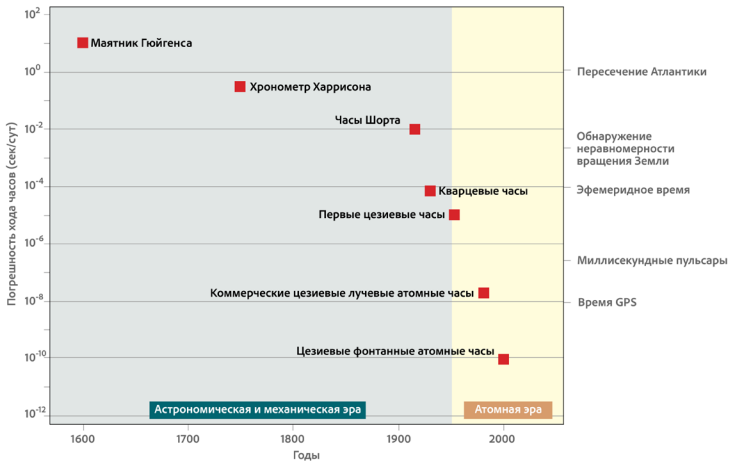
Источник: TFR: A Novel Approach for Clock Synchronization Fault Recovery in Precision Time Protocol (PTP) Networks DOI:10.3390/app8010021

Интернет в цифрах

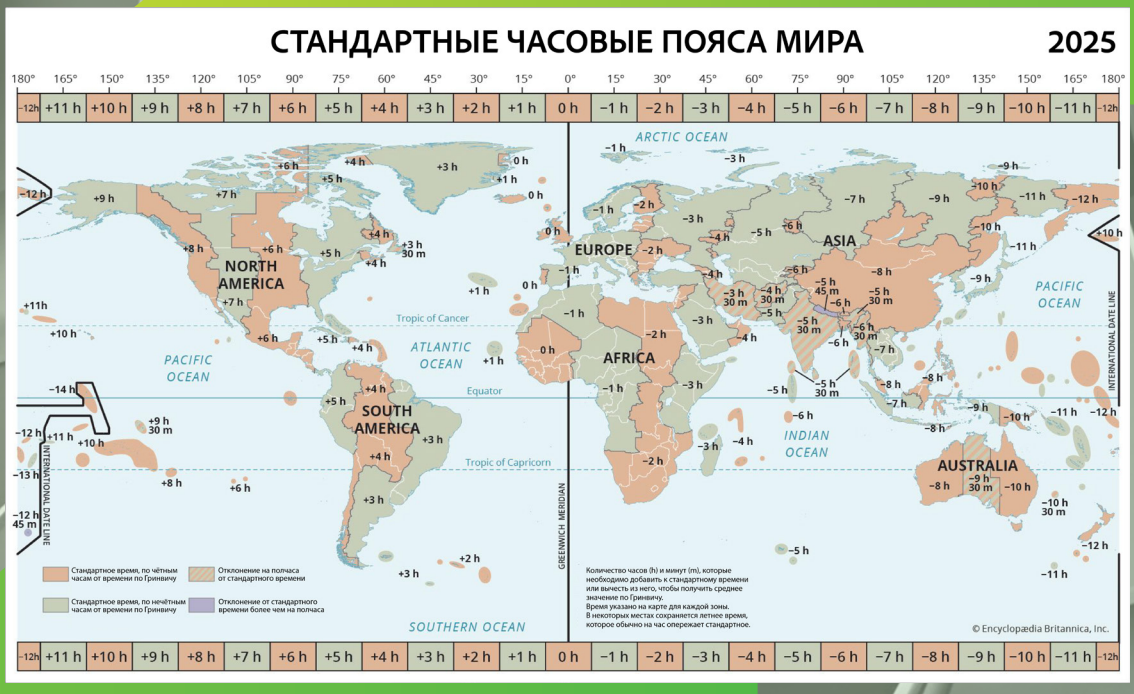
Основные вехи в усовершенствовании часов за последние 400 лет

За 50 лет развития цезиевые атомные часы достигли относительной погрешности менее одной квадриллионной (1×10^{-15}). Такой точности ещё не удавалось добиться ни в одной другой области современной метрологии. А в последние несколько лет особенно быстро развиваются оптические атомные часы, которые смогут обеспечить ещё более высокую точность измерения времени.

В 1750 году для безопасного пересечения Атлантики потребовались часы с погрешностью около 1 секунды в сутки. Хронометр Харрисона стал настоящим прорывом, позволившим достичь такой точности и сделать навигацию значительно надёжнее. Часы Шорта до сих пор считаются самыми точными среди всех механических часов. Эфемеридное время, рассчитываемое на основе астрономических наблюдений, обеспечивало точность примерно 0,1 миллисекунды в сутки. Часы, основанные на наблюдении пульсаров, могут иметь погрешность менее 1 миллисекунды в сутки. Время GPS показывает уровень точности с погрешностью менее 30 наносекунд. В гражданских приёмниках обычно используется время с погрешностью в несколько микросекунд или миллисекунд в зависимости от качества оборудования.



Источник: Standards of Time and Frequency at the Outset of the 21st Century, https://tf.nist.gov/general/pdf/1961.pdf



MSK-IX

Платформа цифровой устойчивости

Сервисы MSK-IX для операторов, медиа, облаков и бизнеса.
Нейтральная инфраструктура. Национальный масштаб.

Internet Exchange

Прямая связность.
Минимальная задержка.
Снижение затрат
на транзит.

Instanet

Защищённый
и быстрый доступ
к облакам и сервисам.
Стабильность
при пиковых нагрузках.

Anycast DNS

Устойчивость сервисов.
Защита от атак.
Соответствие требованиям
регуляторов.

- 1150+ участников экосистемы
- DNS / NTP
- Единый SLA: 99,99%
- Защищённые пиринговые группы

Узнайте, как MSK-IX усиливает устойчивость вашей сети

В поисках потерянной микросекунды: как Интернет договаривается о времени

Александр Ильин

Аннотация

Статья посвящена критической роли временной синхронизации в современных распределённых телекоммуникационных системах. Рассматриваются технические различия между протоколами NTP и PTP, их точность, инструменты сетевых инженеров, специфика внедрения в операторских и корпоративных сетях. Особое внимание уделено практическим аспектам работы сетевого инженера и типовым проблемам реализации. Материал содержит рекомендации по построению отказоустойчивой иерархии серверов времени.

.

Ключевые слова:

синхронизация времени, протоколы PTP и NTP, иерархия Stratum, сетевые задержки и асимметрия трафика, Software vs Hardware Timestamping, мониторинг временных сдвигов, инфраструктура точного времени, отказоустойчивость пулов времени

«Тот, кто осознаёт ценность времени, владеет миром» – Леонардо да Винчи

Современный мир, технологии, которые нас окружают, смартфоны, ноутбуки, планшеты, устройства умного дома и множество всевозможных систем не могут обеспечить полноту и точность данных без точного времени. Однако эта задача, обычно остающаяся в тени, зачастую имеет свою специфику и решается не так просто. Во многих устройствах (например, в часах) используются кварцевые чипы, которые могут «убегать» на несколько секунд в день. Чтобы все системы работали как единое целое, им необходимо постоянно сверять свои часы с общим эталоном.

Всё начинается с физики. Эталонное время почти 60 лет измеряют по цезиевым атомным часам. Они основаны на квантовых переходах атомов. В основе большинства таких часов заложены колебания атома цезия-133, и это с 1967 года используется для определения секунды. Однако в настоящее время существуют оптические атомные часы, которые в 100 раз точнее цезиевых.

Такие часы обеспечивают сверхвысокую точность (например, за 100 миллионов лет они «убегут» меньше, чем на одну секунду), но чтобы построить такие часы, требуются огромные и дорогие установки, поэтому, как правило, эти часы размещаются в научных центрах и лабораториях.

В Интернете многие технологии построены по иерархическому принципу. Это коснулось и базового протокола NTP (Network Time Protocol, RFC 5905), который обеспечивает передачу информации о времени. NTP позволяет скорректировать естественную погрешность кварцевых резонаторов в большинстве конечных устройств. Иерархические уровни NTP называют стратумами:

- уровень 0 (Stratum 0) – это, как правило, атомные часы или спутники с атомными часами. Они отсутствуют в Интернете;
- уровень 1 (Stratum 1) – серверы, обеспечивающие высокую доступность и зачастую спроектированные с учётом высокой нагрузки. Они получают время от нулевого уровня и раздают по сети время дальше. Это самые авторитетные источники времени в сети;
- уровень 2 и больше – обычные серверы компаний. Чем выше цифра уровня – тем дальше мы находимся от первоисточника, но для бытовых нужд такой точности более чем достаточно.

Stratum NTP – это не фиксированная настройка, а динамический показатель удалённости от атомных часов. Каждый сервер определяет свой уровень на основе простого правила: уровень выбранного им источника сигнала +1. У серверов, как правило, несколько источников сигнала с разными уровнями - и важно понимать, что уровень может расти, если один источник испортился или вообще исчез для данного сервера, что привело к использованию другого источника. Этот уровень позволяет конечным системам ориентироваться на точность получаемых часов при выборе сервера.

«Человек, имеющий одни часы, твёрдо знает, который час. Человек, имеющий несколько часов, ни в чём не уверен» – Закон Сегала

В Интернете существует огромное количество серверов времени, но зачастую не все из них работают идеально. Чтобы конечное устройство работало корректно, применяется алгоритмический отбор достоверных источников. Протокол NTP ведет себя как следователь – опрашивает сразу несколько источников, убирает те, что выдают явные ошибки или имеют большую задержку, и считает среднее арифметическое. Если какой-то из серверов внезапно начнет выдавать ошибочное время – его данные проигнорируют.

Зачастую при настройке устройств требуется указать часовой пояс (TimeZone). При этом все программы и серверы живут по единому стандарту UTC (Всемирное координированное время), а уже пользовательское устройство определяет, где вы находитесь, и в зависимости от места показывает вам эти часы с учётом TimeZone. Это позволяет избежать хаоса при обмене данными между устройствами на разных континентах.

Зачем в сети нужно точное время?

Давайте представим себе ситуацию, что на сервере популярного маркетплейса внезапно часы отстали на сутки. Для обывателя это превратится в настоящую проблему:

«Ваше интернет-соединение не защищено». Браузер заблокирует вход, так как SSL-сертификат имеет срок валидности. Может так случиться, что сертификат ещё не начал действовать или уже «протух».

«Несуществующие скидки». Маркетплейс может показать товары по акциям, которые уже закончились, и не показать те, которые начались.

«Платёж не прошёл». Банки могут отклонять транзакции, так как одноразовые пароли (OTP) привязаны к точному времени. Если время в системах не совпадает – код будет не валиден и платежи не пройдут. Это лишь малый пример того, что может произойти, если собьётся время на критичном ресурсе.

«Человек, который осмеливается потратить впустую час времени, ещё не осознал цену жизни» – Чарльз Дарвин

Точное время — это, по сути, возможность соединить всю инфраструктуру воедино. Сетевые устройства, использующие динамические протоколы маршрутизации, такие как BGP4, казалось бы, напрямую не используют точное время для выбора маршрутов, но для защиты от перехвата трафика BGP Hijacking всё чаще используется RPKI (Resource Public Key Infrastructure) – система цифровых сертификатов, подтверждающая право владельца автономной системы на анонсирование IP-адресов. Для проверки валидности маршрутов проверяется сертификат ROA (Route Origin Authorization), который имеет срок действия, и если время на системе некорректно, то маршрут может стать не валидным, и трафик через узел не пойдёт.

Современные серверные системы зачастую имеют распределённую инфраструктуру для повышения надёжности и резервируемости. Именно для них особый статус имеет точное время. Например, распределённые системы хранения данных не смогут собрать корректно работающий кластер без точных синхронизированных часов. В распределённых базах данных могут возникать проблемы конфликтов записи. Давайте рассмотрим ситуацию: пользователи в разных городах редактируют один и тот же документ. Пользователь в Москве внёс правку в 11:00:01, а пользователь во Владивостоке - в 11:00:03. Если сервер во Владивостоке спешит на 5 секунд, то он примет правку от пользователя со временем 10:59:58. При синхронизации баз данных с Москвой может оказаться, что система примет правку из Владивостока раньше, чем правку из Москвы - и правки пользователя во Владивостоке исчезнут, так как будут записаны поверх правки из Москвы.

Проблема со временем может затронуть и целостность кешей на серверах. Вот простой пример:

Вы сменили свой пароль, информация об этом поступила на главный сервер, однако вторичный сервер (кеш) проверяет и сравнивает время жизни (TTL) своей копии с текущим временем. Если часы отстают, то он будет считать, что старый пароль ещё свежий и годен, что не даст вам возможности зайти на эту систему.

В иерархической системе доменных имён DNS время играет роль срока годности. Это критично для работы DNSSEC (Domain Name System Security Extensions, RFC 9364) – набора расширений, которые защищают DNS от подмены данных.

Для подтверждения подлинности ответов в DNSSEC используются цифровые подписи RRSIG (Resource Recode Signature). Каждая такая подпись имеет фиксированные метки начала и окончания действия (Validity Period). Если системное время на сервере или клиенте выйдет за эти рамки, подпись будет признана невалидной, проверка безопасности будет провалена, а домен станет недоступным для пользователя.

Также сбои часов могут вызвать проблемы с интерпретацией TTL в DNS, что ведёт к преждевременному удалению записей из кеша или их некорректному обновлению. У каждой записи DNS есть свой TTL (время жизни записи, в течение которого она считается верной). Если вы переехали на новый сервер и обновили IP-адрес сайта, а на кеширующем сервере провайдера часы отстали, то он может продолжать отдавать старую запись, несмотря на то, что она должна была уже «протухнуть».

Часы крайне важны для своевременного и грамотного анализа событий в сети. Для правильной корреляции различных событий необходимо, чтобы время совпадало, иначе логи (сетевые журналы) будут показывать неправильный порядок событий, и их будет невозможно анализировать. Это же касается и событий систем мониторинга. Системы визуализации типа Grafana рисуют графики на основе ме-

ток времени. При рассинхронизации графики «уплывут», и данные наложатся друг на друга или возникнут временные промежутки. Ошибки во времени могут приводить к дырам в мониторингах уровня сервиса и проблемам с дальнейшим анализом. Для оперативного контроля состояния сети используется BMP (BGP Monitoring Protocol, RFC 7854) – протокол, который в реальном времени транслирует данные о состоянии BGP-маршрутов с роутеров на серверы мониторинга. Однако при его работе критически важна синхронизация: если BMP-события приходят с некорректными временными метками, системы автоматизации и управления могут ошибочно решить, что информация устарела, и проигнорировать важные обновления.

Когда на маршрутизаторах сбито время, анализ инцидентов (например, DDoS-атак) превращается в детектив, где все улики перепутаны, а свидетели указывают разное время и даты. В контексте анализа трафика (Netflow) это критичная проблема. Если на маршрутизаторе часы уходят вперёд, то Flow-коллектор получит данные об атаке, которая случилась в будущем. В итоге система мониторинга не сможет сопоставить этот всплеск трафика с реальным временем, и инженеры не смогут корректно проанализировать и составить корреляцию с событиями на других системах. Аналитики видят рваный график и не могут понять реальную мощность DDoS-атаки, так как данные могут размазаться по разным интервалам. Сбой часов может негативно повлиять и на работу BGP FlowSpec (BGP Flow Specification, RFC5575). Этот механизм позволяет динамически передавать на роутеры правила фильтрации трафика (по портам, протоколам или размерам пакетов), работая в связке с системами защиты от DDoS. Аномалия в статистике приводит к формированию FlowSpec-правил DDoS-защиты для маршрутизаторов, что позволяет оперативно блокировать вредоносный трафик на определённое время. Если часы на роутере и системе защиты не совпадают, то блокировка может закончиться раньше времени или затянуться на часы, блокируя легитимный трафик.

В системном администрировании часы тоже играют ключевую роль. Помимо корреляции с другими устройствами, часто запускаются различные события по Cron, что может приводить к непредсказуемым последствиям. Например, сервер собирает логи с устройств, и он запускает ротацию логов и удаление старых данных раньше положенного времени. В итоге ценная информация может быть утеряна. На ряде серверов к сбоям может приводить повышенная нагрузка на систему в те моменты времени, когда она не ожидается. Например, большинство системных архивных процессов проходит ночью, при малой нагрузке, а если время смещено на несколько часов, то эти события могут произойти в разгар рабочего дня и привести к существенным проблемам.

«Точность — вежливость королей» – Людовик XVIII

Мы уже разобрались, что время передаётся по иерархической модели (стратум), но кто именно владеет этими серверами и как конечное устройство находит путь к атомным часам?

Самый известный проект в этой области – NTP Pool Project (pool.ntp.org). Это система контроля, мониторинга, связи мирового кластера NTP-серверов в единый каталог, который поддерживается сообществом волонтёров по всему миру.

Как это работает: вместо того, чтобы миллиарды устройств обращались к одному конкретному серверу (который может и не справиться с нагрузкой), запрос отправляется на DNS-адрес вроде o.pool.ntp.org или ru.pool.ntp.org для устройств из РФ. Система сама выбирает серверы из пула и отдает их IP-адреса для доступа по протоколу NTP.

Этим пулом пользуются почти все дистрибутивы Unix, домашние роутеры, умные гаджеты, смартфоны. Это абсолютно бесплатно и доступно, но никто не даст 100% гарантии точности и корректности работы сервера. Справедливости ради отметим, что если сервер начинает отдавать некорректные данные, то через некоторое время pool.ntp.org это замечает и исключает его из выдаваемого списка.

Крупные компании не полагаются на публичные доступные серверы. Они, как правило, строят свои собственные системы точного времени. Основная цель обусловлена не только недоверием к публичным ресурсам, но и содержанием внутри своей инфраструктуры единого центра времени, который не создаст внутри проблем с синхронизацией данных. Схожая картина и у финансовых компаний, где зачастую требуется сверхвысокая точность часов с целью участия в биржевых сделках.

В последнее время с появлением облачных решений возникла новая модель - TaaS (Time as a Service). Пользователям в облаке зачастую не нужно ходить в Интернет за временем, если его можно раздать внутри прямо в облаке.

Если говорить о российском сегменте Интернета, то одним из часто используемых является MSK-IX NTP Server. Это не просто очередной сервер в сети, а распределённая инфраструктура по технологии Anycast для раздачи точного времени, результат работы многоуровневой иерархической системы технических средств. Ключевыми особенностями этого решения является резервируемость, синхронизация со спутниковыми группировками ГЛОНАСС и географическое распределение (Москва, Санкт-Петербург, Новосибирск, Екатеринбург). Это обеспечивает минимальные задержки для пользователей в разных частях страны, а также даёт возможность участникам MSK-IX получать данные сервера с минимальной сетевой задержкой. NTP-сервис в сети MSK-IX эксплуатируется уже более 15 лет. Многие тезисы этой статьи являются результатом этого опыта.

«Каждая секунда имеет бесконечную ценность» – Иоганн Вольфганг Гёте

В мире точных часов и синхронизации времени нет единого универсального решения. Выбор решения и протокола – это всегда баланс между точностью, сложностью внедрения и стоимостью оборудования.

Рассмотрим два ключевых протокола – NTP и SNTP. Хотя оба протокола используют один и тот же формат пакетов UDP и работают на 123 порту, между ними есть принципиальная разница в логике.

NTP (Network Time Protocol) – это полноценный аналитический протокол. Он опрашивает несколько серверов, анализирует сетевые задержки, отсеивает «лживые» источники и плавно подстраивает ход системных часов. NTP умеет компенсировать дрейф кварцевого резонатора конечного устройства, даже если связь временно пропала.

SNTP (Simple NTP) – это упрощённая версия для ленивых устройств (устройств Интернета вещей, дешёвых камер, микроконтроллеров). Он не делает сложных вычислений, а просто запрашивает время у одного сервера и выдаёт результат. Очевидный минус заключается в том, что если пакет задержится или сервер ошибётся, то SNTP примет некорректное время.

Очевидна область применения этих протоколов. Для серверов и критичных систем нужен полноценный NTP, а для бытовых устройств, Интернета вещей достаточно SNTP.

За счёт чего же обеспечивается точность часов при использовании NTP? Магия протокола заключается в том, что он не просто принимает на веру пришедшее время, а вычисляет, сколько секунд пакет проходил через Интернет. Для этого протокол использует математическую формулу:

Когда клиент (устройство) запрашивает время у сервера, фиксируются четыре временных метки:

T_1 – время на устройстве в момент отправки запроса;

T_2 – время сервера при получении запроса;

T_3 – время сервера в момент оправки ответа;

T_4 – время получения ответа клиентским устройством.

Далее клиент считает две величины: RTT и Offset по формулам:

$RTT = (T_4 - T_1) - (T_3 - T_2)$

Это время, которое пакет провёл в сети, исключая время, пока сервер готовил ответ.

$Offset = ((T_2 - T_1) + (T_3 - T_4))/2$

Это разница между часами клиента и часами сервера.

Учитывая, что задержки на сети могут варьироваться, применяется алгоритм Марзулло, благодаря которому делается серия запросов и выбираются те, где задержка была минимальной и самой стабильной. Дополнительно накапливается статистика – отбрасываются пакеты, которые слишком надолго задержались в пути, и строится средневзвешенное значение.

Когда точности в миллисекунды (как у NTP) становится мало, используется протокол PTPv2 (Precision Time Protocol, стандарт IEEE 1588). Этот протокол появился из мира промышленной автоматизации и систем телефонии. PTP использует аппаратные метки времени. Пакет помечается на аппаратном уровне прямо сетевым чипом устройства перед выходом в сеть. Ключевое отличие от NTP заключается в высокой точности протокола. Если NTP дает точность 1-50 мс, то PTP позволяет добиться наносекундной точности. Однако для PTP требуется специальное сетевое оборудование (коммутаторы и сетевые карты), которые умеют обрабатывать такие пакеты с приоритетом. Кроме оборудования необходимо ещё учитывать и профили PTP, которые применяются для различных отраслей и классов устройств – таких как энергетика, радиовещание, автоматизация, телекоммуникации. Одно из ключевых отличий в этих протоколах – специфика всех промежуточных устройств, а не только конечного оборудования. Для PTP необходима поддержка протокола всеми промежуточными устройствами, что делает этот протокол узкоспециализированным и не позволяет широко распространять по сети.

В PTP-протоколе используется сообщение Sync, которое, по сути, является сердцем прокола PTP. В отличие от NTP, этот протокол начинает работу с рассылкой сообщения Sync от Master-часов. Дочерние устройства получают пакет Sync, фиксируют время прихода и, сравнивая его с меткой внутри пакета, вычисляют задержку с точностью до наносекунд.

Разумный компромисс в современных реалиях: применение NTP везде, а PTP - там, где есть особые запросы. Этот гибридный подход позволяет закрыть основные требования по времени для большинства устройств Интернета и создать особые условия для проектов, которым требуется высокая точность – таким как финансовые биржи, энергетические подстанции, вышки сотовой связи 5G.

«Время — сотворённая вещь. Сказать: „У меня нет времени" — всё равно что сказать: „Я не хочу"» – китайский философ Лао-цзы

Выбор режима работы NTP – это не просто настройка конфигурационного файла, а проектирование надёжности сети. В зависимости от поставленной задачи инженер выбирает один из четырёх основных методов.

1. **Клиент-Сервер (Unicast)**

Самый распространённый и очевидный режим. Клиентское устройство инициирует запрос к конкретному IP-адресу сервера или пулу адресов сервера. Идеально подходит для связи через Интернет между разными сегментами сети. Плюсом здесь является максимальная точность, так как NTP вычисляет задержку индивидуально для конкретной пары клиент-сервер. Однако есть и минус – если у вас в сети 100 тысяч клиентов, то каждый будет отсылать запросы, создавая лишний трафик.

2. Симметричный активный/пассивный режим (Peering) (устаревший)

Этот режим ранее использовался для связи между серверами одного уровня (например, между Stratum 1). Ключевое отличие этого режима от других заключено в том, что серверы обмениваются данными о своём состоянии на одном уровне. Если один из серверов потеряет связь с атомными часами (спутником), он сможет брать время у соседа по пирингу. Плюсом здесь является высокая отказоустойчивость инфраструктуры. Однако в последние годы после появления атак типа NTP DDoS Amplification от этого режима было решено отказаться в пользу модели клиент-сервер, так как протокол NTP использует UDP, и злоумышленники могут подделать адреса пиров и вынудить сервер отправлять огромное количество пакетов жертве.

3. Broadcast/Multicast в локальных сегментах

Режим для экономных и ленивых администраторов. Сервер раз в несколько секунд сообщает в локальную сеть точное время, а клиенты просто слушают эфир и подстраивают часы по этим объявлениям. Плюсом тут является минимум трафика – одним пакетом можно обслужить сколь угодно много устройств в одном сетевом сегменте. Из минусов - низкая точность, так как нет возможности точно вычислить задержку передачи по сети, и поэтому погрешность чуть выше. Ну и ключевой недостаток – это вопрос информационной безопасности: можно поднять поддельный NTP-сервер, выдать с него некорректное время и сломать всю сеть.

4. Anycast NTP

Это современное решение, на базе которого построены современные публичные высоконагруженные NTP-серверы. Как и в типовом Anycast, настраивается несколько географически распределённых серверов (например, в Москве, Санкт-Петербурге, Екатеринбурге, Новосибирске) с единым публичным адресом. Далее протокол динамической маршрутизации направляет входящие пакеты от клиентов в сторону доступного сервера. Так работает и наш ntp.msk-ix.ru. Достоинство такой модели в том, что получается высокая отказоустойчивость и масштабирование сервиса. Помним, что серверы размещаются на точках обмена трафиком, и таким образом обеспечивается минимальная задержка для участников платформы обмена, что положительно сказывается на точности определения времени.

Протоколу NTP уже больше 40 лет, и конечно, за эти годы протокол претерпевал изменения. Протокол использует UDP, и поэтому он оказался уязвим для различного вида атак. В течение последних нескольких лет выходили расширения протокола с целью закрыть возможные уязвимости, но многие из них оказались сложны в настройке и не были приняты сообществом. Ключевыми в публичном пространстве остались две технологии: клиент-сервер и anycast.

Точность в NTP – это не только качество атомных часов, но и умение протокола выживать в условиях зашумлённой среды передачи данных.

В стандартной реализации NTP использует программные метки времени (software timestamping). Пакет, содержащий метку, проходит через драйверы сетевой карты, стоит в очереди прерываний процессора и только потом попадает к приложению NTP. Пока процессор занят другими задачами, проходит несколько микросекунд (возможно миллисекунд). Информации об этой задержке у NTP нет, и он считает, что пакет шёл дольше по сети, чем на самом деле. Из-за этих погрешностей внутри операционной системы NTP редко даёт точность выше 1-10 мс. Для анализа логов это вполне достаточно, но, например, для синхронизации электрооборудования этого может быть недостаточно.

Протокол NTP оптимистичен. Он считает, что пакет идёт до сервера столько же времени, сколько идёт обратно. Однако очень часто в сети бывает асимметричная маршрутизация, что может приводить к разному времени приёма-передачи пакетов. В этом случае входящий пакет приходит через одного провайдера, а ответ может идти по совершенно другому маршруту. Дополнительным фактором задержек могут служить перегрузки на каком-нибудь из элементов цепи передачи данных. В итоге NTP увидит, что RTT (Round Trip Time) вырос, поделит задержку пополам и неправильно вычислит смещение времени (offset). Например, путь для входящего пакета занял 10 мс, а обратный - 100 мс, NTP посчитает, что часы на сервере спешат на 45 мс. В итоге, корректировка времени будет с ошибкой. По сути, асимметричный роутинг – это один из главных врагов протокола.

Рассмотрим алгоритм фильтрации, или как NTP выявляет «лжецов»? В отличие от протокола PTP (IEEE 1588), который выбирает лучшего мастера (Best Master Clock Algorithm) и безоговорочно ему доверяет, NTP полагается на статистический анализ:

NTP собирает выборку измерений и отсеивает результаты с аномальной дисперсией.

Также применяется алгоритм пересечения (Intersection Algorithm). Если в конфигурации присутствуют несколько серверов и один, например, утверждает, что сейчас 12:00, а три других говорят – что 12:05, то NTP пометит первый сервер как falseticker (неточный сервер) и исключит его из расчёта, даже если его Stratum высокий. Это помогает NTP быть устойчивым к сбоям отдельных узлов, в то время как PTP более уязвим к ошибке одного выбранного мастера. Поэтому NTP оказывается гораздо более живучим в хаосе мирового Интернета.

Для сетевого инженера критически важно не только настроить синхронизацию времени, но и иметь инструменты для проверки точности и стабильности. Ошибки NTP часто бывают малозаметными: процесс запущен, но время постепенно деградирует из-за сетевых задержек или отказа тех или иных источников.

Для проверки применяются, как правило, утилиты командной строки Unix: ntpq, ntpdate. Это, по сути, базовый набор инструментов, доступный практически в любой Unix-системе.

Ntpq (NTP Query): ключевой инструмент мониторинга работающего процесса. Команда ntpq -p (peers) выводит табличку:

$ ntpq -p

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*ntp.ix.ru	.GLN.	1	u	14	64	17	1.303	+0.222	0.038
time.cloudflare	.INIT.	16	u	-	64	0	0.000	+0.000	0.000
+ntp2.vniiftri.r	.FTRI.	1	u	16	64	17	4.283	+0.503	0.166

Этот вывод – пример стабилизации системы после недавнего запуска. Для сетевого инженера тут есть несколько важных маркеров:

1. Состояние разогрева (reach 17). Значение reach 17 в восьмеричной системе соответствует 00010001. Это значит, что было получено два успешных ответа, но между ними был пропуск (запрос не ушёл или ответ потерялся). Система работает несколько минут. До полной достоверности (когда reach станет 377) алгоритм продолжает набирать статистику, чтобы отфильтровать сбойные серверы.

2. Идеальный jitter (0.038). У ntp.ix.ru jitter 0,038 (38 микросекунд) – это великолепный показатель для NTP, говорит о том, что канал до MSK-IX стабилен, нет очередей и заторов. Именно такой низкий jitter позволил выбрать ix.ru основным (*), несмотря на то, что reach ещё не полный.

3. Смещение (offset +0.222 vs +0.503). ntp.ix.ru считает, что наши часы отстают на 0,222 мс, в то время как ntp2.vniiftri.ru считает, что отстают сильнее – на 0,503 мс. Разница около 280 микросекунд. Для синхронизации через Интернет это ничтожно малая величина, которая подтверждает, что оба источника надёжны.

4. Проблема с Cloudflare (.INIT./Stratum 16). Сервер time.cloudflare находится в состоянии «INIT: Stratum 16» - по сути, недостижимость. Для NTP этот сервер не существует. Вероятные причины - в блокировке доступа к этому серверу.

В итоге система выбрала ntp.ix.ru в качестве мастера из-за кратчайшей задержки (1,3 мс) и идеальной стабильности сигнала. Сервер ВНИИФТРИ выступает в роли «запасного игрока» (знак «+»), готового подхватить синхронизацию в любой момент.

Кроме типового процесса ntpd возможно построить синхронизацию с помощью chronyc (Chrony). Chronyc лучше справляется с мониторингом в условиях нестабильных соединений, и с помощью ряда опций можно получать консолидированный отчёт о состоянии системы. Например, с помощью команды chronyc sources -v можно получить более детальное представление о погрешности (ошибки измерения):

$ chronyc sources -v

```
210 Number of sources = 3
.-- Source mode  '^' = server, '=' = peer, '#' = local clock.
.-- Source state '*' = current synced, '+' = combined, '-' = not combined,
'?' = unreachable, 'x' = time may be error, '~' = time too variable.
.- xxxx [ [delta] ] +/- [err]
```

Name/IP address	Stratum	Poll	Reach	LastRx	Last sample
^* ntp.ix.ru	1	6	17	14	+222us[+222us]+/-150us
^? time.cloudflare	16	6	0	-	+0ns[+0ns]+/-0ns
^+ ntp2.vniiftri.ru	1	6	17	16	+503us[+503us]+/-450us

Тут сразу видно статус Cloudflare (знак вопроса – говорит об отсутствии ответов от сервера), видно смещение в микросекундах (+222us) и доверительный интервал (+- 150us). По сути, киллер-фича Chrony, показывающая погрешность измерения, где видно, что ntp.ix.ru имеет малую погрешность и высокую достоверность, в отличие от ntp2.vniiftri.ru, что обусловлено сетевыми задержками. В квадратных скобках отражается отклонение от предыдущего измерения.

Кроме Ntpd и Chrony системные администраторы часто применяют NTPsec. По сути, это глубоко переработанная реализация классического Ntpd, из которого удалено огромное количество строк устаревшего кода и добавлен новый функционал. Ключевое преимущество NTPsec – поддержка стандарта NTS (Network Time Security, RFC 8915). Это достаточно современный протокол (2020 год), использует TLS для первоначального обмена ключами и эффективно противодействует спуфингу, атакам типа отказ в обслуживании через усиление (Amplification) и перехвату данных (MITM), хотя он всё ещё недостаточно широко распространён в массовых системах и сервисах. Сетевым инженерам важно учитывать, что для реализации NTS потребуется дополнительно разрешать трафик по TCP-порту 4460 (NTS Key Establishment) для аутентификации, кроме стандартного UDP 123 для NTP.

Кроме команд анализа состояния NTP-сервиса часто применяются команды для разовой синхронизации. Много лет во FreeBSD, например, использовалась команда ntpdate, которая и сейчас весьма популярна, однако в современных системах она считается устаревшей и заменяется на ntp -gq, но в скриптах эта команда по-прежнему ещё фигурирует.

Когда парк серверов исчисляется сотнями, то ручной проверки через CLI явно недостаточно, поэтому применяются комплексные решения, такие как Zabbix/Prometheus + Exporters. Данные из NTP-демонов собираются экспортёрами. Это позволяет строить графики смещения времени (offset) в динамике. Резкий скачок offset на графике может сигнализировать о проблемах с маршрутизацией и перегрузкой канала. Для глубокого анализа логов полезен инструмент ntpviz. Он генерирует графические отчёты, где можно визуализировать стабильность локального осциллятора и точность внешних серверов за длительный период. Это очень полезно для тонкой настройки серверов Stratum 1.

Вообще, интересен факт, что для сетевого инженера мониторинг NTP через Zabbix это классическая проблема «курицы и яйца». Если время «убежит» на самом сервере мониторинга, он может перестать адекватно оценивать состояние всей сети. Zabbix-сервер и целевые узлы могут синхронизироваться от одного и того же неисправного источника времени, который может начать «врать», и в этом случае Zabbix может не увидеть проблему, так как offset между ним и целевыми узлами будет близок к нулю, хотя все системы будут показывать отстающее время. Чтобы такого избежать, необходимо анализировать не только разницу во времени, но и внутренние параметры на каждом узле (ntp discovery, stratum, max jitter, root dispersion). Для выхода из замкнутого круга опытные инженеры настраивают Zabbix на синхронизацию с независимым от остальной сети источником.

Завершающим инструментом в арсенале сетевого инженера является глубокий анализ пакетов. Ntpd и Chronyc показывают результат алгоритма, в то время как Wireshark позво-

ляет увидеть сам процесс обмена данными и найти скрытые аномалии. Зачастую это полезно, когда консольные утилиты показывают статус REJECT или INIT или имеются проблемы с сетевыми задержками. Wireshark позволяет увидеть и проблему аутентификации (если используются ключи, которые не совпадают), в то время как NTP может молча игнорировать пакеты. Также Wireshark позволяет вычислить время обработки пакета внутри самого сервера, что позволяет проводить более точную диагностику и отделить проблему сети от проблемы самого сервера.

Ещё одним немаловажным подспорьем для системного администратора является анализ поля Leap Indicator (LI) в Wireshark. Это поле позволяет увидеть, когда вышестоящий сервер потерял связь со своими эталонами и его время стало недостоверным. В то время как NTP просто отбросит такой сервер, Wireshark покажет, что сервер отвечает, но время его не достоверно.

Безусловно, анализатор необходим для обнаружения DDoS-атак. Это тема отдельной и большой дискуссии. В качестве примера можно посмотреть, когда Wireshark показывает огромное количество мелких запросов monlist с одного IP. Это явный признак того, что сервер пытаются использовать для DDoS Amplification атаки на другие системы.

«Малая ошибка в начале становится большой в конце» – Фома Аквинский, «О сущем и сущности»

На практике довольно часто бывают ситуации, связанные не только с атаками на NTP-серверы, но и с ошибками конфигурации. Хотелось бы рассмотреть один интересный случай, с которым нам довелось столкнуться чуть больше года назад. Этот случай вошёл в историю как пример того, что бывает, когда масштабируемость облачного сервиса сталкивается с хрупкостью волонтёрского проекта. Один из производителей умных колонок во время создания своей системы не уделил должного внимания вопросу NTP, и в качестве серверов времени по умолчанию были прописаны адреса пула 0.ru.pool.ntp.org, 1.ru.pool.ntp.org. Количество устройств (и продаж) неуклонно росло и в какой-то момент перевалило за критическую массу. С нашей стороны (как администраторов NTP-серверов) это выглядело как планомерный рост нагрузки, который потребовал от нас умощнения систем, выстраивания новых NTP-узлов в Anycast NTP.IX.RU, так как нагрузка не была похожа на атаку. Главный враг NTP-сервера – это плохо написанный алгоритм повторов (Retry). Если колонка не получала ответ от сервера (из-за задержек в сети), она начинала слать запросы каждую секунду (или даже чаще). Миллионы устройств начинали одновременно стучаться в один и тот же список IP-адресов (адреса pool), и это выглядело как всплеск нагрузки. У многих участников NTP Pool сервис построен «на энтузиазме», зачастую серверы стоят в небольших ЦОДах или даже используют домашние каналы связи (!). Трафик вырос настолько, что участники ntp.pool.org стали выходить из проекта по разным причинам, что, в свою очередь, приводило к ещё большей нагрузке на оставшиеся системы. В итоге сообщество обнаружило причину проблемы, и специалисты обратились к производителю умных устройств за исправлением ситуации.

Как в итоге эту проблему можно решить? Обычно для вендоров, которые строят большие распределённые системы, рекомендуется использовать выделенную именную зону (vendor zone) в pool.ntp.org. Например, такие зоны есть у Ubuntu, FreeBSD, Amazon и т.д. Использование выделенных зон позволяет отделить трафик такого проекта от общего пула. Но в случае, описанном выше, производитель пошёл иным путем и сделал свои собственные адреса NTP. Дополнительно производитель переписал прошивку, добавив туда алгоритм Exponential Backoff, при котором устройство после неудачной попытки ждёт всё дольше и дольше, прежде чем спросить снова.

Какие выводы можно сделать из подобной ситуации? При построении подобных систем, где может быть миллион устройств, не используйте публичные ресурсы и всегда ограничивайте частоту запросов (poll), если сервер не отвечает.

Говоря о проблемах NTP, нельзя не затронуть несколько критических моментов, хотя это и тема для отдельной публикации. Если раньше главной проблемой сетевого инженера были перегруженные каналы, то сегодня на первый план выходят атаки на «физику» процесса – спутниковые сигналы, на которых часто держатся серверы Stratum 1.

Например, Jamming (заглушение сигнала), по сути, создаёт радиопомехи на частоте спутниковой навигации. Для инженера это выглядит как антенна, переставшая видеть спутники. В итоге сервер уходит в режим holdover и держится на внутреннем осцилляторе. Если на сервере нет дорогого рубидиевого чипа, то время может постепенно начать «уплывать», и сервер станет выдавать ошибку.

Гораздо опаснее выглядит Spoofing (подмена данных). В этом случае сервер видит искажённый сигнал и принимает его за основу. Это гораздо сложнее определить и требует вдумчивого подхода к мониторингу.

В целом, главный правильный подход к защите от подобных ситуаций – это построение резервируемой системы: георазнесение точек, использование нескольких антенн, задействование разных спутниковых группировок (GPS/GLONASS/BeiDoo) и наземных эталонов.

В заключение хотелось бы рассмотреть ещё две практические проблемы NTP. Проблема прыжка секунды (Leap Second) – это настоящий кошмар для баз данных, а вопрос часовых поясов часто путают с работой самого протокола.

Известно, что Земля вращается неравномерно, и когда разница между астрономическим и эталонным временем UTC приближается к одной секунде, Международная служба вращения Земли объявляет о добавлении «високосной секунды». Как это работает на практике: в пакете NTP есть поле Leap Indicator (LI). За сутки до этого события серверы Stratum

1 выставляют значение в Li=1. Когда наступает полночь, системные часы показывают 23:59:60 вместо 00:00:00. Это настоящий кошмар для программистов, который в прошлом приводил даже к падениям систем, а в базах данных возникает путаница в последовательности транзакций. В результате, чтобы не прыгать резко, крупные компании (Amazon, Google, Yandex) применяют leap smearing, когда они вместо прыжка в одну секунду замедляют ход NTP-серверов на миллисекунды. В результате процесс выглядит плавнее и лишняя секунда не так заметна.

Один из самых распространенных мифов: «NTP неправильно перевёл время на сервере». Однако хочется напомнить, что NTP всегда передает время в UTC и ничего не знает о часовых поясах. Эти изменения выполняются на самой системе. Кстати, многие, думаю, помнят, как в России отменили переход на летнее время. Это стало проблемой для целого ряда программного и аппаратного обеспечения, в которых этот переход уже был вшит заранее.

Что нас ждёт в будущем? В 2036 году протокол NTPv4 столкнётся с аналогом проблемы 2000 года (Rollover NTP Era 0). Формат времени в NTP представляет собой 64-битное число. Из них 32 бита отведены под целое количество секунд с начала эпохи (1 января 1900 года 00:00:00 UTC). Нетрудно подсчитать, что это количество секунд истечёт 7 февраля 2036 года. Хотя «Время Ч» наступит в 2036 году, подготовка и первые сбои ожидаются значительно раньше. Производители оборудования и ПО уже сейчас находятся у черты: устройства, выпускаемые сегодня, должны иметь запас эксплуатации 10-15 лет, а значит, обязаны уметь работать в новой эпохе «из коробки».

Для решения проблемы переполнения 32-битного счётчика NTP индустрия использует несколько подходов:

1. Переход на 64-битные метки. Это самое фундаментальное решение – расширение формата времени. В новых реализациях протокола под секунды отведено уже 64 бита (вместо 32), а под дробные доли секунды - ещё 64. Этого объёма хватит на время, сопоставимое с жизнью Вселенной, что навсегда снимет вопрос конца эпох.

2. Механизм эпох (Era Number). Это решение для сохранения совместимости со старыми системами. Вводится номер эпохи, и системы считают, что после достижения максимума счётчик обнуляется, но это уже эпоха 1. Однако это требует поддержки на уровне ОС, устройство должно понимать, что ноль на часах - это 2036 год, а не 1900-й.

3. Использование 64-битных типов данных внутри ОС. Современные ядра (Linux, BSD) перешли на 64-битное представление времени (time_t). Это позволит на уровне операционной системы корректно отрабатывать даты далеко за пределами 2036 года во внутренних вычислениях.

4. Метод коррекции. Некоторые системы могут считать, что если метка времени меньше определённого порога, то это уже следующая эпоха. Это, по сути, временная мера, позволяющая не потерять старые устройства после наступления новой эпохи.

Своевременное обновление парка оборудования и переход на современные реализации NTP – это единственный способ избежать цифрового паралича в 2036 году. Важно проводить аудит систем уже сегодня, чтобы к моменту наступления новой эпохи сеть продолжала работать бесшовно и предсказуемо.

Так откуда всё-таки берётся время в Интернете?

Короткий ответ: из космоса или из лаборатории. Время в Интернете – это результат сложной эстафеты, где эстафетной палочкой является радиосигнал или сетевой пакет, а бегунами – протоколы синхронизации, постоянно сражающиеся с физической задержкой света и несовершенством железа. Точное время – следствие работы многоуровневой иерархической системы технических средств, но во многом результат зависит от каждого сисадмина – архитектора сети.

«У каждых часов своё точное время» ;))))

Список литературы:

[1] Mills D., Martin J., Burbank J., Kasch W.// Network Time Protocol Version 4: Protocol and Algorithms Specification // RFC 5905, Internet Engineering Task Force (IETF), 2010. URL: https://datatracker.ietf.org/

[2] IEEE Standard Association// IEEE 1588-2019 - IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems // IEEE, 2019. 499 p. URL: https://standards.ieee.org/

[3] Mills D.// Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI // RFC 4330, 2006. URL: https://datatracker.ietf.org/

[4] Mills D. L.// Network Time Synchronization: the Network Time Protocol on Earth and in Space, Second Edition // CRC Press, 2011. 495 p.

[5] Lichvar M. et al.// Chrony Documentation // Chrony Project, 2024. URL: https://chrony-project.org/

[6] Sullivan N.// Roughtime: Securing Time with Digital Signatures // Cloudflare Blog, 2018. URL: https://blog.cloudflare.com/roughtime/

Об авторе:

Александр Юрьевич Ильин,
технический директор АО ЦВКС МСК-IX

ВРЕМЯ
и протокол сетевого времени

Джефф Хьюстон

Аннотация

Статья посвящена фундаментальной, но часто недооценённой роли времени в функционировании Интернета. Автор проводит читателя через эволюцию измерения времени — от астрономических наблюдений и механических часов до современных атомных стандартов — и показывает, насколько сложной является задача согласования «физического» времени, основанного на вращении Земли, с высокоточным атомным временем. Особое внимание уделяется таким понятиям, как UTC, UT1 и практике добавления дополнительных секунд, которая, несмотря на свою необходимость, регулярно становится источником технических сбоев.

Хьюстон также подробно рассматривает протокол сетевого времени (NTP) как ключевой механизм синхронизации времени в Интернете. Он объясняет принципы его работы, архитектуру серверов и клиентов, а также методы компенсации задержек и отклонений. Автор подчёркивает, что, несмотря на кажущуюся простоту, NTP обеспечивает критически важную функцию — согласованность времени в распределённых системах, от которой напрямую зависят устойчивость, корректность и безопасность современных интернет-сервисов.

.

Ключевые слова:

NTP, UTC, UT1, синхронизация времени, атомное время, дополнительная секунда

Создание высокоточных часов можно считать одним из самых древних устремлений человечества. История того, как измерение времени становилось всё более точным, во многом связана с установлением связи между измерениями наблюдаемой вселенной и продолжительностью наблюдаемых событий, что постепенно углубляет наше понимание небесной механики.

Земное время

Использование шестидесятеричной системы счисления для обозначения секунд и минут восходит к древним шумерам в III тысячелетии до нашей эры. Этот подход к измерению времени переняли вавилоняне, затем греки, за ними древние римляне, а от них его унаследовали и мы с вами. В применяемой нами системе измерения мы делим время, которое требуется Земле для осуществления одного оборота вокруг своей оси, на 86 400 интервалов – секунд.

Шли века. Механические часы становились всё более совершенными, проделав путь от элементарных солнечных часов до водяных, песочных и огненных. Затем человечество переключилось на колебания маятника – появились маятниковые механизмы и регуляторы хода. Такие часы широко применялись в разных сферах жизни. Однако сти-

мулом для существенного повышения точности измерения времени в XVIII веке стали практические потребности морской навигации, а именно расчёт координат местонахождения судна. В 1761 году появился морской хронометр Джона Гаррисона модели H4. За 81 день плавания погрешность хода этого механизма составила всего 216 секунд, или 2,6 секунды в день. Но процесс совершенствования механических хронометров на этом не остановился. Эти устройства ещё более века использовались для измерения времени вплоть до появления генератора колебаний с кварцевым резонатором в начале XX века.

Кварцевые генераторы характеризуются исключительной стабильностью. Если не подвергать их резким перепадам температуры, то погрешность кварцевых часов составляет менее полсекунды в сутки. Применение блока из нескольких генераторов, а также регулирование температуры цифрового счётчика позволяет ещё больше снизить погрешность часов – до менее 15 миллисекунд в день. Кварцевые часы использовались Национальным бюро стандартов США для установления стандартного времени с 1929 по 1960-е годы.

В своём стремлении добиться ещё большей точности в измерении времени мы стали опираться на колебания на уровне атомов. Погрешность колебаний изотопа цезий-133 составляет менее 2 наносекунд в день. Таким образом, атомные часы не только являются стандартом определения хода времени, но и выполняют функцию определения самого времени.

Следующая задача заключалась в том, чтобы соотнести такой точный метод измерения единицы времени со скоростью оборота планеты вокруг своей оси. В этом отношении добиться такого же уровня точности просто невозможно! Дело в том, что под влиянием вызванных Луной приливных сил скорость вращения Земли замедляется, так что продолжительность дня увеличивается за сто лет на 2,3 миллисекунды. Но дело не только в изменении скорости вращения Земли вокруг своей оси. Другим существенным фактором выступают периодические изменения климата и вызванные им ледниковые периоды. Свою роль играет и распределение континентальных плит на поверхности земли. Плиты подвижны, что сказывается на скорости вращения Земли. По мере повышения точности астрономических наблюдений и устройств измерения времени мы получили возможность измерять эти, хоть и совершенно небольшие, отклонения в угловой скорости.

На рис. 1 приведены данные по годовым колебаниям продолжительности суток в миллисекундах с 1730 года.

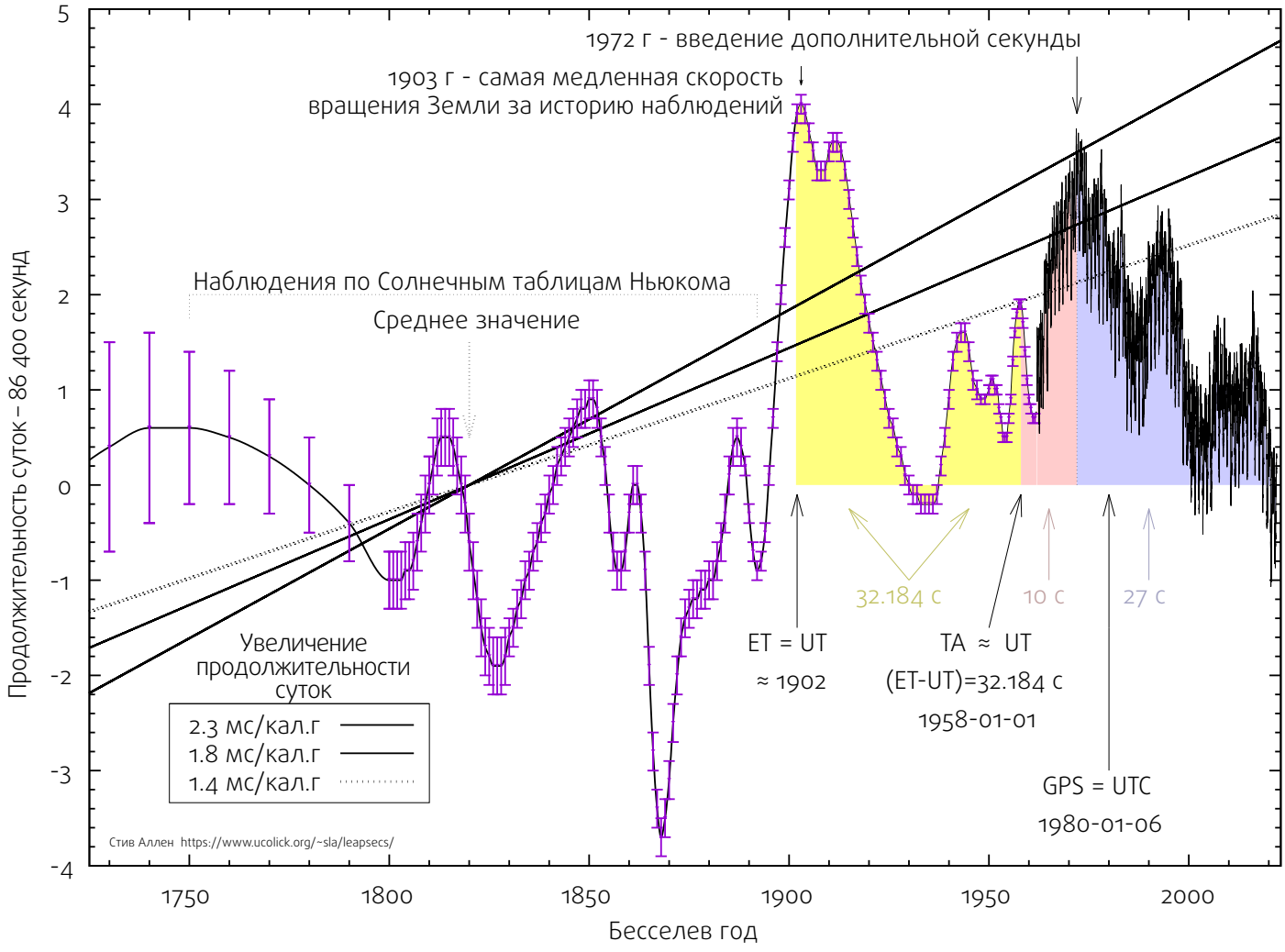


Рис. 1. Динамика продолжительности суток в историческом разрезе.

Стандарты всемирного времени

Если скорость вращения Земли постоянно меняется, можно ли считать секунду постоянной величиной? Впервые этим вопросом задались астрономы, а затем физики.

В настоящее время всеобщим стандартом продолжительности секунды выступает определение Международного бюро мер и весов, согласно которому секунда в Международной системе единиц составляет по длительности 9 192 631 770 периодов излучения, которые соответствуют переходу между двумя сверхтонкими уровнями атома цезий-133 в состоянии покоя при температуре 0K– это называется «Международным атомным временем» (TAI, фр. Temps Atomique International).

Проблема заключается в том, чтобы соотнести такое определение времени со скоростью вращения Земли и другими доступными нашему восприятию феноменами. Существует несколько версий стандарта всемирного времени, но для целей измерения времени особый интерес представляют два стандарта.

UT1 – основная версия всемирного времени. По идее, UT1 представляет собой среднее солнечное время (среднее значение периода, когда Солнце находится на одном и том же уровне несколько дней подряд) на нулевой параллели, но точно измерить среднее солнечное время путём наблюдения за Солнцем представляется затруднительным. UT1 вычисляется пропорционально углу вращения Земли относительно квазаров согласно Международной небесной системе координат с использованием радиоинтерферометрии с длинными базами. Время UT1 определяется с точностью до 15 микросекунд.

UTC (всемирное координированное время) представляет собой атомную шкалу времени, которая связана с временем по UT1, но обеспечивает гораздо более высокую степень точности. Именно время по UTC стало международным стандартом для определения времени в гражданских целях. В UTC в качестве единицы времени используется секунда по Международной системе единиц, поэтому UTC идёт синхронно с международным атомным временем (TAI). Поскольку в основе UTC лежит международное атомное время, этот стандарт лишён непосредственной привязки к скорости вращения Земли вокруг своей оси. Тем не менее, согласно UTC сутки также состоят из 86 400 стандартных секунд.

Дополнительные секунды

Итак, продолжительность суток при определении продолжительности на основе скорости вращения Земли вокруг своей оси представляет собой непостоянную величину. Как же соотнести этот показатель с равномерным ходом атомных часов, обусловленным излучением атома цезия? Можно отдать приоритет стандартным атомным часам, и тогда продолжительность суток будет составлять 86 400 стандартных секунд. В таком случае расхождение между стандартным атомным временем и временем, определённым в зависимости от скорости вращения Земли, может составить целый час за тысячу лет, если предположить, что скорость вращения Земли вокруг своей оси будет постепенно снижаться. Можно также периодически корректировать атомное время согласно UTC, чтобы синхронизировать его со скоростью вращения. Сделать это можно за счёт добавления так называемой дополнительной секунды или «секунды координации». Практика введения «дополнительных секунд» действует с 1972 года.

Службы времени пришли к соглашению о возможности добавить такую секунду в два определённых времени года, а именно в последнюю минуту июня и декабря каждого года с продлением последней минуты на 1 секунду. Такие дополнительные секунды добавляются ко времени по UTC по мере необходимости таким образом, чтобы отклонение UTC от UT1 не превышало 0,9 секунды. По состоянию на сегодняшний день, с 1972 года ко времени по UTC было добавлено 27 секунд. График добавления дополнительных секунд приведен на рис. 2.

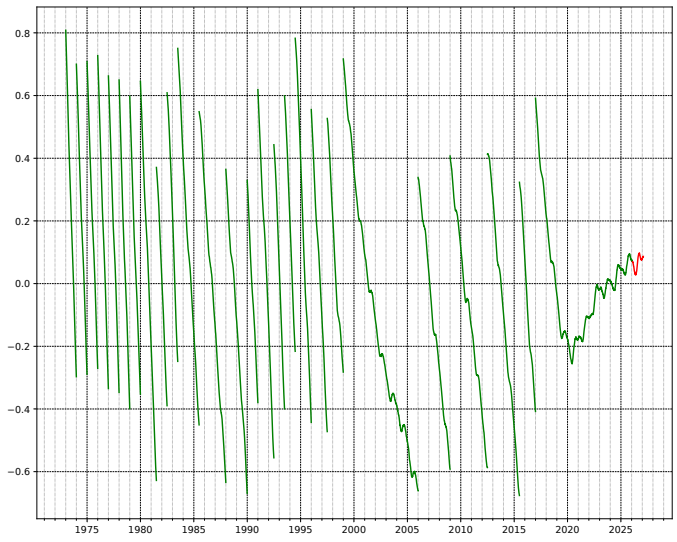


Рис. 2. Добавление дополнительных секунд к всемирному координированному времени (UTC).

Возможно также вычитание секунд из времени по UTC в случае ускорения вращения Земли, чтобы, опять же, расхождение со временем по версии UT1 не превышало 0,9 секунды. Если наблюдаемая в настоящее время тенденция к ускорению скорости вращения планеты сохранится на протяжении следующих 40 лет, потребуется вычесть секунду из времени по версии UTC.

Введение дополнительных секунд приводит к повсеместным сбоям в работе информационных систем. Из-за введения дополнительной секунды 30 июня 2012 года вышли из строя несколько важных систем, включая программу бронирования и оформления билетов крупной авиакомпании. Компьютерной отрасли пришлось разработать специальное решение для того, чтобы предотвращать сбои, вызванные корректировкой времени на целую секунду. Эта секунда «размазывается», то есть заблаговременно

добавляется по несколько миллисекунд за раз до запланированного срока добавления секунды корректировки. Однако это не решает саму проблему скачков в потоке времени.

Потратив несколько лет на изучение этого вопроса, Международный союз электросвязи (МСЭ) в 2015 году передал полномочия по дальнейшему использованию дополнительных секунд в пользу Генеральной конференции по мерам и весам; 18 ноября 2022 года в рамках Генеральной конференции по мерам и весам была принята резолюция о том, чтобы призвать МСЭ отказаться от практики добавления «секунд координации» с 2035 года. Предполагается, что этот отказ будет действовать как минимум 100 лет, хотя это решение может быть изменено по итогам дальнейших консультаций с другими международными ведомствами. Однако МСЭ сохранил за собой контроль над распространением сигнала точного времени по версии UTC и ещё может отказаться от исполнения принятой резолюции.

Передача времени

Как осуществляется синхронизация времени? Если у вас есть доступ к цезиевым часам, то это ваш источник точного времени. Вы также можете использовать водородный мазер или чуть более мобильные рубидиевые атомные часы. Ведутся активные исследования по возможности применения источников света на основе стронция и иттербия, которые позволяют на два порядка повысить точность измерения времени по сравнению с существующими моделями цезиевых атомных часов.

Эксплуатация источника атомных часов, в действительности, целого ряда источников, осуществляется Военно-морской обсерваторией США (https://www.cnmoc.usff.navy.mil/usno/). В её ведении находятся атомные часы, которые работают в условиях неизменной температуры и влажности. Сигнал времени корректируется путём введения «дополнительных секунд» по графику, который раз в полугодие распространяется в Бюллетене «C» Международной службы вращения Земли (IERS, https://www.iers.org/). Есть аналогичные источники времени и в других странах.

В случае с США сигнал UTC передаётся на космическую базу Шривер в Колорадо, которая, помимо прочего, управляет спутниковой группировкой, передающей сигнал времени для глобальной системы позиционирования (GPS).

В компьютерах с датчиком GPS можно обеспечить синхронизацию их внутренних часов по сигналу GPS.

С этого момента за установление времени в Интернете отвечает протокол сетевого времени (NTP).

Протокол сетевого времени

Если одни протоколы связи по IP появились сравнительно недавно, то другие уже имеют достаточно долгую и богатую историю, которую ведут со времён появления Интернета. Сеть ARPANET перешла на протокол TCP/IP в январе 1983 года, а с 1985 года в сети действует протокол сетевого времени. Некоторые даже утверждают, что NTP стал самым старым постоянно действующим распределённым приложением Интернета.

Цель протокола сетевого времени проста: дать возможность клиенту синхронизировать часы по времени UTC, обеспечив высокий уровень точности и стабильности. Протокол сетевого времени обеспечивает точность времени с погрешностью всего несколько миллисекунд в пределах глобальной вычислительной сети (WAN). Чем компактнее сеть, тем точнее работа протокола NTP. В рамках локальных вычислительных сетей (LAN) достигается точность с погрешностью менее миллисекунды, а при использовании таких высокоточных источников времени, как приёмник сигнала GPS или цезиевые часы, погрешность не превышает микросекунду.

Если несколько клиентов используют протокол NTP, то они могут работать с синхронизированным сигналом времени. Одним из примеров применения протокола сетевого времени в сетевом контексте является единая модель данных, для которой изменение временных параметров данных имеет очень большое значение. (Я использовал протокол сетевого времени для обеспечения точности измерения времени до микросекунды при комбинировании различных источников дискретных данных – например, веб-логов с сервера в сочетании с логом запросов системы доменных имён с использованием DNS-преобразователей и трассировки пакетов.)

Чтобы понять работу протокола NTP, нужно затронуть саму проблему измерения времени. В этой связи важно обозначить ряд терминов, связанных с этой тематикой.

Стабильность –	Способность обеспечить постоянную частоту.
Точность –	Соответствие частоты и абсолютного значения времени по часам со стандартным эталонным временем.
Прецизионность –	Возможность сохранения точности часов в рамках конкретной системы измерения времени.
Отклонение –	Разница между абсолютным значением времени двух часов.
Сдвиг –	Изменение отклонения с течением времени (производная первого порядка от отклонения времени).
Дрейф –	Изменение сдвига с течением времени (производная второго порядка от отклонения времени).

Протокол сетевого времени создан для того, чтобы компьютер мог принимать в расчёт три основные показателя времени: отклонение внутренних часов от выбранных эталонных часов, двусторонняя задержка сетевого трафика между компьютером и сервером используемого источника опорного времени, а также дисперсия внутренних часов, то есть показатель максимальной погрешности внутренних часов по отношению к источнику опорного времени. Каждый из этих компонентов отражается в протоколе NTP по отдельности. Это позволяет не только точно измерить показатели отклонения и задержки, что обеспечивает возможность синхронизации внутренних часов по сигналу опорного времени, но и учитывать максимальную погрешность при синхронизации. За счёт этого можно не только определить время, но и оценить его точность в рамках пользовательского интерфейса.

В качестве эталонного источника времени в протоколе сетевого времени применяется стандарт UTC, а не среднее время по гринвичскому меридиану (GMT). Версия UTC, в свою очередь, основана на международном атомном времени, что подразумевает добавление «дополнительных секунд» по мере необходимости. Таким образом, время по протоколу сетевого времени приходится периодически корректировать путём добавления дополнительных секунд.

Протокол NTP является протоколом «абсолютного» времени. Это означает, что в его непосредственные функции не входит перевод абсолютного значения времени в конкретные дату и время для определённого места на поверхности Земли. Функция преобразования значений по UTC в показания обычных часов, а именно функция определения локальных даты и времени, возлагается на локальный сервер.

Серверы, клиенты, слои

В основе функционирования протокола сетевого времени лежат понятия сервера и клиента. Сервер выступает источником информации о времени, а клиент действует в качестве системы, пытающейся синхронизировать свои часы с сервером.

Среди серверов выделяются первичные и вторичные серверы. Первичный сервер также иногда называют сервером слоя 1 (stratum 1), если заимствовать терминологию архитектуры обозначения времени в телефонных сетях. Этот сервер получает сигнал времени по UTC непосредственно от официального источника времени – например, от настроенных атомных часов или источника сигнала GPS. Вторичный сервер получает сигнал времени от одного из вышестоящих серверов. На него возложена задача по передаче сигнала времени одному или нескольким нижестоящим серверам и клиентам. Вторичные серверы, по сути, занимаются воспроизведением сигнала времени. Их задача заключается в том, чтобы разгрузить первичные серверы, взяв на себя обработку поступающих от клиентов запросов, при этом обеспечивая клиентам доступ к сигналу времени сопоставимого качества. Вторичные серверы выстраиваются по чёткой иерархической системе и делятся на вышестоящие и нижестоящие. Нередко для оптимизации этого процесса применяется система слоёв (strata).

Сервер слоя 2 получает сигнал времени от сервера слоя 1, а сервер слоя 3 - от сервера слоя 2, и так далее. Сервер слоя n может взаимодействовать со множеством серверов слоя n-1 для стабильного получения сигнала времени. Архитектура слоёв используется для того, чтобы избежать петли синхронизации при обращении к нескольким серверам времени. (См. инфографику «Иерархия временной синхронизации NTP» - ред.)

Для синхронизации своих внутренних часов с сигналом времени по протоколу NTP клиенты взаимодействуют с серверами.

Протокол сетевого времени

Если говорить простыми словами, то протокол сетевого времени NTP – это операция по запросу времени. Клиент направляет серверу запрос о текущем времени вместе со своими показателями. Сервер добавляет показатели времени в пакет данных и перенаправляет пакет обратно клиенту. Из полученного пакета клиент может извлечь два ключевых вида информации: опорное время сервера и измеренное с помощью внутренних часов время прохождения сигнала от клиента на сервер и обратно. Многократное повторение этой процедуры позволяет клиенту решить проблему временной задержки сети и определить точное отклонение внутренних часов от опорных часов сервера. Это значение используется для корректировки внутренних часов и их синхронизации с сервером. Дальнейшее выполнение протокола позволяет локальному клиенту в режиме реального времени корректировать внутренние часы, чтобы решить проблему рассинхронизации часов.

Протокол NTP использует для своей работы протокол UDP (протокол пользовательских датаграмм). Сервер протокола NTP принимает пакеты данных клиента посредством порта 123. Сервер не сохраняет данные о запросах и отвечает на каждое поступление пакета от клиента по протоколу NTP простой операцией: он добавляет поля к полученному пакету данных и отправляет пакет обратно отправителю без какой-либо отсылки к предшествующим транзакциям.

Получив пакет данных NTP от клиента, сервер оперативно фиксирует время получения запроса, следуя алгоритму формирования пакетов данных на сервере. Затем пакет поступает в обработку процессом NTP. Обработка включает замену полей адреса и порта заголовка пакета, перезапись различных полей в пакете с их заменой на показания внутренних часов, проставку времени отправки пакета обратно, перерасчёт сигнатуры и отправку пакета обратно клиенту.

Пакеты, отправленные клиентом по протоколу сетевого времени, и ответы сервера клиента оформляются согласно единому формату, который приведён на рис. 3.

Рис. 3. Формат сообщения по протоколу сетевого времени.

Заголовок сообщения по протоколу сетевого времени составляется следующим образом:

ИК — **Индикатор коррекции** (2 бит).

В данном поле указывается сообщение о добавлении секунды координации к последней минуте текущего дня.

Используются следующие значения:
0: нет добавления секунды коррекции;
1: последняя минута дня содержит 61 секунду;
2: последняя минута дня содержит 59 секунд;
3: время не синхронизировано.

Номер версии — **Номер версии протокола NTP** (3 бит) (номер текущей версии – 4).

Режим — **Режим пакета по протоколу NTP** (3 бит).

Значения поля «Режим»:
0: зарезервировано;
1: симметричный активный режим;
2: симметричный пассивный режим;
3: клиент;
4: сервер;
5: широковещательный режим;
6: контрольное сообщение NTP;
7: зарезервировано для частного использования.

Часовой слой — **Слой источника времени** (8 бит).

Значения поля «Часовой слой»:
0: не определено или недопустимо;
1: первичный сервер;
2–15: вторичный сервер, использующий протокол NTP;
16: не синхронизировано;
17–255: зарезервировано.

Интервал опроса — **Интервал опроса** (8 бит, целое число со знаком). Максимальный интервал между последовательными сообщениями NTP, в секундах.

Точность — **Точность часов** (8 бит, целое число со знаком).

Точность системных часов. Значение равно двоичному логарифму секунд.

Задержка — **Общее время циклической задержки от сервера к первичному эталонному источнику.**

Значение выражается числом с фиксированной запятой длиной 32 бит в секундах с запятой между 15-м и 16-м битом. Данное поле имеет значение только для сообщений сервера.

Дисперсия **Максимальная допустимая погрешность тактовой частоты.**

Значение выражается числом с фиксированной запятой длиной 32 бит в секундах с запятой между 15-м и 16-м битом. Данное поле имеет значение только для сообщений сервера.

Идентификатор источника **Для серверов слоя 1 значением является код из четырёх символов ASCII, назначенный для опорного времени** (см. рис. 4). Для вторичных серверов данное значение выражается адресом IPv4 источника синхронизации (32 бит) или первыми 32 битами хеша MD5 IPv6-адреса источника синхронизации.

Код	Внешний источник
GOES	Геостационарный эксплуатационный спутник наблюдения за окружающей средой
GPS	Система глобального позиционирования
GAL	Система местоопределения «Галилео»
PPS	Общий радиосигнал с длительностью импульса, равной 1 секунде.

Рис. 4. Основные коды идентификации (Из «Параметров протокола сетевого времени NTP»).

Для следующих четырёх полей используется отметка времени длиной 64 бит, состоящая из обозначения целых секунд длиной 32 бит и дробной части длиной 32 бит. При такой системе обозначения значение «2,5» было бы представлено в формате 64 бит следующим образом:

0000|0000|0000|0000|0000|0000|0000|0010 . |1000|0000|0000|0000|0000|0000|0000|0000

Целая часть | Дробная часть (десятичная)

Единица времени – секунда, а дата – 1 января 1900 года. Соответственно, 32-битный счётчик обнулится в 2036 году, а через два года, в 2038 году, обнулится счётчик по 32-битному Unix.

Минимальное значение в данном формате – 232 пикосекунды.

Время обновления Данное поле отражает время, когда система последний раз устанавливала или корректировала время. Длина – 64 бит.

Начальное время Данное поле отражает время клиента, когда запрос отправляется серверу. Длина – 64 бит.

Время приёма Данное поле отражает время сервера, когда запрос приходит от клиента. Длина – 64 бит.

Время отправки Данное поле отражает время сервера, когда запрос отправляется клиенту. Длина – 64 бит.

Как работает протокол? Клиент отправляет пакет на сервер и фиксирует время отправки пакета в поле «Начальное время» (T1). Сервер фиксирует время получения пакета (T2). После этого формируется пакет отклика с указанием первоначального значения «Начальное время» и времени приёма, когда пакет получен сервером, а затем к пакету добавляется значение «Время отправки», то есть время передачи пакета клиенту (T3). После этого клиент фиксирует время получения пакета (T4). Таким образом, в распоряжении клиента оказывается четыре временных показателя, приведённых на рис. 5.

Временная метка	Идентификатор	Стадия генерации
Начальное время	T1	Клиент отправил запрос
Время приёма	T2	Сервер получил запрос
Время отправки	T3	Сервер отправил ответ
Время прихода отклика	T4	Получение клиентом ответа

Рис. 5. Временные метки по протоколу NTP (Спецификация RFC 4330).

Эти четыре параметра загружаются во внутренние часы клиента для обеспечения их синхронизации. Описание данного алгоритма приведено в следующем разделе.

Необязательные поля «Ключ» и «Профиль сообщения» обеспечивают возможность обмена секретным 128-битным ключом между клиентом и сервером. Секретный ключ используется для формирования полей хеша MD5 ключа и сообщения по протоколу NTP длиной 128 бит. За счёт этого клиент получает возможность выявлять попытки включить в передаваемую информацию ложные ответы за счёт атаки через посредника.

В завершение обзора функционирования протокола приведём описание алгоритма интервала опроса. Клиент NTP отправляет сообщения на NTP-сервер с одинаковой периодичностью. Как правило, интервал между запросами составляет 16 секунд. Если сервер недоступен, протокол NTP увеличивает интервал опроса – с каждым неудачным запросом интервал увеличивается вдвое до достижения минимальной частоты, которая составляет один запрос каждые 36 часов. При попытке возобновить синхронизацию с сервером протокол NTP сокращает продолжительность интервалов опроса и отправляет блоки из восьми пакетов с интервалом 2 секунды.

Если отклонение часов клиента от часов сервера достаточно мало, протокол NTP увеличивает интервал опроса путём отправки блоков из восьми пакетов с интервалом от 4 до 8 секунд (от 256 до 512 секунд).

Отсчёт времени клиентом

Следующая стадия работы протокола сетевого времени связана с использованием клиентом информации, полученной за счёт отправки запросов на сервер с определённой периодичностью, для корректировки внутренних часов.

Опрос NTP-сервера позволяет клиенту оценить время задержки по отношению к серверу. Время задержки рассчитывается с применением временных меток, описанных на рис. 5, и составляет время от передачи запроса до получения ответа за вычетом времени, которое потребовалось серверу для обработки запроса и формирования ответа.

$$\delta = (T_4 - T_1) - (T_3 - T_2)$$

Рассчитать отклонение часов клиента по отношению к часам сервера можно также следующим образом:

$$\Theta = ½ [(T_2 - T_1) + (T_3 - T_4)]$$

Необходимо отметить, что при осуществлении данных расчётов предполагается, что задержка при передаче сообщения между клиентом и сервером одинакова в обоих направлениях.

Для расчётов показателя δo протокол NTP использует минимальное значение последних восьми замеров времени задержки. В качестве величины отклонения выбирается значение, измеренное при наименьшей задержке. Значения (Θo, δo) становятся обновлёнными значениями NTP.

Если в конфигурации клиента только один сервер, показания часов клиента корректируются путём их сдвига таким образом, чтобы нивелировать отклонение относительно часов сервера, при условии, что отклонение по отношению к серверу находится в допустимых пределах.

При включении нескольких серверов в конфигурацию клиента им применяется выборный алгоритм для назначения приоритетного сервера синхронизации из числа серверов-кандидатов. Для исключения серверов с нерелевантными показаниями осуществляется группировка сигналов времени. Затем алгоритм выбирает сервер самого низкого слоя с минимальными значениями отклонения и помех. Алгоритм для этой операции в рамках протокола NTP называется алгоритмом Марзулло.

Включённый в конфигурацию клиента, протокол NTP пытается обеспечить синхронизацию часов клиента с опорным временем. Для этого NTP по мере необходимости корректирует показания внутренних часов в несколько заходов, каждый раз сокращая отклонение на небольшую величину, поскольку существенное изменение показателей может негативно сказаться на работе запущенных приложений, подтверждением чему служит ситуация с добавлением секунд корректировки. Поэтапная подстройка времени осуществляется за счёт вызова системной функции adjtime(), которая позволяет менять показания часов путём изменения частоты программных часов до полной коррекции. При высоких показателях отклонения изменение показаний часов становится достаточно длительным процессом. Как правило, темп составляет 0,5 миллисекунд в секунду.

Разумеется, это довольно схематичное описание общих принципов работы достаточно сложного алгоритма и задействованных в нём сложных математических формул. Если вы хотите более подробно погрузиться в суть работы протокола NTP, советуем ознакомиться с приведённым далее по тексту списком литературы. В ней представлено гораздо более глубокое описание алгоритмов и лежащих в их основе моделей выбора часов и синхронизации.

В последние годы ведётся активная работа по обеспечению безопасности протокола сетевого времени. Итогом этих усилий стала публикация стандарта RFC8915, в котором приводится описание взаимодействия клиента и сервера по протоколу NTP с использованием протокола TLS (безопасность транспортного уровня), а не UDP. В рамках IETF также ведётся работа по описанию протокола NTP через протокол QUIC, чтобы обеспечить поддержку протокола сетевого времени в режиме пакетной обработки или датаграммном режиме.

По сути, протокол NTP представляет собой необычайно простой протокол взаимодействия между клиентом и сервером без сохранения информации о состоянии клиента на сервере. Однако он позволяет добиться удивительных результатов. Регулярно обмениваясь с сервером показаниями времени, клиент получает возможность настроить свои часы таким образом, чтобы обеспечивать высокую степень точности, несмотря на потенциальные проблемы со стабильностью и точностью внутренних часов, также несмотря на то, что синхронизация осуществляется по сети и может сопровождаться помехами в виде изменчивости задержки при обмене пакетами между клиентом и сервером. Большая часть современной распределённой инфраструктуры интернет-сервисов опирается на общую временную базу, и эта база обеспечивается общим использованием протокола сетевого времени (NTP).

Список литературы:

[1] David L. Mills, "A Brief History of NTP Time: Confessions of an Internet Timekeeper", ACM SIGCOMM, Computer Communication Review, Vol. 33, No. 2, pp. 9–12, April 2003, http://www.eecis.udel.edu/~mills/database/papers/history.pdf

[2] K. A. Marzullo, "Maintaining the Time in a Distributed System: An Example of a Loosely-Coupled Distributed Service", Ph.D. dissertation, Stanford University, Department of Electrical Engineering, February 1984, http://en.wikipedia.org/wiki/Marzullo%27s_algorithm

[3] David L. Mills, "NTP Architecture, Protocol and Algorithms", University of Delaware, www.eecis.udel.edu/~mills/database/brief/arch/arch.ppt

[4] Jack Burbank, William Kasch, and David Mills, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

[5] David L. Mills, "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC 4330, January 2006.

[6] http://www.ntp.org

[7] http://www.eecis.udel.edu/~mills/ntp.html

[8] David Mills, Computer Network Time Synchronization: the Network Time Protocol on Earth and in Space, Second Edition, CRC Press, 2011.

[9] http://en.wikipedia.org/wiki/Universal_Time

[10] RFC 5905: Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, «Network Time Protocol Version 4: Protocol and Algorithms Specification», RFC 5905, DOI 10.17487/RFC5905, June 2010, https://www.rfc-editor.org/info/rfc5905

[11] RFC 8915: Franke, D., Sibold, D., Teichel, K., Dansarie, M., and R. Sundblad, «Network Time Security for the Network Time Protocol», RFC 8915, DOI 10.17487/RFC8915, September 2020, https://www.rfc-editor.org/info/rfc8915

Правовая оговорка

Изложенные в данной статье взгляды могут не совпадать с позицией или точкой зрения Азиатско-Тихоокеанского сетевого информационного центра.

Об авторе

Джефф Хьюстон имеет степени бакалавра и магистра наук. Занимает должность ведущего научного сотрудника Азиатско-Тихоокеанского сетевого информационного центра, региональной интернет-регистратуры Азиатско-Тихоокеанского региона. Он посвятил многие годы развитию Интернета, в особенности в Австралии, где от лица научного-исследовательского сообщества отвечает за формирование инфраструктуры Интернета. Автор книг по связанным с Интернетом темам. Входил в Совет по архитектуре Интернета с 1999 по 2005 год, а с 1992 по 2001 год был членом Попечительского совета общества «Интернет»
www.potaroo.net

Обзор методов безопасной синхронизации времени[1]

Инг Вэн, Имин Чжан

Аннотация

В наши дни использование беспроводных сенсорных сетей стремительно набирает обороты, однако они подвержены киберфизическим атакам. Синхронизация времени является фундаментальным требованием для протоколов проводных и беспроводных сенсорных сетей, поэтому безопасная синхронизация времени также имеет решающее значение. В этой статье мы расскажем о синхронизации времени, в том числе о концепциях, проблемах и требованиях, предъявляемых к протоколам синхронизации времени. Мы рассмотрим как программные, так и аппаратные протоколы. Затем проанализируем различные методы синхронизации времени. Кроме того, мы рассмотрим прогресс исследований в области безопасной синхронизации времени. В обзоре также обсуждаются недостатки существующих систем безопасной синхронизации времени и предлагаются рекомендации для будущих направлений исследований. Цель данного обзора — выделить прогресс и тенденции в области синхронизации времени и безопасной синхронизации времени.

.

Ключевые слова:

синхронизация времени, сетевое время, GPS, NTP, PTP, облегчённая синхронизация, потоковая синхронизация

1. Введение

В процессе промышленного развития беспроводные сенсорные сети (БСС) быстро вытеснили проводные сети благодаря своим преимуществам. БСС — это совокупность пространственно распределённых узлов, объединённых в кооперативную сеть для мониторинга и регистрации физических параметров и условий окружающей среды. Сегодня сенсорные сети используются в самых разных сферах нашей жизни, таких как медицинское обслуживание пожилых людей, видеонаблюдение, ликвидация последствий стихийных бедствий и сбор разведывательной информации на поле боя. Синхронизация времени имеет решающее значение для сенсорных сетей, поскольку она обеспечивает точную и безопасную локализацию, более эффективное чередование режимов работы, формирование диаграммы направленности и выполнение других задач по совместной обработке сигналов. Одной из важных особенностей беспроводных сенсорных сетей является возможность плавного и бесконфликтного роуминга от одной станции к другой, что возможно только при наличии точной информации о времени. Кроме того, синхронизация времени является ключевым элементом для определения точного местоположения. Аналогичным образом, при синхронизации сети различные процедуры, такие как передача данных, вычисление фреймов, анализ и инкапсуляция протоколов, могут приводить к значительным задержкам в зависимости от конфигурации аппаратного и программного обеспечения, что может привести к сбоям в синхронизации времени. Синхронизация времени является ключевым элементом для объединения данных, управления энергопотреблением, определения местоположения, координации действий в будущем, присвоения временных меток событиям и чередования режимов работы в беспроводных сенсорных сетях. Широкое распространение беспроводных приложений, таких как отслеживание целей, мониторинг окружающей среды и научные исследования в опасных условиях, привлекло внимание злоумышленников к БСС. Кроме того, авторы отмечают, что для обеспечения точности и надёжности работы этих приложений важно, чтобы все сенсорные узлы синхронизировались по единому времени. Необходимость ограничения энергопотребления, а также вычислительных и коммуникационных ресурсов узлов в БСС усложняет процесс разработки эффективного протокола. Кроме того, миниатюризация аппаратного обеспечения и разработка маломощных устройств привели к появлению небольших устройств с питанием от аккумулятора, способных определять такие параметры, как температура и уровень шума. Однако миниатюризация и разработка маломощных устройств ограничили возможности датчиков по обработке данных и передаче информации, что усложняет обеспечение безопасности протокола.

2. Синхронизация времени

2.1. Постановка задачи

В последние годы в научной литературе широко изучается проблема синхронизации времени в беспроводных сетях, направленная на достижение более высокого уровня точности при большей масштабируемости топологии и приложений. Однако до сих пор не существует надёжной схемы синхронизации времени из-за сложности, связанной с взаимодействием узлов. Синхронизация времени — это метод синхронизации узлов.

Компьютерные часы состоят из двух частей: генератора и счётчика. C(t) — это часы, в которых счётчик сетевого узла увеличивает своё значение в соответствии с угловой частотой генератора. В идеальных условиях угловая частота по-

1 Печатается в сокращении. Оригинальный текст: Weng, Y.; Zhang, Y. A Survey of Secure Time Synchronization. Appl. Sci. 2023, 13, 3923. https://doi.org/10.3390/app13063923, доступен https://www.mdpi.com/2076-3417/13/6/3923

стоянна, но она может меняться из-за физических факторов, таких как температура, вибрация и давление. Локальные часы узла i и реальное время t связаны следующим соотношением:

$$C_i(t) = a_i t + b_i \quad (1)$$

где a_i – отклонение (дрейф) часов узла i, а b_i – смещение. Дрейф – это изменение частоты генератора, а смещение – это разность значений от реального времени t. Локальные часы узлов 1 и 2 сравниваются как:

$$C_1(t) = a_{12} \times C_2 + b_{12} \quad (2)$$

где a_{12} – относительный дрейф, а b_{12} – относительное смещение часов узлов 1 и 2. Если относительный дрейф равен 1, а относительное смещение равно 0, то оба узла идеально синхронизированы. Тактовая частота сетевого узла и смещение могут быть использованы для корректировки его локального времени согласно приведённым выше уравнениям. В настоящее время существует множество протоколов для достижения синхронизации времени; однако эти протоколы уязвимы для многих атак.

2.2. Важность синхронизации времени

Киберфизические атаки на синхронизацию времени сети могут ухудшить производительность сети, например, вызвать нарушение порядка передачи данных, несинхронизированное выполнение задач, периодические отключения и неисправности. В статье «Безопасная синхронизация времени в беспроводных сенсорных сетях: подход, основанный на максимальном консенсусе», опубликованной еще в 2013 году в журнале IEEE Transactions on Parallel and Distributed Systems, подробно разъясняется, как атаки, которые могут нарушить синхронизацию времени, могут привести к усилению помех в сети, перехвату пакетов и задержкам в передаче сообщений. Таким образом, безопасная синхронизация времени становится ключевым элементом беспроводных сенсорных сетей, обеспечивающим их надёжную работу. Плохая синхронизация времени может привести к искажению временных меток, ложным оценкам местоположения узлов, потере пакетов и повышенному энергопотреблению из-за нарушения режима сна и бодрствования. Сенсорные узлы мониторят данные, которые могут быть подвержены утечке, и привести к нарушению личной конфиденциальности, а увеличение киберфизических атак приведёт к большим затратам энергии на повторную синхронизацию. БСС требуют, чтобы все узлы работали эффективно путём синхронизации друг с другом для экономии энергопотребления. Схема синхронизации времени может быть подвержена влиянию многих факторов, происходящих в сети, таких как коммуникационные накладные расходы, доступная пропускная способность, требования к точности, масштабируемость и требования к инфраструктуре. Как описано выше, сенсорные узлы имеют ограниченные ресурсы и низкое энергопотребление, и поэтому энергия, сэкономленная в процессе синхронизации, может быть использована для целей безопасности. Чтобы избежать описанных выше проблем, при проектировании сенсорных сетей необходимо уделять особое внимание вопросам безопасности, конфиденциальности данных и защиты персональных данных.

2.3. Распространённые проблемы синхронизации времени

Синхронизация времени – это обширная область, в последние несколько десятилетий ей были посвящены многие исследования, в которых предлагалось использовать несколько алгоритмов и механизмов.

Узел A отправляет сообщение узлу B со своим текущим временем, чтобы синхронизироваться с узлом B. Если доставка и получение сообщения не задерживаются, узел B может сразу же вычислить разницу во времени и скорректировать его в соответствии с показаниями узла A. Однако в реальной беспроводной сети на доставку сообщений влияют различные типы задержек, обусловленные описанными выше факторами, что значительно усложняет синхронизацию времени. Чтобы оценить относительные отклонения и смещения в показаниях часов на разных узлах, можно передавать серию синхронизирующих сообщений. Таким образом, синхронизацию времени можно рассматривать как процесс устранения задержек при передаче синхронизирующих сообщений.

Однако в БСС нецелесообразно использовать текущие методы синхронизации из-за уникальных характеристик БСС, таких как ограниченная мощность батареи, ограниченная доступная пропускная способность и ограниченные вычислительные ресурсы и объём памяти. Эти характеристики делают традиционные схемы синхронизации времени, т. е. сетевой временной протокол (NTP) и глобальную систему позиционирования (GPS), непригодными для БСС. Для достижения синхронизации времени необходимо учитывать следующие проблемы:

2.3.1. Недетерминированные задержки

Недетерминированные задержки при доставке сообщений и сложности с оценкой времени передачи напрямую влияют на проблемы, связанные с безопасной синхронизацией времени. Например, время доступа на физическом уровне может быть в разы больше, чем требуемая точность синхронизации в сети. Как показано на рисунке 1, задержки при доставке сообщений состоят из следующих компонентов:

время отправки (send time) – время формирования сообщения на прикладном уровне. Сюда также входят задержки, связанные с накладными расходами операционной системы и обработкой протокола;

время доступа (access time) – время, которое необходимо подождать после перехода на уровень управления доступом к среде (MAC), чтобы получить доступ к каналу передачи данных;

время передачи (transmission time) – время, необходимое для передачи сообщения на физическом уровне (PHY). Эта задержка является детерминированной и может быть рассчитана исходя из размера пакета;

время распространения (propagation time) – фактическое время передачи сообщения от отправителя к получателю. Эта задержка является детерминированной и зависит от расстояния, но в большинстве случаев она настолько мала, что ею можно пренебречь при оценке времени передачи;

время приёма (reception time) — время, необходимое для приёма сообщения на физическом уровне (PHY), которое совпадает со временем передачи сообщения;

время получения (receive time) — время, которое требуется получателю для формирования и отправки полученного сообщения на прикладной уровень.

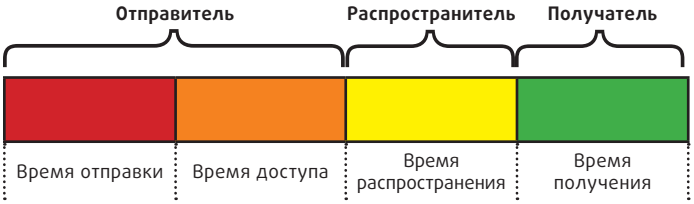


Рис. 1. Компоненты задержки пакетов.

2.3.2. Устойчивость к сбоям (Robustness)

Сенсорные сети остаются без присмотра на длительное время в условиях агрессивной среды. В случае выхода из строя некоторых узлов или нарушения связи оставшиеся узлы должны продолжать синхронизироваться. Мобильные узлы перемещаются, что может нарушить работу схем маршрутизации и привести к разделению сети на сегменты.

2.3.3. Скорость сходимости

Беспроводные сенсорные сети всегда состоят из большого количества сенсорных узлов, и два узла могут взаимодействовать друг с другом через множество промежуточных узлов, что затрудняет снижение скорости сходимости при разработке алгоритмов синхронизации времени. Эти проблемы необходимо тщательно проанализировать и устранить, чтобы избежать недетерминированной задержки при передаче радиосообщений, которая может повлиять на точность синхронизации времени. Помимо этих проблем, существует ряд требований, определяющих, какой метод синхронизации следует использовать.

2.4. Требования к синхронизации времени

Синхронизация времени важна для некоторых распределённых систем и для всех типов сетей. В других системах, особенно не зависящих от внешних факторов, синхронизация времени не требуется. В последнее время были предложены и стали использоваться различные механизмы и алгоритмы синхронизации времени, однако беспроводные сенсорные сети обладают рядом характеристик, из-за которых эти механизмы и алгоритмы не подходят для них. Например, из-за ограниченной ёмкости аккумуляторов и пропускной способности датчиков невозможно часто отправлять синхронизирующие сообщения, а миниатюрное оборудование снижает вычислительную мощность и объём памяти. Таким образом, традиционные методы синхронизации, такие как NTP и GPS, не подходят для БСС, поскольку их общие требования невозможно выполнить при ограниченных ресурсах. В предыдущем разделе мы проанализировали текущие проблемы, которые влияют на различные методы синхронизации времени и делают их непригодными для использования.

3. Текущие методы синхронизации времени

В последнее время были проведены ценные исследования по методам безопасной синхронизации времени. Некоторые результаты исследований описаны ниже.

3.1. Глобальная система позиционирования (GPS)

Глобальная система позиционирования — это навигационная система, основанная на 32 спутниках, которая изначально использовала 24 спутника, разработанная Министерством обороны США (DoD). Она предоставляет точную информацию о местоположении и времени при любой погоде, в любом месте на Земле или вблизи Земли, где есть прямая видимость трёх или более спутников GPS. Синхронизация времени GPS (рисунок 2) обеспечивает точность порядка 200 нс, но оборудование стоит дорого и потребляет много энергии. Кроме того, для правильной и точной работы хотя бы три спутника должны быть постоянно в прямой видимости. В настоящее время по крайней мере четыре спутника находятся в прямой видимости всё время, как показано на рисунке ниже; однако это может быть невозможно в некоторых случаях, например, внутри зданий или под водой.

Рис. 2. Синхронизация времени GPS.

Для обеспечения синхронизации времени устройства GPS принимают данные со спутников. Для этого требуется GPS-приёмник в каждом устройстве, что нецелесообразно, особенно для беспроводных устройств, из-за затрат на оборудование и ограничений по питанию. Узлы получают информацию о реальном времени от GPS и синхронизируются следующим образом. Каждый узел имеет свои собственные аппаратные часы; обозначим значение аппаратных часов узла i как $H_i(t)$.

Мы предполагаем, что аппаратные часы каждого узла имеют ограниченный дрейф ρ<11. Для всех узлов i:

$$\forall t : 1-\rho \leq \left(\frac{dH_i(t)}{dt}\right) \leq 1+\rho \quad (3)$$

где t — реальное время, d — расстояние, и ρ — ограниченный дрейф. Каждый узел вычисляет значение логических часов, используя свои аппаратные часы и полученное сообщение от других узлов. Отметим значение логических часов узла i в момент времени t как $L_i(t)$. Алгоритм синхронизации часов пытается убедиться, что логические значения узлов близки к реальному времени и близки к значениям друг друга.

Точность синхронизации времени GPS будет варьироваться в разное время, в зависимости от количества спутников, которые могут обмениваться данными с приёмником. Кроме того, требуется некоторое время для сообщения GPS, чтобы распространиться по всей сети. Например, сообщение GPS получено на узле i входным действием $gps(t)_i$. Цель сообщения — информировать i, что текущее реальное время есть t. Однако может потребоваться больше времени для сообщения, чтобы достичь узла i в большой сети, и узел i может получить это сообщение после реального времени t. Дорогостоящее оборудование, такое как GPS-приёмник, и высокие энергетические требования протокола GPS приводят к использованию увеличенной пропускной способности и вычислительной мощности, что делает его непригодным, потому что сенсоры имеют ограниченную мощность батареи, ограниченную доступную пропускную способность, ограниченное пространство хранения и ограниченную вычислительную мощность.

3.2. Протокол сетевого времени (NTP)

NTP использует несколько алгоритмов для уменьшения джиттера, повышения отказоустойчивости и предотвращения некорректной работы серверов, что позволяет ему обеспечивать точность менее десятков миллисекунд в глобальных сетях (WAN) и субмиллисекунд в локальных сетях (LAN).

Синхронизация узла A и узла B осуществляется путём обмена пакетами. Узел A хранит свое локальное время в пакете запроса T_1. Затем узел B ставит временную метку T_2 согласно текущему локальному времени по прибытии запроса и отправляет ответ T_3, который включает текущее локальное время отправления пакета. Когда Узел A получает ответ, он помечается как T_4, как показано на рисунке 3. Затем NTP вычисляет смещение часов и задержку кругового пути соответственно:

$$\text{offset} = \frac{(T_2 - T_1) + (T_3 - T_4)}{2} \quad (4)$$

$$\text{delay} = (T_4 - T_1) - (T_3 - T_2) \quad (5)$$

NTP не учитывает энергопотребление и постоянно нагружает процессор, чтобы синхронизировать работу генератора, что невозможно в случае с сенсорными узлами, потому что они имеют ограниченные ресурсы и не могут тратить весь цикл CPU на синхронизацию времени.

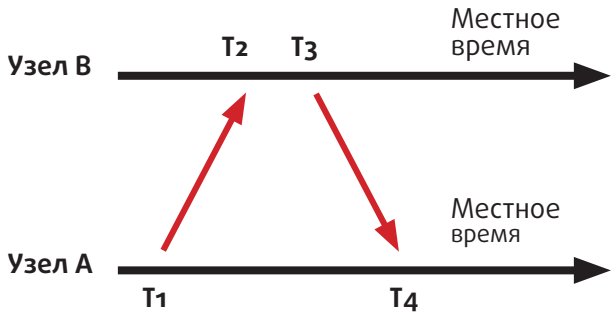


Рис. 3. Двустороннее «рукопожатие» между парой узлов.

3.3. Протокол синхронизации времени для сенсорных сетей (TPSN)

Протокол синхронизации времени для сенсорных сетей TPSN (Timing-Sync Protocol for Sensor Networks) был предложен Ганеривалом и его коллегами для синхронизации времени во всей сети. В модели TPSN используется структура «отправитель — получатель». Получатель синхронизирует свои часы с часами отправителя с помощью двустороннего подтверждения, как показано на рисунке 4:

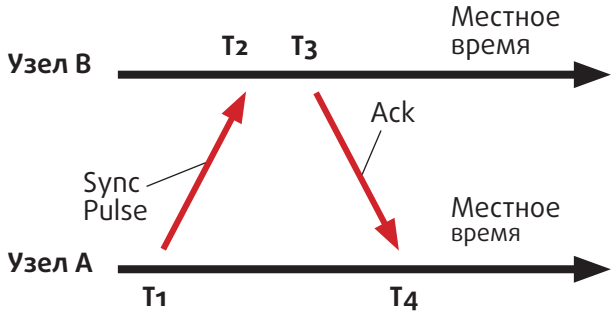


Рис. 4. Синхронизация между двумя узлами.

Узел A отправляет импульсный пакет в T_1, чтобы начать синхронизацию, которая включает его номер уровня и значение T_1 согласно его локальным часам. Узел B получает это сообщение в T_2, и $T_2=T_1+D+d$, где T_1 — сообщение от узла A, D — относительный дрейф часов между узлом A и узлом B, и d — задержка распространения импульса, отправленного между узлами. Узел B отправляет пакет подтверждения в момент времени T_3, который включает номер уровня узла B и значения T_1, T_2 и T_3. Узел A синхронизирует себя с узлом B после вычисления дрейфа часов и задержки распространения, как показано ниже:

$$D = \frac{(T_4 - T_1) - (T_3 - T_2)}{2} \quad (6)$$

$$\text{offset} = \frac{(T_2 - T_1) + (T_3 - T_4)}{2} \quad (7)$$

TPSN работает в две фазы: сначала фаза обнаружения, а затем фаза синхронизации. Цель первой фазы — присвоить уровень каждому узлу и создать иерархическую топологию в сети. Только корневому узлу присваивается уровень 0, как показано ниже на рисунке 5.

Во второй фазе все узлы подключаются к родительскому узлу в иерархической структуре через сообщение двустороннего «рукопожатия», аналогично NTP, показанному

выше. Таким образом, все узлы синхронизируются с корнем, и синхронизация всей сети достигается за счёт двусторонней передачи сообщений о подтверждении между узлами A и B, как показано на рисунке 4.

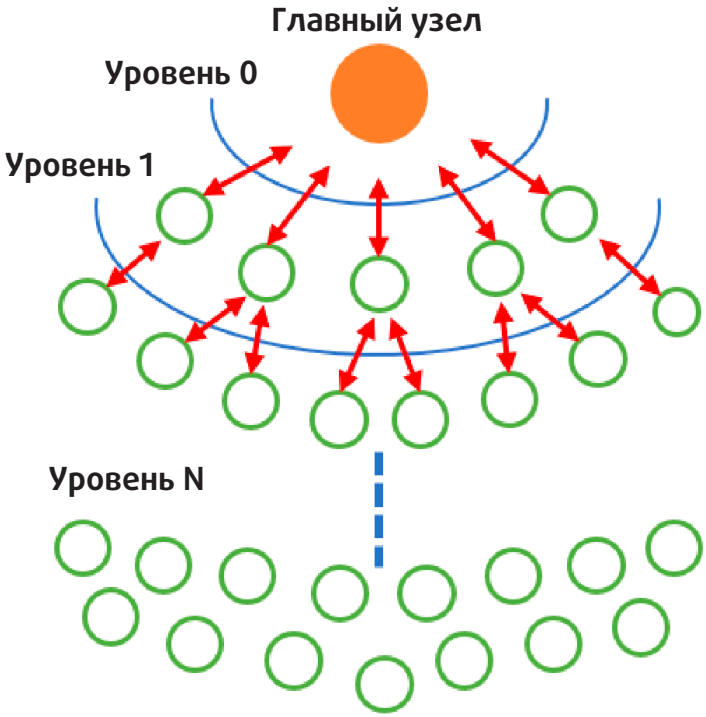


Рис. 5. Иерархическая структура.

Синхронизация зависит от родителей узлов в иерархической структуре; поэтому высокая точность синхронизации может быть достигнута даже при увеличении размера сети. Однако в случае отказа обслуживание этой структуры увеличивает энергопотребление. Поскольку связность узла в иерархической структуре меняется, когда узел перемещается, структура должна быть сформирована соответственно, так как в TPSN узел корректирует свои часы согласно своему родительскому узлу. Эти сложности обслуживания и высокое энергопотребление делает TPSN непригодным для безопасной синхронизации времени, потому что в БСС узлы могут постоянно перемещаться.

3.4. Протоколы Tiny-Sync и Mini-Sync

Сичитиу и Вирариттифан в статье «Простая и точная синхронизация времени для беспроводных сенсорных сетей», опубликованной в 2003 году в сборнике трудов конференции IEEE Wireless Communications and Networking, предложили два легковесных алгоритма синхронизации, т.е. tiny-sync и mini-sync. Чтобы получить смещение и разницу скоростей между двумя узлами, как алгоритм tiny-sync, так и алгоритм mini-sync используют технику измерения времени множественного кругового пути и технику линейной аппроксимации. Множественные круговые пути выполняются для получения точек данных для линейной аппроксимации, как показано на рисунке 6, где узел A является клиентом, а узел B - эталоном.

В этой же статье было высказано предположение, что узел A ставит временную метку на сообщении с t_o и отправляет его узлу B. Узел B ставит временную метку на сообщении с t_b, как только получает его, и отправляет его обратно узлу A,

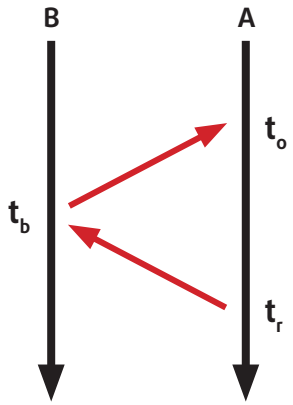


Рис. 6. Расчёт точек данных.

который получает сообщение и ставит временную метку с t_r, как показано на рисунке 6.

Каждое измерение кругового пути приводит к точке данных (t_b,[t_o,t_r]), которая эффективно ограничивает возможные значения параметров a_{12} и b_{12}. Поскольку t_o произошло до t_b, и t_b произошло до t_r, следующие неравенства должны выполняться:

$$t_0(t) < a_{12}t_b(t) + b_{12} \quad (8)$$

$$t_r(t) > a_{12}t_b(t) + b_{12} \quad (9)$$

Описанные выше вычисления повторяются несколько раз, и данные всех временных точек сохраняются. Две линии с минимальным и максимальным наклоном определяются с использованием техники линейной аппроксимации, которая предоставляет нам границы для относительного смещения и разницы скоростей двух узлов, используя их наклон и ось. Линия, которая имеет средний наклон и пересечение, используется для определения смещения и разницы в скорости между этими двумя узлами.

Протоколы tiny-sync и mini-sync используют метод оценки для предоставления решения относительного дрейфа и относительного смещения, что уменьшает сложность и энергопотребление; однако это требует более высоких вычислительных ресурсов и памяти для генерации точных результатов. Вычислительные ресурсы и память зависят от количества точек данных. Меньшее количество точек данных предоставляет субоптимальное решение, тогда как большее количество точек данных предоставляет оптимальное решение, но занимает большое количество памяти и вычислительных ресурсов. Миниатюризированные современные технологии имеют меньше памяти и меньше доступных вычислительных ресурсов, что делает этот алгоритм непригодным для них.

3.5. Протокол облегчённой синхронизации времени (LTS)

Основной фокус протокола облегчённой синхронизации времени (LTS) — минимизировать энергетические затраты путём уменьшения накладных расходов, оставаясь при этом надёжным и самоконфигурирующимся. Облегчённая синхронизация времени строит древовидную структуру внутри сети для обеспечения общесетевой синхронизации. Основная функция

протокола заключается в том, что он продолжает работать эффективно, даже если есть отказ узла. Он направлен на максимизацию точности при минимизации сложности синхронизации и использования вычислительных ресурсов. Предполагается, что требуемая точность в сенсорных сетях низкая; поэтому целесообразно использовать легковесную схему синхронизации. Однако в некоторых приложениях, таких как измерение времени прохождения звука, распределение акустического формирования диаграммы направленности, обнаружение оползней, предотвращение стихийных бедствий и обнаружение лесных пожаров, требуется высокоточная синхронизация времени. Кроме того, при увеличении размеров сети точность синхронизации уменьшается линейно, например, от корневого узла к листовому узлу точность уменьшается. Рисунок 7 объясняет, как выполняется синхронизация LTS.

Протокол попарной синхронизации LTS использует технику удалённого чтения часов для синхронизации двух соседних узлов. Например, узел i хочет синхронизировать свои часы с узлом j. Узел i отправляет сообщение запроса синхронизации, и когда синхронизация запускается, сообщение помечается временем $C_i(t_1)$. После задержки при доступе к среде с произвольным доступом узел i отправляет пакет в момент времени t_2, и узел j получает его в момент времени $t_3=t_2+\tau+t_p$, где τ — задержка распространения, и t_p — время передачи пакета. В момент времени t_4 прибытие пакета сигнализируется прерыванием и помечается временем t_5 с $C_j(t_5)$, за которым следует пакет ответа, помеченный временем $C_j(t_6)$ в момент времени t_6 (также включает предыдущие временные метки $C_j(t_5)$ и $C_i(t_1)$).

Узел i получает пакет ответа в t_7 и помечает его временем $C_i(t_8)$ в момент времени t_8. Узел i предполагает, что нет дрейфа часов между t_1 и t_8, $O=\Delta(t^*)$ для всех $t^* \in [t_1, t_8]$ и оценивает смещение O путём оценки $\Delta(t_5)$ следующим образом:

$$O = \Delta(t_5) := C_i(t_5) - C_j(t_5) \quad (10)$$

Однако t_5 является неизвестной величиной между t_1 и t_8. Неопределённость можно уменьшить, как видно из приведённого выше рисунка, где показано время распространения τ и время передачи t_p между t_1 и t_5 , а также между t_5 и t_8. Мы предполагаем, что оно одинаково в обоих направлениях. Поскольку у нас есть t_5 и t_6, мы можем получить разницу как $C_j(t_6)$-$C_j(t_5)$. Мы также предполагаем, что операционная система, доступ к каналу, прерывание и задержка доступа к среде тоже одинаковы в обоих направлениях, как показано на рисунке 7. Поэтому $C_j(t_5)$ генерируется в момент времени:

$$C_i(t_5) = \frac{C_i(t_1) + \tau + t_p + C_i(t_8) - \tau - t_p - (C_j(t_6) - C_j(t_5))}{2} \quad (11)$$

Поэтому смещение O равно:

$$= \Delta(t_5) = C_i(t_5) - C_j(t_5) \quad (12)$$
$$= \frac{C_i(t_8) + C_i(t_1) - C_j(t_6) - C_j(t_5)}{2}$$

Узел i может корректировать свои часы, добавив смещение O, потребовалось только два пакета для синхронизации узла i и узла j. Третий пакет от узла i к узлу j может быть использован, включая O, если цель состоит в том, чтобы узел j знал о смещении.

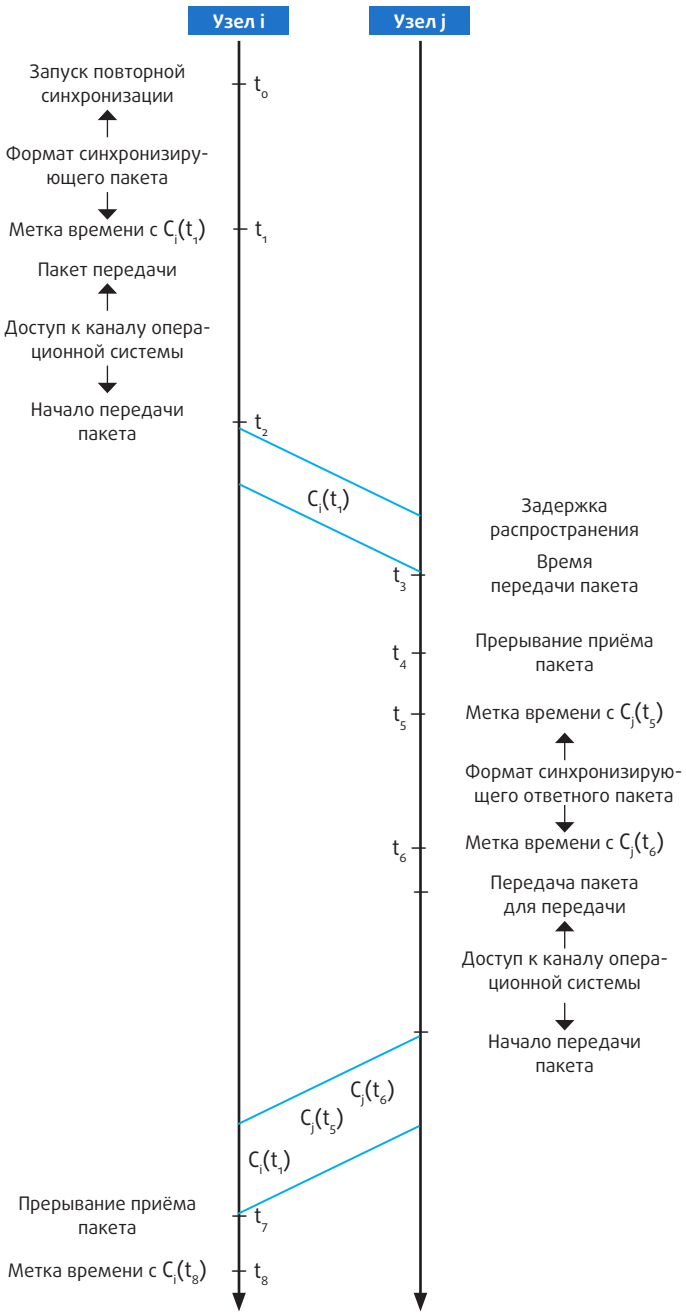


Рис. 7. Попарная синхронизация LTS.

После обеспечения попарной синхронизации протокол LTS решает синхронизацию всех узлов с опорным узлом. Для этой цели предложены два разных подхода, т.е. централизованный подход и распределённый подход.

В централизованном подходе строится связующее дерево, и затем синхронизируются узлы. Опорный узел является корневым узлом связующего дерева и отвечает за запуск синхронизации сети. Корневому узлу передаётся информация о глубине связующего дерева, поскольку она влияет на время синхронизации всей сети, а значит, эту информацию можно использовать для определения времени повторной синхронизации. Важнейшим фактором здесь являются затраты на передачу данных, поскольку для попарной синхронизации требуется три пакета, а синхронизация всей сети потребует количества пакетов, равного числу узлов, умноженному на 3, что увеличивает энергопотребление при построении связующего дерева.

В распределённом подходе структура связующего дерева не

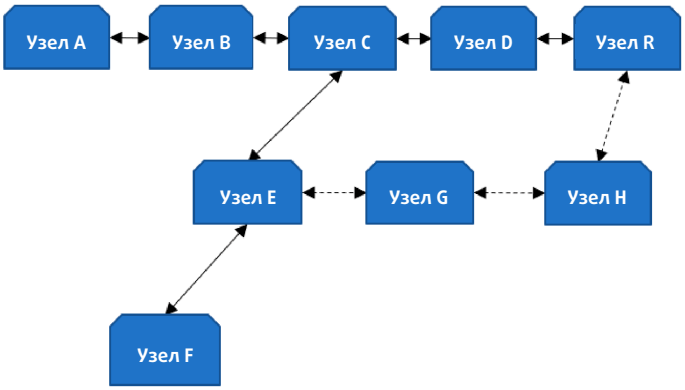


Рис. 8. Многоступенчатая синхронизация.

используется, и каждый узел может решать время своей собственной синхронизации. Когда любой узел, такой как узел A, нуждается в синхронизации, он отправляет запрос синхронизации своему ближайшему опорному узлу, как показано на рисунке 8.

По пути от опорного узла к узлу A должны быть синхронизированы все узлы, что позволяет избежать ненужной частой синхронизации. Поскольку синхронизировать нужно все узлы - от опорного до узла-инициатора, можно отправить коллективный запрос на синхронизацию, чтобы сократить количество используемых ресурсов.

3.6. Протокол потоковой синхронизации времени (FTSP)

Протокол потоковой синхронизации времени (FTSP) был предложен Мароти и соавторами в статье «Протокол синхронизации времени распространения сигнала», опубликованной в 2004 году в сборнике трудов 2-й Международной конференции по встроенным сетевым сенсорным системам, Балтимор, Мэриленд, США. Его цель — добиться синхронизации во всей сети путём отправки широковещательных синхронизирующих сообщений. Широковещательное сообщение начинается с преамбулы, за которой следуют байты Sync, затем — фактические данные сообщения, описывающие его, и завершаются они байтами CRC. Пунктирными линиями на рисунке 9 обозначены фактические байты, а сплошными — байты в буфере. Когда отправитель передаёт преамбулу, получатель настраивает несущую частоту входящих сигналов. Как только получены байты Sync, получатель может вычислить смещение байтов, необходимое для восстановления сообщения с правильным выравниванием байтов. В поле данных содержится адрес назначения, длина данных и другие поля сообщения, о которых необходимо уведомить получателя. Сообщение проверяется на целостность с помощью байтов CRC.

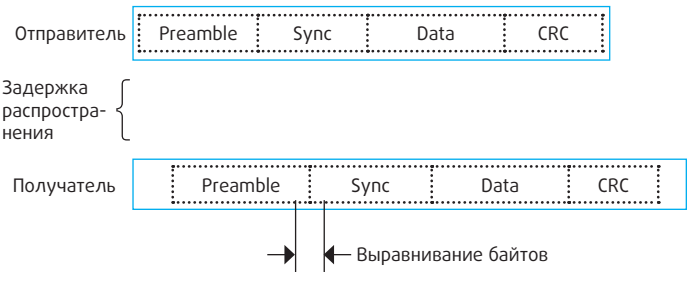


Рис. 9. Вещательное сообщение FTSP.

В протоколе FTSP узлы могут образовывать ячеистую сеть, в которой каждый узел отправляет сообщение о синхронизации всем остальным узлам, или звездообразную сеть, в которой один из узлов выступает в роли ведущего, а все остальные — в роли ведомых. Узел с наименьшим идентификатором выбирается в качестве ведущего, который периодически рассылает по сети сообщения о синхронизации и служит источником эталонного времени. В случае выхода из строя текущего ведущего узла новым ведущим узлом становится следующий узел с наименьшим идентификатором. Каждый узел собирает временные метки и данные о времени поступления, а на основе этих данных с помощью линейной регрессии вычисляются смещение и разница в скорости передачи данных с ведущим узлом. Протокол FTSP обеспечивает глобальную синхронизацию при низкой пропускной способности и использует временные метки на уровне MAC, что позволяет исключить многие источники ошибок. Однако для работы протокола необходим доступ к аппаратному обеспечению, и он не является чисто программным протоколом. Главный недостаток протокола заключается в том, что любой узел может объявить себя ведущим по истечении определённого периода времени, если он не получил новых временных меток, что делает его уязвимым для атак. Злонамеренный узел может объявить себя ведущим и ввести в заблуждение другие узлы, нарушив синхронизацию с настоящим ведущим узлом.

3.7. Протокол эталонной широковещательной синхронизации (Reference Broadcast Synchronization, RBS)

Протокол эталонной широковещательной синхронизации был предложен Элсоном, Жиро и Эстрином в 2002 году. Почти все остальные протоколы синхронизации используют метод синхронизации «от отправителя к получателю». Однако протокол RBS работает по-другому: в нём используется метод синхронизации «от получателя к получателю» с привлечением третьей стороны. Суть метода в том, что третья сторона отправляет двум получателям один широковещательный сигнал, который не содержит никакой информации о времени или временных метках. Получатели обмениваются данными о времени получения этого сигнала и о разнице в показаниях своих часов. Например, как показано на рисунке 10, опорный узел R отправляет сообщение синхронизации всем ведомым узлам. Два узла, узлы A и B, находятся в зоне действия узла R и получают это сообщение. Времена приёма сообщения записываются как T_a на узле A и T_b на узле B.

Узлы A и B обмениваются этой временной информацией друг с другом, узел B вычисляет разницу во времени с узлом A и записывает её с помощью переменной d следующим образом:

$$d = T_a - T_b \quad (13)$$

После этого узел B может скорректировать своё время для синхронизации с узлом A, используя d следующим образом:

$$T_b = T_a - d \quad (14)$$

Полученной информации достаточно для поддержания локальной шкалы времени. Таким образом, время отправки и время доступа исключаются из критического пути, как показано на рисунке 11.

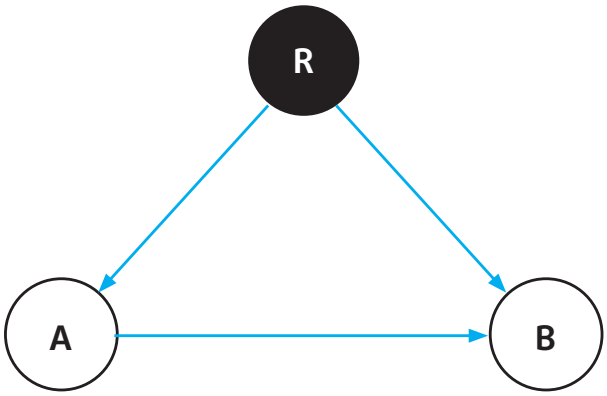


Рис. 10. Обмен сообщениями протокола RBS.

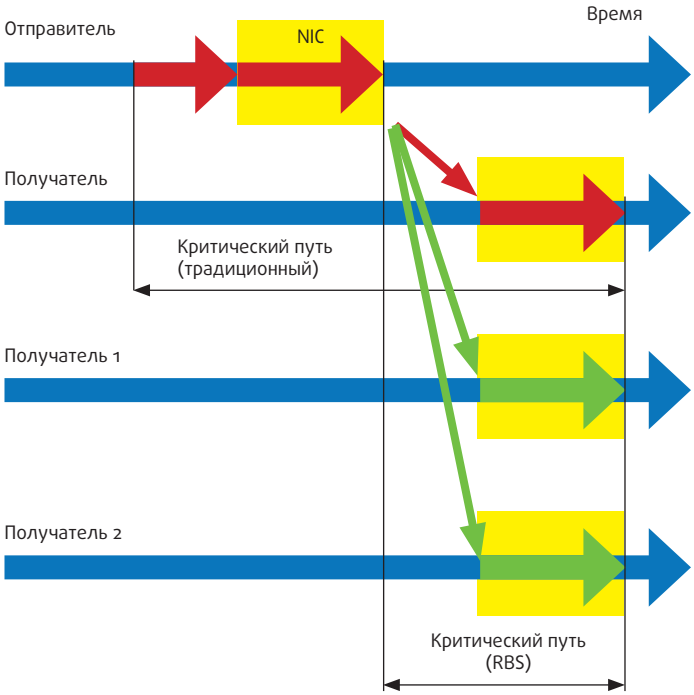


Рис. 11. Анализ критического пути (протокол RBS).

В протоколе RBS третья сторона отправляет широковещательный сигнал, что позволяет легко подменять узлы и блокировать передачу информации от реальных отправителей. Кроме того, из-за больших накладных расходов при обмене пакетами этот протокол потребляет больше энергии, что делает его небезопасным и непригодным для сетей с низким энергопотреблением. Приведённая выше информация свидетельствует о том, что безопасность не была главным приоритетом при разработке существующих протоколов. Эту проблему можно решить, снизив накладные расходы на передачу данных, что уменьшит энергопотребление, а сэкономленную энергию можно будет направить на обеспечение безопасности. В следующих разделах мы рассмотрим суть проблемы и изучим аналогичные исследования, проведённые ранее, чтобы найти подходящее решение.

3.8. IEEE 1588 (PTP)

Первая версия протокола точной синхронизации IEEE 1588 (PTP) была выпущена в 2002 году, а вторая — в 2008 году. Это прикладной протокол, основанный на архитектуре «ведущий — ведомый» и предназначенный для обеспечения высокой точности и надёжной процедуры синхронизации. Этот протокол позволяет осуществлять синхронизацию с точностью до наносекунды. По сравнению с ранее упомянутыми протоколами, такими как GPS и NPT, PTP обеспечивает более надёжную синхронизацию времени. Протокол IEEE 1588 PTP позволяет синхронизировать время по сетям пакетной передачи, таких как Ethernet. Для точной синхронизации сети необходимо обмениваться пакетами с метками времени между распределёнными узлами.

3.9. Сравнительный анализ различных протоколов синхронизации времени

NTP — это протокол синхронизации времени, широко используемый в Интернете. Клиенты NTP используют статистический анализ времени прохождения сигнала в обе стороны для синхронизации своих часов с серверами NTP с точностью до миллисекунд. Для синхронизации серверов времени используются внешние источники, например GPS. Доказано, что протокол NTP эффективен, безопасен и надёжен в Интернете, поэтому он широко распространён. Однако в беспроводных сенсорных сетях время передачи данных может варьироваться, поскольку на каждом этапе управления доступом к среде передачи (MAC) может возникать задержка в несколько сотен миллисекунд.

Был предложен протокол синхронизации по широковещательной рассылке, в котором используется синхронизация между приёмниками, а не между отправителем и приёмником, как во многих других протоколах. Идея заключается в том, чтобы отправлять маячок с помощью третьей стороны без какой-либо информации о времени, а приёмники будут сравнивать время получения этого маячка со своим смещением. Таким образом, остаётся только два фактора неопределённости: время распространения сигнала и время получения. Утверждается, что все узлы сразу же получат опорный маячок, что исключает влияние времени распространения сигнала, но в протоколе всё равно остаётся неопределённость, связанная со временем получения сигнала.

Ганеривал и соавторы в статье «Безопасная служба синхронизации времени для сенсорных сетей», опубликованной в 2008 году в сборнике трудов 4-го семинара ACM по беспроводной безопасности, предложили традиционный протокол синхронизации времени на основе взаимодействия отправителя и приёмника под названием «Протокол синхронизации времени для сенсорных сетей» (timing-sync protocol for sensor networks, TPSN). Он разделён на два этапа. На первом этапе создаётся иерархическая топология сети, в которой каждому узлу присваивается уровень, а узел с самым низким уровнем становится корневым узлом. На втором этапе все узлы в дереве синхронизируются со своим родительским узлом с помощью метода синхронизации по времени прохождения сигнала в обе стороны.

Протокол синхронизации времени по широковещательной рассылке (FTSP) был предложен Мароти и соавторами и является наиболее известным подходом к синхронизации времени. Для достижения относительно высокой точности в нём используются высокоточные часы, оценка дрейфа часов и временная маркировка на уровне MAC для снижения джиттера.

Протоколы tiny-sync/mini-sync используют несколько попарных измерений времени прохождения сигнала в обе стороны и ме-

тод аппроксимации прямой линии для определения смещения и дрейфа двух узлов, а не для непосредственного расчёта смещения.

Протокол IEEE 1588 PTP точнее, чем NTP. Кроме того, в протоколе PTP главный сервер синхронизирует все подчинённые узлы, что позволяет избежать дополнительной задержки, возникающей при перераспределении данных в протоколе NTP. Протоколы NTP и PTP сложно использовать в беспроводных сетях из-за ограниченности ресурсов и асимметрии каналов связи.

Большинство существующих протоколов используют определённые опорные тактовые частоты и иерархическую структуру, однако при использовании опорных тактовых частот учитывается только компенсация смещения тактовой частоты, что делает протоколы более уязвимыми для интеллектуальных атак и сбоев в работе отдельных узлов.

Для сравнения характеристик различных протоколов мы выбрали несколько наиболее показательных. Для всестороннего сравнения и анализа характеристик мы выбрали различные конфигурации тактовых частот (1 МГц, 50 МГц, 32,678 МГц и 32,678 кГц) с разными отклонениями, а также аппаратные тактовые частоты (на платформе MICAz или на платформе FPGA) и тактовые частоты, полученные в результате моделирования. На рисунке 12 в виде гистограммы представлено сравнение максимальных ошибок синхронизации времени в различных протоколах. Синие и красные столбцы соответствуют результатам оценки протоколов PISync и FTSP на аппаратной платформе MICAz, а оранжевые и фиолетовые столбцы — результатам экспериментальной оценки протоколов PISync и DCBTS на тестовом стенде с FPGA. Кроме того, для оценки характеристик протоколов PISync, D-PkCO и TPSN использовался симулятор на базе MATLAB. Результаты моделирования представлены зелёными, чёрными и коричневыми столбцами соответственно.

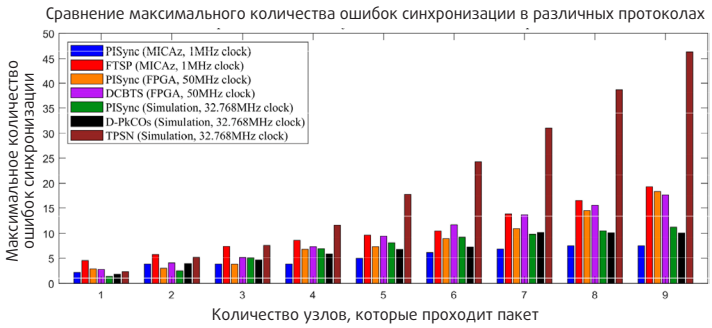


Рис. 12. Сравнение точности синхронизации времени при использовании различных протоколов в многоузловой сенсорной сети. Для всестороннего сравнения используются различные конфигурации часов, включающие как результаты аппаратных тестов, так и результаты моделирования.

В целом неудивительно, что все протоколы демонстрируют рост ошибок синхронизации при увеличении расстояния между узлами, но с разной скоростью. При тактовой частоте аппаратного обеспечения 1 МГц на широко известной платформе беспроводных сенсорных сетей MICAz протокол PISync обеспечивает наилучшую точность синхронизации с наименьшей скоростью роста ошибок в зависимости от расстояния между узлами. Например, при одном переходе задержка составляет 2 мкс, а при девятом — около 7 мкс, что лучше, чем у давно существующего протокола FTSP. Однако при тактовой частоте аппаратного обеспечения FPGA 50 МГц задержка при использовании PISync увеличивается до 3 мкс при одном переходе и до 17 мкс при девятом, а результаты, полученные с помощью DCBTS, немного лучше, чем у PISync, несмотря на то, что тактовая частота стала выше. Аналогичные результаты были получены при моделировании на тактовой частоте 32,768 МГц. Возможно, это связано с тем, что использовалась более качественная конфигурация тактового генератора с частотой 1 МГц (например, очень стабильный генератор с минимальными отклонениями), но в реальных и смоделированных генераторах отклонения были выше. Для объективного сравнения необходимо учитывать больше факторов, связанных с платформой и тактовой частотой.

4. Заключение

Результаты исследования показали, что почти все существующие протоколы синхронизации времени имеют ошибки, и эти ошибки характерны для некоторых популярных протоколов. Протокол LTS не подходит для обеспечения высокой точности, поскольку его точность снижается по мере удаления от корневого узла, в то время как протокол FTSP обеспечивает высокую точность и устойчивость к сбоям в работе узлов и изменениям топологии. Однако протокол FTSP требует больших энергозатрат и вычислительных ресурсов (которые ограничены для сенсорных узлов), поскольку он не является программным протоколом. Протокол RBS предполагает большое количество обменов сообщениями для обеспечения высокой точности, что увеличивает энергопотребление и, соответственно, затраты. Протокол TPSN обеспечивает точность до 10 микросекунд, которая зависит от величины смещения, влияющего на время распространения сигнала. Несмотря на то, что в этих протоколах недетерминированная задержка, вызванная распространением сигнала, ограничена по сравнению с достижимой точностью, для обеспечения требуемой точности каждому протоколу необходимо отправлять и получать пакеты данных. Отправка и получение пакетов данных потребляют большую часть энергии при сетевой синхронизации. Энергопотребление сети можно снизить, уменьшив количество обменов пакетами данных. В рамках дальнейшей работы необходимо устранить эти ошибки, чтобы добиться лучших результатов при использовании этих протоколов. Синхронизация времени играет важнейшую роль в концепции «Индустрия 4.0» и «Здравоохранение 4.0», а безопасная синхронизация времени является одним из ключевых компонентов. Для приложений, работающих в рамках концепции «Индустрия 4.0» или «Здравоохранение 4.0», внедрение безопасной синхронизации времени должно гарантировать высокую точность синхронизации, чтобы удовлетворять потребности приложений в обмене данными в режиме реального времени. Кроме того, она должна предотвращать атаки и обеспечивать безопасность связи. Весьма перспективным подходом является интеграция синхронизации времени с технологией блокчейн.

Об авторах:

Ин Вэн и Имин Чжан — сотрудники Школы компьютерных наук, факультет естественных и инженерных наук Ноттингемского университета в Нинбо, Китай

Основные подходы к частотно-временному обеспечению (синхронизации)

Юрий Миронов

Аннотация
В предметной области к настоящему времени активно используется целый ряд протоколов синхронизации, среди которых можно выделить наиболее распространённые: NTP, PTP, SyncE, IRIG-B и др.
В зависимости от конкретной ситуации используются различные протоколы синхронизации, которые обеспечивают требуемую степень точности и надёжности передачи данных, а также учитывают специфику работы с конкретными устройствами и системами. Сетевые элементы инфокоммуникационных систем, наряду с автоматизированными средствами управления, информационно-аналитическими системами, цифровыми средствами расчётных финансовых инструментов, виртуализации и т.д., имеют различные требования к временной синхронизации, невыполнение которых приводит к нарушению функционирования, а иногда отказу соответствующего оборудования или системы в целом. В настоящей статье производится обобщение, анализ и систематизация существующих подходов к частотно-временному обеспечению (синхронизации).

Ключевые слова:
частотно-временное обеспечение, синхронизация, телекоммуникационные сети

Основные подходы обеспечения синхронизации

На сегодняшний день в телекоммуникационных сетях активно используются несколько протоколов синхронизации [1], среди которых можно выделить наиболее распространённые: NTP (Network Time Protocol) [2], PTP (Precision Time Protocol) [3], Sync Ethernet (Synchronous Ethernet) [4-6], IRIG-B [7] и сигнал 1PPS [8].

В зависимости от требований потребителя используются различные протоколы синхронизации, которые обеспечивают требуемую степень точности и надёжности передачи данных, а также учитывают специфику работы с конкретными устройствами и системами.

NTP представляет собой сетевой протокол, предназначенный для синхронизации внутренних часов компьютера через сети с переменной латентностью. Основанный на алгоритме Марзулло [9] и использующий протокол UDP, NTP обеспечивает устойчивость к изменениям латентности среды передачи. В четвёртой версии протокол NTP достигает точности 10 мс при работе через Интернет и 1 мс внутри локальных сетей [10, 11].

Протокол PTP изначально был определён в стандарте IEEE 1588-2002 и предназначен для синхронизации часов по компьютерной сети [12]. На данный момент существует три версии данного протокола: PTPv1 [12], PTPv2 [13], PTPv2.1 [14]. Точность протокола PTP зависит от архитектуры сети и интенсивности сетевого трафика. Программные реализации PTP позволяют передавать сигналы синхронизации с точностью порядка 100 мкс. При программно-аппаратной реализации можно добиться точности порядка 20 нс. В случае полной аппаратной реализации протокола PTP точность составляет порядка 10 нс [15].

Synchronous Ethernet (SyncE) является стандартом Международного союза электросвязи (МСЭ, ITU) для компьютерных сетей, который обеспечивает синхронизацию путём передачи тактовых импульсов на физическом уровне Ethernet. SyncE был стандартизирован МСЭ-Т в сотрудничестве с IEEE в виде трёх рекомендаций: ITU-T Rec. G.8261 [16], ITU-T Rec. G.8262 [17], ITU-T Rec. G.8264 [18]. Механизм синхронизации сети SyncE основан на иерархии тактовых генераторов. В корне иерархического древа тактовых генераторов расположен наиболее точный (по сравнению с другими используемыми генераторами) генератор. Практически во всех сетях SyncE самый точный генератор представлен PRC-генератором (Primary Reference Clock, первичный эталонный генератор, который используется для построения сети синхронизации) с точностью 10–11 Гц [19].

IRIG-B – промышленный стандарт GPS-синхронизации, разработанный компанией Inter-Range Instrumentation Group. Этот стандарт может применяться на объектах энергетики для контроля качества и стабильности процессов. В этом случае последовательность событий с временной синхронизацией записывается с шагом 1 мс. Коды временной синхронизации IRIG-B могут быть переданы только по выделенным физическим каналам типа витой пары или коаксиальных кабелей. IRIG-B также требует внешнего источника точного времени. Точность передаваемых значений точного времени лежит в микросекундном диапазоне. С помощью кодов IRIG-B коммерческие устройства синхронизируются с точностью до 1 мкс [7].

Технология 1PPS (Pulse Per Second) основана на сигнале временной синхронизации, который означает начало каждой секунды. Сигнал 1PPS передаётся потребителю по выделенной линии. Потребители не могут с помощью 1PPS получить информацию по дате и времени, поэтому его чаще используют совместно с другими протоколами синхронизации. Точность сигналов PPS сильно варьируется в зависимости от источника: приёмники ГНСС (глобальная навигационная спутниковая система) обеспечивают погрешность от нескольких десятков до сотен наносекунд, в то время как высокостабильные атомные часы поддерживают точность пикосекундного диапазона [20]. IRIG-B и 1PPS считаются стандартными протоколами для прямой синхронизации, т.е. работают только при прямом подключении к серверу времени по выделенному каналу связи.

Основные потребители синхронизации и их требования

Основными потребителями синхронизации являются сети связи, системы часофикации, автоматизированные системы управления, автоматизированные рабочие места информационных и информационно-управляющих систем, автоматизированные системы расчётов, оборудование тарификации и т.д. [21]. Перспективным потребителем синхронизации является наземный беспилотный транспорт. Но на данный момент отдельных стандартов по точности синхронизации таких потребителей нет, и используется существующая инфраструктура синхронизации (ГНСС). Следовательно, требования к точности синхронизации шкал времени аналогичны требованиям к GPS/ГЛОНАСС.

Пределы допускаемой абсолютной погрешности при измерении разности (расхождения) шкал времени в диапазоне от 10-7 до 8,64·104 с [22] относительно национальной шкалы времени Российской Федерации UTC(SU) не должны превышать ± 60 мс для протокола NTP. Для протокола PTP расхождение шкал времени не должно превышать ± 10 мкс. Пределы допускаемой абсолютной погрешности смещения собственной шкалы времени (ШВ) относительно ШВ UTC(SU) в режиме синхронизации по сигналам ГНСС ГЛОНАСС/GPS не должны превышать ± 1 мкс в диапазоне от 10-7 до 8,64·104 с, при этом реальные значения точности синхронизации шкал времени составляют порядка 10 нс при использовании дифференциальных технологий и порядка 100 пс при использовании технологии PPP (Precise Point Positioning) [23].

Для обеспечения работы основных подсистем сетей связи 4G, 5/6G необходима подсистема частотно-временной синхронизации. К этой подсистеме предъявляются требования по точности синхронизации ШВ – не выше 1,5 мкс по отношению к ШВ UTC для сетей 4G и 65-150 нс для сетей 5/6G [24-29].

Для служб предоставления услуг, основанных на определении текущего местоположения мобильного телефона, и некоторых реализаций LTE-A требования к точности временной синхронизации составляют порядка 100 нс [30].

Отдельные требования предъявляются к точности синхронизации в средствах автоматизации управления воздушным движением. В России данные требования закреплены в [31]. По данному стандарту погрешность синхронизации шкалы времени средств обработки информации наблюдения (СОИН) не должна превышать 5 мс.

В финансовом секторе для обеспечения синхронизации используется протокол точного времени PTP. Точность синхронизации в данном случае регламентируется MiFID 2 (Директива о рынках финансовых инструментов 2014 г.) [32]. Для высокочастотной алгоритмической торговли допустимое отклонение от UTC – не более 100 мкс.

В энергетическом секторе в качестве примера рассматриваются требования по точности синхронизации шкал времени ПАО «Россети Московский регион». В [33] в качестве требований указано обязательное требование по использованию протокола SNTP v3+. В настоящее время актуальная версия данного протокола SNTP v4. Согласно [2] точность синхронизации составляет 1-10 мс.

Заключение

В настоящее время в качестве основного источника сигнала синхронизации используются сигналы ГНСС, таких как ГЛОНАСС, GPS Navstar, Galileo и BeiDou. Параллельно с этим развиваются региональные навигационные спутниковые системы (региональные НСС), такие как QZSS (Япония), IRNSS (Индия) [34]. Кроме того, в качестве источника эталонного времени используются атомные часы – например, они применяются в Государственном первичном эталоне единиц времени, частоты и национальной шкалы времени (ГЭВЧ), от сигналов рабочих шкал которого работают NTP-серверы Всероссийского научно-исследовательского института физико-технических и радиотехнических измерений (ВНИИФТРИ) Росстандарта.

Но, несмотря на широкое распространение и длительную эксплуатацию, ГНСС имеют ряд уязвимостей. Основываясь на исследовании «Лаборатории Касперского» [35], можно выделить следующие уязвимости: подавление спутникового сигнала, перекрытие сигнала большими конструкциями, подделка спутникового сигнала (спуфинг), физические атаки на спутник (маловероятно) и на приёмники ГНСС. Реализация описанных уязвимостей может привести к нарушению работы ГНСС, что негативно повлияет на функционирование значительной части критически важной инфраструктуры страны. Наряду с уязвимостями на функционирование ГНСС может оказывать влияние космическая погода [36].

За последнее время участились случаи нарушения работы ГНСС [37-42]. Так, авиационная ассоциация Eurocontrol сообщает о 3500 сообщений о нарушении работы ГНСС в 2019 году. По данным компании SiTime минимум 100 тысяч случаев отказа в доступе к GPS происходит ежегодно: 27 апреля 2024 года два самолёта финской авиакомпании Finnair не смогли приземлиться в городе Тарту из-за сбоев в работе GPS [39]. Аналитическая компания RTI International [40] подсчитала предварительные убытки при глобальном сбое в работе GPS в течение одних суток. Потери в экономике составят порядка $1 миллиарда [41]. В октябре 2024 года была нарушена работа 120 из 140 российских NTP-серверов [42]. Причиной нарушения стала новая прошивка умных колонок серии «Станция» компании «Яндекс», которая перегружала запросами NTP-серверы. Отсутствие своевременного вмешательства привело к тому, что к 23-24 ноября этого года в Сети осталось всего четыре сервера. Данная статистика обуславливает целесообразность разработки и испытаний альтернативных способов доставки сигналов синхронизации конечным потребителям.

Источники:

[1] Воробьёв, А.С. Тенденции развития оборудования сетевой синхронизации / А.С. Воробьёв, Н.Л. Сторожук // Радионавигация и время. – 2022. – Т. 10, № 18. – С. 29-34.

[2] RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification. RFC Editor, USA. – DOI: 10.17487/RFC5905.

[3] EEE Std 1588-2008: IEEE Standard for A PrecisionClock Synchronization Protocol for Networked Measurementand Control Systems, 2008.

[4] ITU-T Recommendation G.8261: Timing and synchronization aspects in packet networks, 2008.

[5] ITU-T Recommendation G.8262: Timing characteristic of equipment clocks, 2008.

[6] ITU-T Recommendation G.8264: Distribution of timing information through packet networks, 2008.

[7] IRIG STANDARD 200-04. – URL: https://www.irigb.com/pdf/wp-irig-200-04.pdf (дата обращения 09.03.2026).

[8] L. Mengtong and T. Linwei, "Synchronization Technology and System Based on 1 Pulse Per Second Signal", 2021 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xi'an, China, 2021, pp. 1-5, DOI: 10.1109/ICSPCC52875.2021.9565027.

[9] Marzullo, K. Maintaining the time in a distributed system. / K. Marzullo, S. Owicki // PODC '83: Proceedings of the second annual ACM symposium on Principles of distributed computing. – 1983. – С. 295-305. – DOI: 10.1145/800221.806730.

[10] The NTP FAQ and HOWTO. – URL: http://ntp.org/ntpfaq (дата обращения: 09.03.2026).

[11] Fubin, P. "The accuracy of IEEE 1588 time synchronization protocol and its improvement" / Pang Fubin, Yuan Yubo, Gao Lei and Song Liangliang // 2015 12th IEEE International Conference on Electronic Measurement & Instruments (ICEMI), Qingdao, China. – 2015. – С. 280-284. – DOI: 10.1109/ICEMI.2015.7494173.

[12] IEEE Std 1588-2002 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurements and Control Systems.

[13] IEEE Std 1588-2008 IEEE Standard for a Precision Clock Synchroniza-

tion Protocol for Networked Measurements and Control Systems.

[14] IEEE Std 1588-2019 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurements and Control Systems.

[15] Телегин, С.А. Протокол PTP для синхронизации сетей NGN. Вопросы применения / С.А. Телегин // Первая миля. – 2009. – Т. 5, № 6. – С. 20-23.

[16] ITU-T Recommendation G.8261: Timing and synchronization aspects in packet networks, 2008.

[17] ITU-T Recommendation G.8262: Timing characteristic of equipment clocks, 2008.

[18] ITU-T Recommendation G.8264: Distribution of timing information through packet networks, 2008.

[19] Ибрагимов, И. Синхронизация в больших и неоднородных сетях SyncE / И. Ибрагимов // Электронные компоненты. – 2020. – №6. – С. 30-33.

[20] ITU-R Handbook on Selection and Use of Precise Frequency and Time Systems, 1997, https://www.itu.int/dms_pub/itu-r/opb/hdb/R-HDB-31-1997-PDF-R.pdf (дата обращения 09.03.2026).

[21] Прошин, Ф.А. Методы синхронизации в сетях связи / Ф.А. Прошин, М.Н. Сторожук, Н.Л. Сторожук // Первая миля – 2024. – Т. 2, №118. – С. 62-69. – DOI: 10.22184/2070-8963.2024.118.2.62.69.

[22] Приказ Министерства связи и массовых коммуникаций РФ от 9 октября 2017 г. № 538 "Об утверждении Методики измерений разности (расхождения) шкал времени на основе протоколов NTP и PTP (МИ РШВ.01.08-2017)".

[23] Скакун, И.О. Сличение шкал времени с использованием сигналов ГНСС / И.О. Скакун // Труды МАИ. – 2014. - №73. – 26 с.

[24] Рыжков, А.В. Опыт внедрения систем частотно-временного обеспечения сетей связи / А.В. Рыжков, М.Л. Шварц, В.М. Аладин, А.В. Исупов // T-Comm: Телекоммуникации и транспорт. – 2022. – Т. 16, № 7. – С. 21-28. – DOI: 10.36724/2072-8735-2022-16-7-21-28.

[25] Рыжков, А.В. Предпосылки создания когерентной сети связи общего пользования – основы сквозных цифровых технологий / А.В. Рыжков, М.Л. Шварц // T-Comm: Телекоммуникации и транспорт. – 2021. – Т. 15, №7. – С. 14-22. – DOI: 10.36724/2072-8735-2021-15-7-14-22.

[26] Шварц, М.Л. Современные тенденции развития систем сетевой синхронизации в сетях электросвязи. От плезиохронных до когерентных сетей / М.Л. Шварц, А.В. Рыжков // Системы синхронизации, формирования и обработки сигналов. – 2021. – Т. 1, № 4. – С. 27-38.

[27] Рыжков, А.В. Пути формирования прецизионной шкалы времени национальной сети связи / А.В. Рыжков, М.Л. Шварц // T-Comm: Телекоммуникации и транспорт. – 2020. – Т. 14, №2. – С. 17-24. – DOI: 10.36724/2072-8735-2020-14-2-17-24.

[28] Рыжков, А.В. Частотно-временное обеспечение сети связи общего пользования: состояние и перспективы развития / А.В. Рыжков, А.Ю. Насонов // T-Comm: Телекоммуникации и транспорт. – 2014. – Т. 8, №2. – С. 41-46.

[29] Рыжков, А.В. Частотно-временное обеспечение в сетях электросвязи. Учебное пособие для вузов // М.: Горячая линия – Телеком. – 2018. – 270 с.

[30] ITU-T Recommendation G.8271.1: Network limits for time synchronization in packet networks with full timing support from the network, 2022.

[31] ГОСТ Р 59406-2021. Национальный стандарт Российской Федерации. «Обработка информации наблюдения в средствах автоматизации управления воздушным движением единой системы организации воздушного движения Российской Федерации» (утверждён и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 23 марта 2021 г. N 161-ст).

[32] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

[33] Методические указания по применению в ПАО «Россети Московский регион» основных технических решений по эксплуатации, реконструкции и новому строительству электросетевых объектов. – 2023. - №6. – 267 с.

[34] Куприянов, А.О. Глобальные навигационные спутниковые системы: Учебное пособие / А.О. Куприянов // М.: МИИГАиК. – 2017. – 76 с.

[35] Уязвимости ГНСС. – URL: https://securelist.ru/internet-exposed-gnss-receivers-in-2024/111056/ (дата обращения 16.04.2025).

[36] Demyanov, V. Space Weather Impact on GNSS Performance / V. Demyanov, Y. Yasyukevich, M. A. Sergeeva, A. Vesnin. // Springer Cham. – 2022. – DOI: 10.1007/978-3-031-15874-2.

[37] Нарушения работы ГНСС. – URL: http://vestnik-glonass.ru/news/tech/v-2020-godu-gnss-glushili-tysyachi-raz/ (дата обращения 09.03.2026).

[38] Alternative PNT. – URL: https://www.mpdigest.com/2022/10/24/alternative-pnt-solutions-patch-gnss-vulnerabilities/ (дата обращения 09.03.2026).

[39] Сбои в работе GPS. – URL: https://www.dp.ru/a/2025/05/25/zamedlenie-tempov-rosta-dohodov (дата обращения 09.03.2026).

[40] RTI International. – URL: https://www.rti.org/impact/gps-14-trillion-economic-engine (дата обращения 09.03.2026).

[41] Нарушения работы ГНСС. – URL: https://oninvest.com/article/vnezony-dostupa-pocemu-my-teraem-svaz-s-kosmosom-i-cem-eto-grozit (дата обращения 09.03.2026).

[42] Нарушения синхронизации. – URL: https://3dnews.ru/1114713/oshibka-v-obnovlenii-yandeks-stantsiy-narushila-rabotu-serverov-sinhronizatsii-vremeni-v-runete (дата обращения 09.03.2026).

Об авторе:

Миронов Юрий Борисович, ведущий научный сотрудник,
Федеральное государственное бюджетное учреждение
«Национальный исследовательский центр «Курчатовский институт»

Альтернативные способы частотно-временного обеспечения

Юрий Миронов

Аннотация
Существующая глобальная навигационная спутниковая система (ГНСС) по характеристикам точности, надёжности и защищённости всё чаще оказывается не в состоянии обеспечить функционирование современных и перспективных автоматизированных систем управления, информационных и телекоммуникационных систем и сетей, цифровых расчётных финансовых инструментов, средств виртуализации и пр. Кроме того, практика показывает, что эти традиционные средства синхронизации подвержены техническим отказам и злонамеренным воздействиям извне. Для разработки и построения собственной национальной системы синхронизации, отвечающей современным вызовам, требуется всестороннее исследование перспективных мировых достижений в предметной области, оценка возможности применения этих технологических инноваций для российских условий, в том числе высокой (до 9000 км) протяжённости каналов и трактов передачи между источниками и конечными потребителями эталонных сигналов времени и частоты. В связи с изложенным, в статье производится обобщение, анализ и систематизация существующих направлений и противоречий развития национальных систем синхронизации, в том числе на базе сочетания традиционных и альтернативных платформ синхронизации.

Ключевые слова:
глобальная навигационная спутниковая система, частотно-временное обеспечение, синхронизация, телекоммуникационные сети

Страны, такие как США, члены ЕС, Китай, Австралия и др., ведут разработки альтернативных способов распределения ЭСВЧ (эталонных сигналов времени и частоты), поскольку отказ ГНСС нарушит функционирование критически важной инфраструктуры стран, что повлечёт за собой значительные экономические и операционные потери.

Европейский союз

В 2021-2022 годах на территории ЕС (Европейского союза) был объявлен конкурс и проведено тестирование различных платформ A-PNT (Alternative Positioning, Navigation, and Timing— Альтернативные системы позиционирования, навигации и синхронизации). В отчёте о тестировании [1] представлены результаты тестирования семи различных платформ A-PNT [2-8].

Платформа, представленная голландским предприятием OPNT [9], предполагает использование существующих волоконно-оптических линий для передачи сигналов синхронизации. Предполагаемая точность синхронизации при использовании волоконно-оптической линии протяжённостью 250-1000 км составляет 2,5 нс [2].

Компания EASii IC представила на конкурс комплексную систему для производства и распространения универсального, отслеживаемого и высокозащищённого времени SCPTime [3]. Передача сигналов синхронизации осуществляется через Интернет с точностью порядка 10 мс [10].

Компания Satells представила платформу PNT Satellite Time and Location (STL). Данная платформа предусматривает использование низкоорбитальной группировки из 66 спутников, расположенных на высоте около 780 км. Сигнал от таких спутников мощнее сигналов от GPS на 30 дБ [4]. Ожидаемая точность синхронизации при использовании STL - порядка 150 нс.

Испанская компания GMW Innovating Solutions представила систему генерации корректирующих сообщений для сигналов, передаваемых спутниками GPS и Galileo [5]. Данная система также будет обнаруживать сбои в работе спутников и генерировать предупреждения для пользователей. В ноябре 2022 года компания объявила о сотрудничестве с корпорацией Lockheed Martin с целью создания спутниковой системы вспомогательного позиционирования SouthPAN [11]. Предполагается, что система SouthPAN повысит точность позиционирования GPS и Galileo до 10 см.

Компания Seven Solutions [12] представила альтернативную платформу PNT на основе протокола PTP [6]. Предлагается развернуть магистраль синхронизации на базе профильных каналов IEEE-1588-2019 High Accuracy. В качестве среды распространения сигналов синхронизации предполагается использование оптических волокон, которые уже используются телекоммуникационными компаниями. В ходе испытаний точность синхронизации составила менее 1 нс.

Частная технологическая компания Locata [13] представила локальную систему позиционирования [7]. Сеть наземных передатчиков LocataNets выполняет функции, аналогичные группировкам спутников ГНСС. Данная технология рассчитана на применение в условиях многолучевого распространения сигнала (городская застройка, каньоны, внутри помещений). В пределах зоны покрытия точность синхронизации составляет менее 10 нс.

Компания NextNav [14] представила отказоустойчивую систему PNT TerraPoiNT [8]. В данной системе используется наземная сеть радиомаяков, совместимых с сигналами ГНСС. Передача сигналов осуществляется на частоте 5,115 МГц. Точность синхронизации с UTC при использовании данной технологии составляет менее 100 нс.

В ходе испытаний все семь платформ были признаны эффективными и соответствующими требованиям, предъявляемым к данным платформам в рамках проводимого конкурса [11].

Наряду с этим начато развёртывание интегрированной спутниковой и наземной системы квантового распределения ключей (КРК) EuroQCI, которая позволит повысить надёжность обмена данными и информацией [15]. Технология КРК, подробно описанная в [16, 17], является одним из перспективных методов защиты информации [18, 19], устойчивым к атакам злоумышленников независимо от того, какой вычислительной мощностью они могут располагать (в том числе квантовыми компьютерами) [16, 20]. Система EuroQCI будет состоять из наземного сегмента (оптоволоконные сети связи) и космического сегмента. Космический сегмент будет реализован как часть системы IRIS [21]. Реализация проекта EuroQCI была начата в январе 2023 года.

США

Аналогичный конкурс платформ A-PNT проводился в США [22]. По результатам конкурса стартап TrustPoint выиграл контракт со SpaceWERX [23]. Альтернативная платформа PNT, разработанная TrustPoint, описана в [24]. Данное решение представляет собой использование группировки низкоорбитальных спутников в С-диапазоне.

Ещё одним решением для повышения надёжности синхронизации шкал времени стало использование группировки низкоорбитальных спутников. Так, американская спутниковая корпорация Iridium Communications Inc. завершает развёртывание системы STL (Satellite Time and Location) [25]. Подробная информация о данной системе представлена на сайте компании [26].

Также в США агентство перспективных оборонных исследовательских проектов (DARPA) ведёт разработки по созданию версий атомных часов, способных работать при установке на самолёт или спутник [27]. При этом данные часы должны обеспечивать точность до пикосекунд в течение 100 секунд и выдерживать перепады температур окружающей среды, ускорение и вибрацию платформы, на которой планируется установка атомных часов. Данный исследовательский проект направлен на улучшение синхронизации времени.

В конце 2021 года корпорации Locata и Ursa Navigation Solutions, Inc. объявили о технологическом партнёрстве для предоставления надёжных решений PNT [28]. Техническая реализация предложенного решения заключается в сочетании высокоточного локального PNT от Locata и низкочастотных решений PNT, таких как Loran-C [29], Loran-D [30], eLoran [31] и LFPhoenix [32] от UrsaNav. Реализация устойчивой архитектуры PNT в США разделена на три фазы. По завершению третьей фазы на всей территории США будет обеспечена погрешность синхронизации менее 500 нс.

Китайская Народная Республика

В Китае была представлена работа о тенденциях развития национальной защищённой системы PNT на базе BDS (BeiDou Navigation Satellite System - Навигационная спутниковая система BeiDou) [33], в которой рассматривается реализация резервного канала передачи ЭСЧВ и возможность создания единой национальной системы распределения ЭСВЧ и навигации на поверхности, под землёй, на воде, под водой, в воздушном пространстве и в дальнем космосе.

Высокоточная наземная система хронометража является одним из проектов Национального плана развития крупной научно-технической инфраструктуры Китая. При передаче сигналов синхронизации по волоконно-оптическим линиям планируемая точность синхронизации составит менее 100 пс. Общая протяжённость волоконно-оптической сети составит более 20 000 км [34]. Также будет произведена модернизация длинноволновых систем синхронизации с целью получения точности синхронизации порядка 100 нс. Сочетание нескольких платформ PNT позволит создать в Китае национальную систему позиционирования, навигации и синхронизации, устойчивую к внешним дестабилизирующим воздействиям. Также необходимо отметить, что данная система будет обеспечивать синхронизацию на всей территории Китая, включая воздушное, водное и подводное пространство. С развитием свехширокополосной технологии (СШП) технология позиционирования СШП представляет собой ещё одну альтернативу ГНСС. Использование технологии СШП позволяет достичь высокой точности позиционирования и помехоустойчивости [35].

Австралия

В марте 2024 года австралийская компания FrontierSI [36] рассмотрела вопрос надёжности существующей системы PNT в Австралии и предложила программу по созданию устойчивой системы позиционирования, навигации и синхронизации.

В июле 2024 года на 30-м съезде по вопросам позиционирования, навигации и точного времени [37] акцентировалось внимание на зависимости многих секторов экономики стран от американской системы ГНСС GPS Navstar, которая является уязвимой к внешним дестабилизирующим воздействиям (подавление сигнала, спуфинг, физические атаки на спутники и приемники ГНСС). Исходя из этого была обоснована необходимость создания альтернативных платформ PNT с целью повышения надёжности доставки сигналов ЭСВЧ до потребителей и уменьшения экономической зависимости от США.

Индия

Исследования альтернативных платформ PNT были проведены в 2022-2023 годах в Индии [38]. В рамках исследований проводилась оценка возможности использования тёмного оптического волокна как среды передачи сигналов синхронизации. Экспериментально полученное значение точности синхронизации составляет 2,5 нс при длине волоконной линии 11 км. Синхронизация была основана на применении протокола IEEE 1588 (PTP). По результатам проведённого исследования использование волоконно-оптических линий связи для синхронизации признано целесообразным.

Япония

На данный момент Япония продолжает развёртывание своей региональной независимой системы глобального позиционирования Quasi-Zenith Satellite System (QZSS) [39]. Главной целью данной системы является повышение доступности GPS в городских каньонах Японии. QZSS состоит из одного геостационарного спутника и трёх спутников на квазизенитной орбите. Планируется расширение данной системы до семи спутников: четыре спутника на квазизенитной орбите, два спутника на геостационарной орбите и один спутник на квазигеостационарной орбите.

Турция

Работы по созданию региональной системы определения местоположения, синхронизации и навигации начаты в Турции, поскольку правительство решило принять превентивные меры по обеспечению безопасности экономики страны в случае сбоев ГНСС. Основой для будущей системы PNT станет навигационная спутниковая группировка. Предполагается развёртывание региональной навигационно-временной системы (BKZS). Первый спутник данной системы станет испытательным полигоном для отработки технологических решений. Полный спектр услуг PNT будет предоставлен пользователям после окончательного формирования спутниковой группировки [40].

Также существует потребность в спутниковой системе усиления (SBAS), которая будет обеспечивать обслуживание потребителей услуг PNT в Турции. На данный момент у Турции такой системы нет. Однако система EGNOS Европейского союза частично охватывает территорию страны. Для обеспечения полного покрытия планируется проведение переговоров с целью развёртывания дополнительных наземных опорных станций [40].

Великобритания

После выхода страны из Европейского союза последовал выход Великобритании из программы Galileo. За время участия в этой программе правительство инвестировало около 1,2 миллиарда фунтов стерлингов, что составляет более 10% от общего бюджета Galileo. Хоть услуги PNT, предоставляемые США и ЕС, всё ещё доступны в Великобритании, назрела необходимость создания собственной системы позиционирования, навигации и синхронизации [41].

В 2020 году правительство Великобритании выкупило долю компании OneWeb. Планируется использование программы OneWeb LEO (Low Earth Orbit - спутниковая группировка на низкой околоземной орбите) для обеспечения услуг PNT и организации противоракетной обороны за пределами Galileo. Компания OneWeb заявила, что её спутники Gen2 будут предоставлять полный спектр услуг PNT к 2026 году. Программа OneWeb LEO предполагает использование спутниковой группировки на низкой околоземной орбите, несмотря на ряд технических трудностей использования такого решения (высокое энергопотребление, сложная система наземного мониторинга, растущее количество космического мусора на низкой околоземной орбите и др.).

Альтернативные платформы PNT в России

Основной целью исследований альтернативных платформ PNT в России является создание единой национальной системы частотно-временного обеспечения. Данная цель соответствует стратегии развития отрасли связи [42]. В данной стратегии прописано внедрение сетей мобильной связи 5GA/6G. Необходимым условием для развёртывания сети связи нового поколения является ужесточение требований к точности синхронизации. Следовательно, возникает необходимость создания единой национальной системы частотно-временного обеспечения. Требования к данной системе изложены в [43].

В настоящее время рассматривается возможность реализации опорного узла формирования шкалы времени (ОУФШВ) когерентной сети связи общего пользования (КССОП) [44]. Существующие на данный момент предпосылки к созданию когерентных сетей связи общего пользования описаны в [45]. Для реализации таких сетей необходимо учитывать требования к комплексному составу первичных эталонов времени и частоты (ПЭВЧ) [46]. Частотно-временное обеспечение сетей связи обусловило перспективность внедрения комбинированных систем частотно-временного обеспечения на базе отечественного оборудования для существующих сетей связи [47]. Такой подход реализации частотно-временного обеспечения предоставляет возможность применения в сетях связи оборудования, которое частично или полностью не имеет программно-аппаратной поддержки протокола PTP и SyncE.

В [48] предлагается реализация альтернативного канала передачи ЭСВЧ по выделенным волоконно-оптическим линиям передачи. Такие линии имеют ряд преимуществ по сравнению со спутниковыми каналами передачи: отсутствие влияния электромагнитных помех, в том числе преднамеренных, независимость от условий космической погоды и невозможность перехвата и подделки сигналов ЭСВЧ. Следовательно, такая система устойчива к внешним дестабилизирующим воздействиям и может стать надёжным резервным каналом передачи сигналов синхронизации. В настоящее время на московском сегменте Межуниверситетской квантовой сети (МУКС) при поддержке АНО «РосНИИРОС» создан полигон «ВНИИФТРИ – НИЦ «Курчатовский институт», представляющий собой сеть квантовых сенсоров (квантовых стандартов времени и частоты) (рис. 1). На полигоне ведутся работы по созданию системы распространения сигналов синхронизации с привязкой к на-

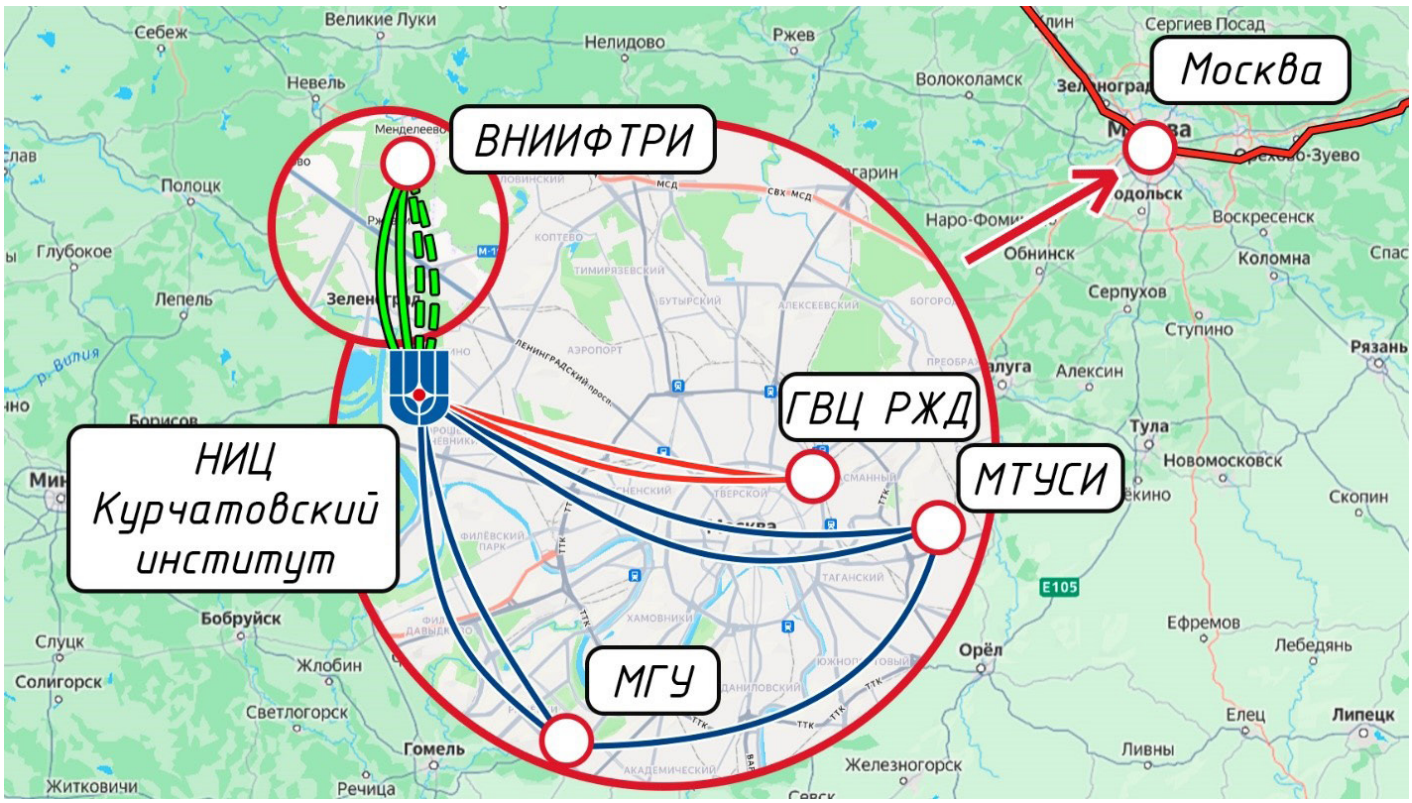


Рис. 1. Полигон для квантовой сенсорики и квантовой метрологии ФГУП ВНИИФТРИ – НИЦ «Курчатовский институт».

циональной шкале времени Российской Федерации (государственному первичному эталону единиц времени, частоты и национальной шкалы времени ГЭТ 1) для осуществления единого частотно-временного обеспечения квантового Интернета.

Таким образом, проводимые исследования альтернативных PNT за рубежом и в России позволят реализовать в будущем A-PNT. Поскольку комплексы ведущих часов требуют пристального внимания в части обнаружения помех и ошибок в приеме ЭСВЧ, то необходима реализация технологии A-PNT на отечественном оборудовании, как это показано в [49]. Это позволит создать национальную систему частотно-временного обеспечения, которая будет устойчива к внешним дестабилизирующим воздействиям. Использование отечественного оборудования предоставляет ряд преимуществ, таких как снижение зависимости от импорта и обеспечение стабильных поставок комплектующих. Кроме того, отечественное оборудование адаптировано к специфическим условиям эксплуатации на территории Российской Федерации, что повышает его эффективность и надёжность. Важно отметить, что в отечественном оборудовании отсутствуют недекларированные возможности и скрытые уязвимости, что существенно повышает уровень безопасности и защищённости систем. Прозрачность разработки и производства позволяет более эффективно проводить аудит и тестирование на наличие потенциальных угроз, тем самым минимизируя риски, связанные с эксплуатацией оборудования

Заключение

В условиях стремительного развития телекоммуникационных технологий современные телекоммуникационные сети сталкиваются с возрастающими требованиями к точности синхронизации, что обусловлено не только увеличением объёмов передаваемых данных, но и необходимостью повышения требований к качеству обслуживания потребителей (Quality of Service, QoS).

Существующая система PNT, реализованная посредством ГНСС, имеет ряд уязвимостей. Поскольку критически важная инфраструктура стран напрямую зависит от этих технологий, разработка альтернативных методов распределения ЭСВЧ становится одним из приоритетных направлений для многих государств.

Из описанных примеров проводимых исследований и испытаний можно сделать вывод, что проблема создания и внедрения альтернативного PNT актуальна. Ведущие специалисты многих стран ведут разработки и испытания в данной области.

Создание устойчивой системы PNT позволит уменьшить воздействие внешних дестабилизирующих факторов на критически важную инфраструктуру государств. Отказ системы PNT на длительное время может привести к неблагоприятным последствиям для различных секторов экономики и инфраструктуры страны. Таким образом, создание устойчивой системы PNT является необходимым условием для безопасности государства в целом.

В текущих международных условиях нельзя исключать возможность использования уязвимостей ГНСС для нанесения ущерба экономике и безопасности страны. Существующие решения могут быть адаптированы для реализации A-PNT на территории России, при условии проведения дополнительных испытаний и адаптации к существующим условиям и требованиям.

Источники:

[1] Bonenberg, L. Assessing Alternative Positioning, Navigation and Timing Technologies for Potential Deployment in the EU / L. Bonenberg, B. Motella, J. Fortuny Guasch // Publications Office of the European Union. – 2023. – DOI: 10.2760/596229.

[2] OPNT Technical Report + Test Plan v1.6. – URL: https://joint-research-centre.ec.europa.eu/system/files/2023-03/AD_1_OPNT_v3.pdf (дата обращения 17.04.2025).

[3] SCPTime Technical Report. – URL: https://joint-research-centre.ec.europa.eu/system/files/2023-03/Report_SCPTime.pdf (дата обращения 17.04.2025).

[4] Satelles Technical Report. – URL: https://joint-research-centre.ec.europa.eu/system/files/2023-03/Report_Satelles.pdf (дата обращения 17.04.2025).

[5] WANTIME4EC Technical Report. – URL: https://joint-research-centre.ec.europa.eu/system/files/2023-03/Report_7Sol.pdf (дата обращения 17.04.2025).

[6] Seven Solutions Technical Report. – URL: https://joint-research-centre.ec.europa.eu/system/files/2023-03/Report_7Sol.pdf (дата обращения 17.04.2025).

[7] Locata Technical Report v1.5. – URL: https://joint-research-centre.ec.europa.eu/system/files/2023-03/AD_6_Locata.pdf (дата обращения 17.04.2025).

[8] NextNav TerraPoiNT Technical Report. – URL: https://joint-research-centre.ec.europa.eu/system/files/2023-03/AD_7_NextNav.pdf (дата обращения 17.04.2025).

[9] OPNT. – URL: https://www.opnt.nl/ (дата обращения 09.05.2025).

[10] SCPTime. – URL: https://easii-ic.com/scptime (дата обращения 09.05.2025).

[11] GMV. – URL: https://insidegnss.com/gmv-signs-new-agreements-with-lockheed-martin-and-u-blox/ (дата обращения 09.05.2025).

[12] Seven Solutions. – URL: https://www.sevensols.com/ (дата обращения 09.05.2025).

[13] Locata. – URL: https://www.locata.com/ (дата обращения 09.05.2025).

[14] NextNav. – URL: https://nextnav.com/ (дата обращения 10.05.2025).

[15] Quantum technology at the European Commission Joint Research Centre. – URL: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (дата обращения 02.05.2025).

[16] Gisin, N. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Reviews of Modern Physics. – 2002. – Vol. 74, Issue 1. – P. 145-195. – DOI: 10.1103/RevModPhys.74.145.

[17] Pirandola, S. Advances in quantum cryptography / S. Pirandola, U.L. Andersen, S. Pirandola, et al. // Advanced in Optics and Photonics. – 2020. – Vol. 12, Issue 4 – P. 1012-1236. – DOI: 10.1364/AOP.361502.

[18] Bernstein, D.J. Post-quantum cryptography / D.J. Bernstein, T. Lange // Nature. – 2017. – Vol. 549. – P. 188-194. – DOI: 10.1038/nature23461.

[19] Boev, A.A. Possibility of creating a modular system for quantum key distribution in the atmosphere / A.A. Boev, S.S. Vorobey, S.Y. Kazantsev et al. // Technical Physics Letters. – 2022. – Issue 8. – P. 11-14. – DOI: 10.21883/TPL.2022.08.55051.19192.

[20] Bolotov, D.V. Modular Facility of Quantum Key Distribution in a Free Space / D.V. Bolotov, S.Y. Kazantsev; N.V. Pchelkina et al. // 2023 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). – IEEE, 2023. – DOI: 10.1109/WECONF57201.2023.10148017.

[21] IRIS. – URL: https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en (дата обращения 02.04.2025).

[22] SpaceWERX AltPNT. – URL: https://afwerxchallenge.com/spacewerx26/altpnt (дата обращения 18.04.2025).

[23] Alternative PNT. – URL: https://spacenews.com/trustpoint-wins-spacewerx-contracts-fot-alternative-pnt/ (дата обращения 18.04.2025).

[24] TrustPoint. – URL: https://trustpointgps.com (дата обращения 18.04.2025).

[25] Satellite Time and Location. – URL: https://satmobile.ru/news/news_post/iridium-zavershaet-razvertyvanie-sputnikov-predstavlyaet-sputnikovuyu-sistemu-opredeleniya-vremeni-i-mestopolozheniya-iridium-stl (дата обращения 18.04.2025).

[26] Iridium Communications Inc. – URL: https://www.iridium.com/ (дата обращения 18.04.2025).

[27] ROCkN. – URL: https://www.airforce-technology.com/news/darpa-optical-clocks/ (дата обращения 19.04.2025).

[28] Alternative PNT. – URL: https://insidegnss.com/alternative-pnt-companies-partner/ (дата обращения 20.04.2025).

[29] Loran-C. – URL: https://skybrary.aero/articles/loran-c (дата обращения 21.04.2025).

[30] Loran-D. – URL: https://jproc.ca/hyperbolic/loran_b_d.html (дата обращения 21.04.2025).

[31] eLoran. – URL: https://ursanav.com/what-is-eloran/ (дата обращения 21.04.2025).

[32] LFPhoenix. – URL: https://ursanav.com/lfphoenix/ (дата обращения 21.04.2025).

[33] Yang, Y. Development trends of the national secure PNT system based on BDS / Y. Yang, X. Ren, X. Jia. // Sci. China Earth Sci. – 2023. – Т. 66. – С. 929-938. – DOI: 10.1007/s11430-022-1069-7.

[34] China PNT. – URL: https://mp.weixin.qq.com/s?__biz=MzA5MjI2MjQyOA==&mid=2651184687&idx=1&sn=39b1e0b129e8c86a803699e02b96f326 (дата обращения 25.05.2025).

[35] UWB. – URL: https://ru.nicerf.com/news/uwb-module-uwb.html (дата обращения 31.05.2025).

[36] Critchley-Marrows, J. A Time and a Place for Resilience / J. Critchley-Marrows, E. Rubinov, P. Delaney, J. Lee, A. Linossier. – URL: https://frontiersi.com.au/wp-content/uploads/2024/02/FrontierSI_Resilient-PNT_Report.pdf (дата обращения 19.04.2025).

[37] Space-based PNT. – URL: https://www.gps.gov/governance/advisory/recommendations/2024-07-PNTAB-chair-memo.pdf (дата обращения 19.04.2025).

[38] Kumar, K. Indian standard time dissemination using precision time protocol: Towards resilient time synchronization using optical fibers for critical infrastructure in India / K. Kumar, S. K. Ghosh, Neelam, S. C. Pandey, V. Bharath, S. Panja, A. Agarwal, M. Das // MAPAN. – 2024. – T. 39. – C. 475-482. – DOI: 10.1007/s12647-024-00739-0.

[39] QZSS. – URL: https://qzss.go.jp/en/ (дата обращения 10.05.2025).

[40] 'National Space Program Strategy Document 2022-2030', Turkish Space Agency, 2022.

[41] 'UK space strategy and UK satellite infrastructure', House of Commons Science and Technology Committee, Second Report of Session 2022–23, Oct. 2022.

[42] Стратегия развития отрасли связи Российской федерации на период до 2035 года (утверждена распоряжением правительства Российской Федерации от 24 ноября 2023 г. № 3339-р).

[43] ГОСТ Р 71148-2023. Национальный стандарт Российской Федерации. «Требования по построению систем синхронизации сетей связи: сетей связи с коммутацией каналов, сетей связи с коммутацией пакетов» (утв. и введен в действие приказом Росстандарта от 13.12.2023 N 1571-ст).

[44] Рыжков, А.В. Предпосылки создания когерентной сети связи общего пользования – основы сквозных цифровых технологий / А.В. Рыжков, М.Л. Шварц // T-Comm: Телекоммуникации и транспорт. – 2021. – Т. 15, №7. – С. 14-22. – DOI: 10.36724/2072-8735-2021-15-7-14-22.

[45] Медведев, С.Ю. Формирование шкалы времени в когерентой сети связи общего пользования / С.Ю. Медведев, К.Г. Мишагин, А.В. Рыжков, Б.А. Сахаров, М.Л. Шварц // T-Comm: Телекоммуникации и транспорт. – 2023. – Т. 17, №12. – С.29-35. – DOI: 10.36724/2072-8735-2023-17-12-29-35.

[46] Шварц, М.Л. Перспективный первичный эталон времени и частоты для систем частотно-временного обеспечения сетей связи / М.Л. Шварц, А.В. Рыжков, В.М. Аладин // T-Comm: Телекоммуникации и транспорт. – 2022. – Т. 16, №8. – С. 12-20. – DOI: 10.36724/2072-8735-2022-16-8-12-20.

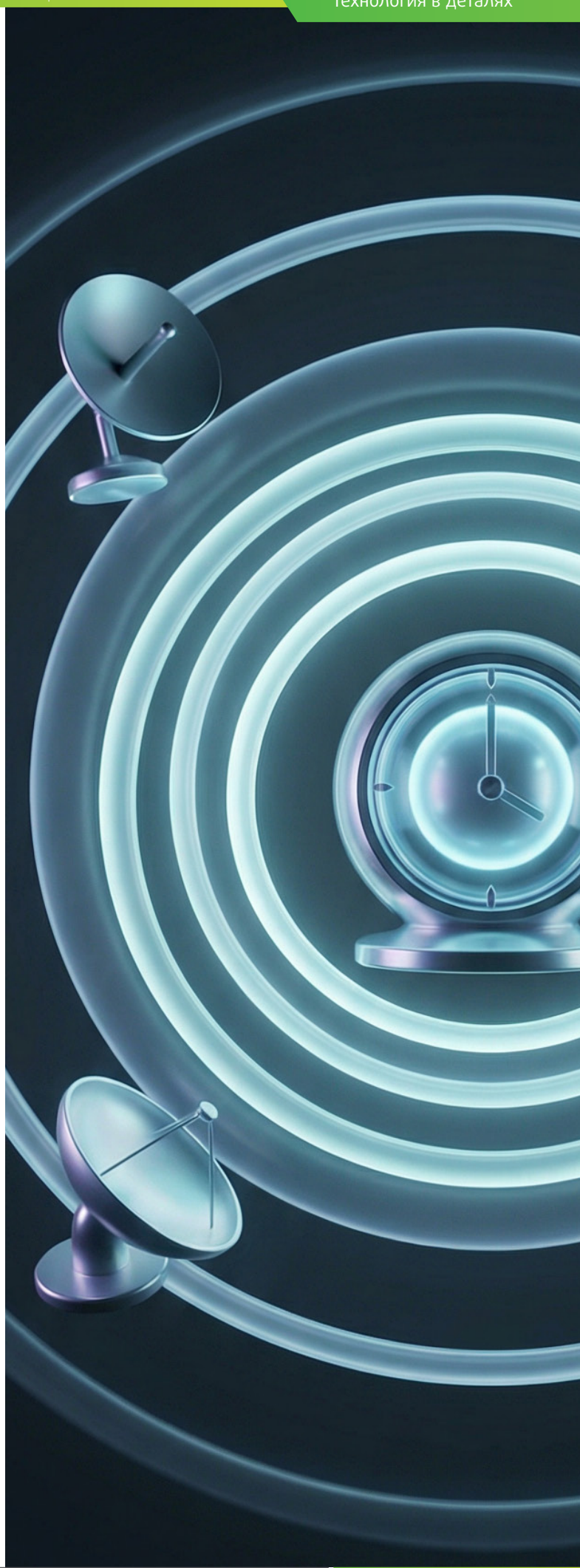
[47] Рыжков, А.В. Опыт внедрения систем частотно-временного обеспечения сетей связи / А.В. Рыжков, М.Л. Шварц, В.М. Аладин, А.В. Исупов // T-Comm: Телекоммуникации и транспорт. – 2022. – Т. 16, № 7. – С. 21-28. – DOI: 10.36724/2072-8735-2022-16-7-21-28.

[48] Балаев, Р.И. Современные требования к обеспечению сетей связи нового поколения эталонными сигналами времени и частоты / Р.И. Балаев // Альманах современной метрологии. – 2021. – Т. 4, №28. – С. 109-114.

[49] Рыжков, А.В. Поддержание достоверности шкалы времени в ведущих сетевых часах в условиях преднамеренных помех / А.В. Рыжков, М.Л. Шварц, В.М. Аладин // T-Comm: Телекоммуникации и транспорт. – 2023. – Т.17, №11. – С.4-9. – DOI: 10.36724/2072-8735-2023-17-11-4-9.

Об авторе:

Миронов Юрий Борисович, ведущий научный сотрудник, Федеральное государственное бюджетное учреждение «Национальный исследовательский центр «Курчатовский институт»



Роль времени в спутниковых сетях Интернета

Владимир Глебский

Аннотация
Спутниковые сети Интернета долгое время находились на вторых ролях, заполняя места, куда физически не могла дойти наземная инфраструктура. Они выполняли роль дорогостоящего резерва или дорогой, но «безальтернативной альтернативы», и немалой причиной тому был аспект времени – большие временные задержки. Но по мере развития космических технологий и «приближения» спутниковых сетей к Земле спутниковые интернет-сети практически сравнялись по характеристикам с наземными и, более того, становятся важной и неотъемлемой частью новой гибридной архитектуры Интернета, рождающейся буквально на наших глазах.

Ключевые слова:
спутник, низкие орбиты, Интернет, временные задержки, Старлинк, ГСО, НГСО, межспутниковые линии, смартфон, гибридные сети

Как и в наземные линии, Интернет пришёл в спутниковые линии связи на уже существовавшие до его появления сети, осуществлявшие к тому моменту преимущественно передачу аналоговых сигналов телефонии, радио и телевидения. Данные для телеметрии и других нужд в них тоже передавались, но, естественно, с помощью других протоколов. Однако, как пишут специалисты [1], когда «...учёные в своей лаборатории изобретали Интернет и его родной протокол TCP/IP, они ни разу не думали, что будут передавать информацию не в соседнюю комнату, а через спутник на другой континент... и этот всемирно популярный протокол теперь требует, чтобы после отправки одного пакета отправляющее устройство сначала получило от адресата «квитанцию», что пакет получен и теперь можно отсылать следующий пакет...» Это требование на долгие годы дополнительно усложнило одну из серьёзнейших проблем, связанную с аспектом времени в спутниковых сетях Интернета.

Дело в том, что в момент появления Интернета услуги спутниковой связи для нужд рядовых потребителей осуществлялись со спутников, расположенных на геостационарной орбите (ГСО). Расстояние до этих спутников составляет около 36 тысяч километров от экватора, а от других точек на поверхности Земли - и того больше. Если условно принять такое усреднённое расстояние от спутника до абонента за 40 тысяч км, то радиоволны от абонентского спутникового терминала достигнут спутника со скоростью, равной скорости света 300000 км/с, за 133 мс, что уже многократно превосходит временные задержки передачи сигналов в наземных сетях. И это только в одну сторону и без учёта «аппаратных задер-

жек» в электронных приёмо-передающих системах спутника и наземного оборудования, превращающих «цифру» в радиоволну и обратно. То есть 133 мс необходимо только для того, чтобы цифровой пакет Интернета «прошёл» расстояние от наземной станции провайдера до спутника на ГСО. Затем ему надо преодолеть путь от спутника до абонента, а затем снова повторить весь этот путь в обратном направлении, чтобы в итоге доставить от абонента столь необходимую протоколу TCP/IP квитанцию о доставке пакета. Итого набирается 133 х 4 = 532 мс (рис. 1). Добавьте к этому аппаратные задержки, задержки сигнала при распространении в наземных сетях от источника Интернета (POP) до спутниковой станции провайдера, а также задержки прохождения сигнала, вызванные физическими свойствами атмосферы, и мы получаем совокупную (двойную) задержку (ping/пинг) в спутниковой сети интернета в 600-700 мс. Задержки в спутниковых системах на негеостационарных орбитах (НГСО) намного меньше, но НГСО появились гораздо позже (рис. 2, примеры задержек (latency) в сетях ГСО и НГСО).

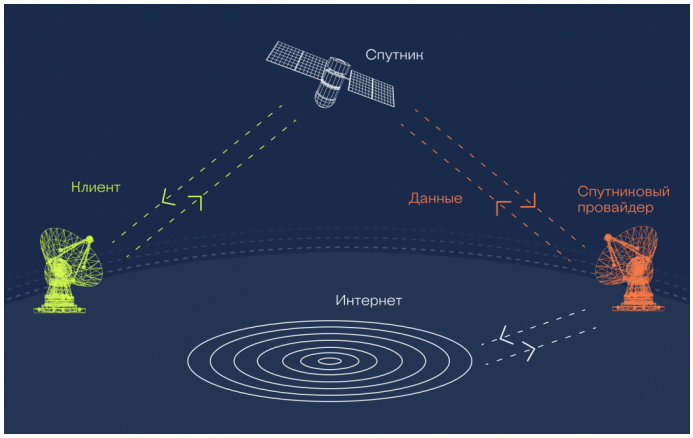


Рис. 1. Схема прохождения сигналов Интернета в спутниковой сети на ГСО.

Такие значительные временные задержки в спутниковых ГСО-сетях создали ряд серьёзных препятствий развитию спутникового Интернета. Сервисы, требующие интерактивности, такие как онлайн-игры, банковские приложения и т.п., оказались для спутниковых сетей Интернета попросту неприемлемыми, что исключало из числа пользователей большой пул платёжеспособных клиентов и нередко ставило спутниковый Интернет в ряд сервисов «на самый худой случай». При появлении малейшей возможности взять Интернет из наземного канала клиенты практически мгновенно отказывались от спутника. Долгие годы появление рядом наземного или мобильного Интернета было страшным сном спутниковых операторов, вынужденных постоянно искать клиентов в удалённых или недоступных для наземной инфраструктуры местах. Клиентская база спутникового Интернета сохранялась у оператора только до того момента, пока до клиентов не доходил Интернет по кабелю или оптоволокну. Цена мегабита и временные задержки в наземной сети были ниже почти на порядок! Там, где требовалась высокая надёжность и было востребовано резервирование через спутник, например, в банковских сетях, приложения Интернета приходилось специально дорабатывать, подстраивая их работу под «особенности» спутниковых сетей с длинными интервалами задержек. Но, опять-таки, это никак не делало спутниковый Интернет пригодным для тех же геймеров.

Таким образом, именно проблема времени, требующегося для распространения сигналов в спутниковых сетях, послужила многолетним тормозом развития спутникового Интернета.

Решение было известно давно – приблизить спутники к земле, т.е. перейти на более низкие орбиты, но ему мешал целый ряд технологических препятствий:

- спутников надо много, «живут» на низких орбитах они меньше, и нужно серьёзно снизить стоимость их создания и запуска;
- управление многоспутниковыми группировками намного сложнее, чем спутниками на ГСО, нужна разработка новых технологий управления;
- абонентские терминалы должны «уметь» быстро переключаться с одного на другой низколетящий спутник без потери связи, нужны принципиально новые терминалы и антенны;
- для обеспечения высокой скорости Интернета нужны высокочастотные диапазоны Ka, Ku и C, уже выделенные для геостационарных сетей связи, надо решать проблемы интерференции и т.д.

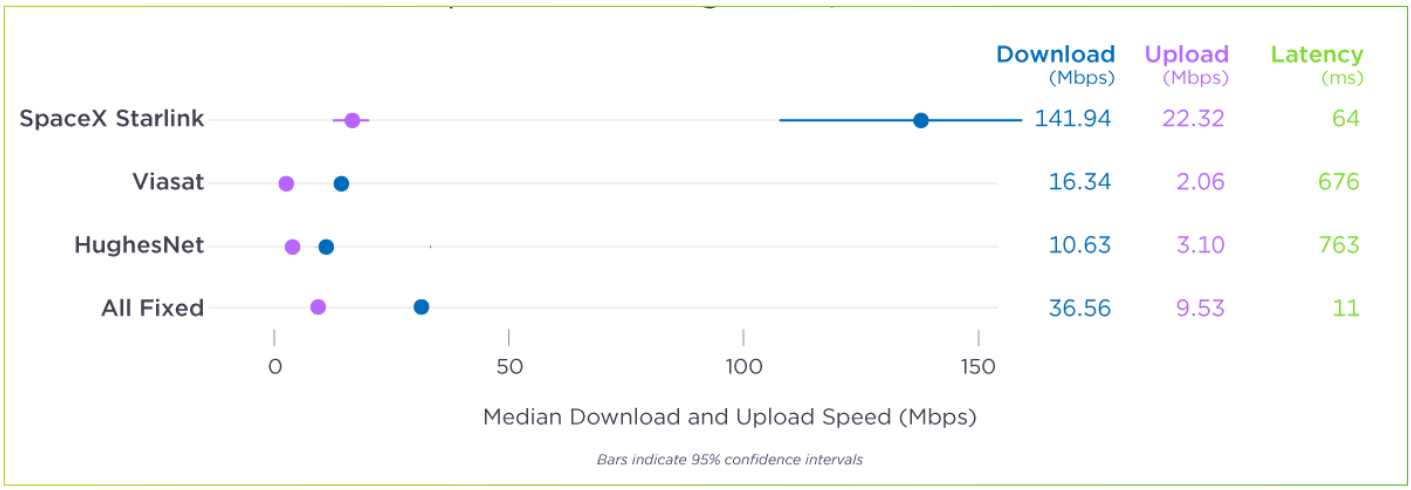


Рис. 2. Сравнение временных задержек в сетях ГСО (Viasat, HughesNet), НГСО (SpaceX Starlink).

Первой НГСО-сетью, которая дала спутниковый Интернет с близкими к наземным сетям временными задержками (около 20–70 мс), стала американская Iridium с 66-ю спутниками в системе, двигающимися на низких круговых орбитах на высоте 781 км от поверхности Земли в шести плоскостях (рис. 3.). Но используемый в ней для передачи данных L-диапазон (1616–1626,5 МГц) позволял обеспечить максимальную скорость Интернета только в 2,4 Мбит/с (при телефонной связи скорость цифрового потока была вдвое больше – 4,8 Мбит/с, но, собственно, обеспечение спутниковой телефонной связи и было основной задачей этой системы). Конечно, в начале 2000-х годов и это было прорывом! Тем более, что сеть уже имела межспутниковые линии связи в Ka-диапазоне (23,18-23,38 ГГц), с пропускной способностью 10 Мбит/с, использовала многолучевые системы и другие новые технологии, но ни по скорости, ни по цене такой спутниковый Интернет всё равно не мог конкурировать с наземными сетями.

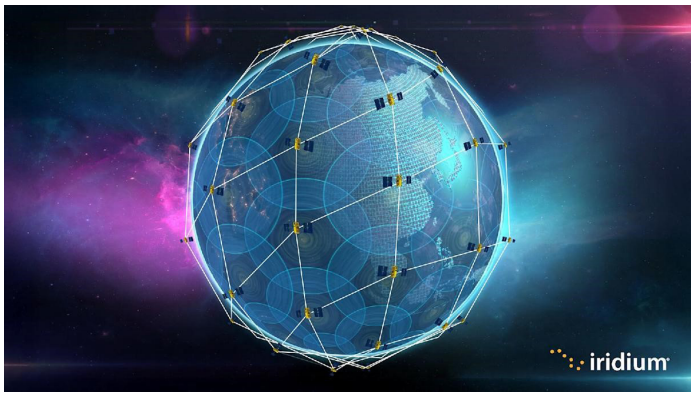


Рис. 3. Схематическое изображение расположения спутников в низкоорбитальной сети Iridium.

Дальше было много попыток «приблизить спутниковый Интернет к совершенству» (спутниковые системы LeoSat, O3B, OneWeb и т.д.). Многие из этих систем продолжают существовать и работать, но поистине революционный прорыв, за которым сегодня следит весь мир, совершил Илон Маск, запустив реализацию проекта SpaceX Starlink («Старлинк», рис. 4). Этот проект предусматривает размещение на низких орбитах (около 550 км над Землёй) нескольких тысяч спутников (в 2017 году их было заявлено до 7518 в системе), но, самое главное, использует для передачи на наземный пользовательский терминал Ku-диапазон (10,7–12,7 ГГц и 14–14,5 ГГц), что позволяет обеспечить поток Интернета до клиента со скоростью до 1 Гбит/с и задержкой в 20 мс (по утверждениям разработчиков).

Очевидно, что такие скорости и задержки вполне могут конкурировать с наземными сетями, но, к тому же, имеют и ещё одно неоспоримое преимущество – терминал Starlink можно установить и подключить где угодно, нет необходимости искать наземную инфраструктуру, достаточно иметь источник питания.

Поскольку нас интересует, прежде всего, удалось ли сети Starlink и ей подобным решить проблему временных задержек, то посмотрим, какие данные [2] имеются на этот счёт (рис. 5).

Как видим из представленного в июле 2025 года Starlink графика, средняя скорость в часы пик для двух миллионов активных пользователей доходит до 200 Мбит/с, а средняя задержка составляет около 25,7 мс, при этом, по утверждению разработчиков Starlink, менее 1% измерений показывают задержку более 55 мс.

Что касается отдельных тестов [3], то в них данные показывают скорость в 300-500 Мбит/с с задержками 15-25 мс (для оборудования Starlink второго поколения), разработчики сети OneWeb (Phase 2 – тоже второе поколение) заявляют, что достигли скоростей до 400 Мбит/с с задержками 20 мс, похожие характеристики предполагают и китайские варианты Starlink (один так и называется – G60 Starlink и предполагает использование 12 тысяч спутников в этой многоспутни-

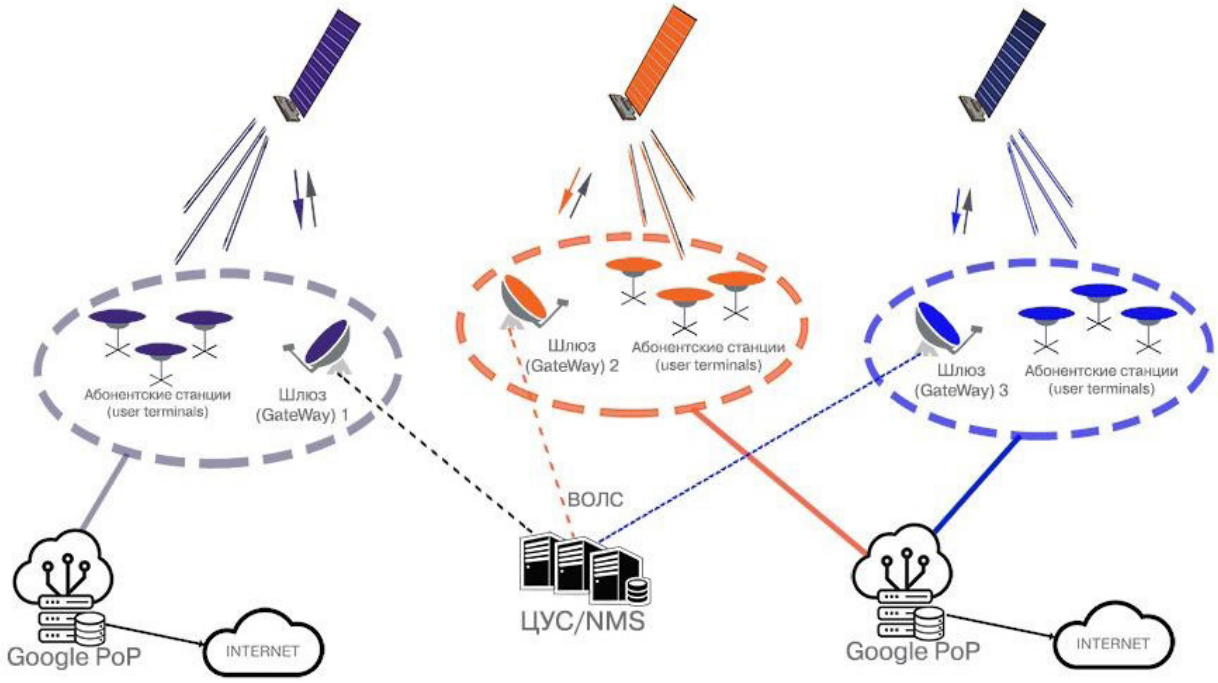


Рис. 4. Схема организации управления и доставки потоков Интернета в сети Starlink.

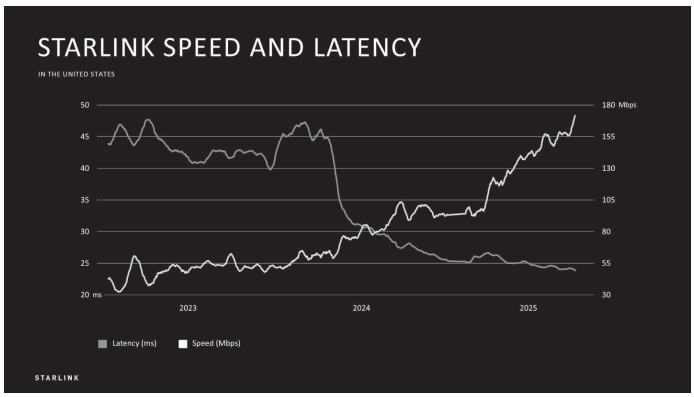


Рис. 5. График изменения скорости и задержек в сети Starlink по мере наращивания и развития системы.

ковой системе, второй, на 13 тысяч спутников, SatNet, должен быть развёрнут в рамках национального проекта Guowang). То есть в целом можно утверждать, что спутниковые сети Интернета вплотную приблизились по характеристикам к пользовательским параметрам наземных сетей и становятся вполне конкурентоспособными оптоволокну.

Справедливости ради нужно всё-таки отметить, что в силу того, что спутниковый Интернет работает через естественную среду распространения, т.е. данные попадают в пользовательский терминал, проходя через космическое пространство и атмосферу, да ещё и не с одного источника, а с постоянно «переключающихся» спутников, подверженность спутникового Интернета воздействию окружающей среды остаётся, хотя и не очень существенной [4]. Спутниковый Интернет может на короткое время прерываться из-за затенения спутников какими-то объектами (качающимися деревьями, летящим мусором, пролетающим низко самолётом или стаей птиц и т.д.), при сильных атмосферных осадках и наэлектризованности атмосферы и т.п. К примеру, если сравнить характеристики джиттера, то «картинка» спутникового канала и наземного канала отличаются (рис. 6).

Рис. 6. Сравнение джиттера в сети Интернета «Старлинка» и в кабеле наземного провайдера.

Впрочем, и в наземных сетях случаются сбои, например, по питанию, так что 100% непрерывный и стабильный по своим характеристикам канал гарантировать не может никто.

С развитием спутникового Интернета появились и новые перспективы, о которых раньше никто даже не задумывался. В борьбе за сокращение времени доставки сигналов по низкоорбитальным спутниковым системам учёные и инженеры начали активно развивать оборудование для межспутниковой оптической связи, позволяющей передавать потоки данных со скоростями, превышающими возможности наземных линий. Проще говоря, если раньше для переброски потока Интернета на другую сторону земного шара надо было найти или проложить оптоволоконную линию связи, то с появлением выхода на спутники и межспутниковых оптических линий появляются новые «обходные» пути. При необходимости возможности наземных и спутниковых линий можно комбинировать, создавая развитые гибридные системы, а с учётом возможности выноса в космос дата-центров, проекты которых сегодня активно разрабатываются, инфраструктура Интернета получит принципиально новое качество. И будущее таких систем уже не за горами. Параллельно идут активные разработки и апробирование низкоорбитальных спутников для прямой связи со смартфонами (технологии D2D и D2C), около 300 таких спутников уже запущены и работают в той же сети Starlink. Из-за низкой мощности и слабых приёмных антенн смартфонов скорость в этих сетях не превышает 5 Мбит/с, и тем не менее, они тоже становятся важной и очень мобильной составляющей будущих гибридных сетей Интернета.

В заключение надо отметить, что есть и другие аспекты работы спутниковых сетей и Интернета, связанные со временем, прежде всего это касается точности применяемых стандартов времени и измерений. Если говорить о временных задержках при передаче потоков Интернета, то их влияние не столь существенно. Но, например, в системах и приложениях для расчёта координат при управлении различными объектами эти временные аспекты играют важную роль и составляют основу целого ряда более тонких технологий, заслуживающих отдельного рассмотрения.

Список литературы:

[1] https://vsatman888.livejournal.com/196669.html

[2] https://dzen.ru/a/aHcc2VckRk23VHfS?ysclid=mmurb8nscd44803667

[3] https://tele2site.com/sputnikovaya-i-alternativnaya-svyaz/poslednie-standarty-sputnikovoy-svyazi-chto-izmenitsya-v-skorosti-i-zaderzhkah/?ysclid=mmt6c9r7r5420802714

[4] https://habr.com/ru/news/569306/

Об авторе:

Владимир Леонидович Глебский, директор отдела развития региональных проектов Международной организации космической связи «Интерспутник»

Национальная шкала времени Российской Федерации UTC(SU) в сети Интернет и результаты эксперимента её международного сравнения со шкалой времени Республики Казахстан UTC(KZ)

Сергей Семёнов, Екатерина Семёнова, Султанбек Смагулов

Аннотация

В настоящей статье рассказывается о Государственном первичном эталоне единиц времени, частоты и национальной шкалы времени (далее – ГЭВЧ), описан процесс формирования национальной шкалы времени (далее – ШВ) Российской Федерации UTC(SU), приведены способы распространения информации о точном значении московского времени и календарной дате, а также эталонных сигналов времени.

Рассказано о достоверных источниках точного времени в сети Интернет. Представлены результаты измерений смещения формируемых шкал времени потребителей при синхронизации по NTP-серверам времени в Интернете.

Дополнительно представлен международный опыт сравнения шкал времени национальных эталонов Российской Федерации UTC(SU) и Республики Казахстан UTC(KZ) посредством NTP-серверов в рамках проекта КООМЕТ 605/RU/13. Приведены оценки расширенной неопределённости измерений и результаты мониторинга шкал времени NTP-серверов

.

Ключевые слова:

атомные часы, шкала времени, синхронизация, UTC(SU), UTC(KZ), NTP

Введение

Время – это положение Солнца на небосводе, это часики, это тик-так, это цифры в телефоне, это то, к чему мы все привыкли и что составляет нашу повседневную жизнь, и без этого мы себя уже не представляем. Что же такое время и откуда оно берётся? Для исчисления суток всё просто: день сменяет ночь. Для исчисления месяца удобно брать фазы Луны. Год – это смена сезонов и удобно брать начало от зимнего солнцестояния (актуально для северного полушария). Со временем эти понятия немного видоизменились, но общий принцип построения понятен – астрономические явления. А как же быть со временем в течение дня и откуда взялось число 12? Самый простой способ – это палка в земле, а самая короткая тень – это полдень. Число «12» и двенадцатеричная система счисления, скорее всего, были придуманы древними шумерами: происхождение такой системы объясняют методом пальцевого счёта: большим пальцем руки считали каждую фалангу четырёх пальцев той же руки. Сутки разделили до полудня и после полудня. Часы и минуты удобно поделить на 60, так как у этого числа много делителей. Скорее всего, число пришло от круга, который астрономы делили на 360°, для удобства его сократили до 60. Оставалось найти стабильное физическое явление, например, колебание маятника или пьезоэлектрический эффект, явление механического резонанса кварца или квантовые переходы тяжёлых металлов.

Информация о точном значении времени широко используется в повседневной жизни в таких сферах, как навигация, управление движением всех видов транспорта, фиксация нарушений правил дорожного движения, проведение банковский операций, торги на биржах, оказание услуг связи, в Интернете при использовании различных услуг и т.п.

С развитием современных технологий, включая мобильные сети пятого и шестого поколений (5G/6G), Интернет вещей (IoT), умные города и автономные транспортные системы, точная синхронизация времени становится основополагающим фактором для их эффективного функционирования. Международный союз электросвязи (ITU) установил для мобильных сетей 5G требо-

вания к точности синхронизации на уровне ±30 нс относительно UTC. Финансовые системы требуют синхронизации с точностью до 100 мкс согласно регламенту MiFID II, энергетические сети – до 1 мкс в соответствии со стандартом IEC/IEEE 61850-9-3 [1].

Определение секунды дано на 13-й Генеральной конференции мер и весов в 1967 году, а в 1997 году было уточнено. Секунда – это основная единица времени международной системы единиц (СИ), численно равная длительности 9 192 631 770 периодов излучения, соответствующего переходу между двумя сверхтонкими уровнями основного состояния атомов цезия-133 в состоянии покоя при температуре 0 К.

В соответствии с федеральным законом от 3 июня 2011 года № 107-ФЗ «Об исчислении времени» национальная шкала времени Российской Федерации – упорядоченная числовая последовательность размеров единиц времени, воспроизводимая и хранимая Государственной службой времени, частоты и определения параметров вращения Земли (далее – ГСВЧ) на основе государственного первичного эталона единиц времени, частоты и национальной шкалы времени [2].

ГЭВЧ состоит из комплексов воспроизведения, хранения, передачи единиц величин и комплекса средств технического обеспечения.

Комплекс воспроизведения независимо воспроизводит единицу времени – секунду. В его состав входят цезиевые реперы частоты фонтанного типа (воспроизводят секунду согласно определению), оптические реперы частоты на холодных атомах стронция ^{87}Sr, рубидиевый репер частоты фонтанного типа на основе холодных атомов ^{87}Rb. В основу заложен процесс квантового перехода, при котором фиксируется частота этого перехода.

Комплекс хранения основан на стандартах частоты и времени водородных активного типа (далее СЧВВ) – это приборы, которые обеспечивают воспроизведение частоты и времени. СЧВВ обладают наилучшей стабильностью на интервалах времени наблюдений от 10 до 30 суток. СЧВВ попарно сравниваются, образуя систему уравнений, количество которых равно количеству СЧВВ. Таким образом контролируется метрологическая исправность каждого СЧВВ. Комплекс предназначен для хранения единиц времени и частоты, проведения внутренних и внешних сличений эталона, формирования рабочих шкал времени, расчёта национальных шкал атомного времени TA(SU) и координированного времени UTC(SU).

В комплекс передачи единиц входят средства измерений, предназначенные для проведения поверки и калибровки средств измерений, и средства сравнения шкал времени.

Комплекс средств технического обеспечения предназначен для обеспечения бесперебойного электроснабжения ГЭВЧ, поддержания и мониторинга условий эксплуатации технических средств ГЭВЧ (температуры и влажности окружающего воздуха, атмосферного давления).

ГЭВЧ утверждён приказом Федерального агентства по техническому регулированию и метрологии от 16.02.2022 № 382 и имеет следующие метрологические характеристики, приведённые в таблице 1.

Таблица 1. Метрологические характеристики ГЭВЧ

Характеристика, единица измерения	Значение
Номинальное значение частоты, при котором воспроизводятся единицы, Гц	9 192 631 770
Доверительные границы относительной неисключённой систематической погрешности воспроизведения единиц времени и частоты при P=0,99	$\leq 5{,}0\cdot10^{-16}$
Относительная нестабильность частоты эталона (СКДО) при интервалах времени измерения 10÷30 сут., интервале времени наблюдений 1 год, не более	$\leq 1{,}0\cdot10^{-15}$
Среднее квадратическое отклонение результатов измерений при воспроизведении единиц времени и частоты при интервале времени наблюдений 1 сут., не более	$\leq 1{,}0\cdot10^{-15}$
Пределы допускаемых смещений национальной шкалы времени UTC(SU) относительно Международной шкалы координированного времени UTC, нс	±3

Формируемый на ГЭВЧ эталонный импульсный сигнал 1 Гц поступает на тайм машины и отсчитывает секунды, минуты, часы, дни.

Шкала атомного времени TA реализуется на основе квантовых переходов в атомах и молекулах [3]. Международная шкала атомного времени TAI – шкала атомного времени, реализуемая и поддерживаемая Международным бюро мер и весов (далее – МБМВ) [3]. TAI формируется на основе шкал времени воспроизводимыми и хранимыми национальными эталонами. Национальные эталоны периодически сличаются, и чем меньше нестабильность формирования национальной шкалы времени, тем больше средневзвешенный вклад в TAI.

ГЭВЧ непрерывно (ежедневно) участвует в международных ключевых сличениях CCTF-K001.UTC с использованием глобальных навигационных спутниковых систем (далее – ГНСС) ГЛОНАСС и GPS.

Параметры вращения Земли (далее – ПВЗ) характеризуют взаимное расположение земной системы координат и небесной системы координат относительно друг друга. Среднеквадратическое отклонение ПВЗ ГСВЧ от данных Международной службы вращения Земли и опорных систем (далее – МСВЗ) по Всемирному времени в апостериорном режиме составляет несколько десятков микросекунд [4].

Шкала всемирного времени UT реализуется на основании наблюдений за вращением Земли вокруг своей оси [3]. Шкалу времени UT формируют относительно начального момента времени последующих суток, принятого за нижнюю кульминацию Среднего Солнца на начальном меридиане.

Шкала всемирного координированного времени UTC устанавливается и поддерживается МБМВ и МСВЗ так, что значение (UTC–TAI) составляет целое число секунд, а значение |UTC–UT| не превышает 0,9 с [3].

В связи с тем, что Земля вращается вокруг своей оси неравномерно, в атомную шкалу времени периодически вводят (вычитают) дополнительную (високосную, скачущую) секунду. По данным французской обсерватории определения параметров вращения земли [5], за последние 50 лет было введено 27 дополнительных секунд. График ввода секунды представлен на рисунке 1.

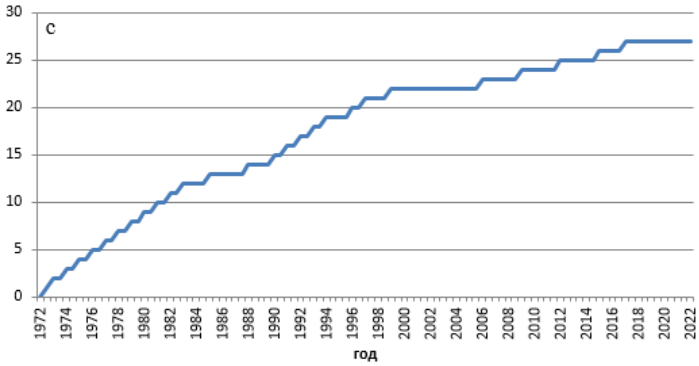


Рис. 1. График ввода (вычитания) дополнительной секунды.

Московское время – время часовой зоны, в которой расположена столица Российской Федерации город Москва. Московское время служит исходным временем при исчислении местного времени в часовых зонах. Московское время соответствует третьему часовому поясу в национальной шкале времени Российской Федерации UTC(SU)+3 [3].

Информация о точном значении московского времени и календарной дате формируется на основе национальной шкалы времени РФ UTC(SU), является официальной, общедоступной и обязательной для использования в Российской Федерации.

Распространение информации о точном значении московского времени и календарной дате

Для передачи эталонных сигналов частоты и времени Государственная служба времени, частоты и определения параметров вращения Земли использует разветвлённую сеть средств передачи, которая включает в себя ГЛОНАСС; две длинноволновые (ДВ) специализированные радиостанции РБУ и РТЗ; коротковолновую (КВ) специализированную радиостанцию РВМ; ДВ-и СДВ-радиостанции Минобороны РФ, средства передачи сигналов точного времени через глобальную сеть Интернет.

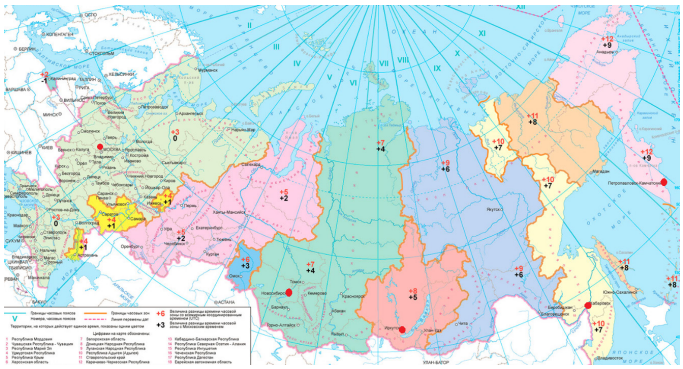


Рис. 2. Территориальное расположение эталонов единиц времени и частоты.

Для передачи сигналов точного времени через Интернет в настоящее время эксплуатируется пять NTP-серверов уровня Stratum 1, расположенных непосредственно во ФГУП ВНИИФТРИ, по два NTP-сервера уровня Stratum 1 - в филиалах ФГУП «ВНИИФТРИ» в г. Иркутске, г. Хабаровске и г. Новосибирске и один NTP сервер - в г. Петропавловск-Камчатский. Все NTP-серверы внесены в официальный международный список доступных NTP-серверов. Доменные имена и IP-адреса NTP-серверов приведены в таблице 2 [6]. Территориальное расположение ГЭВЧ и вторичных эталонов единиц времени и частоты представлены на рисунке 2.

Таблица 2. IP адреса NTP серверов ФГУП «ВНИИФТРИ»

Доменное имя, DNS (IP-адрес)	Место нахождения
ntp1.vniiftri.ru (89.109.251.21)	Московская. обл., пгт. Менделеево
ntp2.vniiftri.ru (89.109.251.22)	
ntp3.vniiftri.ru (89.109.251.23)	
ntp4.vniiftri.ru (89.109.251.24)	
ntp5.vniiftri.ru (89.109.251.25)	
ntp1.niiftri.irkutsk.ru (46.254.241.74)	г. Иркутск
ntp2.niiftri.irkutsk.ru (46.254.241.75)	
vniiftri.khv.ru (212.19.6.218)	г. Хабаровск
vniiftri2.khv.ru (212.19.17.26)	
ntp.sstf.nsk.ru (80.242.83.227)	г. Новосибирск
ntp.sniim.ru (80.242.83.228)	
ntp.kam.vniiftri.net (91.189.237.182)	г. Петропавловск-Камчатский

Национальная шкала времени Республики Казахстан UTC(KZ)

Аналогичная работа по формированию и распространению национальной шкалы времени ведётся в Республике Казахстан. Государственный первичный эталон единиц времени, частоты и национальной шкалы времени Республики Казахстан (далее – ГЭВЧ РК) был впервые создан в 2000 году в Южно-Казахстанском филиале РГП «КазИнМетр» (г. Алматы) и утверждён Госстандартом от 08.11.2001 года. Приказом Комитета по техническому регулированию и метрологии от 18.11.2005 г. № 400 была создана Государственная служба времени и частоты Республики Казахстан [7].

В 2006 году по завершении строительства нового здания «Эталонный центр» в городе Астане был приобретён и введён в эксплуатацию новый эталонный комплекс времени и частоты на основе цезиевых стандартов частоты, который был утверждён в качестве государственного первичного эталона в 2007 году. ГЭВЧ РК содержится и применяется в РГП «Казахстанский институт стандартизации и метрологии» (далее – РГП «КазСтандарт») [7].

В 2021 году ГЭВЧ РК был оснащён новым эталонным комплексом времени и частоты ЯКУР.411735.024 производства АО «Время-Ч» (Россия), в состав которого входят подсистема стандартов частоты и времени VCH-1008, ГНСС-приёмник GTR-55, подсистема формирования и измерения сигналов 5–100 МГц, подсистема измерений сигналов шкалы времени и формирования выходных импульсных сигналов, подсистема бесперебойного питания [7].

Включение в состав эталона новых технических средств позволило значительно улучшить его характеристики. Основные метрологические характеристики ГЭВЧ РК до и после совершенствования приведены в таблице 3 [7].

Таблица 3. Метрологические характеристики ГЭВЧ РК

Наименование характеристики	ГЭВЧ-2007	ГЭВЧ-2021
Номинальное значение частоты, Гц	9 192 631 770	1 420 405 751,77
СКО результатов измерений, не более	$1{,}0\cdot10^{-13}$	$1{,}0\cdot10^{-14}$
Доверительные границы НСП при P=0,99	$\pm1{,}0\cdot10^{-13}$	$\pm5{,}0\cdot10^{-15}$
Относительная нестабильность (СКДО) при 10÷30 сут.	$2{,}0\cdot10^{-14}$	$5{,}0\cdot10^{-15}$
Пределы допускаемых смещений UTC(KZ) относительно UTC, нс	±1000	±20

Начиная с 15 января 2022 года подстройка шкалы времени UTC(KZ) осуществляется путём автоматической коррекции частоты выходного сигнала эталона с помощью генератора фазовых сдвигов VCH-317. Управляющее воздействие рассчитывается пропорционально ошибке по фазе и частоте шкалы времени UTC(KZ) относительно UTC на момент времени управления по еженедельным данным UTCr, публикуемым МБМВ. В результате среднеквадратическая погрешность шкалы UTC(KZ) составила менее 2,3 нс, а абсолютное отклонение UTC(KZ) – UTC не превысило 7,6 нс [7, 8].

Для передачи информации о точном значении времени и календарной дате в сети Интернет в Республике Казахстан в составе ГЭВЧ РК эксплуатируются три NTP-сервера Meinberg M300 уровня Stratum 1, получающие эталонные сигналы 1 Гц (1PPS) и 10 МГц непосредственно от государственного первичного эталона. IP-адреса NTP-серверов «КазСтандарта» приведены в таблице 4 [9].

Таблица 4. IP-адреса NTP-серверов РГП «КазСтандарт»

Доменное имя, DNS (IP адрес)	Место нахождения
ntp1.ksm.kz (77.245.109.11)	г. Астана, Казахстан
ntp2.ksm.kz (77.245.109.12)	г. Астана, Казахстан
ntp3.ksm.kz (77.245.109.13)	г. Астана, Казахстан

ГЭВЧ РК начиная с 2008 года непрерывно участвует в международных ключевых сличениях CCTF-K001.UTC. Еженедельная публикация результатов UTC–UTC(KZ) на сайте МБМВ осуществляется с 31 января 2022 года. По публикуемым данным МБМВ национальная шкала времени UTC(KZ) по своим характеристикам входит в топ-25 лучших реализаций UTC среди ведущих лабораторий мира [7].

Результаты измерений

Рассмотрим погрешность синхронизации национальной шкалы времени UTC(SU), которая состоит из следующих составляющих, приведенных ниже.

Разность шкал времени UTC–UTC(SU) находится в пределах ±3 нс.

Пределы допускаемых смещений шкал координированного времени UTC(k) относительно национальной шкалы времени UTC(SU) составляют ±10 нс. UTC(k) – шкалы времени, формируемые Государственными вторичными эталонами единиц времени и частоты ВЭТ 1-5 (г. Иркутск), ВЭТ 1-7 (г. Хабаровск), ВЭТ 1-19 (г. Новосибирск) и ВЭТ 1-41 (г. Петропавловск-Камчатский).

NTP-серверы, приведённые в таблице 2, получают эталонные сигналы 1 Гц (1PPS) и 10 МГц непосредственно от государственных первичного и вторичных эталонов единиц времени и частоты. Задержка прохождения сигнала 1 Гц (1PPS) до NTP серверов не превышает 300 нс.

Проведён эксперимент, в ходе которого в локальную сеть связи (LAN) ФГУП «ВНИИФТРИ» подключили NTP-сервер «Метроном» версии 1000 (регистрационный номер в ФИФ ОЕИ 74018-19) и настроили его на синхронизацию ШВ от NTP-сервера уровня Stratum 1, находящегося в этой сети связи. По результатам эксперимента можно утверждать, что погрешность формирования ШВ NTP-серверами ФГУП «ВНИИФТРИ» относительно национальной шкалы времени находится в пределах ±100 мкс [10]. Результаты измерений смещения формируемой шкалы времени NTP-сервера относительно национальной шкалы времени UTC(SU) представлены на рисунке 3.

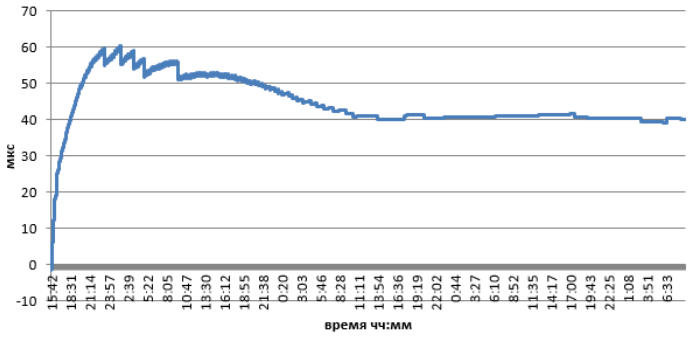


Рис. 3. Результаты измерения смещения формируемой шкалы времени NTP-сервера относительно национальной шкалы времени UTC(SU).

Для определения погрешности синхронизации шкалы времени в сети Интернет проведён ряд экспериментов, отражённых в работе [11]. С помощью утилиты ntpdc, контролирующей работу ntpd-демона, определена погрешность синхронизации шкалы времени в Интернете, которая находилась в пределах от минус 1,0 мс до 2,5 мс. При этом задержка прохождения NTP-пакета до Иркутска составила 70 мс, до Хабаровска - 103 мс.

Результаты сравнений шкал времени NTP-серверов ВНИИФТРИ и «КазСтандарт»

В Казахстанском институте стандартизации и метрологии («КазСтандарт») в период с 01.12.2021 по 01.02.2023 проводились регулярные сличения шкал времени посредством NTP-серверов национальных служб времени стран-членов КООМЕТ [12]. Работа проводилась в рамках темы КООМЕТ 605/RU/13 «Сличение шкал времени NTP-серверов с использованием сети INTERNET» с публикацией текущих результатов на сайте ТК 1.11 «Время и частота».

Сличения производились круглосуточно, с интервалом 20 минут, со следующими NTP-серверами точного времени: ntp1.ksm.kz, ntp2.ksm.kz, ntp3.ksm.kz («КазСтандарт», г. Астана); ntp1.vniiftri.ru, ntp2.vniiftri.ru, ntp3.vniiftri.ru, ntp4.vniiftri.ru (ФГУП «ВНИИФТРИ», пгт. Менделеево); ntp1.niiftri.irkutsk.ru, ntp2.niiftri.irkutsk.ru (ФГУП «ВНИИФТРИ», г. Иркутск); vniiftri.khv.ru, vniiftri2.khv.ru (ФГУП «ВНИИФТРИ», г. Хабаровск) [12].

Для сравнения шкалы системного времени компьютера пункта контроля с NTP-серверами точного времени использовалась программа-демон ntpd. Принцип определения смещения шкал времени заключался в следующем: а) системное время компьютера синхронизировалось от собственного NTP-сервера «КазСтандарт», реализующего шкалу времени UTC(KZ); б) средствами ntpd регистрировались значения смещения шкал времени контролируемых NTP-серверов; в) с помощью специального программного обеспечения рассчитывалась расширенная неопределённость измерений [12].

Результаты измерений показали, что среднемесячные значения разности шкал времени контролируемых удалённых NTP-серверов «КазСтандарт» в месте контроля (пгт. Менделеево) относительно UTC(SU) составили:

- для NTP-сервера «Астана 1» – от минус 2,1 до 9,1 мс;
- для NTP-сервера «Астана 2» – от минус 2,9 до 9,1 мс;
- для NTP-сервера «Астана 3» – от минус 2,8 до 10,6 мс.

При этом расширенная неопределённость измерений составляла от 2,1 до 20,1 мс [12].

Среднемесячные значения разности шкал времени контролируемых удалённых NTP-серверов ВНИИФТРИ в месте контроля (г. Астана) относительно UTC(KZ) не превышали:

- для NTP-сервера «Менделеево 1» – от минус 9,1 до 2,5 мс;
- для NTP-серверов г. Иркутск 1 и 2 – от минус 6,1 до 5,2 мс;
- для NTP-серверов г. Хабаровск 1 и 2 – от 0,8 до 14,2 мс.

Расширенная неопределённость для серверов Иркутска и Хабаровска достигала 19 мс [12].

Основной вклад в расширенную неопределённость измерений вносит неопределённость по типу А, связанная с задержками в канале связи сети Интернет, которая составляет от 0,2 до 9,5 мс. Неопределённость измерений по типу В составляет от 0,2 до 0,4 мс. Необходимо отметить, что при увеличении времени задержки в канале связи приблизительно на 100 мс разность шкал времени увеличивалась на вдвое меньшую величину – 50 мс. Это свидетельствует о том, что задержка увеличилась только в одном направлении, что привело к асимметрии в ~100 мс [12].

Обсуждение

Из приведённых результатов измерений можно сделать вывод, что синхронизация шкалы времени в сети Интернет составляет единицы миллисекунд, однако при возникновении асимметрии канала погрешность может достигать сотни миллисекунд.

При использовании космической связи или мобильного Интернета приведённые выше значения будут гораздо хуже из-за асимметрии канала связи.

На сайте https://www.ntppool.org/ представлены NTP-серверы всего мира [13]. При этом легитимна на территории Российской Федерации национальная шкала времени UTC(SU), которая распространяется NTP-серверами ФГУП «ВНИИФТРИ».

Аналогично, на территории Республики Казахстан легитимной является национальная шкала времени UTC(KZ), распространяемая NTP-серверами РГП «КазСтандарт». Информация о точном значении времени и календарной дате, распространяемая Государственной службой времени и частоты Республики Казахстан, является обязательной для использования в Республике Казахстан [7].

Используя в сети Интернет неизвестные NTP-серверы уровня Stratum 1, следует отметить следующие особенности их работы.

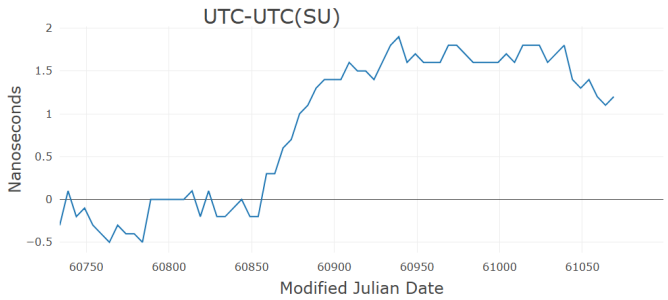


Рис. 4. Смещение ШВ UTC(SU) относительно ШВ UTC.

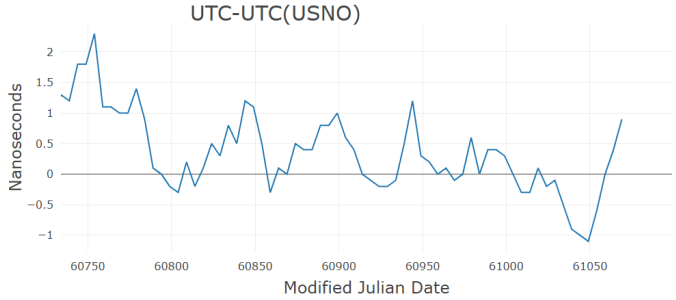


Рис. 5. Смещение ШВ UTC(USNO) относительно ШВ UTC.

К уровню Stratum 1 относятся NTP-серверы, синхронизированные по сигналам ГНСС ГЛОНАСС/GPS. Несмотря на «интимную» близость шкал времени, передаваемых ГНСС ГЛОНАСС и GPS, надо понимать, что спутники GPS могут передавать искажённую информацию о точном значении времени, что может привести к ухудшению точности определения координат на местности. Разность шкал времени UTC(SU) и UTC(USNO) (шкала времени, формируемая в ГНСС GPS военно-морской обсерваторией США; United States Naval Observatory) незначительна, результаты смещений представлены на рисунках 4 и 5 [14].

Проблема надёжности сигналов ГНСС в последние годы существенно обострилась. Помимо спуфинга (spoofing – передача заведомо ложных данных) и джемминга (jamming – помехи на частотах L1 и L2), возрастают риски воздействия промышленных шумов и ограничений, связанных с плотной застройкой. Эти факторы создают серьёзные риски для работы телекоммуникационных сетей и других критически важных систем, что повышает значимость собственных национальных эталонов времени и их NTP-серверов как независимых от ГНСС источников точного времени [1].

В соответствии с федеральным законом от 26 июня 2008 г. № 102-ФЗ «Об обеспечении единства измерений» в сфере государственного регулирования должны использоваться средства измерений утверждённого типа. Многие организации при оказании различного вида услуг в своих локальных сетях связи используют устройства синхронизации времени, в том числе NTP-серверы, утверждённого типа. Передача единиц величин осуществляется в соответствии с Государственной поверочной схемой для средств измерений времени и частоты, утверждённой приказом Росстандарта от 26 сентября 2022 года № 2360.

Выводы

На территории Российской Федерации в качестве источника точного времени рекомендованы к использованию NTP-серверы ФГУП «ВНИИФТРИ» и NTP-серверы утверждённого типа, имеющие нормированные метрологические характеристики.

На территории Республики Казахстан рекомендованным источником точного времени являются NTP-серверы РГП «КазСтандарт», привязанные к национальной шкале времени UTC(KZ).

Погрешность синхронизации шкалы времени в сети Интернет относительно национальной шкалы времени UTC(SU) в локальных сетях составляет не более ±100 мкс, в глобальной сети Интернет - ±3 мс, при этом сильно зависит от асимметрии канала связи и топологии сети.

Результаты сравнений шкал времени NTP-серверов ФГУП «ВНИИФТРИ» и РГП «КазСтандарт» в рамках проекта КООМЕТ 605/RU/13 подтвердили, что расширенная неопределённость измерений при сравнении через Интернет на международных расстояниях составляет от единиц до десятков миллисекунд, а основным источником погрешности является асимметрия задержки прохождения пакетов NTP в каналах связи. Точность, обеспечиваемая протоколом NTP, изменяется в зависимости от нагрузки на сеть. Гарантировать более высокую точность синхронизации шкал времени по протоколу NTP не представляется возможным из-за непредсказуемых сетевых задержек [9].

Перспективным направлением повышения точности сравнений является переход на протокол PTP (IEEE 1588) и технологию White Rabbit с использованием волоконно-оптических каналов связи, что позволит достичь точности синхронизации на уровне субнаносекунд [1].

Источники:

[1] С.Б. Смагулов. Перспективы развития систем синхронизации в сетях связи и инфраструктурных объектах Республики Казахстан // Научный журнал «Smart». – 2025. – № 3(93).

[2] Федеральный закон «Об исчислении времени» от 03.06.2011 № 107-ФЗ.

[3] ГОСТ 8.567-2014 «Государственная система обеспечения единства измерений. Измерения времени и частоты. Термины и определения».

[4] С.Л. Пасынок, И.В. Безменов, И.Ю. Игнатенко, Е.Н. Цыба, В.Е. Жаров, «Совершенствование методов и средств Главного метрологического центра Государственной службы времени, частоты и определения параметров вращения Земли», Измерительная техника № 5, 2020.

[5] https://hpiers.obspm.fr/iers/bul/bulc/TimeSteps.history

[6] https://www.vniiftri.ru/catalog/services/sinkhronizatsiya-vremeni-cherez-ntp-servera

[7] С.Б. Смагулов. Государственный первичный эталон единиц времени, частоты и национальной шкалы времени Республики Казахстан // Альманах современной метрологии. – 2024. – № 4(40). – С. 243–255.

[8] С.Б. Смагулов. Применение пассивных водородных стандартов частоты для формирования национальных шкал атомного времени. Автореферат дисс. на соискание учёной степени канд. техн. наук. – Томск: ТПУ, 2026. (защита назначена на 29.06.2026).

[9] Smagulov, S.B., Mishagin, K.G., Kagan, S.N. et al. Experimental Study of Uncertainty in Comparing Time Scales of National Standards of Kazakhstan and Russia on the Internet Using NTP Servers. Russian Physics Journal 66, 591–596 (2023). https://doi.org/10.1007/s11182-023-02980-7

[10] Каган С.Н., Блинов И.Ю., Семёнов С.А. В книге: Метрология в радиоэлектронике. Тезисы докладов X Всероссийской научно-технической конференции. Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт физико-технических и радиотехнических измерений» (ФГУП «ВНИИФТРИ»). 2016. С. 333-338.

[11] С.Н. Каган, С.В. Пестерев «Результаты экспериментальных исследований реальной неопределённости шкал времени потребителей NTP-серверов уровня Stratum I», Альманах современной метрологии, 2016, № 8.

[12] Smagulov, S.B., Mishagin, K.G., Kagan, S.N. et al. Experimental Study of Uncertainty in Comparing Time Scales of National Standards of Kazakhstan and Russia on the Internet Using NTP Servers. Russian Physics Journal 66, 591–596 (2023). https://doi.org/10.1007/s11182-023-02980-7

[13] http://www.ntp.org

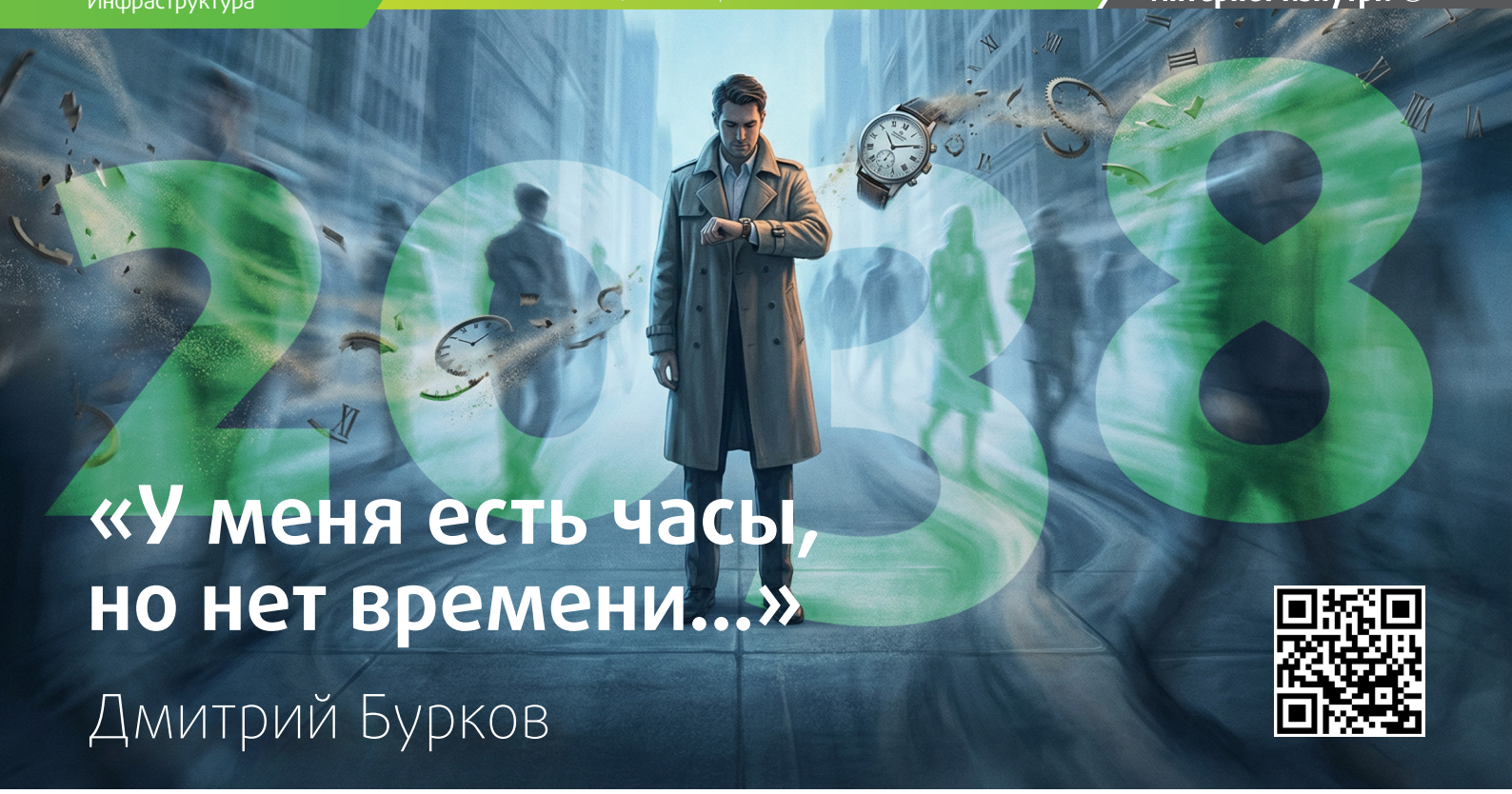
[14] https://webtai.bipm.org/database/canvas.html

Об авторах:

Семёнов Сергей Александрович,
ФГУП «ВНИИФТРИ», Россия, пгт. Менделеево.

Семёнова Екатерина Игоревна,
ФГУП «ВНИИФТРИ», Россия, пгт. Менделеево.

Смагулов Султанбек Берикулы, магистр электроэнергетики и электротехники, учёный-хранитель ГЭВЧ РК, РГП «КазСтандарт», Казахстан, Астана; аспирант Национальный исследовательский Томский политехнический университет, Томск, Россия.



«У меня есть часы, но нет времени...»

Дмитрий Бурков

Многие уже забыли о шумихе, поднятой вокруг так называемой проблемы Y2K. Однако уже тогда, на рубеже тысячелетий, в профессиональном сообществе говорили о следующей потенциальной угрозе, связанной с компьютерными системами, — о проблеме Y2038. В отличие от Y2K, эта тема не привлекла широкого внимания в медиа, не стала причиной громких инициатив и государственных программ, хотя по глубине и масштабу возможных последствий она может оказаться даже более серьёзной. Она не воспринимается на том же уровне, что экологические проблемы или глобальное потепление: существует негласное ожидание, что её удастся решить по мере приближения критической даты.

Однако человеческая природа такова, что мы склонны откладывать сложные задачи — особенно те, последствия которых проявятся лишь через десятилетия.

Что такое проблема 2038 года?

Проблема 2038 года (также известная как Y2K38, или ошибка Unix-времени) возникает из-за особенностей хранения и обработки дат в некоторых программных системах. Когда счётчик времени достигнет значения, соответствующего 03:14:07 UTC 19 января 2038 года, системы, использующие устаревший способ хранения времени, могут либо выдавать ошибки, либо некорректно интерпретировать даты.

Чтобы понять природу этой проблемы, необходимо обратиться к истории.

Одним из наиболее распространённых способов представления времени является так называемая временная метка Unix (Unix timestamp), или время эпохи Unix. В этой модели дата выражается как количество секунд, прошедших с полуночи 1 января 1970 года (UTC). Этот подход оказался настолько удобным, что стал широко применяться — не только в Unix-подобных операционных системах, но и в языках программирования, базах данных и различных прикладных платформах.

Проблема возникает, когда для хранения таких значений используется 32-битное знаковое целое число. Максимальное значение, которое может быть представлено в этом формате, составляет 2 147 483 647 секунд. Этот предел достигается 19 января 2038 года в 03:14:07 UTC. Уже в следующую секунду происходит переполнение, и значение становится отрицательным, что в большинстве систем интерпретируется как дата в декабре 1901 года.

Важно отметить, что эта проблема не ограничивается только Unix-системами. Поскольку формат Unix-времени широко использовался как де-факто стандарт, уязвимыми могут оказаться самые разные системы — от встроенных устройств до корпоративных информационных платформ.

Как проверить, затронута ли система?

Проверка системы на уязвимость к Y2038 — сложная и трудоёмкая задача. Не существует универсального теста, позволяющего быстро получить однозначный результат. Вместо этого требуется комплексный аудит архитектуры системы и всех её компонентов.

Дополнительную сложность создаёт тот факт, что сбои могут проявляться по-разному в зависимости от логики работы системы. Например, система, сравнивающая текущую дату с будущими значениями, может выйти из строя раньше, чем та, которая лишь фиксирует временные метки в журналах.

При аудите следует обратить внимание на:

- встроенные системы, использующие 32-битные знаковые временные метки;
- аппаратное обеспечение под управлением 32-битных

операционных систем или ПО;
- базы данных, где время хранится в виде 32-битных целых чисел;
- программное обеспечение, работающее с такими представлениями времени;
- исходный код, содержащий операции сравнения дат и временных интервалов;
- алгоритмы, выполняющие расчёты с использованием времени в будущем или прошлом.

Особое внимание следует уделить критически важным системам, отказ которых недопустим даже на короткое время.

Ограничения и ложные гарантии

Важно понимать: даже использование 64-битных систем не гарантирует отсутствия проблемы. Внутри таких систем данные могут по-прежнему храниться в 32-битном формате — например, в устаревших модулях, сторонних библиотеках или при обмене данными с другими системами. Более того, даже полностью обновлённая система может зависеть от внешних компонентов, сохраняющих уязвимость.

С другой стороны, не всякое 32-битное программное обеспечение подвержено этой проблеме. Многие современные программы используют структуры данных, способные корректно работать с временными диапазонами, выходящими далеко за пределы 2038 года. Поэтому единственный надёжный способ оценки — это тщательный анализ конкретной реализации.

Как исправить проблему?

Универсального решения проблемы Y2038 не существует — каждая система требует индивидуального подхода. После выявления уязвимостей возможны следующие варианты:

- переход на 64-битные типы данных — наиболее надёжное и долгосрочное решение;
- использование альтернативных форматов представления времени — адаптация кода для работы с расширенными временными диапазонами;
- изоляция уязвимых компонентов и введение промежуточного слоя (middleware), транслирующего временны́е значения, — как временная мера для систем, которые невозможно обновить напрямую;
- плановая замена устаревших систем — особенно встроенного оборудования и промышленных контроллеров, для которых обновление программного обеспечения технически невозможно.

Выбор зависит от архитектуры системы, доступных ресурсов и критичности её функций.

Y2038 и Y2K: сходства и различия

Проблему 2038 года часто сравнивают с Y2K. В обоих случаях корень проблемы — ограниченность формата представления даты. Однако различия между ними принципиальны.

Проблема Y2K была связана с хранением года в двухзначном формате («00» вместо «2000») и затрагивала преимущественно прикладной уровень. В свою очередь, Y2038 обусловлена фундаментальным ограничением разрядности и затрагивает более глубокие уровни — операционные системы, протоколы и встроенное ПО. Это делает её технически сложнее и труднее поддающейся локализованному исправлению.

Кроме того, Y2K сопровождалась масштабной подготовкой и значительным финансированием, что позволило минимизировать последствия. Проблема Y2038 пока не получила сопоставимого внимания — и именно в этом заключается главный риск.

Приведёт ли это к катастрофе?

Скорее всего, нет.

К 2038 году большая часть программного обеспечения, вероятно, будет переведена на 64-битные системы. Критически важные инфраструктуры, вероятно, будут модернизированы заранее. Более того, часть решений, разработанных в рамках подготовки к Y2K, уже учитывала проблему 2038 года.

Тем не менее, риск остаётся. Ошибки могут сохраняться годами и проявляться неожиданно. Особую опасность представляют системы без доступного исходного кода или те, которые невозможно обновить — например, встроенные устройства и промышленное оборудование с длительным сроком службы.

Заключение

Проблема 2038 года способна по-разному повлиять на различные системы: для одних она станет незначительным техническим эпизодом, для других — источником критических сбоев.

Проблема Y2038 — не технический курьёз и не повод для паники, а напоминание о том, что цифровая инфраструктура несёт в себе архитектурные решения прошлого, принятые в условиях иных ограничений. История Y2K показала: когда общество и индустрия мобилизуются заблаговременно, катастрофы удаётся избежать. Вопрос в том, будет ли урок усвоен снова — или мир вновь предпочтёт ждать, пока проблема не постучит в дверь сама.

«Не говорите о том, что у вас нет времени...» — время есть.
Вопрос лишь в том, как мы им распорядимся.

Об авторе:

Дмитрий Владимирович Бурков — один из пионеров интернет-отрасли в России, был председателем президиума Фонда содействия развитию технологий и инфраструктуры Интернета (FAITID), один из инициаторов создания Евроазиатской группы сетевых операторов (ENOG), бывший криптоофицер Западного центра ICANN. АНО «ЦВКС МСК-IX»

Влияние неверного времени на отказ систем и инциденты безопасности

Глеб Дубодел

Аннотация
Статья рассматривает влияние сбоя сетевого времени в телекоммуникационной инфраструктуре на её работоспособность. Проанализированы варианты ошибок, к которым может привести сбой времени, и их возможное влияние на анализ и расследование инцидентов информационной безопасности. Также в статье рассматриваются меры по минимизации рисков ошибок времени в IT-инфраструктуре.

Ключевые слова:
NTP, шифрование, IT-инфраструктура, SIEM, инциденты информационной безопасности

Время – величина, определяющая длительность протекания процессов, оно позволяет нам определять себя в направлениях «было», «сейчас», «будет». Но если живые существа могут осознавать время, его движение, то техника и инструменты не имеют данного восприятия. Следовательно, у них нет понятия единого правильного восприятия времени, у каждой техники, каждого инструмента своё «правильное» время.

При постепенном развитии компьютерных сетей возникла проблема несогласованности времени на хостах, разница во времени искусственно увеличивала время доставки сетевых пакетов, из-за чего они считались уже недействительными при получении. Для согласования времени был создан протокол NTP (Network Time Protocol). Данный протокол принёс согласование времени в сети относительно UTC, с формированием иерархии NTP-серверов.

Со временем компьютерные сети расширялись, соединялись и постепенно стали общедоступными. Изначально для работы было достаточно использовать протоколы, работающие в открытом виде, без применения методик скрытия или защиты передачи данных. Интернет вошёл в жизнь общества. Количество пользователей начало стремительно расти, появилась необходимость решения ряда вопросов по защите передаваемой информации:

- точно ли, что никто кроме получателя не сможет понять передаваемую информацию?
- точно ли итоговый получатель является изначально запланированным получателем?

Для ответа на данные вопросы было принято решение развивать криптографию в компьютерных технологиях.

Данное решение привело к развитию двух направлений:

- криптография для передачи: для безопасной передачи данных было введено шифрование данных, что позволяло обеспечить защиту данных при передаче. В качестве обеспечения однозначного шифрования/дешифрования данных в качестве общего секрета было решено использовать время, поскольку оно уже было синхронизировано через протокол NTP;
- сертификаты для подтверждения идентичности: для подтверждения конечных хостов была сформирована концепция PKI, в основе которой используются сертификаты безопасности для подтверждения идентичности. Сертификат безопасности выступает гарантом того, что владелец является тем, за кого себя выдаёт. Сертификаты безопасности имеют срок применения, а также используют в своей работе время UTC для шифрования.

Таким образом время укоренилось в компьютерных технологиях, став их неотъемлемой частью. Когда используется верное и согласованное время, всё хорошо и все системы работают штатно. Рассмотрим, к чему может привести неверное сетевое время, появившееся в результате ошибки или целенаправленного влияния.

Можно выделить следующие основные группы последствий:

- сетевые сбои;
- сбои отдельных хостов;
- сбои отдельных приложений.

Сбои в работе сети

Несинхронизированное в сети время может привести к ошибкам взаимодействия следующего рода:

- Некорректная работа контроллеров домена, состоящего из множества компьютеров: контроллеры домена во время своей работы используют время во множестве сетевых протоколов, и несогласованность домена во времени может парализовать весь домен. Первые ошибки возникнут на уровне протоколов аутентификации, работа которых связана с использованием временных меток. Неправильная аутентификация приведёт к прекращению работы инфраструктурных служб, что приведёт к отказу доступности некоторых функций домена.

- Изоляция инфраструктуры: чаще всего контроллер домена выступает в качестве локального NTP-сервера инфраструктуры. Если NTP-сервер настроен неверно, он также будет реплицировать неверное время на другие устройства сети, что сделает невозможным доступ во внешнюю сеть. Для безопасности в NTP-серверах применяют безопасные версии протоколов, которые в своей работе используют временные метки.
- Неправильная работа протоколов аутентификации: протоколы аутенти-фикации используют в своей работе временные метки для повышения вероятности корректного и однозначного идентифицирования пользователя в сети. Если на конечном хосте используется неверное время, при попытках аутентификации его сессия будет считаться уже истекшей или невалидной, за счёт использования временных меток в криптографических протоколах. В качестве примера можно привести протокол Kerberos, формирование тикетов которого привязано к времени.
- Использование неактуальных данных аутентификации: в доменных именах, отключённых от сети домена, последние данные, с которыми был совершён успешный вход в домен, некоторое время считаются верными и хранятся в качестве кеша. Смена времени позволит вернуть актуальность уже истекшим данным аутентификации, что может быть использовано злоумышленником.
- Недоступность сетевых ресурсов: несогласованность во времени внутри сети приводит к вопросу согласования протоколов: невозможность использования безопасных сетевых протоколов приведёт либо к выбору менее защищённых протоколов, либо к невозможности установки соединения.
- Истекшие сертификаты: как было описано выше, для передачи данных в сети было внедрено шифрование, использующее время UTC в своей основе. Если хост в сети имеет время, отличное от локального, его сертификаты будут считаться некорректными, что приведёт к некорректной работе сетевых протоколов.

Сбои в работе отдельных хостов

Рассмотрев обще инфраструктурные ошибки, можно перейти к аномалиям на отдельных хостах. Неправильное время отдельного хоста может сильно ограничить его связь с миром либо привести к ряду ошибок:

- Ошибки работы приложений: некоторые приложения активно используют сеть Интернет во время работы или во время запуска для проверки лицензии. Такие приложения используют собственные или стандартизированные безопасные протоколы для доступа в Интернет, неправильное время хоста может привести к невозможности использования безопасных протоколов, что повлияет на работу приложений.
- Ошибки в работе планировщика задач: некоторые задачи на отдельных хостах, такие как проверка доступных обновлений, создание бэкапов, настроены работать через планировщики задач по триггерам или по времени. Разовые ошибки подобного рода не являются критичными, однако при их накоплении это может привести к неприятным последствиям.
- Установка локальных обновлений: если в инфраструктуре есть свой центр распределения обновлений Windows, то конечный хост с неправильным временем не сможет получать локальные обновления системы, что сделает его уязвимым.

Сбои в работе приложений

Ну и последняя линия, где возможны ошибки, возникшие из-за неправильного времени, - уровень приложений. Неправильное время конечного хоста может привести к ошибкам следующего рода:

- Использование неактуальных протоколов: при инициализации сетевого соединения на уровне приложений определяется, какие сетевые проколы будут задействованы. Выбор всегда осуществляется от наиболее защищённых к менее защищённым, при условии, что все члены соединения должны поддерживать предлагаемый протокол. Все современные протоколы содержат в себе временные метки, из-за чего выбор будет осуществлён в сторону менее защищённых. В качестве примера можно привести ситуацию, когда нет возможности установить соединение через протокол FTPS (FTP over SSTL/TLS), в таком случае для передачи будет использоваться протокол FTP, протокол не шифрует данные, передавая их в открытом виде.
- Ошибки синхронизации данных: подобные ошибки могут возникнуть по нескольким причинам: хост не может связаться с сервером синхронизации данных или хост не может валидировать актуальность данных. В первом случае ошибка возникает из-за невозможности установки соединения по безопасным сетевым протоколам. Во втором случае из-за смены времени конечный хост не может подтвердить актуальность данных на сервере синхронизации, считая их либо устаревшими, либо более актуальными, что может привести к потере данных.
- Ошибки работы лицензии программного обеспечения: при работе с коммерческими продуктами лицензия подтверждается за счёт нескольких факторов: текущая дата, время действия лицензии, подтверждение со стороны сервера лицензирования. Неактуальность одного из факторов может привести к прекращению работы лицензионного ПО.

Инциденты информационной безопасности

Разобравшись с влиянием неверного времени на инфраструктуру, можно перейти к анализу влияния на инциденты информационной безопасности.

Неверное время конечного хоста приведёт к ряду взаимосвязанных проблем:

- Отправка логов событий в прошлое/будущее: SIEM-системы берут логи событий систем с помощью агентов-сборщиков. Агенты собирают данные с конечных хостов, проводя первичное обогащение событий (добавление временных меток и другой метаинформации) с последующим отправлением данных на коллектор событий. Коллектор событий собирает данные со множества устройств без их анализа, его главная задача - передать данные на обработку в SIEM-систему. Иногда коллектор производит обогащение данных (добавление служебных меток). Такой алгоритм событий приводит к возможности отправки событий в прошлое или будущее.
- Обход правил безопасности: SIEM-системы анализируют трафик, поступающий с коллектора в реальном времени, с помощью правил корреляции (событие А и последующее

событие В = срабатывают правила безопасности). При этом правила безопасности работают с определённым временным интервалом. В качестве примера: правило срабатывает один раз в 10 минут с анализом событий за прошедшие 10 минут. Однако из-за некорректных временных меток события не попадают во временные рамки правил безопасности SIEM или нарушается временная корреляция между взаимосвязанными событиями, что приводит к обходу правил безопасности SIEM, кратно снижая эффективность системы в зависимости от размера инфраструктуры.

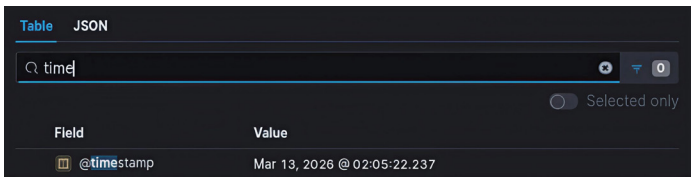
- Осложнённый сбор дельты событий: поскольку логи событий были отправлены по неправильной временной метке, а также на каждом этапе перемещения логов добавляются своя метаинформация и свои временные метки, возникает проблема корреляции созависимых событий, а именно дельта событий распределяется по всем временным меткам, что в разы усложняет составление таймлайна инцидента безопасности.
- Повторное использование сетевых пакетов: если IT-инфраструктура не подразумевает средств одноразового и однозначного использования сетевых пакетов, злоумышленник может использовать сетевые пакеты повторно, проводя атаки рода replay. Подобные атаки направлены на перехват сетевого трафика. Проанализировав трафик, злоумышленник определяет пакет успешной аутентификации, актуализирует в нём временные метки и повторно его отправляет, тем самым успешно аутентифицируясь.

Proof of concept

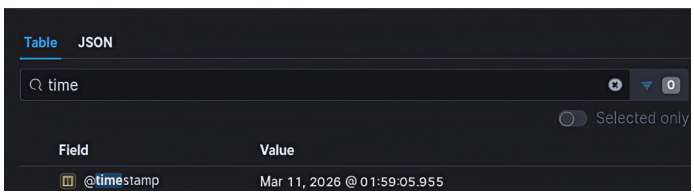
Для практического доказательства возможности обхода средств мониторинга и антифорензики с помощью времени был создан стенд с SIEM-системой с подключённым к ней хостом под управлением ОС Windows.

Был смоделирован кейс: на целевом хосте было изменено время (с 13 марта 2:00 на 11 марта 2:00), что отразилось на графике событий:

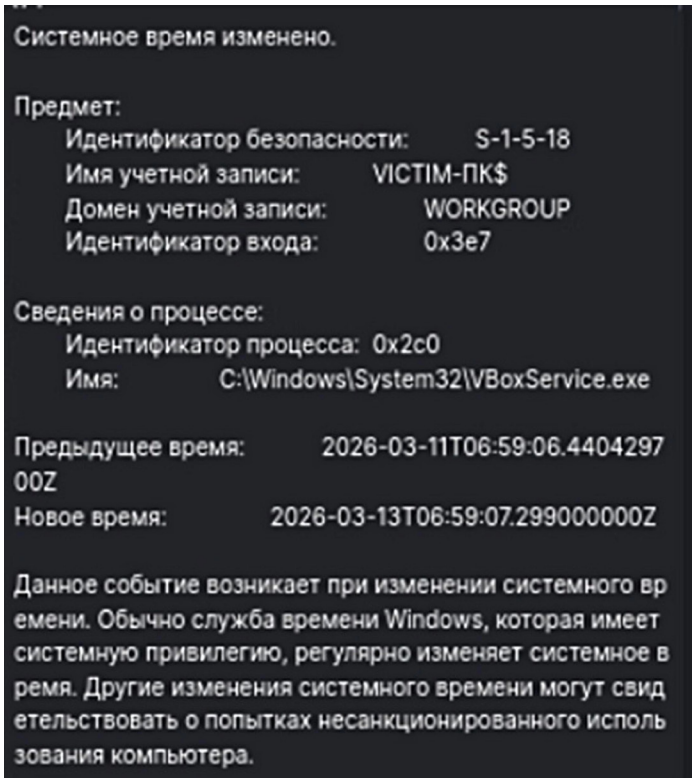
Временная метка события до смены времени:



Временная метка события после смены времени:



Событие изменения времени:



Также смена времени приводит к артефактам на хосте, что может быть использовано злоумышленником для антифорензики:

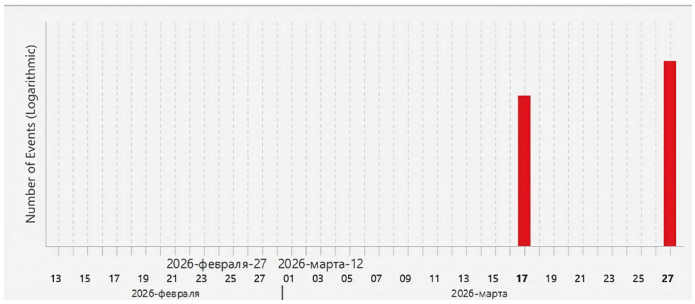


Рис. 1. Появление на хосте артефактов.

В данном тесте предполагаемый злоумышленник отправил хост в будущее, что видно из расследования при форенсическом анализе снятого образа хоста-жертвы. Использование данной техники злоумышленником усложнит расследование.

Итог:

В данном кейсе получилось смоделировать изменение времени конечного хоста, что повлияло на корректность работы SIEM-системы: данные с хоста пришли в «прошлое», что позволило событиям хоста обойти правила корреляции, не скрывая сам факт активности. Данная особенность средств защиты может быть использована злоумышленником в своих целях.

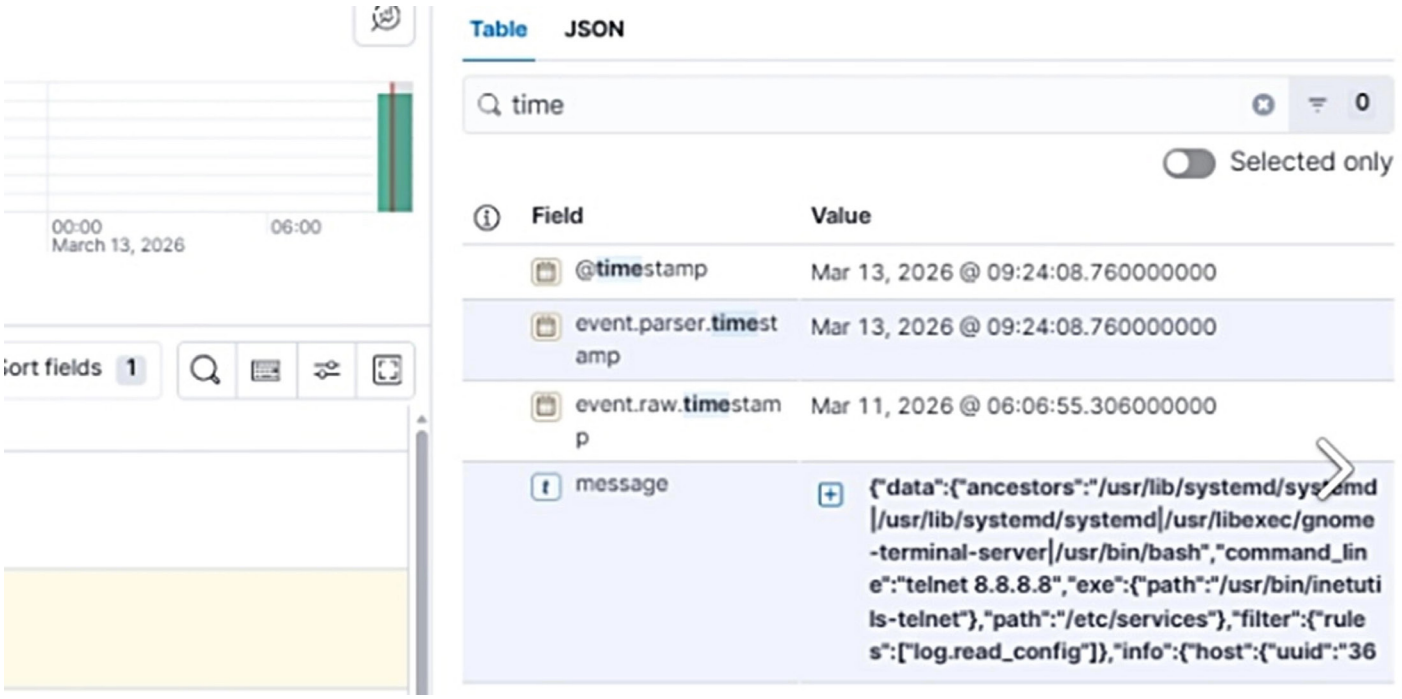


Рис. 2. Добавление дополнительных временных меток.

Защита:

Рассмотрев методы реализации угрозы, крайне важно также рассмотреть методы противостояния этой угрозе.

В данном случае наиболее простым и надёжным методом защиты будет обогащение данных. А именно, добавление дополнительных временных меток. В описываемом случае было решено добавить данные времени на каждом этапе прохождения события:

Мы можем видеть сразу несколько временных меток: event.raw.timestamp (время события с хоста источника), event.parser.timestamp (время получения события коннектором), @timestamp (время получения события ядром SIEM-системы). В данном случае @timestamp является основной временной меткой, что делает изменения времени хоста бесполезным для обхода правил корреляции SIEM-системы.

Выводы

Определив, как присутствует время в инфраструктуре, к каким ошибкам может привести сбой времени и как неверное имя может повлиять на инциденты информационной безопасности, необходимо определить основные методы защиты от подобных ошибок:

- Использование сервисов синхронизации времени с шифрованием: использование NTP-серверов внутри инфраструктуры явная необходимость. Однако стоит отметить важность использования защищённых версий протокола NTP: NTPv4, NTS.
- Создание своего NTP-сервера: исторически сложилось так, что число публичных NTP-серверов в пространстве интернет-сегмента .ru относительно небольшое, и это может стать фактом их ненадёжности. Для повышения надёжности необходимо использование своего NTP-сервера в инфраструктуре, что можно обеспечить с помощью контроллера домена, так как они поддерживают данный функционал.
- Ограничение количества обращений к источникам времени: NTP-протокол уязвим для атак типа DoS и Poising, поэтому при настройке крайне важно ограничить как количество пользователей, которые могут обращаться к NTP-серверу, так и количество возможных обращений.

Источники:

[1] https://www.ntp.org/reflib/exec/

[2] https://learn.microsoft.com/ru-ru/windows-server/networking/windows-time-service/how-the-windows-time-service-works

[3] https://habr.com/ru/articles/942932

[4] https://habr.com/ru/articles/876536

[5] https://support.kaspersky.ru/xdr-expert/1.1.8/265140

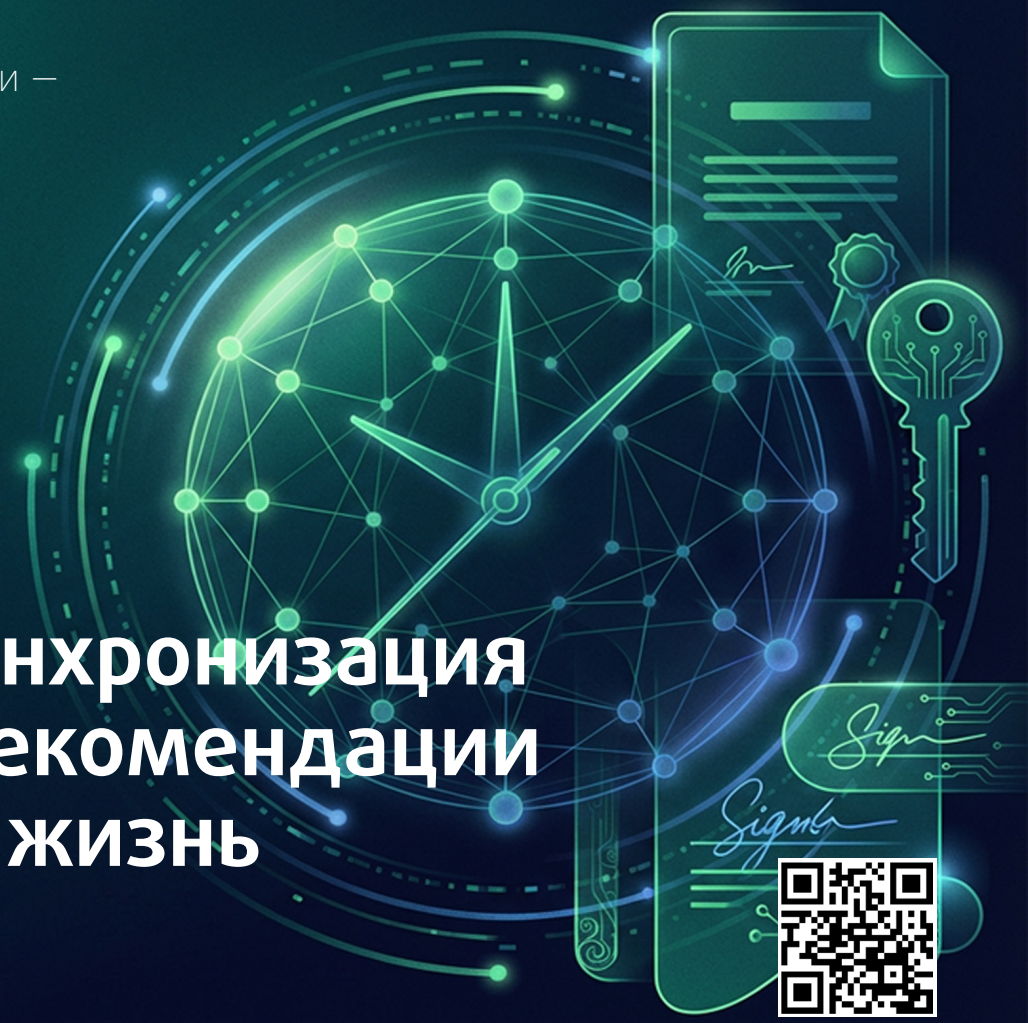
[6] https://mikrotik.wiki/wiki/%D0%A2%D0%B5%D0%BE%D1%80-%D0%B8%D1%8F:%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B:NTP

Об авторе:

Дубодел Глеб Дмитриевич, аналитик SOC L1, ООО «Юзергейт»

«Единственная причина для существования времени — чтобы всё не случилось одновременно»

Альберт Эйнштейн



DNSSEC и синхронизация времени: рекомендации и реальная жизнь

Павел Храмцов

Аннотация
Критичность времени в DNSSEC обусловлена использованием криптографических подписей (RRSIG) с ограниченным сроком действия (обычно 1–4 недели). Синхронизация времени необходима для предотвращения недоступности сайтов из-за просроченных подписей. Слишком короткие сроки действия могут вызвать сбои при смене ключей, а слишком длинные — риски безопасности.
Требуемая точность — в пределах нескольких минут (обычно безопасным считается расхождение не более 1–5 минут), чтобы избежать проблем с преждевременным истечением или запоздалым вступлением подписей в силу.

Ключевые слова:
DNSSEC, резолвинг, домен

Расширение безопасности DNS, или DNSSEC, призвано детектировать подмену ответов авторитетных DNS-серверов и тем самым предотвратить атаки типа «отравление кеша».

Концепция DNSSEC позволяет DNS-резолверу (серверу, который обслуживает приложения конечного клиента) принимать ответы от любого DNS-сервера, где бы он ни был расположен и под чьим бы управлением ни находился. При этом за счёт построения цепочки доверия на основе криптографии с открытым ключом ответы проверяются на корректность и истинность. На основе этой проверки DNS-резолвер принимает решение об их трансляции и соответствующим образом отвечает приложениям конечного клиента.

При таком раскладе поломка механизма DNSSEC может привести к полному прекращению процедуры резолвинга. Такие сервисы, как, например, веб или электронная почта, станут недоступны. Вообще говоря, недоступными станут любые сервисы, в которых используются доменные имена.

Наиболее наглядно это видно, когда поломка случается в критически важных точках, например, на серверах корня DNS (m.root-servers.net – 2010, j.root-servers.net – 2013), в национальных зонах (например, зона .ru - 2024) или в зонах домена in-addr.arpa (зоны под управлением APNIC - 2016).

В настоящее время по технологии DNSSEC подписано примерно 25 миллионов доменов (столько DS размещено в файлах зон доменов разных уровней) [1]. При этом доменов второго уровня в доменах верхнего уровня (Top Level Domains

– TLD) всего насчитывается чуть меньше 387 миллионов. Если учесть, что среди подписанных доменов доля доменов третьего уровня и ниже исчезающе мала, то DNSSEC используется примерно для 6,5% доменных имён.

Однако следует иметь в виду, что на 30 марта 2026 года из 1594 TLD подписаны 1486 (93%) [2]. Это все домены общего назначения и подавляющая часть национальных доменов. В национальной доменной зоне .ru на 30 марта 2026 года из 6 115 946 доменов подписано только 9793 (0,16%) [3].

В целом статистика применения DNSSEC на 30 марта 2026 года представлена на рисунке 1 [4].

Цепочка доверия в DNSSEC выстраивается от корня системы DNS. Следовательно, поломка DNSSEC в TLD приведёт к «отключению» всего TLD, даже если домены второго и ниже уровней подписаны не будут.

Самая частая причина таких поломок – это ротация ключей DNSSEC. Как показывает статистика [4], до 30% подписанных доменов, главным образом национальных, имели те или иные проблемы с применением DNSSEC. Большая часть «поломок» приходится на NSEC3 (70%).

При использовании DNSSEC администратор DNS-зоны встречается с последовательностью действий (последовательность изменения набора ключей/подписей, например) и установками времени в полях записей описания ресурсов DNSSEC.

Следующие поля определяют временные параметры и временные интервалы:

А) TTL – время кеширования записей описания ресурсов на DNS-резолверах. Это стандартное поле для любой записи описания ресурсов (resource record - RR), которая имеет формат:

[Name] [TTL] [Class] [Type] [RDATA]

Где:
[Name] – доменное имя;
[TTL] – время кеширования на DNS-резолвере;
[Class] – IN/CH/CS/HS;
[Type] – тип записи (например, A – задает IP-адрес формата IPv4);
[RDATA] – содержание данного поля зависит от типа записи.

Записи, определённые в стандартах DNSSEC, как и прочие RR имеют поле TTL.

Б) Поля времени в записи RRSIG (подпись набора однотипных RR-записей) в поле [RDATA]:

Original TTL – установленное на авторитетном сервере время TTL для набора RR (RR Set). Данное поле необходимо указывать, т.к. в ответах DNS-резолверов время TTL всё время уменьшается, фактически показывая, сколько времени осталось записи существовать в кеше резолвера.

Signature inception – дата и время начала действия подписи. Указывается с точностью до секунды в секундах от 1 января 1970 года.

Signature expiration - дата и время окончания действия подписи. Указывается с точностью до секунды в секундах от 1 января 1970 года.

Два этих последних параметра абсолютного времени определяют время жизни (валидности) подписи (RRSIG). Максимальный период, который можно задать этими двумя параметрами, равен примерно 136 годам. Поскольку данные поля задают десятичные числа без знака и имеют ограниченную размерность, то возможна ситуация wrap-around, когда время окончания действия подписи выходит за максимально возможное десятичное число (32-битовое целое без знака). В этом случае число, определяющее начало периода действия подписи, будет больше числа, задающего конец периода действия подписи.

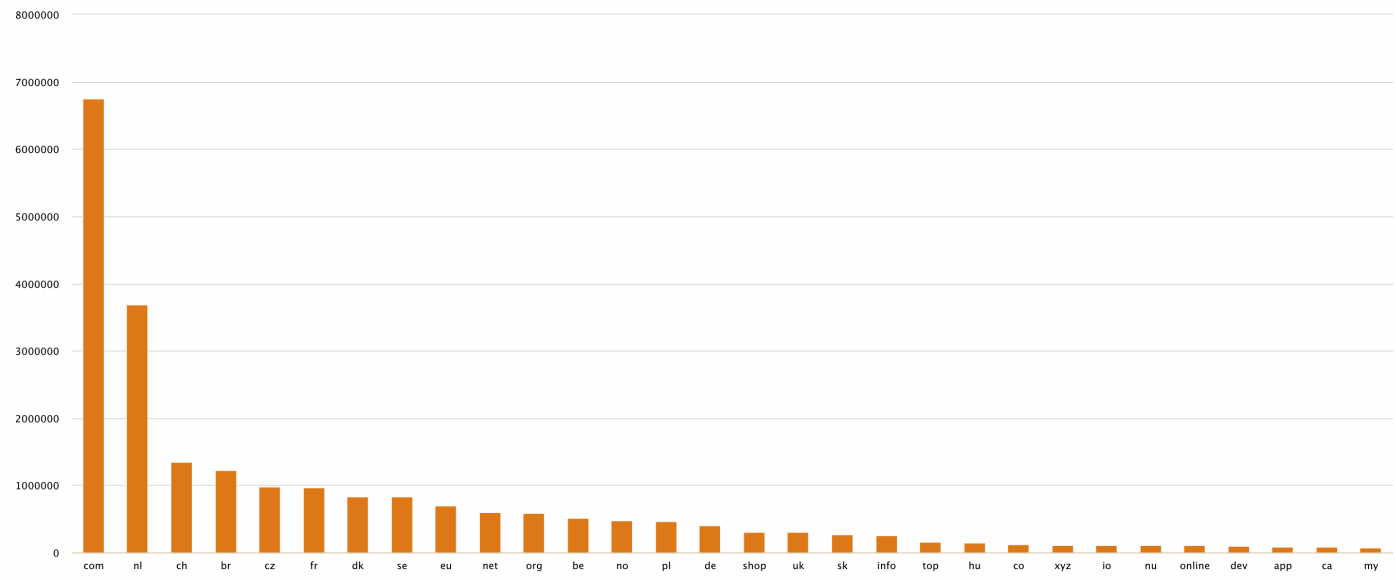


Рис.1. Статистика внедрения DNSSEC в доменах верхнего уровня.

Числа эти могу быть заданы либо в формате целого десятичного числа, либо в виде «YYYYMMDDHHMMSS». Форматы легко различимы: 32-битное целое – это десятичное число не более 10 цифр, а во втором случае всегда будет ровно 14 цифр.

Собственно, вокруг этих параметров и происходят «пляски с бубнами», которые возникают при ротации ключей.

Ротация ключей определяется требованиями безопасности. Ключ можно подобрать или сломать, хоть это и сложно. Следовательно, ключ нужно регулярно менять, т.е. ключ действителен в течение ограниченного промежутка времени. Соответственно, и подписи наборов RR-записей тоже надо менять в порядке замены ключей.

Таким образом, понятие времени жизни ключа, процедура его замены и синхронизация по времени ключей и других записей DNS становится критически важной для работы всего Интернета.

А ещё важна последовательность действий – «чтобы всё не случилось одновременно» или в неправильном порядке.

Переподписывание зоны и ротация ключей (это, вообще говоря, не одно и то же) выглядит следующим образом:

1. Выбор алгоритмов (например, RSA/SHA-256, ECDSAP256SHA256) и политики ротации ключей (ZSK — ключ подписи RR-сетов, KSK — ключ подписи ключей).

2. Создание пары новых ключей (публичный и приватный).

3. Подписи всех записей зоны новыми ключами. В результате создаётся подписанный файл зоны.

4. Временное хранение старых и новых ключей (pub-переход) для обеспечения плавного перехода без перерыва в обслуживании.

5. Если ротируется KSK, хеш нового публичного ключа (DS-запись) отправляется в корневую зону (ICANN для gTLD) для проверки.

6. Переподписанный файл зоны загружается на DNS-серверы, обновляется серийный номер зоны (SOA) для инициации передачи зон (AXFR/IXFR).

Первый пункт в этом списке имеет косвенное отношение ко времени – типа, «всё течет, всё изменяется», и алгоритмы тоже меняются.

Так какие же временные интервалы и значения параметров времени рекомендовано устанавливать? Ниже приведены две основные рекомендации:

- частоту ротации ключа ZSK разумно взять в интервале от одного до трёх месяцев (в национальных доменах Российской Федерации – три месяца);

- частоту ротации ключа KSK рекомендуют выбрать в 1-3 года.

Толстовское «гладко было на бумаге...» справедливо и к исполнению данных рекомендаций.

Согласно данным IANIX [5], с 2009 года в TLD зафиксирована 221 поломка DNSSEC.

Чаще всего проблемы связаны с ротацией ключей.

Во-первых, встречается ситуация, когда новый KSK уже опубликован, а в старшей зоне остаётся старая запись DS. Таким образом, проблема вызвана неправильной последовательностью действий во времени.

Во-вторых, DNS-резолверы кешируют записи описания ресурсов на время TTL. Кешируют в том числе ключи и подписи DNSSEC. Если ключ будет удалён из зоны раньше, чем истекает время его кеширования (TTL), то резолверы будут выдавать ошибки.

В-третьих, ротация ключей KSK требует координации с размещением DS-записи в старшей зоне. Данная процедура неавтоматическая и требует участия персонала. Как показывает практика, на этом этапе возникает много несогласованности, что приводит к «поломкам».

В-четвертых, критической ошибкой является удаление ключа из файла зоны, который связан DS-записью в кеше. Здесь возможно неправильно выбрать соотношения времени жизни записи/ключа и TTL.

В-пятых, к ошибкам может приводить наличие старых ключей в зонах.

А ещё к ошибкам может приводить процедура генерации ключей в различном специализированном ПО. Так, например, в зоне .ru 16 августа 2019 года резолверы не могли найти подписи RR-сетов [6]. Или можно вспомнить другой сбой в зоне .ru 30 января 2024 года, о причине которого Координационный центр национального домена сети Интернет написал – «главной причиной сбоя стало несовершенство программного обеспечения, используемого при создании ключей шифрования» [7].

А сами по себе поломки DNSSEC могут привести к недоступности серверов времени, как это случилось с NTP-серверами NIST 12 сентября 2016 года, когда произошёл сбой DNSSEC на nist.gov. Надо отметить, что это был не первый сбой DNSSEC на nist.gov и даже не первый сбой DNSSEC на nist.gov за период в 30 дней. Это был полный сбой DNSSEC, затронувший все имена на nist.gov, включая веб-сайты, службу NTP (time.nist.gov) и все другие интернет-сервисы nist.gov, требующие функционирующей службы DNS [9].

Но на этом тема DNS/time не исчерпана. Есть ещё DNS over TLS и DNS over HTTPS. TLS-сертификаты, как известно, тоже «живут» не вечно. Часто встречаются рекомендации включить на своих сетях/компьютерах NTP, чтобы время не мешало DNS-резолвингу [11]. Но, как мы видим из приведённого выше примера с NIST, проблемы с DNSSEC могут породить «замкнутый круг».

В общем, если говорить коротко, то DNSSEC решил одну про-

блему, а породил массу других. В том числе и организационных. Гидра, одним словом.

И самое главное – если нужно будет подменить национальную зону, то PTI [12] всегда это сможет сделать, т.к. контролирует корень доверия. Но там, во-первых, как я надеюсь, работают честные люди, а во-вторых, со стороны независимого мониторинга это можно обнаружить вовремя и принять меры.

Источники:

[1] Proceedings of the 2025 ACM Internet Measurement Conference, https://dl.acm.org/doi/proceedings/10.1145/3730567?tocHeading=-heading4

[2] https://www.iana.org/domains/root/db

[3] https://statdom.ru/tld/ru/report/domainsdnsseccount/#31

[4] https://stats.dnssec-tools.org/#/?top=tlds&tld_tab=0

[5] Proceedings of the 2025 ACM Internet Measurement Conference, https://dl.acm.org/doi/proceedings/10.1145/3730567?tocHeading=-heading4

[6] https://ianix.com/pub/dnssec-outages.html

[7] https://ianix.com/pub/dnssec-outages/20190816-ru/

[8] https://cctld.ru/media/news/kc/35566/

[9] https://ianix.com/pub/dnssec-outages/20160912-nist.gov/

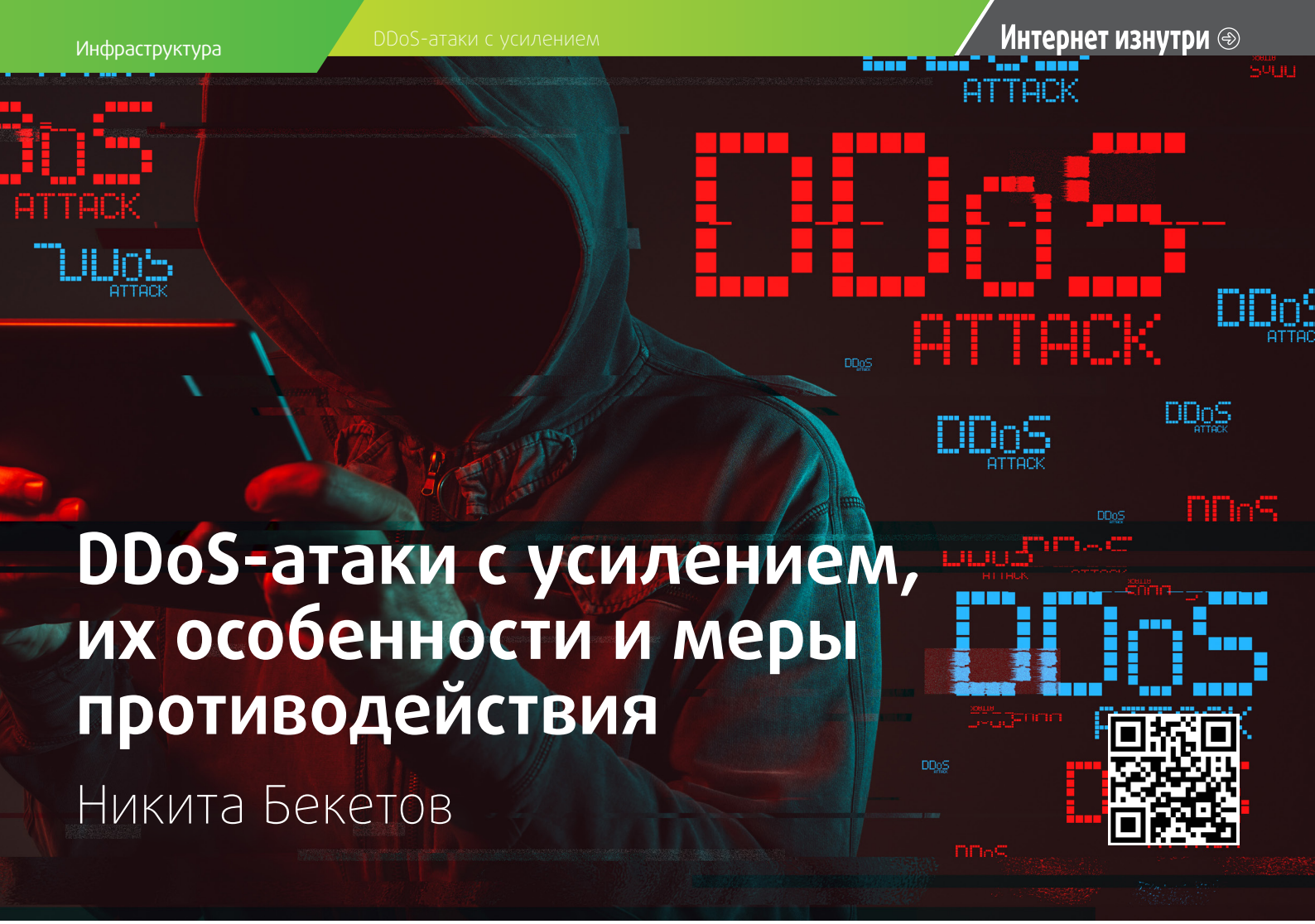
[10] https://ianix.com/pub/dnssec-outages/20141203-fbi.gov/

[11] https://cyounkins.medium.com/encrypted-dns-ntp-deadlock-9e378940b79f

[12] https://pti.icann.org/

Об авторе:

Храмцов Павел Брониславович, к.т.н., доцент, руководитель проектов DNS АО «ЦВКС МСК-IX», научный руководитель учебных проектов Фонда развития сетевых технологий «ИнДата», лауреат награды Virtuti Interneti 2025



DDoS-атаки с усилением, их особенности и меры противодействия

Никита Бекетов

Аннотация
DoS- и DDoS-атаки остаются одними из самых опасных угроз в цифровом мире. В статье дано комплексное представление о механизме DDoS-атак с усилением, их опасность иллюстрируется на конкретных примерах и статистике. Особое внимание уделяется техническим деталям (протоколы, коэффициенты усиления, шаги атаки) и актуальным уязвимостям (например, SLP). Завершается материал кратким обзором базовых мер защиты, в котором подчеркивается необходимость комплексного подхода к кибербезопасности.

Ключевые слова:
DoS, DDoS, усиление DoS-атак, тренды DoS-атак

В последнее время мир изменился, причём не всегда в лучшую сторону, и про DoS-атаки узнали даже люди, далёкие от темы ИБ. Многие ощутили на себе последствия подобных атак, среди которых:

- медленная работа Интернета (в случае атаки на провайдеров);
- недоступность или медленная работа различных веб-сервисов (сайтов);
- неработающие мобильные приложения.

Что же такое DoS-атаки? Это атаки типа «отказ в обслуживании» — denial of service, DoS. Если DoS-атака проводится одновременно со множества устройств, её называют распределённой, то есть DDoS-атакой (distributed denial of service).

Главное отличие DDoS от DoS заключается в количестве источников атаки: DoS использует один компьютер для перегрузки цели, тогда как DDoS задействует тысячи заражённых устройств (ботнет), что делает атаку масштабнее, мощнее и сложнее для защиты. Основная задача злоумышленника — перегрузить сеть, веб-сервер или онлайн-сервис потоком запросов, чтобы вывести его из строя или сделать недоступным для пользователей.

Мы рассмотрим особый вид DDoS-атак — отражённые атаки с усилением (амплификацией). Такие атаки используют архитектурные недостатки протоколов, ошибки конфигурации и уязвимости. К их техническим особенностям относятся:

- **IP-спуфинг (IP spoofing)**. Обязательный элемент, без него атака невозможна. Атакующий подделывает IP-адрес источника в пакетах запроса, чтобы ответы шли на адрес жертвы.

- **Использование уязвимых публичных сервисов**. Атакующий сканирует Интернет на наличие неправильно настроенных или уязвимых сервисов (DNS-серверов, NTP-серверов, сервисов Memcached, SSDP и т.п.), которые можно использовать как «усилители». Часто это легитимные серверы организаций. Усиление происходит за счёт того, что маленький запрос на промежуточный уязвимый сервер провоцирует большой ответ, который в результате подмены IP-адреса направляется на адрес жертвы.

- **Отражение (reflection)**. Трафик направляется не напрямую от атакующего или ботнета к жертве, а отражается от сторонних публичных серверов — это маскирует истинный источник атаки и усложняет фильтрацию.

Наиболее эффективны такие атаки при использовании протоколов с UDP-транспортом, из-за отсутствия необходимости создания соединения (connection less). Однако TCP тоже подвержен подобным атакам. Например, атака с помощью пакетов SYN-ACK может быть отражена и усилена во flooding-атаке (подробнее об этом — на сайте Akamai: https://www.akamai.com/blog/security/anatomy-of-a-syn-ack-attack).

Принцип работы DDoS-атак с усилением можно объяснить на примере атаки на DNS-протокол — этот протокол чаще других используется в подобных атаках. Злоумышленник посылает множество DNS-запросов с поддельным обратным IP-адресом жертвы в заголовках. В этом случае ответ на запрос отправляется на IP-адрес жертвы. Поскольку DNS-ответ может быть намного больше запроса, итоговый объём данных, который приходит на сервер жертвы, становится большим и может привести к недоступности. Злоумышленник, имея меньшие ресурсы, может атаковать жертву, обладающую большими ресурсами. Также злоумышленник может использовать заражённые компьютеры (ботнеты), чтобы многократно увеличить мощность атаки.

Для DDoS-атак с усилением также могут использоваться следующие протоколы: TCP, UDP, ICMP, DNS, SSDP/UPnP, NTP, RIPv1, rpcbind, SNMP, SQL RS, L2TP, Memcached.

Главной количественной характеристикой атак с амплификацией является коэффициент усиления (amplification factor). Это значение рассчитывается как отношение размера ответа к размеру запроса. Ниже приведена таблица усиления, которое можно получить при эксплуатации уязвимостей в различных протоколах.

Протокол	Усиление, раз	Уязвимая команда
NTP	994	Monlist request
DNS	28–92	DNS server request
SNMP	29	GetBulk request
CharGEN	350	Character generation request
BitTorrent	4	File search
RIPv1	131	Malformed request
SSDP	31	SEARCH request
NetBIOS	4	Name resolution
Quake Network Protocol	64	Server info exchange
Stream Protocol	5,5	Server info exchange
memcached	51200	GET reqeust with large data
WS-discovery	95	IoT multicast discovery
CLDAP	50–70	
RPD	89	
SLP	2200	Create service

Наиболее мощного коэффициента усиления в более чем 50 тысяч раз удалось добиться с помощью уязвимого сервиса Memcached. Самый часто используемый протокол — DNS, так как это обязательный протокол в Интернете и чаще всего он открыт на файрволах для корректной работы. Атака возможна из-за неправильной настройки DNS-сервера.

Рассмотрим пример реализации атаки с усилением: уязвимость в протоколе SLP (Service Location Protocol) позволила осуществлять DoS-атаку с коэффициентом усиления в 2200 раз. Уязвимости был присвоен идентификатор CVE-2023-29552 (CVSS: 8,6). Она затрагивала на тот момент больше двух тысяч

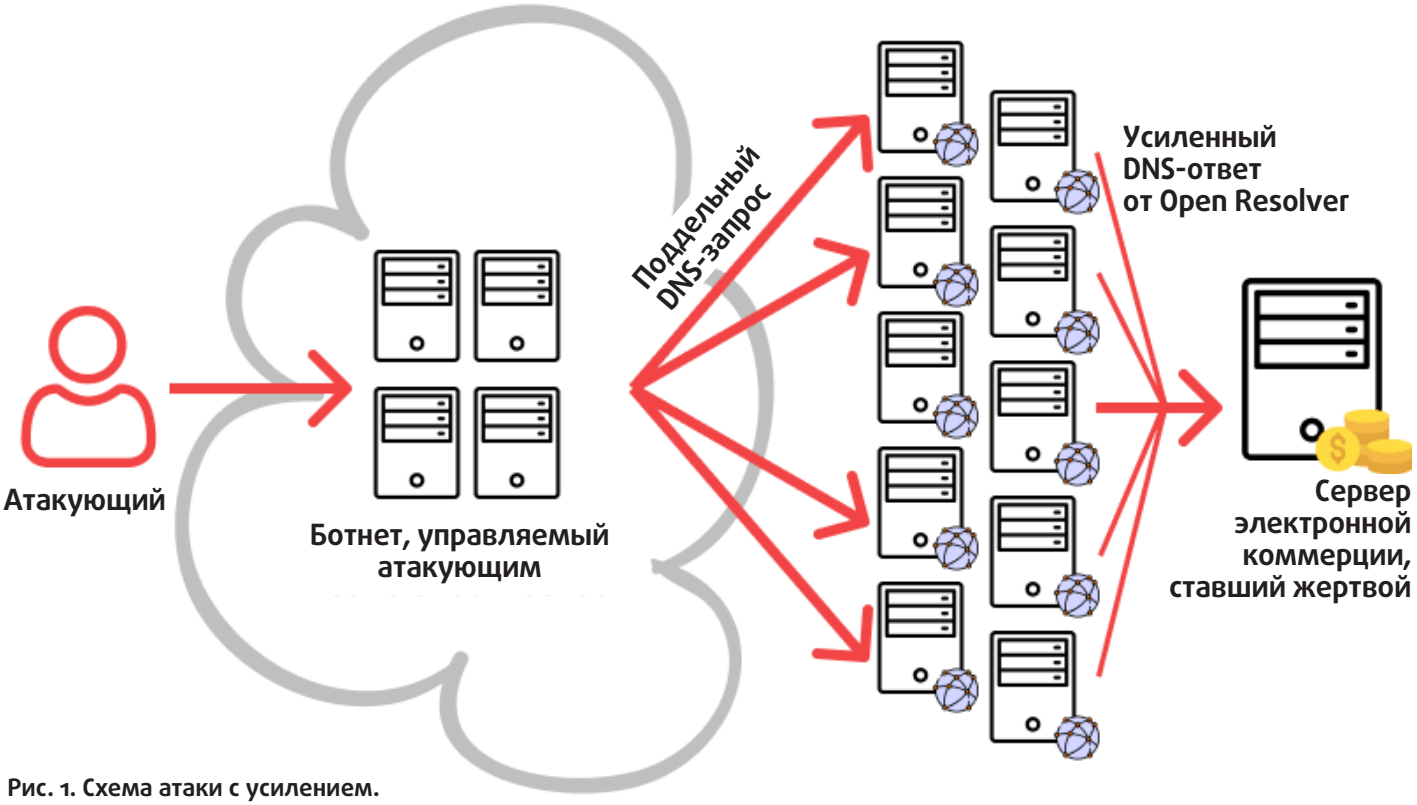
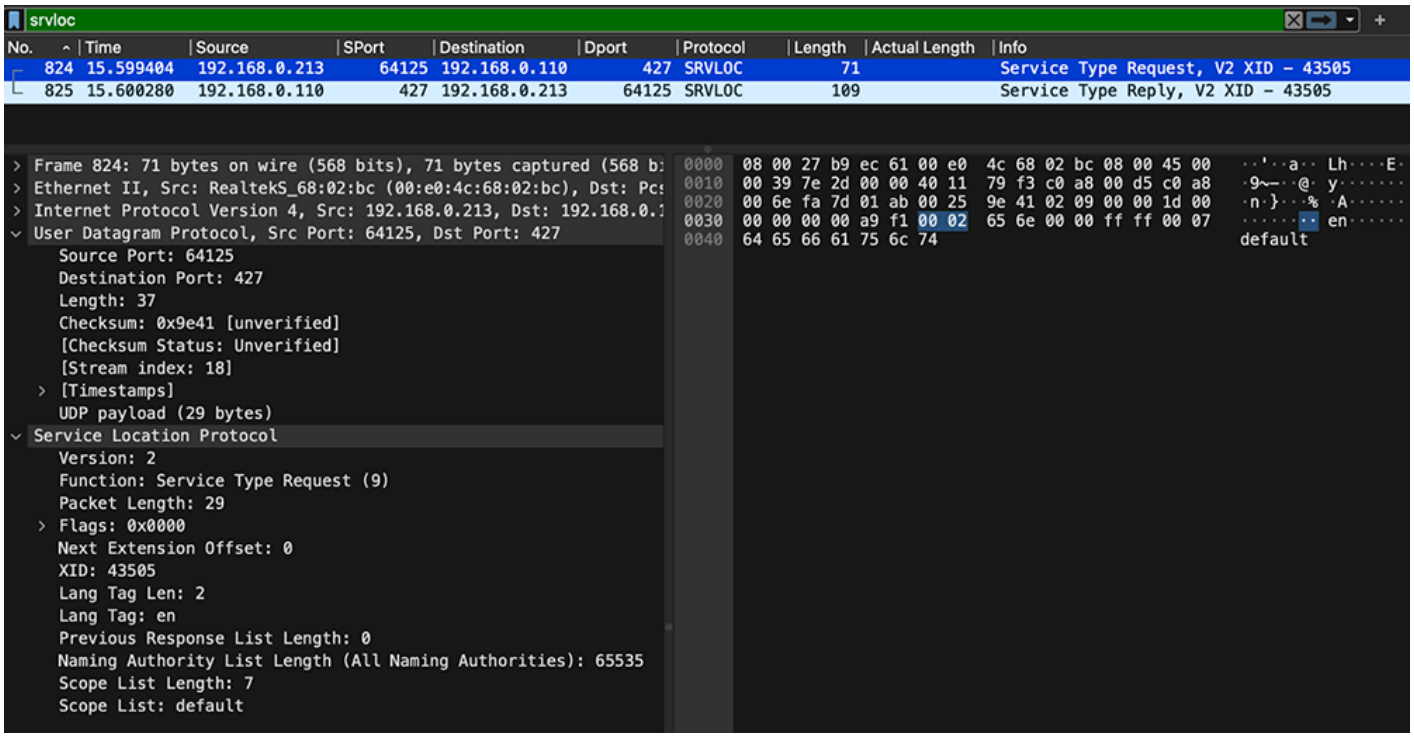


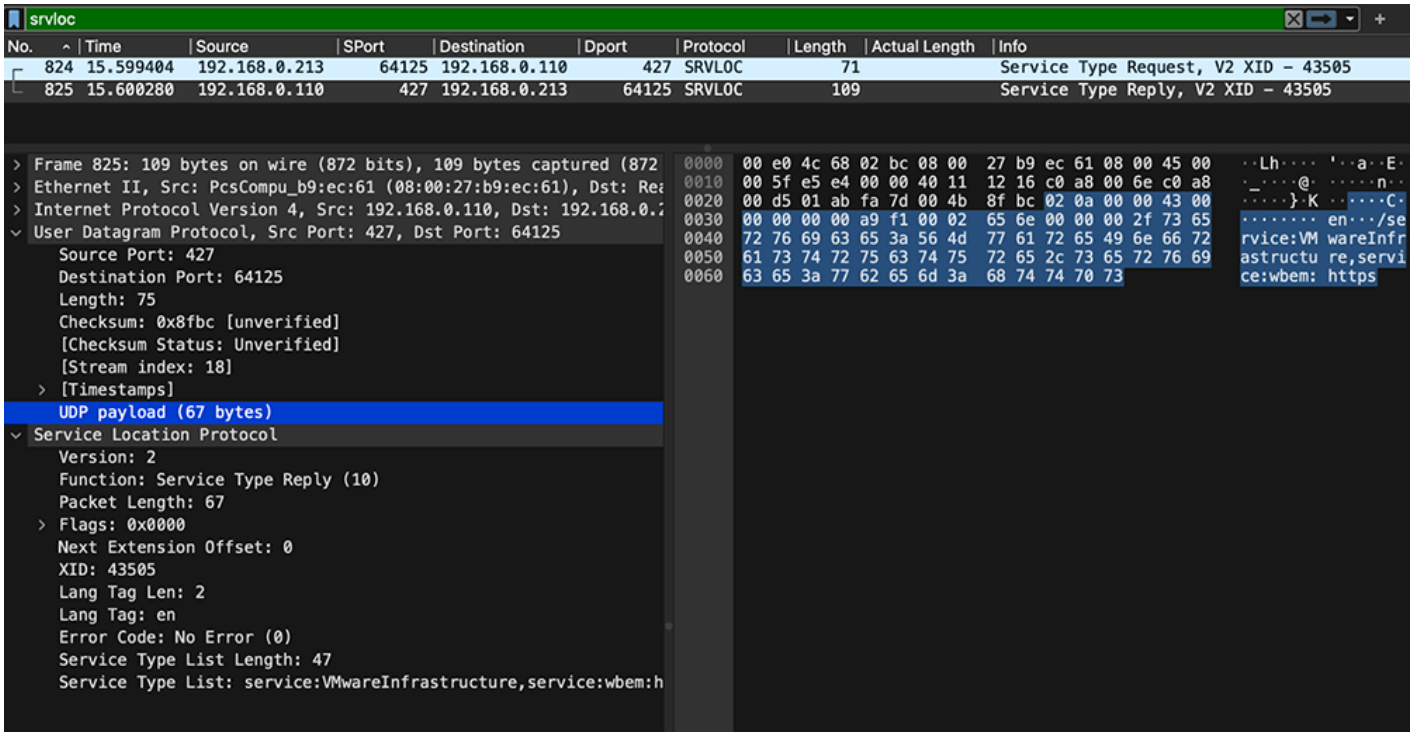
Рис. 1. Схема атаки с усилением.

международных организаций и больше 54 тысяч экземпляров SLP, доступных через Интернет. Туда входили гипервизоры VMware ESXi, принтеры Konica Minolta, маршрутизаторы Planex, интегрированный модуль управления IBM (IMM), SMC IPMI и 665 других типов продуктов.

Запрос от клиента выглядел следующим образом.



Ответ от сервера — следующим.



Для осуществления атаки злоумышленники проводили следующие шаги:

1. Атакующий находит SLP-серверы с открытым UDP-портом 427.
2. Атакующий регистрирует службы до тех пор, пока SLP не отклонит дополнительные запросы.
3. Атакующий подделывает запрос к службе, используя IP-адрес жертвы в качестве исходящего.
4. Атакующий повторяет шаг 3, пока не закончится атака.

srvloc

No.	Time	Source	SPort	Destination	Dport	Protocol	Length	Actual Length	Info
824	15.599404	192.168.0.213	64125	192.168.0.110	427	SRVLOC	71		Service Type Request, V2 XID = 43505
825	15.600280	192.168.0.110	427	192.168.0.213	64125	SRVLOC	109		Service Type Reply, V2 XID = 43505
22…	244.132224	192.168.0.213	49199	192.168.0.110	427	SRVLOC	1406		Service Registration, V2 XID = 28975
22…	244.134296	192.168.0.110	427	192.168.0.213	49199	SRVLOC	60		Service Acknowledge, V2 XID = 28975
22…	244.134444	192.168.0.213	49199	192.168.0.110	427	SRVLOC	71		Service Type Request, V2 XID = 17586
22…	244.135447	192.168.0.110	427	192.168.0.213	49199	SRVLOC	1409		Service Type Reply, V2 XID = 17586
22…	246.137331	192.168.0.213	59659	192.168.0.110	427	SRVLOC	1406		Service Registration, V2 XID = 64950
22…	246.139250	192.168.0.110	427	192.168.0.213	59659	SRVLOC	60		Service Acknowledge, V2 XID = 64950
22…	246.139471	192.168.0.213	59659	192.168.0.110	427	SRVLOC	71		Service Type Request, V2 XID = 25002
22…	246.140607	192.168.0.110	427	192.168.0.213	59659	SRVLOC	1229	2675	Service Type Reply, V2 XID = 25002
22…	248.142085	192.168.0.213	49304	192.168.0.110	427	SRVLOC	1406		Service Registration, V2 XID = 64820
22…	248.143566	192.168.0.110	427	192.168.0.213	49304	SRVLOC	60		Service Acknowledge, V2 XID = 64820
22…	248.143782	192.168.0.213	49304	192.168.0.110	427	SRVLOC	71		Service Type Request, V2 XID = 32323
22…	248.144772	192.168.0.110	427	192.168.0.213	49304	SRVLOC	1049	3975	Service Type Reply, V2 XID = 32323
22…	250.147089	192.168.0.213	64499	192.168.0.110	427	SRVLOC	1406		Service Registration, V2 XID = 63572
22…	250.148705	192.168.0.110	427	192.168.0.213	64499	SRVLOC	60		Service Acknowledge, V2 XID = 63572
22…	250.149023	192.168.0.213	64499	192.168.0.110	427	SRVLOC	71		Service Type Request, V2 XID = 6074
22…	250.150363	192.168.0.110	427	192.168.0.213	64499	SRVLOC	869	5275	Service Type Reply, V2 XID = 6074
22…	252.151800	192.168.0.213	59635	192.168.0.110	427	SRVLOC	1406		Service Registration, V2 XID = 5848
22…	252.153167	192.168.0.110	427	192.168.0.213	59635	SRVLOC	60		Service Acknowledge, V2 XID = 5848
22…	252.153357	192.168.0.213	59635	192.168.0.110	427	SRVLOC	71		Service Type Request, V2 XID = 63747
22…	252.154288	192.168.0.110	427	192.168.0.213	59635	SRVLOC	689	6575	Service Type Reply, V2 XID = 63747
22…	254.156233	192.168.0.213	50955	192.168.0.110	427	SRVLOC	1406		Service Registration, V2 XID = 10088
22…	254.158479	192.168.0.110	427	192.168.0.213	50955	SRVLOC	60		Service Acknowledge, V2 XID = 10088
22…	254.158702	192.168.0.213	50955	192.168.0.110	427	SRVLOC	71		Service Type Request, V2 XID = 51731
22…	254.159840	192.168.0.110	427	192.168.0.213	50955	SRVLOC	509	7875	Service Type Reply, V2 XID = 51731
22…	256.161456	192.168.0.213	52994	192.168.0.110	427	SRVLOC	1406		Service Registration, V2 XID = 11684
22…	256.164887	192.168.0.110	427	192.168.0.213	52994	SRVLOC	60		Service Acknowledge, V2 XID = 11684
22…	256.165195	192.168.0.213	52994	192.168.0.110	427	SRVLOC	71		Service Type Request, V2 XID = 17366
22…	256.167626	192.168.0.110	427	192.168.0.213	52994	SRVLOC	329	9175	Service Type Reply, V2 XID = 17366

«Коэффициент усиления» при этом мог доходить до 2200 раз. Для сравнения, в 2020 году в DoS-атаке на сервисы AWS с использованием протокола CLDAP усиление доходило до 55 раз. (Исследование BitSight).

По данным статистики «Гарда Технологии», за 2025 год наблюдалось следующее распределение DDoS-атак по типам.

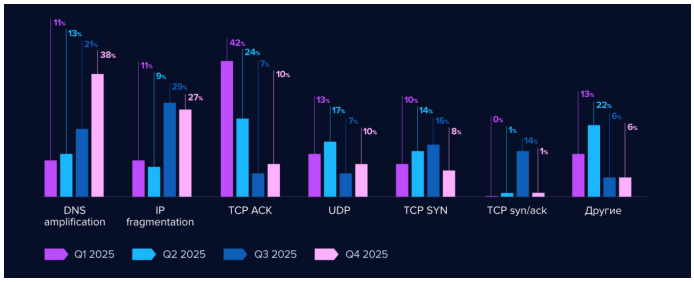


Рис. 2. Распределение DDoS-атак по типам в 2025 году.

Видно, что атаки типа DNS amplification последовательно увеличивали долю в каждом квартале — и стали основным типом DDoS-атак. Данный вид атаки позволяет с меньшими ресурсами наносить больший ущерб.

Защита

Для защиты от атак с усилением используются различные механизмы. Из них можно выделить следующие:

1. **Валидация IP-источника (антиспуфинг)**. Такая защита может быть выполнена на стороне интернет-провайдера, где расположены серверы атакующего. Всем интернет-провайдерам рекомендуется проверять факт подмены IP-адреса источника и удалять такие пакеты.
2. **Отключение или фильтрация трафика уязвимых сервисов на стороне провайдера**. Настройка ACL (access control list) на файрволах для доступа к ресурсам только с известных IP-адресов, автономных систем (ASN) или ограничения на основании GeoIP.
3. **Использование rate limit на стороне провайдера атакуемого сервиса**. Метод ограничения количества пакетов, которые можно отправить с одного узла на сервис в течение определённого времени. Ограничения также могут быть установлены относительно конкретного пользователя — по географическому признаку, по интервалу времени.
4. **Использование специализированных сервисов по защите от DoS- и DDoS-атак**. Наиболее эффективный метод — использование коммерческих сервисов защиты от DDoS-атак. Такие сервисы применяют комплексный подход: защита строится с помощью специальных аппаратных, программных средств, а также с помощью методов машинного обучения (ML).

Источники:

https://www.akamai.com/blog/security/anatomy-of-a-syn-ack-attack

https://www.bitsight.com/blog/new-high-severity-vulnerability-cve-2023-29552-discovered-service-location-protocol-slp

https://garda.ai/blog/analytics/analitika-ddos-atak-za-q4-i-ves-2025-god

https://qrator.net/library/learning-center/Ddos/What-Are-Amplification-DDoS-Attacks/

http://microsoft.com/en-us/security/blog/2022/05/23/anatomy-of-ddos-amplification-attacks/

https://www.f5.com/labs/articles/old-protocols-new-exploits-ldap-unwittingly-serves-ddos-amplification-attacks-22609

https://doznpp.medium.com/dns-amplification-attacks-explained-36ed5bd11f9a

Об авторе:

Бекетов Никита Михайлович, ведущий инженер
по информационной безопасности uFactor, компания UserGate.

Интернет-наука и образование

Ведущий рубрики: Марат Биктимиров

Уважаемые читатели!

Как мы и обещали, наш журнал продолжает публиковать студенческие работы, выполняющиеся в Фонде развития сетевых технологий «ИнДата» в рамках совместных с вузами-партнёрами мероприятий, направленных на профессиональную подготовку будущих специалистов отрасли. Напомним также, что все студенческие проекты осуществляются при поддержке ведущих сотрудников Фонда «ИнДата».

В этом номере мы представляем вашему вниманию работу, выполненную старшекурсниками МИЭМ НИУ ВШЭ Виктором Чертовым и Иваном Печерским под кураторством Василия Фунтикова и подводящую некоторый итог исследованиям возможностей эффективного применения протокола SRT для потоковой передачи видео- и аудиоинформации.

Приятно отметить, что за два года нашего сотрудничества авторы продемонстрировали вполне зрелый подход к работе и уверенный рост квалификации, что подтверждается успешными защитами учебных проектов и выступлениями на конференциях.

Применение технологии eBPF для мониторинга сетевого трафика в реальном времени

Иван Печерский
Виктор Чертов

Аннотация
В работе рассматривается подход к реализации системы мониторинга сетевых соединений протокола SRT (Secure Reliable Transport) на основе технологий Extended Berkeley Packet Filter и Express Data Path (eBPF/XDP). Предлагаемое решение обеспечивает сбор статистики SRT в реальном времени в ядре Linux без нарушения работы существующих соединений, о чём свидетельствует успешно проведённый эксперимент на разработанном функциональном прототипе.

Ключевые слова:
SRT, eBPF, Linux, мониторинг, UDP, сбор статистики

Введение

Протокол Secure Reliable Transport (далее SRT) используется для потоковой передачи видео и аудио в режиме реального времени [1]. Согласно отчёту компании-разработчика протокола Haivision за 2026 год, SRT пятый год подряд остаётся ведущим протоколом доставки видеоконтента (рис. 1).

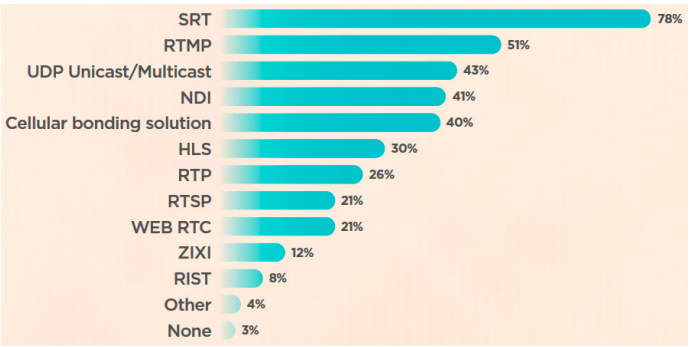


Рис. 1. Результат опроса «Какой транспортный протокол для видео вы используете в настоящий момент?» (из отчёта компании Haivision).

Источник: https://www.haivision.com/white-papers/broadcast-ip-transformation-reports/#pform

Поскольку эта технология использует в качестве транспортного механизма протокол UDP, применение SRT в рабочих средах со сложной сетевой инфраструктурой сопровождается дополнительными трудностями, связанными с отслеживанием состояний соединений между источниками на стороне поставщика видеоконтента и клиентами.

На ранних этапах развития Интернета протокол UDP [2] использовался для обмена запросами и ответами без учёта состояния, например, с помощью таких протоколов, как DNS или NTP. Перезапуск обслуживающего серверного процесса в этом контексте не являлся проблемой, поскольку ему не нужно сохранять состояние при обслуживании нескольких запросов. Однако современные протоколы, в том числе SRT, используют соединения с отслеживанием состояния. В этом контексте удаление старых соединений при перезагрузке серверного приложения напрямую влияет на доступность сервиса и качество обслуживания конечного клиента, из-за чего в некоторых компаниях применяются собственные решения, обеспечивающие плавное и неразрывное применение изменений в конфигурацию серверного процесса [3].

В представленной работе рассматривается сценарий, в котором проблема «изящной» перезагрузки (от англ. graceful reload) решена внутренней разработкой компании, но в ней отсутствуют средства мониторинга и анализа SRT-трафика, поэтому нет информации о состоянии соединений, такой как задержки, потери или повторные передачи пакетов. При та-

Рис. 2. Взаимодействие компонентов разработанного прототипа.

ком раскладе известные инструменты мониторинга сети оказываются недостаточно удобными. Ручная отладка проблем SRT-соединений с помощью сетевых анализаторов, таких как Wireshark с SRT-диссектором, и изучение разрозненных логов значительно снижают скорость реагирования на инциденты [4]. Поэтому целью проведённого исследования являлась разработка прототипа решения для мониторинга SRT-соединений в режиме реального времени.

Extended Berkeley Packet Filter

Для решения проблем, возникающих при использовании UDP-сервисов, создаются очень интересные решения. Например, компания Cloudflare разработала механизм udpgrm для плавного перезапуска сервисов (преимущественно ориентированных на работу с протоколом QUIC, также использующим UDP), который использует специальные параметры сокетов и eBPF-программу, сохраняющую привязку пакетов к конкретному рабочему процессу, чтобы при обновлении конфигурации сервера продолжать обслуживать существующие потоки без потерь [5]. Это позволяет решить задачу сохранения состояния соединений при перезапусках, однако вопрос мониторинга качества соединений остаётся открытым. Тем не менее, udpgrm демонстрирует высокий потенциал технологии eBPF в обработке UDP-трафика.

eBPF – это технология безопасной загрузки и выполнения кода внутри ядра Linux [6]. В контексте проведённого исследования eBPF привлекателен тем, что позволяет отфильтровывать и анализировать SRT-пакеты непосредственно при прохождении через сетевой стек, без необходимости нести затраты на переключение между ядром и пользовательским пространством для обработки каждого пакета, обеспечивая тем самым высокую производительность в обработке данных, а возможность динамической загрузки программ eBPF в ядро даёт существенное преимущество по сравнению с обновлением кодовой базы ядра и последующей перезагрузкой сервера. Наличие встроенного верификатора значительно снижает риск сбоя в работе ядра, который может вызвать загружаемая программа [7].

Подсистема XDP – это высокопроизводительный пакетный процессор, интегрированный в ядро Linux, который выполняет программы BPF, когда драйвер сетевой карты получает пакет [8]. XDP-программы выполняются на самом раннем этапе приёма пакетов (на уровне драйвера сетевой карты), позволяя обрабатывать миллионы пакетов в секунду с минимальными задержками [9].

По этой причине сочетание eBPF/XDP было выбрано как основа для непрерывного мониторинга SRT-трафика в режиме реального времени. Такой подход сочетает в себе отсутствие необходимости вмешательства в код приложений и работу сервера с высокой производительностью и безопасностью исполнения программ в ядре.

Архитектура решения

Разработанный прототип системы мониторинга SRT-соединений функционирует как в пространстве ядра, так и в пространстве пользователя (рис. 2).

Компоненты пространства ядра взаимодействуют с компонентами пространства пользователя через BPF-карты – разделяемые структуры данных, представляющие собой хранилища ключей и их значений, размещённые в ядре и

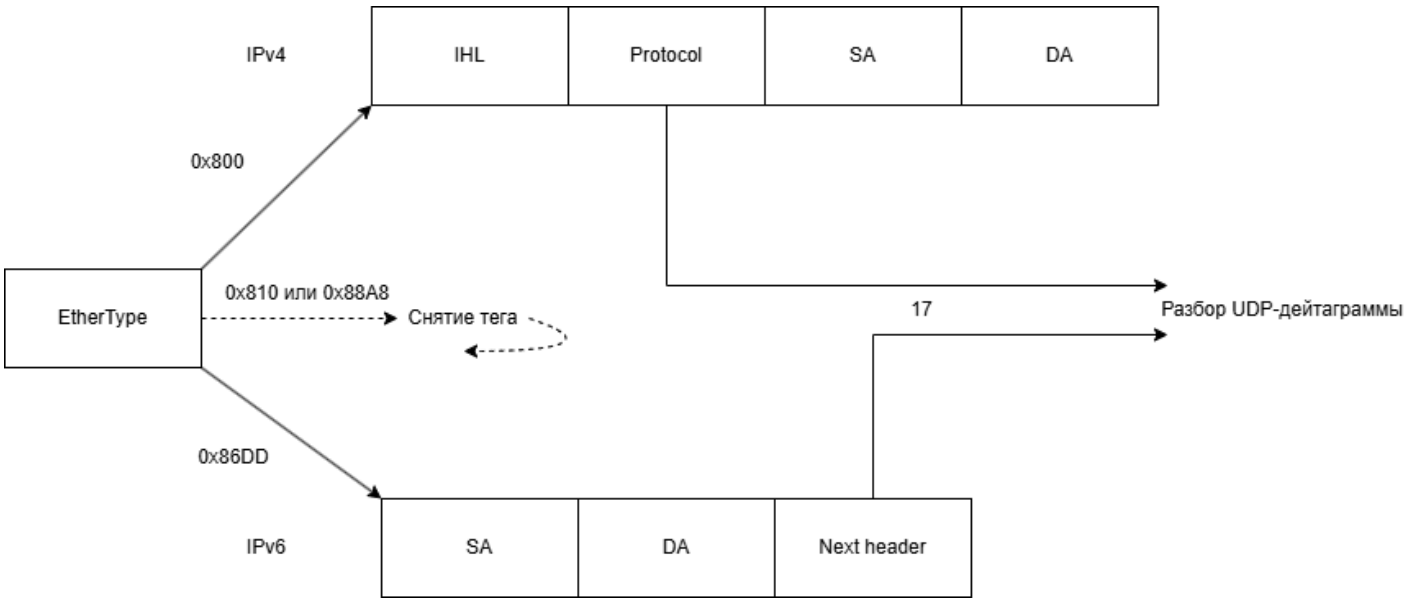


Рис. 3. Порядок разбора полученного фрейма данных.

доступные обеим сторонам. В разработанной системе используется четыре вида таких карт [10–12].

В пространстве ядра функционирует сама eBPF-программа. После загрузки в ядро она прикрепляется к двум сетевым точкам перехвата, описанным далее.

В пространстве пользователя функционирует привилегированный управляющий процесс – демон, который загружает eBPF-программу в ядро и периодически опрашивает BPF-карты для получения информации о сессиях. Более подробно роль демона будет описана далее.

Также в пространстве пользователя работают утилита командной строки, позволяющая пользователю запрашивать у демона текущую статистику и отображать её в удобном виде, а также управлять самим демоном, и HTTP-сервер, публикующий измеряемые характеристики наблюдаемых сессий в формате, совместимом с системой мониторинга Prometheus.

Перехват и идентификация SRT-пакетов

Перехват трафика осуществляется на двух точках присоединения. Первая точка обеспечивает перехват входящего трафика с использованием механизма XDP. Программа прикрепляется к сетевому интерфейсу и вызывается для каждого входящего пакета ещё до его передачи в сетевой стек. По завершении анализа пакет в любом случае передаётся вверх далее по сетевому стеку, система не отбрасывает и не модифицирует наблюдаемый трафик.

Вторая точка обеспечивает перехват исходящего трафика посредством подсистемы управления трафиком (TC). Мониторинг исходящего трафика является необязательным: он активируется соответствующим параметром в конфигурации или аргументом командной строки при запуске демона. На обеих точках перехвата вызывается одна и та же процедура разбора пакета, различается лишь направление передачи.

Сначала программа обрабатывает Ethernet-заголовок и определяет тип вышестоящего протокола, используя поле EtherType (рис. 3). Если кадр содержит метку виртуальной локальной сети (VLAN-тег) стандарта IEEE 802.1Q, то он снимается путём увеличения смещения разбора на четыре байта [13]. Поскольку на практике нередко применяется двойное тегирование (стандарт 802.1AD, известный также как QinQ), программа способна последовательно снять обе метки: сначала внешний тег провайдера, затем внутренний тег клиента [14].

Далее программа разбирает IPv4- или IPv6-заголовок. Для пакетов IPv4 из заголовка извлекаются адреса источника и назначения, поле протокола верхнего уровня, а также длина заголовка, необходимая для определения начала полезной нагрузки пакета. Для пакетов IPv6 также извлекаются адреса, но принадлежность к транспортному протоколу UDP устанавливается по полю «следующий заголовок» [15].

В обоих случаях пакеты, не принадлежащие протоколу UDP, не обрабатываются. Затем из UDP-заголовка считываются порты источника и назначения. Если в конфигурации задан конкретный UDP-порт для SRT, то он сохраняется в соответствующей карте, после чего программа пропускает без дальнейшей обработки все пакеты, у которых ни порт источника, ни порт назначения не совпадают с заданным значением (о конфигурации мы расскажем позже).

Наконец выполняется идентификация пакета как принадлежащего протоколу SRT. Поскольку SRT не имеет зарезервированного номера порта, идентификация производится по структуре внутреннего заголовка, минимальный размер которого составляет 16 байт. Тип пакета определяется по старшему биту первого слова заголовка: единица означает управляющий пакет, а ноль - пакет данных. Данное разграничение закреплено в спецификации протокола SRT (рис. 4 на следующей странице) [16].

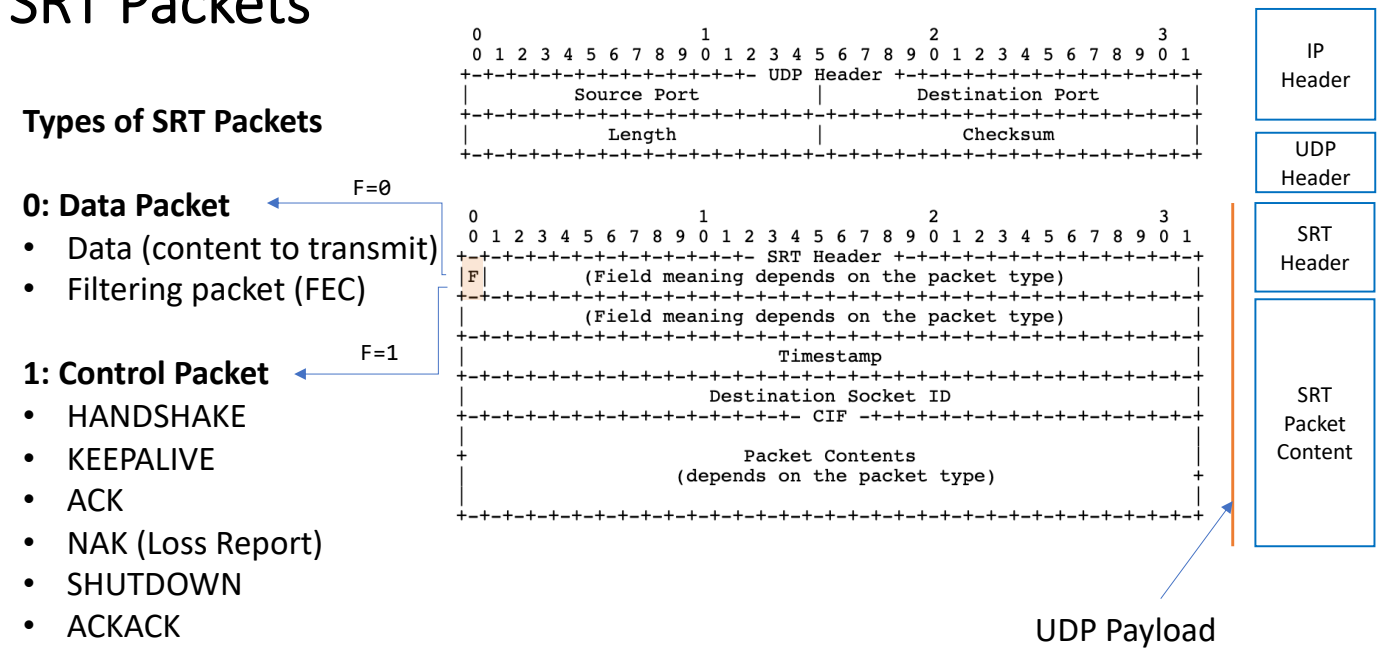


Рис. 4. Структура SRT-пакета.

Источник: https://datatracker.ietf.org/meeting/interim-2020-mops-01/materials/slides-interim-2020-mops-01-sessa-srt-protocol-overview-00.pdf

Из управляющих пакетов извлекается их контрольный тип. Система распознаёт следующие типы для наблюдения за жизненным циклом соединения: установление соединения (HANDSHAKE), поддержание активности (KEEPALIVE), подтверждение получения (ACK), уведомление о потере (NAK), завершение соединения (SHUTDOWN) и подтверждение подтверждения (ACKACK). Для пакетов данных анализируются два признака: биты поля шифрования (KK), указывающие на применение шифрования к данному пакету, а также бит повторной передачи пакета (R).

Для объединения встречных направлений потока пакетов, идущих от узла А к узлу Б, и пакетов, идущих от Б к А, в единую запись карты сессий применяется процедура сортировки кортежа из четырёх компонентов, образованного адресами и портами обеих сторон. Ключ сессии хранит два поля адресов, признак версии протокола IP и два поля портов. Упорядочивание выполняется путём лексикографического побайтового сравнения двух адресов. Адрес, лексикографически меньший, всегда помещается в первое поле ключа и обозначает первое направление потока, а адрес, лексикографически больший, во второе поле. При равенстве адресов, что возможно, например, при работе через интерфейс обратной петли (loopback), для окончательного упорядочивания сравниваются номера UDP-портов. Благодаря такому подходу пакеты обоих направлений одного соединения всегда порождают одинаковый ключ, и их статистика консолидируется в единой записи карты сессий.

Новая сессия создаётся только при поступлении управляющего пакета одного из перечисленных ранее управляющих типов, пакеты данных не инициируют создание новой записи. При её создании в поле начала сессии фиксируется текущее время ядра. При каждом последующем обновлении записи, независимо от типа пакета, метка времени последней активности перезаписывается текущим временем, что впоследствии позволяет обнаруживать и удалять неактивные сессии. Одновременно с созданием новой записи в карте сессий программа пытается зарезервировать место в кольцевом буфере событий и опубликовать туда структурированное событие о появлении новой сессии. Аналогичное событие о завершении сессии публикуется при обнаружении управляющего пакета типа SHUTDOWN для уже существующей сессии. Если кольцевой буфер переполнен и резервирование места невозможно, инкрементируется счётчик потерянных событий в соответствующей карте.

Для каждой активной сессии обновляются счётчики пакетов и байт, а также показатели качества соединения. Основным источником данных о состоянии канала служат управляющие пакеты типа ACK. Принимающая сторона отправляет их передающей, дополнительно сообщая внутри них свои измерения параметров соединения. Первым является двусторонняя задержка (RTT) в микросекундах – оценка, вычисленная принимающей стороной, как время между отправкой ACK-пакета и приемом ACKACK-пакета (рис. 5).

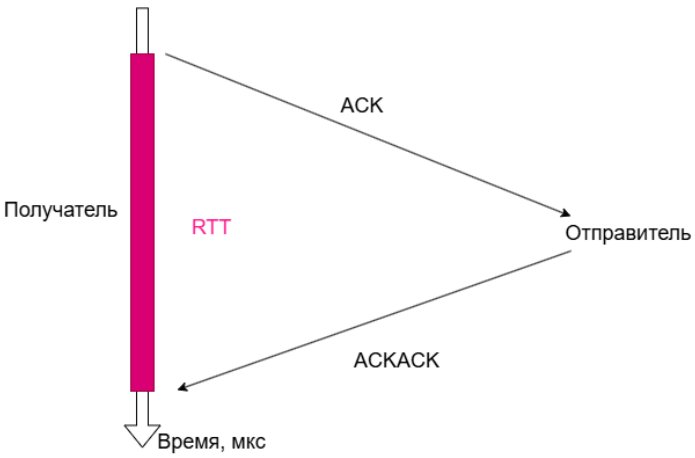


Рис. 5. Оценка RTT в протоколе SRT.

Следом идёт вариация этой задержки, или джиттер, измеряемый также в микросекундах. Далее находится значение доступного объёма буфера приёмника в пакетах. Затем идёт значение скорости приёма в пакетах в секунду. Наконец, последним из извлекаемых полей является оценочная пропускная способность канала, тоже в пакетах в секунду. Все эти значения являются последними из наблюдаемых и при каждом поступлении ACK-пакета перезаписываются.

Помимо вышеперечисленных показателей, обновляются счётчик пакетов типа HANDSHAKE, счётчики пакетов ACK и NAK, счётчик пакетов данных, счётчик управляющих пакетов, счётчик повторно переданных пакетов данных, счётчик пакетов данных с признаком шифрования, а также идентификатор SRT-сокета.

Конфигурация и демон

Конфигурация системы описывается в YAML-файле (рис. 6). При отсутствии этого файла программа запускается с предопределёнными по умолчанию значениями.

```
# cat srt-monitor-demo.yaml
interface: br-9f212711f990
egress: true
socket_path: /run/srt-monitor.sock

thresholds:
  retrans_pct: 5.0
  rtt_ms: 200
  session_timeout_sec: 120
  min_packets: 100

monitor:
  interval_ms: 1000

metrics:
  enabled: true
  addr: ":9090"

bpf:
  max_sessions: 10240
  srt_port: 0

filter:
  unhealthy_only: false

display:
  resolve_dns: false
  dns_ttl_sec: 60

log_level: info
#
```

Рис. 6. Пример содержимого конфигурации.

Конфигурация включает несколько групп параметров. Параметры привязки к сетевому интерфейсу определяют, на каком интерфейсе вести наблюдение, нужен ли мониторинг исходящего трафика и путь до Unix-сокета. Пороговые значения задают критерии оценки состояния сессий: допустимую долю повторных передач, порог RTT, порог неактивности сессии и минимальное число пакетов для активации проверок. Параметр мониторинга определяет частоту опроса BPF-карты сессий. Параметры экспорта метрик включают флаг активации и адрес HTTP-сервера. Параметры BPF задают максимальное число отслеживаемых сессий и фильтр UDP-порта. Фильтр сессий позволяет отображать только сессии, удовлетворяющие заданным условиям, подробнее о нём рассказано далее. Параметры отображения управляют обратным разрешением DNS и временем жизни кеша DNS-имён. Уровень журналирования задаётся как строка, принимающая значение уровня отладки, информации, предупреждения или ошибок.

Механизм фильтрации позволяет ограничить множество сессий, возвращаемых в ответе на запрос статистики. Фильтр описывается набором критериев, которые применяются одновременно:

1. IP-адрес любой из сторон соединения.
2. Блок IP-адресов в CIDR-нотации любой из сторон соединения.
3. Порт любой из сторон соединения.

Предусмотрены также строгие критерии: отдельно по IP-адресу источника или получателя и отдельно по порту источника или получателя. Также имеется специальный критерий, который ограничивает вывод только сессиями, у которых зафиксировано превышение хотя бы одного из настроенных пороговых значений.

При запуске демон выполняет следующую последовательность инициализации. Вначале разбираются аргументы командной строки, среди которых: имя сетевого интерфейса, признак включения мониторинга исходящего трафика, путь к файлу конфигурации и флаг вывода версии.

Следующим действием является запись идентификатора процесса в специальный файл. Если он существует и содержит идентификатор активного процесса, тогда осуществляется проверка существования такого процесса и, если она оказывается удачной, запуск прерывается, предотвращая одновременную работу двух экземпляров демона. Устаревший же файл перезаписывается. При нормальном завершении демона этот файл удаляется.

После успешной инициализации демон загружает конфигурацию из YAML-файла, при необходимости переопределяя отдельные её параметры значениями из командной строки. Затем в ядро загружается eBPF-программа и запускается фоновый мониторинг сессий. Подсистема мониторинга непрерывно читает события из кольцевого буфера. При получении события о появлении или завершении сессии регистрируется соответствующее информационное сообщение. Одновременно периодически опрашивается BPF-карта сессий с заданным интервалом. При каждой итерации опроса выполняется полное считывание текущего состояния BPF-карты сессий. Для каждой обнаруженной сессии проверяется её время последней активности, и если с момента последнего принятого пакета прошло больше времени, чем заданный порог неактивности, запись признаётся устаревшей и удаляется. Для каждой активной сессии выполняется проверка «здоровья» путём сравнения текущих показателей с пороговыми. Про-

верка активируется только после накопления в данном направлении пакетов более установленного минимума, чтобы предотвратить ложные срабатывания на начальном этапе соединения, когда имеющихся данных ещё недостаточно для достоверного вывода.

Дополнительно при каждом опросе сравнивается текущее значение счётчика рукопожатий с сохранённым значением из предыдущего опроса. Если счётчик вырос и предыдущее значение было ненулевым, значит в рамках уже существующей сессии произошло повторное рукопожатие, что свидетельствует о переподключении клиента. Это событие тоже регистрируется в журнале.

При включённом экспорте метрик запускается HTTP-сервер, публикующий характеристики наблюдаемых сессий в формате, совместимом с Prometheus. При каждом HTTP-запросе от системы мониторинга модуль запрашивает актуальный снимок сессий из BPF-карты и карты потерянных событий и формирует набор метрик, которые отправляются в качестве ответа.

Затем запускается сервер межпроцессного взаимодействия. Он принимает подключения через доменный сокет UNIX [17]. Одновременное число активных соединений ограничено шестнадцатью - и при исчерпании лимита новые соединения отклоняются без обработки. При создании сокета производится определение идентификатора группы. Если группа уже существует в системе, сокет передаётся во владение этой группе с правами доступа, разрешающими чтение и запись владельцу и членам группы. При отсутствии группы права сужаются до доступа исключительно для привилегированного пользователя. Авторизация подключения выполняется через специальный параметр сокета. При получении нового соединения через системный вызов запрашиваются реальные идентификаторы пользователя и группы подключающегося процесса. Соединение авторизуется, если идентификатор пользователя равен нулю или идентификатор группы совпадает с идентификатором группы приложения.

Демон поддерживает пять команд взаимодействия с ним:

1. запрос текущей статистики - возвращает массив описаний активных сессий с применением фильтрации, либо разовой из запроса, либо постоянной из конфигурации;

2. запрос на установку фильтра - сохраняет параметры отбора сессий для применения ко всем последующим запросам статистики;

3. запрос на смену уровня журналирования - позволяет переключить детализацию журнала демона;

4. запрос конфигурации - возвращает полную текущую конфигурацию демона в формате JSON;

5. запрос на перезагрузку конфигурации - инициирует повторное считывание YAML-файла и применение новых параметров.

Завершающим этапом инициализации является регистрация обработчиков сигналов операционной системы. Сигнал SIGHUP обрабатывается как команда перезагрузки конфигурации, при получении которой повторно считывается YAML-файл. Сигналы SIGTERM и SIGINT инициируют завершение работы.

Интерфейс командной строки и отображение данных

Утилита командной строки подключается к доменному сокету демона и поддерживает два режима работы. В режиме разового опроса клиент выполняет единственный запрос и завершает работу. По умолчанию результат выводится в виде форматированной таблицы, но при указании соответствующего флага данные выводятся в виде массива JSON-объектов для обработки внешними инструментами через конвейер оболочки.

В режиме наблюдения клиент периодически повторяет запрос с заданным интервалом, предварительно очищая экран перед каждым обновлением. При включённом обратном разрешении DNS выполняется разрешение всех IP-адресов текущего снимка и рядом с IP-адресом в скобках выводится доменное имя, если оно доступно в кеше (рис. 7).

Ширина терминала определяется через системный вызов запроса размера его окна, чтобы адаптировать набор отображаемых столбцов к доступной ширине. Проблемные сессии выделяются в таблице красным цветом. Отображение объёмов трафика поддерживает как автоматический режим выбора единиц измерения в зависимости от порядка величины числа, так и заданный через соответствующий флаг: байты, килобайты, мегабайты или гигабайты.

Заключение

В ходе эксперимента успешно опробован метод мониторинга SRT-соединений на базе технологии eBPF. Результаты представленной работы имеют прикладное значение для компаний, использующих SRT-протокол в своей инфраструктуре. Предложенный подход может быть внедрён как самостоятельный сервис мониторинга или интегрирован в существующие системы наблюдения за сетью.

```
# srt-cli -resolve
SESSION: fd00::1 (host-gateway-v6.local):7001 <-> fd00::2 (sender-ipv6.local):49475  [Last Seen: 0s ago, Duration: 2m15s]
  FLOW            HOST                  SOCK_ID    RX_P  RX_VOL    TX_P  TX_VOL    DATA(R)  %RET   ENC  CTRL  ACK  NAK  RTT      JITTER   BW         BUF     RATE(R)
  fd00::1->fd00::2  host-gateway-v6.local  0x2d03035  0     0 B       136   10.99 KB  0(0)     0.00%  No   136   0    0    0.00 ms  0.00 ms  0 pkts/s   0 pkts  0 pkts/s
  fd00::2->fd00::1  sender-ipv6.local      0x948c477  136   10.99 KB  0     0 B       0(0)     0.00%  No   136   0    0    0.00 ms  0.00 ms  0 pkts/s   0 pkts  0 pkts/s

-------------------------------------------------------------------------------
SESSION: 10.99.0.1 (host-gateway.local):7000 <-> 10.99.0.2 (sender-ipv4.local):46396  [Last Seen: 0s ago, Duration: 2m15s]
  FLOW                HOST                SOCK_ID     RX_P  RX_VOL   TX_P  TX_VOL   DATA(R)  %RET   ENC  CTRL  ACK  NAK  RTT      JITTER   BW         BUF     RATE(R)
  10.99.0.1->10.99.0.2  host-gateway.local  0x17a67967  0     0 B      136   8.34 KB  0(0)     0.00%  No   136   0    0    0.00 ms  0.00 ms  0 pkts/s   0 pkts  0 pkts/s
  10.99.0.2->10.99.0.1  sender-ipv4.local   0x111b55a5  136   8.34 KB  0     0 B      0(0)     0.00%  No   136   0    0    0.00 ms  0.00 ms  0 pkts/s   0 pkts  0 pkts/s
```

Рис. 7. Пример отображаемых данных об имеющихся SRT-сессиях.

Список литературы:

[1] Haivision/srt: Secure, Reliable, Transport [Электронный ресурс]. URL: https://github.com/haivision/srt (дата обращения: 19.03.2026).

[2] RFC 768 - User Datagram Protocol [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc768 (дата обращения: 19.03.2026).

[3] Everything you ever wanted to know about UDP sockets but were afraid to ask, part 1 [Электронный ресурс]. URL: https://blog.cloudflare.com/everything-you-ever-wanted-to-know-about-udp-sockets-but-were-afraid-to-ask-part-1/ (дата обращения: 19.03.2026).

[4] Wireshark. Go Deep | Display Filter Reference: SRT Protocol [Электронный ресурс]. URL: https://www.wireshark.org/docs/dfref/s/srt.html (дата обращения: 19.03.2026).

[5] QUIC restarts, slow problems: udpgrm to the rescue [Электронный ресурс]. URL: https://blog.cloudflare.com/quic-restarts-slow-problems-udpgrm-to-the-rescue/ (дата обращения: 19.03.2026).

[6] Райс. Л. Изучаем eBPF: Пер. с англ. – Астана: Алист, 2024. – 224с. ISBN 978-601-08-4118-5

[7] The eBPF Runtime in the Linux Kernel [Электронный ресурс]. URL: https://arxiv.org/abs/2410.00026 (дата обращения: 19.03.2026).

[8] Calavera David, Fontana Lorenzo, Frazelle Jessie. Linux observability with BPF : advanced programming for performance analysis and networking. O'Reilly Media, Inc., 2020. P. 162.

[9] Hoiland-Jorgensen T. et al. The eXpress data path: Fast programmable packet processing in the operating system kernel // CoNEXT 2018 - Proceedings of the 14th International Conference on Emerging Networking EXperiments and Technologies. Association for Computing Machinery, Inc, 2018. Vol. 18. P. 54–66.

[10] BPF_MAP_TYPE_ARRAY and BPF_MAP_TYPE_PERCPU_ARRAY — The Linux Kernel documentation [Электронный ресурс]. URL: https://docs.kernel.org/bpf/map_array.html (дата обращения: 19.03.2026).

[11] BPF_MAP_TYPE_HASH, with PERCPU and LRU Variants — The Linux Kernel documentation [Электронный ресурс]. URL: https://docs.kernel.org/bpf/map_hash.html (дата обращения: 19.03.2026).

[12] BPF ring buffer — The Linux Kernel documentation [Электронный ресурс]. URL: https://docs.kernel.org/6.2/bpf/ringbuf.html (дата обращения: 19.03.2026).

[13] Таненбаум Эндрю, Фимстер Ник, Уэзеролл Дэвид. Компьютерные сети. 6-е изд. — СПб.: Питер, 2023. 397–403 с. ISBN 978-5-4461-1766-6

[14] Олифер Виктор, Олифер Наталья. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание, доп. и испр. — СПб.: Питер, 2024. 378–396 с. ISBN 978-5-4461-4085-5

[15] Робачевский А. Интернет изнутри: Архитектура экосистемы Интернета / Андрей Робачевский. — 3-е изд., перераб. и дополн. — М.: Серпантин Эджженси, 2024. 17–41 с. ISBN 978-5-6052033-0-8

[16] draft-sharabayko-srt-00 [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/draft-sharabayko-srt-00 (дата обращения: 19.03.2026).

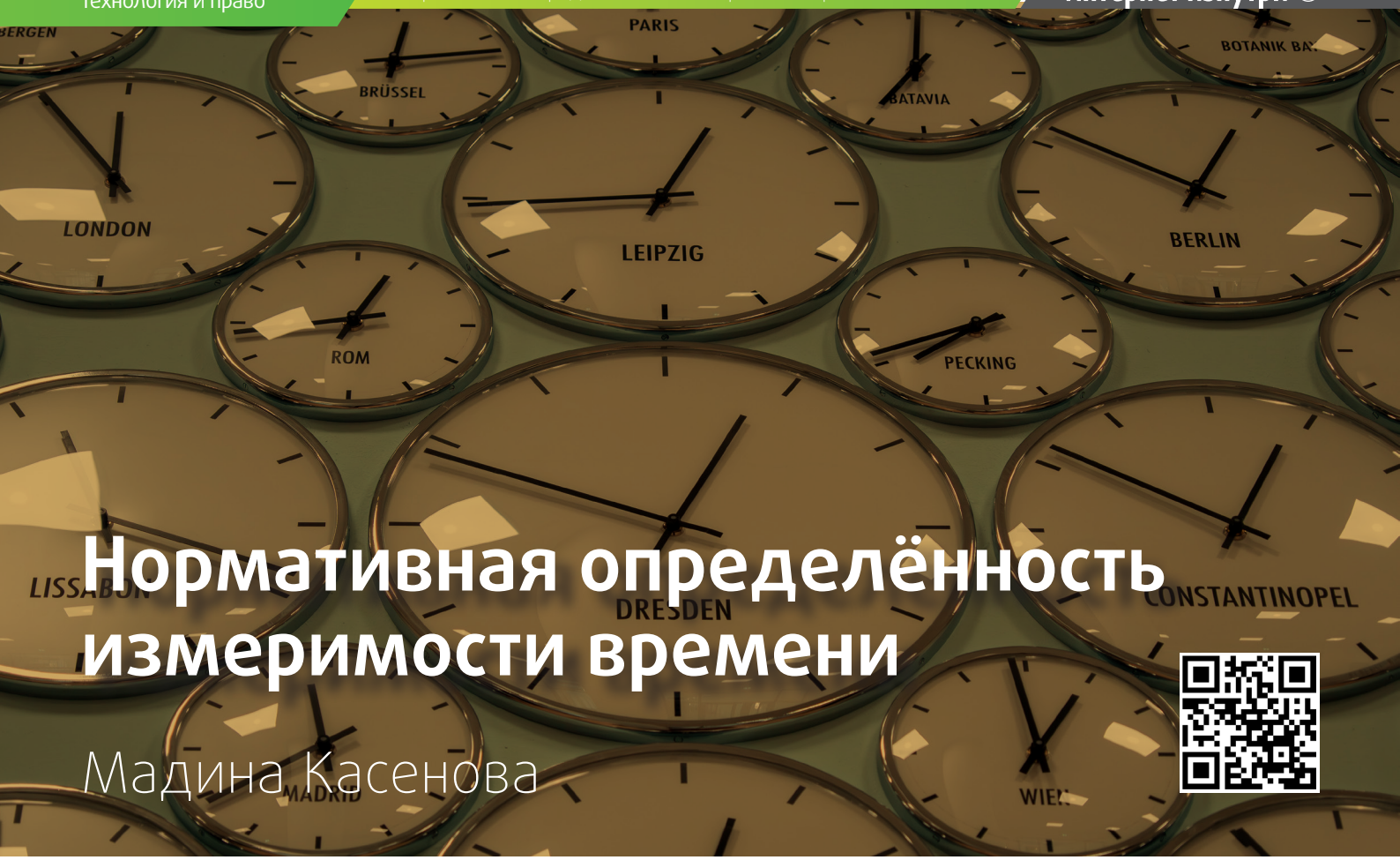
[17] Уорд Б. Внутреннее устройство Linux. 3-е изд. — СПб.: Питер, 2022. 342–343 с. ISBN 978-5-4461-3946-0

Об авторах:

Печерский Иван Васильевич, студент магистерской программы «Компьютерные системы и сети» МИЭМ НИУ ВШЭ.

Чертов Виктор Дмитриевич, студент магистерской программы «Компьютерные системы и сети» МИЭМ НИУ ВШЭ.

Научный руководитель: Александр Владимирович Белов, профессор, руководитель Департамента прикладной математики, МИЭМ НИУ ВШЭ.



Нормативная определённость измеримости времени

Мадина Касенова

Аннотация

Матрица измерения времени современной «цифровой реальности» аккумулирует регуляторные механизмы, функционал которых зиждется на нормативном комплексе, охватывающем унифицированные нормы международных стандартов, технологические нормы протоколов и стандартов Интернета, и сопрягается со стремительно расширяющимся установлением правовых норм в национальных правопорядках современных государств. Обращение к ряду нормативно-правовых документов свидетельствует об устойчивой тенденции установления нормативно-правовых требований синхронизации времени и строгих временных сроков соответствующих инструментов отчётности, что оценивается, по сути, как необходимая мера, оптимизирующая переход к отслеживаемой, управляемой в цифровом формате цепочке поставок цифровой продукции и транзакций во всех секторах.

Ключевык слова:

система SI, Всемирное время UTC, високосная секунда, протокол NTP, протокол PTP, время «UTC/NIST», правовая система Европейского Союза, синхронизация времени

Одним из самых устойчивых стремлений человечества является измерение такой универсальной константы как время. На протяжении веков был пройден длительный эволюционный путь поиска ответов на вопросы о сути времени, способов хронометража времени, определения методов точности его исчисления и т.д. Ретроспективный взгляд позволяет вспомнить, что представление о значимости времени и его измеримости восходит ещё к цивилизации шумеров (третье тысячелетие до н.э.), а способы и методы исчисления времени использовали вавилоняне, греки, древние римляне. Оставляя за скобками детали развития разнообразных концепций измерения времени, целесообразно обратить внимание на конец XIX – начало XX вв., когда бурный технический прогресс объективировал необходимость универсального согласования и стандартизации существующих во многих областях эталонных единиц систем отсчёта, включая систему единиц измерения времени.

Процесс стандартизации эталонных единиц систем отсчёта развивался нелинейно, и только во второй половине XX века удалось согласовать и утвердить глобальные стандарты измерения систем отсчёта в целом. В этой связи можно обозначить ключевые документы, не только определившие формат последующей нормативной унификации систем отсчёта времени, но во многом оказавшие влияние на формирование и содержание норм права большинства национальных правопорядков государств.

Во-первых, необходимо назвать Международную систему единиц (от фр. Système international d'unités, SI, далее – «Система СИ») [1], закрепившую семь базовых единиц систем отсчёта, в которой фундаментальной единицей измерения времени установлена секунда, исчисляемая по шкале атомного времени (TAI); производными единицами времени Системы СИ считаются минута и час, а их значения выводятся с использованием секунды.

Во-вторых, следует сказать об официальном закреплении (1972) международного стандарта скоординированного во всемирном масштабе эталона времени – т.н. всемирного времени (Coordinated Universal Time, далее – «Всемирное время UTC», «UTC»), иначе именуемого «универсальное ко-

ординированное время», которое используется для определения и регулирования текущего гражданского времени (civil time) в его «широком значении».

Установленные международные стандарты систем отсчёта и измерения времени институционально поддерживаются как на международном, так и на национальном уровне. Ведущими международными организациями выступают, в частности, Международная служба вращения Земли и систем отсчёта (далее – «Международная служба IERS» или «IERS») [2], а также Международный союз электросвязи (МСЭ), который в настоящее время определяет соответствующие рекомендации и варианты спецификаций стандарта UTC, включая его текущие версии [3].

Представляется важным сказать, что эталон Всемирного времени UTC исходит из единиц измерений времени Системы СИ; опирается на параметры универсального времени стандарта UT1; зиждется на атомной шкале времени (TAI), определяющей время с точностью до 10^{-9} секунды с корректировкой учета т.н. високосной секунды (leap second) [4]. Обобщённо, Всемирное время UTC измеряется в секундах (и их меньших единицах времени – миллисекунда, микросекунда, наносекунда и т.д.) и в минутах, а также в больших единицах времени (час, день, сутки, неделя и т.д.). Согласно UTC, каждые сутки содержат 24 часа, каждый час — 60 минут; каждая минута – 60 секунд; номера дней определяются как по григорианскому, так и по юлианскому календарю. Попутно заметим, что упомянутая високосная секунда характеризуется «непредсказуемостью» и периодичностью появления, что объясняется объективной обусловленностью существующего фактора переменности длительности времени и периода вращения Земли. Високосная секунда учитывается в шкале времени UTC, а коридор её значения определяется в пределах одной секунды от астрономического времени. В практическом плане високосная секунда корректирует последнюю минуту дня (как правило, июня и декабря) с шагом в одну секунду – до 61 или 59 секунд соответственно [5]. Исторически впервые високосная секунда была добавлена в шкалу времени UTC 30.06.1972; а в последнее десятилетие текущего века, начиная с декабря 2016 года, високосная секунда в её положительном значении добавлялась несколько раз. В текущем 2026 году ожидалось изменение в хронометраже измерения времени в связи с необходимостью введения високосной секунды в её «отрицательном значении» (negative leap second), однако эта необходимость была отложена как минимум до 2029 года [6].

Изложенное отнюдь не является отвлечёнными рассуждениями, поскольку едва ли оспоримым является то, что в современном глобально взаимосвязанном «цифровом мире» точность времени продолжает сохранять своё первостепенное значение. Несмотря на то, что de facto вышеупомянутые стандартизированные системы отсчёта и измерения времени преимущественно соотносимы с «доинтернетовской эпохой» в её современном понимании, сам по себе факт их существования с разной динамикой не мог не оказать влияния на формирование и развитие регулирующего комплекса как технологических норм, так и правовых норм национальных правопорядков современных государств. Так, генезис ряда ключевых протоколов и стандартов Интернета, включая временной период их появления, свидетельствует, что функционал компьютеров учитывал «точность времени», и практически каждый подключённый к Интернету компьютер/устройство изначально использовал протокол сетевого времени (Network Time Protocol, далее – «протокол NTP»), который является ключевым и непрерывно функционирует уже почти 40 лет.

Примечательно, что ранняя история интернет-технологий развивалась в контексте принятой в 1985 году экспериментальной версии протокола NTP (NTPv0). Тремя годами позже в своей первой версии Протокол NTP был утверждён и опубликован в качестве RFC 1059 (1988); он основывался на использовании иерархических, синхронизированных и распределённых систем отсчёта времени и базово опирался на универсальные, стандартизированные системы отсчёта времени и прежде всего – UTC, включающие в себя атомные/радиочастотные эталоны времени для достижения точности на уровне миллисекунд/наносекунд. В настоящее время каждый подключённый к Интернету компьютер/устройство так или иначе использует текущие версии протокола NTP с тем, чтобы интернет-хронометраж часов компьютеров/устройств синхронизировал время и корректно выравнивался относительно Всемирного времени UTC [7].

Говоря о протоколе NTP, было бы упущением не упомянуть протокол точного времени (Precision Time Protocol, далее «протокол PTP), установленный стандартом IEEE 1588. Протокол NTP обеспечивает точность менее десяти миллисекунд и используется в компьютерах, ноутбуках, иных устройствах и системах мониторинга сети, тогда как протокол PTP – это высокоточный сетевой протокол, предназначенный для синхронизации часов в распределённых системах, обеспечивающий точность времени до менее чем микросекунды [8]. Протокол PTP имеет решающее значение, в частности, для телекоммуникаций, когда важна синхронизация в реальном времени; в высокочастотном трейдинге (High-Frequency Trading, HFT) как особом виде биржевой торговли, в которой без участия человека ежесекундно осуществляются тысячи транзакций с ценными бумагами, и где ключевое значение имеет скорость принятия решений, а также точность синхронизации времени при их осуществлении. Актуализируется в настоящее время обсуждение проблематики доминирования протокола PTP и новых спецификаций, согласно которым обеспечение требуемой высокой точности требует перехода от «почтенного» протокола NTP к «высокоточному» протоколу PTP, например, в плане обеспечения корректной регистрации частных онлайн-банковских транзакций до синхронизации высокочастотных финансовых операций и т.д. [9]

Представляется, что вне зависимости от подходов, существующих в национальных правопорядках современных государств, матрица временного измерения современной «цифровой реальности» аккумулирует регуляторные механизмы, функционал которых зиждется на нормативном комплексе, включающем унифицированные нормы международных стандартов, технологические нормы протоколов и стандартов Интернета (прежде всего NTP/PTP), со стремительно расширяющимся охватом соответствующих правовых норм.

Измерение времени так или иначе сопрягается с правовой определённостью категориального аппарата целого ряда понятий, например: «разумное время», «своевременно», «ежедневно», «временные рамки отчётности» и т.д., содер-

жательное определение которых осуществляется в рамках конкретных правовых систем, при этом их закрепление (либо отсутствие такового), безусловно, в целом влияет на адекватность регулирующего воздействия права. Кроме того, практическую значимость приобретает, например, правовое закрепление порядка фиксации временных сроков определения момента начала/окончания обязательств, метки времени осуществления торговых и финансовых транзакций и т.д.

Современный рынок торговых и финансовых транзакций преимущественно осуществляется в цифровом формате и регулируется строгими нормативно-правовыми правилами, к числу которых относятся обязательные требования фиксации времени заключения сделок и их регистрации, а также необходимость предоставления соответствующей отчётности, что в общем комплексе регуляторных мер нацелено на обеспечение целостности глобальных финансовых систем, надёжности и точности синхронизации времени и бизнес-часов. Как отмечалось ранее, с одной стороны, такого рода правила учитывают соответствующие нормативы международных стандартов и, с другой стороны, основываются на конкретных законодательных нормах, установленных регулирующими органами национальных правопорядков государств. Сказанное наиболее наглядно можно продемонстрировать на некоторых примерах в сфере регулирования финансовых операций и рынка ценных бумаг.

Так, Акт о биржах США предусматривает строгие обязательства по созданию ежедневно пополняемой базы своевременных (подчеркнуто нами – М.К.) и точных данных о жизненном цикле торговых приказов/ордеров и фактически совершённых транзакциях на рынках акций, включая требования соблюдения точности временных меток в отношении их инициирования, маршрутизации, изменения и исполнения. Нелишне отметить, что в рассматриваемой сфере отношений «основным хранителем времени» в США является Национальный институт стандартов и технологий (NIST), ответственный за ведение хронометража и обеспечивающий поддержание Всемирного времени UTC. В этой связи становится объяснимым содержание установленных правовых требований Акта о биржах (и в т.ч. связанных с ним правовых актов) о том, что рабочие часы бизнес-процессов должны быть синхронизированы с точностью до 50 миллисекунд от т.н. времени UTC/NIST [10].

Безусловный интерес представляют современные реалии Европейского Союза (далее – «Евросоюз», «ЕС»), поскольку последние годы свидетельствуют о динамичном развитии т.н. европейского цифрового права. Принимая во внимание предметную область настоящей статьи, достаточно упомянуть ряд важных актов вторичного законодательства правовой системы ЕС, в частности, Акт о киберустойчивости (CRA), обновлённую Директиву об устойчивости критически важных объектов (NIS2), Регламент о цифровой операционной устойчивости (DORA), Директиву о рынках финансовых инструментов (MiFID II), Регламент ЕС о мгновенных безналичных расчётах в евро (IPR) и др.

Значение этих правовых актов не только в том, что они сами по себе создают всеобъемлющую нормативно-правовую базу правовой системы ЕС и определяют параметры её дальнейшего совершенствования, но также в их расширенном территориальном охвате. Речь идёт о юрисдикционном действии названных законодательных актов, которое распространяется как на правопорядки 27 стран-членов ЕС, так и охватывает государства Европейской экономической зоны (Исландия, Лихтенштейн, Норвегия). Закрепляемые в обозначенных законодательных актах нормы, наряду с прочим, предусматривают чёткие и строгие параметры времени, нацеленные на обеспечение надёжности и точности фиксации рабочих часов в бизнес-процессах, синхронизации времени по торговым и финансовым транзакциям, соблюдение обязательных требований по их регистрации и предоставления отчётности о времени осуществления транзакций (по дням, датам, временным меткам) и т.д. Ограниченный объём статьи позволяет лишь лапидарно проиллюстрировать два «блока» некоторых правовых предписаний.

Первый блок относится к обеспечению целостности глобальных финансовых систем и связан с введением правил детализации синхронизации времени, что сопрягается со строгими стандартизированными требованиями регистрации точности временных меток по осуществляемым финансовым транзакциям, включая предоставление соответствующей отчётности [11].

Например, ключевые моменты Директивы о рынках финансовых инструментов (MiFID II) [12] предусматривают стандарт синхронизации времени, что в практическом плане, в частности, означает:

- синхронизацию бизнес-часов для электронных транзакций, которая должна осуществляться с точностью до 1 микросекунды и коррелировать Всемирному времени UTC;
- проверку регистрации проставления временных меток согласно установленной временной последовательности для обеспечения прослеживаемости хронометража транзакций до и после их заключения;
- предоставление отчётности по транзакциям, соответствующей не менее 100 микросекундам, для компаний, занимающихся высокочастотным трейдингом (High-Frequency Trading Firms, HFT), а для голосовых сделок — 1 секунде.

Стандартизированные законодательные требования функционирования интегрированного европейского кредитно-финансового рынка закреплены упомянутым выше Регламентом ЕС о мгновенных безналичных расчётах в евро (далее – «Регламент IPR») [13]. Средства транзакций мгновенных безналичных расчётов зачисляются в течение нескольких секунд и круглосуточно. Важно отметить значимость Регламента IPR в плане определения содержательного объёма ряда ключевых понятий, среди которых: «мгновенный безналичный платёж», «незамедлительно», «круглосуточная доступность», «согласованное время» и т.д. Так, «мгновенный безналичный платёж» означает безналичный перевод средств, осуществляемый незамедлительно, т.е. 24 часа в сутки и в любой календарный день года; незамедлительно означает, что транзакции по переводу средств обрабатываются круглосуточно в режиме реального времени, и средства зачисляются на счёт получателя в течение нескольких секунд 24 часа в сутки и в любой календарный день года; круглосуточная доступность охватывает каждый день года.

Помимо этого, Регламент IPR устанавливает строгий 10-секундный коридор для:

- мгновенного перевода средств в любое время суток, включая нерабочее время, как в рамках одной страны ЕС, так и в другое государство-член ЕС;
- подтверждения получения и зачисления средств на счёт;
- уведомления отправителя перевода и получателя средств.

Второй блок относится к пакетному комплексу законодательных мер Евросоюза по устойчивому развитию, именуемому «Omnibus I» [14], и включает в том числе Директиву ЕС «Остановка отсчёта времени» (EU Directive «Stop-the-clock»), утверждённую в апреле 2025 года. Названная директива рассматривается как ограниченная во времени законодательная мера, призванная не только снизить первоначальную административную нагрузку на бизнес, но и способствовать повышению конкурентоспособности предприятий в масштабе ЕС. Эта директива, во-первых, продлевает (до 26.07.2027) временные сроки предоставления отчётности в области устойчивого развития, установленные Директивой о корпоративной отчётности в области устойчивого развития (Corporate Sustainability Reporting Directive, CSRD), во-вторых, откладывает на два года (до 26.07.2028) предусмотренные Директивой о комплексной проверке в области корпоративного устойчивого развития (Corporate Sustainability Due Diligence Directive, CSDDD) временные сроки исполнения требований по обязательствам для определённых компаний [15].

***

Представленный материал по понятным причинам во многом фрагментарен, однако, думается, он даёт общее представление о сути нормативно-правовых регуляторных параметров времени цифровой реальности, в которой все мы живём. Вероятнее всего, технологии точного измерения времени будут динамично развиваться и, по предположениям многих интернет-исследователей, фиксация времени современных цифровых устройств может быть откалибрована в пределах нескольких десятков наносекунд. Вот уж поистине измерение универсальной константы – времени – требует определённой рефлексии поэтического текста Роберта Рождественского: «... не думай о секундах свысока».

Список литературы:

[1] Международная система единиц SI официально применима в правопорядках большинства стран мира, включая Россию, см., например, Федеральный закон № 102-ФЗ (26.06.2008) «Об обеспечении единства измерений», СПС «КонсультантПлюс».

[2] International Earth Rotation and Reference Systems Service. https://www.iers.org/IERS/EN/Home

[3] См., например, Рекомендация МСЭ-R TF.460-6* – Излучение стандартных частот и сигналов времени. https://www.itu.int/dms_pubrec/itu-r/rec/tf/R-REC-TF.460-6-200202-I!!PDF-R.pdf

[4] Leap second and UT1-UTC information. https://www.nist.gov/pml/time-and-frequency-division/time-realization/leap-seconds

[5] См. об этом подробнее, например, Geoff Huston. Leaving it to the Last Second - The Leap Seconds Conundrum. https://circleid.com/posts/20161216_leaving_it_to_the_last_second_the_leap_seconds_conundrum

[6] Days Are Getting Slightly Longer As Earth's Spin Is Slowing At An «Unprecedented Rate». https://www.ndtv.com/science/days-are-getting-slightly-longer-as-climate-change-slows-the-earths-spin-unprecedented-rate-11217464

[7] Об этом подобнее, David L. Mills. A Brief History of NTP Time: Memoirs of an Internet Timekeeper. https://www.eecis.udel.edu/~mills/database/papers/history/historya.pdf; а также What Time Is It, Really? – The Science Behind Coordinated Universal Time (UTC). https://blog.meinbergglobal.com/2025/11/03/what-time-is-it-really-the-science-behind-coordinated-universal-time-utc/

[8] Подробнее, например, Precision Time Protocol (PTP) Explained. https://networklessons.com/ip-services/precision-time-protocol-ptp-explained

[9] NTP vs PTP: Choosing the Right Time Synchronization Protocol. https://resources.l-p.com/knowledge-center/network-time-protocol-ntp-vs-precision-time-protocol-ptp

[10] About Time.GOV. https://www.nist.gov/pml/time-and-frequency-division/about-timegov

[11] Biran G. How Can the Financial Industry Meet New Timestamping Regulations? https://www.blog.adtran.com/en/how-can-the-financial-industry-meet-new-timestamping-regulations

[12] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) Text with EEA relevance https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng

[13] Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro (Text with EEA relevance) https://eur-lex.europa.eu/eli/reg/2024/886/oj/eng

[14] Omnibus I (2025). https://commission.europa.eu/publications/omnibus-i_en

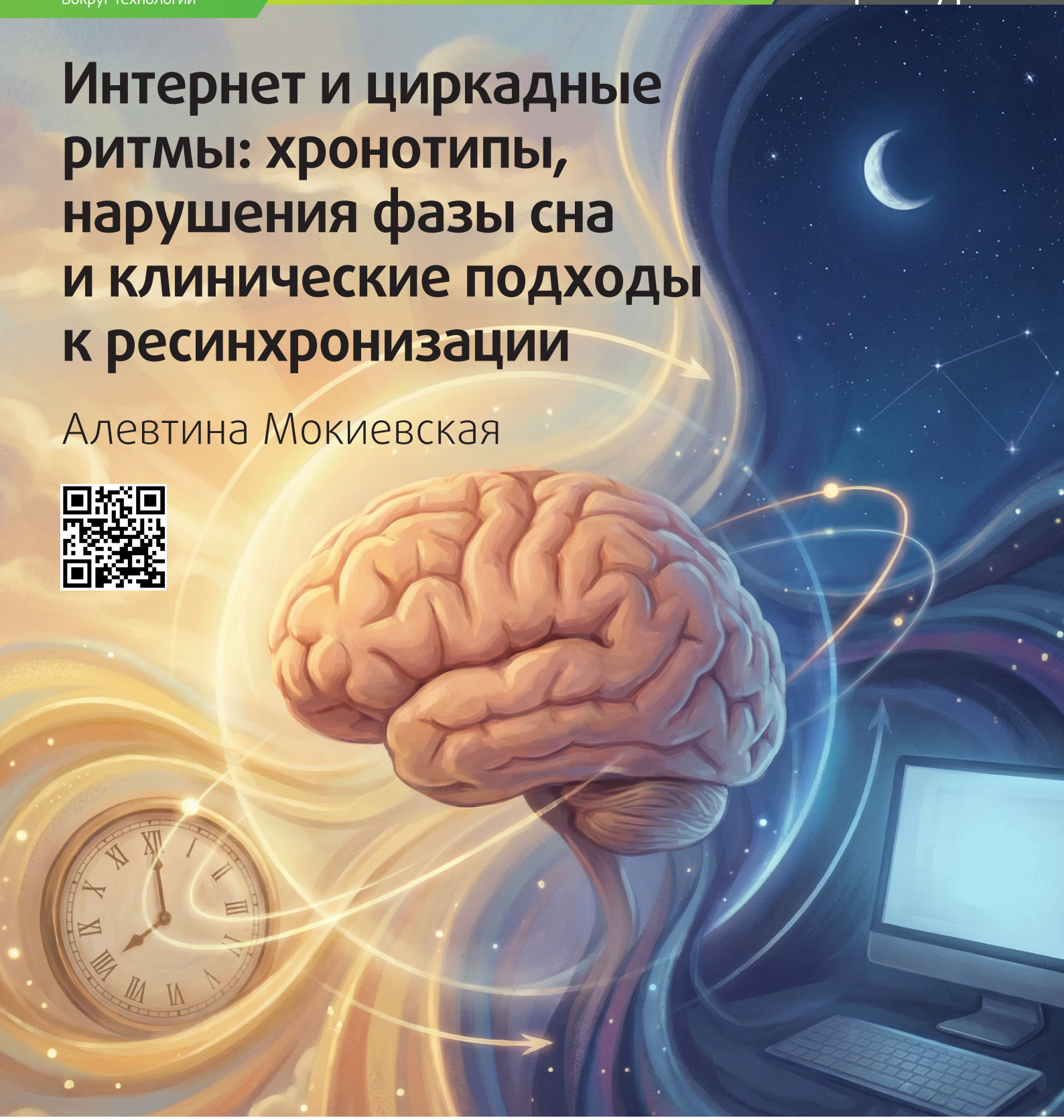
[15] Simplification: Council gives final green light on the 'Stop-the-clock' mechanism to boost EU competitiveness and provide legal certainty to businesses https://www.consilium.europa.eu/en/press/press-releases/2025/04/14/simplification-council-gives-final-green-light-on-the-stop-the-clock-mechanism-to-boost-eu-competitiveness-and-provide-legal-certainty-to-businesses/

Об авторе:

Мадина Балташевна Касенова – д.ю.н, юридическая фирма «Лиджист» (научно-консультативный совет)

Интернет и циркадные ритмы: хронотипы, нарушения фазы сна и клинические подходы к ресинхронизации

Алевтина Мокиевская



Аннотация
Статья посвящена роли циркадных ритмов как ключевого механизма синхронизации функций организма и клиническим последствиям их нерегулярности, характерной для IT-специалистов. Кратко изложены клеточные основы (супрахиазматическое ядро, TTFL), ключевые цейтгеберы (свет, температура, питание), спектр нарушений — от социального «джетлага» до метаболических и нейропсихических рисков, включая онкологические. Представлены практические подходы к ресинхронизации и разбор хронотипов («совы», «жаворонки»), синдромов запаздывания/опережения фазы сна и пошаговой хронотерапии..

Ключевые слова:
циркадные ритмы, биологические часы, супрахиазматическое ядро, хронотипы («совы», «жаворонки»), синдром запаздывания фазы сна, синдром опережения фазы сна, светотерапия, хронотерапия

Интернет и циркадные ритмы

Будучи врачом с многолетним опытом и имея собственных детей-айтишников, я пришла к выводу, что IT-специалисты — это особая группа мегаталантливых людей, которые, в большинстве своём, достаточно беспечно относятся к своему здоровью, таким образом «собственными руками» создавая себе проблемы в этой сфере. Это и послужило для меня причиной углубиться в эту ситуацию.

Дело в том, что наш мозг — это самый дорогой и сложный процессор, который у нас когда-либо был или будет. И он живёт и работает по своим законам, которые необходимо соблюдать для его максимально эффективной работы. И, как ни крути, в итоге всё упирается в закон циркадных ритмов.

Я не буду говорить про пользу сна, но я знаю, что IT-специалисты порой спят по четыре часа, живут в дедлайнах, страдают от прокрастинации, периодически их продуктивность падает, а «второе дыхание» открывается в 2 часа ночи.

Давайте посмотрим на проблему глазами врача и поговорим об этих самых циркадных ритмах. Смысл и функция циркадных ритмов — заранее готовить организм к определённым важным событиям, чтобы очередной приём пищи или отход ко сну, физическая и другая активности не застали организм врасплох и не привели к перерасходу энергии. Иными словами, смысл циркадных ритмов — экономия энергии и ресурсов.

Циркадные ритмы — это биологические ритмы, циклические повторения биологических процессов, которые занимают сутки. Например, циклы:

- сон—бодрствование;
- изменение температуры тела,
  изменение выработки гормонов;
- колебания работоспособности физической и умственной.

Наряду с циркадными ритмами существуют:

- ультрадианные ритмы (сердцебиение, дыхание, пищеварительные циклы, фаза сна, мочеиспускание, метаболические процессы, ощущение голода и насыщения, колебания эмоций). Продолжительность этих ритмов менее 12 часов;

- инфрадианные ритмы, которые продолжаются от суток до года (сезонная депрессия, маниакальные и депрессивные фазы, у животных — гон, линька, нерест (у рыб), периоды миграции птиц).

Почему мы обсуждаем эту тему?

Потому что корректность работы механизмов, настраивающих биологические часы в супрахиазматическом ядре гипоталамуса и на периферии, то есть во всех органах и тканях, влияет на все сферы нашего здоровья, включая психическое и интеллектуальное [1, с. 164–179].

Что же происходит при сбое циркадных ритмов?

Поначалу мы видим все симптомы джетлага (и не только при резкой смене часовых поясов, но чаще — социального джетлага, возникающего, например, при смене выходных и рабочих дней): запоры, диарея, вздутие, снижение аппетита, снижение работоспособности, усталость, недостаток энергии, нарушение когнитивных функций, снижение концентрации внимания, заторможенность, снижение памяти. И если разобраться, всё это — симптомы вегето-сосудистой дистонии. (Кстати, существует мнение, что вегето-сосудистая дистония — это «неуважительное отношение к себе».) В долгосрочной перспективе постоянные нарушения циркадных ритмов ведут уже не просто к лёгким функциональным нарушениям, а могут вызвать более серьёзные проблемы со здоровьем.

Внимание! К этим нарушениям ведёт именно и прежде всего нерегулярность циркадных ритмов, а не время отхода ко сну и подъёма.

Давайте в этом разберемся.

Для начала нужно понять, как работает система циркадных ритмов. Итак. Ритм работы часовых генов и их белковых продуктов на периферии зависит от клеточных механизмов в супрахиазматическом ядре гипоталамуса. И циркадные ритмы регулируются клеточными генетическими механизмами, а именно работой транскрипционно-трансляционной петли с обратной связью (TTFLs — transcription–translation feedback loops). Одни гены работают, когда светло, другие — когда темно. И основными факторами, с которыми синхронизируются циркадные ритмы, являются свет и температура [1, с. 164–179; 2, с. 433–446]. Механизм биологических часов есть практически во всех клетках тела, и он должен быть синхронизирован с ритмом работы биологических часов супрахиазматического ядра гипоталамуса [1, с. 164–179]. Знание механизмов регуляции биологических часов нужно, чтобы понимать механизмы развития некоторых заболеваний, обусловленных полиморфизмами или мутациями генов биологических часов. Влияние на работу этих генов (социальные причины, состояние здоровья, особенности экспрессии этих генов, регулирующих циркадные ритмы) обусловливает склонность к психическим заболеваниям, нейродегенеративным заболеваниям, онкологическим заболеваниям, хронизации инфекции, нарушению сна [3].

Рассмотрим такой пример. Какая связь существует между циркадными ритмами и раком? Каким образом нарушение циркадных ритмов способствует этому заболеванию?

Все гены, обеспечивающие работу биологических часов, влияют на многие процессы, включая внутриклеточные. Для резистентности организма к раку нужна качественная ДНК и работа антионкогенов. Например, белок PER2 из системы биологических часов соединяется с белком p53, запускающим апоптоз.

Это способствует стабильной и корректной работе этого белка. Если образование PER2 нарушено, то стабильного p53 мало, и нарушается апоптоз (то есть избавление организма от повреждённых, мутагенных, инфицированных клеток) [4; 5]. Качество сна влияет на активность клеток иммунной защиты, а сон сильно зависит от биологических часов. Есть работы, доказывающие, что само по себе налаживание циркадных ритмов вызывает регресс рака (например, «Enhancing circadian clock function in cancer cells inhibits tumour growth») [6].

Циркадные ритмы — важнейший фактор нейропластичности. От правильной работы циркадных ритмов зависит способность мозга к регенерации, адаптации к внешним условиям, поведению, способность к обучению, усвоению новой информации, память. Нарушение циркадных ритмов, связанное с нарушением гигиены сна, приводит к бессоннице, депрессии, тревоге, нарушению обмена веществ, артериальной гипертонии, метаболическому синдрому. Очень ярко это продемонстрировала пандемия COVID-19 [7, с. 2053–2064].

Теперь разберёмся, какие факторы влияют на синхронизацию механизма биологических часов в клетках с ритмом работы биологических часов гипоталамуса.

Самый главный фактор — это суточные колебания света и темноты. NB! Не просто темноты во время сна, а именно чередование достаточной освещённости и полной темноты [1, с. 164–179].

С ним синхронизируется ритм изменения температуры тела и цикл сон—бодрствование.

Ещё один очень важный фактор — это приём пищи по четкому расписанию, так как на генетический механизм влияют сигналы и процессы, связанные с выработкой глюкозы, инсулина [1, с. 164–179].

И на это всё мы реально можем повлиять для налаживания циркадных ритмов.

Как это сделать?

Первый фактор — свет и темнота.

Циркадные ритмы зависят не от астрономических часов, а от освещения и темноты.

В ответ на темноту вырабатывается мелатонин («гормон сна»). Но он также быстро разрушается, не исполнив своей «миссии», под воздействием света, попадающего к нам в зрачок, а именно — от экранов телевизоров, компьютеров, телефонов. Поэтому так часто мы слышим призывы убрать «из поля зрения» экраны не менее чем за час, а лучше — за два часа до сна. В крайнем случае, если есть острая необходимость, нужно перевести свой сотовый в режим ночного экрана.

Кроме того, любая зрительная информация, попадая к нам в мозг, возбуждает в нём определённые структуры, которые успокаиваются не ранее чем через 20 минут от этого момента. Если «с темнотой» нам более-менее всё ясно, и придумать, как ее создать, не представляет труда, то что же делать «со светом»? В идеале, попадание в зрачок яркого солнечного света стимулирует все правильные процессы бодрствования, настраивая организм на продуктивный день. Но, как вы понимаете, осенью и зимой этого не бывает, по крайней мере, в Москве. Можно ли это исправить? Оказывается, можно. Существуют приборы — лампы для лечения сезонной депрессии, 30-минутное воздействие которых может в большой степени заменить солнечный свет. Включать эти лампы следует за 11 часов до сна. Таким образом, ко сну мы готовимся с утра, настраивая свои циркадные ритмы.

Вторым важным фактором является температура тела. Колебания температуры составляют от 0,5 до 1 градуса. Чем ниже температура, тем проще заснуть. И этот факт мы тоже можем использовать, чтобы ускорить засыпание. Например, после принятия теплой ванны температура тела снижается в течение двух часов. Поэтому рекомендовано принять теплую ванну за два часа до сна. После физической нагрузки, которая повышает температуру тела, в течение четырёх часов наблюдается ее снижение. Поэтому для лучшего засыпания за четыре часа до сна рекомендовано осуществлять физическую нагрузку [2, с. 433–446].

И ещё один немаловажный фактор — это регулярный приём пищи: таким образом происходит влияние на циркадные ритмы изменения уровня глюкозы. Поэтому для более чёткой синхронной работы биологических часов регулярный приём пищи — очень действенный метод [1, с. 164–179].

Хронотипы «жаворонки—совы»

Поговорим о нарушении циркадных ритмов, а именно — о синдромах, которые входят, в том числе, в Международную классификацию болезней (МКБ):

- синдром запаздывания фазы сна (это «совы»);
- синдром опережения фазы сна (это «жаворонки») [8].

Сначала о «совах»

Что характерно для таких людей?

Напомню, что у нас существуют суточные колебания температуры тела на 0,5–1 градус. У «сов» минимальная температура тела приходится на 3–4 часа утра. И если они ложатся раньше, они не могут заснуть, так как все системы их тела настроены на засыпание именно в 3–4 часа утра (то есть на 2–3 часа позже конвенционального времени).

Как нам определить — сова вы или жаворонок?

1. Метод называется актиграфия — трекинг сна-бодрствования в течение 7–14 дней. Осуществляется с помощью специального прибора, надеваемого на запястье [9, с. 1199–1236; 8].

2. «В быту» это можно сделать достаточно просто — измерением температуры тела каждый час в течение суток и построением графиков. Таким образом мы сможем поймать пик, когда температура тела станет самой низкой.

Как мы будем изменять графики, если мы «совы»?

Прежде чем принимать такое решение, нужно вспомнить, что это может быть вариантом нормы. Если «сова» живёт в таком графике, и ей удобно, то надо оставить всё как есть. Тем более, если сове не нужно рано вставать. Просто создайте оптимальные условия. Какая проблема у «сов»? Если они поздно ложатся, особенно в летнее время, они будут рано просыпаться из-за дневного света. Но если в спальне обеспечить полное затемнение, то проблемы не будет. Главное — регулярность. Таким образом, если «сова» регулярно входит в одно и то же время отхода ко сну и пробуждения (особенно если она контактирует с достаточным количеством дневного света в период бодрствования, и спальня достаточно затемнена в период, когда она спит), то проблемы нет.

Если «сова» просыпается очень поздно и не имеет никаких шансов контактировать со световым днём, то подключаем приборы (специальные лампы), чтобы обеспечить фоторецепторы тем светом, который нам жизненно необходим для хорошего качества сна и жизни.

Возьмём другую ситуацию. Вы — «сова», ложитесь в 3 часа ночи, но график работы подразумевает раннее вставание. И каждый раз для вас это становится проблемой. Вы не можете раньше уснуть и мучаетесь бессонницей из-за того, что у вас запаздывает фаза сна. И не можете проснуться, потому что ваши биологические часы в это время еще спят. Что нужно сделать? Мы не можем просто сказать себе: «В 23:00 отходи ко сну и вставай в 07:00». Таким образом мы устроим себе стресс и фрустрацию. И эти часы нужно просто постепенно подвинуть.

Раз в шесть дней смещаем свой график укладывания на 1 час раньше. Но, чтобы синхронизировать наши внутренние биологические часы с этим желаемым временем укладывания, мы будем использовать рычаги, которые мы уже обсуждали: изменение температуры тела, физическую нагрузку, свет [9, с. 1199–1236].

Напомню, что световое воздействие нужно дать в первой половине дня. От этого воздействия температура тела будет повышаться, затем очень постепенно снижаться. Важно, чтобы световое воздействие (лампы, солнечный свет) происходило не позже, чем за 11 часов перед отходом ко сну.

Кстати, если, наоборот, вы — «жаворонок», и у вас раньше наступает сонливость и засыпание, то световое воздействие рекомендовано отодвинуть. Оно должно проводиться в вечернее время [9, с. 1199–1236].

Физические нагрузки осуществляются за 4–6 часов до желаемого отхода ко сну. Например, если вы обычно ложитесь спать в 3 часа ночи, то шесть дней подряд рекомендовано ложиться в 2 часа, а в 22:00 осуществлять физическую нагрузку. В следующие шесть дней вы ложитесь в час ночи, а физической нагрузкой занимаетесь в 21:00. И так далее.

График изменения температуры тела можно понять, измеряя температуру после физической нагрузки каждый час. И в зависимости от этого физическая нагрузка будет осуществляться за четыре, пять или шесть часов до отхода ко сну.

Это может быть также тёплая ванна за два часа до предполагаемого отхода ко сну.

Но не каждый человек будет ежедневно принимать ванну или давать себе физические нагрузки. Поэтому проще всего использовать световые приборы. Под ними можно работать, заниматься делами.

Таким образом, двигать график, чтобы превратиться из «совы» в «жаворонка», стоит лишь в том случае, если это целесообразно. И никаких резких перемен во времени «укладывания»! Так как это приведет к сбою биологических ритмов. Поэтому действуем аккуратно и подключаем такие рычаги, как свет, влияние температуры тела и физические нагрузки [9, с. 1199–1236].

Теперь поговорим о «жаворонках»

Синдром опережения фазы сна («жаворонки») — это нарушение циркадных ритмов, при котором засыпание происходит, как минимум, на два часа раньше конвенционального времени отхода ко сну. Это может быть проблемой, если человеку надо участвовать в социальных активностях в вечернее время, а он при этом чувствует выраженную сонливость. Тогда это требует лечения, в остальных случаях — нет [8]. Если ритм жизни человека не совпадает с тем, что ему нужно, с его биологическими часами, можно сдвигать время укладывания на более позднее. Принципы такие же, как при работе с «совами», только двигаем график на час позже [9, с. 1199–1236].

Кстати, есть генетическая предрасположенность синдрома опережения фазы сна. Но и в этом случае возможно посте-

пенно смещать график сна, используя физиологические механизмы: регулярный график отхода ко сну, светотерапию в ранние вечерние часы, хронотерапию — смещение времени отхода ко сну на один час позже каждые шесть дней до достижения желаемого времени [9, с. 1199–1236].

Таким образом, дорогие друзья, всего лишь несколько простых правил — и наши циркадные ритмы наладятся, а это, в свою очередь, избавит нас от многих проблем, связанных со здоровьем. Болезнь гораздо проще предотвратить, чем вылечить. Это аксиома, которая подтверждается тысячелетиями врачебной практики и научными данными. Тем более, что многие заболевания являются неизлечимыми. Это как раз те хронические болезни, которые сейчас стоят «во главе угла» современной медицины. Например, гипертоническая болезнь или мерцательная аритмия (фибрилляция предсердий), однажды появившись, останутся с человеком навсегда. Но даже в этом случае нужно помнить, что практически у любого хронического заболевания существуют периоды обострения и ремиссии. И в наших силах увеличить эти самые периоды ремиссии, снизить риски и избежать осложнений.

Так что изменить ситуацию можно, если понять простую истину — здоровье — это не подарок судьбы, а результат определённой «работы», ежедневных усилий и осознанного выбора.

Конечно, никто ещё не прожил 200 лет, но я точно знаю, что важно не только количество прожитых лет, но и качество жизни. Поэтому, друзья, «берегите здоровье смолоду».

Список литературы:

[1] Takahashi J.S. Transcriptional architecture of the mammalian circadian clock. Nature Reviews Genetics. 2017;18(3):164–179. Nature Publishing Group. URL: https://www.nature.com/articles/nrg.2016.150 (дата обращения: 12.03.2026).

[2] Preußner M., Goldammer G., Neumann A., Haltenhof T., Heyd F., et al. Body Temperature Cycles Control Rhythmic Alternative Splicing in Mammals. Molecular Cell. 2017;67(3):433–446.e4. Cell Press. DOI: 10.1016/j.molcel.2017.06.006. URL: https://pubmed.ncbi.nlm.nih.gov/28689656/ (дата обращения: 12.03.2026).

[3] Liu H., Liu Y., Hai R., Liao W., Luo X. The role of circadian clocks in cancer: Mechanisms and clinical significance. Genes & Diseases. 2023. Elsevier. URL: https://www.sciencedirect.com/science/article/pii/S2352304222001490 (дата обращения: 12.03.2026).

[4] Gotoh T., Vila-Caballer M., Liu J., et al. Association of the circadian factor Period 2 to p53 influences p53's function in DNA-damage signaling. Molecular Biology of the Cell. 2015. American Society for Cell Biology. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC4294682/ (дата обращения: 12.03.2026).

[5] Gotoh T., et al. Model-driven experimental approach reveals the complex regulatory distribution of p53 by the circadian factor Period 2. Proceedings of the National Academy of Sciences of the USA. 2016. National Academy of Sciences. DOI: 10.1073/pnas.1607984113. URL: https://www.pnas.org/doi/10.1073/pnas.1607984113 (дата обращения: 12.03.2026).

[6] Kiessling S., Beaulieu-Laroche L., Blum I.D., Landry G., et al. Enhancing circadian clock function in cancer cells inhibits tumor growth. BMC Biology. 2017;15:13. BioMed Central. DOI: 10.1186/s12915-017-0349-7. URL: https://link.springer.com/article/10.1186/s12915-017-0349-7 (дата обращения: 12.03.2026).

[7] O'Regan D., Jackson M.L., Young A.H., Rosenzweig I. Understanding the Impact of the COVID-19 Pandemic, Lockdowns and Social Isolation on Sleep Quality. Nature and Science of Sleep. 2021;13:2053–2064. Dove Medical Press. DOI: 10.2147/NSS.S266240. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8593898/ (дата обращения: 12.03.2026).

[8] American Academy of Sleep Medicine. International Classification of Sleep Disorders, 3rd ed. Text Revision (ICSD-3-TR): Circadian Rhythm Sleep-Wake Disorders (Draft Chapter). AASM. URL: https://aasm.org/wp-content/uploads/2022/05/ICSD-3-TR-CRSWD-Draft.pdf (дата обращения: 12.03.2026).

[9] Auger R.R., Burgess H.J., Emens J.S., Deriy L.V., Thomas S.M., Sharkey K.M. Clinical practice guideline for the treatment of intrinsic circadian rhythm sleep-wake disorders: advanced sleep-wake phase disorder (ASWPD), delayed sleep-wake phase disorder (DSWPD), non-24-hour sleep-wake rhythm disorder (N24SWD), and irregular sleep-wake rhythm disorder (ISWRD). An update for 2015. Journal of Clinical Sleep Medicine. 2015;11(10):1199–1236. American Academy of Sleep Medicine. DOI: 10.5664/jcsm.5100. URL: https://aasm.org/resources/clinicalguidelines/crswd-intrinsic.pdf (дата обращения: 12.03.2026).

Об авторе:

Мокиевская Алевтина Николаевна - врач высшей квалификационной категории, врач-кардиолог, аритмолог, липидолог, врач интегративной медицины. Медицинский Центр «Парацельс», г. Истра, Московская область, Россия.

Новости науки и техники

До 60% поисковых запросов в сети уже обходятся без кликов

Уже около 60% поисковых запросов в сети обходятся сегодня без кликов по ссылкам. Поиск выполняет искусственный интеллект, предлагая пользователю готовые варианты. И даже именитые бренды рискуют в такой ситуации внезапно исчезнуть из поля зрения потребителей.

На протяжении многих лет браузеры служили доминирующими порталами в Интернет. И интернет-маркетинг предлагал понятный и проверенный путь: поиск, клик, сайт, конверсия. Но развитие ИИ нарушило эту модель: на смену «поиск - клик» всё активнее идёт «спросил - решил». Эксперты говорят о фундаментальном сдвиге, самой значительной трансформации со времён революции мобильных устройств. И она непосредственно затрагивает интересы бизнеса. Многие крупные компании уже констатируют резкое снижение посещаемости из поиска, несмотря на то, что выручка и использование продуктов продолжают расти.

Это не означает, что традиционная браузер-ориентированная модель умерла, она просто эволюционирует. Меняется место, где принимаются решения: всё чаще это происходит внутри ИИ-среды ответов, а не на отдельных веб-страницах. И если покупатель, например, попросит ИИ-помощника найти лучшие наушники с шумоподавлением, сравнить цены у разных ретейлеров, проверить различия в характеристиках и показать самые надёжные отзывы, он сможет получить уверенную рекомендацию, не посещая при этом ни один из сайтов десятков брендов или маркетплейсов.

В основе маркетинга лежит верно сформулированное сообщение и выбор целевой аудитории. Раньше это означало привлекательность ключевых слов и креативных решений. Но в мире ИИ-помощников решение всё чаще принимается промежуточной системой, которая пытается определить намерение пользователя, взвесить варианты и предоставить единый синтезированный ответ. Несогласованные названия, противоречивые сообщения или устаревшие описания продукта не только дезориентируют покупателей, они увеличивают риск того, что ИИ-системы оценят продукт неверно или вовсе не включат его в обзор.

Бренды, которые адаптируются быстрее других, максимально серьёзно относятся к консистентности. Они следят за тем, чтобы их история, данные и язык продукта были согласованы везде, где они появляются, чтобы инструменты ИИ могли представлять их точно, а клиенты узнавали их быстро. По сути, речь идёт о том, что искусственный интеллект сам становится аудиторией маркетинговых сообщений. И в этой связи эксперты называют главной задачей года решение проблемы машиночитаемости информации брендов.

Источник: Techradar
https://www.techradar.com/pro/ai-first-browsers-and-the-end-of-the-pageview-economy

Доменные имена как «якоря доверия»

Интернет-поиск с использованием искусственного интеллекта ставит вопрос о роли доменных имён. И может показаться, что эта роль становится второстепенной: получая нужную ему информацию, пользователь может вообще не видеть ссылок и не иметь представления о том, откуда это информация поступила. Но это неверно. Доменные имена по-прежнему чрезвычайно важны, однако новая эпоха меняет их роль. В известном смысле можно говорить о том, что сегодня доменные имена всё чаще выступают в качестве «якорей доверия».

Системы искусственного интеллекта постоянно развиваются и всё чаще опираются на данные о поведении пользователей. Метрики вовлечённости, такие как CTR, время на сайте и прямые запросы по домену, учитываются алгоритмами для

определения достоверности. Домены с лояльной аудиторией посылают сильные сигналы о том, что их стоит включать в ИИ-обзоры. Если пользователи постоянно позитивно взаимодействуют с доменом, искусственный интеллект рассматривает это как важное подтверждение. Допустим, пользователь ищет финансовую информацию. В этой ситуации условный домен TrustedFinance.com будет иметь больше веса для ИИ, чем нишевый микросайт с малоизвестным именем. Узнаваемость формирует авторитет в восприятии людей, и AI-модели отражают этот сдвиг.

В то же время искусственный интеллект не нуждается в точных совпадениях по ключевым словам, он понимает контекст и семантику. Вместо этого доминируют сигналы авторитета. К ним относятся история домена, качество обратных ссылок и соответствие тематической экспертизе. Домен, который последовательно публикует достоверную информацию в данной нише, с большей вероятностью будет процитирован ИИ, даже если плотность ключевых слов ниже, чем у конкурентов. Искусственный интеллект меньше интересует, совпадает ли имя домена с запросом, и больше — заслужил ли домен доверие.

Можно говорить о том, что системы искусственного интеллекта заботятся о своей репутации, отфильтровывая рискованные или неактуальные источники. И в этой связи доменные имена приобретают дополнительную ценность. Бизнесу необходимо идти на долгосрочные инвестиции в создание брендируемых доменов, укрепление тематического авторитета и отдавать приоритет доверию пользователей, а не краткосрочным тактикам ключевых слов. По сути, ИИ не устраняет домены, возвышает их. Доменное имя нужно уже не просто для ранжирования на первой странице поисковой выкладки, оно нужно для того, чтобы быть выбранным в качестве источника достоверной информации.

Источник: NameSilo
https://www.namesilo.com/blog/en/ai/can-domains-influence-ai-search-rankings-what-we-know-so-far

Дипфейки наступают

Технологии генеративного искусственного интеллекта развиваются стремительно. И одним из следствий этого развития становится лавина дипфейков - сгенерированных ИИ изображений и видео публичных персон. «Граница между политической карикатурой и реальностью становится всё более размытой», - констатирует Дэниел Шифф, преподаватель кафедры политических технологий Университета Пардью и содиректор Лаборатории управления и ответственного AI (Governance and Responsible AI Lab - Grail). Согласно данным этой лаборатории, количество политических дипфейков резко возросло за последние годы. С начала 2025 года организация зарегистрировала более 1000 публикаций в социальных сетях на английском языке с поддельными изображениями или видео известных политических фигур и политически значимых социальных событий. За предыдущие восемь лет организация зафиксировала 1344 подобных случая.

По иронии судьбы, политические дипфейки всё чаще используют сами политики, причём самого высокого уровня. Так, во время выборов 2024 года Дональд Трамп публиковал сгенерированные искусственным интеллектом изображения, на которых фанаты Тейлор Свифт выражали ему свою бурную поддержку. Согласно базе данных Grail, с 2024 года Трамп и Белый дом поделились по крайней мере 18 дипфейками в социальных сетях.

Впрочем, не отстают и оппоненты. Губернатор Калифорнии Гэвин Ньюсом, который, по многим прогнозам, будет баллотироваться в президенты в 2028 году, также начал делиться дипфейками, направленными против Трампа. В частности, на одном из опубликованных им изображений президент Трамп улыбается голограмме Джеффри Эпштейна.

Исследователи всё чаще говорят о том, что политические дипфейки могут быть убедительными, даже если потребители понимают, что изображения не настоящие. «Люди не обязательно ищут то, что реально, они скорее ищут то, что соответствует их убеждениям», - отмечает Сэм Грегори, исполнительный директор некоммерческой организации Witness, посвящённой правам человека и борьбе с обманами в использовании искусственного интеллекта.

Причём в ближайшее время ситуация может стать ещё хуже. Согласно недавнему исследованию, опубликованному в журнале Science, современные технологии уже могут использоваться как «ИИ-рой», способный «координироваться автономно, проникать в сообщества и эффективно создавать консенсус». То есть действовать как «фермы троллей», но вообще без всякой необходимости в людях.

Способ остановить волну цифровых фальшивок и тех, кто за ними стоит, есть. Организация Coalition for Content Provenance and Authenticity разработала «технический стандарт для издателей, создателей и потребителей, устанавливающий происхождение и правки цифрового контента». Он встраивается в фото, сделанное камерой, или в контент, созданный с помощью ИИ-инструмента или отредактированный им, а затем размещённый на платформе, как набор криптографически подписанных метаданных. И технологические компании должны использовать эту информацию, чтобы помечать, создан ли тот или иной контент с использованием ИИ.

LinkedIn, Pinterest, TikTok и YouTube уже обязались маркировать сгенерированный искусственным интеллектом контент. Однако ресурс Indicator недавно провёл эксперимент: разместил 200 сгенерированных изображений и видео на перечисленных платформах, чтобы проверить, будут ли публикации помечены. Как выяснилось, самые старательные — LinkedIn и Pinterest — пометили только 67% контента, Instagram же отметил лишь 15 из 105 фейковых изображений.

Источник: The Guardian
https://www.theguardian.com/technology/2026/mar/28/military-deepfakes-ai-propaganda-money

Новости доменной индустрии

Сервис GlobalBlock начал работу в национальных доменах Китая и Германии

Организация Brand Safety Alliance, созданная по инициативе компании GoDaddy, сообщила о том, что расширила число доменных зон, в которых действует её сервис GlobalBlock. Он начал работу два года назад и является ведущим сервисом защиты брендов в доменном пространстве. GlobalBlock позволяет правообладателям включать наименования своих брендов в блок-лист, препятствующий регистрации доменных имён, которые совпадают с наименованиями брендов, во множестве доменных зон. А расширенная версия сервиса GlobalBlock+ блокирует ещё и возможность регистрации сходных доменных имён (использующих омоглифы, дефисы, изменённый порядок букв и т.д.).

Кроме того, в сервисе действует функция автоматического «перехвата» доменных имён Priority AutoCatch. Если совпадающий или сходный с наименованием бренда домен был зарегистрирован до включения в блок-лист, он блокируется, как только его регистрация не продлевается после истечения срока. Это исключает возможность того, что домен будет выставлен на аукцион и окажется в чужих руках. За время своей работы сервис уже предотвратил регистрацию около пяти миллионов доменных имён, ещё более десяти тысяч имён были «перехвачены» с помощью Priority AutoCatch.

Сервис GlobalBlock расширил свои возможности сразу на 70 доменных зон и теперь покрывает 780 доменных зон, включая общие домены верхнего уровня, национальные домены и блокчейн-домены. Главным приобретением следует, безусловно, считать включение в этот список национальных доменов Китая .cn и Германии .de. В первом из них зарегистрировано более 20 миллионов доменных имён, во втором – 17,8 миллиона. Таким образом, сервис GlobalBlock распространяется теперь на две крупнейших после .com доменных зоны. Впрочем, ложкой дёгтя в данном случае является то, что домен .com по-прежнему недоступен для GlobalBlock.

Источник: Domain Incite
https://domainincite.com/31614-globalblock-signs-the-two-best-deals-it-will-ever-get

Число зарегистрированных доменных имён выросло за год на 2,2%

Доменная торговая площадка Sedo и компания-регистратор и хостинг-провайдер InterNetX представили очередной выпуск своего ежегодного отчёта Global Domain Report. Он подводит итоги 2025 года, и цифры свидетельствуют о том, что год оказался в достаточной мере позитивным для доменной индустрии. Число зарегистрированных доменных имён достигло 386,9 миллиона, увеличившись на 2,2% по сравнению с предыдущим годом.

Максимальный рост продемонстрировали новые общие домены верхнего уровня, которые «подросли» сразу на 29,9%. Для сравнения, национальные домены, например, показали рост в 3,4%. Именно представители новых доменов лидируют и в «индивидуальном зачёте»: доменная зона .channel выросла на 1050%, .forum – на 1005%, а .locker – на 796%. Впрочем, неоспоримым лидером в абсолютных цифрах остаётся, разумеется, общий домен верхнего уровня .com, прибавивший пять миллионов регистраций. Однако сразу вслед за ним идёт представитель новых доменов – .xyz, который вырос на 4,2 миллиона зарегистрированных имён.

Источник: Координационный центр доменов .RU/.РФ
https://cctld.ru/media/news/industry/39879/

Блокчейн-домены клонятся к закату?

Глава компании Unstoppable Domains Мэттью Гулд на днях объявил о том, что компания впредь будет отдавать предпочтение традиционным (Web2) доменным именам, поскольку блокчейн-домены (Web3) не оправдали возложенных на них ожиданий. Заявление весьма примечательно, поскольку Unstoppable Domains на протяжении нескольких лет была одной из самых крупных и известных компаний, продвигавших блокчейн-домены.

«Домены, существующие только в Web3, были частью криптовалютного бума 2021 года, но не смогли достичь массового использования. И уже некоторое время мы считаем, что они останутся нишевым рынком как сейчас, так и в будущем. Они были отличной отправной точкой для нашего пути в мире доменов, но в дальнейшем мы будем ещё больше сосредоточены на традиционном рынке, поскольку именно он является по-настоящему массовым», – написал Гулд.

Как и следовало ожидать, заявление Мэттью Гулда вызвало бурю негативных комментариев. Некоторые даже упрекают компанию в обмане инвесторов, припоминая, как активно Unstoppable Domains продвигала блокчейн-системы доменных имён. Но эти упрёки вряд ли заслужены, скорее, они звучат как претензии игроков, поставивших деньги не на ту лошадь. Да, блокчейн-домены в период криптовалютной лихорадки выглядели чрезвычайно перспективными. Да, они были очень удобны в качестве адресов криптовалютных кошельков. Но при этом они оказались не в состоянии полноценно выполнять свою главную функцию – собственно, функцию доменных имён. Если браузеры не распознают такие доменные имена, то на них нельзя создавать сайты, а если нет сайтов, то какой смысл в доменах?

Unstoppable Domains – далеко не единственная компания, пришедшая к этому очевидному выводу. Компания Namecheap, например, уже продала свой сервис Handshake, работавший с Web3-доменами, а немногие аккредитованные ICANN регистраторы, которые вообще продавали такие домены, отодвинули их «на задворки» своих сайтов. Это вполне логично: там, где речь идёт о глобальных системах, людям и рынку нужны не децентрализация, а напротив, централизация, последовательность и единые для всех правила.

Источник: Domain Name Wire
https://domainnamewire.com/2026/03/19/web3-domains-are-dead/

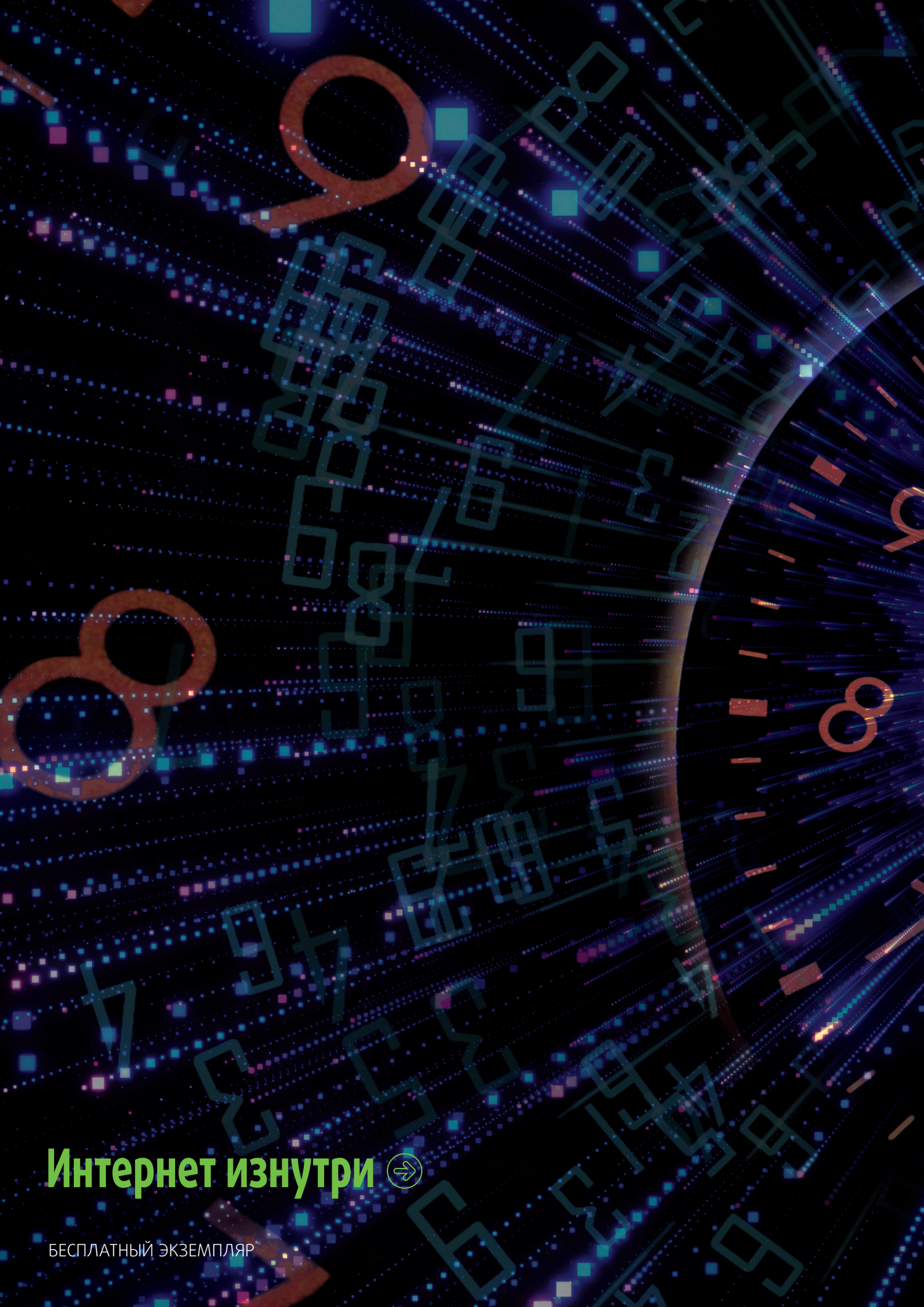
Названы сроки запуска нового домена .latino

Регистратура DISH DBS раскрыла сроки запуска своего домена .latino. Он был делегирован ещё в ходе первого этапа программы новых общих доменов верхнего уровня. Но и сегодня, когда остается всего месяц до старта второго этапа этой программы, многие домены, получившие зеленый свет более десяти лет назад, продолжают оставаться бездействующими. К счастью, регистратуры все же иногда о них вспоминают. Месяц назад та же DISH DBS запустила новый домен .mobile. Теперь у неё дошли руки и до .latino.

Как сообщает ресурс Domain Incite, период общедоступной регистрации откроется в этой доменной зоне 12 июня. Ему будет предшествовать период приоритетного доступа для правообладателей (Sunrise), который продлится месяц. Изначально регистратура планировала использовать .latino исключительно как домен-бренд, адресуя его аудитории своих спутниковых телеканалов на испанском языке. Однако затем она полностью пересмотрела планы, и в итоге домен будет открыт для всех желающих. Слово latino используется для обозначения жителей и уроженцев Латинской Америки. Впрочем, в последнее время его употребляют и шире – в отношении людей, говорящих по-испански и проживающих за пределами Испании.

Таким образом, потенциальная аудитория домена выглядит весьма широкой. Насколько домен сумеет эту аудиторию привлечь – покажет время. Пока же стоит иметь в виду, что у .latino есть конкурент – домен .lat, регистрация в котором открылась ещё в августе 2015 года. Его успехи нужно признать достаточно скромными. При цене регистрации менее 2 долларов он за 10 с половиной лет смог набрать всего лишь порядка 125 тысяч регистраций.

Источник: Domain Incite
https://domainincite.com/31601-latino-gtld-to-launch-soon



Интернет изнутри

БЕСПЛАТНЫЙ ЭКЗЕМПЛЯР