### **ДОКЛАДЫ**

# **УСТОЙЧИВЫЙ PNT: КАК ОБНАРУЖИВАТЬ, ЗАЩИЩАТЬ И ПРЕДОТВРАЩАТЬ СБОИ В РАБОТЕ СИГНАЛОВ И ИСТОЧНИКОВ GPS / GNSS / PNT**

## **Обзор текущих и будущих технологий с рекомендациями для критически важной инфраструктуры**

## **Краткое описание**

Последние два десятилетия мы полагались на GPS Global Positioning System - навигационную спутниковую систему. Смотрите также/ GNSS о позиционировании, навигации и хронометражах (PNTМестоположение, навигация и хронометраж: PNT и картографические данные объединяются для создания сервиса GPS.) компания civilian applications добилась ошеломляющего успеха, предоставляя все более точную и надежную информацию PNT повсюду бесплатно. Однако в последние годы появились вредоносные угрозы, обнажившие ахиллесову пяту GPS / GNSS: ее слабая мощность и незашифрованный формат сигнала делают ее уязвимой для помех и подмены. Потеря информации PNT может привести к редким, но катастрофическим событиям, выводящим из строя критически важную инфраструктуру, необходимую для нашего выживания.

К счастью, доступно множество альтернативных технологий для расширения возможностей GPS и предоставления точной и достоверной информации PNT даже в крайне неблагоприятных условиях. К ним относятся:

* Низкая околоземная орбита (LEOLEO - низкая околоземная орбита. LEO относится к орбите, по которой перемещается большинство искусственных спутников. LEO находится ближе к Земле по сравнению с другими спутниковыми группировками, такими как спутниковые системы GPS и GEO. LEO находится примерно в 1200 милях над Землей или меньше, что означает, что спутники на этой орбите движутся с высокой скоростью (например, 15 000 миль в час) и могут облететь Землю менее чем за 2 часа. Большинство полетов человека в космос осуществлялось в рамках LEO.) Спутниковые сигналы PNT – работают близко к Земле, мощность сигнала примерно в 1000 раз выше, чем у GPS, для преодоления помех. И зашифрован для предотвращения подмены.
* Миниатюрные доступные атомные часы для обеспечения внутреннего точного времени – что является основой любой системы позиционирования - без подключения к внешним источникам или зависимости от них, которые могут снизить точность.
* Распределение времени в волоконно-оптической сети с помощью безопасных протоколов высокой точности.

В этом техническом документе мы обсудим эти альтернативные технологии и предложим рекомендации по процедурам и процессам для управления рисками кибератак и предотвращения их, применяя лучшие практики, известные на сегодняшний день. Мы сосредоточимся на устойчивой PNT и опишем стратегии, технологии и процедуры, позволяющие избежать этих рисков кибербезопасности и  
обеспечить непрерывность любой критической операции.

### **Введение**

Подходы к противодействию сбоям в работе сигналов и источников GPS / GNSS / PNT могут отличаться в различных секторах критической инфраструктуры, которые федеральное правительство определило как электросети, инфраструктуру связи и мобильные устройства, все виды транспорта, точное земледелие, прогнозирование погоды и реагирование на чрезвычайные ситуации.

К этому списку следует добавить центры обработки данных. С переходом к повсеместным облачным вычислениям центры обработки данных управляют тысячами серверов по всему миру одновременно, используя одни и те же данные. Эти операции требуют точной синхронизации по времени. Более того, поскольку большая часть данных поступает из мобильных приложений, определение местоположения имеет решающее значение. Центры обработки данных, лежащие в основе большинства облачных вычислений – например, поисковых систем Google, электронной коммерции, служб электронной почты и размещенных приложений, – в значительной степени зависят от PNT.

Центры обработки данных часто объединяют в ”инфраструктуру связи", но у них есть свои уникальные проблемы. Конкретным примером центров обработки данных могут быть финансовые услуги. Фондовым биржам и, в частности, приложениям для высокочастотной торговли требуется точная синхронизация времени на уровне субмикросекунд.

### **Стратегии управления рисками кибербезопасности для PNT**

Наиболее важная стратегия - избегать зависимости от какого-либо одного источника PNT. GPS, как бы хороша она ни была в обеспечении необходимой точности и покрытия PNT, очень уязвима к помехам и подмене.

Однако ни один другой источник PNT не является надежным. У каждого есть свои сильные и слабые стороны. Следовательно, наилучшей стратегией является совместное использование нескольких различных источников PNT – источников с разными режимами сбоя и характеристиками, чтобы уязвимости одного источника компенсировались сильными сторонами другого. Существуют алгоритмы, которые могут разумно выбирать и комбинировать различные источники PNT в составном решении.

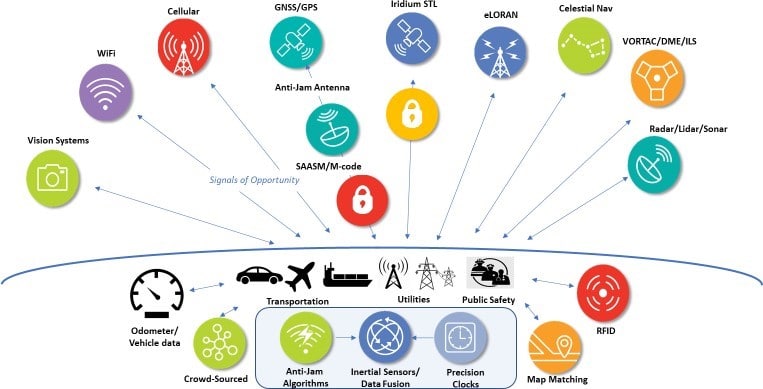


Рисунок 1 – Различные источники PNT для повышения устойчивости критически важной инфраструктуры

На рисунке 1 мы определяем множество доступных источников технологии PNT, а в таблице 1 мы показываем применимость каждого источника к секторам критической инфраструктуры.

Как показано в условных обозначениях, технология либо применима, либо нет. В таблице 1 также указано, не хватает ли применимой технологии точности или охвата – другими словами, ее можно использовать, но крайне желательно повысить точность или охват.

В других случаях технология может быть неприменима, поскольку, например, она обеспечивает определение местоположения только тогда, когда требуется синхронизация, или потому, что точность или охват недостаточны для удовлетворения даже минимальных требований. Эти классификации носят очень общий характер, и всегда есть исключения и особые случаи, но это отправная точка для первичного использования каждой технологии.

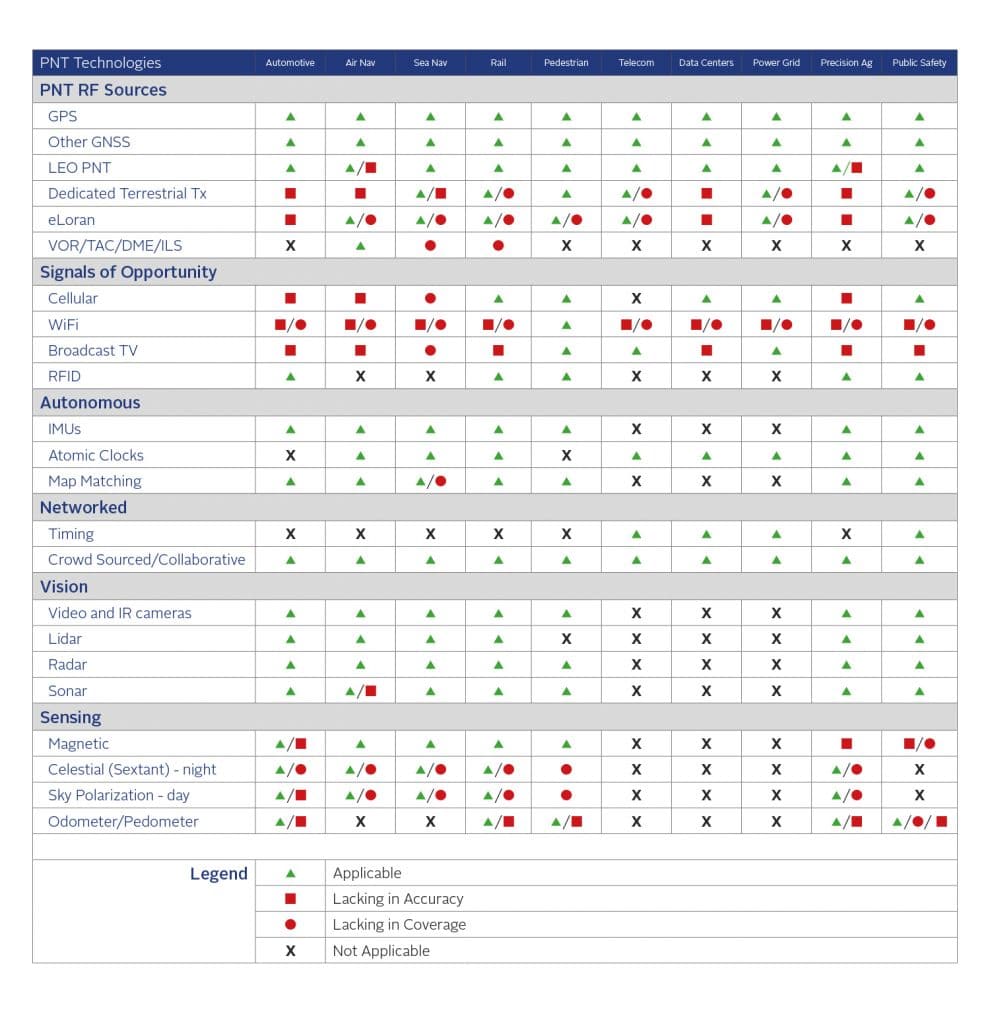


Таблица 1 – Применимость технологий источников PNT к секторам критической инфраструктуры

### **Характеристики технологии**

* Глобальная навигационная спутниковая система (GNSS): общий термин, описывающий любую группировку спутников, которая предоставляет услуги определения местоположения, навигации и хронометража (PNT) на глобальной или региональной основе. Смотрите также**GNSS против GPS –** все системы GNSS (ГЛОНАСС, Galileo, Beidou и GPS) очень похожи по работе и имеют схожие уязвимости и сильные стороны, поэтому использование нескольких созвездий не обеспечивает большого разнообразия. Все они используют одни и те же несколько частотных диапазонов. В общем, если одна система заблокирована, то это происходит со всеми. Однако использование нескольких созвездий приведет к независимой проверке каждой системы. Требуется более сложный подменитель, чтобы подделать все созвездия, но это возможно.

Другим преимуществом использования нескольких созвездий является то, что оно позволяет обнаруживать аномалии в отдельной системе. Например, 13-микросекундный [**сбой GPS в январе 2016 года**](https://www.gpsworld.com/world-dodges-gps-bullet/), [**ошибка в системе ГЛОНАСС в апреле 2014 года**](https://www.bbc.com/news/science-environment-26957569) и [**сбой синхронизации Galileo летом 2019 года**](https://insidegnss.com/lessons-to-be-learned-from-galileo-signal-outage/) - все они были бы обнаружены системами, использующими несколько приемников GNSS с соответствующими алгоритмами перекрестной проверки. С другой стороны, эти другие системы являются совершенно новыми, и способы их отказа пока неизвестны. Кроме того, зависимость от источников за пределами США также создает проблемы национальной безопасности.

* **LEO PNT –** заявленная здесь широкая применимость основана не только на том, что доступно сегодня благодаря STL, передающей с 66 спутников созвездия Iridium, но также включает в себя конечную производительность, ожидаемую, когда сигналы LEO PNT будут доступны на тысячах спутников из других созвездий, таких как OneWeb, Boeing, Space-X и др. Сегодняшние ограничения точности STL обусловлены двумя основными факторами: геометрическим разбавлением, поскольку одновременно видно недостаточное количество спутников, и ограниченной полосой пропускания сигнала. Ни один из этих двух факторов не должен быть проблемой для будущих систем.
* **Специализированные наземные передатчики –** включает технологию, представленную [**NextNav LLC**](https://www.nextnav.com/), [**Locata**](http://www.locata.com/), [**Phasor Lab**](https://www.phasorlab.com/) и другими. Эти системы требуют установки передающей инфраструктуры, поэтому их лучше всего использовать в определенных условиях, таких как городские центры, склады или испытательные полигоны. Зона покрытия зависит от допустимой мощности передатчика.
* **eLoran –** сегодня не существует в США в рабочем режиме, но он применим в ряде секторов, если будет реализовано крупномасштабное внедрение. До появления GPS навигационная система дальнего действия (LORAN) использовалась для прибрежной и речно-морской навигации в США. Несколько десятков станций большой мощности обеспечивали это покрытие до начала 2000-х годов. Благодаря современной технологии цифровой обработки сигналов (DSP) возможны более высокая точность и покрытие. При наличии менее 100 станций должно быть возможным полное покрытие населенных районов США; еще меньше потребуется только для приложений синхронизации.
* **VOR / TAC / DME / ILS –** Всенаправленный диапазон ОВЧ, тактическое управление самолетом, оборудование для измерения расстояния и системы посадки по приборам - все это наземные радиосигналы, генерируемые вблизи аэропортов и вокруг них для руководства полетом. Можно представить, что эти старые системы были адаптированы для других целей, но структуры сигналов были  
  разработаны в начале-середине 20 века для примитивной беспроводной электроники, поэтому можно представить гораздо лучшие подходы. Однако внесение изменений в эти форматы сигналов затруднено из-за огромной установленной базы авионики, совместимость с которой необходимо поддерживать.

**Сигналы возможности** - это радиочастотные сигналы, которые не были предназначены для передачи информации PNT, но с небольшими изменениями или вообще без них могут использоваться для определения местоположения или времени.

* **Сотовая связь** включает сети 4G / LTE и 5G. Определение местоположения с помощью сотовой связи осуществляется уже сегодня с точностью более 100 метров. 5G может обеспечить более высокую точность, чем 4G / LTE,  
  и могут быть рассмотрены дальнейшие усовершенствования, чтобы приблизить точность определения местоположения к GNSS, но на сегодняшний день она менее точная. Здесь не указано, как сотовая связь обеспечивает  
  функцию “Вспомогательной GNSS” - использование сети передачи данных для передачи навигационных сообщений приемникам GNSS быстрее и надежнее, чем прием их непосредственно со спутника.
* **Wi-Fi** не является точным и не обеспечивает достаточного практического покрытия, чтобы его можно было использовать только для пешеходов – обычно для определения местоположения внутри помещений.
* **Broadcast TV** предполагает, что будут внесены улучшения для синхронизации существующих передач, но дальнейшее наращивание, скорее всего, не произойдет в будущем,  
  поскольку полоса пропускания слишком ценна для 5G. Любое конкретное применение этого технологического подхода для PNT связано с описанным ранее случаем высокой мощности сигнала выделенного наземного передатчика.
* **RFID** обеспечивает индикацию местоположения по близости и, следовательно, не используется в приложениях синхронизации.

**Автономные датчики** относятся к автономным устройствам, которые не полагаются на внешние соединения или сигналы и, следовательно, в целом устойчивы к помехам или подмене.

* **IMUs** Инерциальный измерительный блок (или, в сочетании с блоком обработки навигации и устройством точного хронометражирования, называется INSINS или инерциальная навигационная система, иногда используется как синоним IMU) - это устройство, используемое для измерения скорости, положения, направленности и ориентации транспортного средства с помощью акселерометра и гироскопа. – Инерциальная навигационная система), измеряет силы, действующие на объект (транспортное средство) для определения местоположения или изменения ориентации.
* **Атомные часы** становятся все меньше, легче, потребляют меньше энергии и становятся более доступными, что позволяет использовать их сегодня во многих приложениях. Они поддерживают точное время при отсутствии GNSS в течение нескольких часов или даже дней, в зависимости от требований. Мы называем этот интервал отсутствия доступа к GNSS Временем ожидания. Поскольку хронометраж является частью инерциальной навигации, точные часы также помогают в навигации.
* **Сопоставление с картой** используется в сочетании с другими датчиками. Он обеспечивает регистрацию заранее определенных полос движения и может помочь повысить точность. Примерами могут служить автомобили, привязанные к улицам, или воздушное судно, использующее рельеф местности, полученный на основе измерений радара / лидара, сопоставленных с внутренними цифровыми картами, для определения местоположения и курса. По мере того, как память дешевеет, а сетевое подключение становится повсеместным, подробные карты всего мира могут быть доступны по запросу.

**Для сетевых** схем требуется подключение к сети, как проводной, так и беспроводной.

* Точный **хронометраж** может передаваться по сети, и это очень эффективный и безопасный метод синхронизации. Сегодня широко используются [**протокол сетевого времени (NTP)**](https://tools.ietf.org/html/rfc5905) и [**протокол точного времени (PTP)**](https://standards.ieee.org/standard/1588-2019.html). Высокоточная версия PTP Precision Time Protocol - это протокол, используемый для синхронизации часов по всей компьютерной сети. В локальной сети PTP может позволить синхронизировать часы на каждом сервере в диапазоне до микросекунд, что делает его подходящим для требовательных приложений, требующих точной синхронизации по времени и контроля. PTP стандартизирован в соответствии с IEEE-1588v2., в просторечии известный как “Белый кролик” (WR), обеспечивает наилучшее на сегодняшний день распределение времени с точностью до одной наносекунды. Сетевое распределение времени по оптоволокну является идеальным разнообразным дополнением к синхронизации времени на основе GNSS. Вместе они создают точную, надежную синхронизацию времени, гораздо более устойчивую к атакам. Более того, недавно Инженерная группа по Интернету (IETF) приняла[**Стандарт безопасности сетевого времени (NTS),**](https://datatracker.ietf.org/doc/draft-ietf-ntp-using-nts-for-ntp/) чтобы эти протоколы могли быть безопасными. Кроме того, [**Опубликован документ о лучших текущих практиках**](https://www.rfc-editor.org/rfc/rfc8633.html), который выходит за рамки простого соблюдения стандартов и информирует инженеров-проектировщиков систем о том, как наилучшим образом  
  избегать атак.
* **Методы краудсорсинга / совместной работы** основаны на идее, что если другие узлы в сети, к которым вы подключены, знают свое местоположение, и у вас есть некоторые указания на вашу относительную близость к ним, вы можете определить свое собственное местоположение. Индикаторы близости включают уровень радиосигнала в беспроводной сети или задержку передачи пакетов в оба конца в проводной сети. Аналогично в ситуации с синхронизацией времени несколько узлов в сети могут согласованно синхронизироваться друг с другом без необходимости подключения к главному источнику, такому как GPS. Чем больше участников в сети, тем выше вероятность принятия решения по PNT и тем меньше будет эллипс ошибки. Конечно, совместная работа сама по себе не является источником PNT, но в сочетании с различными источниками это мощный метод оценки.

**Системы визуального наблюдения** обеспечивают определение местоположения почти так же, как люди узнают о своем местоположении, – посредством визуальных сигналов к распознанным ориентирам. Однако они не помогают определять время.

* **Изображение с камеры** в сочетании с сопоставлением с картой обеспечивает определение местоположения и ориентации.
* **Лидар** использует лазерный дальномер для создания трехмерной точечной карты окружающей местности.
* **Радар** работает аналогично лидару, но с гораздо меньшим угловым разрешением. Дым / туман / дождь / снег оказывают меньшее влияние, чем оптические методы, а последние достижения в области полупроводников сделали его очень доступным.
* **Гидролокатор** непригоден для высокоскоростных самолетов, но он обеспечивает обнаружение приближения для использования с другими методами.

**Зондирование** похоже на зрение, но обладает этими уникальными характеристиками:

* Измерение **магнитного** поля Земли - не очень точный метод определения курса, но он может обеспечить приблизительное начальное состояние для инерциальной навигации.
* **Астрономическая** навигация - это древняя форма навигации для моряков, которая была автоматизирована с помощью камер и обработки изображений распознавания. Однако звезды видны только ясными ночами или на чрезвычайно больших высотах.
* **Измерениеполяризации неба** использует в своих интересах явление, при котором солнечный свет поляризуется по-разному под разными углами падения на атмосферу. Зная дату и время и приблизительную оценку вашей широты и долготы, вы можете получить точную оценку ориентации на север. В сочетании с астронавигацией это может обеспечивать направление по компасу как днем, так и ночью, хотя и не работает должным образом при любых условиях неба с облачным покровом.

### **Характеристики сектора инфраструктуры**

* **Кавтомобилестроению** предъявляются два основных требования:
  1. Управление автомобилем для автономного вождения. Это вопрос безопасности жизни, и GNSS недостаточно надежна, чтобы быть частью этой функции.
  2. Навигация – знание местоположения автомобиля и направление, куда ему следует ехать. Это касается как случаев с водителем, так и случаев без водителя. Пример: вызов совместного автомобиля.
* **Аэронавигация** имеет свои собственные уникальные приборные системы (см. VOR / TAC выше), но два растущих фактора, вызывающих озабоченность::
  1. ADS-B – автоматическая зависимая система наблюдения и вещания зависит от точных и надежных указаний местоположения, получаемых от GPS. Целостность этих отчетов о местоположении определяет ее безопасную работу. Более того, сам сигнал ADS-B может быть подделан, создавая дополнительный риск.
  2. Беспилотные летательные аппараты – растущее использование беспилотных летательных аппаратов во все большем количестве приложений обуславливает необходимость их интеграции в национальное воздушное пространство. Для достижения этой цели первостепенное значение имеет точная, надежная и высоконадежная PNT.
* **Морская навигация** в значительной степени зависит от GNSS и в последние годы подверглась нескольким атакам с подменой и постановкой помех по всему миру. Отчеты о местоположении GNSS поступают в Систему автоматической идентификации (AIS), которая взаимодействует с другими объектами в этом районе, поэтому неточные отчеты могут вызвать массовую путаницу. Международная  
  морская организация (IMO) изучает новые методы устойчивой навигации.
* **Железной дороге** требуется PNT для надежного управления движением поездов (PTC) для повышения безопасности и эффективности операций.
* На этой диаграмме мы предполагаем, что к **пешеходу** не предъявляются критические требования к точности, надежности или целостности, и он используется преимущественно внутри помещений.
* **Утелекома** было два традиционных применения PNT:
  1. Для беспроводной сотовой сети, как показано на рисунке 2:
  2. Для устаревшей проводной синхронизации сети синхронной иерархии данных (SDH). Это возвращает нас к тому времени, когда линии “T1” были магистралью соединения для сетей передачи данных. Первичные опорные часы (PRC), которые представляли собой атомные часы на основе цезия, обеспечивали основную синхронизацию для всей сети. Сегодня они в основном заменены асинхронными пакетными соединениями (IP / Ethernet), хотя некоторые устаревшие системы все еще существуют. Синхронизация по проводной сети для SDH не должна определять будущие требования к отказоустойчивости

Обратите внимание, что проводную синхронизацию для SDH (приложение) не следует путать с сетевой синхронизацией (технология). Технология по-прежнему очень жизнеспособна, как описано ранее. Просто приложения, которые его используют, эволюционировали. SDH сейчас устарела, и нам не нужно поддерживать точное время для передачи по сети.

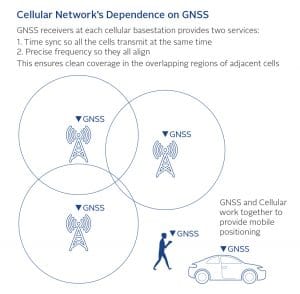


Рисунок 2: Сотовые беспроводные сети и PNT

### **Взаимосвязь сотовой связи и GNSS**

актуальные

1. Синхронизация времени и частоты соседних ячеек
2. Сообщения GNSS – NAV, время суток и общее местоположение, полученные с помощью сотовой сети (Мбит / с) вместо канала GNSS (50 бит / с) для сокращения времени сбора данных GNSS
3. e911/ eCall – сотовая сеть обеспечивает требуемое законом позиционирование на расстоянии ~ 100 м за счет комбинации GNSS и местоположения сектора / времени ariival

* **Центры обработки данных –** Основная потребность в PNT здесь заключается в синхронизации каждого элемента обработки с общей временной привязкой. Это необходимо для того, чтобы каждый элемент знал, какая транзакция произошла первой, какая - второй и т.д. Примерами операторов центров обработки данных являются Google, AWS, Azure и Verizon. В большинстве случаев все, что требуется, - это относительная, а не абсолютная синхронизация с Всемирным координированным временем (UTC). Однако, когда элементы обработки разделены на обширных территориях (например, в разных городах или странах), синхронизация по GPS является самым простым и точным способом достижения этой цели. Точность синхронизации определяет эффективность мультипроцессорной обработки. Чем более неопределенны два обрабатывающих элемента в отношении своих относительных временных привязок, тем больше времени “защиты” или “ожидания” они должны использовать, чтобы согласовать транзакции перед продолжением или снизить вероятность ошибки.

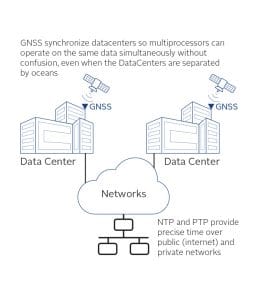


Рисунок 3: Приложение синхронизации Центра обработки данных

Вторичная потребность в PNT связана с мобильными данными. По мере выполнения большего количества транзакций от мобильных пользователей и с появлением Интернета вещей (IoT) транзакции выполняет все больше объектов, которые физически перемещаются. Для осмысленной обработки этих пакетов данных необходимо точно установить географическую временную метку. Качество  
информации, извлеченной в результате интеллектуального анализа “больших данных”, во многом зависит от достоверности метки PNT.

Благодаря 5G увеличивается пропускная способность, что позволяет запускать в облаке больше приложений реального времени. С учетом этой тенденции мониторинг производительности с задержкой и временем становится более важным.

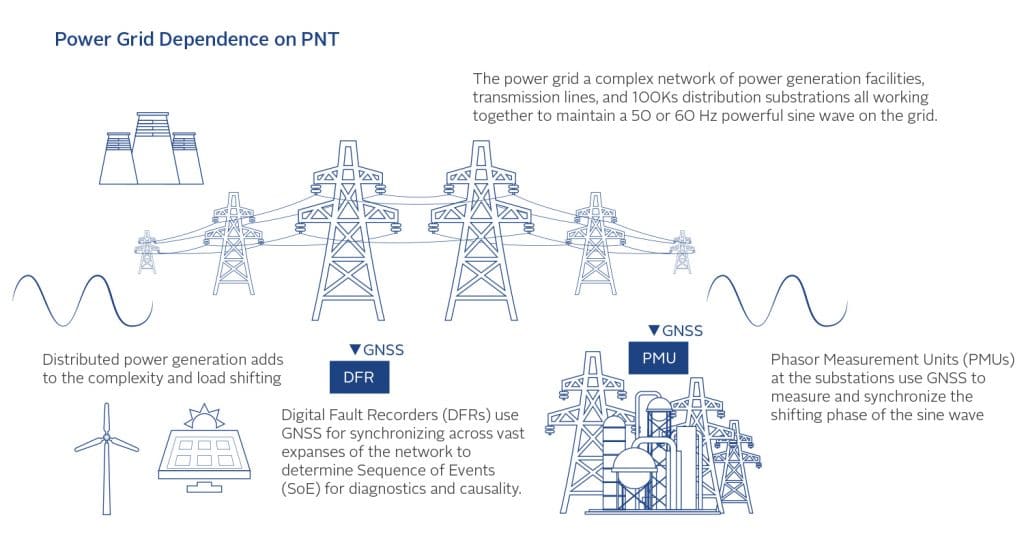
* **Электросеть** зависит от точной синхронизации времени, как показано на рисунке 3. Поддержание фазового соответствия мощности переменного тока частотой 60 Гц в сети является сложной задачей. Основным устройством, поддерживающим этот процесс, является PMU – блок измерения фазы. Он отслеживает синусоидальную волну относительно эталонного времени, обычно GPS, и обеспечивает обратную связь с системами,  
  контролируя выравнивание фаз. Одна степень фазовой погрешности в этой синусоидальной волне 60 Гц составляет 46 микросекунд, поэтому желательна точность измерения в десятки микросекунд, хотя погрешности ~ 100 микросекунд могут допускаться. Другим классом устройств, требующих синхронизации, являются цифровой регистратор неисправностей (DFR) и регистраторы последовательности событий (SER). Для диагностики неисправностей и определения причинно-следственных связей у вас должна быть общая временная привязка, чтобы знать, что произошло первым, что было дальше и т.д. Как и во многих других секторах, энергосистеме требуется только относительное время, а не абсолютное время UTC, но при работе на больших расстояниях время UTC или GPS - это самый простой способ получить доступ к обычным часам. В электроэнергетике наблюдаются две тенденции, которые повлияют на растущую потребность в устойчивой PNT:
  1. 1. Распределенная выработка электроэнергии – по мере перехода от централизованной выработки электроэнергии на угольных, нефтяных, газовых и атомных станциях к возобновляемым источникам энергии, таким как ветер и солнечная энергия, источники энергии становятся более распределенными, более динамичными и менее контролируемыми, чем раньше. Это усложняет алгоритмы управления фазой, требуя большего количества  
     точек измерения и более строгого соблюдения точности и надежности.
  2. 

Рисунок 4: Зависимость электросети от точного времени

**Интеллектуальная сеть** – сеть передачи данных накладывается на сеть, чтобы каждое устройство в сети имело сетевое подключение. Для управления этими миллионами устройств и взаимодействия друг с другом им необходима информация PNT, позволяющая знать, где находятся эти устройства, и для того, чтобы все они имели общую временную привязку.

* **Требования к точному земледелию** аналогичны автомобильным в том, что контролируется положение транспортного средства (трактора, комбайна и т.д.). Однако существуют некоторые уникальные факторы.:
  1. В первую очередь они предназначены для использования в сельской местности, где стационарная инфраструктура обычно недоступна.
  2. Для операций измерения требуется сантиметровая точность – например, расположение почек на фруктовых деревьях, датчики влажности, выравнивание с помощью БПЛАБеспилотный летательный аппарат. Летательный аппарат с дистанционным управлением, обычно называемый дроном. Смотрите также камеры, измерения урожайности с точностью до отдельного растения и т.д.
  3. Они первыми внедряют беспилотные транспортные средства, потому что у них нет сложной проблемы совместного использования  
     “дороги” с людьми-водителями.
  4. Необходим контроль ориентации и измерение (тангажа, крена, рыскания).

В этот сектор мы также включаем строительство и геодезию, поскольку к ним предъявляются схожие требования.

* **Общественная безопасность** охватывает три основных аспекта:  
  1. Точное местоположение и навигация для полицейских, пожарных и медицинских бригад в чрезвычайных ситуациях. Примеры: в  
  горящем или поврежденном землетрясением здании, под землей в туннеле метро, при физической нетрудоспособности из-за травмы.  
  2. Частотная и временная синхронизация выделенных радиосетей первого реагирования (одновременная трансляция).  
  3. Юридически отслеживаемая синхронизация времени для центров обработки вызовов 911, чтобы записи и время отклика могли быть использованы в качестве доказательства в суде.



### **Методы обнаружения сбоев или манипулирования источниками PNT**

После настройки зависимой инфраструктуры с несколькими разнообразными источниками PNT лучшим и простым методом обнаружения является поиск разногласий между источниками. При использовании различных источников каждый из них будет иметь разные точки уязвимости и разные режимы сбоя, так что сбои или атаки будут проявляться в каждом источнике по-разному. Рассмотрим систему синхронизации с тремя различными источниками: приемником GNSS, атомными часами и временем оптоволоконной сети PTP WR. Глушение или подмена сигнала GNSS приведет к несогласию с атомарными часами и временем, производным от PTP; сбой атомных часов будет обнаружен по несогласию с GNSS и временем PTP; взлом сети с помощью атаки типа "Отказ в обслуживании" (DoS) или атаки с задержкой пакетов будет обнаружен GNSS и atomic clock. Единого точечного сбоя не существует.

Аналогично, для примера определения местоположения рассмотрим транспортное средство с приемником GNSS, IMUIMU или инерциальный измерительный блок - это электронное устройство, которое измеряет курс, ориентацию и скорость транспортного средства. Он содержит как акселерометр, так и гироскоп для предоставления необходимых данных для маневрирования самолетом или космическим кораблем, особенно когда сигналы GPS недоступны., и приемник STL. Помехи в приемнике GNSS обычно приводят к разомкнутому контуру слежения, полагающемуся только на IMU, который со временем будет смещаться. Однако с обновлениями  
сигналов STL, которые в 1000 раз сильнее GPS и более устойчивы к помехам, отклонение ошибки неограниченно ограничено десятками метров.

Подмена сигнала GNSS обнаруживается либо из-за несогласия с STL, который представляет собой зашифрованный сигнал, который нельзя подделать, либо с помощью IMU, который не распознает движение в ложном направлении. Отказ любого из этих трех источников отмечается по соглашению двух других. Побеждает большинство.

Для каждого отдельного источника PNT существуют свои собственные меры обнаружения и предотвращения. Например, существует [**множество алгоритмов обнаружения помех и подмены,**](https://safran-navigation-timing.com/products/timing-sync/broadshield-ods) которые могут применяться к приемникам GNSS для предупреждения инфраструктурной системы о возможном перебое. Ложные срабатывания являются проблемой, поэтому использование системы оценки на основе вероятности с программируемыми пороговыми значениями может быть полезным для снижения частоты как ложных срабатываний, так и пропущенных обнаружений.

Простой метод обнаружения подмены GNSS заключается в использовании двух отдельных приемников и антенн, разнесенных на известное расстояние. Например, размещение одной комбинации приемника и антенны на носу судна, а другой - на корме, всегда дает две разные индикации местоположения в нормальных условиях эксплуатации, основанные на их разделении. Если они когда-либо указывают одно и то же местоположение, это указывает на подмену из внешнего источника.

Обнаружение выпадений, разрывов или другого аномального поведения от конкретного датчика - это еще один метод оповещения. В нашей вселенной объект не может “перепрыгнуть” через пространственно-временной континуум; он должен плавно перемещаться из одной точки пространства-времени в другую и не существовать более чем в одной точке в любом отдельном случае. Таким образом, указание на прерывистость – в пределах шума измерений и эффектов квантования –  
является потенциальным сбоем или ложным манипулированием источником. Разрывы, проверка диапазона измерений и мониторинг поведения датчиков могут быть мощными методами обнаружения.

### **Методы восстановления и реагирования – повышение устойчивости систем PNT**

Опять же, при использовании множества различных источников PNT, питающих комплексное решение PNT, обнаружение компрометации или неисправности в любом источнике позволяет отказаться от него. Чем раньше обнаружение, тем быстрее и эффективнее восстановление.

Методы фильтрации по Калману, фильтрации частиц и искусственного интеллекта (ИИ) обеспечивают интеллектуальное объединение нескольких источников PNT в единое решение на основе вероятностных моделей.

Принятие превентивных мер до того, как произойдет атака, иногда может быть лучшим ответом. Эти меры включают:

* **Тестирование на уязвимость** – системы PNT следует анализировать и тестировать до того, как они станут частью критически важной инфраструктуры. Например, Техасский университет в Остине разработал стандартную серию тестов на подмену для приемников GNSS ([**TEXBAT**](https://radionavlab.ae.utexas.edu/index.php?option=com_content&amp;view=article&amp;id=289%3Atexas-spoofing-test-battery-texbat&amp;catid=50&amp;Itemid=27)), [**системы тестирования уязвимости GNSS**](https://safran-navigation-timing.com/products/gnss-simulation) доступны у различных поставщиков, некоторые организации по стандартизации проводят [**сертификационное тестирование**](https://www.navcert.de/en/home/) приемников GNSS, которое требуется, а DHS (Департамент внутренней безопасности) создает [**систему соответствия отказоустойчивости PNT**](https://www.gps.gov/governance/advisory/meetings/2019-11/wong-villee.pdf) для характеристики всех источников PNT и их поведения в условиях кибератака.
* **–** **Защита отдельного источника PNT** Приемники GNSS могут быть защищены от кибератак с помощью “умных антенн”. Они варьируются от дорогих многоэлементных антенн с регулируемой диаграммой направленности излучения (CRPA), которые отслеживают отдельные спутники узкими лучами по мере их перемещения по небу и блокируют помехи, до недорогих  
  антенн защиты от помех, блокирующих горизонт, или простых двухэлементных антенн нулевого наведения, которые ищут и блокируют помехи.
* **Мониторинг и протоколирование событий атак –** ландшафт угроз динамичен, и мы должны адаптироваться с помощью новых стратегий. Создание библиотек угроз по мере их возникновения и распространение их среди сообщества PNT помогает противостоять им.

### **Другие соображения**

В этом разделе мы предлагаем несколько инновационных, “готовых” идей по повышению устойчивости систем PNT:

* **Подумайте о прекращении високосной секунды.** Хотя для этого требуется изменение международного соглашения, NIST (Национальный институт стандартов и технологий), наряду с USNO (Военно-морская обсерватория США) и BIPM (Международное бюро мер и весов – Франция) являются признанными мировыми лидерами в области хронометражирования. Если они проявят инициативу, все последуют их примеру. Неоправданная сложность управления этим представляет угрозу безопасности – каждые несколько лет мы рискуем столкнуться с сбоем. Например, большее количество систем, основанных на атомных часах, могло бы работать автономно от GNSS месяцами (и, следовательно, быть менее уязвимыми), если бы им не приходилось подключаться к GNSS для получения времени UTC так часто, чтобы реагировать на возможные уведомления о скачкообразной секунде. При создании система GPS признала високосные секунды ненужным риском и не использует их внутри компании. Вместо этого GPS просто публикует данные об изменении високосных секунд, чтобы пользователи могли преобразовать время GPS во время UTC. Это управляемо, потому что большинство систем должным образом реагируют на события високосной секунды, но время от времени какая-то система обрабатывает это неправильно. Почему бы не избежать нагрузки на систему, полностью исключив ее?
* **Рассмотрите возможность использования GPS-приемников SAASM** в наших наиболее уязвимых точках критически важной инфраструктуры. Например, разместите подразделение USMC с оборудованием SAASM на бирже NYSE для защиты точного хронометража, управления крипто-ключами и т.д. Федеральное правительство обладает конституционными полномочиями регулировать торговлю между штатами, и это может быть реализовано в этом контексте и без нарушения Закона о патрульных комитатах, если это будет согласовано со штатами. Некоторые примеры: губернаторы Нью-Йорка или Нью-Джерси могли бы запросить федеральное правительство предоставить эту защиту сектору финансовых услуг, если бы им было известно о ее доступности; Содружество Вирджинии могло бы разрешить ее для своего нового центра обработки данных Amazon; и т.д. Более того, по мере того, как вооруженные силы США продвигаются к активации M-кода, более старый сигнал P (Y) имеет меньшую полезность для военного использования, и любое беспокойство по поводу компрометации из-за распространения крипто-ключей в гражданском секторе в конечном итоге уменьшится. Тем временем Orolia запатентовала технологию, которая может преобразовывать аутентифицированный сигнал SAASM в локальную ретрансляцию гражданского сигнала, уменьшая количество необходимых приемников SAASM. В долгосрочной перспективе сигнал P (Y), используемый в SAASM, может стать безопасным зашифрованным гражданским источником после того, как военные полностью перейдут на M-код. В Европе программа Galileo применила этот подход, предоставляя Государственную  
  регулируемую службу (PRS) в качестве безопасного гражданского сигнала для критически важной инфраструктуры.
* **Рассмотрите возможность защиты спектра GNSS с помощью принудительного применения** сегодня доступно оборудование для обнаружения помех и подмены, которое можно разместить в аэропортах и морских портах для обнаружения и локализации злоумышленников, чтобы их можно было задействовать и обезвредить. Однако нам было сложно определить государственное учреждение, которое уполномочено обеспечивать такое наблюдение и преследовать виновных. FAA Федеральное авиационное управление является регулирующим транспортным агентством в Соединенных Штатах, ответственным за регулирование всех аспектов гражданской авиации в США. (Федеральная авиационная ассоциация) обеспечивает безопасность в аэропортах посредством организации воздушного движения, но мониторинг сбоев GPS и отчетность оставлены на усмотрение пилотов. DHS имеет полномочия по защите портов, но нет программы наблюдения за сигналами GNSS в портах. Проблема выходит за рамки простой безопасности и касается поддержания эффективных операций. Обработка контейнеров в портах зависит от GNSS в определении местоположения каждого контейнера для погрузки, разгрузки и обработки. Сбои в работе GNSS могут создать хаос, и уже создали его. Водители грузовиков нередко используют незаконные глушилки GPS “для обеспечения конфиденциальности”, которые при въезде в порт нарушают работу. Кто в правительстве уполномочен решать эту проблему? У [**USCG NAVCEN**](https://www.navcen.uscg.gov/?pageName=gpsUserInput), у [**FAA**](https://www.faa.gov/air_traffic/nas/gps_reports/) и у [**USAF**](https://www.af.mil/) есть веб-сайты для ввода отчетов вручную, но они слишком медленные и громоздкие, чтобы эффективно устранять любые динамические угрозы.
* В дополнение к обеспечению соблюдения, **настройка сети станций мониторинга** может предоставить интеллектуальные данные, необходимые для устранения любых помех GNSS или подмены. Представьте, если бы на каждой вышке сотовой связи были недорогие датчики помех GNSS и они сообщали бы о любых обнаруженных сбоях сигнала обратно в центральную базу данных. Так же, как NOAA, Национальное управление океанических и атмосферных исследований является агентством федерального правительства США, ответственным за формирование политики в отношении использования океана, климата и погоды. NOAA собирает данные о погоде, а также проводит обширные научные исследования, чтобы предоставить гражданам, планировщикам и другим лицам, принимающим решения, достоверную информацию и данные. (Национальная ассоциация океанических и атмосферных исследований) располагает сетью радаров и публикует предупреждения о суровых погодных условиях в режиме реального времени, аналогичная система отчетности “Погода GPS” могла бы предоставлять предупреждения и рекомендации в режиме реального времени. Владельцы инфраструктуры могли бы быстро реагировать на эти сообщения, зная, где и когда возникают проблемы. Также будет создана библиотека угроз, чтобы производители приемников GNSS могли постоянно совершенствовать свои конструкции для противодействия этим угрозам. Это не надуманная концепция. Вышки сотовой связи уже оснащены приемниками GNSS для обеспечения точной синхронизации времени и частоты. По мере установки более устойчивых приемников и антенн уязвимые компоненты могут оставаться, действуя как датчики и передавая оповещения по сети. В Европе [**программа STRIKE3**](https://www.gps.gov/governance/advisory/meetings/2018-05/dumville.pdf) годами отслеживает и каталогизирует события, связанные с помехами GNSS, предоставляя Eurocontrol информацию о сигналах, необходимую для поддержания безопасной аэронавигации. Аналогичная программа в Северной Америке была бы очень ценной.
* **Рассмотрите возможность одобрения NIST зашифрованного времени как услуги (TaaS).** Хотя ни один метод обеспечения PNT не является невосприимчивым к атакам, обеспечение синхронизации времени по оптоволоконной сети общего пользования является разнообразной и безопасной альтернативой GNSS для распределения времени. NIST уже много лет предлагает свой сервис [**интернет-времени**](https://www.nist.gov/news-events/news/2016/03/nists-internet-time-service-serves-world) продолжительностью ~ 1 миллисекунда. Кроме того, NIST предлагает [**специальную услугу калибровки**](https://shop.nist.gov/ccrz__ProductDetails?viewState=DetailView&amp;cartID&amp;portalUser&amp;store&amp;cclcl=en_US&amp;sku=78110S), которая обеспечивает оптоволоконное соединение с NIST, предварительно откалиброванное при установке. Однако для поддержания уверенности требуются повторные кампании по калибровке, поездки на объект клиента с портативным измерительным оборудованием. Вместо этого мы предлагаем, чтобы NIST предоставил некоторую сертификацию или одобрение любых коммерческих организаций, предоставляющих TaaS. Здесь есть две основные альтернативы: публичное или частное предложение. При полностью публичном размещении правительство США будет предлагать TaaS общественности за определенную плату; при полностью частном размещении NIST одобрит стандарты, которым должна соответствовать любая компания, предлагающая TaaS. Более реалистичным подходом могло бы быть государственно-частное партнерство, при котором частные фирмы предоставляли бы оборудование и сетевые операции, а правительство обеспечивало бы национальные объекты инфраструктуры и процессы сертификации для обеспечения качества обслуживания. Частным компаниям, например, может быть непрактично устанавливать несколько атомных часов H-мазера по всей стране и объединять их в сеть, но совместное размещение оборудования сетевого времени на объектах NIST в Боулдере, Колорадо или Гейтерсберге, Мэриленд, или в Военно-морской обсерватории США в Вашингтоне, округ Колумбия, могло бы обеспечить надежную TaaS. Владельцы и операторы критически важных инфраструктур будут уверены, что их время определяется по национальному стандарту времени и передается по безопасной, сертифицированной сети  
  соединений.

## **В заключение**

Сбои в работе сигналов и источников GPS / GNSS / PNT - очень реальная проблема. Слабая мощность GPS / GNSS и его незашифрованный формат сигнала делают его уязвимым для помех и подмены, а потеря информации PNT может привести к катастрофическим событиям, которые могут вывести из строя нашу критически важную инфраструктуру. Однако доступно множество альтернативных технологий для усиления GPS и предоставления точной и достоверной информации PNT даже в неблагоприятных условиях,  
включая спутниковые сигналы LEO PNT, миниатюрные атомные часы и распределение времени по оптоволоконной сети. Принятие превентивных мер до того, как произойдет атака, иногда может быть лучшим ответом. Наилучшей стратегией защиты критически важной инфраструктуры является совместное использование нескольких различных источников PNT. И чем раньше будет обнаружено, тем быстрее и эффективнее будет восстановление.

### [**# ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ**](https://safran-navigation-timing.com/resources/?types=637)

# **ВЫСОКОТОЧНЫЙ ХРОНОМЕТРАЖ ДЛЯ ОБОРОННЫХ ПРИЛОЖЕНИЙ**

## **Проблема, которую мы решаем**

Для успешного выполнения оборонных операций радарам противоракетной обороны и другим распределенным сенсорным системам необходимо обмениваться синхронизированными данными с высокой точностью по времени и частоте. Ориентируясь на точные сигналы времени и частоты, эти системы позволяют надежно выполнять критически важные задачи по обнаружению, где важна каждая наносекунда. Поскольку мультистатические радиолокационные системы и сенсорные системы разделены большими расстояниями, они подвержены потере точной синхронизации данных друг с другом. Это может привести к дрейфу некоторых частей радиолокационных систем и получению ненадежных данных. Существует также проблема прокладки кабелей, поскольку для подключения распределенных систем требуются длинные кабели, что создает проблемы с масштабируемостью.

Одним из решений для отправки точных сигналов времени и частоты по всей системе является использование существующей сети системы. Вместо необходимости установки отдельного коаксиального кабеля, который передавал бы только время и частоту, такие решения, как [**HATI**](https://safran-navigation-timing.com/product/high-accuracy-timing-ip-core-hati/) и [**White Rabbit**](https://safran-navigation-timing.com/solution/white-rabbit-solutions/), могут повторно распределять субнанометры на существующем сетевом оборудовании вашей системы.

## **Почему это важно**

Военная система, которая включает в себя технологии и оборудование для командования, контроля, компьютеры, средства связи, киберзащиту для разведки, наблюдения и рекогносцировки. C5ISR разработан для обеспечения надежной ситуационной осведомленности на поле боя.C5ISR (Командование, контроль, связь, компьютеры, кибернетика, разведка, наблюдение и рекогносцировка) системы – работающие на суше, воздухе или на море – нуждаются в способах генерации надлежащих синхронизирующих сигналов для фазовых антенных решеток. Им также необходимы альтернативные резервные копии для обеспечения работы в случае сбоя или любых других ошибок синхронизации.

[**Поскольку целью систем C5ISR является обнаружение и отслеживание неминуемых угроз в режиме реального времени, правильная временная и частотная синхронизация оборудования становится решающей.**](https://safran-navigation-timing.com/keeping-warfighters-safer-with-resilient-mission-timing-and-synchronization/)

## **Как мы решаем эту проблему**

Если в вашей сенсорной системе уже есть маршрутизаторы и PTPPrecision Time Protocol - это протокол, используемый для синхронизации часов по всей компьютерной сети. В локальной сети PTP может позволить синхронизировать часы на каждом сервере в диапазоне до микросекунд, что делает его подходящим для требовательных приложений, требующих точной синхронизации и контроля. PTP стандартизирован в рамках стандарта IEEE-1588v2. на платах с ПЛИС вы можете просто установить прошивку HATI. Никакого дополнительного оборудования не требуется.

### [HATI](https://safran-navigation-timing.com/product/high-accuracy-timing-ip-core-hati/)

HATI – High Accuracy Timing IP Core - это лицензированное программное обеспечение, обеспечивающее распределение временных и частотных сигналов по стандартным оптоволоконным кабелям. Это означает, что вы можете установить HATI на любую существующую матрицу вентилей с полевым программированием FPGA: интегральную схему, предназначенную для настройки заказчиком или разработчиком после изготовления – отсюда термин "программируемая в полевых условиях". Смотрите также на карте PTP в любом месте вашей сети, и у вас будет решение для распределения высокоточного времени по остальной части системы.

Преимущества HATI:

* Интегрируется с большинством существующих ПЛИС.
* Также может использоваться для передачи стандартных данных, таких как UDP / TCP пакеты, без ущерба для качества сети.
* Распределяет время на расстоянии до 50 миль.
* Обеспечивает точность хронометража до наносекунды.

### [White Rabbit Z-семейство](https://safran-navigation-timing.com/solution/white-rabbit-solutions/)

В качестве альтернативы, если вам требуется специальное оборудование для распределения времени, семейство White Rabbit Z является подходящим решением. Расположенный в верхней части стойки WR-Z16 может распределять стандарт PTP IEEE 1588-2008 для последнего перехода через свои 16-кратные оптоволоконные порты, используя наиболее распространенные профили, такие как телекоммуникационные профили (G.8265.1, G.8275.1) и профили питания (IEEE C37.238-2011). Он также обеспечивает NTPNTP, или протокол сетевого времени, является широко используемым сетевым протоколом, который позволяет компьютерам и устройствам синхронизировать свои системные часы с источником опорного времени. Он обеспечивает точное ведение хронометража в компьютерных сетях, позволяя устройствам получать точную информацию о времени от серверов NTP, которые обычно синхронизированы с высокоточными атомными часами. NTP необходим для различных приложений и служб, которые полагаются на синхронизированное время, таких как сетевая безопасность, аутентификация и регистрация данных. совместимость и распределение 10 МГц / PPS. WR-Z16 реализует протокол White-Rabbit (WR), высокоточное расширение PTP на основе SyncESyncE - синхронный Ethernet - это сетевой протокол, который синхронно отправляет IP-пакеты от одного узла к другому. Это позволяет синхронно отправлять данные и сигналы в IP-сетях. Это решает проблему синхронизации в сетях, потому что без SyncE сети полностью асинхронны и не могут отправлять пакеты предсказуемым образом., что позволяет легко распределять время в субнаносекунды на расстояниях сети метро и за их пределами. Стоит отметить, что на сеть синхронизации, использующую протокол WR, не влияют ни нагрузка на трафик, ни количество переходов.

## **Почему выбрали нас**

* **Простая интеграция** – Вы можете установить HATI на любую существующую плату FPGA или PTP, которая уже есть в вашей сети. Нет необходимости приобретать дополнительное оборудование. HATI интегрируется непосредственно в вашу существующую сеть, обеспечивая высокоточное время и частоту.
* **Универсальность** – совместим с каналами Ethernet емкостью 1 ГБ или 10 ГБ без использования внешнего оборудования.
* **Прочный** – Динамическая компенсация асимметрии, вызванной погодными условиями.
* **Потрясающе точное** разрешение менее наносекунды для синхронизации хронометража, идеально подходящее для критически важных приложений и систем радиолокационной защиты.
* **Надежный** – Может распределять время и частоту на большие расстояния без использования усилителей или калибровки.
* **Отказоустойчивость** – включает механизм аварийного переключения, позволяющий переключать заранее определенные источники синхронизации только при обнаружении сбоя.
* **Интуитивно понятный** веб–интерфейс, разработанный для обеспечения превосходного взаимодействия с пользователем.
* **Расширенное управление** – обширный мониторинг через SNMP, включая комбинацию интеллектуальных оповещений с перехватами. Предоставление шаблонов облегчает интеграцию с инструментами InfluxDB, Graphana и Zabbix. Более того, он позволяет автоматически обнаруживать топологию с помощью LLDP и вести понятный удаленный журнал через rsyslog.

### [**# ТЕМАТИЧЕСКИЕ ИССЛЕДОВАНИЯ**](https://safran-navigation-timing.com/resources/?types=10)

# **ВЫСОКОТОЧНЫЙ ХРОНОМЕТРАЖ ДЛЯ РАДАРА**

### **WHITE RABBIT и IEEE-1588-2019 – Приложения для защиты**

Военная система, которая включает в себя технологии и оборудование для командования, контроля, компьютеры, средства связи, киберзащиту для разведки, наблюдения и рекогносцировки.

C5ISR разработан для обеспечения надежной ситуационной осведомленности на поле боя.C5ISR (Системы командования, контроля, связи, компьютеры, кибернетика, разведка, наблюдение и рекогносцировка) позволяют интегрировать сохраненную информацию и информацию в режиме реального времени для обеспечения точной осведомленности о ситуации на поле боя.

Эта система систем (SoS) будет состоять, среди прочего, из набора датчиков (радаров), вооружения и центров командования и контроля, которые обмениваются синхронизированными своевременными данными по надежным сетям с низкой задержкой.

### **Проблемы пользователей**

* Обеспечивает очень стабильный частотный сигнал с низким фазовым шумом для гетеродинов радара и повышающих/понижающих преобразователей.
* Обеспечивает очень точный сигнал синхронизации с низким дрожанием для запуска события и отметки времени.
* Генерируйте надлежащие синхронизирующие сигналы для излучающих элементов фазовых антенных решеток.
* Максимальная доступность системы и сигналов синхронизации.
* Обеспечивают меры противодействия помехам, глушению и подмене.
* Обеспечение масштабируемости системы.
* Обеспечивают механизмы отработки отказа, кибербезопасность и функции обнаружения ошибок синхронизации.
* Позволяют использовать сетевые настройки и инструменты мониторинга.
* Обеспечивают совместимость с устройствами COTS на основе интерфейсов Ethernet.
* Обеспечивает производительность синхронизации менее чем за ns в глобальных сетях.

### **Контекст**

Системы C5ISR (командование, контроль, связь, компьютеры, кибернетика, разведка, наблюдение и рекогносцировка) позволяют интегрировать хранимую информацию и информацию в режиме реального времени для обеспечения точной осведомленности о ситуации на поле боя и достижения технического превосходства.

Эта система систем (SoS) будет состоять, среди прочего, из набора датчиков (радаров), оружия и центров командования и управления, которые обмениваются синхронизированными данными по надежным сетям с низкой задержкой (рисунок 1).

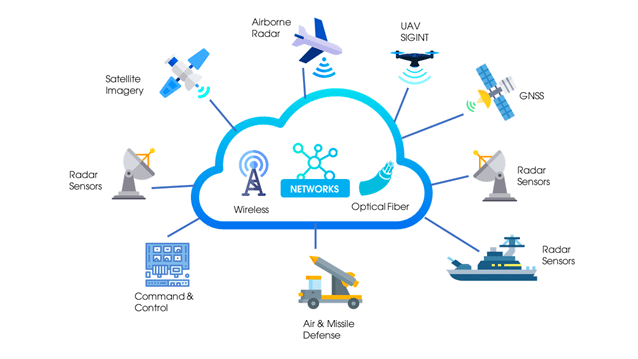


Рисунок 1: C5ISR

Цель этой связи между радарами, оружием и центрами командования и управления - найти противника, зафиксировать его, отследить, вступить в бой и оценить его. Для достижения этого эффективным способом и с максимально возможной производительностью в распределенных системах решающее значение приобретает правильная временная и частотная синхронизация оборудования.

Чтобы понять ключевые моменты этой синхронизации, необходимо разобраться в главном элементе системы - радаре.

Радар в вооруженных силах в основном используется для управления воздушным движением (УВД), наблюдения за воздухом и землей, раннего предупреждения об обнаружении ракет и навигации на море. Как правило, радары подразделяются на наземные, воздушные, космического базирования и военно-морские.

Благодаря развитию технологий (гораздо более эффективные передатчики, фазированные антенные решетки, улучшенные фазово-частотные характеристики и т.д.) Стало возможным развертывать сети и объединять информацию о воздушной обстановке из многих источников (1000 треков одновременно) путем высокоскоростного обмена данными между многими узлами.

Учитывая упрощенную схему, в которой используются передатчик, антенна и приемник (рис. 2), сигнал с высоким уровнем энергии будет передаваться, приниматься и обрабатываться  
после попадания в цель.

Исходя из этого, можно будет определять положение и скорость цели в режиме реального времени путем измерения трех параметров:

1. Временная задержка от момента передачи до момента приема для определения дальности: 3 нс ~ 1 м.
2. Частотный (или доплеровский) сдвиг отраженного сигнала для определения радиальной скорости.
3. Угол наведения антенны слежения (азимут и угол места), который перемещается для максимального увеличения принимаемого от цели сигнала.

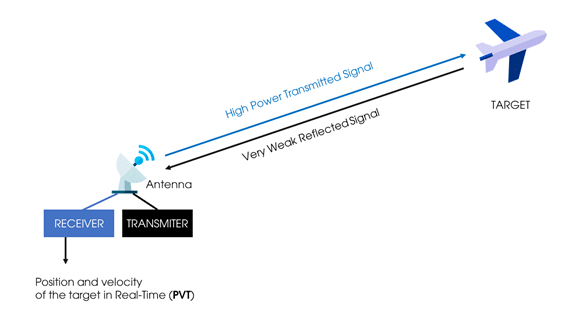


Рисунок 2: Работа радара

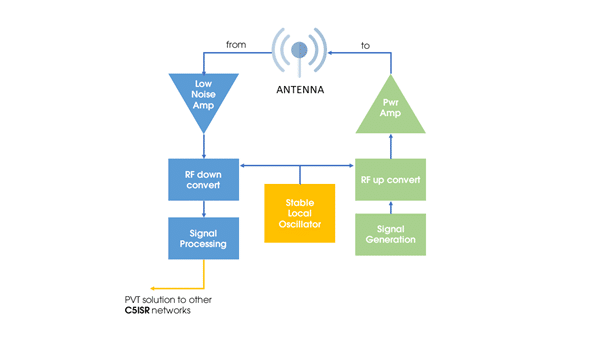


Рисунок 3: Процессы передачи и приема когерентного сигнала

Более детальный обзор этой упрощенной схемы (рис. 3) расширяет возможности передатчика и приемника. После генерации сигнала в передатчике (правая сторона изображения) необходимо преобразовать радиочастотный сигнал с повышением его мощности. Аналогично, в приемнике (левая сторона изображения) необходимо тщательно усилить (с низким уровнем шума) принимаемый слабый сигнал и преобразовать его в основную полосу частот. Оба процесса преобразования управляются гетеродином, частота которого должна быть очень стабильной в краткосрочной перспективе из-за скорости цели и с очень низким фазовым шумом, поскольку он будет смешиваться с передаваемым и принимаемым сигналом при преобразовании вверх и вниз. Чем стабильнее сигнал, тем лучше отраженный сигнал от цели может быть выделен из шума (улучшается дальность обнаружения более мелких и медлительных целей).

В рамках обработки сигнала последовательные данные фиксируются по времени для корреляции сигнала и, в зависимости от типа радара, используются для интерферометрии. Надежность синхронизации по времени в течение длительных периодов времени и очень низкое дрожание в короткие периоды времени необходимы для выполнения этих функций локально и их корреляции между системами.

Для простоты объяснения в качестве примера был использован моностатический радар. Однако реальная проблема возникает, когда система распределена (бистатические и мультистатические радары). Такое распределение является ключевым для систем C5ISR.

В следующем разделе мы опишем, как протокол высокой точности IEEE-1588- 2019 (HA) может быть полезен для этого типа распределенных приложений с очень высокими требованиями ко времени и частоте. Мы также расскажем некоторые подробности о том, как она используется для синхронизации фазированных антенных решеток, все с использованием интерфейсов Ethernet.

### **Решение**

Недавно был выпущен новый стандарт протокола HA IEEE-1588-2019. Эта новая версия включает расширение для использования глобальной сети (WAN), механизмы кибербезопасности, профиль высокой точности (HA) для распределения времени с точностью передачи времени более 1 нс и частоту с очень низким дрожанием и фазовым шумом. Как указано в стандарте, этот профиль в значительной степени основан на протоколе White Rabbit (WR). Были продемонстрированы его масштабируемость и точность на расстояниях в тысячи километров и при нескольких переходах, то, как его точность сохраняется при нескольких переходах, а также возможность интеграции технологии с использованием существующих оптических телекоммуникационных сетей. Кроме того, реализация стандарта IEEE-1588-2019 HA от Orolia обеспечивает отказоустойчивость на основе сети, мониторинг отслеживаемости и совместимость с несколькими временными протоколами.

Упомянутые характеристики технологии White Rabbit (WR) делают ее очень подходящей альтернативой для удовлетворения самых жестких требований с точки зрения распределения времени и частоты, связанных с приложениями для радаров, и, в то же время, обладающей всеми преимуществами использования сетей передачи данных ethernet.

White Rabbit (WR) позволяет распределять частоту по сети для передачи одинаковой тактовой частоты ко всем элементам передатчика и приемника нескольких радаров по сети, обеспечивая очень низкое дрожание и фазовый шум частотных сигналов, так что нет необходимости полагаться только на гетеродины.

В то же время White Rabbit (WR) позволяет передавать время с очень высокой точностью в отдельные распределенные местоположения, где происходит сбор и обработка сигнала, обеспечивая точную информацию о фазе во всех элементах одной и той же радиолокационной системы.

На рисунке 4 показана общая эталонная топология того, как может быть реализована сеть White Rabbit (WR) для предоставления необходимых сигналов времени и частоты распределенным радиолокационным системам, а также распределенным элементам передачи и приема этих систем.

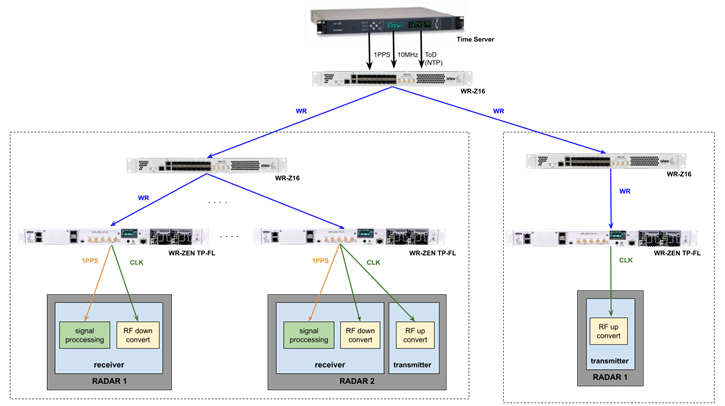


Рисунок 4: Пример топологии сети синхронизации для распределенных радиолокационных систем

Одним из наиболее актуальных применений технологии White Rabbit (WR) для радаров являются системы с фазированной антенной решеткой (рис. 5). В этом сценарии большое количество излучающих элементов взаимосвязано и должно быть синхронизировано с высокой точностью для цифрового программирования частоты и фазы, распределенных в каждой точке.

Использование White Rabbit (WR) по оптоволокну здесь имеет решающее значение для обеспечения требуемой производительности и облегчения интеграции решения синхронизации в существующую инфраструктуру радара. На рисунке 6 показан пример топологии сети синхронизации для частотного и фазового распределения элементов фазированной антенной решетки.

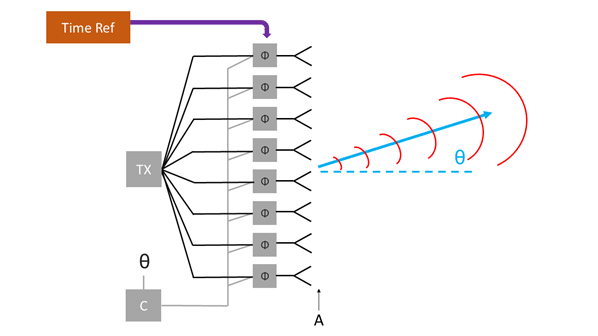


Рисунок 5: Синхронизация фазированной антенной решетки

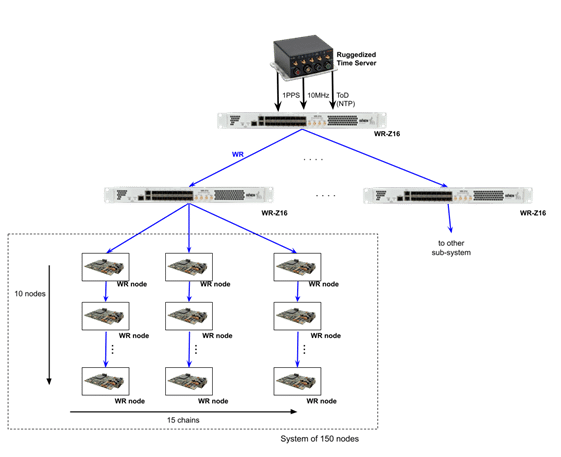


Рисунок 6: Пример топологии сети синхронизации для применения в фазированной антенной решетке

Как видно на этом рисунке, сеть White Rabbit (WR), основанная на двух уровнях устройств WR-Z16, используется для получения внешней ссылки с сервера времени и распределения ее по различным подсистемам сети, которые могут быть распределены по обширной территории.

Каждая подсистема сформирована матрицей узлов на базе White Rabbit, которые могут подавать сигналы частотой 1PPS и 10 МГц на различные элементы фазированной антенной решетки. Эти узлы на базе WR могут быть реализованы различными способами в зависимости от требований интеграции, включая: автономные блоки WR, пользовательские платы WR или HATI (High Accuracy Timing IP): ядро WR IP, которое может быть интегрировано в ПЛИС сторонних производителей для обеспечения совместимости узла с WR.

Следующая таблица иллюстрирует производительность решения на базе White Rabbit в сценариях, включающих большое количество переходов. В этом примере показаны точность по времени и дрожание сигналов 1PPS, которые распределяются от подсистемы White Rabbit в конфигурации последовательной цепочки из десяти узлов, наряду с гистограммой временной ошибки в десятом узле.

| **Узел** | **Точность (ps)** | **Peak2Peak (ps)** | **Дрожание (ps)** |
| --- | --- | --- | --- |
| 1 | 25.5 | 114 | 12.9 |
| 2 | 76 | 156 | 15.7 |
| 3 | 131.5 | 140 | 14.3 |
| 4 | 142.6 | 166 | 19.2 |
| 5 | 183.2 | 217 | 23.3 |
| 6 | 224.8 | 218 | 25.5 |
| 7 | 351.6 | 278 | 33.3 |
| 8 | 359.2 | 376 | 43.1 |
| 9 | 376.8 | 559 | 61.5 |
| 10 | 401.3 | 682 | 82.5 |

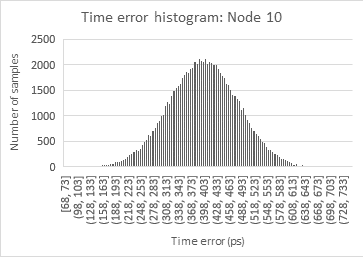


Таблица 1: Пример выполнения передачи времени в конфигурации последовательной передачи для фазированной антенной решетки

Эти результаты показывают точность определения времени ниже 500 пс для десятого узла последовательной цепочки. Дрожание увеличивается с каждым переходом, так же как и ошибка времени от пика к пику, но его дрожание все еще ниже 100 пс для последнего узла цепочки, поэтому стабильность сигнала хорошо сохраняется на всем пути.

Что касается возможности распределения частоты с низким уровнем дрожания, то на следующем рисунке показано сравнение фазовых шумов для всех узлов последовательной цепочки.

Как можно видеть, все узлы системы демонстрируют фазовый шум лучше, чем -90 дБк/Гц при частоте 10 Гц.

Также видно снижение джиттера, вносимого каждым звеном последовательной цепочки, поскольку устройство grandmaster (GM) обеспечивает наилучшую производительность (среднеквадратичное дрожание 1,1 пс, интегрированное с частотой от 1 Гц до 100 кГц) и увеличение джиттера до последнего узла, который обеспечивает наихудшую (3,8 пс).

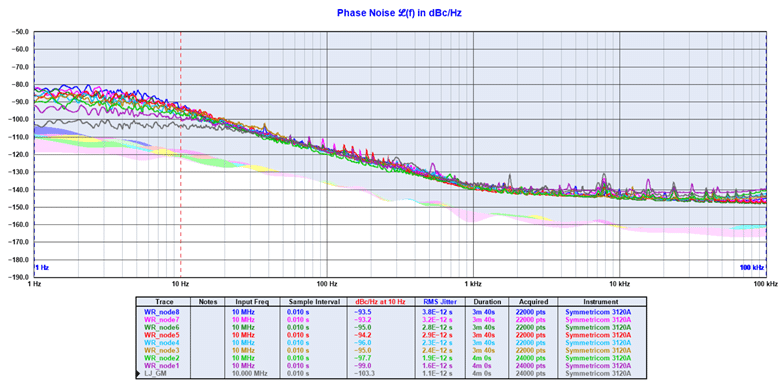


Рисунок 7: Пример выполнения частотного распределения в конфигурации последовательной цепи для фазированной антенной решетки

### **Выводы**

Системы C5ISR по своей сути распределены и, в силу своей природы систем систем, могут анализироваться как сеть датчиков. Одним из важнейших датчиков в сети является радар, и его очень высокие требования к синхронизации по времени и частоте делают новый стандарт высокой точности IEEE-1588-2019, основанный на протоколе White Rabbit, идеальным.

Этот протокол обеспечивает цифровое программирование частоты с низким фазовым шумом в повышающих и понижающих преобразователях, имеющихся в передатчике и приемнике, а также времени с очень низким дрожанием для блоков обработки сигналов, триггеров, временных ограничителей и фазированных антенных решеток.

Наконец, Orolia расширила преимущества своего оборудования за счет таких функций, как механизмы кибербезопасности, отказоустойчивость (алгоритм аварийного переключения, сохранение и т.д.) и мониторинг, что позволит пользователю всегда иметь надежную систему под полным контролем.

### [**# ТЕМАТИЧЕСКИЕ ИССЛЕДОВАНИЯ**](https://safran-navigation-timing.com/resources/?types=10)

# **БЕЛЫЙ КРОЛИК ДЛЯ ФИНАНСОВ**

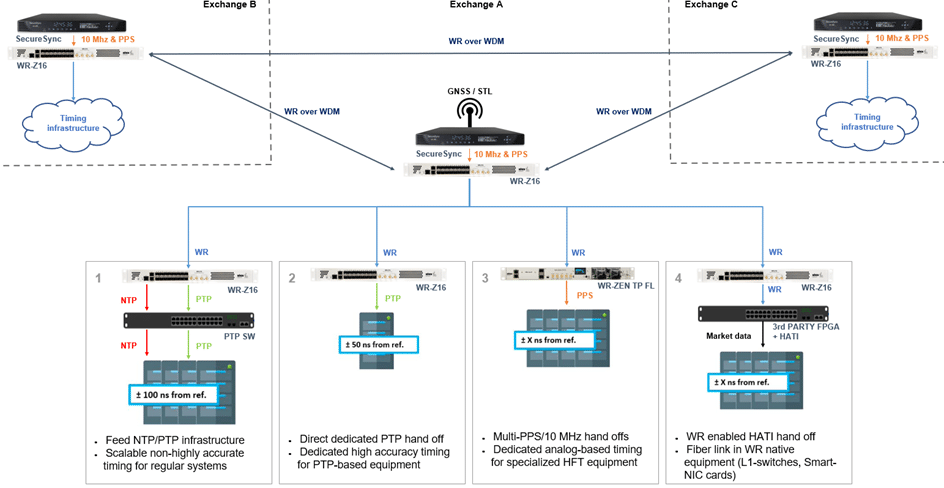
[С ПРИНТАМИ](javascript:window.print()) ПОДЕЛИТЬСЯ ПОЛУЧИТЬ ЦЕНОВОЕ ПРЕДЛОЖЕНИЕ

White Rabbit - это сверхточный протокол точного времени IEEE 1588 (PTP), используемый для синхронизации часов по всей компьютерной сети. В локальной сети PTP может позволить синхронизировать часы на каждом сервере в диапазоне до микросекунд, что делает его подходящим для требовательных приложений, требующих точной синхронизации и контроля. PTP стандартизирован в рамках реализации IEEE-1588v2.), которая обеспечивает точность до наносекунд. Разработанный для использования в авионике, телекоммуникациях, космосе, оборонных и научных объектах, White Rabbit стал золотым стандартом распределения времени в электронных торговых сетях.  
Компания White Rabbit, занимающаяся электронной торговлей в финансовом секторе для повышения точности внутри торговых точек и между ними, использует новейшие технологии для улучшения электронных торговых решений, анализа данных, обратного тестирования и мониторинга задержек в режиме реального времени.  
Операторы обмена также используют White Rabbit для повышения точности в своих сетях сопоставления. White Rabbit предоставляет значительные преимущества, включая лучшую прозрачность для участников биржи, метку времени с высоким разрешением для мониторинга задержек в сети и возможность монетизировать распределение времени и точные данные с метками времени в качестве сервиса для участников рынка.

## **Почему White Rabbit?**

Разработанный для улучшения, дополнения или замены существующей инфраструктуры хронометража, White Rabbit повышает ценность бизнеса, предоставляя:

* Повышение точности между торговыми площадками
* Автоматическое переключение между GNSSГлобальная навигационная спутниковая система (GNSS): общий термин, описывающий любую группировку спутников, которая предоставляет услуги определения местоположения, навигации и синхронизации (PNT) на глобальной или региональной основе. Смотрите также источники на сайтах, расположенных в разных регионах
* Упрощение существующих схем PTP-сетей с повышенной точностью
* Повышена точность карточек с метками времени или переключателей
* Устранены требования к коаксиальным кабелям PPS в инфраструктуре синхронизации
* Сокращение общей инфраструктуры хронометража при использовании сервисов White Rabbit time от бирж или поставщиков услуг



## **Пример использования: Собственная торговая фирма**

Торговая фирма, базирующаяся на собственной компании, внедрила White Rabbit для повышения точности внутренних временных меток с помощью FPGAпрограммируемой в полевых условиях матрицы вентилей: интегральной схемы, предназначенной для настройки заказчиком или разработчиком после изготовления – отсюда и термин "программируемая в полевых условиях". Смотрите также переключатели на основе.

Из-за отсутствия возможностей GNSS во всех точках устойчивость между объектами и источниками времени была ключевым бизнес-требованием. White Rabbit использовался для обеспечения устойчивости между оборудованием синхронизации и географическими местоположениями.

Был развернут многоуровневый сервис, позволяющий использовать PPS там, где требовалась субнаносекундная точность, и улучшенный сервис PTP с точностью ~ 30 нс, доступный менее чувствительным ко времени пользователям и приложениям.

## **Пример использования: Обменный оператор**

Биржа внедрила White Rabbit для повышения точности внутренних временных меток с помощью коммутаторов на базе FPGA.

Временные метки были установлены для всех перекрестных подключений участников в одном месте, всего более 500 портов, 60 устройств и 4 модуля центра обработки данных.

White Rabbit обеспечивает точность на уровне субнаносекунд для всего трафика с отметкой времени, проходящего через инфраструктуру. Это расширяет возможности мониторинга, улучшает сбор исторических данных и предоставляет возможность предоставления дополнительных клиентских услуг, связанных с хронометражем.

Впоследствии эта биржа предложила своим участникам торговли высокоточные услуги на основе файлов временных меток и доступ White Rabbit к совместному местоположению.

### [**# ТЕМАТИЧЕСКИЕ ИССЛЕДОВАНИЯ**](https://safran-navigation-timing.com/resources/?types=10)

# **ТЕХНОЛОГИИ WHITE RABBIT РАСШИРЯТ ВОЗМОЖНОСТИ 5G ДЛЯ МОБИЛЬНОЙ МАГИСТРАЛИ**

[С ПРИНТАМИ](javascript:window.print()) ПОДЕЛИТЬСЯ ПОЛУЧИТЬ ПРЕДЛОЖЕНИЕ

МСЭ определяет три основные области применения расширенных возможностей 5G: расширенная мобильная широкополосная связь (eMBB), сверхнадежная связь с низкой задержкой (URLLC) и массовая машинная связь (mMTC), причем до последних двух в большинстве мест осталось несколько лет, но в то же время они являются драйверами самых передовых приложений 5G. Это предъявляет повышенные требования к синхронизации для мобильных сетей, делая правильную синхронизацию решающим фактором для достижения ожидаемой производительности 5G и обязательным для будущих критически важных задач и приложений с низкой задержкой.

Существует несколько протоколов (в основном, NTPNTP, или протокол сетевого времени, является широко используемым сетевым протоколом, который позволяет компьютерам и устройствам синхронизировать свои системные часы с эталонным источником времени. Это обеспечивает точное ведение хронометража в компьютерных сетях, позволяя устройствам получать точную информацию о времени с серверов NTP, которые обычно синхронизированы с высокоточными атомными часами. NTP необходим для различных приложений и служб, которые полагаются на синхронизированное время, таких как сетевая безопасность, аутентификация и регистрация данных. и PTPPrecision Time Protocol - это протокол, используемый для синхронизации часов по всей компьютерной сети. В локальной сети PTP может позволить синхронизировать часы на каждом сервере в диапазоне до микросекунд, что делает его подходящим для требовательных приложений, требующих точной синхронизации и контроля. PTP стандартизирован в соответствии с IEEE-1588v2.) для выполнения синхронизации мобильной сети, но оба предназначены для работы по сетям передачи данных, и на их точность влияют нагрузка на сеть и количество переходов в топологии. В среднем это хорошие решения для передачи данных по времени, но в худшем случае доставка по времени не может быть гарантирована. Время - это концепция первого порядка, и ее нелегко исправить, а ее ухудшение очень сложно обнаружить и измерить на более поздних этапах развертывания. Мобильные сети необходимо проектировать с учетом этих проблем с самого начала.

По этой причине развертывание выделенной сети синхронизации позволяет полностью контролировать время и то, как оно распределяется по сети, гарантируя правильную работу системы и предлагаемых в ней услуг. Это также может быть ключевым элементом сети visibility network для проверки качества обслуживания сети (QoS) во время работы.

Сеть такого типа будет состоять из трех отдельных уровней: ядра или магистрали, уровня агрегации и уровня доступа, при этом магистраль является наиболее важной частью топологии, поскольку остальная часть сети будет зависеть от ее устойчивости, точности и прецизионности.

### **Решение**

Компания Orolia разработала концепцию магистрали междугородной связи (рисунок 1), опираясь на следующее поколение протокола передачи времени IEEE 1588-2019 и конкретно на профиль высокой точности (HA) (широко известный как протокол White Rabbit). Эта новая версия протокола включает расширение для использования глобальной сети (WAN), механизмы кибербезопасности и профиль высокой точности (HA) для распределения времени и частоты с детерминированной производительностью выше 1 нс и очень низким джиттером.

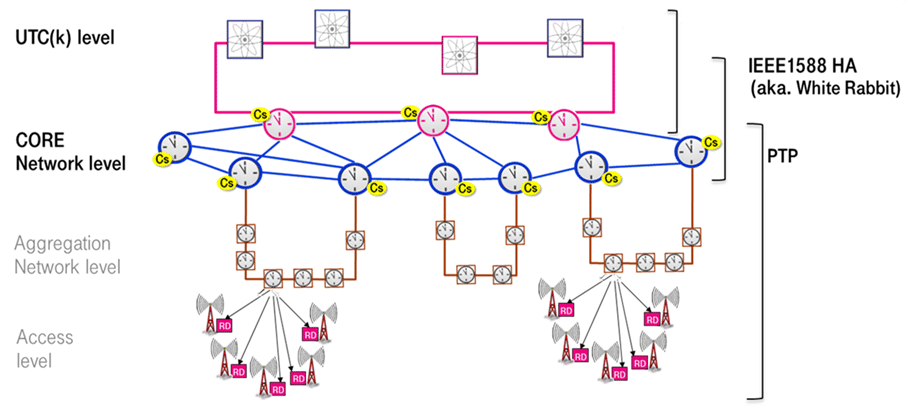


Рисунок 1: Магистраль междугородней связи – Источник: Deutsche Telekom

Решение, основанное на этом новом профиле, использует в качестве основы инфраструктуру распределенной резервной и откалиброванной GNSS Глобальной навигационной спутниковой системы (GNSS): общий термин, описывающий любую группировку спутников, которая предоставляет услуги определения местоположения, навигации и синхронизации (PNT) на глобальной или региональной основе. Смотрите также приемники времени и оптоволоконные линии связи, ссылки на которые разбросаны на сотни километров. Таким образом, система сможет получать и распределять временные привязки, доступные из нескольких (и безопасных) мест, по тем, в которых произошел сбой или возникли помехи GNSS (рисунок 2).

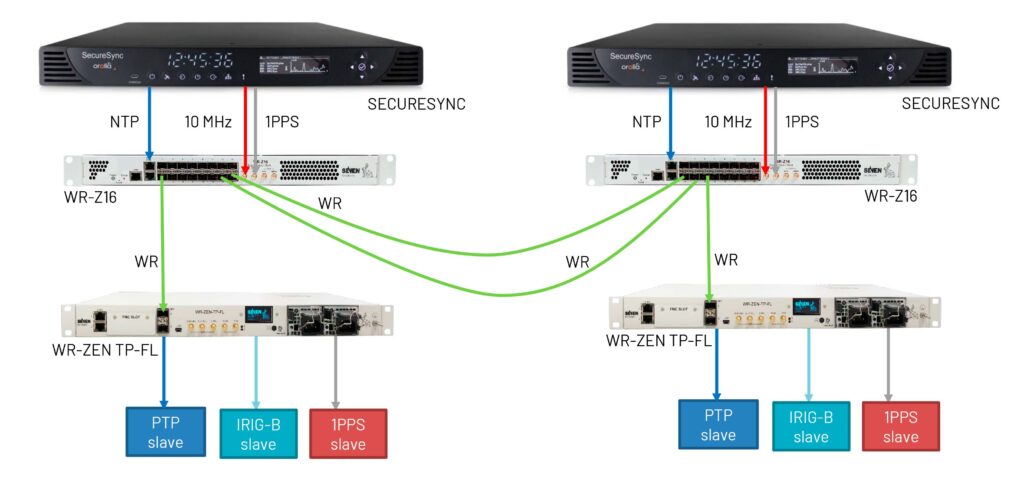


Рисунок 2: пример устойчивой линии GNSS для двух местоположений.

В конфигурации, представленной в этом случае, используются два канала DWDM для соединения обоих местоположений. Это рекомендуется для повышения устойчивости системы и в качестве механизма устранения асимметрии сети (рисунок 3). Могут использоваться любые длины волн, а калибровку можно легко выполнить с помощью параметров протокола или непосредственно с откалиброванных приемников GNSS.

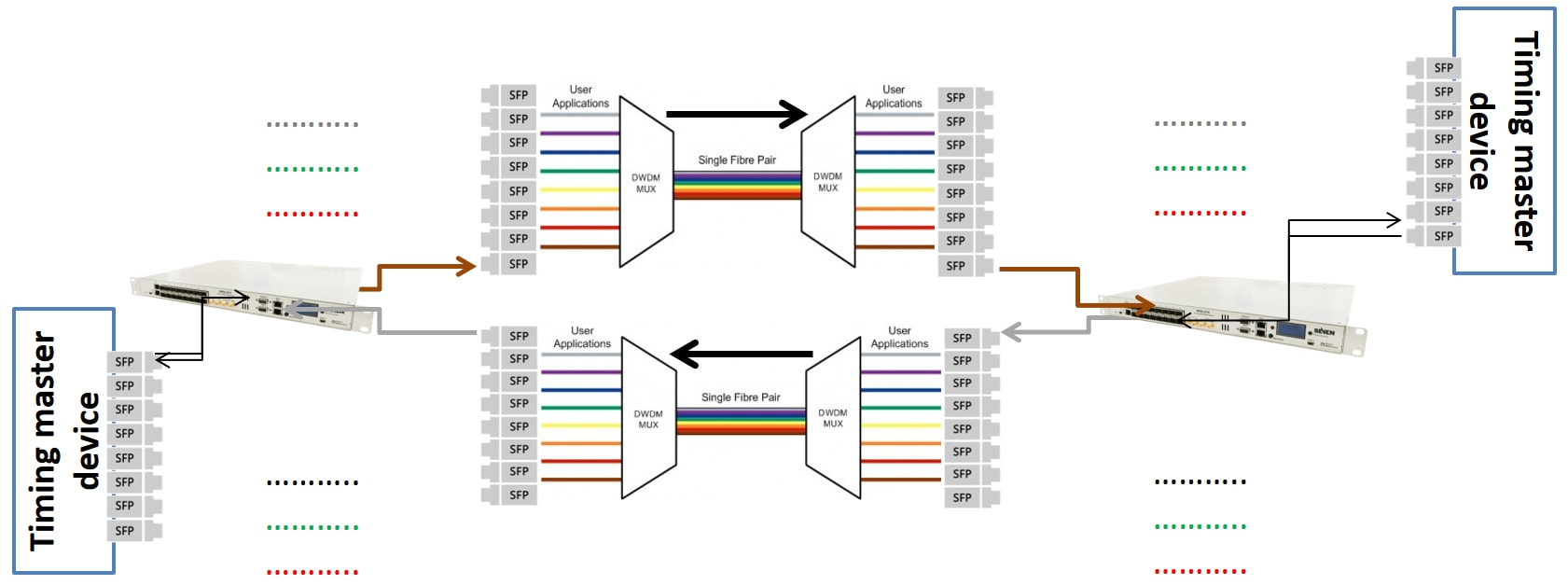


Рисунок 3: DWDM-каналы

Независимо от этого механизма перекрестной защиты, ключом к обеспечению устойчивости и безопасности ядра сети является защита каждого узла в магистрали сети. Эти технологии, как видно на рисунке 2, реализованы с использованием Orolia SecureSync GrandMaster и распределительного узла WR Z16 White Rabbit. Оба устройства отличаются своими механизмами безопасности, и среди них стоит выделить следующие функции:

### **О WR Z16**

* Алгоритм синхронизации при отказе (FOCA), который автоматически переключается с одного источника синхронизации на другой в случае обнаружения сбоя в активном источнике синхронизации.
* Задержка, которая допускает максимальный временной сдвиг в 1,5 мкс через 24 часа.
* Возможности опроса нескольких источников времени для перекрестной проверки привязки к времени.
* Улучшенный API для интеграции с журналами, метриками, конфигурацией и оповещениями со сторонними инструментами, включая не только SNMPv2 / v3, но и поддержку Elasticsearch, Logstash, Kibana, Telegraf, InfluxDB, Zabbix, Grafana и многих других широко используемых библиотек и инструментов.
* Функции безопасности, включая новейшую аутентификацию IEEE 1588-2019 и функции защиты от кибератак, позволяют развертывать гибкие политики безопасности в соответствии с уровнем безопасности, требуемым для инфраструктуры.

### **О SecureSync**

* Определение опорных приоритетов и аварийный переход, который автоматически переключается с одного источника синхронизации на другой в порядке приоритета в случае обнаружения сбоя в активном источнике синхронизации.
* Опции сохранения, которые допускают максимальный временной сдвиг в 1 мкс через 24 часа.
* Улучшенный API для интеграции с журналами, метриками, конфигурацией и оповещениями со сторонними инструментами, включая не только SNMPv2 / v3, но и полнофункциональный REST API.
* Функции безопасности, включая списки контроля доступа, настраиваемые политики паролей и централизованную аутентификацию через LDAP, RADIUS и TACACS +.
* Обнаружение и смягчение помех ГНСС с помощью вышестоящих элементов, таких как антенные системы защиты от помех, и программных элементов, таких как IDM Suite от Orolia с BroadShield, для защиты и обнаружения помех в сигнале ГНСС.

В качестве дополнительного преимущества продукты Orolia поддерживают широкий спектр вариантов взаимодействия с различными интерфейсами и протоколами синхронизации (PTPv2, NTP, PPS / 10 МГц, IRIG и др.). Эти опции расширяют возможности сети за счет обеспечения протоколов взаимодействия ниже по потоку от магистрали до более низкого уровня сети.

### **Оптимизация магистрали**

Ядро сети опирается на технологически продвинутое оборудование синхронизации, такое как устойчивые серверы времени GNSS, атомные часы или их сочетание (часы ePRTC) для обеспечения точности, прецизионности, стабильности, а также надежности и отказоустойчивости сети.

Однако, поскольку некоторые из этих устройств (атомные часы, ePRTC и т.д.) Имеют высокую стоимость, учитывая компромисс, который существует между этой стоимостью и производительностью сети, оптимизация магистрали становится ключевым фактором для развертывания, как видно из следующего примера (рисунок 4).

.

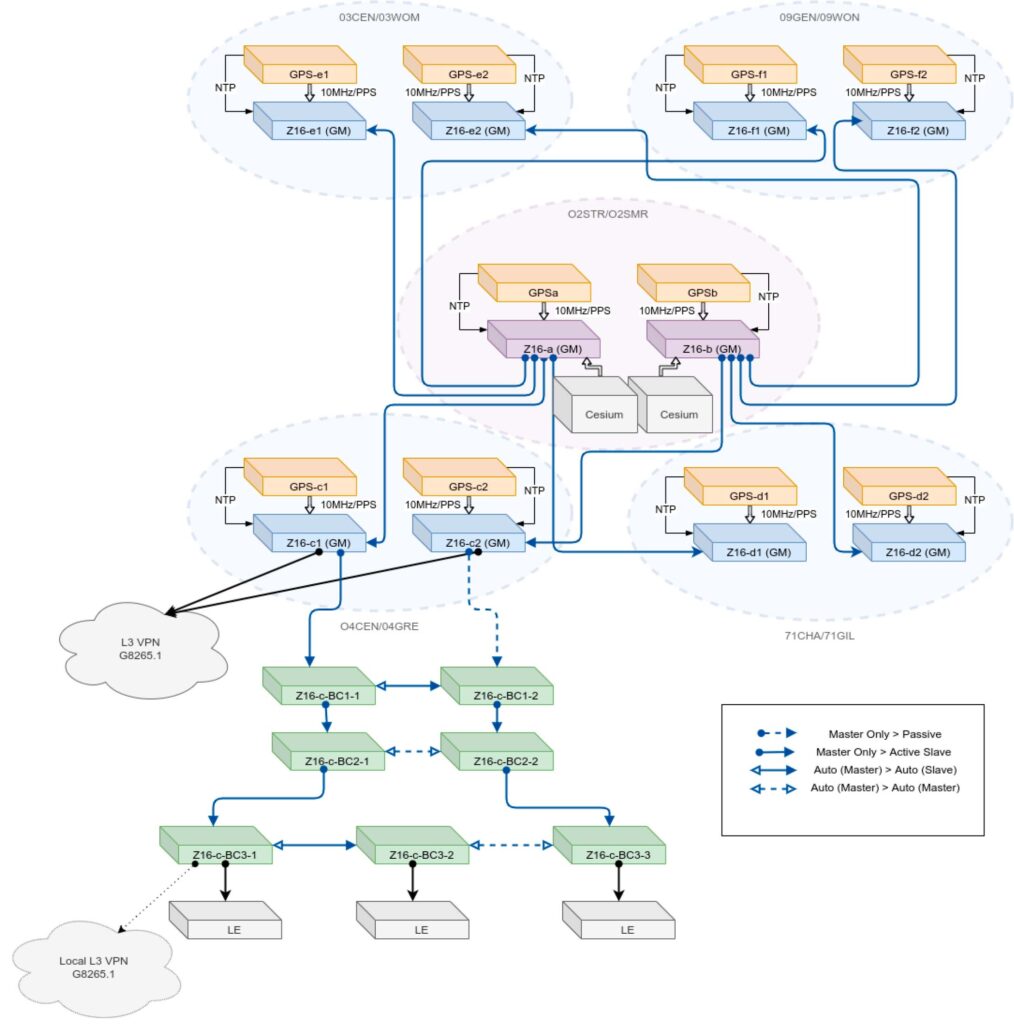


Рисунок 4: Сценарии подключения узлов

Резервный центральный узел (узел A), состоящий из устойчивых серверов времени GNSS (SecureSync) производства Orolia, атомных часов cesium и устройств распределения времени (WR-Z16). С этого сайта остальные сайты в топологии могут быть синхронизированы следующим образом:

Сайты C, D и E имеют свои собственные серверы времени GNSS и устройства распределения времени, но также получают резервную синхронизацию с сайта A, чтобы воспользоваться преимуществами имеющихся там серверов времени GNSS и часов cesium.

Сайт F показан в качестве примера сайта с особыми условиями, которые не позволяют использовать локальные серверы времени GNSS. Местоположение сайта может не обеспечивать хорошего приема GNSS, как в условиях городского каньона. Установка антенны GNSS может быть затруднена по логистическим причинам. Это могут быть просто бюджетные ограничения, ограничивающие тип разрешенного оборудования. Независимо от причины, развертывание по-прежнему поддерживает синхронизацию, включая отказоустойчивость, на площадке F благодаря каналам синхронизации с площадки A, а также находящимся там серверам времени GNSS и часам cesium.

Окончательное развертывание магистрали с использованием этих примеров конфигурации сайта может сбалансировать затраты со всеми требованиями к точности, прецизионности, стабильности, надежности и отказоустойчивости, которые могут потребоваться заказчику в магистральной сети.

### **Наглядность**

Наконец, Orolia разработала специальные шаблоны, которые облегчают интеграцию их устройств через SNMP с наиболее используемыми внешними инструментами мониторинга и управления сетями, такими как Zabbix (рисунок 5), InfluxDB, Grafana, Chronograf и др. Это решение упрощает контроль за большим количеством устройств синхронизации времени очень наглядным и простым в использовании способом.

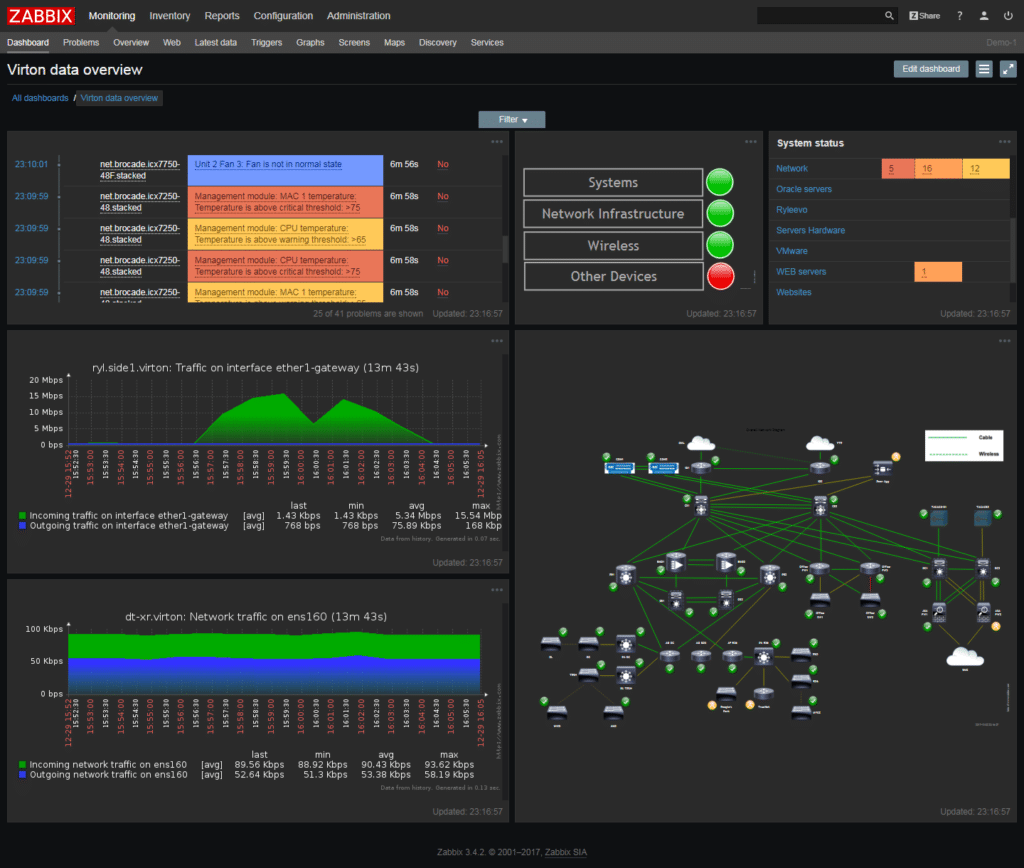


Рисунок 5: Zabbix

# **ВЕДУЩИЙ ЦЕНТР ОБРАБОТКИ ДАННЫХ ВЫБИРАЕТ SECURESYNC ДЛЯ ГЛОБАЛЬНОЙ СИНХРОНИЗАЦИИ**

### **Справочная информация**

Этот заказчик, ведущий корпоративный центр обработки данных и поставщик услуг коллокации для ряда крупнейших компаний мира, находится в процессе внедрения глобальной синхронизации для своих центров обработки данных, чтобы предоставить своим клиентам высокоточное время как услугу (TaaS). Они пришли в Safran в поисках платформы синхронизации, оснащенной протоколом точного времени (PTPPrecision Time Protocol - это протокол, используемый для синхронизации часов по всей компьютерной сети. В локальной сети PTP может позволить синхронизировать часы на каждом сервере с точностью до микросекунд, что делает его подходящим для требовательных приложений, требующих точной синхронизации и контроля. PTP стандартизирован в соответствии с требованиями стандарта IEEE-1588v2.) и выходами 1PPS для обеспечения точной и стабильной синхронизации времени для своих финансовых заказчиков и заказчиков больших данных.

### **Решение**

Компания предпочла SecureSync® от Safran конкурентам, потому что SecureSync была хорошо известна своей надежностью, она проходила тщательную проверку на протяжении многих лет и потому что Safran имела репутацию поставщика отличного сервиса по разумной цене.

Компания приобрела несколько устройств в октябре 2020 года и планирует добавить дополнительные устройства при развертывании весной 2021 года. Они смогут воспользоваться преимуществами нового встроенного средства SecureSync для обнаружения помех, которое теперь входит в стоимость без дополнительной оплаты.

Гибкость SecureSync позволяет клиентам этой компании выбирать между PTP и протоколом сетевого времени (NTPNTP, или Network Time Protocol, является широко используемым сетевым протоколом, который позволяет компьютерам и устройствам синхронизировать свои системные часы с эталонным источником времени. Он обеспечивает точное ведение хронометража в компьютерных сетях, позволяя устройствам получать точную информацию о времени от серверов NTP, которые обычно синхронизированы с высокоточными атомными часами. NTP необходим для различных приложений и служб, которые полагаются на синхронизированное время, таких как сетевая безопасность, аутентификация и протоколирование данных.), обеспечивает автоматическую подготовку серверов и использует их центр технической документации для различных методов каскадирования времени.

### **Результат**

SecureSync от Safran теперь предоставляет компании новый источник дохода. Первый этап их внедрения был распространен на центры обработки данных в Азиатско-Тихоокеанском регионе, Германии и Англии. Второй этап, который начнется в 2021 году, охватит части США, Австралии, Сингапура и Бразилии.

# **ВАЖНОСТЬ ТОЧНОГО ХРОНОМЕТРАЖА И СИНХРОНИЗАЦИИ В ТОРГОВЫХ СИСТЕМАХ**

## **Аннотация**

В этом техническом документе рассматриваются технические аспекты синхронизации времени в финансовых торговых системах. В нем исследуется важность точного учета времени, проблемы, с которыми приходится сталкиваться при достижении точной синхронизации, и последствия сбоев во времени и синхронизации. В документе также обсуждаются потенциальные решения и лучшие практики для обеспечения надежной синхронизации времени в контексте финансовой торговли.

## **Введение**

* Обзор важности точного хронометража и синхронизации в торговых системах.

## **Проблемы с синхронизацией времени**

* Обсуждение распространенных препятствий, с которыми приходится сталкиваться, включая задержку в сети, смещение часов, детализацию временных меток и сложности распределенных систем.
* Изучение влияния этих проблем на производительность и надежность торговли.

## **Последствия сбоев времени и синхронизации**

* Изучение последствий сбоев во времени и синхронизации, таких как проблемы с исполнением ордеров, неточности данных, проблемы с соблюдением нормативных требований, сбои в алгоритмической торговле, фрагментация рынка, операционные риски, потеря доверия инвесторов, нарушение управления рисками и сбои в высокочастотной торговле.

## **Рекомендации по синхронизации времени**

* Презентация набора лучших практик для достижения надежной синхронизации времени в финансовых торговых системах.
* Освещение таких тем, как источники точного времени, протоколы точного времени, алгоритмы синхронизации часов, оптимизация сети и методы мониторинга.
* Особое внимание уделяется резервированию, отказоустойчивости и механизмам отработки отказа для непрерывной синхронизации времени.

## **Технологии синхронизации времени**

* Изучение широко используемых технологий синхронизации времени, включая протокол сетевого времени (NTP). NTP, или Протокол сетевого времени, является широко используемым сетевым протоколом, который позволяет компьютерам и устройствам синхронизировать свои системные часы с эталонным источником времени. Он обеспечивает точное хронометражирование в компьютерных сетях, позволяя устройствам получать точную информацию о времени с серверов NTP, которые обычно синхронизированы с высокоточными атомными часами. NTP важен для различных приложений и служб, которые полагаются на синхронизированное время, таких как сетевая безопасность, аутентификация и регистрация данных.), протокол точного времени (PTPПротокол точного времени - это протокол, используемый для синхронизации часов по всей компьютерной сети. В локальной сети PTP может позволить синхронизировать часы на каждом сервере с точностью до микросекунд, что делает его подходящим для требовательных приложений, требующих точного хронометража и контроля. PTP стандартизирован в рамках стандарта IEEE-1588v2.), источников времени на основе GPS, атомных часов и [**новых технологий, таких как White Rabbit и IEEE 1588v2**](https://safran-navigation-timing.com/product/white-rabbit-z16).
* Оценка каждой технологии с точки зрения точности, масштабируемости, сложности и применимости к различным архитектурам торговых систем.

## **Мониторинг и диагностика**

* Изучение методов мониторинга, таких как измерение смещения часов, измерение задержки, оценка качества синхронизации и протоколирование событий.
* Обсуждение использования аналитики и машинного обучения для обнаружения аномалий и упреждающего управления синхронизацией времени.

## **Избыточность и устойчивость**

* Подчеркивается важность резервных источников времени, разнообразных сетевых путей, резервных ссылок на часы и стратегий резервного копирования синхронизации для снижения рисков сбоев времени и синхронизации.
* Особое внимание уделяется механизмам аварийного переключения и постоянному мониторингу для бесперебойной синхронизации времени.

## **Соображения по соблюдению нормативных требований**

* Обзор соответствующих нормативных актов, таких как MiFID II и CAT, и их требований к точным меткам времени, отчетности о сделках, журналам аудита и ведению учета.
* Особое внимание уделяется важности синхронизированного времени для расследований регулирующих органов и реконструкции последовательности событий.

## **Будущие тенденции и инновации**

* Перспективы внедрения блокчейна для определения времени, интеграция квантовых технологий и потенциальное влияние сетей 5G и периферийных вычислений на синхронизацию времени.

## **Заключение**

* Краткое изложение ключевых моментов, обсуждаемых в белой книге, и важности точной синхронизации времени в финансовых торговых системах.
* Признание проблем, передовой практики, технологий, мониторинг и соображения соответствия нормативным требованиям.
* Освещаем будущие тенденции и инновации, которые, как ожидается, сформируют область синхронизации времени в торговых системах.

## **1. Введение**

В быстро меняющемся и высококонкурентном мире [**финансового трейдинга**](https://safran-navigation-timing.com/solution/finance/) способность добиться точной синхронизации времени становится все более важной. Эффективное исполнение ордеров, точный анализ рыночных данных, соблюдение нормативных требований и эффективное управление рисками - все это в значительной степени зависит от синхронизированного хронометража. В этом разделе мы углубимся в важность точного хронометража и синхронизации в торговых системах, выделив причины, по которым они необходимы для успешных операций на финансовых рынках.

Точное хронометражирование имеет фундаментальное значение для обеспечения надлежащей последовательности и координации торговой деятельности. На финансовых рынках, где транзакции совершаются в течение миллисекунд и даже микросекунд, даже малейшие расхождения во времени могут иметь серьезные последствия. Задержка исполнения ордеров на несколько микросекунд может привести к упущенным возможностям или неоптимальным результатам торговли, что потенциально может привести к финансовым потерям. Таким образом, точная синхронизация времени необходима для поддержания равных условий игры и обеспечения честной и эффективной торговли для всех участников.

Более того, точная синхронизация времени играет жизненно важную роль в анализе рыночных данных. Трейдеры и аналитики в значительной степени полагаются на исторические рыночные данные и данные в режиме реального времени для принятия обоснованных решений. Синхронизируя временные метки в различных торговых системах и источниках данных, участники рынка могут точно анализировать и сравнивать данные с различных платформ, бирж и участников рынка. Эта синхронизация обеспечивает всесторонний анализ данных, облегчает идентификацию торговых моделей и поддерживает разработку сложных торговых стратегий.

Соблюдение нормативных требований - еще одна область, где точное отслеживание времени и синхронизация имеют первостепенное значение. Финансовые регуляторы, такие как комиссии по ценным бумагам и биржи, предъявляют строгие требования к отметкам времени для обеспечения прозрачности, справедливости и подотчетности на рынках. Участники рынка должны придерживаться этих правил, точно отмечая время своих ордеров, транзакций и других действий. Несоблюдение предписанных стандартов синхронизации может привести к штрафам регулирующих органов, ущербу репутации и даже юридическим последствиям. Таким образом, надежная синхронизация времени становится важным компонентом поддержания соответствия нормативной базе.

Более того, точная синхронизация времени имеет решающее значение для эффективного управления рисками в финансовой торговле. Своевременная и точная синхронизация позволяет системам управления рисками точно отслеживать последовательность событий, обнаруживать аномалии или нарушения и оперативно принимать меры по снижению рисков. Будь то мониторинг высокочастотных торговых алгоритмов, управление подверженностью волатильным рыночным условиям или внедрение механизмов аварийного переключения в случае сбоев системы, синхронизированный хронометраж служит основой для надежных методов управления рисками.

В свете важности точного хронометража и синхронизации в финансовой торговле крайне важно решать проблемы, возникающие при достижении точной синхронизации. Такие факторы, как задержка в сети, смещение часов и ограничения точности временных меток, могут создавать препятствия для достижения последовательной и надежной синхронизации времени в различных торговых системах. В последующих разделах этого документа мы рассмотрим эти проблемы более подробно и обсудим потенциальные решения и лучшие практики для обеспечения надежной синхронизации времени в контексте финансовой торговли.

## **2. Проблемы с синхронизацией времени**

В сфере финансовых торговых систем возникает несколько проблем, когда дело доходит до достижения точной синхронизации времени. Одной из основных проблем является задержка в сети. В распределенной торговой среде, где торговые системы распределены по нескольким местоположениям и соединены через сети, время, необходимое для передачи данных из одной системы в другую, может приводить к задержкам. Задержка в сети может варьироваться в зависимости от таких факторов, как географическое расстояние, загруженность сети и эффективность сетевой инфраструктуры. Эти задержки могут существенно повлиять на точность синхронизации, поскольку время, в которое происходит событие в одной системе, может отличаться от времени его получения в другой системе из-за задержки в сети.

Смещение часов - еще одна серьезная проблема синхронизации времени. Часы в разных системах имеют тенденцию отклоняться от идеального времени из-за различий в их аппаратных компонентах, колебаний температуры и других факторов. Смещение часов относится к постепенному расхождению, возникающему по мере того, как часы со временем становятся менее точными. Если не обращать внимания на смещение часов, это может привести к существенной разнице во времени между торговыми системами, что затруднит синхронизацию. Важно использовать механизмы, которые постоянно отслеживают и настраивают часы, чтобы смягчить последствия смещения часов и поддерживать точную синхронизацию времени.

Детализация временных меток также является проблемой для достижения точной синхронизации времени. Торговые системы часто полагаются на временные метки для регистрации наступления событий, таких как подача ордеров, исполнение сделок и обновление данных. Однако степень детализации временных меток может варьироваться в разных системах и компонентах, варьируясь от миллисекунд до микросекунд или даже наносекунд. Когда разные системы используют временные метки с разной степенью детализации, становится сложной задачей точное выравнивание и сравнение событий. Непоследовательная детализация временных меток может привести к расхождениям в расчетах времени и затруднить усилия по синхронизации.

Сложности распределенных торговых систем создают дополнительные проблемы для синхронизации времени. В распределенной архитектуре множество компонентов и подсистем работают вместе, облегчая торговую деятельность. Каждый компонент может иметь свои собственные внутренние часы и работать независимо, что затрудняет достижение единого и синхронизированного времени во всей системе. Координация и согласование часов в распределенных системах требуют тщательной разработки, внедрения протоколов синхронизации и надежных механизмов связи.

Эти проблемы с синхронизацией времени оказывают значительное влияние на производительность и надежность торговли. Неточная синхронизация может привести к неправильному порядку или пропущенным сделкам, неправильному анализу данных и нарушениям в соблюдении нормативных требований. Это также может подорвать стратегии управления рисками, поскольку ставится под угрозу своевременный и точный мониторинг событий. Более того, проблемы с синхронизацией могут нарушить общую стабильность и отказоустойчивость торговых систем, что приведет к операционной неэффективности, системным сбоям и финансовым потерям.

В последующих разделах этого документа мы углубимся в каждую из этих проблем, обсудив их глубинные причины, потенциальные последствия и эффективные стратегии смягчения последствий. Решая эти проблемы, финансовые торговые системы могут расширить свои возможности синхронизации времени и обеспечить надежную и эффективную работу в динамичной и конкурентной торговой среде.

## **3. Последствия сбоев времени и синхронизации**

Сбои во времени и синхронизации в торговых системах могут иметь серьезные последствия для различных аспектов финансовой торговли. Эти сбои могут нарушить исполнение ордеров, поставить под угрозу точность данных, создать проблемы с соблюдением нормативных требований, нарушить алгоритмические торговые стратегии, способствовать фрагментации рынка, увеличить операционные риски, подорвать доверие инвесторов, скомпрометировать методы управления рисками и нарушить высокочастотную торговлю.

Одно из основных последствий сбоев времени и синхронизации связано с исполнением ордеров. Неточная синхронизация времени может привести к неправильному порядку или пропущенным сделкам. Когда ордера не исполняются в ожидаемой последовательности из-за проблем с синхронизацией, это может привести к неблагоприятным результатам, таким как задержка исполнения или исполнение по невыгодным ценам. Такие сбои могут привести к финансовым потерям для трейдеров и инвесторов и подорвать справедливость и целостность рынка.

Неточности данных являются еще одним важным следствием сбоев времени и синхронизации. Анализ рыночных данных в значительной степени зависит от точных и синхронизированных временных меток для анализа торговых моделей, выявления рыночных тенденций и принятия обоснованных решений. Когда происходит сбой синхронизации времени, точность временных меток ставится под угрозу, что приводит к неправильному анализу данных. Неточный анализ данных может помешать трейдерам эффективно реагировать на рыночные условия, что приводит к неоптимальным торговым решениям и потенциальным убыткам.

Проблемы с соблюдением нормативных требований также возникают из-за сбоев во времени и синхронизации. Финансовые регуляторы требуют от участников рынка придерживаться точных стандартов хронометража для обеспечения прозрачности и справедливости на рынках. При сбое синхронизации точность временных меток, используемых для составления нормативной отчетности и обеспечения соответствия требованиям, ставится под угрозу. Это может привести к штрафным санкциям регулирующих органов, репутационному ущербу и юридическим последствиям для участников рынка, подрывая доверие и целостность финансовой системы.

Алгоритмические торговые стратегии в значительной степени зависят от точной синхронизации времени для совершения сделок на основе предопределенных условий и рыночных событий. Сбои во времени и синхронизации могут нарушать алгоритмическую торговую деятельность, в результате чего торговые алгоритмы неверно интерпретируют или пропускают важные рыночные сигналы. Такие сбои могут привести к непреднамеренному исполнению сделок, неустойчивому поведению торговых алгоритмов и потенциальным убыткам. Кроме того, сбои во времени и синхронизации могут способствовать фрагментации рынка, когда расхождения во временных метках между различными торговыми системами создают диспропорции в портфеле рыночных ордеров. Эта фрагментация может препятствовать эффективности и справедливости рыночных операций.

Операционные риски возрастают, когда в торговых системах происходят сбои во времени и синхронизации. Несоответствия во временных метках могут привести к сбоям в работе системы, торговым ошибкам и техническим сбоям. Эти сбои могут повлиять на стабильность и надежность торговых платформ, приводя к неэффективности работы, финансовым потерям и репутационному ущербу для участников рынка.

Сбои во времени и синхронизации могут подорвать доверие инвесторов к финансовым рынкам. Когда трейдеры и инвесторы сталкиваются со сбоями или аномалиями из-за проблем с синхронизацией, это может подорвать их веру в честность и надежность рынка. Инвесторы могут не решаться участвовать в торговой деятельности, что приводит к снижению ликвидности и общей эффективности рынка.

Практика управления рисками ставится под угрозу при возникновении сбоев во времени и синхронизации. Своевременная и точная синхронизация имеет решающее значение для эффективного мониторинга рисков и их снижения. Сбои в синхронизации могут затруднять отслеживание подверженности риску, задерживать обнаружение нештатных торговых операций и препятствовать реализации мер по снижению риска. Это может повысить уязвимость торговых систем к финансовым потерям и системным рискам.

Высокочастотная торговля (HFTHFT расшифровывается как высокочастотная торговля и используется в банковской и финансовой индустрии, особенно для крупных банков и международных корпораций.) стратегии в значительной степени зависят от точной синхронизации времени для совершения сделок с невероятно высокой скоростью. Сбои во времени и синхронизации могут нарушить сверхбыструю природу HFT, что приведет к упущенным торговым возможностям, снижению прибыльности и конкурентным недостаткам для высокочастотных трейдеров.

В заключение, сбои во времени и синхронизации в торговых системах имеют значительные последствия для различных аспектов финансовой торговли. От проблем с исполнением ордеров и неточностей в данных до проблем с соблюдением нормативных требований и операционных рисков, эти сбои могут нарушить справедливость, эффективность и стабильность финансовых рынков. Для устранения этих последствий требуются надежные механизмы синхронизации времени и лучшие практики для обеспечения надежного и точного учета времени в торговых системах.

## **4. Рекомендации по синхронизации времени**

Для снижения рисков, связанных со сбоями времени и синхронизации в финансовых торговых системах, решающее значение имеет внедрение набора передовых практик для достижения надежной синхронизации времени. Эти рекомендации охватывают несколько ключевых областей, включая источники точного времени, протоколы точного времени, алгоритмы синхронизации часов, оптимизацию сети и методы мониторинга. Кроме того, для обеспечения непрерывной синхронизации времени важно уделять особое внимание механизмам резервирования, отказоустойчивости и перехода на другой ресурс.

Выбор точных источников времени имеет фундаментальное значение для обеспечения надежной синхронизации времени. Рекомендуется использовать сертифицированные и высокоточные источники времени, такие как атомные часы или спутниковую глобальную навигационную спутниковую систему (GNSSГлобальная навигационная спутниковая система (GNSS): общий термин, описывающий любую группировку спутников, которая предоставляет услуги определения местоположения, навигации и синхронизации (PNT) на глобальной или региональной основе. Смотрите также) приемники. Эти источники предоставляют точные и отслеживаемые ссылки на время, которые служат основой для достижения точной синхронизации в торговых системах.

Протоколы точного времени играют жизненно важную роль в достижении надежной синхронизации времени. Такие протоколы, как протокол точного времени (PTP) и Сетевой протокол времени (NTP), обычно используются в финансовых торговых системах. [**PTP особенно подходит для высокоточной синхронизации**](https://safran-navigation-timing.com/product/high-accuracy-timing-ip-core-hati), поскольку обеспечивает субмикросекундную точность. С другой стороны, NTP обеспечивает точность синхронизации в миллисекундном диапазоне и хорошо подходит для синхронизации в крупных сетях. [**Выбор соответствующего протокола точного хронометража на основе**](https://safran-navigation-timing.com/solution/timing-and-synchronization/) конкретных требований торговой системы имеет важное значение.

Алгоритмы синхронизации часов имеют решающее значение для поддержания точной синхронизации времени. Такие алгоритмы, как White Rabbit, алгоритм Беркли и алгоритм Марзулло, обычно используются для синхронизации часов в распределенных системах. Эти алгоритмы учитывают смещение часов, задержку в сети и ограничения точности временных меток для достижения согласованной и надежной синхронизации в нескольких системах. Внедрение надежных алгоритмов синхронизации часов повышает точность и стабильность синхронизации времени в торговых системах.

Оптимизация сетевой инфраструктуры имеет решающее значение для минимизации задержек в сети и повышения точности синхронизации времени. Использование высокоскоростных сетевых подключений с низкой задержкой, внедрение механизмов контроля качества обслуживания (QoS) для приоритизации трафика, зависящего от времени, и снижение перегрузки сети за счет эффективного проектирования сети может значительно повысить производительность синхронизации времени. Меры по оптимизации сети помогают обеспечить своевременную и точную передачу данных, уменьшая влияние сетевых задержек на синхронизацию.

Непрерывный мониторинг синхронизации времени необходим для оперативного обнаружения любых отклонений или сбоев и устранения их последствий. Методы мониторинга включают измерение точности и стабильности часов, мониторинг задержек в сети и анализ показателей производительности синхронизации. Мониторинг в режиме реального времени позволяет упреждающе выявлять потенциальные проблемы с синхронизацией и способствует своевременным корректирующим действиям для поддержания надежной синхронизации времени.

Создание механизмов резервирования, отказоустойчивости и перехода на другой ресурс в инфраструктуре синхронизации времени имеет решающее значение для обеспечения непрерывной работы в случае сбоев. Резервные источники времени, несколько серверов синхронизации и устойчивые сетевые архитектуры помогают смягчить влияние отдельных точек сбоя и повысить общую надежность синхронизации времени. Механизмы аварийного переключения могут автоматически переключаться на резервные источники времени или серверы синхронизации, когда в основных источниках или серверах происходят сбои, обеспечивая непрерывную синхронизацию времени.

Включение этих передовых практик в разработку, внедрение и поддержание синхронизации времени в финансовых торговых системах может значительно повысить надежность, точность и производительность. [**Выбирая источники точного времени**](https://safran-navigation-timing.com/product/securesync-time-and-frequency-reference-system), используя протоколы точного времени и алгоритмы синхронизации часов, оптимизируя сетевую инфраструктуру, внедряя методы мониторинга и обеспечивая механизмы резервирования и отработки отказа, торговые системы могут обеспечить надежные и отказоустойчивые возможности синхронизации времени. Эти методы способствуют снижению рисков, связанных со сбоями во времени и синхронизации, позволяя участникам финансового рынка работать уверенно и эффективно.

## **5. Технологии синхронизации времени**

Синхронизация времени в торговых системах основана на различных технологиях, которые предлагают разные уровни точности, масштабируемости, сложности и применимости к различным системным архитектурам. В этом разделе рассматриваются некоторые из широко используемых технологий, включая протокол сетевого времени (NTP), протокол точного времени (PTP), источники времени на основе GPS, атомные часы и новые технологии, такие как White Rabbit и IEEE 1588v2.

Сетевой протокол времени (NTP) - это широко распространенный протокол синхронизации времени, который использует Интернет для распределения времени. NTP обеспечивает точность синхронизации в миллисекундном диапазоне и подходит для систем, где субмикросекундная точность не является существенной. NTP относительно прост в реализации и может синхронизировать время в крупных сетях. Однако на его точность могут влиять задержки в сети и асимметрия, что ограничивает его применимость в высокочастотной торговле и средах, чувствительных к задержкам.

Precision Time Protocol (PTP) - это протокол, специально разработанный для достижения высокоточной синхронизации времени в распределенных системах. PTP обеспечивает субмикросекундную точность и подходит для приложений, требующих точной синхронизации, таких как алгоритмическая торговля и высокочастотная торговля. PTP работает путем обмена сообщениями синхронизации между устройствами для расчета смещений тактовых импульсов и корректировки хода тактовых импульсов. PTP может быть более сложным в реализации, чем NTP, и требует тщательной настройки и оптимизации сети для достижения оптимальной производительности.

Источники времени на основе GPS используют сигналы глобальных навигационных спутниковых систем (GNSS), таких как GPSГлобальная система позиционирования - это навигационная спутниковая система. Смотрите также, чтобы обеспечить точную привязку времени. Приемники GNSS принимают сигналы от нескольких спутников и вычисляют точное время на основе временных меток, встроенных в эти сигналы. Источники времени на основе GPS обеспечивают высокую точность, обычно в диапазоне наносекунд, что делает их хорошо подходящими для приложений, требующих чрезвычайно точной синхронизации времени. Однако эти источники зависят от прямой видимости спутников, что делает их уязвимыми к блокировке сигнала или помехам в городских условиях или районах с ограниченной видимостью в небе.

Атомные часы - это высокоточные источники времени, которые обеспечивают точные и стабильные отсчеты времени. Их работа основана на колебаниях атомов или молекул, которые служат постоянным и надежным механизмом отсчета времени. Атомные часы обеспечивают исключительную точность, часто в диапазоне субмикросекунд или даже субнаносекунд. Эти часы обычно используются в качестве основных ориентиров для хронометража и служат основой для технологий синхронизации времени. Однако атомные часы дороги, требуют тщательного обслуживания и не подходят для прямой интеграции в торговые системы из-за их специализированного характера.

Emerging technologies like White Rabbit and IEEE 1588v2 are gaining attention in the realm of time synchronization for trading systems. White Rabbit is an extension of the PTP protocol that introduces additional features for deterministic time synchronization over Ethernet networks. It provides sub-nanosecond accuracy and is highly scalable, making it suitable for high-frequency trading and latency-sensitive applications. White Rabbit incorporates precise hardware timestamps and advanced synchronization algorithms to achieve exceptional performance. However, the adoption of White Rabbit may require specialized hardware and modifications to existing network infrastructure.

IEEE 1588v2, also known as Precision Time Protocol version 2, is an updated version of the PTP standard. It enhances the accuracy and performance of PTP by introducing improvements in clock synchronization algorithms and network optimization techniques. IEEE 1588v2 offers sub-microsecond accuracy and is widely supported by network devices and systems. It provides scalability and flexibility, making it applicable to a wide range of trading system architectures. IEEE 1588v2 can be a suitable choice for achieving high-precision time synchronization in trading systems.

При выборе технологии синхронизации времени торговые системы должны учитывать свои специфические требования, включая требуемую точность, масштабируемость, сложность и совместимость с существующей инфраструктурой. Такие факторы, как необходимость высокой точности, низкая задержка и устойчивость к изменениям в сети, играют решающую роль при определении подходящей технологии. Путем тщательной оценки и внедрения правильной технологии торговые системы могут добиться надежной и точной синхронизации времени, что позволяет им эффективно работать в динамичной финансовой торговой среде.

## **6. Мониторинг и диагностика**

Для обеспечения надежности синхронизации времени в торговых системах важно установить эффективные механизмы мониторинга и диагностики. В этом разделе рассматриваются различные методы и инструменты, которые позволяют осуществлять комплексный мониторинг производительности синхронизации времени, включая измерение смещения часов, измерение задержки, оценку качества синхронизации и протоколирование событий. Кроме того, в нем раскрывается потенциал аналитики и машинного обучения в обнаружении аномалий и облегчении упреждающего управления синхронизацией времени.

Измерение смещения часов - это фундаментальный метод мониторинга, используемый для оценки точности синхронизации времени. Сравнивая местное время на часах с надежным эталонным источником времени, можно рассчитать смещение между ними. Непрерывный мониторинг смещений тактовых импульсов позволяет выявлять любые отклонения от ожидаемых показателей синхронизации. Когда смещения тактовых импульсов превышают заданные пороговые значения, могут генерироваться оповещения в режиме реального времени, что позволяет оперативно проводить расследование и принимать корректирующие действия.

Измерение задержки является еще одним важным аспектом мониторинга синхронизации времени. Оно включает в себя измерение времени, необходимого для передачи сообщений синхронизации между устройствами или системами. Мониторинг задержки помогает выявить потенциальные узкие места или перегрузку сети, которые могут приводить к задержкам в синхронизации времени. Отслеживая задержки, торговые системы могут оптимизировать сетевые конфигурации и инфраструктуру для минимизации задержек синхронизации и повышения общей производительности.

Оценка качества синхронизации включает в себя оценку стабильности и непротиворечивости синхронизации времени в течение определенного периода времени. Эту оценку можно выполнить путем анализа показателей синхронизации, таких как дрожание часов и стабильность. При мониторинге качества синхронизации могут быть обнаружены отклонения или флуктуации в производительности синхронизации. Эта информация ценна для выявления потенциальных проблем и оптимизации параметров или алгоритмов синхронизации для повышения общего качества синхронизации.

Протоколирование событий является важным компонентом мониторинга и диагностики при синхронизации времени. События, связанные с синхронизацией времени, такие как сбои синхронизации, корректировки часов или перебои в работе сети, могут регистрироваться для последующего анализа. Журналы событий содержат хронологическую запись событий синхронизации и могут использоваться для устранения неполадок, анализа первопричин и аудита. Они помогают выявлять закономерности или повторяющиеся проблемы, позволяя принимать упреждающие меры для решения потенциальных проблем с синхронизацией.

Применение аналитики и методов машинного обучения в мониторинге синхронизации времени имеет большой потенциал для повышения эффективности управления синхронизацией. Анализируя исторические данные синхронизации и показатели производительности системы, можно выявить аномалии и закономерности. Алгоритмы машинного обучения можно обучить обнаруживать ненормальное поведение синхронизации или прогнозировать потенциальные сбои синхронизации. Эти передовые методы позволяют упреждающе управлять синхронизацией времени, выявляя проблемы до того, как они повлияют на торговые операции, и обеспечивая своевременное вмешательство.

Кроме того, машинное обучение может помочь в оптимизации алгоритмов и параметров синхронизации на основе исторических данных и характеристик системы. Используя модели машинного обучения, торговые системы могут постоянно улучшать производительность синхронизации времени и адаптироваться к изменяющимся условиям сети или торговым требованиям. Эти методы позволяют осуществлять динамическое и адаптивное управление синхронизацией времени, обеспечивая оптимальную производительность и устойчивость в условиях меняющейся торговой среды.

В заключение, мониторинг и диагностика являются важнейшими аспектами поддержания надежной синхронизации времени в торговых системах. Измерение смещения часов, измерение задержки, оценка качества синхронизации и протоколирование событий дают ценную информацию о производительности синхронизации и позволяют своевременно обнаруживать и устранять проблемы. Кроме того, использование аналитики и машинного обучения облегчает упреждающее управление синхронизацией времени и ее оптимизацию. Внедряя комплексные механизмы мониторинга и диагностики, торговые системы могут обеспечить надежную и точную синхронизацию времени, повышая эффективность и достоверность своей работы.

## **7. Избыточность и устойчивость**

Для снижения рисков, связанных со сбоями времени и синхронизации в торговых системах, внедрение механизмов резервирования и устойчивости имеет первостепенное значение. В этом разделе подчеркивается важность наличия резервных источников времени, разнообразных сетевых путей, резервных ссылок на часы и стратегий резервного копирования синхронизации.

Резервные источники времени играют решающую роль в обеспечении непрерывной и надежной синхронизации времени. Используя несколько сертифицированных и точных источников времени, таких как атомные часы или привязки времени на основе GPS, торговые системы могут поддерживать синхронизацию, даже если один источник становится недоступным или скомпрометирован. Резервирование источников времени помогает защитить от единичных точек сбоя и повышает общую устойчивость инфраструктуры синхронизации.

Разнообразные сетевые маршруты необходимы для устойчивости синхронизации времени. Устанавливая несколько сетевых подключений или используя разных сетевых провайдеров, торговые системы могут смягчить последствия перебоев в работе сети. Резервные сетевые пути позволяют системе перенаправлять сообщения о синхронизации времени и поддерживать синхронизацию даже в случае сбоев сети. Это резервирование гарантирует надежную передачу и прием данных, зависящих от времени, сводя к минимуму риск сбоев синхронизации.

Резервные ссылки на часы обеспечивают дополнительный уровень резервирования и устойчивости при синхронизации времени. В дополнение к основным источникам времени, торговые системы могут иметь резервные ссылки на часы, такие как вторичные атомные часы или источники времени на основе GNSS. Эти резервные ссылки служат надежной альтернативой в случае сбоев основного источника времени или уязвимостей. Имея резервные ссылки на часы, торговые системы могут быстро переключаться на альтернативные источники без ущерба для целостности синхронизации.

Стратегии резервного копирования синхронизации необходимы для поддержания непрерывной синхронизации времени. Эти стратегии включают в себя создание резервных серверов синхронизации или хронометристов, которые могут взять на себя обязанности по синхронизации в случае сбоев основного сервера. Стратегии резервного копирования синхронизации гарантируют, что даже в случае сбоев в основной инфраструктуре синхронизации существует механизм отработки отказа для плавного перехода к резервным серверам или хронометристам. Такое резервирование в инфраструктуре синхронизации гарантирует бесперебойную синхронизацию и снижает риски сбоев во времени и синхронизации.

Механизмы отработки отказа являются критически важными компонентами устойчивой архитектуры синхронизации времени. Эти механизмы автоматически обнаруживают сбои в основных источниках времени, серверах синхронизации или сетевых подключениях и инициируют процесс отработки отказа для переключения на резервные источники или серверы. Механизмы аварийного переключения гарантируют, что торговые системы могут быстро и плавно переходить на резервные компоненты, минимизируя время простоя и поддерживая непрерывную синхронизацию времени.

Непрерывный мониторинг жизненно важен для обеспечения эффективности механизмов резервирования и устойчивости. Отслеживая состояние и производительность источников времени, сетевых подключений, серверов синхронизации и систем резервного копирования, можно быстро выявить любые отклонения или сбои. Мониторинг в режиме реального времени позволяет упреждающе выявлять проблемы и способствует своевременным корректирующим действиям. Непрерывный мониторинг гарантирует оптимальное функционирование механизмов резервирования и устойчивости, обеспечивая бесперебойную синхронизацию времени.

Важно отметить, что в дополнение к рискам естественных сбоев и сбоев в работе сети, торговые системы также подвержены преднамеренным атакам, таким как глушение GNSS и подмена. Подавление ГНСС предполагает преднамеренное вмешательство в спутниковые сигналы, в то время как подмена предполагает создание ложных сигналов ГНСС. Эти вредоносные действия могут нарушать синхронизацию времени в торговых системах или манипулировать ею, приводя к неточным временным меткам и потенциальным финансовым потерям. Снижение рисков помех и подмены GNSS требует внедрения надежных мер по защите от помех и подмены, таких как мониторинг сигналов, методы аутентификации и резервные ссылки на хронометраж, которые устойчивы к таким атакам.

В заключение, включение механизмов резервирования и устойчивости в синхронизацию времени важно для снижения рисков сбоев времени и синхронизации в торговых системах. Резервные источники времени, разнообразные сетевые пути, резервные ссылки на часы, стратегии резервного копирования синхронизации, механизмы отработки отказа и непрерывный мониторинг в совокупности способствуют бесперебойной и надежной синхронизации времени. Внедряя эти меры, торговые системы могут повысить свою устойчивость, минимизировать время простоя и поддерживать точную синхронизацию времени даже в условиях сбоев или вредоносных атак.

## **8. Соображения по соблюдению нормативных требований**

Синхронизация времени в финансовых торговых системах имеет решающее значение не только для операционной эффективности, но и для соблюдения нормативных требований. В этом разделе освещаются нормативные базы, которые предъявляют особые требования к синхронизации времени на финансовых рынках, такие как MiFID II (Директива о рынках финансовых инструментов II) в Европейском Союзе и CAT (Сводный контрольный журнал) в Соединенных Штатах.

MiFID II, всеобъемлющая нормативная база, регулирующая финансовые рынки в Европейском Союзе, требует точной фиксации времени торговых операций. В соответствии с MiFID II участники рынка обязаны отмечать время ордеров, исполнения и связанных с ними событий по Всемирному координированному времени (UTC) для обеспечения согласованности и отслеживаемости. Точная временная метка торговых операций позволяет регулирующим органам точно восстанавливать последовательность событий и проводить расследования в случае злоупотреблений на рынке или нарушений.

Аналогичным образом, в Соединенных Штатах инициатива CAT (Consolidated Audit Trail) направлена на создание всеобъемлющего аудиторского журнала всех сделок с акциями и опционами, совершаемых на биржах США. Требования CAT включают точные и синхронизированные временные метки для отчетности о сделках. Участники рынка должны убедиться, что их торговые системы синхронизируют время с центральной системой хронометражирования CAT для обеспечения точной и последовательной отчетности о сделках. Синхронизированные временные метки облегчают создание точного и надежного аудиторского журнала, повышая прозрачность и надзор регулирующих органов.

Точная отметка времени - это лишь один аспект соблюдения нормативных требований. Отчетность о сделках - еще одно важное условие соблюдения требований, где важно синхронизированное время. Финансовые нормативы часто требуют, чтобы участники рынка сообщали о сделках и связанных с ними данных регулирующим органам в определенные сроки. Точная синхронизация времени обеспечивает точную и своевременную отчетность по сделкам, обеспечивая соблюдение обязательств по отчетности.

Более того, синхронизированный хронометраж играет жизненно важную роль в создании журналов аудита и соблюдении требований к ведению учета. Регулирующие органы часто требуют от участников рынка вести подробные записи о торговой деятельности, включая размещение ордеров, исполнение ордеров и подтверждения сделок. Точные и синхронизированные временные метки имеют решающее значение для создания всеобъемлющего аудиторского журнала и выполнения обязательств по ведению учета.

При расследованиях регулирующих органов синхронизированное время становится незаменимым. При проведении расследований злоупотреблений на рынке, нерегулярных торговых схем или потенциальных нарушений регулирующие органы полагаются на синхронизированные временные метки для точного восстановления последовательности событий. Возможность точной корреляции событий в различных торговых системах и у участников рынка позволяет регулирующим органам выявлять нарушения, выявлять манипулятивные действия и обеспечивать целостность рынка.

Стоит отметить, что различные нормативные базы могут предъявлять особые требования к точности синхронизации времени, аккуратности и срокам хранения аудиторского журнала. Участники рынка должны быть в курсе соответствующих нормативных актов и соблюдать особые требования, применимые к их юрисдикции. Соображения соответствия должны выходить за рамки технических аспектов синхронизации времени и охватывать управление, политику, процедуры и внутренний контроль для обеспечения соблюдения нормативных требований.

В заключение следует отметить, что соблюдение нормативных требований является важнейшим фактором синхронизации времени в финансовых торговых системах. Такие нормативные акты, как MiFID II и CAT, предъявляют особые требования к точным меткам времени, отчетности о сделках, журналам аудита и ведению учета. Синхронизированное время позволяет регулирующим органам восстанавливать последовательность событий, проводить расследования и обеспечивать целостность рынка. Участники рынка должны придерживаться нормативно-правовой базы, соответствующей их юрисдикциям, и внедрять надежные методы синхронизации времени для выполнения обязательств по соблюдению требований и поддержания прозрачности регулирования.

## **9. Будущие тенденции и инновации**

Область синхронизации времени в торговых системах продолжает развиваться с развитием технологий. В этом разделе представлен обзор будущих тенденций и инноваций, которые, как ожидается, сформируют ландшафт синхронизации времени на финансовых рынках.

Одной из новых тенденций является внедрение технологии блокчейн для целей установления временных меток. Присущие блокчейну свойства неизменности и децентрализации делают его хорошо подходящим для обеспечения целостности и отслеживаемости временных меток. Используя блокчейн, торговые системы могут создавать прозрачную и защищенную от несанкционированного доступа запись событий с отметками времени, повышая достоверность торговых данных и обеспечивая более надежные маршруты аудита. Внедрение решений для определения временных меток на основе блокчейна потенциально способно произвести революцию в точности и проверяемости временных меток в финансовых торговых системах.

Еще одной областью инноваций является интеграция квантовых технологий в синхронизацию времени. Квантовые технологии, такие как квантовые часы и квантовая коммуникация, обеспечивают беспрецедентную точность и безопасность хронометража. Квантовые часы используют квантовые явления для достижения замечательной точности, что может повысить точность синхронизации времени в торговых системах. Кроме того, протоколы квантовой связи могут обеспечивать безопасную и проверяемую передачу сообщений о синхронизации времени, защищая от потенциальных атак или уязвимостей. Интеграция квантовых технологий потенциально может значительно повысить точность, надежность и безопасность синхронизации времени в финансовой торговле.

Ожидается, что появление сетей 5G и периферийных вычислений также окажет влияние на синхронизацию времени в торговых системах. Сети 5G обещают сверхнизкую задержку и высокую пропускную способность, что позволит быстрее и эффективнее передавать сообщения о синхронизации времени. Это высокоскоростное подключение позволяет сократить задержки синхронизации, повышая производительность торговых систем в режиме реального времени. Кроме того, децентрализованный характер периферийных вычислений позволяет выполнять задачи синхронизации времени ближе к торговой инфраструктуре, минимизируя задержки в сети и повышая точность синхронизации. Сочетание сетей 5G и периферийных вычислений потенциально способно революционизировать возможности синхронизации времени, обеспечивая более быструю и точную синхронизацию в высокораспределенных и чувствительных к задержкам торговых средах.

Более того, достижения в области машинного обучения и искусственного интеллекта (ИИ) могут революционизировать управление синхронизацией времени. Алгоритмы ИИ могут анализировать огромные объемы исторических данных синхронизации, показатели производительности сети и системные характеристики для динамической оптимизации алгоритмов и параметров синхронизации. Модели машинного обучения могут обнаруживать закономерности, аномалии и потенциальные сбои синхронизации, обеспечивая упреждающее управление и автоматизированное принятие решений в режиме реального времени. Эти усовершенствования могут повысить устойчивость, адаптивность и производительность синхронизации времени в торговых системах.

В заключение следует отметить, что будущие тенденции и инновации в области синхронизации времени для торговых систем являются многообещающими и обладают потенциалом для повышения точности, безопасности и производительности. Ожидается, что внедрение технологии блокчейн для определения времени, интеграция квантовых технологий, достижения в сетях 5G и периферийных вычислениях, а также применение машинного обучения и искусственного интеллекта сформируют будущее синхронизации времени на финансовых рынках. Используя эти инновации, торговые системы могут достичь более высоких уровней точности, безопасности и эффективности синхронизации времени, что позволяет им идти в ногу с меняющимися требованиями финансовой индустрии.

## **10. Заключение**

Точная синхронизация времени имеет первостепенное значение в финансовых торговых системах. В этом техническом документе рассмотрены технические аспекты синхронизации времени, включая возникающие проблемы, последствия сбоев времени и синхронизации, лучшие практики, технологии, мониторинг и диагностику, механизмы резервирования и устойчивости, соображения соответствия нормативным требованиям и будущие тенденции.

Проблемы достижения точной синхронизации времени в торговых системах, такие как задержка в сети, смещение часов, детализация временных меток и сложность распределенных систем, могут оказать значительное влияние на производительность и надежность торговли. Сбои во времени и синхронизации могут привести к проблемам с исполнением ордеров, неточностям в данных, нарушениям соблюдения нормативных требований, сбоям в алгоритмической и высокочастотной торговле, операционным рискам и потере доверия инвесторов.

Для обеспечения надежной синхронизации времени необходимы передовые методы, такие как выбор источников точного времени, протоколов точного времени, алгоритмов синхронизации часов, оптимизации сети и методов мониторинга. Резервирование, отказоустойчивость, механизмы отработки отказа и непрерывный мониторинг играют решающую роль в [**поддержании надежной синхронизации времени.**](https://safran-navigation-timing.com/solution/timing-and-synchronization/)

Такие технологии, как Network Time Protocol (NTP), Precision Time Protocol (PTP), источники времени на основе GPS, атомные часы и новые инновации, такие как White Rabbit и IEEE 1588v2, предоставляют возможности для достижения точной синхронизации времени. Каждая технология имеет свои сильные стороны, масштабируемость, сложность и применимость к различным архитектурам торговых систем.

Механизмы мониторинга и диагностики, включая измерение смещения часов, измерение задержки, оценку качества синхронизации и протоколирование событий, необходимы для эффективного управления синхронизацией времени. Кроме того, использование аналитики и машинного обучения может обеспечить обнаружение аномалий и упреждающее управление синхронизацией времени.

Механизмы резервирования и устойчивости, такие как резервные источники времени, разнообразные сетевые пути, резервные ссылки на часы, стратегии резервного копирования синхронизации, механизмы отработки отказа и непрерывный мониторинг, имеют решающее значение для снижения рисков сбоев времени и синхронизации. Эти механизмы обеспечивают непрерывную синхронизацию времени даже в условиях сбоев или вредоносных атак, таких как глушение GNSS и подмена.

Соображения соответствия нормативным требованиям подчеркивают важность точных временных меток, отчетности о сделках, аудиторских проверок и ведения учета в финансовых торговых системах. Соблюдение таких нормативных актов, как MiFID II и CAT, требует точной синхронизации времени для реконструкции событий, расследований регулирующих органов и соблюдения обязательств по отчетности.

Заглядывая в будущее, мы видим тенденции и инновации, такие как блокчейн для определения времени, квантовые технологии, влияние сетей 5G и передовых вычислений, а также интеграцию машинного обучения и искусственного интеллекта, которые обладают большим потенциалом для расширения возможностей синхронизации времени в торговых системах.

В заключение, достижение точной синхронизации времени в финансовых торговых системах является сложной и критически важной задачей. Понимая проблемы, внедряя лучшие практики, используя соответствующие технологии, механизмы мониторинга и диагностики, обеспечивая избыточность и устойчивость, а также соблюдая нормативные требования, торговые системы могут поддерживать надежную и точную синхронизацию времени. Поскольку технологии продолжают развиваться, внедрение будущих тенденций и инноваций еще больше повысит точность, безопасность и результативность синхронизации времени, что позволит финансовым рынкам работать эффективно.

# **ПРОТИВОДЕЙСТВИЕ АТАКЕ NTP С РАСПРЕДЕЛЕННЫМ ОТКАЗОМ В ОБСЛУЖИВАНИИ (DDOS)**

## **Для кого этот документ**

* Сетевых и системных инженеров, сетевых и системных администраторов;
* Директора / менеджеры ИТ-инфраструктуры.

## **Введение**

Многие компании не считают обслуживание сетевого времени ключевым компонентом своих критически важных инфраструктур. На практике, его часто полностью упускают из виду. В результате сетевой архитектор или инженер часто по умолчанию выбирает простую альтернативу: использует сервер или сетевой коммутатор в качестве источника сетевых часов и синхронизирует эти источники с интернет-серверами времени с использованием протокола сетевого времени NTP/PTP. Данные протоколы позволяет компьютерам и устройствам синхронизировать свои системные часы с эталонным источником времени. NTP необходим для различных приложений и служб, которые полагаются на синхронизированное время, таких как сетевая безопасность, аутентификация и протоколирование данных.).

Однако действительно ли “NTP через Интернет” является безопасным методом решения задач сетевой синхронизации времени?

## **NTP через Интернет: насколько это безопасно?**

NTP, один из старейших используемых интернет-протоколов времени, является стандартом для синхронизации часов между компьютерами в сети с коммутацией пакетов. Согласно отчетам о глобальном состоянии безопасности Интернета (на 2023 г.), протокол NTP через является вторым по распространенности протоколом, подвергающимся DDoS-атакам.

Всего за год количество DDoS-атак увеличилось на 16%.

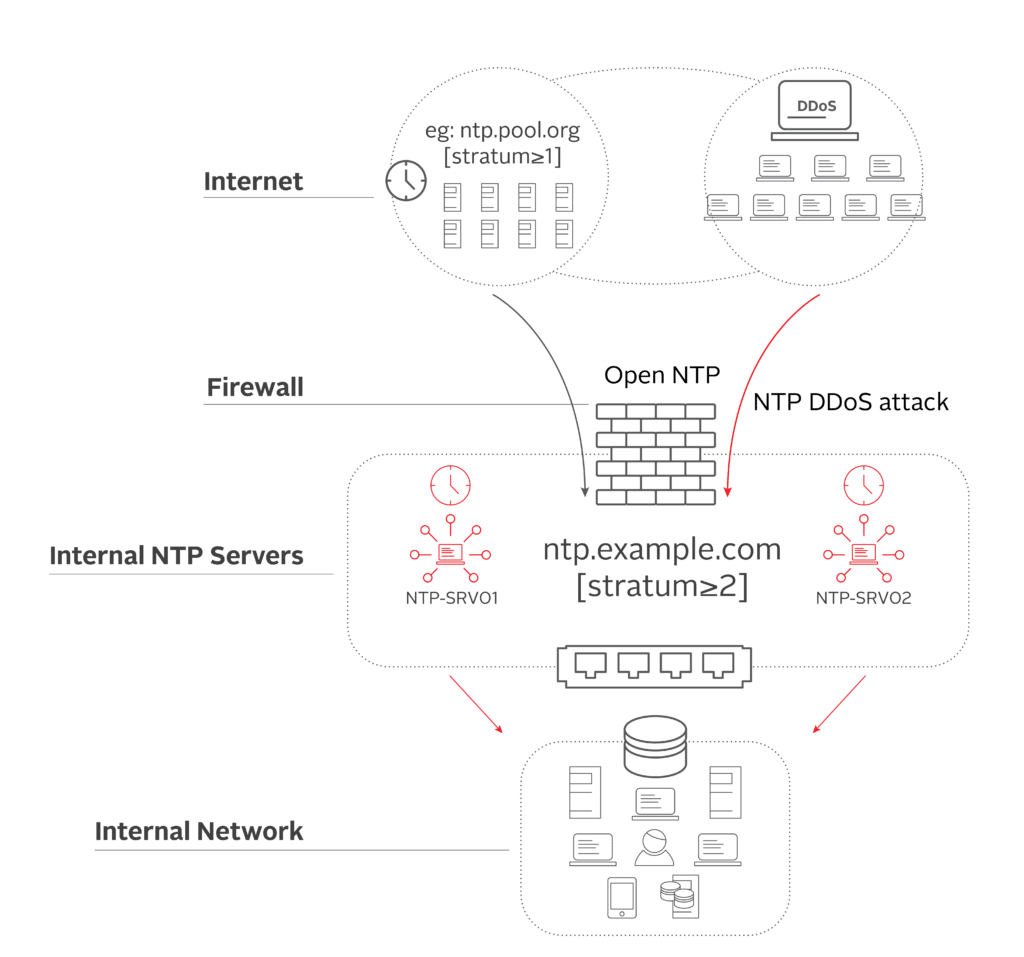


Рисунок 1: Типичное корпоративная синхронизация

с использованием NTP-через Интернет.

На рисунке 1 показано, как работает типичная настройка NTP через Интернет в инфраструктуре. Она состоит из общедоступного пула серверов NTP (уровень NTP 1), который используется внутренними серверами времени в качестве эталона для получения времени. Для этого подхода требуется канал связи между Интернетом и внутренними серверами времени через брандмауэр, который открывает доступ к сети и создает уязвимость, которую хакеры могут использовать для проникновения во всю вашу систему. В сетях, использующих этот метод, инфраструктура синхронизации может не только стать готовой к кибератакам, но и качество времени будет поставлено под угрозу с точки зрения точности.

## **Лучшее решение: ваш собственный NTP/PTP-сервер Stratum 1**

Если вы используете сеть Интернет в качестве источника своего сетевого времени, к сожалению — полагать, что ваш брандмауэр - даже брандмауэр нового поколения, который поставляется с функциями IDS (система обнаружения вторжений) или IPS (система предотвращения вторжений) – защитит вас от DDoS-атак.

## **Итак, как вы можете смягчить последствия DDoS-атак для службы time**

Выражение “цепочка настолько прочна, насколько прочно ее самое слабое звено” как нельзя более верно в случае DDoS-атак. В решениях Shiwa/Qantum мы рекомендуем нашим клиентам очень эффективное и простое решение: устранить самое слабое звено в цепочке. Другими словами, не полагайтесь на Интернет в отношении времени работы в сети.

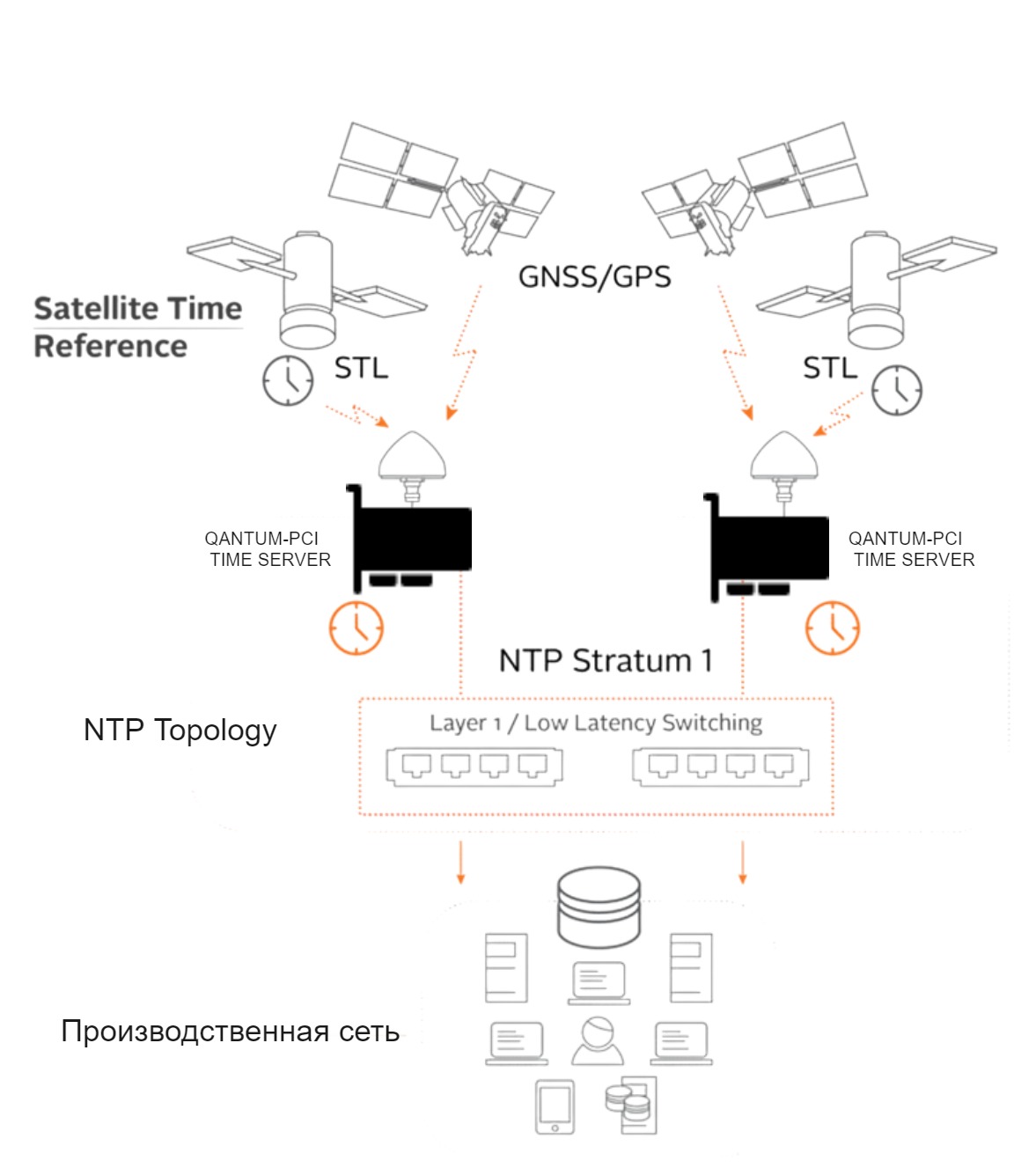


Рисунок 2. Типичная устойчивая инфраструктура синхронизации для предприятия с серверами времени Qantum/SHIWA

На рисунке 2 показано, как предприятие может устранить “ слабое звено” – создав собственную устойчивую и резервированную инфраструктуру сетевой синхронизации внутри компании, используя серверы времени **Qantum PCIe**, либо **SHIWA Time+** (для защищенных сред, с поддержкой согласования времени через распределенный реестр (блокчейн)).

Каждый такой сервер времени получает сигналы времени через Глобальную навигационную спутниковую систему (ГНСС). Затем время с точностью до наносекунд распределяется по сети. Если в качестве предпочтительного протокола используется NTP/PTP, сервер будет работать на уровне 1 и распределять безопасное время по остальной части вашей сети без использования подключения к Интернету.

## **Другие преимущества внутренней синхронизации**

Помимо снижения опасности DDoS-атак, серверы времен SHIWA/Qantum, предлагают ряд других преимуществ, в том числе:

1. Отказоустойчивость – каждый сервер времени может использовать несколько ГНСС для привязки времени. В случае, если сигнал ГНСС недоступен, сервера времени содержат внутренний высокостабильный резервный генератор, способный поддерживать точное время в течение нескольких дней или даже месяцев с использованием технологии Atomic clock;
2. Защита радиочастотного сигнала – защита от помех, подмены и защиты сигнала встроены в серверы времени. В наших решениях мы применяем защиту от помех в антенных системах;
3. Высокая целостность, отслеживаемое время по UTC - сложные угрозы могут подделывать ГНСС сигналы. В данном случае технология SHIWA Time+ готова прийти на помощь. В качестве альтернативного зашифрованного сигнала, использующего мощную аутентификацию через распределенный реестр, для подтверждения того, что у вас истинное значение UTC;
4. Дополнительные опций – в дополнение к полной совместимости с NTP/PTP, серверы времени поддерживают множество протоколов и опций расширений для распределения времени.
5. **Заключение**

В современной информационной среде, насыщенной угрозами, слишком легко заблокировать или подделать сеть, вызвав что угодно - от незначительных сбоев до чрезвычайного хаоса в критически важной инфраструктуре. Зависимость от NTP через Интернет сопряжена с присущими ей рисками, которые можно легко снизить, используя ваш собственный NTP/PTP-сервер Stratum 1, который обеспечит высокую целостность отслеживаемого времени по UTC. Добавление программного обеспечения для защиты от помех и подделки данных обеспечить вам еще более высокий уровень отказоустойчивости и безопасности. Реальный вопрос, который следует задать себе: может ли ваша компания позволить себе риск DDoS-атаки?

Если ответ отрицательный, то обновление до NTP-сервера Stratum 1 должно быть обязательным.