БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИЙ

Указом Президента Российской Федерации от 5 декабря 2016 г. №646 утверждена “Доктрина информационной безопасности РФ”. Сейчас готовится новая редакция. Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества, государства. Экономически эффективное решение проблем телекоммуникаций является фактором ускорения развития государства и формирования информационного общества. Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов России.

Информационная безопасность базируется на безопасности информационной инфраструктуры, определяется уровнем технологий защиты каналов связи. Каналы передачи данных — наиболее уязвимый компонент информационной инфраструктуры. Тропосферная радиосвязь, сотовая связь, радиорелейные линии, спутниковые радиоканалы, все виды беспроводной радиосвязи, в разной степени, но все подвержены перехвату. Протяжённые кабельные каналы (ВОЛС, надземные, подземные, подводные) не способны исключить несанкционированное подключение и физическое повреждение.

Распределённая сеть передачи способна обеспечить повышение надёжности связи. Традиционно защиту важной информации в каналах связи выполняет криптография. Криптография не творит чудеса, «делает большие секреты из очень маленьких секретов». Системы криптографической защиты информации (СКЗИ) базируются на критической инфраструктуре распределения ключей шифрования (PKI). Квантовые компьютеры в битве стран за «квантовое превосходство» неуклонно наращивают возможности криптоанализа криптографическими систем с открытыми ключами. Начался радикальный пересмотр оценок стойкости криптографической защиты. Качественные перемены неизбежны, вопрос стоит не о сроках, не о длительности лага, а о масштабах последствий.

В последние десятилетия активировались исследования и разработки, пришло понимание, защиту инфраструктуры криптографических ключей не способна обеспечить **математическая сложность,** необходима **физически гарантированная безопасность.** Защиту каналов возлагают на квантовую криптографию, точнее, на технологию квантового распределения ключей шифрования (КРК, QKD), реализуемую на тёмных (резервных) волокнах кабельных сетей ВОЛС. Квантовые коммуникационные сети активно разворачиваются в Евросоюзе, в Китае, в Японии, в США, в России.

Квантовая криптография призвана увеличить стойкость систем связи, позволяет обнаруживать попытки перехвата информации с высокой вероятностью, теоретически, но практические реализации таких систем ограничены параметрами неидеальных каналов. Жёсткие законы физики ограничивают практическую дальность квантовой связи по оптоволоконным каналам **до сотни километров**, попытки увеличения дальности передачи приводят к снижению скорости передачи ниже десятка бит в секунду.

Работа криптомаршрутизатора между двумя узлами связи на расстоянии 143 километра идёт с оптическими потерями в канале 37 дБ. Среднее значение скорости генерации квантовых ключей в канале позволило менять 256-битный ключ шифрования до двух раз в минуту. Источник: https://d-russia.ru/kvantovoe-shifrovanie-na-vols-s-rekordnym-rasstoyaniem-uspeshno-protestirovali-v-rossii.html

В масштабе региона кабельная квантовая сеть ВОЛС не имеет альтернатив, но на дальность >100км эта технология не эффективна, становится затратна, слаба, опасна. Транзитные узлы регенерации квантового сигнала, снижают безопасность системы связи. Сложная инфраструктура кабельных линий КРК требует больших затрат на обустройство, обслуживание и охрану узлов. Слабое звено безопасности - человеческий фактор с высоким уровнем неопределённости, пока не удаётся исключить из критической инфраструктуры.

Исторический факт, именно для обеспечения устойчивости связи, для решения ***фундаментальной проблемы государственной безопасности и обороны****, Агентство DARPA Министерства обороны США создало телекоммуникационную отказоустойчивую сеть ARPANET, так в 1969 году возник прототип современной мировой сети Интернет с маршрутизацией пакетов данных по протоколу IP.*

> ***Безопасность телекоммуникаций*** *– базовая, краеугольная мировая проблема. Эффективное решение обеспечит технологический суверенитет России, выведет на лидирующие позиции в мировой цифровой экономике на длительную перспективу.*

Технический прогресс разгоняется на волнах бурной революция телекоммуникаций. Магистрали ВОЛС многократно опоясали планету, подводные кабели соединили континенты в единую сеть Интернет. Регулярно каждые 10 лет идёт переход на новые поколения мобильной сотовой связи, каждые 5 лет появляются промежуточные стандарты. Мир стал глобальным, но проблема «цифрового неравенства» оставляет странам разные шансы на экономический успех, на технологический и государственный суверенитет. Кто неверно вкладывает, не успевает в темп прогресса, выпадает из эволюционной гонки, теряет технологический и политический суверенитет, платит лидерам высокую цену.

В XXI веке телекоммуникации - краеугольный камень цифровой экономики, государственной безопасности, управления, обороны, банковских транзакций, энергетики, транспорта, здравоохранения, с возрастающей ролью во всех областях социальной жизни.

Российские операторы сотовой связи бодро рапортуют о высоком уровне проникновения мобильной связи >172%. Действительно, количество проданных SIM-карт превышает численность населения, это - последствие национального роуминга до 2018г, реально сотовой связью покрыто <20% территории России, а зона мобильного интернета ещё меньше. Проблема «цифрового неравенства» остро стоит в России, 2/3 территории – вечная мерзлота, без сетевой энергетики, с проблемами прокладки кабельных сетей, с плотность населения менее 4 чел/км^2. **3/4 территории РФ фактически исключены из полноценной хозяйственной деятельности**. Невозможно 17 млн км^2, включая Арктику и Сибирь покрыть вышками сотовой связи, нет кабельных каналов, нет электросетей.

Печальнее всего, что каждый переход на новые поколения сотовой связи, в более скоростные высокочастотные диапазоны, сокращает зону покрытия, обостряется проблема «цифрового неравенства», и в России, и в мире. Наземные технологии 5G не имеют шансов выхода из центров мегаполисов. Традиционные наземные технологии кабельной и сотовой связи не рентабельны для покрытия территорий с низкой плотностью абонентов. И России, и миру необходимы экономически эффективные технологии телекоммуникаций 5G+.

Спутниковая связь метеозависима, чувствительна к помехам, допускает перехват сигнала в широких лучах радиоканалов, не обеспечивает безопасность телекоммуникаций без криптографического закрытия, не способна справиться с резко возрастающими объёмами данных даже для ограниченного числа абонентов. Дорогая фиксированная связь через абонентский терминал с громоздкой антенной физически и экономически не способна решить проблему «цифрового неравенства» ни в России, ни в мире. Коммерциализация спутниковой связи ограничена сегментами телевещания и телефонии над морем. Всё.

Спутниковая связь несовместима с сотовой связью, сигнал сотового телефона не доходит до орбиты, даже 2G. Проекты спутникового интернета не о связи, а о спасении ракетных программ. Спутниковый интернет сложнее, затратнее и проблемнее спутниковой телефонии, проекты (StarLink, OneWeb, …) коммерчески бесперспективны, без многомиллиардного государственного финансирования им предстоит путь к банкротству, более крутой и более короткий, чем у всех операторов спутниковой телефонии.

Оптическая связь через тропосферу метеозависима, возможна ясными ночами, ненадёжна, имеет ограниченные нишевые возможности, не подходит для построения надёжных сетей.

ВЫСОТНЫЕ ТЕЛЕКОММУНИКАЦИОННЫЕ ПЛАТФОРМЫ

Возможно новое экономически эффективное решение двух главных проблем связи: **магистральных каналов и «проблемы последней мили»**, как альтернатива и как органичное дополнение к существующим наземным магистральным кабельным оптоволоконным каналам и наземным технологиям сотовой связи. Кратко, 3 фактора:

1. Нет альтернативы подъёму базовых станций на оптимальную высоту (до 15-20 км) для увеличения зоны прямой видимости, **для снижения стоимости покрытия** связью обширных территорий с низкой плотностью абонентов.

2. С ростом высоты в тропосфере растёт скорость и стабильность ветра. Высотный ветер тропопаузы 9…12 км - надёжный глобальный возобновляемой источник энергии (ВИЭ) высокой плотности мощности ~10 кВт/м^2 с малыми суточными и сезонными колебаниями, **единственный** надёжный ВИЭ в умеренных и высоких широтах зимой.

3. Энергию высотного ветра способны взять только привязные высотные аэродинамические платформы на инновационных несущих роторах – **геостационарные атмосферные спутники (ГАС)**.

Нерационально поднимать тяжёлые аккумуляторы и пытаться собирать слабую солнечную энергию низкого Солнца днём для борьбы с высотным ветром, имеющим в 10 раз более высокую плотность мощности. Известные технологии атмосферных спутников с солнечными панелями ***неработоспособны*** *в умеренных и высоких широтах России. Пёстрый букет проектов летающих радио-ретрансляторов, способных раздавать 3G, дружно завял вместе с устаревшим стандартом. Базовой стации LTE, 5G нужна оптика.*

Высотные аэродинамические привязные платформы ГАС способны поднять базовые станции (BS) на тонком прочном леере с оптоволоконным каналом над узлами магистральной кабельной сети ВОЛС. Экологически чистые платформы с высоты 9…14 км с шагом ~200 км обеспечат сплошную зону покрытия в прямой видимости BS мобильной связи 5G макросотами радиусом до 100 км, площадью до 30 000 км^2. ГАС органично совместимы с наземными сетями сотовой связи и магистральной кабельной сетью. Технология ГАС глобальная, способна работать везде, кроме полюсов и экватора.

При стоимости, сопоставимой с мачтой сотовой связи, платформа ГАС выше в 300 раз, площадь покрытия больше в 300 раз. Каждая поднятая BS заменяет сотни наземных. На одном леере возможен подвес нескольких BS. В сравнении с наземными сотами капитальные и операционные **затраты покрытия снижаются на порядки** (на 1 порядок для линейных объектов, на 2 порядка для территорий). Экономически эффективная технология универсальна для покрытия связью 5G, как городов с плотной высотной застройкой, так и обширных территорий Арктики и Сибири без опорной инфраструктуры.

Энергетически автономная экологически чистая технология ГАС независима от сетей электроснабжения. **Стратосферные оптические каналы** (FSO, АОЛС) между платформами ГАС дают независимость от дорогой наземной кабельной сети ВОЛС. Свет в стратосфере распространяется без метео-помех, на 50% быстрее, чем в кабеле. Канал АОЛС в десять раз дешевле прокладки кабеля. На рынке есть модули FSO на 10-100 Gbps.

РЖД – драйвер развития технологии ГАС. Пилот в 2 этапа по 2 года:
1. 5 ГАС покроют 1000 км магистралей ОЖД.
2. 100 ГАС покроют 100% инфраструктуры ОАО «РЖД».
3. +500 ГАС покроют 100% России (включая Сибирь, Арктику, СМП, …).

СЕТЬ ГАРАНТИРОВАННОЙ БЕЗОПАСНОСТИ

SKYNET – сеть геостационарных атмосферных спутников (ГАС), аэродинамических привязных телекоммуникационных платформ на высотах 10 - 14 км, связанных стратосферными каналами лазерной связи (FSO) в транспортную стратосферную оптическую распределённую сеть.

SKYNET.RU 600 ГАС покроют 100% России базовыми сетевыми сервисами:

- **атмосферная оптическая сеть** 300т.км FSO-каналов гарантированной безопасности;
- **сеть сотовой связи 5G** IMT-2020, полное покрытие макро-сотами радиусом до 100км;
- **распределённая вычислительная сеть** 600 мини-ЦОД (edge computing +free cooling);
- **навигационная сеть** DGNSS высокой точности, поддержка и дополнение ГЛОНАСС;
- **сеть высотного видеомониторинга** инфраструктуры, территорий, акваторий, границ;
- **сеть цифрового вещания** федеральных и коммерческих каналов HDTV, UHDTV, …;
- **сеть аэронавигации**, управления воздушным движением, метео- и другие сервисы.

Одно из главных качеств SKYNET, как распределённой сети передачи данных – **контролируемые (доверенные) оптические каналы гарантированной безопасности,** исключает возможность скрытого несанкционированного доступа/перехвата/подмены на всём протяжении между любыми наземными доверенными узлами сети:

1. **Исключён доступ к вертикально поднятому оптоволокну** над контролируемыми (доверенными) наземными узлами связи, в точках входа/выхода сигнала, в точках сопряжения сети SKYNET с наземной региональной кабельной сетью КРК.
2. **Распределённая высотная оптическая сеть** (SDN) работает как шредер, тонко нарезает любую информацию на пакеты данных с разными маршрутами до адресата, обладает надёжностью, гибкостью, устойчивостью к отказам, метео-независимостью.
3. Физически невозможен доступ в стратосферные оптические каналы между подвижными платформами ГАС распределённой сети. Лишён практического смысла.
4. Энергетически автономная высотная распределённая сеть независима от электросетей.

Геостационарная атмосферная сеть SKYNET - доверенная телекоммуникационная оптическая сеть гарантированной безопасности, позволяет вести передачу данных на скоростях 10…100 Gbps без угрозы перехвата, подавления связи, без обязательного криптографического закрытия, имеет преимущества над альтернативными решениями по важнейшим параметрам: скорости сигнала, латентности, надёжности, устойчивости, энергетической автономности, стоимости. **Гарантированная безопасность** доверенной распределённой стратосферной оптической сети востребована для инфраструктуры ключей СКЗИ магистральных наземных каналов ВОЛС. Стратосферные оптические каналы по скорости передачи гарантированной безопасности в миллионы раз быстрее квантовой связи (кабельной, спутниковой), затраты в десятки раз ниже прокладки наземного кабеля.

Задачи Национальной программы Цифровая Экономика (НП ЦЭ), ФП устранения «цифрового неравенства», построения информационной инфраструктуры, невыполнимые на уровне существующих технологий имеют единственное экономически эффективное экологически чистое решение в рамках <4% бюджета госпрограмм.

Безопасная телекоммуникационная сеть – основа государственной безопасности России, обороны, современной цифровой экономики, финансов, логистики, всех сторон жизни граждан страны, управления инфраструктурой, субъектами Федерации, база развития экономики обширного региона ответственности на длительную перспективу. **Континентальная геостационарная атмосферная оптическая сеть SKYNET –** масштабный интеграционный геоэкономический проект. Чей?

БЕЗОПАСНАЯ МАГИСТРАЛЬНАЯ СЕТЬ

Технологии безопасных телекоммуникаций делают ставку на криптографию + КРК. Региональная оптоволоконная кабельная сеть КРК гарантирует безопасность на дальность до 100 км. Скорость квантовой передачи в кабеле обратно пропорциональна дальности связи, на дальность 60 км между узлами практичная скорость 300 kbps.

Протяжённые национальные сети на технологии «доверенных узлов» приемлемы для густой сети абонентов КРК, возможны в странах с высокой плотностью населения (Японии, побережья Китая, Западной Европы, …).

Транзитные узлы КРК не гарантируют безопасность. Магистральные линии КРК на цепочках транзитных узлов неэффективны, затратны и опасны на дистанциях России.

Так, магистраль кабельной квантовой связи (300bps) Москва – Санкт-Петербург требует 13 доверенных промежуточных узлов, через каждые 60 км. К проблеме охраны 640 км кабельной трассы, добавляется 13 новых режимных объектов с круглосуточной охраной. С учётом стоимости >600 км магистральной кабельной оптоволоконной сети, капитальные затраты на магистральную линию КРК составили более 3 млрд ₽.

- На квантовую магистраль протяжённостью 7000 км до 2024 выделяют 12.8 млрд ₽.
- В планах к 2030 году построить 15 тыс.км магистральной кабельной сети КРК.

Разрыв магистральных оптоволоконных каналов через каждые 60 км наносит ущерб инфраструктуре ИКТ, изымает резервные «тёмные волокна», делает каналы непригодными для скоростной магистральной связи, снижает надёжность сети, создаёт множественные цели для кибератак, потенциальные точки несанкционированного доступа.

Результаты пилотного внедрения линии КРК неоднозначны, и экономические, и технические последствия. Предметный анализ перспективного масштабирования, прямого и косвенного экономического ущерба нуждаются в более тщательной оценке, необходимо более широкое обсуждение за пределами круга заинтересованных лиц и организаций исполнителей конкретной технологии. Необходимо рассмотрение альтернативных, более эффективных решений.

Так, две высотные платформы ГАС над Москвой и Санкт-Петербургом имеют прямую радиовидимость. Две промежуточные платформы (над Новгородской и Тверской областями) обеспечат прямую оптическую видимость без метео-помех на дальности до 200км, образуют **гарантированно безопасную** гигабитную атмосферную оптическую связь. Распределённая геостационарная атмосферная оптическая сеть способна обеспечить надёжную **безопасную магистральную связь** между региональными кабельными сетями.

> *У двух технологий, кабельной квантовой и беспроводной оптической (FSO, WO), разрыв в скорости сигнала на 50% в стоимости (capex+opex) на один порядок, в производительности на 6-9 порядков.*

Объективные факторы: гарантированная безопасность, энергетическая автономность, максимальная скорость сигнала, минимальные задержки в распределённой сети SKYNET не оставляют аргументов игнорировать новую технологию.

Многофункциональная сеть SKYNET коммерчески высоко рентабельна, открываются качественно новые возможности, как покрытие России мобильной связью 5G, так и кратчайший путь в перспективные системы 6G беспроводной голографической радио-фотоники, реализуемой только в прямой видимости нескольких базовых станций, наземных и на разных высотах подвеса геостационарных атмосферных спутников.

Спутниковые оптические каналы дают квантовую связь на дальность >1000 км.
Опыты дальней квантовой передачи через пролетающий орбитальный ретранслятор показали возможность связи в прямой видимости через атмосферу в условиях ясной ночи одновременно на стороне передачи и зоне приёма. Низкая скорость (измеряемая bpm, битами в минуту), низкая вероятность одновременного стечения четырёх событий (видимости спутника и метеоусловий) на короткий период (1…7 минут) отражают низкую практическую ценность данного решения для связи между двумя наземными узлами, которые обязательно должны иметь и классический канал обмена данными.

Подъём высотных платформ ГАС над удалёнными узлами качественно меняет технологию дальней связи. Подъем передатчика и приёмника FSO над тропосферой одновременно увеличивает надёжность, безопасность, эффективность и практичность спутниковой КРК на дальние расстояния. Спутниковая беспроводная оптическая связь через высотные платформы ГАС, по схеме ГАС – (КА) – ГАС обеспечивает метео-независимую связь гарантированной безопасности без квантовых методов на высоких гигабитных скоростях, без необходимости дополнительных магистральных каналов. Появляется возможность **надёжной дальней связи** базы с удалёнными кораблями.

Периодически пролетающий орбитальный ретранслятор (КА) - необязательный элемент, может быть исключен из схемы или заменён на более надёжный **геостационарный ретранслятор**, один или несколько.

Атмосферные геостационарные ретрансляторы ГАС (с наземной базой/морские) надёжнее и экономически эффективнее орбитальных для ближней зоны, в АЗРФ, для СМП, имеют физически минимальные задержки сигнала в SDN-сети дальней морской связи.

Обе парадигмы безопасной связи: **«кабельная квантовая однофотонная»** и **«высокоскоростная мало-фотонная на бит данных»** фундаментально близки, имеют глубокое физическое обоснование гарантий безопасности, рациональны в комбинации для перспективных гетерогенных системах телекоммуникаций.

Объективные законы физики и экономики диктуют разумный баланс трёх технологий связи гарантированной безопасности: *региональной, магистральной и дальней:*

- **В региональной кабельной сети** до 100 км, рациональна технология кабельной КРК.
- Только **высотная оптическая сеть** способна обеспечить **магистральную связь гарантированной безопасности** между региональными кабельными сетями и узлами на гигабитных скоростях.
- Для **безопасной дальней связи** с наиболее удалёнными узлами/сетями/кораблями рациональна метео-независимая оптическая связь через **высотные платформы ГАС и высокоорбитальный** (HEO/GEO) **ретранслятор**.

База –оптоволокно–ГАС–FSO–(КА)–FSO–ГАС–оптоволокно–**Корабль/**

ПЕТРОВСКАЯ АКАДЕМИЯ НАУК И ИСКУСТВ
Специализированное Конструкторское Бюро
«GYRONAUTICA»

член-корреспондент ПАНИ
СЕО Кузиков С.Ю.
gyronautica@mail.ru
gyronautica.ru