



Заглянуть за горизонт
 К истории загоризонтной радиолокации

ИСТОРИЯ УСПЕХА



Космический щит
 России надежен

НОВОСТИ



85 лет на службе страны
 ВЧ-связь отмечает юбилей

ЮБИЛЕЙ



Аутернет бросает вызов
 В ближайшие год-два глобальная система Wi-Fi вытеснит платный Интернет

РЫНОК

ТЕМА НОМЕРА: На острие технического прогресса

ИСТОРИЯ УСПЕХА

Заглянуть за горизонт К истории загоризонтной радиолокации



Загоризонтный радиолокатор является не только средством добывания радиолокационной информации, но и мощным орудием интеллектуальной обработки этой информации, позволяющим решать задачи своевременного обнаружения подготовки воздушного нападения.

Из статьи Ю. М. Давыдова, кандидата технических наук, главного конструктора загоризонтной радиолокации в 1987–1996 гг.

Сегодня эти разработки занимают почетное место в музее. Они отличаются от стоящих на боевом дежурстве РЛС типа «Воронеж» настолько же, насколько героические «ишаки», успешно сражавшиеся в небе Испании, от современных СУ-35. Но когда-то они составляли основу отечественного противоракетного щита. Тридцать лет назад это был совершенно секретный объект — жемчужина советской космической разведки и мечта военных, не только позволявшая следить за перемещением всех видов надземных целей над Европой, но и дававшая возможность «видеть» пуски ракет потенциального противника на североамериканском континенте. С помощью мощнейших и ультрасовременных (на то время) радаров военные смогли в прямом смысле слова заглянуть за горизонт. Очевидно, именно благодаря таким способностям этот комплекс и получил свое название — загоризонтная радиолокационная станция (ЗГРЛС), или «Дуга-1».



ЗГРЛС типа «Дуга» (фото, опубликованное в еженедельнике «Военно-промышленный курьер»)

В Советском Союзе было создано всего три таких радара — в Николаеве, Комсомольске-на-Амуре и печально знаменитом Чернобыле. Уникальные способности радара кроются в новаторских идеях конструкторов, воплотившихся в исполинских размерах конструкций мачт и принимающих антенн. Трудно говорить о точных геометрических размерах ЗГРЛС. Данные открытых источников противоречивы и, вероятно, неточны. Так, высота мачт большой антенны составляет от 135 до 150 м, а длина — от 300 до 500 м. Второй радар несколько скромнее: порядка 250 м в длину и до 100 м в высоту. По данным некоторых источников, стоимость ка-

питаловложений составила 7 млрд советских рублей (хотя есть информация о 600–700 млн рублей). Для сравнения: это вдвое дороже, чем строительство Чернобыльской АЭС. Очевидно, что соседство с атомной электростанцией объясняется большим энергопотреблением объекта. Согласно имеющимся сведениям ЗГРЛС потребляла около 10 МВт. Загоризонтная радиолокация работает в диапазоне декаметровых радиоволн (5–0 МГц), используя свойство радиоволн указанного диапазона отражаться от ионосферы (эффект Кабанова). Ионосфера расположена на высоте 110–400 км в зависимости от сезонно-суточной ситуации и активности солнца.

Изменяя частоту и угол места излучения радиоволн, можно добиться освещения земной поверхности на дальностях от 600 до 10 000 км. В СССР работы над применением этой технологии для обнаружения стартов МРБ США начались в 1972 году в районе города Николаева, где был создан экспериментальный образец загоризонтной РЛС «Дуга-Н» (главный конструктор Ф. А. Кузьминский). Конструктивная зона обнаружения экспериментальной ЗГРЛС («Дуга-Н») была расположена в восточном направлении на дальностях от 3 до 10 000 км. В 1974–1975 годах были проведены пробные работы по оценке возможностей обнаружения воздушных

целей (ВЦ) типа Ту-16 на дальностях 1500–3000 км (руководитель работ Ю. К. Гришин). Результаты были обнадеживающие, но дальнейшее проведение работ на этом макетном аналоговом тракте не имело смысла.

В 1976-м начался второй этап создания опытного образца «Дуга-НМ» с цифровой обработкой сигналов на аппаратуре, аналогичной боевой ЗГРЛС «Дуга № 1», дислоцированной в районе Чернобыля. В 1976–1978 годах на опытном образце «Дуга-НМ» проводились натурные обнаружения пусков МБР на дальностях 6000–10000 км в рамках заводских и совместных испытаний

НОВОСТИ

Войска воздушно-космической обороны запустят военный спутник нового поколения в 2015 году

Войска воздушно-космической обороны (ВВКО) и промышленность постоянно работают над восполнением орбитальной группировки космического эшелона Системы предупреждения о ракетном нападении (СПРН). Об этом сообщили журналистам в Минобороны РФ.

Запуск первого космического аппарата нового поколения намечен на вторую половину 2015 года. Он будет выполнен с помощью ракеты-носителя «Союз».

«Никакой брешы в орбитальной группировке СПРН нет и не будет», — заверил представитель Минобороны. Он отметил, что «отличительная особенность космических аппаратов нового поколения для космического эшелона СПРН — больший по сравнению с аппаратами предыдущего поколения срок активного существования, улучшенные в разы тактико-технические характеристики». Спутники созданы на новой отечественной элементной базе. «Один такой новый спутник способен заменить 5–6 аппаратов прежнего поколения», — сказал собеседник.

Он подчеркнул, что одновременно развивается наземная составляющая СПРН за счет введения в строй новых РЛС высокой завод-

ской готовности. «Оба эшелона СПРН будут выполнять прежние задачи, но работать на качественно новом уровне и по совершенно новой схеме», — отметил представитель Минобороны.

По его словам, космический и наземный эшелон СПРН будут функционировать в максимально тесном взаимодействии, взаимно дополняя друг друга. Получаемая ими информация будет незамедлительно докладываться на командный пункт СПРН и затем — в Национальный центр управления обороной государства.

Как ранее заявил командующий ВВКО генерал-лейтенант Александр Головкин, «с 2015 года предусматривается развертывание Единой космической системы первого этапа развития, что позволит обеспечить наращивание возможностей по круглосуточному контролю ракетоопасных направлений».



**Начало на стр. 1**

боевого образца «Дуга № 1». Испытания прошли в целом успешно, однако выявили ряд технических трудностей, связанных с особенностями отражения сигнала от ионосферы. Это подвигло к поиску других направлений действия загоризонтной радиолокации, и в 1978 году по заказу ГУВ Войск ПВО была проведена экспериментальная отработка методов загоризонтного обнаружения воздушных целей. Сразу же было принято решение о цифровой обработке сигналов: с выходов приемника аналоговый сигнал преобразовывался аналого-цифровым преобразователем (АЦП) в цифру, а далее вся обработка осуществлялась в специализированной цифровой вычислительной машине (СЦВМ). Были разработаны и программно реализованы алгоритмы обнаружения, сопровождения (траекторная обработка) и др.

В июле 1978-го радиолокатор загоризонтного обнаружения (Николаев) посетил заместитель председателя Совета министров СССР, председатель Военно-промышленной комиссии Л. В. Смирнов. Была впервые поставлена задача по обнаружению крылатых ракет.

После создания экспериментального тракта начались натурные работы по обнаружению заказных самолетов Ту-16, МиГ-29 и попутных гражданских самолетов на трассе Уралск — Алма-Ата. Заказные самолеты вылетали с аэродрома в районе города Приозерска (Сары-Шаган) на дальности 3150 км. Ускоренной отработке алгоритмов очень помогло то, что реальные сигналы, отраженные от самолетов, в цифровом виде записывались на жесткие магнитные диски. Это позволяло пользоваться ими неоднократно различным группам разработчиков алгоритмов (метод распараллели-

вания) для отработки различных вариантов построения алгоритмов и выбирать из них оптимальные по таким критериям, как минимум отношения сигнал/шум и минимум ложных тревог.

В этот же период были проведены эксперименты по обнаружению пары самолетов, летящих на различных высотах — 10 000 и 300 м. Результаты обнаружения были равными. Это подтвердило предположение о том, что обнаружение самолетов не зависит от высоты (это стало предвестником обнаружения влета-посадки самолетов). Тогда же были разработаны критерии надежности обнаружения сигналов от ВЦ на основе спектрального анализа сигнала возвратно-наклонного зондирования (ВНЗ). Проведены различные эксперименты по обнаружению вертолетов, стартов ракет по корпусу, оценки спектров сигналов ВНЗ-1, сигналов, отраженных от различных типов самолетов.

В 1980 году НИОКР были завершены. Однако на вооружение «Дуга» принята так и не была. Точность результатов по пускам МБР, по мнению военных, оказалась недостаточно высока. Разработчики продолжили совершенствовать боевые алгоритмы: а) сопровождения; б) классификации состава цели — одиночная, групповая, количество самолетов в группе; в) классификации типа цели — тяжелый (Ту-16, Ил-62, Ту-154, Ту-134), легкий (МиГ-23, 25, 29) и др. В 1982 году началась модернизация «Дуги», что значительно улучшило ее боевые характеристики. Но в апреле 1986-го произошла авария на Чернобыльской АЭС и приемная позиция была закрыта (попала в 30-километровую зону отчуждения).

Тем не менее полученные наработки не пропали даром. Их логическим продолжением стала ОКР «Корона». Целью данной ЗГРЛС являлось

вскрытие подготовки и начала воздушного нападения. Для обеспечения указанной цели необходимо было осуществлять контроль воздушной обстановки в западном стратегическом направлении, районов дислокации 2 и 4-й ОТАК НАТО, 3-й ВА США, частично 5-й ОТАК и зоны Балтийских проливов. Как известно, в этих районах было сосредоточено свыше 2000 военных самолетов и еще больше гражданской авиации. Поэтому контроль за действиями военных самолетов должен был осуществляться на фоне полетов гражданских (пассажирских, грузовых) самолетов. Это требовало разработки базы данных, которая входила в вычислительный комплекс КП, и целого комплекса новых алгоритмов — системы интеллектуальной поддержки принятия решения (база знаний).

В соответствии с эскизным проектом ЗГРЛС «Корона» размещалась на двух позициях. Приемная позиция — в Могилевской области. В качестве передающей позиции использовалась та, что осталась от ЗГРЛС «Дуга № 1». Мощность станции возросла. Была предложена приемная антенна длиной 1200 м (256 мачт с четырьмя ярусами крестообразных вибраторов — две поляризации). ЗГРЛС «Корона» должна была увеличивать отношение сигнал/помеха не столько за счет увеличения энергетического потенциала передающей позиции, сколько за счет использования узких парциальных диаграмм направленности (ДН) приемной позиции, переключавших широкую ДН передаю-



щей антенны. На передающей позиции главным техническим вопросом была разработка линейно-частотно-модулированных (ЛЧМ) зондирующих сигналов, обладающих минимальным спектром внеполосных помех. В то же время передающая позиция, обладая высоким энергетическим потенциалом, могла служить средством РЭБ.

За время экспериментальных работ — с 1978 по 1988 год — было обнаружено более 400 вылетов самолетов (как одиночных, так и групповых), вертолетов, стартов баллистических ракет по корпусу и т. д. Это говорит о большом и тщательно проработанном комплексе работ и о готовности коллектива переходить к созданию ЗГРЛС «Корона».

Таким образом, к концу завершения эскизного проекта был готов

весь комплекс алгоритмов обнаружения, сопровождения, классификации, адаптации к ионосферной и помеховой обстановке, разработан комплекс конструкторской и строительной документации, изготовлены образец 32-канального приемника, устройство новых зондирующих сигналов (ЛЧМ) и др. Эскизный проект был принят в начале 1989-го, а в мае того же года министр радиопромышленности СССР и главнокомандующий ПВО СССР утвердили техническое задание на ОКР «Корона». Уже на этапе разработки конструкторской документации и изготовления аппаратуры в 1990 году были проведены интересные работы по обнаружению самолета-разведчика АВАКС в Северном море на дальности 2,5 тыс. км с помощью приемной антенны «Корона-Э» и передатчика. К середине 1990 года была разработана рабочая конструкторская документация, выданы ТЗ на программирование всех алгоритмов, поставлены на объект ЭВМ 66И6 и одна СЦВМ производства НИИДАР для отработки программного обеспечения. В 1990–1991 годах совместно с Институтом теплотехники (Москва) рассматривалось очень интересное предложение об увеличении эффективности тракта наведения.

А затем начался распад СССР, что в конечном счете привело к прекращению финансирования ОКР «Корона» и «Корона-Ю» со стороны ГУВ Войск ПВО России.

новости**Ракета-носитель «Рокот» со спутниками запущена с космодрома Плесецк**

Во вторник, 31 марта 2015 года, в 16 часов 48 минут (мск) с пусковой установки № 3 площадки № 133 Государственного испытательного космодрома Плесецк боевым расчетом Войск воздушно-космической обороны успешно осуществлен пуск ракеты космического назначения легкого класса «Рокот» с блоком космических аппаратов связи «Гонец-М» и космическим аппаратом в интересах Минобороны России. В результате на расчетные орбиты выведены три спутника связи «Гонец-М» и

космический аппарат Минобороны России, передает ТАСС. Старт «Рокота» был назначен на 3 марта, но пуск отложили по техническим причинам. По неофициальным данным, понадобились дополнительные проверки некоторых систем и приборов. Ракета-носитель легкого класса «Рокот» создана в рамках конверсионной программы на базе снимаемой с вооружения межконтинентальной баллистической ракеты РС-18. Изготовлением занимается космический центр им. М. В. Хруничева.

Площадка № 133 (также известна как «Радуга») — пусковая площадка на космодроме Плесецк, использовавшаяся с конца 1960-х годов для запусков полезной нагрузки с помощью ракет-носителей «Рокот». Она состоит из одной пусковой установки 133/3, первоначально обозначенной как 133/1. Изначально площадка была построена для запуска ракет-носителей семейства «Космос».

«Информационные спутниковые системы» представили в Москве свои новые разработки

Красноярская компания «Информационные спутниковые системы» им. академика М. Решетнёва» (ИСС) представила свои разработки для космических спутников на Московском международном салоне «Архимед».

«Все изобретения уже используются в производстве космических аппаратов. В числе новейших разработок — модель аппарата на базе платформы тяжелого класса «Экспресс-2000». Она показывает возможности ИСС в создании крупногабаритных спутников связи и вещания в интересах любых пот-

ребителей», — отметили на предприятии.

Кроме того, специалисты салона отметили стенд тепловакуумных испытаний, который предназначен для диагностирования тепловых режимов бортовой радиоэлектронной аппаратуры в условиях, имитирующих открытый космос. «Еще одно изобретение направлено на предотвращение несанкционированного доступа в спутниковых системах связи, — сказали в ИСС. — Оно может быть применено при создании полезной нагрузки спутника и в наземных узловых станциях».

**АКТУАЛЬНО****В Ярославском филиале — новый директор**

Одно из ключевых подразделений ПАО ЦНПО «КАСКАД» — Ярославский филиал возглавил Михаил Николаевич Пискунов. Это выверенное и взвешенное решение руководства Объединения. Его давно ожидали в коллективе и встретили с пониманием. Высокий профессионализм и большой личный вклад в развитие ЦНПО «КАСКАД» стали залогом этого решения. Михаил Николаевич, как и большинство руководящих кадров Объединения, имеет военное прошлое. В 1987 году он окончил Киевское высшее военное инженерное училище имени Калинина по специальности «электропроводная связь». В период с 1987

по 2004 год проходил военную службу на офицерских должностях в ВС РФ. Уволился из армии в воинском звании «подполковник». С 2004 года работал в различных организациях Московской области и Ярославля на инженерных должностях. Возглавляемый им филиал сегодня выполняет большой объем работ в интересах Минобороны, а также других ведомств Российской Федерации. Работу филиала всегда отличали высокий инженерный уровень и качество.

Пожелаем Михаилу Николаевичу и впредь держать высокую планку Ярославского филиала в лучших традициях ЦНПО «КАСКАД».

ЮБИЛЕЙ

85 лет на службе страны

ВЧ-связь отмечает юбилей

В начале 1930 года, 85 лет назад, были сданы в эксплуатацию первые в СССР линии высокочастотной связи Москва — Ленинград и Москва — Харьков. На тот момент это была передовая технология, которая встала на службу стране. Кстати, и ее научное обоснование созрело именно в России, а первые инженерные решения создавались при активном участии специалистов ПМТ-5.

В 1918 году академик М. В. Шулейкин (в 1918–1921 годах начальник радиотехнической лаборатории главного военно-инженерного управления) теоретически обосновал возможность организации высокочастотной связи по проводам. Тема являлась весьма актуальной, поскольку в том же году правительство РСФСР переехало в Москву и государственную связь надо было создавать заново. До этого междугородная связь, в том числе государственная, осуществлялась посредством телеграфных линий.

По сравнению с телеграфной высокочастотная связь обладала рядом преимуществ. Основное ее достоинство состояло в том, что она вносила в условия передачи распоряжений и получения информации элемент личного общения. Но вызовы, стоявшие тогда перед молодой республикой, не позволяли немедленно отказаться от телеграфа. Так, связь с фронтами и флотами в Гражданскую осуществлялась преимущественно по телеграфу.

Следует заметить, что значение телеграфной связи не уменьшилось вплоть до 50-х годов XX века. Долгое время телеграф и ВЧ-связь дублировали друг друга. Некоторые виды телеграфов (в частности, аппарат Бодо, ставший важной вехой на пути разви-

сформировано 5-е отделение оперативного отдела ОГПУ с целью создания и эксплуатации междугородной государственной телефонной связи. В 1930-е годы активно велось строительство магистральных воздушных линий связи, использовавшихся прежде всего для нужд междугородной государственной ВЧ-связи, а также оборудование территориальных и региональных ВЧ-станций.

В 1934 году на заводе «Красная Заря» в Ленинграде (бывший «Эрриксон») закончилась разработка и начался крупносерийный выпуск трехканальной аппаратуры высокочастотного телефонирования СМТ-34, работающей в диапазоне 10,4–38,4 кГц и обеспечивающей удовлетворительное качество связи на расстоянии до 2000 км. Эта аппаратура выпускалась вплоть до Великой Отечественной войны, ею были оборудованы все основные магистрали дальней связи СССР.

В 1935 году для самой длинной в мире магистрали Москва — Хабаровск была выпущена трехканальная аппаратура СМТ-35, находившаяся на уровне лучших мировых образцов. В том же году на базе отдела ВЦИК образован отдел технической связи управления коменданта Московского Кремля под руководством Г. Д. Любимова. Однако технология передачи вы-



же полностью доверять нельзя. Отметим, что эти люди работали в системе НКВД, а не Наркомата связи (НКС), поэтому и требования при приеме на работу к ним были строже.

В 1937 году первая информация о возможности перехвата поступила от агента НКВД БССР, которая в полутора километрах от границы на территории Польши обнаружила специальное подключение к линии связи Москва — Варшава. В 1938 году начальник отделения государственной ВЧ-связи СССР И. Воробьев в одном из рапортов указал, что спецсвязь НКС, которой пользуются абоненты Кремля, не обеспечивает никакой секретности разговоров, так как эта связь предоставляется Кремлю в известные часы и разговор членов правительства проходит через аппаратуру НКС, обслуживаемую тем же техническим составом, который обслуживает и коммерческие разговоры. Пришлось в срочном порядке проложить специальный кабель, соединяющий станцию высокочастотной связи с АТС Кремля.

В столице было много других правительственных зданий, которые пользовались услугами городской телефонной сети. С целью обеспечения конфиденциальности и предотвращения перехвата разговоров по ВЧ-связи в исследовательской лаборатории НКС были изготовлены специальные защитные фильтры, которыми оборудовались все междугородные телефонные линии, уходившие за границу. Позднее, в начале 1941 года, в Таллине установили изготовленную в лаборатории оригинальную аппаратуру «шумовой завесы», которая практически предотвращала возможность

перехвата переговоров. В первом полугодии было налажено производство такой аппаратуры для Москвы, Ленинграда, Риги. Инженеры «Красной Зари» также понимали проблему. Еще с 1935 года постоянно велись работы над усовершенствованием подобной аппаратуры, а вскоре было создано первое отечественное устройство автоматического засекречивания телефонных переговоров — инвертор ЕС (назван по первым буквам фамилий создателей — К. П. Егорова и Г. В. Старичина) и налажен его выпуск.

Государственная связь уверенно становилась самостоятельной отраслью народного хозяйства, которая требовала специфических специалистов, инженерных разработок и промышленных мощностей. В 1938 году последовательно вышли три постановления СНК СССР: № 53/ко от 5 января, № 454-97сс от 9 апреля и № 1240-300сс от 17 ноября «О развитии государственной высокочастотной связи». В состав отдела связи управления коменданта Московского Кремля на январь 1939 года входило 14 подразделений, включая мастерские и склады. В апреле 1941-го аппаратура простого засекречивания стояла уже на 66 из 134 линий государственной ВЧ-связи. 6 мая 1941 года распоряжением СНК СССР утверждено Положение о порядке эксплуатации государственной ВЧ-связи. К началу Отечественной войны высокочастотная телефонная связь была организована с большинством столиц союзных республик, многими областными центрами, военными округами.

Продолжение следует.

Шмаков Павел Васильевич (1885–1982)

Советский ученый в области телевидения и радиотехники. Заслуженный деятель науки и техники РСФСР (1948). В 1913 году окончил Московский университет. С 1921-го преподавал в Институте народного хозяйства в Москве, с 1924-го — в Московском высшем техническом училище, а затем — в Московском энергетическом институте. С 1937 года профессор Ленинградского электротехнического института связи. В 1924 году совместно с М. В. Шулейкиным организовал дуплексную радиотелефонную связь с движущимся поездом. В 1927-м под его руководством была установлена дальняя фототелеграфная связь (Москва — Берлин), в 1931-м разработано малостроичное телевизионное вещание в СССР, в 1955-м — телевизионная система для исследования буровых скважин. Автор ряда изобретений, в том числе системы ультразвукового телевидения (авторское свидетельство № 2238, 1933), усовершенствования конструкции передающей телевизионной трубки с переносом изображения (авторское свидетельство № 45698, 1933, совместно с П. В. Тимофеевым). Также занимался разработкой вопросов цветного и объемного телевидения.



П. В. Шмаков — выдающийся российский инженер, создатель советского телевидения и систем связи

тия этого типа связи) имели высокую степень криптозащиты. Во время ВОВ на всех телеграммах Сталина, поступавших в узел государственной связи, особенно в первые месяцы, непременно стояла пометка: «Передать только по Бодо». Сталин довольно часто вел переговоры с командующими фронтами и армиями. И считалось, что именно аппарат Бодо исключал возможность перехвата сообщений противником.

В 1923 году видные отечественные ученые П. В. Шмаков и В. А. Куприянов практически подтвердили возможность ВЧ-телефонирования. А в 1929-м при одном из управлений ОГПУ было создано отделение государственной связи.

Перед промышленностью была поставлена задача в короткие сроки создать аппаратуру, способную обеспечивать качественную телефонную связь в интересах правительства. Приказом ОГПУ от 10 июня 1931 г. № 308/183 было

сокочастотного сигнала также оказалась небезупречна. Впервые об уязвимости ВЧ-связи можно прочесть в рапорте старшего техника-инженера М. Ильинского на имя начальника 13-го отделения оперативного отдела ГУГБ НКВД СССР И. Воробьева. Документ датирован 8 августа 1936 года. Основные источники угроз — агенты иностранных спецслужб среди обслуживающего персонала и использование различных портативных и простых в обслуживании технических средств. В ходе испытаний, проведенных в том же году вблизи Минска, была выявлена возможность перехвата разговоров на радиоприемник с длинноволновым диапазоном при помощи антенны, подвешенной на расстоянии ближе 50 м от междугородной цепи. В другом документе, появившемся в феврале 1937 года, есть фраза о том, что разговоры могут подслушиваться (и слушаются) нашими работниками ВЧ-связи, а им так-

НОВОСТИ

Космический щит России надежен

Согласно открытым источникам Россия с апреля по июнь 2015 года планирует осуществить девять космических пусков: семь — с космодрома Байконур с космическими аппаратами различного назначения, два — с Плесецка в интересах Минобороны РФ. За аналогичный период 2014 года Россия провела 11 пусков: девять — с Байконура, Плесецка и полигона Домбаровский, один — с «Морского старта». При участии российских специалистов был также проведен один старт «Союза-ST» с европейского космодрома Куру во Французской Гвиане.



В планах стартовых площадок Байконура: пуск грузового корабля «Прогресс М-27М» к МКС (назначен на 28 апреля на «Союзе-2.1А»). Старт ракеты-носителя «Протон-М» со спутником MexSat-1 намечен на 29 апреля. Еще один «Протон-М» со спутником в интересах Минобороны РФ планируется запустить 19 мая. Следующая экспедиция космонавтов на МКС будет запущена в корабле «Союз ТМА-17М» 26 мая на «Союзе-ФГ». Спутник Inmarsat-5 F3 на «Протоне-М» будет запущен 31 мая. Спутник связи «Экспресс-АМВ» на «Протоне-М» намечено вывести

на орбиту 18 июня, а космический аппарат TurkSat-4B на аналогичном носителе — 30 июня.

По словам источника, с космодрома Плесецк на 15 мая запланирован пуск «Союза-2.1А» со спутником в интересах Минобороны РФ. Кроме того, на 5 июня намечен старт второго «Союза-2.1Б» с другим космическим аппаратом также в интересах военных. Однако источники подчеркивают, что указанные даты могут существенно меняться в зависимости от реальных сроков подготовки космических аппаратов и носителей к пуску.

Правительство утвердило новые антитеррористические правила



Премьер-министр Дмитрий Медведев утвердил новые правила антитеррористической безопасности. Все места массового пребывания людей: парки, кафе, торговые центры, улицы, площади — разграничены по степени террористической угрозы. Все объекты вместимостью больше 50 человек должны иметь паспорта безопасности и быть оснащены системой оповещения и видеонаблюдения, записи с которых хранятся до 30 дней. Мероприятия с участием более 1 тыс. человек должны предварять обследования кинологов с собаками.

Площадки вместимостью от 200 до 1 тыс. человек должны быть дополнительно оборудованы стендами со схемами эвакуации, телефонами спецслужб и владельцев объекта. Наконец, публичные пространства, где могут поместиться свыше 1 тыс. человек, должны удовлетво-

рять всем перечисленным требованиям, а непосредственно перед мероприятиями обследоваться кинологами с собаками. Каждое общественное пространство вне зависимости от категории также должно иметь паспорт безопасности. В нем необходимо указывать сведения о работах и арендаторах находящихся рядом помещений, потенциально опасных участках, а также приводить оценку «возможных социально-экономических последствий» теракта.

Разработчиками проекта постановления правительства «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)» выступили представители МВД. Документ предлагает каталогизировать все общественные места с учетом степени потенциальной опасности и угрозы терактов. Оценивать степень угрозы предстоит территориальным межведомственным комиссиям, в которые входят сотрудники органов местного самоуправления, ФСБ, МЧС и полиции.

РЫНОК

Аутернет бросает вызов

В ближайшие год-два глобальная система Wi-Fi вытеснит платный Интернет

Ученые активно оперируют понятиями «биосфера», «ноосфера», но технологии развиваются столь стремительно, что вскоре уже можно будет без всякой натяжки говорить об «инфосфере» Земли. Сотни спутников обеспечат круглосуточный доступ к Wi-Fi. Проект под названием Outernet навсегда изменит коммуникации между людьми.

Важная особенность проекта заключается в том, что услуга доступа по Wi-Fi будет предоставляться бесплатно. Это означает массовое банкротство компаний-провайдеров и... монополизацию информационной среды. Насколько серьезна эта опасность? Как известно, ПАО ЦНПО «КАСКАД» имеет соответствующие лицензии на предоставление интернет-услуг, то есть также является интернет-провайдером. Чего можно ждать от рынка в самое ближайшее время? Наши эксперты постарались разобраться.



Сайед Карим,
директор MDIF по инновациям

Как заверяют инициаторы, надо отдать должное, уникальнейшего в истории человечества проекта, они, дескать, заботятся об интересах стран и регионов, где на данный момент существует цензура¹ на интернет-пространство или вообще отсутствует доступ в Интернет. Бесплатный выход в Сеть земляне получат уже через полтора года, заявили авторы проекта из Инвестиционного фонда по медиаразвитию США (Media Development Investment Fund — MDIF). Разработчики уточнили, что первое время свободный доступ будет предоставляться только к определенным веб-сайтам. На данный момент в мире больше цифровых устройств, чем людей, но лишь 60 % населения планеты имеет доступ в Интернет. Во многих сельских населенных пунктах и отдаленных регионах нет ни вышек сотовой связи, ни проводного доступа к информационной сети. Основатели Outernet надеются, что, когда проект будет запущен, Интернет станет по-

настоящему свободным — к Сети смогут подключиться даже жители стран вроде Северной Кореи, где Интернет запрещен государством. Американцы хотят покончить с дефицитом Интернета.

В 2015 году американская организация MDIF начнет создание новой мировой сети доступа в Интернет под названием Outernet (проект является инициативой Сайеда Карима, директора MDIF по инновациям). Предоставление услуг доступа в Интернет планируется обеспечить через мощную группировку малых и сверхмалых искусственных спутников Земли CubeSat, имеющих объем 1 л и массу 1,33 кг или несколько (кратно) больше. Их создание оказалось возможным благодаря развитию микроминиатюризации и нанотехнологий и стало массовым явлением в XXI веке. В компании планируют разместить на околоземной орбите множество миниатюрных кубических спутников CubeSat и с их помощью покрыть сетью Wi-Fi весь земной шар. Спутниковая сеть будет работать по нескольким распределенным протоколам, включая DVB, Digital Radio Mondiale и многоадресные рассылки, передаваемые по протоколу UDP. Запуск первых спутников состоялся в январе 2015 года. Тестирование оборудования начнется уже через несколько месяцев. Благодаря спутниковой сети можно будет передавать любые интернет-данные через Wi-Fi сигнал, находясь в любой точке планеты, и ничего за это не платя.

Стоит заметить, что спутники будут предоставлять интернет-доступ не с самого момента своего появления на орбите. Сперва они будут использоваться в целях односторонней коммуникации — для передачи срочных сообщений, новостей, цен на урожай и обучающих программ. Пользователи системы помогут определить, какой контент им следует предлагать.

Команда, стоящая за этим проектом, заявляет, что свободный доступ к информации — фундаментальное право человека, поэтому она намерена предоставить доступ к Сети даже в тех странах, где диктаторы его ограничивают. «Мы существуем, чтобы поддерживать поток свобод-

ных новостей, данных и дебатов, которые необходимы людям, чтобы построить свободные, процветающие сообщества», — говорит президент MDIF Питер Уайтхед.

Сам Сайед Карим считает, что пройдет как минимум пять лет, прежде чем Outernet сможет предложить более интерактивный интернет-доступ, который позволит людям как получать, так и загружать информацию. По его мнению, добиться повсеместного распространения Интернета можно и гораздо быстрее, если телеком-гиганты вложатся в несколько суперспутников вроде североамериканского ViaSat-1. Три года и 12 млрд долларов — и работа будет сделана. «У нас нет 12 миллиардов, поэтому мы сделаем все, что только сможем, с помощью CubeSat», — говорит Карим.

А если не 12 млрд, то сколько это будет стоить? Отправка на орбиту груза размером 10 см³ стоит 100 тыс. долларов. Самый крупный спутник Outernet имеет габариты 34 × 10 × 10 — его запуск обойдется более чем в 300 тыс. Теперь уменьшите это на сотни спутников. «Мы хотим, чтобы спутники оставались настолько маленькими, насколько это возможно, ведь размер и вес напрямую транслируются в доллары», — заявляет Карим. — Габариты в основном диктуются потребностями в энергии, поскольку для их удовлетворения необходимо устанавливать солнечные панели». Пока инженеры Outernet тестируют устройства, они ждут поддержки от всех, кто верит в цель их проекта. В дополнение к традиционным ресурсам для пожертвований вроде PayPal они также принимают онлайн-валюту, например Bitcoin и Dogecoin. Специалисты компании надеются на настоящий прорыв и на то, что им действительно удастся сделать доступ в Интернет (причем конфиденциальный) всеобщим достоянием.

Тогда географическое расположение перестанет иметь значение — потребуется только устройство, принимающее Wi-Fi сигнал. Outernet будет представлять собой аналог гигантского Wi-Fi-роутера, накрывающего всю планету и не требующего пароля для подключения. К сети можно будет подключиться

абсолютно бесплатно через любое Wi-Fi-совместимое устройство. Уже в 2015 году в MDIF планируют начать сборку космических аппаратов, принимающих участие в проекте. Для этого понадобятся десятки, а то и сотни миллионов долларов, которые фонд рассчитывает собрать через добровольные пожертвования. Если все сложится так, как планируют в MDIF, корпорация попросит НАСА провести тестирование технологии на МКС.

Предполагается, что Outernet будет транслировать международные и локальные новости, информацию о ценах, цепочки блоков Bitcoin, курсы английского от Британского Совета, прочую обучающую информацию, программное обеспечение, музыку, видео, всю «Википедию» и т. д. Также в Outernet окажутся доступны каналы для экстренной связи со службами спасения, для координации усилий спасательных команд, начнет функционировать глобальная система оповещения. Полноценный двусторонний канал работы с Интернетом в рамках Outernet пока не будет доступен, но в планах он есть. Обмен данными планируется осуществлять по традиционному для Интернета протоколу UDP. Участники Outernet смогут голосовать за то, какой контент должен транслироваться, определяя приоритетный список информации. Повлиять на приоритеты можно будет с помощью СМС или специальных приложений для мобильных устройств. Пользователи также смогут предлагать для трансляции собственный контент, отправив запрос с официального сайта.

Кстати, несколько месяцев назад с подобной инициативой выступил и поисковый гигант Google. В секретной лаборатории GoogleX сейчас работают над новым проектом Project Loon. Это доступ в Интернет с воздушных шаров для территорий, для которых наземный Интернет не лучший вариант. Воздушные шары, паря в стратосфере, смогут предоставлять доступ в Сеть на уровне 3G. На данный момент компания уже запустила пилотный проект, который включает 30 шаров на территории Новой



Зеландии и около 50 станций, тестирующих сервис с Земли. Ранее аналитики предположили, что к 2033 году пользователи забудут понятие «Интернет». Сама Всемирная сеть останется, но люди будут заменять это слово названиями услуг, которые поставляются с ее помощью. Предполагается, что выходить онлайн можно будет через стиральную машину или холодильник.

Кроется ли в этой технологии опасность? Определенная — безусловно. Использование Интернета в военных целях уже давно не фантастика (подробнее см. «Вестник» № 10–11 за 2010 г.). До сих пор его слабыми звеньями были именно ограниченность территории покрытия и слабая защита от средств РЭБ. С появлением столь мощной и многочисленной спутниковой группировки эти проблемы решатся. Вывод из строя даже нескольких спутников не будет существенно влиять на качество сигнала. Появляется дополнительный (дублирующий) канал связи, который для всего мира будет контролироваться с территории США. То есть теоретически может наступить момент, когда, при разрушении основных каналов, он окажется единственным. Монополизация всегда опасна, а монополизация информации опасна вдвойне.

Есть также вероятность использования Outernet в террористических и экстремистских целях, поскольку на сегодняшний день неясен вопрос о контроле контента. Если до сих пор за него отвечал провайдер, то здесь, при отсутствии провайдера как такового, может возникнуть ситуация как тотального информационного хаоса. Перечисленные вопросы еще предстоит обсудить экспертам. Это, несомненно, вызов. Готова ли Россия ответить на него адекватно? Будущее покажет.

Этапы запуска Outernet

- Июнь 2014 года: выпуск первых спутников-прототипов и тестирование ограниченности территории покрытия и слабая защита от средств РЭБ.
- Сентябрь 2014 года: тестирование качества трансляции из космоса (идут переговоры о размещении тестового оборудования на Международной космической станции).
- Январь 2015 года: запуск на орбиту и тестирование работы в групповом режиме нескольких спутников.
- Апрель 2015 года: организация поточного производства спутников.
- Июнь 2015 года: запуск, настройка, ввод в эксплуатацию сети Outernet.
- (Endnotes.)

Есть также вероятность использования Outernet в террористических и экстремистских целях, поскольку на сегодняшний день неясен вопрос о контроле контента. Если до сих пор за него отвечал провайдер, то здесь, при отсутствии провайдера как такового, может возникнуть ситуация как тотального информационного хаоса. Перечисленные вопросы еще предстоит обсудить экспертам. Это, несомненно, вызов. Готова ли Россия ответить на него адекватно? Будущее покажет.

Этапы запуска Outernet

- Июнь 2014 года: выпуск первых спутников-прототипов и тестирование ограниченности территории покрытия и слабая защита от средств РЭБ.
- Сентябрь 2014 года: тестирование качества трансляции из космоса (идут переговоры о размещении тестового оборудования на Международной космической станции).
- Январь 2015 года: запуск на орбиту и тестирование работы в групповом режиме нескольких спутников.
- Апрель 2015 года: организация поточного производства спутников.
- Июнь 2015 года: запуск, настройка, ввод в эксплуатацию сети Outernet.
- (Endnotes.)

¹ Напоминаем, что в Российской Федерации согласно п. 5 ст. 29 Конституции РФ цензура запрещена.

Протокол UDP (англ. User Datagram Protocol — протокол пользовательских датаграмм) — один из ключевых элементов Transmission Control Protocol/Internet Protocol, набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения (в данном случае называемые датаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных. Протокол был разработан Дэвидом П. Ридом в 1980 году и официально определен в RFC 768. UDP использует простую модель передачи, без неявных «рукопожатий» для обеспечения надежности, упорядочивания или целостности данных. Таким образом, UDP предоставляет ненадежный сервис, и датаграммы могут прийти не по порядку, дублироваться или вовсе исчезнуть без следа. UDP подразумевает, что проверка ошибок и исправление либо не нужны, либо должны исполняться в приложении. Чувствительные ко времени приложения часто используют UDP, так как предпочтительнее сбросить пакеты, чем ждать задержавшиеся пакеты, что может оказаться невозможным в системах реального времени. При необходимости исправления ошибок на сетевом уровне интерфейса приложения может задействовать TCP или SCTP, разработанные для этой цели.