Июль 2006 г. *Том 176, № 7*

УСПЕХИ ФИЗИЧЕСКИХ НАУК

КОНФЕРЕНЦИИ И СИМПОЗИУМЫ

Научная сессия Отделения физических наук Российской академии наук, посвященная памяти академика Владимира Александровича Котельникова

(22 февраля 2006 г.)

22 февраля 2006 г. в конференц-зале Физического института им. П.Н. Лебедева РАН состоялась Научная сессия Отделения физических наук Российской академии наук, посвященная памяти академика Владимира Александровича Котельникова. На сессии были заслушаны доклады:

1. **Гуляев Ю.В.** (Институт радиотехники и электроники РАН). *О Владимире Александровиче Котельникове* (вступительное слово).

2. **Котельникова Н.В.** *Владимир Александрович Котельников*: *дорога ученого*.

3. **Арманд Н.А.** (Институт радиотехники и электроники РАН). *Роль В.А. Котельникова в становлении радиофизики и радиотехники*.

4. **Сачков В.Н.** (Академия криптографии Российской Федерации). *В.А. Котельников и отечественная шифрованная связь*.

5. **Молотков С.Н.** (Институт физики твердого тела, г. Черноголовка, Московская обл., Академия криптографии Российской Федерации, Московский государственный университет им. М.В. Ломоносова, факультет вычислительной математики и кибернетики). *Квантовая криптография и теоремы В.А. Котельникова об одноразовых ключах и об отсчетах*.

6. **Черток Б.Е.** (Российская космическая корпорация "Энергия"). *В.А. Котельников и его роль в развитии отечественной космической радиоэлектроники*.

7. **Победоносцев К.А.** (Особое конструкторское бюро Московского энергетического института). *В.А. Котельников как выдающийся инженер и его роль в становлении Особого конструкторского бюро Московского энергетического института*.

Краткое содержание первых шести докладов публикуется ниже.

Владимир Александрович Котельников
(06.09.1908 – 11.02.2005)

PACS numbers: **01.60.+q**

О Владимире Александровиче Котельникове (вступительное слово)

Ю.В. Гуляев

Вот уже год, как ушел из жизни крупнейший ученый в области радиотехники, радиофизики и информатики — академик Владимир Александрович Котельников. С именем Котельникова связана целая эпоха развития

этих важнейших областей науки и техники начиная от систем связи и цифровых вычислительных машин и кончая широкомасштабными исследованиями космического пространства. Теорема Котельникова "вошла в азбуку" образования любого инженера в области систем связи и информатики, теория потенциальной помехоустойчивости, созданная Котельниковым, составляет фундамент всех современных систем связи, радиолокации, радионавигации и телеуправления. Его работы в области радиолокационной астрономии по праву вошли в золотой фонд мировой науки и техники.

Мне выпало счастье работать с Владимиром Александровичем более 45 лет. Позвольте кратко напомнить основные вехи жизненного пути этого замечательного человека.

Выдающийся ученый В.А. Котельников окончил Московский энергетический институт (МЭИ) в 1930 г., получив специальность инженера-электрика по радио, и начал работать инженером в Институте связи Красной Армии, затем поступил в аспирантуру МЭИ (1931 г.) и после ее окончания (1933 г.) стал работать в Научно-исследовательском институте наркомата связи. В то время средства передачи информации были весьма несовершенными, и проблема борьбы с помехами в проводных системах связи требовала кардинально быстрого решения. На начальной стадии своей научной деятельности В.А. Котельников искал пути увеличения эффективности систем связи. В 1933 г. им написана и опубликована фундаментальная работа "О пропускной способности "эфира" и проволоки в электросвязи", в которой впервые сформулирована теорема (известная в радиотехнике как теорема Котельникова) о точном представлении функции с ограниченным спектром совокупностью ее отсчетов, произведенных в отдельно взятых точках. Важно отметить, что позднее эта теорема легла в основу цифровой обработки и передачи сигналов и создания цифровых вычислительных машин, используется при изучении ряда закономерностей в радиофизике и оптике. В.А. Котельников первым сумел осознать всю глубину технических выводов, вытекающих из нее, и фактически придал ей глубокий физический смысл.

В годы Великой Отечественной войны В.А. Котельников занимался созданием аппаратуры специальной связи, за эти разработки был дважды удостоен Государственной премии (1943 и 1946 гг.). В 1947 г. он защищает докторскую диссертацию, в которой изложена теория потенциальной помехоустойчивости, где впервые установлены предельные ограничения чувствительности радиоприемных устройств, обусловленные шумами, и созданы теоретические основы выделения сигналов из помех. Монография *Теория потенциальной помехоустойчивости* получила широкую известность и была издана в нашей стране и за рубежом. Вплоть до настоящего времени теория помехоустойчивости является в мире одной из основных, используемых при разработке систем связи, радиолокации, телеуправления и других радиотехнических систем. Все это вместе взятое принесло В.А. Котельникову мировое признание.

Новый период научной деятельности В.А. Котельникова начинается с момента его избрания действительным членом Академии наук СССР и назначения директором Института радиотехники и электроники (ИРЭ) АН СССР, когда полностью раскрывается его талант крупнейшего ученого, организатора и руководителя большого коллектива. Всю свою энергию и талант он направляет на поиск интересных и многообещающих путей решения различных научных проблем, на становление и развитие фундаментальных исследований: в области дальнего тропосферного распространения ультракоротких радиоволн, волноводных систем связи, выделения слабых сигналов из шумов, обработки и передачи информации, а также в области генерации, усиления и приема сигналов на сантиметровых и дециметровых волнах. Он проводил большую организаторскую работу по привлечению в институт наиболее крупных и талантливых физиков с их сложившимися коллективами.

Сегодня можно только удивляться прозорливости и интуиции В.А. Котельникова, проявленных им при постановке ряда новых фундаментальных проблем современной радиоэлектроники. Так, под его руководством и при непосредственном участии получили свое развитие проблема освоения новых диапазонов радиоволн — миллиметрового, субмиллиметрового, оптического и сверхнизкочастотного, статистическая радиофизика, дистанционное зондирование атмосферы, поверхности Земли и планет; были созданы новые научные направления — планетная радиолокация и радиолокационное изучение планет с помощью космических аппаратов; начаты работы по волноводным и стекловолоконным широкополосным системам связи. (Подробнее результаты этих исследований изложены в работе В.А. Котельникова и К.И. Палатова "Исследования в области радиотехники и электроники, проведенные в ИРЭ АН СССР в 1953–1978 гг.", в сб. *Проблемы современной радиотехники и электроники* (Под. ред. В.А. Котельникова) (1980).) В.А. Котельников активно поддерживал работы в области теоретических основ микроэлектроники, оптоэлектроники, сверхпроводниковой электроники, полупроводниковой электроники, акустоэлектроники, магнитоэлектроники, кристаллофизики, автоматизации научных исследований и уделял этим работам особое внимание. Вклад в развитие каждого из этих направлений не ограничивался только его научно-организационной деятельностью, он всегда принимал самое активное участие в разработке наиболее трудных научных проблем. Будучи длительное время председателем Совета Интеркосмоса, он являлся бессменным научным руководителем многих научно-исследовательских работ по радиолокационному изучению планет Солнечной системы и космического пространства. Многие результаты научных исследований послужили основой для разработки различных радиоустройств и систем на предприятиях бывших министерств радиопромышленности, электронной промышленности, электротехнической промышленности, оборонной промышленности, промышленности средств связи, а также на предприятиях минестерства связи и других ведомств.

Благодаря трудам В.А. Котельникова, его учеников и коллег относительная точность измерения расстояний в радиолокационной астрономии была доведена до 10^{-8} от измеряемой величины. Это позволило уточнить размеры Солнечной системы и глубже понять закономерности движения планет. По инициативе В.А. Котельникова при радиолокации планет были использованы антенна и передатчик Центра дальней космической связи, что позволило принимать слабые отраженные сигналы от Венеры, Меркурия, Марса и Юпитера, а также отражен-

ные сигналы от кометы Галлея и ряда крупных астероидов.

В.А. Котельников активно поддерживал организацию полетов межпланетных космических кораблей. Им вместе с коллегами впервые уточнена астрономическая постоянная, что позволило обеспечить необходимую точность управления космическими аппаратами. После ряда фундаментальных исследований (1984–1992 гг.) впервые в мире было осуществлено картографирование северной части планеты Венера выше 30° с.ш. на площади около 115 млн км с разрешением 1–2 км с помощью автоматических межпланетных станций "Венера-15" и "Венера-16", а также изучены атмосфера и ионосфера этой планеты в рамках проекта "Вега". Проведены исследования точности релятивистской теории движения планет, начато изучение солнечного ветра, ближнего космоса и земной поверхности с помощью космических аппаратов и искусственных спутников Земли.

Свидетельством международного признания научных заслуг В.А. Котельникова является его избрание Почетным членом Международного института инженеров по электронике и радиоэлектронике (IEEE), членом Международного научного радиосоюза, членом Польской, Чехословацкой, Монгольской, Болгарской и Германской (бывшая ГДР) академий наук.

За выдающиеся заслуги в развитии отечественной науки в области радиотехники, электроники и радиоастрономии, а также за успехи в подготовке научных кадров и личные научные достижения В.А. Котельников был дважды удостоен звания Героя Социалистического Труда, награжден орденами СССР "Знак Почета", двумя орденами Трудового Красного Знамени, шестью орденами Ленина, орденом Октябрьской революции, орденом Почета, орденом "За заслуги перед Отечеством" II степени и многими медалями. К 95-летию со дня рождения он был награжден орденом Российской Федерации "За заслуги перед Отечеством" I степени.

Вместе с коллективом сотрудников он был также удостоен двух Государственных и одной Ленинской премий.

Международный институт IEEE за выдающийся вклад в развитие теории и практики радиосвязи, основополагающие исследования и руководство работами в области радиолокационной астрономии наградил Владимира Александровича в 1993 г. медалью им. Хернанда и Созенеса Бенов, а в 2000 г. — Золотой медалью им. Александра Белла. Международный научный фонд Эдуарда Рейна (Германия) в 1999 г. наградил В.А. Котельникова премией за впервые сформулированную теорему о выборках. Огромный творческий вклад В.А. Котельникова в фундаментальные исследования по теории связи и радиолокационные исследования планет отмечен в 1974 г. Золотой медалью им. А.С. Попова.

Президиум Академии наук наградил В.А. Котельникова высшей наградой Академии — Большой золотой медалью им. М.В. Ломоносова и Золотой медалью им. М.В. Келдыша.

В жизни Владимир Александрович был уравновешенным человеком, одинаково доброжелательно относившимся ко всем, начиная от рабочего и кончая академиком, генералом или членом правительства. Вызывали уважение его огромная эрудиция, обязательность и стремление глубоко вникнуть в каждый вопрос — будь это научная проблема, институтские дела или дела Президиума Академии наук или, наконец, жизненные перипетии конкретного сотрудника. При этом Владимира Александровича отличали внимательность к людям и желание помочь в решении вопроса всеми ему доступными способами. Он создал специфический, очень доброжелательный климат в ИРЭ. У нас практически никогда не было никаких склок.

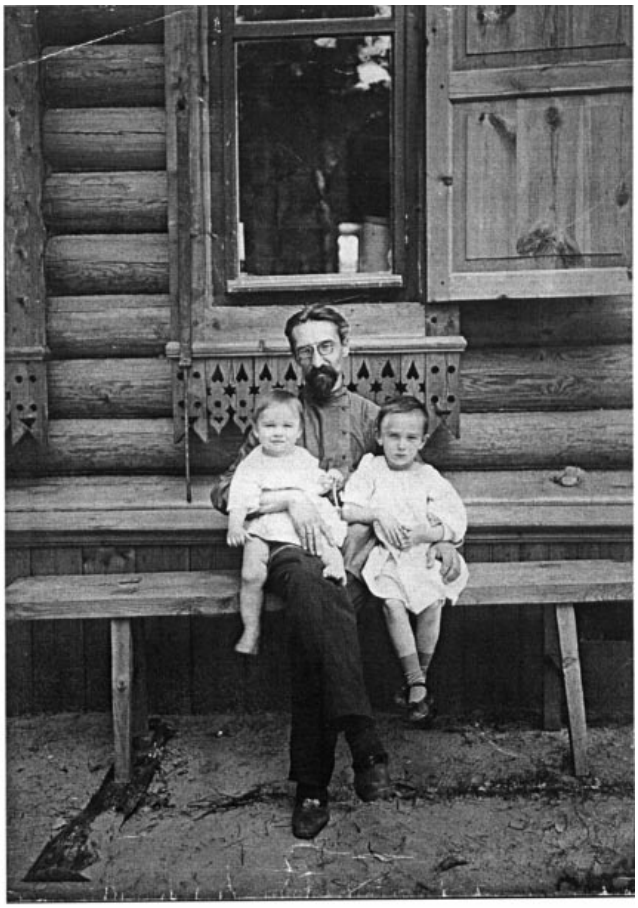
Мы, сотрудники ИРЭ РАН, очень уважали и любили Владимира Александровича и считаем своим первейшим долгом поддерживать созданную им в институте творческую атмосферу и стараться в своих делах следовать его принципам.

PACS numbers: **01.60.+q**, **01.65.+g**

Владимир Александрович Котельников: дорога ученого

Н.В. Котельникова

В этом докладе приводятся наименее известные страницы биографии В.А. Котельникова, охватывающие его "доакадемический" период жизни. Описаны его детство, путь в науку и рассказано об основных этапах его творческого пути в аспекте "как это было". В основу легли воспоминания Владимира Александровича, запи-



Александр Петрович Котельников с сыном Володей (слева) и дочерью Татьяной на даче в поселке Аракчино под Казанью (1909 г.).

санные с его слов, материалы из семейного архива и некоторых публикаций.

Детство. Владимир Александрович Котельников родился 6 сентября 1908 г. в Казани в семье профессора Казанского университета Александра Петровича Котельникова (1865–1944). Его мать — Варвара Петровна Котельникова (Литвиненко) (1878–1921) — родилась, выросла и окончила гимназию в Киеве. В семье было трое детей: Татьяна, Владимир и Всеволод с разницей в возрасте по три года.

Небогатый дворянский род Котельниковых прослеживается начиная с 1622 г. Были в нем военные, подъячий, мелкие служащие, инженеры и ученые. Четырехкратный прадед Владимира Александровича — Семен Кириллович Котельников (1723–1806), математик, был седьмым по счету российским ученым, избранным действительным членом Российской академии наук (1751 г.).

Дед — Петр Иванович Котельников (1809–1879), профессор математики Казанского университета, декан физико-математического факультета, ближайший помощник Н.И. Лобачевского. Он был единственным в мире ученым, который при жизни Н.И. Лобачевского не только понял его геометрию, но и открыто отстаивал ее, бросая вызов всей научной общественности в то время, когда была открыта яростная травля ученого. От него единственного Лобачевский услышал публичное признание своих заслуг создателя новой науки.

Отец — Котельников Александр Петрович, профессор Казанского университета. Выдающийся математик и механик. Создатель винтового исчисления, один из основоположников механики неевклидова пространства и геометрии пространства-времени.

Счастливое и безоблачное детство маленького Володи длилось до 6 лет (до первой мировой войны), и прошло оно в основном в Казани. В доме Котельниковых часто бывали друзья и коллеги из университета, было много книг, звучала музыка. Взрослые много работали. Детей, по мере подрастания, обучали игре на рояле, немецкому языку. К шести годам Володя умел читать, писать, освоил арифметику, начала алгебры и геометрии, правда тригонометрия сразу как-то "не пошла". Он много читал, с отцом они проводили интересные физические опыты, конструировали различные механизмы. Александр Петрович увлекался фотографией, и Володя наблюдал весь процесс от приготовления фотоэмульсии для фотопластинок и до печатания снимков. Ходили на выставки, видели даже настоящий самолет. Отец приводил сына в университет, где показывал созданный им математический кабинет с математическими моделями собственного изготовления. Впоследствии этот кабинет с его богатой библиотекой явился материальной базой для создания Научно-исследовательского института математики и механики при Казанском университете [1].

Летом 1914 г. родители собрались переехать в Киев, на родину мамы. Она никак не могла привыкнуть к Казани, ее климату, часто болела. Наконец ей удалось уговорить мужа принять предложение занять место

Петр Иванович Котельников (1809–1879), дед В.А. Котельникова.

Александр Петрович Котельников (1865–1944), отец В.А. Котельникова.

профессора на кафедре математики в Киевском университете. С сентября Александр Петрович должен был приступить к работе на новом месте. И вдруг вся жизнь перевернулась — началась первая мировая война. В Киев семья приехала в тот день, когда немцы прорвали фронт, поднялась страшная паника, и население хлынуло из города. С этого и началось их "хождения по мукам". С огромным трудом удалось на следующий день выбраться из города и добраться до Казани. А дальше обстоятельства складывались так, что семья оказывалась в центре страшных событий под Казанью, в Казани, а затем, с осени 1918 г., опять в Киеве. С большим трудом им тогда удалось пробраться в Киев. Была надежда, что с установлением там гетманской республики жизнь наладится, и опять начнет работать университет. С 1917 г. занятия в университете, эвакуированном в Саратов, прекратились, и Александр Петрович оказался без работы. Их жизнь в Киеве, как вспоминал Владимир Александрович, очень точно описана в романе М. Булгакова "Белая гвардия". То же время, то же место и те же обстоятельства. "Велик был год и страшен год по рождестве Христовом 1918, но 1919 был его страшней..." Шли бои, город переходил из рук в руки, кругом царила разруха. Время было страшное, голодное. Денег не было, продавать было нечего, а семью кормить надо. Профессор варил мыло по рецепту и из сырья, которые доставали его друзья и бывшие коллеги. Дети расплетали какие-то покрывала и занавески на нитки, сматывали их в клубки. Мама пекла булочки из продуктов, которые также доставали знакомые... И все это отец продавал на рынке. А вечером Александр Петрович садился за письменный стол и допоздна работал. По-видимому, пример отца, увлеченного наукой, привыкшего постоянно трудиться, и воспитал в Володе желание и умение самостоятельно работать. Книги, учебники, которые в этой семье были предметом первой необходимости, переезжали с ней из города в город. Читать их было интересно, и он самостоятельно постигал "науку". Конечно, была возможность выяснить непонятные вопросы у отца, но такой необходимости не возникало.

В 1920 г. Александр Петрович был приглашен работать в Политехнический институт, открывшийся первым из вузов после всех "пертурбаций". Жизнь вроде начала понемногу налаживаться. Но случилась беда: в 1921 г. вся семья, кроме чудом уцелевшего Володи, заболела тифом. А затем семью постигло страшное горе — от тифа умерли мама и тетя Лиза, папина сестра. Все домашние заботы — хозяйственные и воспитание детей легли на плечи отца. Старшие дети — Татьяна и Володя активно помогали. Их обязанностью было следить за порядком в доме, готовить обед, помогать отцу на огороде, за счет которого они в основном кормились, и присматривать за младшим братом Севой — он был у них "на подхвате".

Школа. Институт. Университет. В школу Володя поступил в 1922 г., сразу в 5-ю группу (5-й класс). Учился очень легко, многое он уже знал. Физику у них вел преподаватель Политехнического института. Его уроки всегда были очень интересны и часто проходили в Политехе, где в большой аудитории демонстрировались замечательные опыты. Математик был студентом того же института. С ним Володя решал задачки на равных. В школе выпускалась стенгазета, в которую ученики писали заметки об интересных достижениях науки и техники. Все мальчишки писали только о самолетах.

Володя Котельников. "Как же работает радио?"

Это было время бурного развития авиации. Володя же решил написать о радио. С самолетами ему, как он считал, все было более или менее понятно, а вот радио оставалось загадкой.

Впервые он увидел, вернее, услышал радиопередатчик в Казани в 1918 г. то ли у красных, то ли у белых во время боев за город. Папа рассказал ему, как с помощью невидимых и неслышимых радиоволн передают сообщения. На вопрос сына: "Как это устроено?", он ответил: "Ты этого пока не поймешь". Обычно после такого ответа Володя старался придумать свое объяснение непонятного ему явления или устройства, и это ему както удавалось. В этом же случае он оказался бессилен. Радио его потрясло!

Статью он написал. Для этого, правда, пришлось быстренько выучить тригонометрию, которую в школе они еще не проходили. Однако, чтобы по-настоящему разобраться в статьях журнала по радиотехнике *Телеграфия и телефония без проводов*, который по его просьбе принес отец, этого оказалось мало. (В то время популярных журналов по радиотехнике, еще только зарождавшейся науке, не было.) Тогда-то он и решил, что будет всерьез заниматься радио.

В 1924 г. семья переехала в Москву. В Киеве началась активная "украинизация". Стали требовать, чтобы профессора читали лекции на украинском языке. Александр Петрович решил переехать с детьми в Москву. Его давно приглашали на профессорскую должность в Московское высшее техническое училище (МВТУ). Окончил школу Володя в Москве в 1925 г. Всего в школе он проучился три

года, но поскольку он много занимался сам, то уровень подготовки у него был достаточно высокий для поступления в вуз. По радиоспециальности, о которой мечтал Владимир, готовили в МВТУ, но туда принимали только лиц рабоче-крестьянского происхождения после рабфака. Пришлось пойти в техникум связи. А через год в 1926 г. он поступил в МВТУ — там был объявлен открытый прием. Учиться было легко и интересно. Посещал он только те занятия, которые считал интересными и полезными, в остальном предпочитал разбираться сам по книгам. Параллельно он посещал лекции в Московском государственном университете и прошел всю программу физико-математического факультета, который в то время находился на Моховой в здании, где теперь располагается Институт радиотехники и электроники (ИРЭ РАН).

Аспирантура. Теорема Котельникова. В 1930 г. Владимир окончил Московский энергетический институт (МЭИ), который выделился к тому моменту из МВТУ, и против своей воли оказался в аспирантуре. Он мечтал распределиться в Центральную радиолабораторию (ЦРЛ), в которую была преобразована Нижегородская радиолаборатория после переезда в Ленинград. Будучи студентом, он дважды, после первого и третьего курсов, проходил практику в этой лаборатории под руководством Б.А. Остроумова. По результатам первой практики Владимир опубликовал в журнале Нижегородской радиолаборатории *Телеграфия и телефония без проводов* (№ 46, 1928 г.) свою первую научную работу "Тройной характерограф". Однако в деканате ему как лучшему выпускнику предложили остаться в МЭИ. Он отказался — хотел заниматься наукой. Преподавательская работа его в то время не привлекала. Пока шли переговоры — его уговаривали, он отказывался — все места в ЦРЛ оказались заняты. Остались только самые неинтересные варианты — чисто эксплуатационная работа в других организациях. Он лихорадочно обдумывал, "как жить дальше". Сдаваться он пока не собирался. Неожиданно выход из положения нашел профессор И.Г. Кляцкин, который случайно наткнулся на Владимира в коридоре института и предложил пойти работать к нему в НИИ связи Красной армии (НИИС РККА). Так и решили. Через три месяца о его месте работы узнали в МЭИ. Поднялся жуткий скандал, И.Г. Кляцкина стали обвинять в непорядочности... Делать было нечего, пришлось подчиниться судьбе и вернуться в МЭИ. Там его сразу, без экзаменов, зачислили в аспирантуру (с января 1931 г.) и одновременно приняли на должность старшего лаборанта. Владимир работал сначала старшим лаборантом, налаживая работу учебных лабораторий, а затем ассистентом профессора.

Там же, в "лабораторках", он впервые встретил свою будущую любовь и жену — Анну Ивановну Богацкую (1916 – 1990). Поженившись в 1938 г., они вырастили троих детей и прожили в большой любви до конца своих дней.

Аспирантура в МЭИ тех лет кардинально отличалась от современной. Аспиранты были предоставлены сами себе. Никаких научных руководителей, никаких научных тем. Обязательными курсами были только философия и иностранный язык, остальные курсы выбирали по своему усмотрению. Владимир решил, что раз уж сложилась такая ситуация, то будет заниматься научной работой сам. Он внимательно проанализировал актуальные проблемы радио и проводной связи. В результате, в 1932 г. им были опубликованы три работы, одна из которых — "О пропускной способности "эфира" и проволоки в электросвязи" — была заявлена как доклад на намечавшийся I Всесоюзный съезд по вопросам технической реконструкции дела связи и развития слаботочной промышленности. Съезд не состоялся, но материалы к нему были опубликованы в 1933 г. (доклад принят к печати в ноябре 1932 г.) [2]. Заканчивая аспирантуру, Владимир доложил свои работы на Ученом совете факультета. Доклад был одобрен, но работу "О пропускной способности "эфира" ..." и значение сформулированной в ней теоремы отсчетов на совете не поняли — "все вроде верно, но похоже на научную фантастику". А жаль! Работа замечательна в двух аспектах. Во-первых, это был хорошо аргументированный программный документ, отсекавший тупиковые и указывающий перспективные и реально осуществимые пути развития радиосвязи в плане преодоления "тесноты в эфире и проволоке". В частности, в работе указывалось на перспективность способа передачи "на одной боковой полосе". Как показало время, прогнозы молодого Котельникова оправдались. Сам он уверенно шел по намеченному им пути вместе со своей лабораторией в НИИ связи Народного комиссариата связи (НИИС НКС) и позже с созданным им же Институтом радиотехники и электроники АН СССР (ИРЭ АН СССР). Во-вторых, эта работа была устремлена в будущее. Впервые, содержательно обсуждая информационный аспект проблем связи, Владимир математически обоснованно предсказал возможность цифровой передачи информации (была доказана ставшая впоследствии знаменитой теорема Котельни-

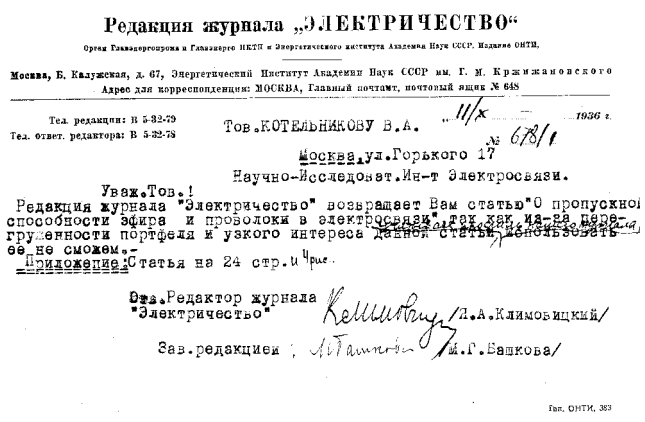
Автор теоремы Котельникова.

кова). Его идея стала основой современной теории информации. В этом аспекте работа опередила свое время, по крайней мере на 15 лет. В полной степени она была оценена лишь в конце 1970-х, когда появилась возможность заменить аналоговую систему передачи сигналов цифровой [3].

Ученой степени тогда не присуждали. Степень кандидата технических наук В.А. Котельникову заочно присудил в 1938 г. Ленинградский электротехнический институт (ЛЭТИ) по собственной инициативе.

Дальнейшая история теоремы Котельникова, сформулированной и доказанной 24-летним "беспризорным" аспирантом, или, как ее еще называют, теоремы отсчетов, — почти детективная. Понимая ее значение, Владимир в 1936 г. попытался опубликовать статью в более широко читаемом специалистами журнале *Электричество* (орган Энергетического института АН СССР), но получил отказ! "Что ж, не принимают, так не принимают! Кому нужно, те прочитают в «Материалах» конференции", — решил он и продолжил работать дальше, забыв об этом эпизоде. Вспомнил об этом он лишь в новом, XXI веке, когда ему показали найденное в его архиве письмо с отказом.

Через 15 лет (1948 г.) Клод Шеннон опубликовал свою теорему отсчетов [4]. Идеи витают в воздухе, и в разных точках земного шара с некоторым разбросом по времени и степени точности формулировки появлялись подобные теоремы. Поскольку эта теорема имеет ключевое значение в теории информации, то к ней было приковано внимание специалистов в этой области, особенно в 1970-е годы, когда с развитием электроники появились технические возможности реализации цифровой передачи и записи информации. В 1977 г. при расстановке приоритетов ее было предложено называть WKS-теоремой — теоремой Whittaker – Kotelnikov – Shannon [5, 6]. И наконец в 1999 г. Фонд Эдуарда Рейна, подводя итоги наиболее выдающихся научных достижений XX века, присудил премию в номинации "за фундаментальные исследования" российскому ученому Котельникову Владимиру Александровичу за "впервые математически точно сформулированную и опубликованную теорему отсчетов", на которую опирается вся современная, ставшая цифровой радиотехника и вычислительная техника.



Редакция журнала „ЭЛЕКТРИЧЕСТВО"

Орган Ленэнергопрома и Ленэнерго НКТП и Энергетического института Академии Наук СССР. Издание ОНТИ.

Москва, Б. Калужская, д. 67, Энергетический Институт Академии Наук СССР им. Г. М. Кржижановского
Адрес для корреспонденции: МОСКВА, Главный почтамт, почтовый ящик № 648

Тел. редакции: В 5-32-79
Тел. ответ. редактора: В 5-32-78

11/X 1936 г.
№ 678/1

Тов. КОТЕЛЬНИКОВУ В.А.
Москва, ул. Горького 17
Научно-Исследоват. Ин-т Электросвязи.

Уваж. Тов.!
Редакция журнала "Электричество" возвращает Вам статью "О пропускной способности эфира и проволоки в электросвязи", так как из-за перегруженности портфеля и узкого интереса данной статьи, используемого, мы не сможем.
Приложение: Статья на 24 стр. и чертеж.

Отв. Редактор журнала "Электричество" /Д.А. Климобицкий/

Зав. редакцией /М.Г. Башкова/

Тип. ОНТИ, 383

Письмо из редакции журнала *Электричество* с отказом в публикации статьи с теоремой Котельникова (рукописная вставка в тексте письма: "...учитывая профиль нашего журнала, ...").

В статье, предшествовавшей выдвижению кандидатуры В.А. Котельникова на эту премию, Hans Dieter Luke о работе "О пропускной способности "эфира" и проволоки в электросвязи" писал: "Поскольку эта замечательная работа никогда не была опубликована в интернационально доступной печати, публикации теоремы отсчетов в теоретически точной формулировке возникали в литературе по технике связи независимо друг от друга" [6]. Учитывая тот факт, что и по сей день эта работа вызывает большой интерес, теперь уже в историческом аспекте, она впервые в "интернационально доступной печати" публикуется в настоящем выпуске *УФН* в приложении к этому докладу.

Научно-исследовательский институт связи Народного комиссариата связи. (Позже стал называться ЦНИИС НКС, добавили "Центральный".) После окончания аспирантуры в 1933 г. Владимир Котельников, оставаясь преподавать в МЭИ (ассистент, затем доцент), поступил на работу в НИИС НКС (инженер, главный инженер института по радио, начальник вновь созданной лаборатории). В 1936 г. в открытой печати Котельников опубликовал две пионерские работы [7, 8], в которых он одним из первых, используя теорию вероятности, выполнил исследование эффективности систем разнесенного приема сигналов в многолучевом канале и предложил общий аналитический метод исследования нелинейных искажений сигналов в различных устройствах. Подобные методы получили развитие начиная с конца 1940-х годов в работах крупнейших отечественных и зарубежных ученых [9]. В 1935 – 1936 гг. правительством была определена стратегия создания магистралей ближней, средней и дальней радиосвязи. В рамках этой программы в НИИС приступили к разработке новой аппаратуры для таких линий связи. Еще из МЭИ Котельников "принес" твердую убежденность в необходимости и возможности реализации замечательной идеи — "аналоговой передачи на одной боковой полосе" [2]. Преодолев сопротивление руководства, Владимиру Александровичу вместе со своими сотрудниками удалось осуществить эту идею, создав уникальную аппаратуру. Промышленность отказалась тогда принять заказ на изготовление разработанных приборов: "Сделать невозможно, так как никто и нигде такого еще не делал". "Сделаем сами", — решил Котельников, и сделали. Аппаратуру установили на линии связи Москва – Хабаровск (1939 г.). Это был выдающийся проект своего времени. Но произошло непредвиденное — готовую и испытанную уникальную радиотелефонную линию к эксплуатации не приняли — "слишком легко подслушать". Пришлось срочно искать выход из сложившейся ситуации. Криптографией до этого заниматься не приходилось, доступа к соответствующей литературе и соответствующим специалистам не было. Поразмыслив, Котельников пришел к выводу, что с задачей они справятся. И срочно взялись за дело. Начали "с нуля". Предстояло решить много научных и технических проблем, поскольку разрабатывалась принципиально новая аппаратура. Прочитав статью Х. Дадли [10], опубликованную в октябре 1939 г., В.А. Котельников сразу оценил потенциальные возможности описанного там вокодера (аппарата искусственной речи) как перспективного устройства для создания на его основе аппаратуры шифрования речи. Уже в начале 1941 г. в лаборатории заработал первый в СССР вокодер. В ходе очень напряженной работы, "сроки поджимали", Влади-

мир Александрович обдумывал основные проблемы шифрования. Свои соображения он изложил в отчете "Основные положения автоматической шифровки", представленном за три дня до начала войны, 19 июня 1941 г. В этом документе впервые были "сформулированы четкие положения о том, каким требованиям должна удовлетворять математически недешифруемая система, и дано доказательство невозможности ее дешифрования" [11]. Эта работа явилась основополагающей в развитии отечественной криптографии. Об этой работе, к сожалению, мало кто знает, поскольку она так и не была опубликована в открытой печати. Через четыре года К. Шеннон изложил подходы к построению стойких систем шифрования в секретном докладе, датированном 1 сентября 1945 г. В открытой печати этот доклад был опубликован в 1949 г. [4].

Война. Начавшаяся война заставила Котельникова и его сотрудников прервать научно-исследовательскую работу и перейти к срочному проектированию образцов аппаратуры. Работали почти круглосуточно. Вскоре, когда фронт приблизился к Москве, НИИС был распущен, все сотрудники уволены. Оставили только лабораторию Котельникова, в которой велись работы по закрытой радиотелефонии, так необходимой для фронта. Им было поручено: получить деньги и расплатиться со всеми уволенными сотрудниками института; сжечь всю документацию, кроме самой важной; подготовить аппаратуру лаборатории к эвакуации; в случае прорыва немцев к Москве взорвать здание института. Первые три пункта приказа были выполнены. Взрывать институт, к счастью, не пришлось. И 17 октября 1941 г. в трудовой книжке В.А. Котельникова появилась запись: "Освобожден от работы в связи с предоставлением отпуска". И "отпуск" начался: в течение октября – ноября поэтапно проводилась эвакуация лаборатории в Уфу. Продолжение работ над аппаратурой осложнялось тем, что была уничтожена значительная часть конструкторской документации. Несмотря на это, уже к осени 1942 г. было изготовлено несколько образцов аппаратуры секретной радиотелефонии, сразу направленных на Закавказский фронт, с которым была прервана связь в период боев под Сталинградом. Тогда в армии использовались проводные линии связи. В результате удалось восстановить эту связь по радиоканалу. К началу 1943 г. было налажено производство аппаратуры, и она стала использоваться в действующей армии, что спасло многие жизни советских солдат и явилось огромным вкладом в дело Победы. В то время это была самая совершенная аппаратура закрытой радиотелефонии, практически не поддававшаяся "вскрытию". Именно такая аппаратура использовалась для связи Москвы с нашей делегацией во время подписания капитуляции Германии в мае 1945 г. За эту работу коллектив лаборатории был отмечен высокими наградами — Сталинскими премиями 1-й степени (1943 г.). Деньги были переданы на нужды фронта. На премию В.А. Котельникова был построен танк.

По мнению специалистов, до начала 1970-х годов не существовало эффективных алгоритмов дешифрования сообщений, зашифрованных с помощью усовершенствованных систем такого типа [12].

Возвращение в Москву. Московский энергетический институт. Весной 1943 г. лаборатория В.А. Котельникова была отозвана из Уфы в Москву и переведена в распоряжение Народного комиссариата внутренних дел (НКВД) СССР. Там ее передавали из отдела в отдел... В этот момент В.А. Котельникова разыскала В.А. Голубцова — новый директор МЭИ. Война еще продолжалась, но страна уже приступила к восстановлению разрушенного войной народного хозяйства. Начал активно восстанавливаться и МЭИ — стране требовались специалисты. Рассказав о проблемах института и перспективах его развития, В.А. Голубцова предложила Котельникову вернуться в МЭИ. Владимир Александрович с готовностью согласился. Он предпочитал заниматься наукой в гражданском учреждении, тем более в родном институте. В.А. Голубцова была женой первого секретаря ЦК КПСС Г.М. Маленкова. По-видимому, благодаря этому и удалось Владимиру Александровичу, будучи руково-

Сотрудники лаборатории В.А. Котельникова (Уфа, апрель 1943 г.). Стоят (слева направо): Е. Кунина, Е.Л. Гаврилов, В.Н. Мелков, Н.Н. Найденов. Сидят (слева направо): А.М. Трахтман, Д.П. Горелов, В.А. Котельников, И.С. Нейман, В.Б. Штейншлегер.

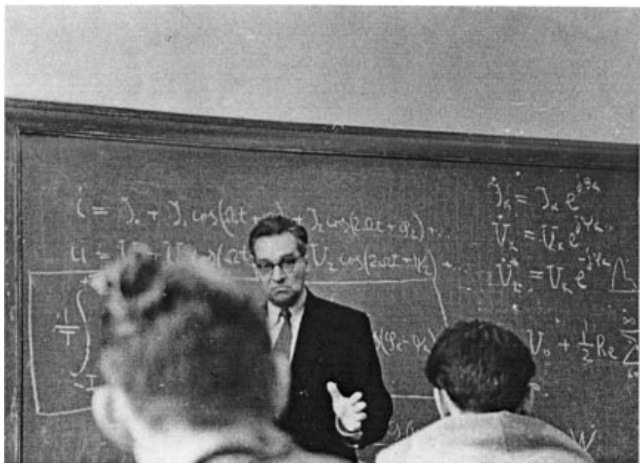
В.А. Котельников (в центре) в учебной лаборатории РТФ МЭИ (1946 г.).

дителем секретной тематики, перейти из системы НКВД в МЭИ. Приказ о переводе в МЭИ на должность заведующего кафедрой "Основы радиотехники" (ОРТ), которую еще предстояло создать на радиотехническом факультете (РТФ), был подписан 1 ноября 1944 г. Позднее Владимир Александрович был избран еще и деканом РТФ. Он считается одним из создателей РТФ. В процессе его многогранной деятельности в МЭИ сформировалась научно-педагогическая школа В.А. Котельникова, получившая развитие по трем основным направлениям: дальнейшее развитие идей созданной им теории потенциальной помехоустойчивости; исследования, связанные с теорией электромагнитного поля и освоением новых диапазонов электромагнитных волн (миллиметрового, субмиллиметрового, инфракрасного и оптического); инженерно-научное [12].

Владимир Александрович всегда считал, что главное в подготовке специалистов — это хорошее знание физики, математики и умение самостоятельно думать. Он первым ввел преподавание курсов теоретической физики в МЭИ. Курсы лекций Котельникова "Основы радиотехники" и "Электродинамика", которые он всегда читал сам, пользовались огромной популярностью. Их слушали студенты и преподаватели не только РТФ, но и других факультетов. Владимира Александровича называли деканом-реформатором. В бытность его деканом, на факультете было осуществлено много полезных преобразований, в частности, им была основана новая специальность — радиофизика [13].

Одновременно Владимир Александрович консультировал свою бывшую лабораторию по основным проблемам секретной телефонии.

Теория потенциальной помехоустойчивости. Весной 1946 г. В.А. Голубцова вызвала как-то Котельникова и решительно сказала: "Владимир Александрович, Вам необходимо защитить докторскую диссертацию". Надо, так надо. Сам он об этом не думал. Никаких идей насчет темы диссертации у него тогда не было. Существует легенда, что в трудные годы эвакуации на обрывках бумаги была набросана будущая докторская диссертация по потенциальной помехоустойчивости, которая, к несчастью, была потеряна при возвращении из эвакуации. Это не так. Действительно, был чемодан, который украли, но диссертации там не было. Тогда ее не было вообще. Самое ценное, что было в чемодане, — это буханка хлеба. Летом Котельников взял очередной отпуск, отправил семью на дачу и принялся сочинять "Теорию потенциальной помехоустойчивости" — так он назвал свою диссертацию. До окончания отпуска закончить ее не удалось и пришлось доделывать по вечерам после работы. Осенью диссертация была готова. С защитой, однако, вышла некоторая заминка. Подыскать оппонентов оказалось не просто — работу никто не понимал. "Она появилась для научной общественности буквально на пустом месте" [14]. Ссылаться автору было не на кого. Работа опережала свое время приблизительно на 10 лет. Обратились к академику Н.Д. Папалекси. Николай Дмитриевич просмотрел работу и сказал, что не понял ее. К тому же ссылок на другие работы в ней не было, руководителя у диссертанта не было — сам по себе. Оппонировать Н.Д. Папалекси отказался. В конце концов оппоненты были найдены, и в январе 1947 г. диссертация была защищена. Очевидцы вспоминали, что было впечатление, будто мало кто и мало что из рассказанного понял, даже оппоненты. Но у всех было ощущение, что на их глазах "рождается что-то очень значительное". Впоследствии стало ясно, что в этот день родилась одна из двух взаимодополняющих ветвей теории информации. Другая ветвь, работа К. Шеннона, появилась в 1948 г. [4]. В работе Котельникова впервые были проанализированы основные проблемы связи с теоретико-вероятностных позиций. Она дала мощный импульс для развития статистической теории передачи сообщений, статистического синтеза оптимальных методов обработки сигналов, разработке эффективных алгоритмов функционирования приемных устройств [15]. По теме диссертации автор опубликовал только одну короткую статью "Проблемы помехоустойчивой радиосвязи" (1947 г.) [16]. Экземпляр диссертации, как положено, был передан в Ленинскую библиотеку. Полностью тогда эта работа опубликована не была. По-видимому, Котельников понимал, что ситуация складывается такая же, как и



"Вот так... совсем просто...". (На лекции в МЭИ (1947 г.).)

Праздник с женой и дочерью Наталией (1948 г.).

со статьей "О пропускной способности "эфира"...". Если уж сам академик Н.Д.Папалекси работу не понял, то кто же ее опубликует? "Кому надо, тот прочитает ее в Ленинке", — решил диссертант. Монография В.А. Котельникова "Теория потенциальной помехоустойчивости" [17] вышла только в 1956 г. после того, как в зарубежной прессе появились первые статьи по этой тематике. Эта работа произвела фурор во всем "радиотехническом мире". К В.А. Котельникову пришла мировая слава!

В 2005 г. в архивах Владимира Александровича был обнаружен "Список печатных работ В.А. Котельникова. 1950 г.". Там было указано: «"Теория потенциальной помехоустойчивости" — монография 12 п. л., рукопись, готовится к печати. Связьиздат». Зная Владимира Александровича, трудно себе представить, чтобы он на шесть лет "затянул" выполнение намеченного им дела. Возможно, тогда эта работа также не была принята в печать.

Марфинская лаборатория или "Круг третий". В книгах А.И. Солженицына "В круге первом" и К.Ф. Калачева "В круге третьем" [18] описываются события, происходившие в одно и то же время в одном и том же месте — Марфинской лаборатории. Оба автора были ее сотрудниками, но переживали и видели происходившее поразному, каждый в своем ракурсе. "Первый круг" Солженицына, специалиста-заключенного, — это круг ада. Третий же "круг" Калачева, "вольного" специалиста — это третий этап развития секретной телефонии. Основной костяк Марфинской лаборатории составляла бывшая лаборатория В.А. Котельникова, которая после возвращения из эвакуации была передана в подчинение НКВД СССР. Калачев также работал у Котельникова, но до войны. Сам Владимир Александрович к моменту создания Марфинской лаборатории уже вернулся на работу в МЭИ.

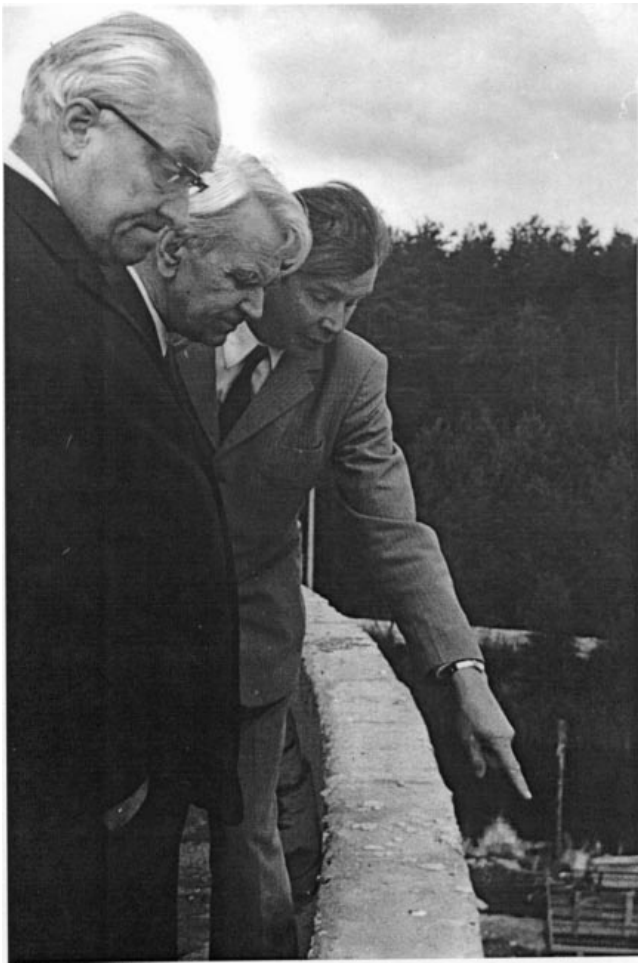
Дважды лауреат Сталинской премии 1-й степени (Государственной премии) (1946 г.).

В 1947 г. Министерством внутренних дел (МВД) и Министерством государственной безопасности (МГБ) СССР было принято решение о создании Специальной лаборатории для разработки аппаратуры "абсолютно стойкого" засекречивания телефонных переговоров правительственной высокочастотной (ВЧ) связи. Учитывая особую важность задач лаборатории, к руководству решили привлечь выдающегося ученого, видного специалиста в этой области. Котельников обоснованно считался основоположником секретной телефонии [11, 18].

Однажды (в 1947 г.) В.А. Котельников был вызван к министру государственной безопасности СССР В.С. Абакумову. Разговор проходил в очень вежливом и уважительном тоне. Рассказав о создании Специальной лаборатории, Абакумов предложил Владимиру Александровичу возглавить ее. Тот отказался. Министр был очень удивлен. По-видимому, он не привык получать отказ. Его "предложение" обычно означало приказ. Он поинтересовался причиной несогласия. Котельников спокойно объяснил, что хочет заниматься наукой. Абакумов попытался уговорить несговорчивого ученого, пообещав множество благ и привилегий. Но Владимир Александрович оставался непреклонным. "Ну, что ж, а жаль ..." — заключил министр, и они распрощались.

Возвращаясь в МЭИ, Котельников обдумывал сложившуюся ситуацию и то, чем для него может обернуться это "ну, что ж...". В институте он сразу пошел к ректору В.А. Голубцовой и рассказал о визите в МГБ. Выслушав, она спросила, чего хочет сам Владимир Александрович. Ответ был: "Работать в МЭИ". "Тогда продолжайте спокойно работать", — сказала Валерия Алексеевна.

От Спецсектора до Особого конструкторского бюро (ОКБ) МЭИ. Создав кафедру ОРТ, Владимир Александрович объединил вокруг себя коллектив талантливых ученых и инженеров. В 1944 – 1947 гг. они разрабатывали телеметрическую аппаратуру для самолетов, которая получила высокую оценку. В 1947 г. началась захватывающая работа в рамках Ракетно-космической программы страны, в которую активно включился и МЭИ. По постановлению правительства был создан Сектор специальных работ для выполнения НИР в интересах реактивного вооружения (Спецсектор). Основу Спецсектора составил существенно расширенный коллектив кафедры ОРТ. В очень короткий срок он стал одной из ведущих организаций ракетно-космической отрасли и впоследствии получил название ОКБ МЭИ. Возглавил его В.А. Котельников. Под его руководством были осуществлены крупные научно-исследовательские и опытно-конструкторские работы по созданию радиотехнических систем и комплексов для бурно развивавшейся ракетно-космической отрасли. Зачастую Спецсектор брался за те задачи, с которыми не справлялась или от которых отказывалась промышленность. Как Главный конструктор Спецсектора Котельников входил в межведомственный Совет главных конструкторов, который возглавлял С.П. Королев. Присутствие всех Главных было непременным условием каждого испытания систем и уж тем более всех пусков — "чтобы было с кого спрашивать в случае каких-либо неполадок". Когда еще



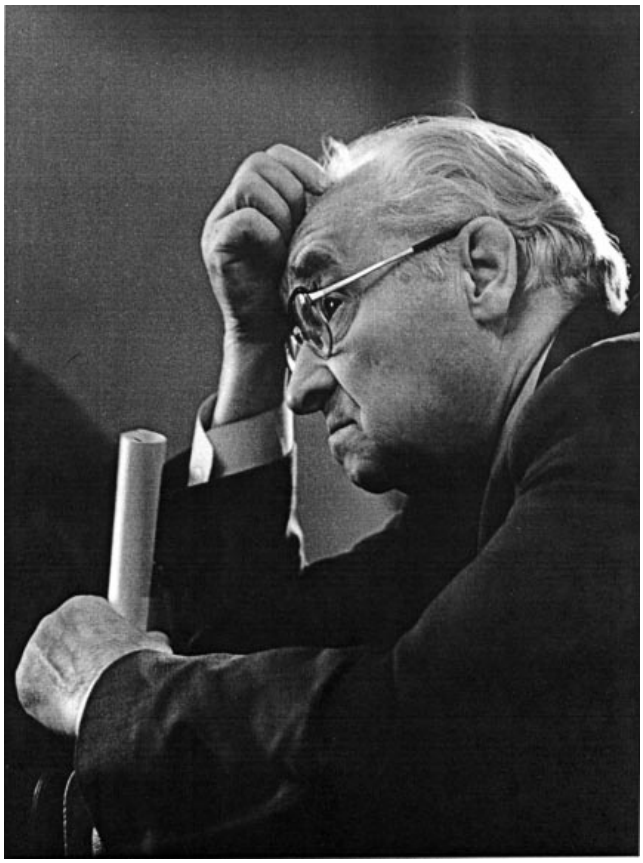
С высоты антенны лучше видно (Медвежьи озера). Слева направо: В.А. Котельников, М.В. Келдыш, А.Ф. Богомолов.

только начиналась Ракетно-космическая программа, быт на ракетодромах был совсем не обустроен. Как и многие другие специалисты, сотрудники Спецсектора жили в землянках, вырытых прямо в степи, недалеко от места проведения испытаний. Руководство размещали в "более комфортабельном" помещении — в каком-то домике, расположенном у железнодорожной станции Капустин Яр, и в вагонах стоявшего в тупике поезда. На полигон их привозили на машинах. Владимир Александрович предпочитал жить в землянке "со своими", и когда ему предлагали поселиться в "начальственных апартаментах", отшучивался: "Слишком далеко ездить до работы". Пуски бывали в разное время года — в страшную жару, в дождь, холод и снег... Но несмотря на трудности все работали с огромным энтузиазмом. Одновременно Владимир Александрович был деканом РТФ, продолжал работать на кафедре ОРТ, являясь ее заведующим, и читал лекции.

В.А. Котельников возглавлял Спецсектор до 1955 г., передав затем "бразды правления" в руки своего талантливого ученика А.Ф. Богомолова (будущего академика). Однако его связь со Спецсектором, который был переименован в ОКБ МЭИ, не прерывалась. В 1983 – 1984 гг. обе организации, созданные Владимиром Александровичем, ИРЭ АН СССР и ОКБ МЭИ, успешно работали "рука об руку" в ходе всего процесса подготовки и проведения придуманного и руководимого им выдающегося проекта радиокартографирования поверхности Венеры. Эксперимент прошел успешно. Результаты были получены уникальные!

Академия наук СССР. Институт радиотехники и электроники. В конце лета или начале осени 1953 г. (Владимир Александрович точно не запомнил) академик Аксель Иванович Берг пригласил его к себе в Центральный научно-исследовательский радиотехнический институт (ЦНИРТИ), директором которого он был в то время. Аксель Иванович рассказал, что появилась идея создать в Академии наук институт, который бы занимался теоретическими исследованиями и инженерными разработками в области радиотехники и электроники, и попросил помочь в составлении учредительных документов. Владимир Александрович с готовностью согласился. Он очень уважал Акселя Ивановича. Знакомы они были очень давно. В предвоенные годы (1933 – 1937 гг.) Берг, будучи начальником НИИ морской связи, приезжал в НИИС НКС и выступал там с докладом. Ему тогда запомнился молодой инженер Котельников, который активно задавал очень грамотные вопросы, что называется в "точку". После доклада они еще долго обсуждали разные радиотехнические проблемы. Потом не раз пересекались пути двух "радистов". Сразу после войны они вместе создавали Общество Попова, сменили один другого на посту председателя Оргбюро Общества, работали в составе Государственной комиссии по оценке работы Марфинской лаборатории и разработанной в ней аппаратуры (1950 и 1952 гг.).

По вечерам Владимир Александрович приезжал в ЦНИРТИ и в кабинете Берга "сочинял" документы. Самому академику было не до этого. Вскоре проекты соответствующих Постановлений и других учредительных документов института, который было решено назвать Институтом радиотехники и электроники, были подготовлены, обсуждены и одобрены. В сентябре вышли все соответствующие Постановления, и ИРЭ АН СССР был учрежден. Директором назначили академика А.И. Берга. Той же осенью В.А. Котельникова пригласил к себе академик-секретарь отделения технических наук Б.А. Введенский и сообщил: "Мы хотим выдвинуть вашу кандидатуру в академики, не возражаете?" После того, как получил согласие от удивленного Котельникова, сказал, что если его изберут, то отделение планирует предложить ему возглавить Институт автоматики и телемеханики, в котором имелись проблемы с директором. В октябре 1953 г. В.А. Котельникова избрали действительным членом АН СССР (минуя ступень члена-корреспондента). Представляли его кандидатуру, судя по всему, академики А.И. Берг и Б.А. Введенский. (Сам Котельников в предвыборной кампании участия не принимал.) Сразу же после выборов Аксель Иванович предложил вновь избранному академику заняться созданием только что учрежденного ИРЭ, став первым заместителем директора. Владимир Александрович согласился. Создавать такой институт! В ноябре 1953 г. В.А. Котельников перешел на должность заместителя директора ИРЭ, существующего пока только на бумаге, а в 1954 г. стал его директором. (А.И. Берг уже в 1953 г. был назначен заместителем министра обороны СССР.) Аксель Иванович был великим стратегом и свои планы до поры до времени держал при себе. Позже он как-то весело заметил, что с самого начала разглядел в Котель-



Интересный доклад.

никове директора института. И началась огромная работа по созданию института: подбор кадров, определение тематики исследований, поиск помещения для института, его обустройство, создание конструкторского бюро и т.д. В очень короткий срок ИРЭ АН СССР стал ведущим институтом в области радиофизики, радиотехники и электроники не только в нашей стране, но и в мире.

Владимир Александрович был не только директором института, но и инициатором, руководителем и непосредственным исполнителем многих выдающихся научно-технических проектов, в результате проведения которых были получены уникальные научные результаты. Все, кто работал с Владимиром Александровичем, отмечали, что он обладал исключительной эрудицией, научной интуицией, умением проникать в суть проблемы и "чудовищной работоспособностью".

На момент избрания Владимира Александровича действительным членом АН СССР и начала создания ИРЭ ему исполнилось 45 лет. Впереди был еще 51 год активной и успешной творческой жизни.

Список литературы

1. Путята Т В и др. *Александр Петрович Котельников. 1865 – 1944* (М.: Наука, 1968)
2. Котельников В А "О пропускной способности "эфира" и проволоки в электросвязи", в сб. *Всесоюзный энергетический комитет. Материалы к I Всесоюз. съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности. По радиосекции* (М.: Управление связи РККА, 1933) с. 1 – 19
3. Витушкин А Г, в сб. *Математические события XX века* (Ред. комиссия: В И Арнольд и др.) (М.: ФАЗИС, 2003)
4. Шеннон К *Работы по теории информации и кибернетике* (М.: ИЛ, 1963)
5. Abdul J *Proc. IEEE* **65** 1585 (1967)
6. Luke H D *IEEE Commun. Mag.* **37** (4) 106 (1999)
7. Котельников В А *Научно-технический сборник Ленинградского электротехнического института связи* (11) (1936)
8. Котельников В А *Научно-технический сборник Ленинградского электротехнического института связи* (14) (1936)
9. Быховский М А, в сб. *Творцы российской радиотехники. Жизнь и вклад в мировую науку* (Сер. История электросвязи и радиотехники, Вып. 3, Под ред. М А Быховского) (М.: Эко-Трендз, 2005) с. 67
10. Dudley H *Bell Labs Record* **17** 122 (1939)
11. Андреев Н Н и др. *Радиотехника* (8) 8 (1998)
12. Удалов Н Н *Радиотехника* (11) 37 (1998)
13. Зиновьев А Л *Электросвязь* (9) 3 (1998)
14. Соколов А В, Филиппов Л И *Радиотехника* (8) 48 (1998)
15. Флейшман Б С *Конструктивные методы оптимального кодирования для каналов с шумами* (М.: Изд-во АН СССР, 1963)
16. Котельников В А, в сб. *Радиотехнический сборник* (М.-Л.: Госэнергоиздат, 1947)
17. Котельников В А *Теория потенциальной помехоустойчивости* (М.-Л.: Госэнергоиздат, 1956); репр. изд. (М.: Радио и связь, 1998)
18. Калачев К Ф *В круге третьем: Воспоминания и размышления о работе Марфинской лаборатории в 1948 – 1951 годах* (М.: Машмир, 2001)

PACS numbers: **84.40. – x**, **89.70. + c**

Приложение

ВСЕСОЮЗНЫЙ ЭНЕРГЕТИЧЕСКИЙ КОМИТЕТ

Материалы к I Всесоюзному съезду
по вопросам технической реконструкции
дела связи и развития слаботочной
промышленности.

ПО РАДИОСЕКЦИИ

О пропускной способности "эфира" и проволоки в электросвязи *

Инж. В.А. Котельников

Как в радио-, так и в проволочной технике для каждой передачи требуется не одна какая-либо частота, а целый диапазон частот. Это ведет к тому, что одновременно может работать лишь ограниченное количество радиостанций (передающих разные программы). По одной паре проводов также нельзя передавать сразу больше определенного количества передач, так как нельзя, чтобы полоса частот одной передачи перекрывала полосу другой, — такое перекрытие привело бы к взаимным помехам.

Чтобы увеличить пропускную способность "эфира" и проволоки (а это имело бы колоссальное практическое значение, в особенности в связи с бурным развитием радиотехники и таких передач, как телевидение), нужно

* Статья 1933 г. воспроизводится по изданию, осуществленному к 70-летию теоремы Котельникова и 95-летию Владимира Александровича Котельникова Институтом радиотехники и электроники Московского энергетического института (МЭИ) (технического университета) в 2003 г. под руководством директора ИРЭ МЭИ (ТУ) Н.Н. Удалова, с незначительными изменениями: запись формул дана в формате, принятом в *УФН*, постраничная нумерация сносок заменена сплошной, орфография и синтаксис приведены в соответствие с современными нормами. Стиль автора сохранен.

как-то сократить диапазон частот, требуемый для данной передачи, не вредя ее качеству, или изобрести способ разделения передач не по частотному признаку, как это делалось до сих пор, а по какому-нибудь другому [1].

По настоящее время никакие ухищрения в этих направлениях не позволяли, даже теоретически, увеличить пропускную способность "эфира" и проволоки в большей степени, чем это позволяет сделать передача "на одной боковой полосе".

Поэтому возникает вопрос: возможно ли вообще это сделать? Или же все попытки в этом направлении будут равносильны попыткам построить perpetuum mobile?

Этот вопрос в настоящее время имеет актуальное значение в радиотехнике ввиду с каждым годом все увеличивающейся "тесноты в эфире". И сейчас особенно важно в нем разобраться в связи с планированием научно-исследовательских работ, так как при планировании важно знать, что возможно и что совершенно невозможно сделать, чтобы направить силы в нужном направлении.

В настоящей работе разбирается этот вопрос и доказывается, что для телевидения и передачи изображений со всеми полутенями, а также для телефонной передачи существует вполне определенная, минимально необходимая полоса частот, которую, не вредя качеству передачи и скорости, нельзя никакими средствами уменьшить; а также доказывается, что для этих передач нельзя увеличить пропускную способность ни эфира, ни проволоки путем применения разного рода нечастотных селекций или других каких-либо способов (исключая, конечно, селекцию по направлению при помощи направленных антенн). Максимально возможная пропускная способность для этих передач может быть получена при передаче "на одной боковой полосе", и она является в настоящее время принципиально вполне достижимой.

Для таких же передач, как телеграфия или же передача изображений и телевидения без полутеней и т.п., в которых передаваемый объект может меняться не непрерывно, а принимая лишь определенные, наперед известные значения, показывается, что необходимая для них полоса частот может быть уменьшена во сколько угодно раз, не вредя ни качеству передачи, ни скорости, за счет увеличения мощности и усложнения аппаратуры. Один из методов такого уменьшения полосы частот указывается в этой работе и показывается, какое увеличение мощности для этого необходимо.

Таким образом, предела для пропускной способности "эфира" и проволоки для передач такого вида теоретически не имеется, дело лишь в техническом выполнении.

Доказательство этих положений в этой работе ведется вне зависимости от метода передачи на основании следующего: во всех видах электросвязи передатчик может передавать, а приемник принимать лишь некоторую функцию времени, которая не может быть вполне произвольной, так как частоты, из которых она состоит и на которые она может быть разложена, должны заключаться в определенных пределах. При радиопередаче такой функцией является сила тока в передающей антенне, которая и воспринимается приемником более или менее точно; при проволочной же передаче это будет электродвижущая сила в начале линии. В обоих случаях передаваемые функции будут состоять из частот ограниченного диапазона, так как, во-первых, очень высокие и очень низкие частоты не дойдут до приемника по условиям распространения, и, во-вторых, частоты, выходящие за пределы определенного узкого диапазона, обычно нарочно уничтожаются, чтобы не мешать другим передачам.

Эта необходимость передавать при помощи функций времени, состоящих из ограниченного диапазона частот, уже приводит, как это будет ниже показано, к вполне определенному ограничению пропускной способности.

Для доказательства высказанных положений займемся изучением функций, состоящих из определенного диапазона частот.

Функции, состоящие из частот от 0 до f_1

Теорема I. Любую функцию $F(t)$, состоящую из частот от 0 до f_1 периодов в секунду, можно представить рядом

$$F(t) = \sum_{-\infty}^{+\infty} D_k \frac{\sin \omega_1 \left[t - k/(2f_1)\right]}{t - k/(2f_1)}, \qquad (1)$$

где k — целое число; $\omega_1 = 2\pi f_1$; D_k — постоянные, зависящие от $F(t)$.

И наоборот, любая функция $F(t)$, представленная рядом (1), состоит лишь из частот от 0 до f_1 периодов в секунду.

Доказательство. Любая функция $F(t)$, удовлетворяющая условиям Дирихле (конечное число максимумов, минимумов и точек разрыва на любом конечном отрезке) и интегрируемая в пределах от $-\infty$ до $+\infty$, что всегда в электротехнике имеет место, может быть представлена интегралом Фурье [2, 3]

$$F(t) = \int_0^{\infty} C(\omega) \cos \omega t \, d\omega + \int_0^{\infty} S(\omega) \sin \omega t \, d\omega, \qquad (2)$$

т.е. как сумма бесконечного количества синусоидальных колебаний с частотами от 0 до ∞ и амплитудами $C(\omega)\,d\omega$ и $S(\omega)\,d\omega$, зависящими от частоты. Причем

$$C(\omega) = \frac{1}{\pi} \int_{-\infty}^{+\infty} F(t) \cos \omega t \, dt,$$
$$S(\omega) = \frac{1}{\pi} \int_{-\infty}^{+\infty} F(t) \sin \omega t \, dt. \qquad (3)$$

В нашем случае, когда $F(t)$ состоит лишь из частот от 0 до f_1, очевидно

$$C(\omega) = 0,$$
$$S(\omega) = 0$$

при

$$\omega > \omega_1 = 2\pi f_1,$$

и поэтому $F(t)$ может быть представлена согласно уравнению (2) так:

$$F(t) = \int_0^{\omega_1} C(\omega) \cos \omega t \, d\omega + \int_0^{\omega_1} S(\omega) \sin \omega t \, d\omega. \qquad (4)$$

[1] Это, правда, можно сделать иногда направленными антеннами, но мы сейчас будем лишь рассматривать случай, когда антеннами это сделать почему-либо нельзя.

[2] См., например, Смирнов *Курс высшей математики* т. II, изд. 1931 г., стр. 427.

[3] В дальнейшем мы также рассматриваем только функции, удовлетворяющие условиям Дирихле.

Функции же $C(\omega)$ и $S(\omega)$, как и всякие другие, на участке

$$0 < \omega < \omega_1$$

могут быть представлены всегда рядами Фурье, причем эти ряды могут, по нашему желанию, состоять из одних косинусов или одних синусов, если мы возьмем за период двойную длину участка, т.е. $2\omega_1$ [4]. Таким образом:

$$C(\omega) = \sum_0^\infty A_k \cos \frac{2\pi}{2\omega_1} k\omega \tag{5а}$$

и

$$S(\omega) = \sum_0^\infty B_k \sin \frac{2\pi}{2\omega_1} k\omega\,. \tag{5б}$$

Введем следующие обозначения:

$$D_k = \frac{A_k + B_k}{2}\,, \qquad D_{-k} = \frac{A_k - B_k}{2}\,, \tag{6}$$

тогда формулы (5а) и (5б) можно переписать так:

$$C(\omega) = \sum_{-\infty}^{+\infty} D_k \cos \frac{\pi}{\omega_1} k\omega\,, \qquad S(\omega) = \sum_{-\infty}^{+\infty} D_k \sin \frac{\pi}{\omega_1} k\omega\,. \tag{7}$$

Подставляя теперь выражения (7) в формулу (4), мы после некоторых преобразований и интегрирования (см. приложение I) получим уравнение (1), т.е. докажем первую часть теоремы I.

Для доказательства второй части теоремы рассмотрим частный случай $F(t)$, когда спектр частот, из которого она состоит, заключен в пределах от 0 до f_1 и выражается уравнениями (7), в которых все D_k, кроме одного, равны нулю. Такая $F(t)$, очевидно, будет состоять из одного члена ряда (1). Значит, и наоборот: если $F(t)$ состоит из одного, любого члена ряда (1), то весь ее спектр заключен в пределах от 0 до f_1. А поэтому и сумма из любых отдельных членов ряда (1), т.е. сам ряд (1), будет состоять из частот, заключенных в пределах от 0 до f_1, что и требовалось доказать.

Все члены ряда (1) подобны и отличаются лишь сдвигом по времени и множителями D_k. Один из членов, имеющий индекс k, изображен на рис. 1, он имеет максимум при $t = k/(2f_1)$ и постепенно уменьшающуюся амплитуду в обе стороны.

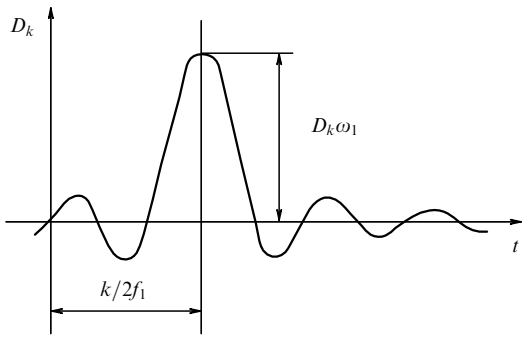


Рис. 1

Теорема II. Любую функцию $F(t)$, состоящую из частот от 0 до f_1, можно непрерывно передавать с любой точностью при помощи чисел, следующих друг за другом через $1/(2f_1)$ секунд. Действительно, измеряя величину $F(t)$ при $t = n/(2f_1)$ (n — целое число), мы получим:

$$F\left(\frac{n}{2f_1}\right) = D_n\omega_1\,. \tag{8}$$

Так как все члены ряда (1) для этого значения t обращаются в нули, кроме члена с $k = n$, который, как это легко можно получить, раскрывши неопределенность, будет равняться $D_n\omega_1$. Таким образом, через каждую $1/(2f_1)$-ю секунду мы сможем узнавать очередное D_k. Передавая эти D_k по очереди через каждые $1/(2f_1)$ секунд, мы сможем по ним согласно уравнению (1) почленно восстановить $F(t)$ с любой точностью.

Теорема III. Можно непрерывно и равномерно передавать произвольные числа D_k со скоростью N чисел в секунду при помощи функции $F(t)$, имеющей слагаемые на частотах больших $f_1 = N/2$ сколь угодно малыми.

Действительно, будем по получению каждого числа строить функцию $F_k(t)$ такую, что

$$\begin{aligned} &\text{при} \quad t < \frac{k}{2f_1} - T \qquad F_k(t) = 0\,,\\ &\text{при} \quad \frac{k}{2f_1} - T < t < \frac{k}{2f_1} + T\\ &\qquad F_k(t) = D_k\,\frac{\sin\omega_1\bigl(t - k/(2f_1)\bigr)}{t - k/(2f_1)}\,,\\ &\text{при} \quad t > \frac{k}{2f_1} + T \qquad F_k(t) = 0\,, \end{aligned} \tag{9}$$

и передавать их сумму $F(t)$. Если бы $T = \infty$, то полученная функция $F(t)$ состояла бы исключительно из частот меньших f_1, так как мы получили бы тогда ряд (1), но, к сожалению, такие бесконечные ряды членов строить невозможно, поэтому будем ограничиваться конечными T. Докажем, что чем больше T, тем амплитуды на частотах $f > f_1$ будут становиться меньше и могут быть сделаны сколь угодно малыми. Для этого найдем амплитуды $C(\omega)$ и $S(\omega)$ для функции (9) подстановкой ее в уравнение (3). Получим:

$$C(\omega) = \frac{1}{\pi}\int_{k/(2f_1)-T}^{k/(2f_1)+T} D_k\,\frac{\sin\omega_1\bigl(t - k/(2f_1)\bigr)}{t - k/(2f_1)}\cos\omega t\,\mathrm{d}t\,,$$
$$S(\omega) = \frac{1}{\pi}\int_{k/(2f_1)-T}^{k/(2f_1)+T} D_k\,\frac{\sin\omega_1\bigl(t - k/(2f_1)\bigr)}{t - k/(2f_1)}\sin\omega t\,\mathrm{d}t\,. \tag{10}$$

После интегрирования (см. приложение II) будем иметь

$$C(\omega) = \frac{D_k}{\pi}\cos\omega\,\frac{k}{2f_1}\left[\mathrm{Si}\,T(\omega+\omega_1) - \mathrm{Si}\,T(\omega-\omega_1)\right],$$
$$S(\omega) = \frac{D_k}{\pi}\sin\omega\,\frac{k}{2f_1}\left[\mathrm{Si}\,T(\omega+\omega_1) - \mathrm{Si}\,T(\omega-\omega_1)\right]. \tag{11}$$

[4] См. Смирнов *Курс высшей математики* т. II, изд. 1931 г., стр. 385.

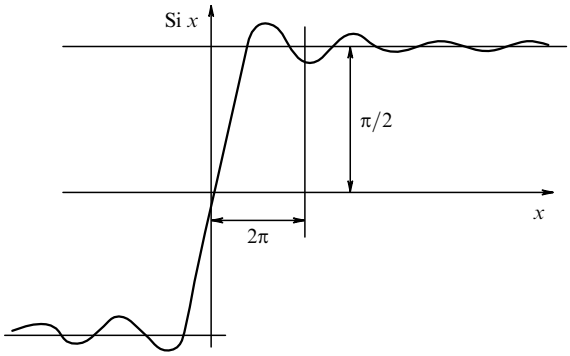


Рис. 2.

В этом выражении Si обозначает интегральный синус, т.е. функцию

$$\mathrm{Si}\, x = \int_0^x \frac{\sin y}{y}\, \mathrm{d}y\,. \qquad (12)$$

Значения этой функции вычислены и имеются в таблицах [5], на рис. 2 она изображена графически.

Как видно из рисунка, $\mathrm{Si}\, x$ при $x \to \pm\infty$ стремится к $\pm\pi/2$.

Рассмотрим значение квадратной скобки в выражении (11). На рисунке 3а дано графическое изображение ее при $T = 3/(2f_1)$, на рис. 3б — при $T = 6/(2f_1)$, на рис. 3в — при $T = 24/(2f_1)$ и на рис. 3г — при $T = \infty$.

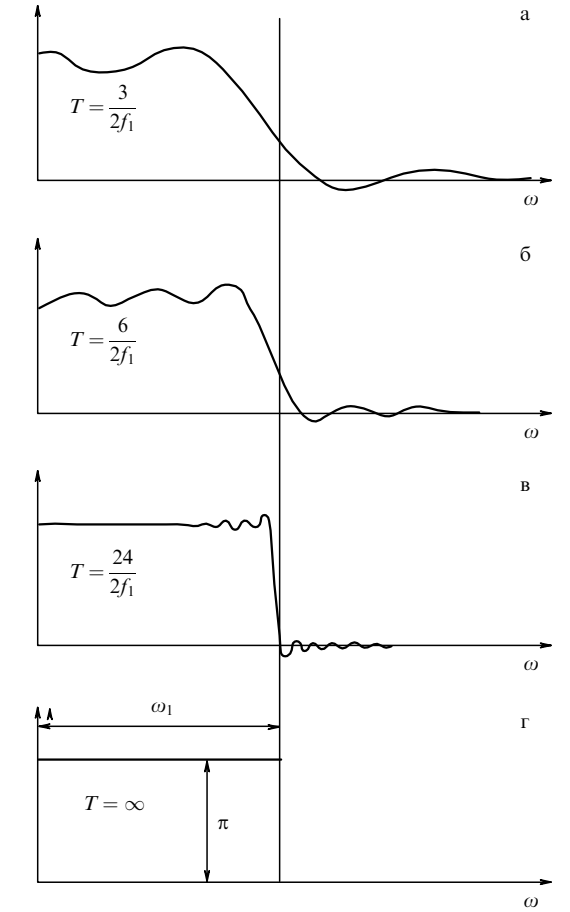


Рис. 3.

Как видно из этих рисунков, квадратная скобка в выражении (11) с увеличением T стремится к пределам рис. 3г, т.е.

при $\omega > \omega_1$ $\quad [\ ] = 0\,,$

при $\omega < \omega_1$ $\quad [\ ] = \pi\,.$

Это также видно и непосредственно из выражения (11), так как при увеличении T увеличивается как бы масштаб при ω и Si делается очень быстро затухающим.

Таким образом, полученная сумма из $F_k(t)$ будет иметь амплитуды на частотах $f > f_1$ сколь угодно малыми, если взять T достаточно большим.

По принятой функции $F(t)$ легко восстановить передаваемые числа D_k. Так как при $t = n/(2f_1)$ все члены равны нулю за исключением члена, для которого $k = n$, последний же равен $D_n\,\omega$. Поэтому

$$F\left(\frac{n}{2f_1}\right) = D_n\,\omega\,.$$

Таким образом, мы из нашей функции, измеряя ее значение при $t = k/(2f_1)$, будем в состоянии получить через каждую $t = 1/(2f_1)$-ю секунду значение нового D_k, в секунду же получим $N = 2f_1$ передаваемых чисел, что и требовалось доказать.

Функции, состоящие из частот от f_1 до f_2

Докажем теорему.

Теорема IV. Любая функция $F(t)$, состоящая из частот от f_1 до f_2, может быть представлена так:

$$F(t) = F_1(t)\cos\frac{\omega_2+\omega_1}{2}\,t + F_2(t)\sin\frac{\omega_2+\omega_1}{2}\,t\,, \qquad (13)$$

где $\omega_1 = 2\pi f_1$, $\omega_2 = 2\pi f_2$, а $F_1(t)$ и $F_2(t)$ есть некоторые функции, состоящие из частот от 0 до $f = (f_2 - f_1)/2$. И наоборот: если в уравнении (13) $F_1(t)$ и $F_2(t)$ есть любые функции, состоящие из частот от 0 до $f = (f_2 - f_1)/2$, то $F(t)$ состоит из частот от f_1 до f_2.

Если $F(t)$ состоит лишь из частот от f_1 до f_2, то, очевидно, $C(\omega)$ и $S(\omega)$ для такой функции могут быть представлены так:

$$C(\omega) = S(\omega) = 0 \quad \text{при} \quad \omega > \omega_2 \quad \text{или} \quad \omega < \omega_1\,,$$

$$\left.\begin{aligned} C(\omega) &= \sum_0^\infty A_k \cos\frac{\pi k}{2(\omega_2-\omega_1)}\,(\omega-\omega_1) \\ S(\omega) &= \sum_0^\infty B_k \sin\frac{\pi k}{2(\omega_2-\omega_1)}\,(\omega-\omega_1) \end{aligned}\right\} \text{при } \omega_1 < \omega < \omega_2,$$

или, опять вводя обозначения

$$\left.\begin{aligned} D_k &= \frac{A_k + B_k}{2}\,, \\ D_{-k} &= \frac{A_k - B_k}{2}\,, \end{aligned}\right. \qquad (6)$$

мы получим

$$\left.\begin{aligned} C(\omega) &= \sum_{-\infty}^{+\infty} D_k \cos\frac{\pi}{\omega_2-\omega_1}\,k(\omega-\omega_1)\,, \\ S(\omega) &= \sum_{-\infty}^{+\infty} D_k \sin\frac{\pi}{\omega_2-\omega_1}\,k(\omega-\omega_1) \end{aligned}\right. \qquad (14)$$

при $\omega_1 < \omega < \omega_2$

[5] См., например, E. Jahuke und F. Emde *Funktionentafeln mit Formeln und Kurvern*.

и

$$C(\omega) = S(\omega) = 0 \quad \text{при} \quad \omega > \omega_2 \quad \text{или} \quad \omega < \omega_1 . \qquad (14)$$

Подставляя уравнения (14) в уравнение (2), мы получим после интегрирования и некоторого преобразования (см. приложение III):

$$F(t) = \left[2\sum_{-\infty}^{+\infty}(-1)^n D_{2n}\,\frac{\sin(\omega_2-\omega_1)/2\{t-k/(f_2-f_1)\}}{t-k/(f_2-f_1)}\right]\times$$
$$\times\cos\frac{\omega_2+\omega_1}{2}\,t+$$
$$+\left[2\sum_{-\infty}^{+\infty}(-1)^n D_{2n+1}\,\frac{\sin(\omega_2-\omega_1)/2\{t-(k+1/2)/(f_2-f_1)\}}{t-(k+1/2)/(f_2-f_1)}\right]\times$$
$$\times\sin\frac{\omega_2+\omega_1}{2}\,t\,, \qquad (15)$$

или, обозначая

$$F_1(t) = 2\sum_{-\infty}^{+\infty}(-1)^n D_{2n}\,\frac{\sin(\omega_2-\omega_1)/2\left[t-k/(f_2-f_1)\right]}{t-k/(f_2-f_1)}\,, \qquad (16)$$

$$F_2(t) = 2\sum_{-\infty}^{+\infty}(-1)^n D_{2n+1}\times$$
$$\times\,\frac{\sin(\omega_2-\omega_1)/2\left[t-(k+1/2)/(f_2-f_1)\right]}{t-(k+1/2)/(f_2-f_1)} \qquad (17)$$

и принимая во внимание, что согласно теореме I $F_1(t)$ и $F_2(t)$ должны обязательно состоять из спектра частот от 0 до $f=(f_2-f_1)/2$, так как ряды (16) и (17) отличаются от ряда (1) лишь обозначением, можно считать первую часть теоремы IV доказанной.

Так как рядами (16) и (17) можно, согласно теореме I, представить любые функции $F_1(t)$ и $F_2(t)$, если они состоят из частот от 0 до $f=(f_2-f_1)/2$, и так как на коэффициенты D_k, входящие в эти ряды, не наложены никакие условия, то, очевидно, верна и вторая часть теоремы IV.

Докажем теперь две теоремы, которые являются обобщением теорем II и III.

Теорема V. Любую функцию $F(t)$, состоящую из частот от f_1 до f_2, можно непрерывно передавать с любой точностью при помощи чисел, передаваемых друг за другом через $1/[2(f_2-f_1)]$ секунд.

Действительно, при $t=k/(f_2+f_1)$ (k — целое число) мы согласно формуле (13) получим:

$$F\left(\frac{k}{f_2+f_1}\right) = F_1\left(\frac{k}{f_2+f_1}\right), \qquad (18)$$

так как при этом значении t косинус равен 1, а синус — 0. Когда же $t=(k+1/2)/(f_2+f_1)$, мы получим

$$F\left(\frac{k+1/2}{f_2+f_1}\right) = F_2\left(\frac{k+1/2}{f_2+f_1}\right)$$

по аналогичным соображениям.

Таким образом, через каждую $1/(f_2+f_1)$-ю секунду мы будем в состоянии узнавать по одному значению $F_1(t)$ и $F_2(t)$, по этим значениям мы сможем воспроизводить и сами функции $F_1(t)$ и $F_2(t)$, так как согласно теореме II по так часто следующим числам можно воспроизводить функции, состоящие из частот от 0 до $(f_2+f_1)/2$, функции же $F_1(t)$ и $F_2(t)$ состоят лишь из частот от 0 до $(f_2-f_1)/2$.

Каждую из полученных таким образом функций можно как состоящую из частот 0 до $(f_2-f_1)/2$ передавать, согласно теореме II, числами, следующими друг за другом через $1/(f_2-f_1)$ секунд, а эти две функции одновременно можно передавать, очевидно, числами, следующими друг за другом через $1/[2(f_2-f_1)]$ секунд, по этим числам восстанавливая сначала $F_1(t)$ и $F_2(t)$, мы по ним сможем по формуле (13) восстановить и саму $F(t)$.

Теорема VI. Можно непрерывно и равномерно передавать произвольные числа D_k со скоростью N чисел в секунду при помощи функции $F(t)$, имеющей слагаемые на частотах $f>f_2$ и $f<f_1$ сколь угодно малыми (т.е. практически их не имеющей), если

$$N = 2(f_2-f_1)\,. \qquad (19)$$

Действительно, мы можем передавать согласно теореме III N чисел в секунду при помощи двух функций $F_1(t)$ и $F_2(t)$, причем каждая будет иметь слагаемые на частотах выше $(f_2-f_1)/2$ сколь угодно малыми.

Эти же функции можно непрерывно передавать функцией $F(t)$, имеющей слагаемые на частотах $f>f_2$ и $f<f_1$ сколь угодно малыми. Действительно, по функциям $F_1(t)$ и $F_2(t)$ согласно уравнению (13) мы получим $F(t)$, передавая которую, мы, как указывалось выше, сможем по ней восстанавливать $F_1(t)$ и $F_2(t)$, а по ним и передаваемые числа.

Для доказательства последней теоремы, в которой будет говориться о невозможности передавать при помощи функции, состоящей из ограниченного диапазона частот, беспредельно многого, докажем следующую лемму.

Лемма. Нельзя при помощи M чисел передавать N произвольных чисел, если

$$M < N\,. \qquad (20)$$

Предположим, что это сделать можно.

Тогда, очевидно, M чисел $m_1,\ldots,m_M$ есть какие-то функции N чисел $n_1,\ldots,n_N$, т.е.

$$\begin{aligned} m_1 &= \varphi_1(n_1,\ldots,n_N)\,,\\ m_2 &= \varphi_2(n_1,\ldots,n_N)\,,\\ &\ldots\ldots\ldots\ldots\\ m_M &= \varphi_M(n_1,\ldots,n_N)\,, \end{aligned} \qquad (21)$$

и мы, очевидно, должны, зная лишь M чисел $m_1,\ldots,m_M$ и, конечно, зная функции $\varphi_1,\ldots,\varphi_M$, суметь восстановить по ним числа $n_1,\ldots,n_N$.

Но это равносильно решению M уравнений (21) с N неизвестными, что сделать невозможно, если уравнений меньше, чем неизвестных, т.е. справедливо неравенство (20).

Теорема VII. Можно непрерывно передавать произвольные, следующие друг за другом равномерно числа со скоростью N чисел в секунду и M произвольных

функций $F_1(t), \ldots, F_M(t)$ с диапазонами частот шириной $\Delta f_1, \ldots, \Delta f_M$ при помощи непрерывно следующих друг за другом чисел со скоростью N' чисел в секунду и при помощи M' функций $F_1'(t), \ldots, F_{M'}'(t)$ с диапазонами частот $\Delta f_1', \ldots, \Delta f_{M'}'$, если

$$N + 2\sum_1^M \Delta f_k \leqslant N' + 2\sum_1^{M'} \Delta f_k' . \qquad (22)$$

И это никаким образом сделать нельзя, если

$$N + 2\sum_1^M \Delta f_k > N' + 2\sum_1^{M'} \Delta f_k' . \qquad (23)$$

Первая часть этой теоремы доказывается на основании теорем V и VI.

Действительно, на основании теоремы V мы можем передавать наши N чисел в секунду и M кривых при помощи P чисел в секунду, если

$$P = N + 2\sum_1^M \Delta f_k . \qquad (24)$$

А эти P чисел в секунду можно отчасти передавать при помощи N' чисел в секунду, а отчасти по теореме VI при помощи кривых $F_1'(t), \ldots, F_{M'}'(t)$, если справедливо равенство (22).

Вторую часть теоремы докажем от противного, исходя из леммы.

Пусть нам нужно передавать P произвольных чисел в секунду, это по теореме VI можно сделать, передавая N чисел в секунду и функции $F_1(t), \ldots, F_M(t)$ с диапазонами частот $\Delta f_1, \ldots, \Delta f_M$, если справедливо равенство (24).

А эти функции и числа, если была бы несправедлива вторая часть теоремы, можно было бы передавать при помощи функций $F_1'(t), \ldots, F_{M'}'(t)$ и N' чисел в секунду. Последние же числа и функции можно согласно теореме V передавать при помощи P' чисел в секунду, если

$$P' = N' + 2\sum_1^{M'} \Delta f_k' . \qquad (25)$$

Другими словами, мы смогли бы непрерывно передавать P чисел в секунду при помощи P' чисел в секунду, хотя согласно равенствам (24) и (25) и неравенству (23)

$$P > P' .$$

Таким образом, предположение, что вторая часть теоремы VII не верна, приводит нас к недопустимому, согласно доказанной лемме, результату.

Пропускная способность при телефонной передаче

Разговор, музыка и другие объекты телефонной передачи являются произвольными функциями времени, состоящими из спектра частот, ширина которого вполне определённа и зависит от того, насколько полно мы хотим передавать звук.

Передавая эту функцию по проволоке или по радио, мы превращаем ее в другую функцию времени, которую собственно уже и передаем. Причем эта последняя функция должна обязательно, согласно теореме VII, при непрерывной передаче иметь спектр частот шириной не меньшей, чем та полоса звуковых частот, которую мы хотим передать.

Таким образом, непрерывная телефонная передача не может занимать в эфире или в проволоке меньший диапазон частот, чем ширина спектра звуковых частот, требуемая для данной передачи. Это верно вне зависимости от способа передачи, и нельзя выдумать такого способа, который позволил бы занять при непрерывной передаче более узкий диапазон частот.

Такой минимальный спектр частот, как известно, может дать уже в настоящее время передача на одной боковой полосе.

Оговорка "при непрерывной передаче" имеет большое значение, так как можно, передавая с перерывами какие-нибудь звуки, скажем музыку, занимать меньший диапазон частот, чем ширина звукового спектра, которую мы при этом будем получать. Для этого достаточно записывать передаваемую музыку сначала на граммофонные пластинки, а затем передавать с них, вращая, скажем, вдвое медленнее, чем при записи. Тогда все частоты будут получаться вдвое меньше нормального и мы при передаче сумеем занять вдвое меньший диапазон частот. Восстанавливать такую передачу можно также посредством граммофона. Ясно, что такая передача не может увеличить пропускную способность, так как при ней "эфир" или проволока будут заняты все время, а передача будет идти с перерывами.

Это также не противоречит и теореме VII, так как там оговорено: "произвольную функцию" и "непрерывно" нельзя передавать, а при такой передаче мы можем передавать или с перерывами произвольную функцию, или беспрерывно функцию не совсем произвольную, а имеющую уже известные перерывы.

Из теоремы VII также следует, что нельзя увеличить пропускную способность путем применения каких-нибудь селекций не частотного характера (не касаясь направленных антенн) или еще чем-нибудь подобным.

Действительно, если бы это можно было бы сделать, то, применяя эти способы, можно было бы с одного места передавать в другое, скажем, n телефонных передач одновременно со спектрами частот шириной Δf каждая, занимая для этого диапазон частот, меньший, чем $n\Delta f$.

Но при такой передаче напряженности поля (или токи в проволоке) от разных передач смешались бы в одну какую-то функцию времени со спектрами частот меньших $n\Delta f$, которая и будет восприниматься приемниками. Получится, что мы смогли передать n функций времени с диапазонами частот шириной Δf при помощи одной функции с диапазоном частот, меньшим, чем $n\Delta f$, что, согласно теореме VII, совершенно невозможно.

Из сказанного ясно, что для телефона увеличить пропускную способность эфира можно, лишь применяя направленные антенны или расширяя эксплуатируемый диапазон частот путем использования ультракоротких волн.

Передача изображений и телевидение со всеми полутенями

При передаче изображений и телевидении нужно передавать степень черноты каких-то N элементов в секунду, а это равносильно передаче произвольных чисел со скоростью N чисел в секунду. Если мы это хотим сделать при помощи функции времени, как это всегда и делается, то по теореме VII она должна занять диапазон частот, не меньший, чем $N/2$ периодов в секунду. Таким образом,

сразу видно, что полосу частот и тут сократить нельзя больше, чем это позволяет сделать передача на одной боковой полосе. Правда, для осуществления и этого могут встретиться большие технические трудности из-за фазовых искажений возможных при такой передаче.

Нельзя сократить полосу частот и при помощи какой-нибудь "групповой развертки изображений" (развертке не по отдельным элементам), так как и при такой развертке придется все же передать, правда, каким-то другим способом, степень почернения тех же N элементов в секунду, т.е. N произвольных чисел в секунду, что сделать никак с уменьшенным диапазоном частот нельзя.

Не смогут и тут помочь нечастотные методы селекций (не включая направленных антенн) по тем же основаниям, как и при телефонной передаче.

Телеграфная передача и передача изображений без полутеней или с ограниченным количеством их

При телеграфной передаче, а также при передаче изображений без полутеней или с вполне определенными заранее известными полутенями, мы имеем дело опять с передачей каких-то N элементов в секунду, что равносильно передаче N чисел в секунду, но величина этих элементов и, значит, чисел не может быть вполне произвольной, а должна иметь вполне определенные, наперед известные значения. Поэтому к этим передачам нельзя прямо применять выше выведенные теоремы, так как там говорится о передаче произвольных, наперед совершенно неизвестных чисел.

Действительно, для этих передач можно сократить необходимый диапазон частот во сколько угодно раз, а следовательно, по крайней мере теоретически, увеличить пропускную способность также в любое число раз.

Для этого можно поступать таким образом: скажем, мы хотим передавать со скоростью N элементов в секунду элементы, которые могут иметь значение либо 0, либо 1, и занять для этого диапазон частот всего лишь шириной $N/4$ (вместо $N/2$ по теореме VII). Для этого будем передавать два таких элемента посредством одного элемента (или числа), хотя бы согласно следующей таблице, где в графе I дано значение первого элемента, в графе II — второго, а в графе III — значение элемента, которым мы хотим их передать.

I	II	III
0	0	0
1	0	1
1	1	2
0	1	3

Таким образом мы сможем передавать N элементов в секунду, имеющих по два значения, при помощи $N/2$ элементов в секунду, могущих иметь по 4 значения, которые, согласно теореме VII, могут передаваться при помощи диапазона частот шириной $N/4$.

Практически такую замену двух элементов одним можно осуществить хотя бы по схеме рис. 4, где Φ_1 и Φ_2 — два фотоэлемента или два телеграфных аппарата, причем Φ_1 приводит в действие модулятор M_1, посылающий в линию амплитуду, равную единице, Φ_2 же работает с модулятором M_2, посылающим амплитуду, равную 3. При работе Φ_1 и Φ_2 сразу приводятся в действие оба

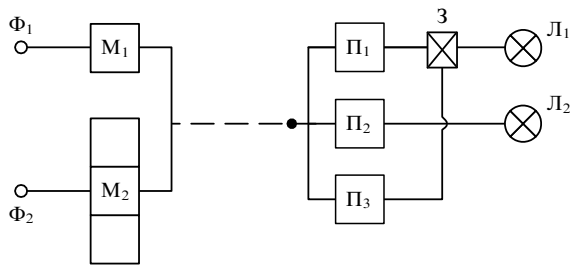


Рис. 4.

модулятора, и так как они включены на встречу, то посылается амплитуда, равная 2. На прием принимаемый сигнал поступает на три приемника, причем первый, $П_1$, начинает работать от амплитуды 1, второй, $П_2$, — от амплитуды 2 и третий, $П_3$, — от амплитуды 3. Первый приемник $П_1$ приводит в действие $Л_1$, второй — $Л_2$, а третий при приходе амплитуды, равной трем, — запирает доступ от 1 приемника на $Л_1$. При помощи такой схемы мы получим указанное выше сокращение полосы частот.

При такой передаче ввиду того, что при ней становится необходимым различать вместо двух четыре градации принимаемых сигналов, необходимо, очевидно, будет увеличить мощность передатчика в $3^2 = 9$ раз, по сравнению с обычной передачей.

Возможно сократить аналогичным образом полосу частот и в n раз, передавая n элементов, могущих иметь по два значения, при помощи одного элемента, который должен для этого, очевидно, иметь 2^n значений (по числу комбинаций из n элементов, имеющих по два значения). Но для такой передачи необходимо увеличение мощности в $(2^n - 1)^2$ раз.

При передаче изображений с определенным количеством заданных наперед полутеней каждый элемент должен иметь несколько, скажем m (для этого случая $m > 2$), значений. Для сокращения полосы частот при такой передаче в n раз можно заменить n передаваемых элементов одним, который должен иметь возможность принимать m^n значений (по числу возможных комбинаций из n элементов, имеющих m возможных значений каждый). Мощность при этом, очевидно, необходимо будет увеличить в $[(m^n - 1)^2]/[(m - 1)^2]$ раз.

Как видно, такое уменьшение полосы частот требует колоссального увеличения мощности.

Кроме того, приведенные здесь способы будут очень плохи при передаче на коротких волнах из-за фадингов **.

Для проволочной связи уменьшение таким способом полосы частот может иметь практическое значение уже и сейчас, так как мощности, там необходимые, малы и нет быстрых изменений силы приема.

Приложение I

Подставляя выражение (7) в уравнение (4), мы получим:

$$F(t) = \int_0^{\omega_1} \sum_{-\infty}^{+\infty} D_k \cos \frac{\pi}{\omega_1} k\omega \cos \omega t \, \mathrm{d}\omega +$$

$$+ \int_0^{\omega_1} \sum_{-\infty}^{+\infty} D_k \sin \frac{\pi}{\omega_1} k\omega \sin \omega t \, \mathrm{d}\omega =$$

** От англ. fading — замирание (сигнала). (*Примеч.* Н.В. Котельниковой.)

$$= \sum_{-\infty}^{+\infty} D_k \int_0^{\omega_1} \left(\cos \frac{\pi}{\omega_1} k\omega \cos \omega t + \sin \frac{\pi}{\omega_1} k\omega \sin \omega t \right) \mathrm{d}\omega =$$

$$= \sum_{-\infty}^{+\infty} D_k \int_0^{\omega_1} \left(\cos \omega \left(t - \frac{\pi}{\omega_1} k \right) \right) \mathrm{d}\omega ,$$

или, интегрируя и заменяя в круглой скобке ω_1 на $2\pi f_1$, получим

$$F(t) = \sum_{-\infty}^{+\infty} D_k \frac{\sin \omega_1 \left(t - k/(2f_1) \right)}{t - k/(2f_1)} .$$

Приложение II

В

$$C(\omega) = \frac{1}{\pi} \int_{k/(2f_1)-T}^{k/(2f_1)+T} D_k \frac{\sin \omega_1 \left(t - k/(2f_1) \right)}{t - k/(2f_1)} \cos \omega t \, \mathrm{d}t$$

сделаем подстановку

$$t = u + \frac{k}{2f_1} , \quad \mathrm{d}t = \mathrm{d}u ,$$

тогда

$$C(\omega) = \frac{1}{\pi} \int_{-T}^{T} D_k \frac{\sin \omega_1 u}{u} \cos \omega \left(u + \frac{k}{2f_1} \right) \mathrm{d}u =$$

$$= \frac{1}{\pi} \int_{-T}^{T} D_k \frac{\sin \omega_1 u \cos \omega u}{u} \cos \omega \frac{k}{2f_1} \, \mathrm{d}u +$$

$$+ \frac{1}{\pi} \int_{-T}^{T} D_k \frac{\sin \omega_1 u \sin \omega u}{u} \sin \omega \frac{k}{2f_1} \, \mathrm{d}u .$$

Функция, стоящая под вторым интегралом, при переходе через нуль меняет свой знак, оставаясь по величине той же, поэтому второй интеграл равен нулю.

Функция же под первым интегралом не меняется при замене u на $-u$, и поэтому пределы этого интеграла можно взять от 0 до T, помножив при этом интеграл на два. Значит,

$$C(\omega) = \frac{2D_k}{\pi} \cos \omega \frac{k}{2f_1} \int_0^T \frac{\sin \omega_1 u \cos \omega u}{u} \, \mathrm{d}u ,$$

или

$$C(\omega) = \frac{D_k}{\pi} \cos \omega \frac{k}{2f_1} \left[\int_0^T \frac{\sin(\omega_1 + \omega) u}{u} \, \mathrm{d}u - \right.$$

$$\left. - \int_0^T \frac{\sin(\omega - \omega_1) u}{u} \, \mathrm{d}u \right] .$$

Заменяя в первом интеграле

$$(\omega_1 + \omega) u = y ,$$

а во втором

$$(\omega - \omega_1) u = y ,$$

получим

$$C(\omega) = \frac{D_k}{\pi} \cos \omega \frac{k}{2f_1} \left[\int_0^{(\omega+\omega_1) T} \frac{\sin y}{y} \, \mathrm{d}y - \right.$$

$$\left. - \int_0^{(\omega-\omega_1) T} \frac{\sin y}{y} \, \mathrm{d}y \right] .$$

Стоящие в скобках интегралы не берутся. Это, очевидно, будут какие-то функции верхнего предела. Принято эти функции называть интегральными синусами. Введя это понятие, получим:

$$C(\omega) = \frac{D_k}{\pi} \cos \omega \frac{k}{2f_1} \left[\mathrm{Si}\, T(\omega + \omega_1) - \mathrm{Si}\, T(\omega - \omega_1) \right] .$$

Проделывая совершенно то же с $S(\omega)$, мы получим уравнение (11).

Приложение III

Подставляя уравнения (14) в уравнение (2), получим

$$F(t) = \int_{\omega_1}^{\omega_2} \sum_{-\infty}^{+\infty} D_k \cos \frac{\pi k (\omega - \omega_1)}{\omega_2 - \omega_1} \cos \omega t \, \mathrm{d}\omega +$$

$$+ \int_{\omega_1}^{\omega_2} \sum_{-\infty}^{+\infty} D_k \sin \frac{\pi k (\omega - \omega_1)}{\omega_2 - \omega_1} \sin \omega t \, \mathrm{d}\omega .$$

Пределы взяты от ω_1 и ω_2, потому что

$$C(\omega) = S(\omega) = 0$$

при

$$\omega < \omega_1 \quad \text{или} \quad \omega > \omega_2 .$$

После тригонометрических преобразований

$$F(t) = \sum_{-\infty}^{+\infty} D_k \int_{\omega_1}^{\omega_2} \cos \left[\omega \left(t - \frac{\pi k}{\omega_2 - \omega_1} \right) + \frac{\pi k \omega_1}{\omega_2 - \omega_1} \right] \mathrm{d}\omega =$$

$$= \sum_{-\infty}^{+\infty} D_k \frac{\sin \left[\omega_2 [t - \pi k/(\omega_2 - \omega_1)] + \pi k \omega_1/(\omega_2 - \omega_1) \right]}{t - \pi k/(\omega_2 - \omega_1)} -$$

$$- \frac{\sin \left[\omega_1 [t - \pi k/(\omega_2 - \omega_1)] + \pi k \omega_1/(\omega_2 - \omega_1) \right]}{t - \pi k/(\omega_2 - \omega_1)} .$$

Заменяя разность синусов на произведение и произведя упрощения, получим:

$$F(t) = 2 \sum_{-\infty}^{+\infty} D_k \cos \left(\frac{\omega_2 + \omega_1}{2} t - \frac{\pi}{2} k \right) \times$$

$$\times \frac{\sin \left[(\omega_2 - \omega_1)/2 \{ t - k/[2(f_2 - f_1)] \} \right]}{t - k/[2(f_2 - f_1)]} ,$$

или, группируя члены с четными и нечетными k вместе, получим уравнение (15).

Выводы

1) Ввиду имеющейся уже в настоящее время "тесноты в эфире" и в связи с дальнейшим бурным развитием радиотехники, в особенности с развитием коротковолновых телефонных передач и передач изображений, вопрос об изыскании способов увеличения пропускной способности эфира должен быть поставлен перед научно-исследовательскими институтами во всей остроте.

Вопрос об увеличении пропускной способности проволоки имеет также большое экономическое значение. Поэтому этот вопрос следует тоже изучать.

2) Так как нельзя никакими способами, как, например, сужением полосы частот отдельных передач, примене-

нием каких-либо методов для разделения передач с накладывающимися друг на друга частотами и т.п., увеличить пропускную способность эфира или проволоки при передаче изображений и телефона больше, чем это позволяет сделать обычная передача с одной боковой полосой, то все попытки в этих направлениях следует оставить как неосуществимые.

3) Для телеграфа и передачи изображений без полутеней или с ограниченным количеством их пропускную способность можно теоретически повысить беспредельно, но это связано с большим увеличением мощности и усложнением аппаратуры. Поэтому надо думать, что такое сужение полосы частот может в ближайшее время найти применение лишь в проволочной связи, где над этим вопросом следует работать.

4) Необходимо для первой категории передач (телефон и передача изображений с полутенями) направить все усилия на разработку методов приема и передачи на одной боковой полосе как методов, позволяющих максимально возможно использовать эфир и проволоку.

Цель разработки — усовершенствовать и упростить аппаратуру, очень сложную в настоящее время.

5) Необходимо изучить вопрос об увеличении пропускной способности эфира при помощи направленных антенн как приемных, так и передающих.

6) Необходимо увеличить диапазон эксплуатируемых в эфире частот путем загрузки, где возможно, ультракоротких волн, а также изучением этого диапазона частот.

7) Необходимо изучать вопрос об увеличении стабильности частоты радиостанций, что позволит уплотнить эфир.

PACS numbers: **89.70.+c**, 95.85.Bh, 96.30.Ea

Роль В.А. Котельникова в становлении радиофизики и радиотехники

Н.А. Арманд

1. Введение

Писать о роли В.А. Котельникова в развитии радиофизики и радиотехники не так просто. Это связано как с многообразием направлений, к становлению и развитию которых он "приложил руку", так и с научными результатами, часть которых была получена более 70 лет тому назад и с современной точки зрения представляется "очевидной". Сложность связана также с тем, что Владимир Александрович не был "любителем" публиковаться. В частности, его знаменитая теорема не была толком опубликована вовсе, а классическая работа по потенциальной помехоустойчивости была издана лишь в 1956 г., спустя 10 лет после ее выполнения.

2. Теорема

В 1932–1933 гг. 25-летний инженер В.А. Котельников задался мыслью о том, можно ли без искажений передавать сигнал в полосе частот меньшей, чем это позволяет передача "на одной боковой полосе". В современном представлении это означает возможность прохождения сигналов без искажения через канал, спектральная пропускная способность которого меньше спектральной ширины сигнала. Нам это представляется абсурдным, но в то время (1933 г.), когда проблемы спектральной фильтрации были не до конца понятны инженерам, подобная постановка вопроса представлялась разумной. В связи с этим следует вспомнить споры того времени о том, что представляет собой амплитудно-модулированный сигнал: синусоидальное колебание с медленно изменяющейся амплитудой или набор спектральных компонент. Результаты исследований В.А. Котельникова были подготовлены в виде доклада "О пропускной способности "эфира" и проволоки в электросвязи" к I Всесоюзному съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности. Съезд не состоялся, но подготовленные к нему материалы были изданы [1], что и явилось официальным подтверждением приоритета В.А. Котельникова в доказательстве знаменитой теоремы отсчетов.

На самом деле работа содержала семь теорем, но все они являлись в той или иной степени развитием основной теоремы, которая гласит, что любая функция $f(t)$ с ограниченным спектром ширины B представима в виде ряда

$$f(t)=\sum_{n=-\infty}^{\infty} f\left(\frac{n}{2B}\right)\operatorname{sinc}(2\pi Bt-n\pi)\,,\qquad \operatorname{sinc}(x)=\frac{\sin x}{x}\,.$$

По существу теорема утверждает, что любая функция полностью представима совокупностью своих отсчетов, выбираемых в дискретные моменты времени $t_n=n/2B$. Если излучить сверхкороткие импульсы с амплитудами, равными отсчетам функции в указанные дискретные моменты, то приемник, имеющий фильтр нижних частот со спектральной шириной B, сформирует колебания вида $\operatorname{sinc}(x)$ и сумма этих колебаний вновь даст неискаженную функцию $f(t)$. Указанная процедура передачи сигнала и его приема поясняется на рис. 1. Поскольку фильтр нижних частот приемника должен иметь ширину полосы не меньшую спектральной ширины сигнала, то попытки уменьшения этой полосы при неискажаемой передаче сигнала подобны попыткам создания perpetuum mobile, о чем и предупреждал автор работы [1] при постановке задачи.

Интересно отметить, что Владимир Александрович в 1936 г. пытался опубликовать свою теорему в журнале *Электричество*. Однако в публикации ему было отказано со ссылкой на перегруженность портфеля журнала и на узкий интерес его статьи. Знали бы инициаторы отказа, о чем они говорят! На самом деле теорема имеет более широкое значение по сравнению с задачей, приведшей к ее доказательству. По существу, она указала путь представления непрерывных функций в цифровом виде и тем самым стала одним из теоретических фундаментов цифровой техники, бурно развивающейся в последние десятилетия. При постановке вопроса о представлении непрерывной функции в цифровом виде в первую очередь возникает вопрос о том, как часто следует выбирать значения функции, чтобы достаточно точно отразить ее вид. Первый и наивный ответ гласит: чем чаще, тем лучше. Это означает, что для неискаженной передачи любого сообщения необходимо использовать достаточно частые выборки. Но в системах связи мы имеем дело с сигналами с ограниченной шириной спектра. Такие сигналы не могут изменяться во времени как угодно быстро. Поэтому выборки сигнала, взятые за слишком короткий интервал времени, могут оказаться

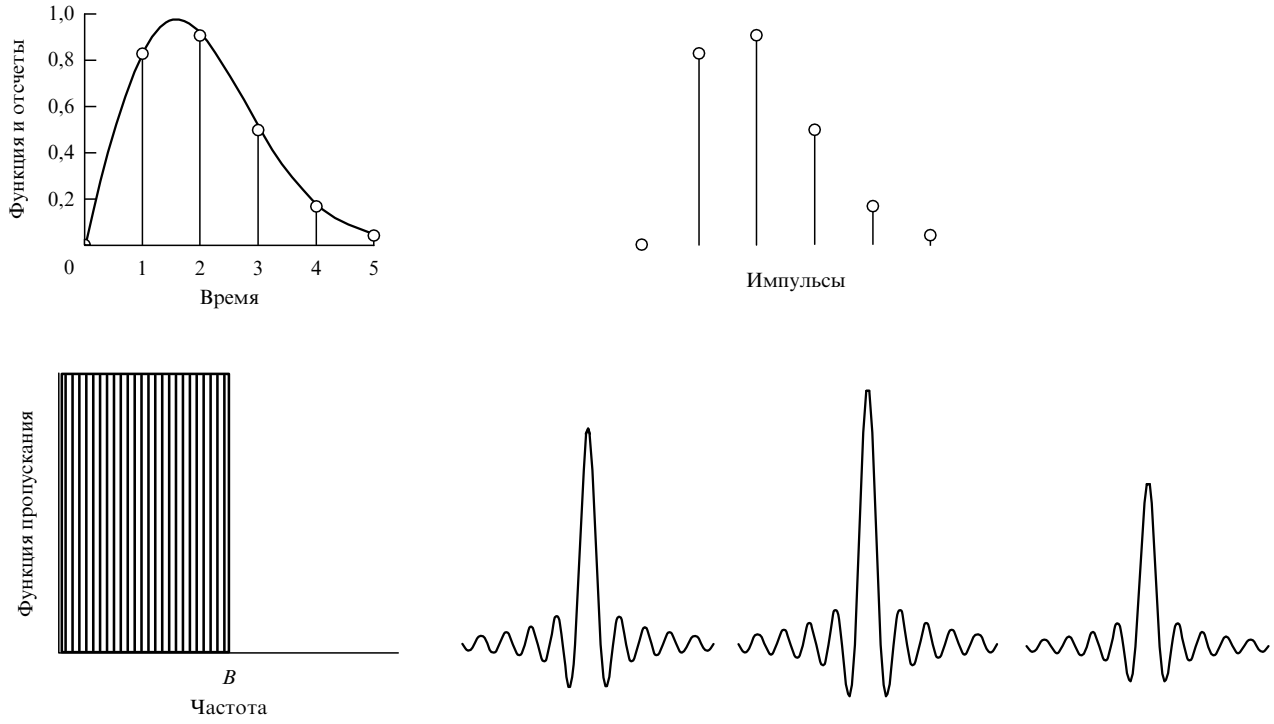


Рис. 1. К теореме отсчетов.

мало отличающимися друг от друга и использование их полной совокупности оказывается излишним. Функция с ограниченным спектром может существенно изменяться лишь за интервалы времени не короче, чем обратная величина ширины полосы их спектра. Это понял Найквист, который, по-видимому, одним из первых выразил мысль, что выборки сигнала должны различаться интервалами времени, равными приблизительно обратной полосе его спектральной ширины [2]. Это часто дает основание, особенно западным ученым, употреблять термин "правило выборок Найквиста". Однако рассуждения Найквиста относились к проблеме неискаженной передачи телеграфного (цифрового) сигнала. Эта проблема отличается от проблемы неискаженной передачи аналогового сигнала, хотя между ними есть много общего, на что указывает профессор Люке в своей статье о происхождении теоремы выборок [3], отмечая, что "первым ученым, точно сформулировавшим теорему о выборках и приложившим ее к проблеме теории и техники связи, является, вероятно, В.А. Котельников". Это утверждение дало основание для награждения Владимира Александровича в 1999 г. премией фонда Эдуарда Рейна за фундаментальные исследования.

Похожая теорема была известна математикам. В частности, ее доказал в 1915 г. Уиттекер, исследуя проблему аппроксимации целых функций конечной степени [4]. В.А. Котельников не был знаком с этой работой. Однако в математике — это одна из многих ординарных теорем. В теории же связи и цифровой технике эта теорема является базовой, и ее доказательство несомненно является заслугой В.А. Котельникова. К сожалению, проблемы с публикацией его теоремы долгое время служили препятствием для широкого ознакомления с ней научной общественности. Теорема выборок стала широко известной лишь после того, как в 1948 г. Шеннон доказал ее вновь [5]. Сейчас нередко эта теорема называется как теорема выборок Уиттекера – Котельникова – Шеннона ("Whittaker – Kotel'nikov – Shannon sampling theorem" [6]).

Теорема Котельникова может быть распространена на любые функции, имеющие ограничения в каком-либо пространстве [7]. Имеется сопряженная теорема, относящаяся к функциям, лимитированным по времени [8]. В частности, возможно формирование коротких импульсов за счет генерации колебаний на дискретных частотах. Диаграмма направленности антенны представляет собой преобразование Фурье от токов, пространственное распределение которых ограниченно апертурой антенны. На этом основании диаграмма направленности также может быть представлена дискретным рядом [9]. При обработке изображений возникает необходимость их представления в цифровом виде, и здесь теорема Котельникова служит одним из важнейших инструментов для осуществления указанной операции.

Одним из интересных примеров является несколько неожиданное применение теоремы для описания дисперсии сигналов [10]. Этот эффект, как известно, возникает при распространении волн в средах, где фазовая скорость является функцией частоты, и выражается в том, что форма сигналов искажается при их распространении. На рисунке 2а представлен неискаженный сигнал, получаемой линейной частотной модуляцией в полосе B. Он имеет форму $\mathrm{sinc}(\xi)$ и поэтому отображается одной компонентой Котельникова. В процессе распространения в плазме форма сигнала искажается и приобретает вид, представленный на рис. 2б. Этот искаженный сигнал имеет уже много компонент Котельникова, количество и амплитуды которых отображают степень искажения сигнала. По их параметрам возможно восстановление формы сигнала [10].

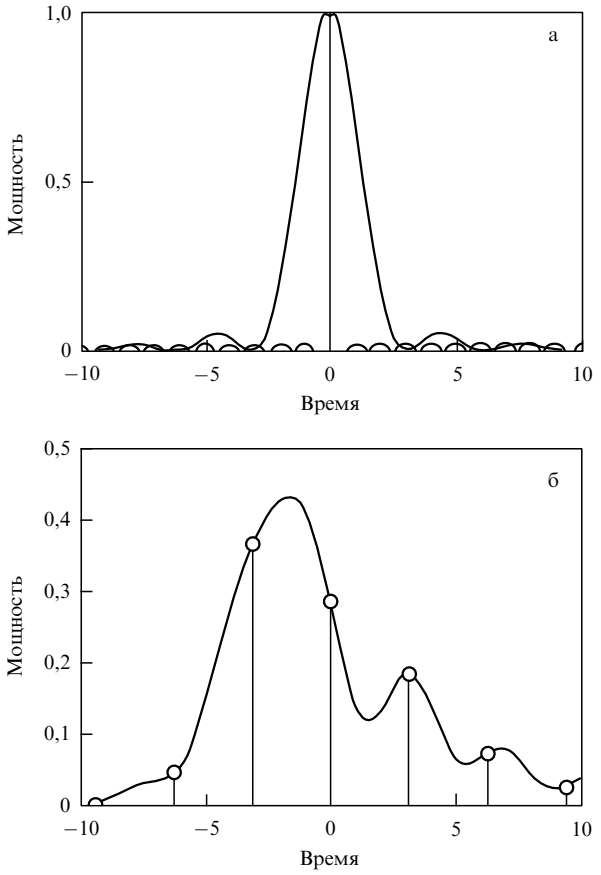


Рис. 2. Теорема отсчетов и дисперсия сигналов.

3. Теория потенциальной помехоустойчивости

В этом разделе мы остановимся на следующей классической работе В.А. Котельникова, посвященной предельной чувствительности приемных систем. В конце 1930-х годов возник кризис в повышении помехоустойчивости систем связи. Всякого рода технические ухищрения наталкивались на некоторый предел, препятствующий дальнейшему повышению чувствительности приемников. Возникал естественный вопрос: является ли это результатом недостаточной изобретательности инженеров или существуют какие-то фундаментальные причины, ставящие предел помехоустойчивости рассматриваемых систем? Ответ на этот вопрос был дан в докторской диссертации В.А. Котельникова "Теория потенциальной помехоустойчивости", написанной в 1946 г. и успешно защищенной в 1947 г. Целью работы было "выявить, можно ли путем усовершенствования приемников при существующих видах сигналов понизить влияние помех? Что может дать в борьбе с помехами изменение формы сигналов? Какие формы сигналов для этого оптимальны?" [11].

В рассматриваемой работе было много принципиально нового и непривычного для инженеров того времени. Прежде всего, это введение ортонормированных функций времени $C_k(t)$, по которым может быть разложен сигнал. Сигнал $A_j(t)$ представлялся в виде суммы

$$A_j(t) = \sum a_{jk}\, C_k(t)\,.$$

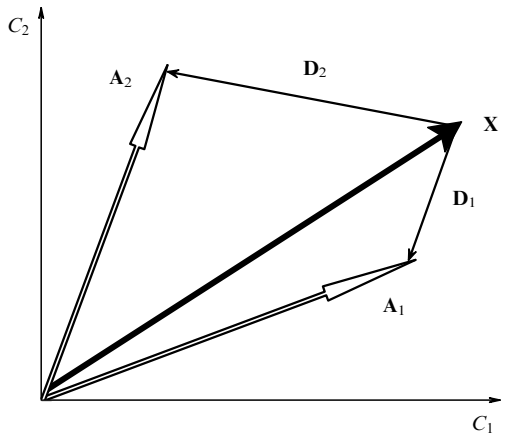


Рис. 3. Геометрическое представление сигналов.

Различные сигналы различаются набором коэффициентов a_{jk}. В случае ограниченного числа базовых функций $C_k(t)$ такое разложение назвали бы представлением сигнала в конечномерном евклидовом пространстве (гильбертовом пространстве) [12]. Сигналы могут рассматриваться в качестве векторов в этом пространстве. Пример такого геометрического представления приведен на рис. 3. Надо заметить, что хотя автор диссертации часто обращается к геометрическому представлению сигнала, однако иллюстраций, подобных рис. 3, в его работе нет. При практических расчетах В.А. Котельников пользуется рядами Фурье, что является естественной данью стандартному спектральному представлению сигнала.

Первой задачей, рассмотренной в работе, является задача распознавания. Ее суть в упрощенном виде представлена на рис. 3. На вход приемника поступает смесь сигнала и шума $\mathbf{X}$. Каков должен быть ответ на выходе приемника — это сигнал $\mathbf{A}_1$ или $\mathbf{A}_2$? Ясно, что это будет $\mathbf{A}_1$, если для евклидовых расстояний справедливо неравенство $|\mathbf{D}_1| < |\mathbf{D}_2|$. Однако соблюдение или несоблюдение этого неравенства носит статистический характер, поскольку из-за случайного поведения шума имеется некоторая вероятность, что рассматриваемое неравенство не соблюдается. Поэтому можно говорить о вероятностной природе правильного выделения сигнала на фоне помех. Отсюда следует определение понятия идеального приемника как дающего минимальное число неправильно воспроизводимых сообщений при наложении помехи. Потенциальная помехоустойчивость характеризуется минимально возможными искажениями. Она равна вероятности неправильного воспроизведения и в случае гауссова шума с равномерным спектром определяется отношением удельной энергии к интенсивности помехи σ^2:

$$\alpha = \frac{1}{2\sigma^2}\int_{-T/2}^{T/2} \left|\mathbf{A}_1(t) - \mathbf{A}_2(t)\right|^2 \mathrm{d}t\,.$$

Здесь T — длительность сигнала. Совсем простой вид это отношение принимает в типичном для радиолокации случае, когда $\mathbf{A}_2(t) = 0$:

$$\alpha = \frac{Q}{2\sigma^2}\,,$$

где Q — энергия сигнала. В этом случае "потенциальная помехоустойчивость будет определяться лишь энергией сигнала и совершенно не будет зависеть от его формы" [11]. Современные специалисты по радиолокации сказали бы, что параметр α является отношением сигнал/шум, которое определяет вероятность ложной тревоги. При большом значении отношения сигнал/шум вероятность правильного выделения сигнала близка к единице, а вероятность ложной тревоги стремится к нулю. Несколько позже (1948 г.) К. Шеннон получил соответствующие результаты для более широкого класса помех. Характерно, что решающую роль для потенциальной помехоустойчивости играет энергия, а не мощность сигнала. Это обстоятельство не всегда всеми понимается. Современные методы формирования сигнала часто рассчитаны на его небольшую мощность, а сам процесс его выделения опирается на сжатие (оптимальную фильтрацию) в приемном устройстве [8]. Окончательный ответ на заданный в начале диссертации вопрос сводится к утверждению, что для повышения помехозащищенности системы связи необходимо увеличивать отношение сигнал/шум, которое оказывается решающим параметром, определяющим вероятность верного выделения сигнала на фоне помех.

В последующих частях работы задача распознавания, о которой мы говорили выше, дополняется задачами оценки параметров и фильтрации. Тем самым охватываются основные проблемы статистической радиотехники. Это и является основой для утверждения о фундаментальном характере диссертации В.А. Котельникова.

Отметим, что ко времени написания работы В.А. Котельникова в теории вероятности и теории случайных процессов математиками был получен ряд важнейших результатов в теории фильтрации, теории оценки параметров, теории статистических решений и т.п. Здесь мы сталкиваемся с ситуацией, аналогичной ситуации с теоремой отсчетов. Результаты математиков не доходили до своего потребителя, и нужны были усилия других специалистов, чтобы они приобрели практический смысл. В 1998 г. была опубликована статья Верду, посвященная пятидесятилетию теории Шеннона [12]. В ней, в частности, говорилось, что наибольший вклад во внедрение теории случайных процессов в инструментарий инженеров связи внесли Винер [13] и Райс [14]. Однако работа Винера, опубликованная в 1949 г., не могла быть известна В.А. Котельникову в 1946 г. Что касается работы Райса, то она была опубликована в 1944 г., и это единственная работа, на которую В.А. Котельников ссылается в своей диссертации. Других ссылок нет потому, что не было предшественников. В связи с этим Владимир Александрович с полным основанием может считаться одним из основоположников статистической радиофизики и радиотехники. Эта его выдающаяся роль почему-то не очень широко отражается в научной печати. То, что статистическое мышление не было распространено среди радиоинженеров в те годы достаточно широко, показывает и сам способ изложения работы В.А. Котельникова. Несмотря на то, что в ней все время речь идет о случайных процессах, там не встретишь термины: корреляция, спектральная плотность и др., хотя неявно они присутствуют. Сама процедура принятия решений строится на байесовской стратегии, но это не упоминается в тексте, а формула для априорной вероятности просто выводится исходя из "разумных" соображений.

Как уже отмечалось, *Теория потенциальной помехоустойчивости* была опубликована лишь в 1956 г., когда широкое признание получили работы многих других авторов. Поэтому эта работа хорошо известна лишь тем, "кто знает", и в последнее время иногда цитируется в основном российскими учеными. Это, в общем-то, естественно. Наука не стоит на месте.

4. Радиолокация планет

Радиолокация планет является еще одним величайшим достижением в научном творчестве В.А. Котельникова. В 1960-х годах развитие ракетно-космической техники открыло возможность запуска космических аппаратов к другим планетам Солнечной системы. Для управления полетами этих аппаратов необходимо было достаточно полное знание положения планет. Астрономические наблюдения, проведенные к тому времени, обеспечили достаточно надежные данные об относительных размерах Солнечной системы, однако для успешной межпланетной навигации необходимо было хорошее знание абсолютных размеров системы. Основной масштабной величиной, характеризующей размеры Солнечной системы, является астрономическая единица (а.е.), равная большой полуоси эллиптической орбиты Земли, или среднему расстоянию Земли от Солнца (около 150 млн км). Она может быть рассчитана, если известно расстояние между двумя планетами. Радиолокация и предоставляет такую возможность. За ее осуществление взялся коллектив, возглавляемый В.А. Котельниковым. При этом Владимир Александрович проявил себя не только как выдающийся ученый, но и как незаурядный организатор. В то время в Евпатории создавался центр дальней космической связи, в состав которого вошли мощный передатчик (≈ 10 кВт) на длине волны 39 см и крупные передающая и приемные антенны АДУ-1000 с эффективной площадью около 1000 м^2. Для успешной реализации радиолокации требовалось создать большое количество аппаратуры для фильтрации сигналов, измерения их спектра, частоты и др. Заметим, что на первых порах вычислительных машин не было, и многие алгоритмы не могли быть реализованы программными методами. Единственным способом было создание соответствующих устройств собственными силами.

То, что в ту пору радиолокация планет была непростым делом, свидетельствовал зарубежный опыт. Первые попытки радиолокации Венеры были предприняты в США в 1958 г. [16] и Англии в 1959 г. [17]. Однако результаты этих экспериментов оказались ошибочными. Это подтвердил и первый опыт группы В.А. Котельникова. В начале работы потенциал радиолокатора был настолько мал, что для выделения сигнала приходилось производить его накопление в течение нескольких часов. Однако по мере развития техники (увеличение мощности передатчика, оснащение приемника малошумящими парамагнитными усилителями, введение линейной частотной модуляции, совершенствование методов выделения сигнала и т.п.) удалось реализовать точность измерения межпланетных расстояний вплоть до относительной величины порядка 10^{-8}, что обусловило определение астрономической единицы с точностью порядка 1 км. Эта точность в тысячи раз лучше точности, достигнутой астрономическими методами. На XVI Генеральной

ассамблее Международного астрономического союза (1967 г.) было принято, что 1 а.е. $= 149597870 \pm 2$ км при скорости света $c = 299792558 \pm 1{,}2$ м с$^{-1}$. Время распространения радиоволн определялось со столь высокой точностью, что при пересчете на расстояние существенной оказалась точность знания скорости света. Следует заметить, что радиолокационные исследования планет проходили одновременно в СССР и США. Существовало соперничество научных групп, и, естественно, многие результаты были аналогичными.

Помимо Венеры проводилась радиолокация Марса, Меркурия и Юпитера. Данные этих измерений также использовались для уточнения величины астрономической единицы. Высокая точность радиолокационных измерений позволила построить теорию движения планет, более точную, нежели теория, построенная на оптических данных. Для построения этой теории пришлось учитывать эффекты общей теории относительности. Тем самым радиолокация планет стала одним из способов, позволяющих проверять выводы этой теории.

Радиолокационные наблюдения позволили уточнить другие параметры планет. Особенно это относится к Венере, для которой удалось уточнить ее радиус, период и направление вращения. В частности, было установлено, что вращение Венеры является обратным (по отношению к направлению ее движения вокруг Солнца) и период равен 243,04 сут. Интересно отметить, что это значение весьма близко к синодическому резонансу с периодом вращения 243,16 сут, при котором Венера при каждом нижнем соединении была бы обращена к Земле одной и той же стороной. Более подробное описание результатов радиолокации планет можно найти, например, в [18].

5. Радиолокационное картографирование Венеры

При осуществлении этой работы, принесшей славу советской космической программе, В.А. Котельников не являлся формальным руководителем. Однако без его активного участия программа радиолокационного картографирования Венеры вряд ли была бы реализована. Здесь необходимо было "синхронизировать", помимо Института радиотехники и электроники АН СССР, работу Научно-производственного объединения им. С.А. Лавочкина, Особого конструкторского бюро Московского энергетического института и ряда других промышленных и академических организаций. Это было под силу лишь такой мощной и авторитетной личности, какой был В.А. Котельников.

В 1983 г. на орбиту вокруг Венеры были запущены искусственные спутники "Венера-15" и "Венера-16", на борту каждого из которых находился радиолокатор с синтезированной апертурой и высотомер. Радиолокатор позволил получить изображение поверхности планеты, перманентно закрытой облаками и потому невидимой в оптическом диапазоне. Таким образом удалось получить карту поверхности планеты с пространственным разрешением 1–2 км, а высотомер обеспечил получение данных о рельефе с разрешающей способностью по высоте 230 м. Тем самым человечество впервые узнало как устроена поверхность северной части Венеры на площади 115 млн км^2 (25 % общей площади Венеры). Результат, несомненно, был выдающимся. Спустя несколько лет эти исследования были продолжены в США во время миссии "Magellan", когда удалось получить изображения почти всей поверхности Венеры с пространственным разрешением порядка 100 м. Планирование этой миссии проводилось уже с учетом результатов советской космической программы. Более подробное описание результатов миссии "Венера-15", "Венера-16" можно найти в [19].

Заметим, что помимо самой радиолокационной съемки проблемой являлись обработка данных радиолокатора и построение изображения планеты. Одной из самых сложных операций обработки в то время был фурье-анализ. Имевшиеся в руках исследователей ЭВМ были слишком маломощны для выполнения этой операции в разумное время. Недаром тогда еще использовались оптические процессоры для обработки данных радаров с синтезированной апертурой, в которых фурье-преобразование радиолокационной голограммы осуществлялось с помощью линзы. Участниками проекта был разработан и создан специальный фурье-процессор, который позволил довести скорость ЭВМ СМ-4 по этому алгоритму до 5×10^7 операций в 1 с и тем самым произвести полностью цифровую обработку радиолокационных данных и построение изображения поверхности. Это был первый в СССР опыт цифровой обработки радиолокационного изображения, который в дальнейшем использовался для создания программ обработки данных радара "Алмаз".

6. Заключение

В столь кратком сообщении трудно описать все результаты деятельности человека, подобного В.А. Котельникову по масштабу и глубине мышления. Мы не коснулись, в частности, его фундаментальных работ в области криптографии, его роли в проектировании и создании в довоенное время системы радиосвязи Москва–Хабаровск, его вклада в теорию параметрических усилителей, его роли в создании систем связи с глубоко погруженными подводными лодками и многого другого. Следует указать, что В.А. Котельников не раз являлся инициатором новых направлений исследований, проводимых как в ИРЭ РАН, где он многие годы был директором, так и в других организациях. Особо следует отметить его роль в развитии космических исследований, которую он осуществлял будучи вице-президентом Академии наук СССР и председателем совета "Интеркосмос".

Подводя итог, можно сказать, что Владимир Александрович Котельников являлся выдающимся ученым и инженером XX в. — одним из основоположников цифровой техники анализа сигналов, теории информации, статистической радиофизики и радиотехники, радиолокационной астрономии. Один только этот краткий перечень ясно указывает, что мы имели дело с крупнейшей в истории страны и науки личностью, внесшей огромный вклад в развитие науки.

Список литературы

1. Котельников В А, в сб. *Всесоюз. энергетический комитет. Материалы к I Всесоюз. съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности* (М.: Управление связи РККА, 1933) с. 1–19; переизд.: *О пропускной способности "эфира" и проволоки в электросвязи* (М.: Институт радиотехники и электроники МЭИ (ТУ), 2003)
2. Nyquist H *AIEE Trans.* **47** 617 (1928)
3. Lüke D *IEEE Commun. Mag.* **37** (4) 106 (1999)

4. Whittaker E T *Proc. R. Soc., Edinburgh* **35** 181 (1915)
5. Shannon C E *Bell Sys. Tech. J.* **27** 379, 623 (1948)
6. Petersen D P, Middleton D *Inform. Control* **5** (4) 279 (1962)
7. Хургин Я И, Яковлев В П *Методы теории целых функций в радиофизике, теории связи и оптике* (М.: Физматгиз, 1962)
8. Вайнштейн Л А, Зубаков В Д *Выделение сигналов на фоне случайных помех* (М.: Советское радио, 1960)
9. Минкович Б М, Яковлев В П *Теория синтеза антенн* (М.: Советское радио, 1969)
10. Арманд Н А *Радиотехника и электроника* **49** 1199 (2004)
11. Котельников В А *Теория потенциальной помехоустойчивости* (М.: Радио и связь, 1998)
12. Левитан Б М "Гильбертово пространство", в кн. *Математическая энциклопедия* Т. 1 (М.: Советская энциклопедия, 1977) с. 978
13. Verdu S *IEEE Trans. Inform. Theory* **44** 2057 (1998)
14. Wiener N *Extrapolation, Interpolation, and Smoothing of Stationary Time Series, with Engineering Applications* (New York: Wiley, 1949)
15. Rice S O *Bell Syst. Tech. J.* **23** 282 (1944); **24** 46 (1945)
16. Price R et al. *Science* **129** 751 (1959)
17. Evans J V, Taylor G N *Nature* **184** 1358 (1959)
18. Котельников В А и др. "Развитие радиолокационных исследований планет в Советском Союзе", в сб. *Проблемы современной радиотехники и электроники* (Под ред. В А Котельникова) (М.: Наука, 1980) с. 32
19. Александров Ю Н и др. "Вновь открытая планета (радиолокационные исследования Венеры с космических аппаратов Венера 15 и Венера 16)", в сб. *Итоги науки и техники* (Сер. Астрономия, Т. 32) (М.: ВИНИТИ, 1987) с. 201

PACS numbers: **01.60.+q**, **89.70.+c**

В.А. Котельников и отечественная шифрованная связь

В.Н. Сачков

Владимир Александрович Котельников — один из выдающихся отечественных ученых, труды и научная деятельность которого обогатили мировую науку и стали классическим наследием не только для нашей страны, но и для всей общечеловеческой науки и культуры.

Среди широкого спектра достижений В.А. Котельникова в целом ряде областей науки и техники особое место занимают работы по созданию засекреченной связи страны. Проблемами секретной телефонии и телеграфии он стал заниматься в 1930-х годах в связи с разработкой аппаратуры засекречивания телеграфных и телефонных передач на коротковолновой линии связи Москва – Хабаровск. Научно-техническими задачами разработки засекречивающей телефонной аппаратуры в то время занималось несколько организаций, результатом деятельности которых был выпуск малых серий такой аппаратуры, используемой на линиях связи.

В основном это была так называемая маскирующая аппаратура, в которой преобразование речевого сигнала представляло собой инверсию спектра речи, состоящую в том, что низкие частоты речи инвертировались с высокими, а остальные частоты перемещались относительно центра полосы спектра. При таком преобразовании восстановление открытой речи при несанкционированном перехвате засекреченной передачи не создавало больших технических сложностей для противника.

Заслуга В.А. Котельникова состоит в том, что он предложил использовать в телефонной аппаратуре засекречивания более сложные, но технически осуществимые преобразования речевого сигнала. Наряду с перестановкой частотных полос с инверсией было предложено применять временны́е перестановки 100-миллисекундных отрезков речи. Управление частотными и временны́ми перестановками на передаче и приеме осуществлялось шифратором. В условиях ограниченных возможностей техники того времени, лежащей в основе эффективных методов несанкционированного восстановления преобразованной речи, метод засекречивания телефонных передач, предложенный В.А. Котельниковым, имел достаточно высокую стойкость.

Для разработки аппаратуры засекречивания телеграфных и телефонных передач, в том числе с использованием преобразований, предложенных В.А. Котельниковым, в 1939 г. в Центральном научно-исследовательском институте Наркомата связи были созданы две лаборатории. Руководство лабораториями было поручено В.А. Котельникову.

В 1940 г. в лаборатории В.А. Котельникова началась разработка крайне необходимой в то время для вооруженных сил государства телефонной засекречивающей аппаратуры. Примерно в течение трех месяцев после начала Великой Отечественной войны благодаря самоотверженному труду сотрудников лаборатории были изготовлены и испытаны лабораторные макеты отдельных основных узлов аппаратуры засекречивания. В трудных условиях военного времени, включающих эвакуацию лаборатории в Уфу, были созданы опытные образцы телефонной засекречивающей аппаратуры, которые получили "боевое крещение" в 1942 г., когда проводные линии связи с Закавказским фронтом были нарушены во время боев в Сталинграде. В дальнейшем эта аппаратура использовалась для засекречивания коротковолновых каналов связи, по которым Ставка Верховного Главнокомандования осуществляла связь с фронтами. Аппаратура засекречивания телефонных передач в последующие годы применялась и на дипломатических линиях связи Москвы с Хельсинки, Парижем и Веной для проведения переговоров по заключению мирных договоров после окончания Второй мировой войны, а также при проведении Тегеранской, Ялтинской и Потсдамской конференций глав трех стран.

Системы засекречивания телефонной информации на основе частотно-временны́х преобразований речевого сигнала по своей сущности не могли обеспечить гарантированной защиты информации в условиях значительного повышения возможностей вычислительной техники и разработки методов дешифрования засекреченных телефонных сообщений. Для создания аппаратуры гарантированного засекречивания речевой информации необходимо было использовать принцип дискретизации при передаче сигналов по каналу связи и разработать способ стойкого шифрования информации в цифровой форме. В решение первой задачи существенный вклад был внесен В.А. Котельниковым еще в 1932 г., когда он опубликовал статью "О пропускной способности "эфира" и проволоки в электросвязи", в которой сформулировал теорему, определяющую условия дискретизации функций и носящую теперь его имя.

Большое значение для создания телефонного шифратора гарантированной стойкости имела разработка вокодера, осуществляющего сокращение спектра сигнала, отображающего речь, в десятки раз. В.А. Котельников сразу оценил перспективность использования

вокодера для засекреченной телефонии, и в его лаборатории настойчиво проводились исследования по созданию отечественного вокодера. Первый, далеко не совершенный образец такого вокодера был создан в 1941 г. В дальнейшем его конструкция совершенствовалась, в результате чего был создан вокодер с приемлемыми техническими данными.

Помимо проблемы дискретизации речевого сигнала и его сжатия в канале связи для создания телефонной засекречивающей аппаратуры гарантированной стойкости необходимо было создать соответствующее шифрующее высокоскоростное устройство дискретного типа. Принципы разработки такого шифрующего устройства были изложены В.А. Котельниковым в машинописной работе "Основные положения автоматической шифровки", подписанной им 18 июня 1941 г. В этой работе В.А. Котельников ввел понятие "совершенной зашифровки" как способа шифрования, при котором по перехваченному шифрованному тексту нельзя ограничить множество открытых сообщений, к которому принадлежит переданное в зашифрованном виде открытое сообщение.

К. Шеннон в 1945 г., используя вероятностный подход, ввел понятие "совершенной секретности". Система шифрования обладает "совершенной секретностью", если условная вероятность любого открытого сообщения при заданном шифрованном тексте совпадает с безусловной вероятностью.

Следует отметить, что системы шифрования, удовлетворяющие обоим определениям (и "совершенной зашифровки", и "совершенной секретности"), существуют. Примером является система шифрования, в которой алфавиты открытого и шифрованного текстов совпадают, шифр представляет собой реализацию случайной равновероятной последовательности независимых испытаний в том же алфавите и длина сообщений фиксирована. При шифровании знак шифрованного текста получается модульным сложением знака открытого текста и знака шифрующей последовательности.

С использованием проведенных исследований по дискретизации речевого сигнала и выбора конструкции вокодера криптографически стойкая аппаратура для засекречивания телефонной информации была создана в 1950-х годах. В этот период В.А. Котельников перешел на работу в Московский энергетический институт и стал заниматься другими научными проблемами. Однако он не только продолжал консультировать разработчиков новой телефонной засекречивающей аппаратуры, но и принимал участие в работе Государственной комиссии по приемке опытных образцов, рекомендовавшей выпуск опытной серии аппаратуры в промышленности.

Начиная с 1950-х годов отечественная криптография как наука получила значительное развитие. В этот период к решению проблем криптографии был привлечен ряд известных ученых и специалистов в области математики, физики и электронно-вычислительной техники. Под их научным руководством стали формироваться новые направления научных исследований, обеспечивающие теоретическую основу практических разработок в области шифрования информации. Коллективы специалистов-криптографов получили значительное пополнение за счет прихода на работу молодых выпускников ведущих вузов страны.

При механико-математическом факультете Московского государственного университета было организовано специальное отделение по подготовке математиков-криптографов. Одновременно было создано специальное высшее учебное заведение по подготовке криптографов и специалистов математического, физико-технического и связного профиля, преемником которого сейчас является Институт криптографии, связи и информатики. Выпускники этих учебных заведений наряду с выпускниками других вузов в течение ряда десятилетий образовали высококвалифицированный коллектив ученых и специалистов, который обеспечил успешное развитие отечественной криптографии и надежное закрытие криптографическими средствами государственных, военных и экономических линий связи страны. К началу 1990-х годов в криптографической службе страны был накоплен значительный научный потенциал и образованы научные школы ученых и специалистов, проводящие исследования на современном научно-техническом уровне. На основе результатов этих исследований была организована система защиты докторских и кандидатских диссертаций. В результате в криптографической службе вырос значительный контингент высококвалифицированных научных работников, имеющих ученые степени докторов и кандидатов наук.

В этих условиях с одобрения Президента Российской академии наук Указом Президента РФ в 1992 г. была создана государственная Академия криптографии Российской Федерации. В настоящее время Академия криптографии ежегодно проводит около 100 научно-исследовательских работ, к выполнению которых привлекаются до 1000 ученых и специалистов из более чем 40 научных организаций страны, включая Российскую академию наук, Московский государственный университет им. М.В. Ломоносова и др. Совместно с РАН Академия криптографии издает *Труды по дискретной математике*. Начиная с 1997 г. выпущено 8 томов, в которых опубликованы статьи открытого содержания членов Академии криптографии и молодых математиков-криптографов.

Творческое сотрудничество В.А. Котельникова с криптографической службой страны с некоторыми перерывами продолжалось в течение всей его жизни. Активная фаза этого сотрудничества приходится на 1992 г., когда была создана Академия криптографии Российской Федерации. В.А. Котельников сыграл ключевую роль в создании Академии криптографии, активно оказывал ей поддержку на всех этапах ее становления и развития. Вместе с другими пятью членами Российской академии наук он вошел в число ее основателей и в дальнейшем принимал непосредственное участие в научной и научно-организационной деятельности Академии криптографии. Беседы и дискуссии членов Академии с Владимиром Александровичем по различным проблемам криптографии, включая обсуждение различных путей построения устройств "совершенной зашифровки", были интересными и плодотворными для собеседников.

Для увековечивания памяти о В.А. Котельникове решением Президиума Академии криптографии Российской Федерации для адъюнктов Института криптографии, связи и информатики Академии Федеральной службы безопасности в 2006 г. были учреждены две стипендии имени В.А. Котельникова.

В Академии криптографии свято чтут имена тех, кто внес свой вклад в становление и развитие современной криптографической службы страны, тех, кто своими трудами внес большой вклад в развитие отечественной криптографии. Среди этих имен имя Владимира Александровича Котельникова — на одном из первых мест.

PACS numbers: 03.67.Dd, **89.70.+c**

Квантовая криптография и теоремы В.А. Котельникова об одноразовых ключах и об отсчетах

С.Н. Молотков

Квантовая криптография представляет собой новое направление в развитии средств конфиденциальной передачи информации. Точнее, квантовые криптографические системы представляют собой системы распределения секретных ключей между пространственно разделенными (удаленными) легитимными пользователями. Обеспечение секретного распространения ключей между такими пользователями играет принципиально важную роль в криптографии. Если бы существовал способ распространения (передачи) секретных ключей от одного легитимного пользователя к другому по открытому (несекретному) каналу связи с гарантией того, что в процессе передачи ключи не станут известны подслушивателю, то в этом случае была бы возможна передача зашифрованных с помощью этих ключей сообщений, которые принципиально не могут быть дешифрованы (взломаны) третьими лицами. Такие принципиально не дешифруемые системы называют абсолютно стойкими, или системами шифрования в режиме одноразового блокнота (one time pad). Позднее такие шифры стали называть совершенными.

Сначала кратко коснемся истории вопроса.

Впервые строгое обоснование того факта, что системы шифрования с одноразовыми ключами являются абсолютно стойкими, было получено в работе Владимира Александровича Котельникова. Эта работа, законченная за несколько дней до начала Великой Отечественной войны 22 июня 1941 г., вошла в один из закрытых отчетов [1] и до сегодняшнего дня не опубликована в открытой печати.

Параллельно и независимо вопросы теоретической стойкости шифров изучались Клодом Шенноном (C.E. Shannon). Результаты его исследований были представлены в закрытом отчете "A Mathematical Theory of Cryptography", датированном 1 сентября 1946 г. После окончания войны этот отчет был рассекречен[1] и опубликован в 1949 г. в виде статьи "Communication Theory of Secrecy Systems" [2], которая стала широко известным классическим трудом по теоретической криптографии.

Идея, очень близкая идее режима шифрования с одноразовым блокнотом, была высказана еще в 1926 г. в работе Вернама (G.S. Vernam) "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communication" [3], где утверждалось, правда, без каких бы то ни было математических обоснований, что шифры с "бегущим" случайным ключом (running key) будут абсолютно не дешифруемыми: "...If, now, instead of using English words or sentences, we employ a key composed of letters selected absolutely at random, a cipher system is produced which is absolutely unbreakable"[2].

Благодаря исследованиям В.А. Котельникова и К. Шеннона возникло четкое и строгое понимание того, каким условиям должен удовлетворять абсолютно стойкий шифр.

Неформально, шифр является абсолютно стойким, если:

1) ключ секретен — известен только легитимным пользователям;

2) длина ключа в битах не меньше длины сообщения;

3) ключ случаен;

4) ключ используется только один раз.

В этом случае зашифрованное сообщение статистически независимо от исходного сообщения.

Принципиальная проблема при реализации криптосистем с одноразовыми ключами состоит в передаче (распространении) секретных ключей между удаленными легитимными пользователями.

Ключ между такими пользователями должен передаваться с помощью какого-либо физического сигнала через открытый (т.е. доступный для подслушивания) канал связи. С точки зрения классической физики в этом случае не существует запретов на измерение передаваемого сигнала без его возмущения. Поэтому принципиально невозможно гарантировать секретность ключа при его распространении.

Если же передавать ключи с помощью квантовых состояний, то возникает принципиально другая, более интересная ситуация. Квантовая криптография, основанная на фундаментальных запретах квантовой механики, открывает возможность передачи ключей с помощью квантовых состояний, секретность при этом гарантируется фундаментальными законами природы. Следовательно, квантовая криптография позволяет реализовать абсолютно стойкие системы шифрования с одноразовыми ключами, истоки которых восходят к работам Г. Вернама, В.А. Котельникова и К. Шеннона. Собственно идея квантовой криптографии как раз и направлена на решение центральной проблемы криптографии — задачи распространения секретных ключей.

Впервые идея использовать квантовую механику для защиты информации была высказана S. Wiesner в 1973 г. (идея "квантовых" денег), но была опубликована [4] лишь спустя десятилетие. Интересно отметить, что идеи использования квантовой механики для защиты информации появились раньше, чем классическая криптография с открытым ключом [5, 6].

Возникновение квантовой криптографии связано с опубликованием в 1984 г. замечательной работы Бен-

[1] Здесь имеет смысл упомянуть высказывание одного из основателей криптографии с открытым ключом У. Диффи (W. Diffie), по мнению которого работа К. Шеннона, возможно, была рассекречена ошибочно (см. предисловие к монографии B. Schneier *Applied Cryptography*, John Wiley & Sons, Inc., 1996).

[2] "...Если же, вместо использования английских слов и предложений, мы воспользуемся ключом, составленным из букв, выбранных абсолютно случайным образом, то полученная система шифрования будет абсолютно стойкой". (*Перевод ред.*)

нета и Брассара, в которой был предложен первый криптографический протокол BB84, ставший впоследствии классическим [7].

Квантовая криптография, или распространение секретных ключей, в принципе позволяет реализовать абсолютно стойкие (не дешифруемые подслушивателем даже теоретически) системы шифрования с одноразовыми ключами. Секретность ключей в квантовой криптографии основана на фундаментальных запретах квантовой механики: 1) неизвестное квантовое состояние не может быть скопировано (no-cloning-теорема [8]); 2) пара наблюдаемых, которым отвечают некоммутирующие эрмитовы операторы, не может быть одновременно достоверно различима, что является следствием соотношений неопределенности Гейзенберга [9], или, говоря более формально, некоммутирующие операторы не могут иметь общих собственных векторов. В квантовой криптографии в качестве наблюдаемых выступают матрицы плотности информационных состояний, соответствующих классическим битам 0 и 1. Для чистых состояний одновременная ненаблюдаемость (достоверная неразличимость) матриц плотности эквивалентна неортогональности информационных квантовых состояний [9]. Сказанное означает, что не существует измерений, которые с вероятностью 1 позволяют различать одно из пары неортогональных состояний и так, чтобы после измерения система осталась в исходном (невозмущенном) состоянии.

Таким образом, любое измерение, если оно дает информацию о передаваемых состояниях, неизбежно приводит к их возмущению, что позволяет детектировать любые попытки подслушивания в канале связи. Другими словами, подслушивание (соответственно возмущение передаваемых состояний) должно неизбежно изменять статистику результатов измерений на приемном конце по сравнению со статистикой результатов измерений на невозмущенных состояниях. Искажение квантовых состояний возникает в неидеальном квантовом канале, что также приводит к изменению статистики результатов измерений. В квантовой криптографии принципиально невозможно различить изменилась ли статистика результатов по сравнению с таковой в идеальном случае за счет шума в канале или вследствие действий подслушивателя, поэтому любые изменения статистики приходится относить к действиям подслушивателя.

Если бы законы квантовой механики позволяли обнаруживать только сам факт возмущения передаваемых состояний, то это было бы малоинтересным для целей криптографии, точнее, передачи ключей. *Квантовая механика позволяет не только обнаруживать возмущение состояний, но и связать изменение статистики результатов измерений с количеством информации, которое может быть получено подслушивателем при наблюдаемом изменении статистики отсчетов по сравнению со статистикой в идеальном случае*.

В квантовой криптографии кроме квантового канала связи (в реальных условиях это либо оптоволокно, либо открытое пространство), по которому передаются квантовые состояния, необходим также открытый классический канал связи. Последний требуется для выяснения легитимными пользователями изменений статистики отсчетов и коррекции ошибок в первичном ключе, переданном по квантовому каналу связи.

Единственное требование, предъявляемое к классическому каналу связи, состоит в том, что передаваемая открыто и доступная всем, включая подслушивателя, классическая информация не может быть изменена подслушивателем — она должна сохранять целостность (так называемый unjamable channel) [7]. Такой открытый классический канал является, конечно, математической идеализацией. Для сохранения целостности открыто передаваемых классических данных в реальных условиях необходимо использовать процедуры аутентификации и контроля целостности данных. Для подобных процедур, в свою очередь, требуется секретный ключ. Если в качестве открытого классического канала используется, например, Интернет, то для целей аутентификации возможна генерация ключей по схеме Хеллмана – Диффи [5]. Однако если для открытого классического канала используется та же самая оптоволоконная линия, что и для квантового, то генерация ключей для аутентификации по схеме Хеллмана – Диффи оказывается неприемлемой из-за очевидной так называемой атаки "man in the middle" (человек посредине).

В такой ситуации требуется небольшой стартовый ключ один раз при первом сеансе. При последующих сеансах этот ключ выбрасывается, и для аутентификации и сохранения целостности данных, передаваемых по классическому каналу, используется часть ключа, сгенерированного по квантовому каналу в предыдущем сеансе обмена. Остальная, бóльшая часть ключа, полученного по квантовому каналу, предназначается собственно для шифрования передаваемой информации. Если для аутентификации и сохранения целостности данных применяются процедуры на основе ГОСТ Р 34.11-94 [10], то длина стартового ключа составляет 256 бит. При этом в течение нескольких секунд обмена по квантовому каналу может быть получен новый секретный ключ, гораздо более длинный, чем исходный.

Разумеется, стартовый ключ мог бы быть использован для шифрования нового ключа и передачи его второму легитимному пользователю. Однако при этом абсолютная секретность нового ключа гарантируется, лишь когда его длина не более длины ключа, на котором он шифруется, т.е. более длинного ключа, чем исходный, получить нельзя. В квантовой криптографии стартовый ключ не используется напрямую для передачи нового ключа, который генерируется по квантовому каналу связи. При этом число бит открытой информации, переданной по открытому классическому каналу на один бит нового секретного ключа, может быть сделано меньше единицы, поэтому возможно расширение ключа.

Подход с использованием небольшого стартового ключа предпочтительнее подходов на основе алгоритмов асимметричной криптографии с открытым ключом, поскольку позволяет свести к минимуму число сеансов обмена по открытому каналу связи в процессе "чистки" и усиления секретности ключа (privacy amplification).

Основная задача теории сводится к выяснению длины секретного ключа, который может быть получен при наблюдаемых изменениях статистики результатов измерений на приемном конце по сравнению со статистикой на невозмущенных состояниях. Как правило, величиной, которая характеризует отклонение статистики измерений от идеальной, является наблюдаемая вероятность ошибки на приемном конце, точнее, вероят-

ность того, что переданный бит был 0, а зарегистрирован как 1, и наоборот. Такая ситуация имеет место в широко применяемом протоколе BB84, хотя возможны и другие критерии изменения статистики, которые используют несколько параметров. Перед выяснением вероятности ошибки через открытый канал происходит сравнение базисов на приемной и передающей стороне (для протокола BB84 [7]) или раскрытие позиций на приемной стороне, где имел место результат измерений с неопределенным исходом (для протокола B92 [9]). Вероятность ошибки оценивается путем сравнения через открытый канал части последовательности, полученной по квантовому каналу информации, с соответствующей частью исходной, в дальнейшем раскрытая часть отбрасывается.

Следующий этап любого квантового криптографического протокола распространения ключей состоит в коррекции ошибок в нераскрытой части последовательности у легитимных пользователей посредством обмена информацией через открытый канал связи. Обычно легитимных пользователей называют Alice и Bob, а подслушивателю присваивают имя Eve (от англ. eavesdropper). В результате коррекции ошибок у Alice и Bob остаются последовательности бит меньшей длины и уже одинаковые. "Одинаковые" здесь означает, что последовательности совпадают с вероятностью сколь угодно близкой к единице: $1-2^{v}$ (например $1-2^{-200}\sim 1-10^{-70}$, напомним, что число атомов в видимой части Вселенной оценивается как 10^{77}). Параметр v выбирается легитимными пользователями.

После "чистки" первичного ключа у подслушивателя имеется строка бит или регистр квантовой памяти с состояниями либо и то, и другое вместе. Последний шаг при получении финального секретного ключа состоит в усилении секретности (privacy amplification [11]) — сжатии "очищенного" ключа с помощью так называемой универсальной функции хэширования 2-го рода (two universal hash function [12]), которая сама является случайной величиной для уже одинаковых последовательностей у Alice и Bob. Случайно выбираемая функция хэширования открыто сообщается одним из легитимных пользователей через открытый канал связи и считается всем известной, включая подслушивателя. Сжатая последовательность бит является для легитимных пользователей общим секретным ключом, для которого гарантируется, что подслушиватель имеет о ключе сколь угодно малую информацию по некоторому, заданному Alice и Bob параметру секретности.

Естественным требованием к процедурам коррекции ошибок и усиления секретности ключа является сохранение как можно большего числа бит в финальном ключе. Еще одно требование состоит в минимизации числа сеансов обмена по открытому каналу связи в пересчете на один бит в финальном секретном ключе.

При коррекции ошибок в первичном ключе задача легитимных пользователей состоит не только в исправлении ошибок, но также в оценке верхней границы информации, которую может получить об оставшемся ключе подслушиватель из обменов по открытому каналу связи. Для коррекции ошибок могут быть использованы различные процедуры, включая хорошо разработанные классические коды, исправляющие ошибки.

Перейдем теперь к обсуждению экспериментальных реализаций систем квантовой криптографии.

Разработки в области квантовой криптографии и реализации различных квантовых криптосистем ведутся во многих университетах всех развитых стран и практически во всех ведущих телекоммуникационных компаниях. За последние пять лет квантовая криптография прошла путь от чисто теоретических исследований до их практической реализации и создания первых коммерческих прототипов.

Имеющиеся прототипы квантовых криптосистем используют в основном следующие принципы кодирования классической информации в состояния квантовых систем.

1. Кодирование информации о ключе в поляризационные степени свободы [13].

2. Фазовое кодирование с помощью интерферометра Маха – Цандера, в котором информация кодируется в разность фаз на приемном и передающем плечах интерферометра [14, 15].

3. Кодирование на основе частотной модуляции несущей частоты [16].

4. Квантовая криптография на когерентных состояниях с использованием гомодинного детектирования на приемном конце [17].

Наибольший прогресс достигнут в криптосистемах с фазовым кодированием и самокомпенсацией [18] с использованием фарадеевских отражателей. Первый лабораторный прототип квантовой криптосистемы, созданный в 1989 г. в Исследовательском центре компании IBM, имел длину квантового канала связи 1 м [19]. Лабораторный вариант криптосистемы на базе интерферометра Маха – Цандера с разделением времени (time division interferometer) был реализован с использованием оптоволоконной линии связи длиной 30 км в исследовательской лаборатории фирмы "British Telecom" в 1995 г. [20] и с суммарной длиной оптоволоконных линий 48 км в Лос-Аламосской лаборатории [21]. В этих схемах применялся принцип фазового кодирования. В 2003 г. в исследовательской лаборатории NEC достигнута дальность 100 км [21], а в 2004 г. — уже 150 км [22]. Данные схемы являются усложнением и развитием идеи фазового кодирования с самокомпенсацией с помощью фарадеевских отражателей. Упомянутые криптосистемы, особенно схемы с фазовым кодированием и самокомпенсацией, достаточно сложны в реализации. Результатом теоретической разработки группы в Женевском университете стала практическая реализация квантовой криптосистемы с волоконно-оптическим кабелем длиной 23 км, проложенным по дну Женевского озера между городами Нион и Женева. Линия, длина которой на сегодня доведена до 67 км, представляет собой сложный оптоволоконный интерферометр с фазовым кодированием и самокомпенсацией с использованием фарадеевских отражателей [18] (первая так называемая plug & play-система квантовой криптографии). Активные исследования ведутся в исследовательской лаборатории IBM (Almaden) [23, 24]. Апробирована первая локальная квантовая криптографическая сеть в Бостоне для распространения секретных ключей между пользователями на расстоянии в 10 км (проект выполняется по заказу DARPA — Defense Advanced Research Projects Agency) [25].

Недавно инновационной фирмой "MagiQ" был анонсирован первый коммерческий вариант квантовой волоконной криптосистемы, действующей на расстоянии

120 км, в которой используется принцип фазового кодирования. Схема реализует квантово-криптографический протокол BB84.

По мнению специалистов из "QinetiQ" и "Toshiba Research Europe" (Великобритания), широкое применение квантовых криптосистем начнется в ближайшие три года, первыми на очереди стоят правительственные учреждения и банки.

Имеются реализации прототипов квантовых криптосистем, осуществляющих передачу секретного ключа через открытое пространство [26–28]. Рекорд по дальности (по опубликованным данным [28]) составляет 23,4 км как в дневное, так и ночное время. Такие квантовые криптосистемы предназначены для генерации и передачи секретных ключей между наземными объектами и низкоорбитальными спутниками (до высот в 1000 км) или между наземными объектами через спутники. По оценкам руководителя проекта из "QinetiQ" планируются эксперименты по передаче криптографических ключей на низкоорбитальные спутники, а лет через семь с их помощью можно будет посылать секретные ключи в любую точку планеты.

На ближайшее время прогнозируются следующие параметры квантовых криптографических волоконно-оптических линий связи:

1. Количество ошибок, не превышающее нескольких процентов при эффективной скорости передачи информации по оптоволоконному квантовому каналу.

2. Длина квантового оптоволоконного канала связи $\sim 100-150$ км.

3. Число подканалов при разделении по длинам волн (мультиплексировании) — 8–16.

Несмотря на впечатляющий прогресс как в понимании криптографической стойкости (секретности) квантовых криптосистем, так и в их реализации, эти системы содержат достаточно сложные оптоволоконные, электронные и программные компоненты, работа с которыми на сегодня представляет собой, скорее, проведение тонкого научного эксперимента и демонстрацию экспериментального искусства, чем практическую деятельность с использованием общеупотребительного и стандартного оборудования. Другим важным обстоятельством, сдерживающим пока широкое распространение квантовых криптосистем на основе принципа фазового кодирования, является то, что квантовые криптосистемы пока плохо встраиваются в стандартные оптоволоконные телекоммуникационные технологии, поскольку содержат специфические компоненты (интерферометры), требующие тонкой юстировки. Наконец, последний принципиальный момент состоит в том, что каждый квантовый криптографический протокол распространения секретного ключа фактически требует "темных" оптоволоконных линий (свободных линий).

Существует три базовых протокола передачи секретного ключа, которые кратко называются BB84 [7], B92 [9] и BB84$(4+2)$ [29]. Протокол BB84 использует четыре квантовых состояния: два ортогональных состояния для 0 и 1 в одном базисе и два ортогональных для 0 и 1 в другом. Между базисами состояния попарно неортогональны, что необходимо для обеспечения секретности. В протоколе B92 используется пара любых неортогональных квантовых состояний, отвечающих 0 и 1. Протокол BB84$(4+2)$ является производным от BB84 и отличается от последнего тем, что внутри базисов состояния также делаются неортогональными. Очевидно, что разные протоколы обмена требуют различных физических устройств для формирования квантовых состояний на передающем конце и соответственно разных устройств для квантово-механических измерений на приемном конце.

Криптографическая стойкость (секретность) данных протоколов достаточно подробно исследована [29–36]. С учетом реальных параметров — нестрогой однофотонности источника, неидеальности лавинных фотодетекторов и затухания в оптоволоконном канале связи, перечисленные протоколы гарантируют секретность распространения ключа до определенной критической длины оптоволоконной линии связи [29]. Протокол B92 является самым минимальным, в смысле числа используемых состояний и измерений, однако обеспечивает секретность только до длин $\sim 15-20$ км [33]. Наиболее подробно исследованный протокол BB84, использующий четыре квантовых состояния, является более сложным в реализации и остается секретным до длин ~ 50 км [29]. Наконец, в протоколе BB84$(4+2)$ применяются четыре попарно неортогональных состояния. Данный протокол еще сложнее в реализации и настройке оптоволоконного интерферометра, однако в смысле секретности "выживает" до длин ~ 150 км [29].

Для экспериментальной реализации требуются однофотонные источники. Подчеркнем, что с точки зрения теории не обязательно использовать однофотонные квантовые состояния для передачи ключей. Однако в многофотонном случае квантово-механические измерения на приемном конце для детектирования попыток подслушивания и изменения квантовых состояний формально должны быть реализованы как проекторы на соответствующие векторы многофотонных квантовых состояний. Подобных измерительных устройств пока не существует, хотя никаких теоретических запретов на реализацию таких квантово-механических измерений нет. То есть использование именно однофотонных квантовых состояний обусловлено существующими детекторами (реально это лавинные фотодетекторы с пельтье-охлаждением, работающие в стробируемом режиме).

Отметим, что уже созданы фотодетекторы на основе сверхпроводников, которые в отличие от лавинных фотодетекторов на гетероструктурах различают состояния с разным числом фотонов.

Однофотонные квантовые состояния (точнее квазиоднофотонные) получаются путем сильного ослабления когерентного состояния — лазерного изучения, которое даже после любого ослабления содержит многофотонные компоненты.

Нестрогая однофотонность источника вместе с затуханием в квантовом канале связи приводят к тому, что секретность передаваемых ключей гарантируется, лишь когда длина канала не превосходит некоторой критической величины.

Негативная роль затухания (при нестрого однофотонном источнике) в квантовом канале связи состоит не столько в том, что затухание, очевидно, снижает скорость передачи ключа из-за того, что не все фотоны достигают приемного конца, сколько в том, и это гораздо более критично, что начиная с некоторой величины затухания уже нельзя гарантировать секретность переданного ключа. Затухание в оптоволоконных линиях связи определяется длиной канала связи. Однако

критическая длина, вплоть до которой система остается секретной, до сих пор строго неизвестна. Оценки варьируются от нескольких десятков километров до 150 км [29].

Ведутся работы по использованию в квантовой криптографии источников излучения, например на основе наночастиц алмаза, которые по своим параметрам приближаются к однофотонным [37].

Если проанализировать основные квантовые криптографические протоколы и доказательства их секретности в канале с затуханием (основными являются протоколы BB84 и B92, остальные представляют собой того или иного вида производные от них), то становится очевидным, что требуется (и используется явно или неявно) априорная информация о потоке ошибок (Quantum Bit Error Rate, QBER), обусловленных затуханием. Например, если затухание в канале связи изменяется в течение времени протокола передачи ключа, то изменяется и поток ошибок (даже в отсутствие подслушивателя). Кроме того, если протокол подразумевает постоянство QBER, то никакую секретность переданного ключа вообще невозможно гарантировать. Если в оптоволоконных квантовых криптосистемах затухание еще можно считать постоянным (последнее составляет для одномодового оптоволокна на длине волны 1550 нм 0,17–0,25 дБ км$^{-1}$), то при передаче через открытое пространство это уже явно не так, поскольку состояние атмосферы невозможно контролировать. Поэтому хотелось бы иметь протоколы распространения ключа, которые были бы устойчивыми и гарантировали секретность ключа при изменении затухания в канале связи в течение времени протокола и секретность которых не зависела бы от априорного знания величины затухания. Данная проблема, на наш взгляд, достаточно серьезна и требует решения, поскольку в противном случае могут возникнуть сомнения в безусловной секретности квантовой криптографии (секретности, которая полностью гарантируется фундаментальными запретами квантовой механики, а не техническими ограничениями подслушивателя).

Все упомянутые выше трудности связаны с тем, что секретность протоколов базируется, по сути, лишь на геометрических свойствах векторов состояний квантовой системы в гильбертовом пространстве $\mathcal{H}$. Точнее, на невозможности копирования (no-cloning-теорема [8]) неизвестного квантового состояния и принципиальной достоверной неразличимости неортогональных квантовых состояний (теорема C.H. Bennett [9]). Грубо говоря, данные протоколы формулируются в гильбертовом пространстве $\mathcal{H}$. То, что все измерения и распространение квантовых состояний происходят в пространстве-времени, никак явно не используется. При распространении квантового состояния затухание имеет место не в гильбертовом пространстве, а в пространстве-времени, поэтому для устранения проблем потери секретности вследствие затухания требуются другие дополнительные *фундаментальные* ограничения, проистекающие из свойств квантовых состояний, и получение информации о них в пространстве-времени. Ограничения, диктуемые лишь геометрическими свойствами квантовых состояний в гильбертовом пространстве, для построения квантовых криптографических протоколов, по-видимому, исчерпаны.

Такими дополнительными фундаментальными и естественными ограничениями являются ограничения, диктуемые специальной теорией относительности. Кроме того, фотоны представляют собой истинно релятивистские безмассовые частицы (состояния безмассового квантованного поля), которые распространяются с предельно допустимой скоростью, поэтому при разработке и реализации квантовой криптографии в открытом пространстве было бы неестественно не воспользоваться дополнительными возможностями, предоставляемыми природой.

Ниже кратко обсудим квантовые криптосистемы для передачи ключей через открытое пространство, которые кроме ограничений на измеримость квантовых состояний, следующих из квантовой механики, используют дополнительные запреты, диктуемые специальной теорией относительности.

Поскольку в обсуждаемых ниже квантовых криптосистемах явно учитывается факт распространения квантовых состояний (ключа) в пространстве-времени, то требуется заранее знать длину квантового канала связи между передающей и принимающей сторонами.

Релятивистские квантовые криптосистемы остаются секретными при любом затухании в канале связи. Величина затухания снижает лишь скорость передачи ключа, но не влияет на его секретность. Кроме того, гарантируется секретность ключа даже для неоднофотонных состояний. Схема остается секретной при любом среднем числе фотонов в квантовом состоянии. Как показывают расчеты (см. подробности в [38]), наибольшая эффективность достигается при небольших средних числах фотонов, $\mu = 1-3$. При таких средних числах заполнения практически отсутствуют холостые посылки (доля вакуумной компоненты в когерентном состоянии мала). Последнее означает, что скорость генерации ключа, как минимум, на порядок выше, чем в схемах, базирующихся только на геометрических свойствах квантовых состояний, где требуется ослабление лазерного излучения до $\mu = 0{,}1-0{,}3$. Дополнительное увеличение скорости возникает за счет того, что ограничения специальной теории относительности позволяют использовать даже ортогональные состояния, что не требует проверки согласования базисов измерений, как в протоколе BB84. Кроме того, поскольку все действия участников (как легитимных, так и подслушивателя) осуществляются в пространстве-времени и состояния ортогональны, то коллективные измерения подслушивателя не дают ему никаких преимуществ по сравнению с индивидуальными измерениями в каждой посылке. И последнее, система гарантирует секретность ключа даже при уровне ошибок в принятой двоичной последовательности, близком к 50 % (см. детали в [38]). Отметим, что, например, для протокола BB84 секретность гарантируется лишь до уровня ошибок в 11 % [30, 32].

Напомним, что теоретически безошибочная передача информации, фактически исправление ошибок в пределе асимптотически длинных последовательностей в классическом бинарном симметричном канале, возможна, если вероятность ошибки не превышает 50 %. *В релятивистской квантовой криптографии при уровне ошибок близком к* 50 % *возможно не только исправить ошибки, но и гарантировать секретность информации (ключей), передаваемой с помощью квантовых состояний через открытое пространство.*

Единственное дополнительное требование в релятивистских квантовых криптосистемах по сравнению с нерелятивистскими квантовыми криптосистемами на неортогональных состояниях — это знание длины квантового канала связи, что, на наш взгляд, является небольшой платой за те преимущества, которые может дать релятивистская квантовая криптография.

В квантовых криптосистемах обнаружение любых попыток подслушивания гарантируется следующими двумя фундаментальными, тесно связанными между собой запретами квантовой механики.

1. Невозможность процесса

$$|\varphi_0\rangle \otimes |A\rangle \mapsto |\varphi_0\rangle \otimes |\varphi_0\rangle \otimes |A_0\rangle\,, \qquad \langle\varphi_0|\varphi_1\rangle \neq 0\,. \quad (1)$$
$$|\varphi_1\rangle \otimes |A\rangle \mapsto |\varphi_1\rangle \otimes |\varphi_1\rangle \otimes |A_1\rangle\,,$$

Такой запрет на копирование неизвестного квантового состояния называется no-cloning-теоремой.

2. Невозможность получения информации об одном из неортогональных состояний без их возмущения, т.е. запрет на процесс

$$|\varphi_0\rangle \otimes |A\rangle \mapsto U\bigl(|\varphi_0\rangle \otimes |A\rangle\bigr) = |\varphi_0\rangle \otimes |A_0\rangle\,, \qquad |A_0\rangle \neq |A_1\rangle, \quad (2)$$
$$|\varphi_1\rangle \otimes |A\rangle \mapsto U\bigl(|\varphi_1\rangle \otimes |A\rangle\bigr) = |\varphi_1\rangle \otimes |A_1\rangle\,,$$

где $|A\rangle$ — состояние прибора наблюдателя, U — некоторый унитарный оператор, описывающий совместную эволюцию исследуемого состояния и состояния прибора. Данные запреты, по сути, являются одним из проявлений фундаментального принципа неопределенности Гейзенберга о невозможности одновременного измерения наблюдаемых, которым отвечают некоммутирующие операторы.

Для ортогональных состояний запреты на копирование и извлечение информации без их возмущения отсутствуют. В рамках нерелятивистской квантовой механики наблюдаемым $\rho_0 = |\varphi_0\rangle\langle\varphi_0|$ и $\rho_1 = |\varphi_1\rangle\langle\varphi_1|$ отвечают коммутирующие измеряющие операторы, являющиеся ортогональными проекторами $\mathcal{P}_{0,1} = |\varphi_{0,1}\rangle\langle\varphi_{0,1}|$ ($[\mathcal{P}_0, \mathcal{P}_1] = 0$). Ограничения (1), (2) являются, по сути, геометрическим свойством векторов состояний квантовой системы $|\varphi_{0,1}\rangle$ в гильбертовом пространстве состояний. Если не использовать каких-то дополнительных фундаментальных ограничений на измеримость ортогональных квантовых состояний, то последние в силу достоверной различимости не могут применяться для целей квантовой криптографии. Такими дополнительными фундаментальными ограничениями являются ограничения на измеримость квантовых состояний, налагаемые специальной теорией относительности.

Для ортогональных состояний нет запрета на достоверное различение без их возмущения [9], точнее говоря, теорема [9] об этом случае ничего не говорит. Часто произносимые при интерпретации данной теоремы слова о том, что ортогональное состояние "проходит" через вспомогательную систему $|A\rangle$, взаимодействует с ней по мере прохождения и изменяет ее состояние, не соответствуют содержанию теоремы. В теореме ничего подобного нет, в том смысле, что она носит чисто геометрический характер и утверждает, что вектор состояния вспомогательной системы $|A\rangle$ может быть унитарно повернут в зависимости от входного вектора $|\varphi_{0,1}\rangle$ и переведен в новое состояние $|A_0\rangle$ или $|A_1\rangle$ без изменения входного вектора. При этом неявно предполагается, что входной вектор $|\varphi_{0,1}\rangle$ доступен как целостный объект, т.е. для совершения унитарного преобразования U нужно иметь доступ ко всему пространству состояний $\mathcal{H}_{\varphi_{0,1}}$, в котором отличен от нуля носитель состояния, в противном случае преобразование не будет унитарным. Тот факт, что в доказательстве фигурирует лишь вектор состояния как целостный объект $|\varphi_{0,1}\rangle$ без внутренней координатной "начинки", как раз и подразумевает, что вектор состояния при унитарном преобразовании участвует "сразу целиком".

Для любой реальной физической системы гильбертово пространство $\mathcal{H}_{\varphi_{0,1}}$ неизбежно привязано к пространству-времени Минковского, в котором состояние имеет амплитуду (сглаживающую волновую функцию). Доступ к гильбертову пространству состояний, таким образом, подразумевает доступ к той области пространства-времени, в которой отлична от нуля амплитуда (волновая функция) состояния. Если же доступна лишь часть такой области, то тогда даже ортогональные состояния невозможно достоверно скопировать или различить. Последнее более или менее очевидно, поскольку никакой процесс, в том числе копирование или различение, не может иметь вероятность исхода бóльшую, чем доля нормировки состояний, которая набирается в доступной пространственно-временнóй области и тем самым автоматически в доступной части гильбертова пространства. Грубо говоря, чтобы с достоверностью скопировать или различить ортогональные состояния, они нужны сразу и целиком.

Поэтому, если амплитуда состояния отлична от нуля в некоторой конечной области пространства-времени, то слова о том, что состояние доступно целиком, означают доступ к этой области. В нерелятивистской квантовой механике, где нет ограничений на предельную скорость, доступ к любой конечной области может быть получен мгновенно. В квантовой теории поля, где существуют ограничения на предельную скорость, доступ к состоянию целиком может быть получен только в том случае, если протяженное состояние предварительно унитарно преобразовано к состоянию с амплитудой, отличной от нуля лишь в сколь угодно малой пространственной области. После этого можно пользоваться теоремой [9]. Согласно принципу релятивистской причинности [39] такое унитарное преобразование состояния, заданного в конечной пространственно-временнóй области, в состояние, локализованное в сколь угодно малой пространственной области, может быть осуществлено лишь за конечное время. Минимально необходимое время определяется из условия накрытия "прошлой" частью светового конуса исходной пространственной области, в которой была отлична от нуля амплитуда состояния (рис. 1а). Вершина этого конуса находится в сколь угодно сильно локализованной области (точке), в которую унитарно преобразуется исходная амплитуда состояния. Каждое из пары ортогональных состояний, унитарно преобразованных ("собранных") в локализованной области, может быть после этого достоверно скопировано или различено. Поскольку речь идет о безмассовых состояниях квантованного поля (фотонов), которые распространяются с предельно допустимой скоростью, то такое унитарное преобразование и дальнейшее копирование приведет к сдвигу (задержке)

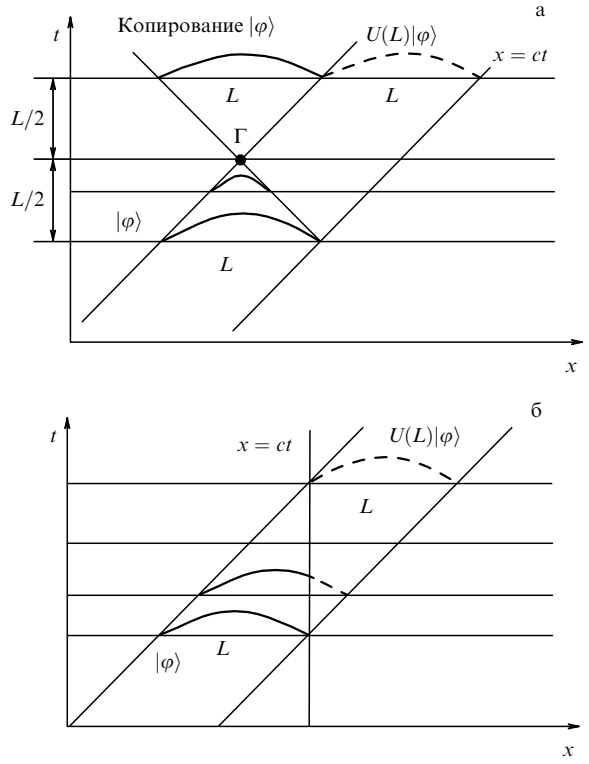


Рис. 1.

состояний в пространстве-времени по отношению к таковым в случае их свободной эволюции (распространения). Данное обстоятельство позволяет детектировать любые попытки подслушивания. Отметим, что ограничения, накладываемые на измерения в релятивистской области, исследовались впервые в работе Л.Д. Ландау и Р. Пайерлса [40], а впоследствии в работе Н. Бора и Л. Розенфельда [41][3].

Иначе говоря, для ортогональных состояний безмассового квантованного поля теорема о запрете копирования звучит следующим образом. Ортогональные состояния могут быть с вероятностью, сколь угодно близкой к единице, скопированы. В результате копирования получаются состояния с той же формой амплитуд, но сдвинутые (транслированные в пространстве-времени). То есть разрешен более слабый, чем в нерелятивистском случае, процесс в (1). Таким образом, имеем

$$|\varphi_0\rangle \mapsto \big(U_L|\varphi_0\rangle\big) \otimes \big(U_L|\varphi_0\rangle\big)\,,$$
$$|\varphi_1\rangle \mapsto \big(U_L|\varphi_1\rangle\big) \otimes \big(U_L|\varphi_1\rangle\big)\,. \qquad (3)$$

Здесь U_L — оператор трансляции в пространстве-времени вдоль ветви светового конуса, $L = \Delta(x-t)$ — размер области, в которой отлична от нуля амплитуда состояний (считаем для краткости, что оба состояния отличны от нуля в одной и той же пространственно-временно́й области, но различаются формой амплитуд $\varphi_{0,1}(x-t)$).

Аналогично модифицируется теорема [9] о различении ортогональных состояний — разрешен лишь более слабый процесс по сравнению с таковым в нерелятивистском случае (2):

$$|\varphi_0\rangle \otimes |A\rangle \mapsto \big(U_L|\varphi_0\rangle\big) \otimes |A_0\rangle\,,$$
$$|\varphi_1\rangle \otimes |A\rangle \mapsto \big(U_L|\varphi_1\rangle\big) \otimes |A_1\rangle\,, \qquad |A_0\rangle \neq |A_1\rangle\,. \qquad (4)$$

Сказанное удобно пояснить с помощью диаграмм, приведенных на рис. 1.

Поскольку амплитуда состояний безмассового квантованного поля, распространяющихся в одном направлении оси x, зависит лишь от разности $x-t$, то можно фиксировать время и считать переменной координату, либо наоборот. Рассмотрим оба случая. Этими двумя случаями исчерпываются все ситуации. Пусть задано одно из ортогональных состояний с амплитудой $\varphi(x-t)$, распространяющихся со скоростью света ($c=1$, индекс состояния 0 или 1 для краткости пока опустим). Пусть состояние сосредоточено в области L, в том смысле, что $\int_L \big|\varphi(x-t_0)\big|^2\,\mathrm{d}x \approx 1$, $\varphi_{0,1}(x-t_0)$ есть амплитуда на временно́м срезе t_0.

Чтобы иметь *сразу все значения амплитуды состояния при всех x в момент t_0* в той области, в которой она отлична от нуля, необходимо совершить унитарное преобразование сразу над всем состоянием. Пусть унитарное преобразование над амплитудой состояния — $U\varphi_{0,1}(x-t_0) = \tilde{\varphi}_{0,1}(x'-t)$ $(t > t_0)$, тогда амплитуда нового состояния $\tilde{\varphi}(x'-t)$ может быть отлична от нуля уже в меньшей пространственной области. По существу, минимальный размер области по x' к моменту t диктуется релятивистским принципом причинности, который был сформулирован в окончательной форме Н.Н. Боголюбовым [39]. Матричные элементы унитарного оператора отличны от нуля только тогда, когда точки (x,t_0) и (x',t) лежат внутри "прошлой" части светового конуса, выпущенного из точки Г, и накрывающей область, в которой отлична от нуля амплитуда состояния в момент t_0. К моменту не более раннему, чем L, амплитуда исходного состояния может быть унитарным образом преобразована в состояние со сколь угодно сильно локализованной амплитудой в окрестности Г. Принципиально важно, что это будет уже *другое* состояние, отличное от исходного $\varphi(x-t_0)$. К моменту Г доступны значения амплитуды состояния при всех x сразу (мгновенно). Теперь можно мгновенно получить исход измерения и иметь полную (с вероятностью 1) информацию о состоянии. Если пара исходных состояний ортогональна, то можно унитарным преобразованием получить также пару ортогональных состояний к моменту Г и, следовательно, достоверно отличить одно от другого (теперь уже можно воспользоваться теоремой [9] о достоверной различимости ортогональных состояний). Подчеркнем еще раз, что это будут уже *другие* ортогональные состояния, отличные от исходных. "Восстановление" или копирование состояния также может быть реализовано обратным унитарным преобразованием, "направленным" вперед во времени. Состояние с той же формой амплитуды, что и исходное, может быть получено к моменту не более раннему, чем момент, определяемый релятивистской причинностью. Амплитуда состояния с той же формой, как у исходного, находится в передней части светового конуса, выпущенного из точки Г. Полученное состояние также *другое* по сравнению с исходным, в том смысле, что оно запаздывает по времени по отношению к исходному состоянию,

[3] Важным является вопрос о локализации состояний в релятивистской области (в связи с этим см. [42–47]).

которое успело бы распространиться вперед по x к моменту L как раз на величину L, если бы не было попыток копирования или получения информации о нем (рис. 1а). Пока речь шла о получении информации о состояниях в канале с вероятностью 1. Те же самые рассуждения годятся для получения информации с вероятностью, меньшей единицы. Задержка при этом будет меньше L (см. рис. 1).

Подобные рассуждения работают и в нерелятивистском случае. Если игнорировать ограничения специальной теории относительности, то в предыдущем рассмотрении нужно отбросить ту часть, которая апеллирует к световому конусу. При этом унитарные преобразования можно делать формально мгновенно, и из рассмотрения можно исключить даже явное присутствие координаты, оставив неявно только то, что при унитарном преобразовании состояния доступны целиком (целиком мгновенно доступна вся пространственная область).

Аналогично можно провести рассуждения, когда состояние унитарным образом преобразуется в состояние вспомогательной локализованной системы. Пример такого унитарного преобразования имеет место при "остановке" света [48]. Данное унитарное преобразование переводит состояние фотонного поля в вакуумное состояние вследствие его безмассовости и невозможности иметь нулевую скорость распространения, а состояние атомной системы — в некоторое новое состояние. Преобразование, будучи унитарным, также требует доступа ко всем значениям амплитуды фотонного пакета в точке локализации атомной системы. Такой доступ достигается естественным образом по мере распространения пакета со скоростью света и достижения им локализованной атомной системы ("вхождение" пакета целиком в атомную систему). Данный процесс, если речь идет о получении результата с вероятностью 1, также требует времени L (однофотонный пакет должен целиком "войти" в атомную систему). При этом фотонное поле оказывается в *другом — вакуумном — состоянии*, а вспомогательная система оказывается в новом состоянии в зависимости от входного фотонного состояния. К моменту времени L с вероятностью 1 можно выяснить, что это за состояние и приготовить такое же, но с задержкой на L, которая неизбежна в этом случае в отличие от случая свободного распространения исходного пакета (рис. 1б).

Таким образом, любое получение информации об одном из ортогональных состояний приводит к неизбежной их модификации — трансляции в пространстве-времени (*задержке*).

Для дальнейшего также важно, что никакая эволюция безмассового квантованного поля, взаимодействующего с окружением (другими квантовыми и классическими степенями свободы в канале), не может привести к "сжатию" состояния, в том смысле, что нормировка состояния будет набираться в пространственной области, выходящей за световой конус, которая меньше, чем таковая при свободном распространении (рис. 2). Как правило, такое взаимодействие приведет к тому, что состояние будет смешанным, но носитель матрицы плотности в пространстве-времени не может быть "сжат" и выведен за световой конус (см. рис. 2). В противном случае это позволяло бы передавать информацию с помощью квантовых состояний быстрее скорости света. Действительно, пусть имеется одно из пары

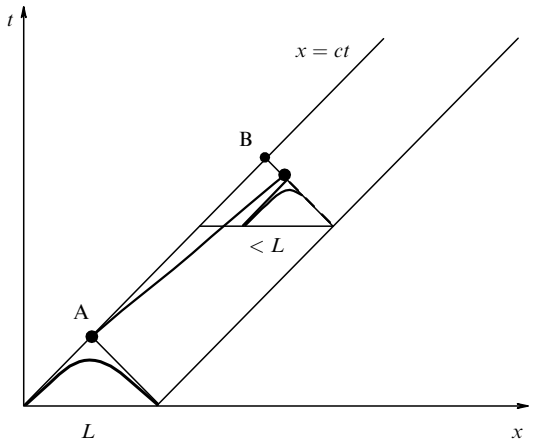


Рис. 2.

ортогональных квантовых состояний (см. рис. 2). Участник A может извлечь классическую информацию из квантового состояния не ранее, чем в момент времени, определяемый условием накрытия амплитуды состояния "прошлой" частью светового конуса. После этого он может передать уже классическую информацию участнику B. Такая передача не может быть сделана быстрее, чем со скоростью света (наблюдатели соединены ветвью светового конуса (см. рис. 2)). Если бы в результате своей эволюции квантовое состояние в канале могло "сжаться" таким образом, что при накрытии состояния "прошлой" частью светового конуса вершина конуса оказывалась в области, пространственноподобной световому конусу с вершиной в точке A, одна из ветвей которого проходит через точку B, то наблюдатель B мог бы извлечь классическую информацию из квантового состояния раньше, чем мог бы передать ее со скоростью света участник A, поскольку вершина светового конуса, накрывающего "сжатое" квантовое состояние, выходит в пространственноподобную область.

С точки зрения криптографии сказанное означает, что шум в канале не дает подслушивателю возможности ни скопировать, ни получить информацию о состоянии раньше, чем это диктуется ограничениями релятивистской причинности и квантовой механикой (*фактически квантовой теорией поля*).

Привлечение новых фундаментальных физических принципов в квантовую криптографию позволяет сформулировать новый подход к обеспечению секретности передачи ключей, который снимает трудности, имеющиеся в нерелятивистской квантовой криптографии (см. детали в [38]). Подобные квантовые криптосистемы естественно называть релятивистскими.

Рассмотрим кратко теоретическую предельно достижимую скорость генерации секретных ключей в квантовой криптографии[4] через квантовый канал связи с конечной частотной полосой пропускания W.

В классическом случае, когда сигнал описывается функцией времени $x(t)$, число бит информации, которое

[4] Сейчас скорость распространения ключей в квантовой криптографии определяется отнюдь не принципиальными ограничениями, а уровнем технологии, точнее, временем возвращения лавинных фотодетекторов в исходное состояние после регистрации фотона и эффектами афтерпалсинга (afterpulsing).

может быть передано через канал с конечной частотной полосой, согласно знаменитой теореме В.А. Котельникова об отсчетах, доказанной в 1933 г. [49] (см. приложение к докладу Н.В. Котельниковой в данном выпуске), определяется числом независимых степеней свободы сигнала, в значение которого можно кодировать передаваемую информацию. В наш цифровой век теорема об отсчетах "работает" в любом устройстве, обрабатывающем или передающем информацию в цифровом виде.

Классический сигнал с конечной частотной полосой описывается функцией времени $x(t)$. На конечном временно́м интервале $(-T, T)$ сигнал $x(t)$, как впервые было показано В.А. Котельниковым [49], определяется $2WT$ степенями свободы в том смысле, что при разложении по ортогональной системе функций,

$$x(t) = \sum_n x_n \theta_n(t)\,, \tag{5}$$

достаточно ограничиться $2WT$ слагаемыми, для которых

$$\int_{-T}^{T} \theta_n(t)\,\theta_m(t)\,\mathrm{d}t = \delta_{nm}\lambda_n(WT), \quad \lambda_n(WT) \approx 1\,. \tag{6}$$

В работе [49] в качестве базисных функций $\theta_n(t)$ использовались так называемые отсчетные функции

$$\theta_n(t) = \frac{\sin W(t - n\pi/W)}{W(t - n\pi/W)}\,. \tag{7}$$

Базис из отсчетных функций обладает замечательным свойством: значения коэффициентов разложения по этому базису x_n равны значениям самого сигнала $x(t)$ в отсчетные моменты времени. Это означает, что для описания непрерывного сигнала в любой момент времени достаточно знать его значения лишь в $2WT$ точках по времени.

Ниже нам будет удобнее использовать другие базисные функции. Число таких функций, наиболее сильно локализованных в окне $(-T, T)$, при этом остается прежним. Кроме того, данные функции возникают и в квантовом случае, где они играют роль одночастичных амплитуд (волновых функций) для фотонов, которые наиболее сильно локализованы во временно́м окне $(-T, T)$.

Ортогональность базисных функций с носителем в конечной частотной полосе W приводит к условию

$$\begin{aligned}
&\int_{-T}^{T} \theta_n(t)\,\theta_m(t)\,\mathrm{d}t = \\
&\quad = \frac{1}{\pi}\int_{k\leqslant|W|}\int_{k'\leqslant|W|} \theta_n(k)\,\frac{\sin(k-k')T}{k-k'}\,\theta_m(k')\,\mathrm{d}k\,\mathrm{d}k'\,, \\
&\theta_n(k) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \theta_n(t)\exp(-\mathrm{i}kt)\,\mathrm{d}t\,.
\end{aligned} \tag{8}$$

Базисные функции ортогональны, если они удовлетворяют следующему интегральному уравнению:

$$\lambda_n(WT)\,\theta_n(k) = \frac{1}{\pi}\int_{k\leqslant|W|} \frac{\sin(k-k')T}{k-k'}\,\theta_n(k')\,\mathrm{d}k'\,. \tag{9}$$

Собственные числа зависят только от произведения WT и образуют бесконечную серию

$$1 > \lambda_1(WT) > \lambda_2(WT) > \ldots > 0\,.$$

Степень локализации квадрата n-й функции во временно́м окне $(-T, T)$ определяется собственным числом

$$\int_{-T}^{T} \theta_n^2(t)\,\mathrm{d}t = \lambda_n(WT)\,. \tag{10}$$

Интегральное уравнение (9) определяет так называемые функции вытянутого сфероида (prolate spheroidal functions) [50]. Собственные числа обладают тем замечательным свойством, что при больших WT, $WT \gg 1$, разбиваются на две группы: одна с номерами $n < 2WT$, для которых $\lambda_n(WT) \approx 1$, и другая с номерами $n > 2WT$, для которых $\lambda_n(WT) \approx 0$. Размер переходной от одного поведения к другому области по номерам составляет $\approx \ln(4\pi WT)$, т.е. для любого $\varepsilon > 0$

$$\lim_{WT\to\infty} \lambda_{2WT(1-\varepsilon)}(WT) = 1\,, \qquad \lim_{WT\to\infty} \lambda_{2WT(1+\varepsilon)}(WT) = 0\,. \tag{11}$$

Это означает, что при больших WT имеется не более $2WT(1-\varepsilon)$ ортогональных (различимых) функций, вклад которых во временно́м окне $(-T, T)$ стремится к единице. Если использовать более чем $2WT(1+\varepsilon)$ степеней свободы, то среди них будут состояния, которые дают во временно́м окне $(-T, T)$ исчезающе малый вклад. При больших WT сигнал $x(t)$ в конечной частотной полосе на конечном временно́м интервале описывается не более чем $2WT$ независимыми (ортогональными и различимыми) степенями свободы и может быть задан $2WT$ независимыми коэффициентами разложения x_n.

Если классический источник с конечной частотной полосой W генерирует сигналы, локализованные во временно́м окне $(-T, T)$ таким образом, что коэффициенты разложения задаются в соответствии с заданным распределением вероятностей $p(x_n)$ на множестве этих коэффициентов x_n (значений амплитуд сигнала), то энтропия источника определяется величиной

$$\begin{aligned}
&I\big(WT, p(x_n)\big) = 2WTH\big(p(x_n)\big)\,, \\
&H\big(p(x_n)\big) = -\sum_n p(x_n)\log p(x_n)\,.
\end{aligned} \tag{12}$$

Далее, если эти сигналы передаются через идеальный (без шума) физический канал связи, например с той же частотной полосой пропускания W, то энтропия источника (12), по существу, совпадает со взаимной информацией между входом и выходом такого канала связи. Тогда пропускная способность в единицу времени (источник + физический канал связи + приемник) определяется как

$$C = \lim_{T\to\infty}\frac{1}{2T}\max_{\{p(x_n)\}} I\big(WT, p(x_n)\big) = W\max_{\{p(x_n)\}} H\big(p(x_n)\big)\,. \tag{13}$$

Для сравнения классического и квантового случаев нам потребуются следующие качественные соображения. В рамках классической физики нет никаких формальных запретов на изменение значений коэффициентов разложения x_n (амплитуд ортогональных базисных функций $\theta_n(t)$) со сколь угодно малой дискретностью (непрерывно). Поскольку интенсивность классического сигнала x_n^2, например для электромагнитного поля, в каждой отдельной моде $\theta_n(t)$ представляет собой с

точностью до множителя $\approx \hbar W$ число фотонов в этой моде, то изменение уровня сигнала может происходить с конечной дискретностью. Для кодирования информации в значения x_n необходимы, по крайней мере, два значения ($x_n^2 \propto N_{\max}$, $N_{\max}$ — максимальное число возможных значений x_n^2). Полное число разных значений для всех мод есть $(\sqrt{N_{\max}})^{2WT}$. Если каждое значение выбирается с равной вероятностью, то энтропия источника (12) равна

$$I\bigl(WT,\, p(x_n)\bigr) = 2WT \log\bigl(\sqrt{N_{\max}}\bigr)\,. \tag{14}$$

Пропускная способность (8) в единицу времени при минимальном уровне сигнала ($N_{\max} = 2$) есть

$$C = W. \tag{15}$$

Формула (15), *являющаяся по существу другой записью теоремы В.А. Котельникова об отсчетах, определяет количество информации в битах на одну степень свободы, которое может быть передано в единицу времени.*

Строго говоря, применять формулы, когда числа заполнения мод малы, нельзя.

Далее нас будет интересовать пропускная способность в однофотонном режиме (числа заполнения мод равны единице). Именно эта величина и будет определять скорость генерации ключа в квантовой криптографии через канал с конечной частотной полосой W.

Приведенные рассуждения были нужны для качественного сравнения классического и квантового случаев. Наша задача будет фактически сводиться к подсчету для источника с конечной частотной полосой W числа возможных ортогональных многофотонных состояний, локализованных во временно́м окне $(-T, T)$. Рассмотрим сначала однофотонные состояния на выходе источника, которые затем распространяются в одном направлении ($k > 0$) и имеют носитель в конечной частотной полосе W ($k \in [0, W]$). Будем игнорировать поляризационные степени свободы при кодировании в различные формы амплитуд состояний, опять ради более близкой аналогии с классическим случаем. Для упрощения выкладок положим $c = \hbar = 1$. Имеем

$$|\varphi^e\rangle = \int_0^W \frac{\mathrm{d}k}{k}\, \varphi\bigl(k, k_0 = |k|\bigr)\, a^+(k)|0\rangle = \int_{-\infty}^{\infty} \mathrm{d}\tau\, \varphi(\tau)|\tau\rangle\,, \tag{16}$$

$\varphi(k,k)$ ($k > 0$) и $\varphi(\tau)$ — амплитуды однофотонного пакета в импульсном и пространственно-временно́м представлении соответственно,

$$\begin{aligned} &\varphi(\tau) = \frac{1}{2\pi}\int_0^W \frac{\mathrm{d}k}{\sqrt{k}}\, \exp\left(-\mathrm{i}k\tau\right) \varphi(k,k)\,,\\ &|\tau\rangle = \int_0^W \frac{\mathrm{d}k}{\sqrt{k}}\, \exp\left(\mathrm{i}k\tau\right) |k\rangle\,, \qquad |k\rangle = a^+(k)|0\rangle\,. \end{aligned} \tag{17}$$

Для безмассового поля $\tau = x - t$ зависит лишь от разности координаты и времени, следовательно, если результат измерения имел место в окрестности точки x в момент времени t, то такой же результат может быть получен в точке x' в момент $t' = t + (x' - x)$. Ниже, упоминая о временно́м окне, будем иметь в виду, что $(-T, T)$ означает $(-(x-t), (x-t))$.

Нам потребуется выбрать амплитуду (волновую функцию) однофотонного пакета с носителем в конечной частотной полосе W так, чтобы от нее набиралась максимальная нормировка в пространственно-временно́й области — окне $(-T, T)$. Формально степень локализации описывается измерением в этом окне. Любое измерение над однофотонным пакетом во временно́м окне описывается разложением единицы в одночастичном подпространстве, которое имеет вид

$$\begin{aligned} I^{(1)} &= \int_0^W \frac{\mathrm{d}k}{k}\, |k\rangle\langle k| = I^{(1)}(T) + I^{(1)}(\overline{T}) = \\ &= \int_{-T}^{T} \frac{\mathrm{d}\tau}{2\pi}\, |\tau\rangle\langle\tau| + \int_{-(\infty,\infty)/(-T,T)} \frac{\mathrm{d}\tau}{2\pi}\, |\tau\rangle\langle\tau|\,. \end{aligned} \tag{18}$$

С учетом (12), (13) оператор, соответствующий временно́му окну $(-T, T)$, представляется в виде

$$I^{(1)}(T) = \sum_{n=1}^{\infty} \lambda_n(WT)|\theta_n\rangle\langle\theta_n|\,, \qquad |\theta_n\rangle = \int_0^W \frac{\mathrm{d}k}{k}\, \theta_n(k)|k\rangle\,. \tag{19}$$

Сами функции $\theta_n(k)$ являются собственными функциями интегрального уравнения, отличающегося от (9) только тем, что интегрирование ведется по отрезку $[0, W]$. Число функций, локализованных во временно́м окне $(-T, T)$, будет равно WT. По сути, векторы $|\theta_n\rangle$ являются собственными векторами оператора $I^{(1)}(T)$ — в базисе этих векторов оператор диагонален. Любое измерение над исходным состоянием, когда доступны исходы лишь во временно́м окне, эквивалентно измерениям над следующей эффективной матрицей плотности:

$$\begin{aligned} \rho(T) = &\sum_{n,n'} \lambda_n(WT)\, \lambda_{n'}(WT)|\theta_n\rangle\langle\theta_n|\varphi\rangle\langle\varphi|\theta_{n'}\rangle\langle\theta_{n'}| + \\ &+ \mathrm{Tr}\left\{I^{(1)}(\overline{T})|\varphi\rangle\langle\varphi|\right\}|?\rangle\langle?|\,. \end{aligned} \tag{20}$$

Здесь введено формальное состояние $|?\rangle$, которое является ортогональным всем состояниям и описывает исходы вне временно́го окна. Такие исходы отвечают ситуации, в которой внутри окна вообще не было срабатывания аппаратуры. Эффективная матрица плотности с учетом таких исходов, которым должен быть приписан неопределенный (inconclusive) результат, имеет единичный след. При больших WT можно выбрать одно из WT ортогональных (различимых) однофотонных состояний, которое с вероятностью, сколь угодно близкой к единице ($\lambda_n(WT) \approx 1$), локализовано в окне $(-T, T)$ и которое имеет в этом окне эффективную матрицу плотности

$$\begin{aligned} &\rho_n(T) = \lambda_n(WT)|\theta_n\rangle\langle\theta_n| + \bigl(1 - \lambda_n(WT)\bigr)|?\rangle\langle?|\,, \qquad (21)\\ &1 \leqslant n \leqslant WT. \end{aligned}$$

Пусть источник генерирует в рабочем временно́м окне $(N = WT)$-фотонные состояния вида

$$\begin{aligned} &|\theta_{n_1}; \ldots; \theta_{n_N}\rangle = \\ &\quad = \int_0^W \ldots \int_0^W \frac{\mathrm{d}k_1}{k_1} \ldots \frac{\mathrm{d}k_N}{k_N}\, \theta_{n_1}(k_1) \ldots \theta_{n_N}(k_N)|k_1, \ldots, k_N\rangle\,,\\ &|k_1, \ldots, k_N\rangle = a^+(k_1) \ldots a^+(k_N)|0\rangle\,, \end{aligned} \tag{22}$$

где обобщенные базисные векторы полностью симметричны по перестановкам частиц:

$$|k_1, \ldots, k_N\rangle = \sqrt{\frac{k_1 k_2 \ldots k_N}{N!}} \sum_{\{j\}} \delta(k_1 - q_{j_1}) \ldots \delta(k_N - q_{j_N})\,, \tag{23}$$

символ $\{j\}$ означает, что суммирование происходит по всем перестановкам. Сконструируем теперь $(N=WT)$-фотонные матрицы плотности. Число заполнения каждой одночастичной моды при этом равно 1. Множество векторов в (17) с различными индексами образуют собственные векторы оператора $I^{(N)}(T)$ в $(N=WT)$-фотонном подпространстве, аналогично однофотонному случаю. Имеем

$$I^{(N)}=\int_0^W\dots\int_0^W\frac{\mathrm{d}k_1}{k_1}\dots\frac{\mathrm{d}k_N}{k_N}|k_1,\dots,k_N\rangle\langle k_1,\dots,k_N|= \\ =I^{(N)}(T)+I^{(N)}(\overline{T}), \tag{24}$$

$$I^{(N)}(T)=\int_{-T}^T\dots\int_{-T}^T\frac{\mathrm{d}\tau_1}{2\pi}\dots\frac{\mathrm{d}\tau_N}{2\pi}|\tau_1;\dots;\tau_N\rangle\langle\tau_1;\dots;\tau_N|= \\ =\sum_{n_1,\dots,n_N=1}^{\infty}\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)|\theta_{n_1};\dots;\theta_{n_N}\rangle\langle\theta_{n_1};\dots;\theta_{n_N}|. \tag{25}$$

Подсчитаем число ортогональных $(N=WT)$-фотонных состояний. Если бы $N=WT$ фотонов являлись бы различимыми, то число ортогональных $(N=WT)$-фотонных векторов в окне $(-T,T)$, локализованных в нем с вероятностью почти единица, равнялось бы N^N (без учета поляризационных степеней свободы). В силу принципа тождественности бозонов (фотонов) число таких векторов, которое обозначим для удобства как $2^{M(WT)}$, равно числу способов размещения $N=WT$ тождественных частиц по $N=WT$ состояниям. Таким образом, имеем [51]

$$2^{M(WT)}=\frac{(N+N-1)!}{(N-1)!N!},\qquad N=WT, \tag{26}$$

при больших N с учетом формулы Стирлинга $(N!\approx(N/e)^N\sqrt{2\pi N})$

$$\log 2^{M(WT)}=2N\log 2=2WT. \tag{27}$$

Пусть в каждом рабочем временно́м окне источник генерирует с равной вероятностью одно из $2^{M(WT)}$ ортогональных $(N=WT)$-фотонных состояний. Если источник работает достаточно долго, то статистический ансамбль, в который может быть закодирована классическая информация, описывается матрицей плотности

$$\rho\big(M(WT)\big)=\frac{1}{2^{M(WT)}}\sum_{n_1,\dots,n_N}|\theta_{n_1};\dots;\theta_{n_N}\rangle\langle\theta_{n_1};\dots;\theta_{n_N}|. \tag{28}$$

Максимальная энтропия фон Неймана ансамбля достигается при равновероятном выборе векторов. Информация в конечном временно́м окне $(-T,T)$ извлекается из эффективной матрицы плотности

$$\rho(T)=\frac{1}{2^{M(WT)}}\times \\ \times\sum_{n_1,\dots,n_N}\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)|\theta_{n_1};\dots;\theta_{n_N}\rangle\langle\theta_{n_1};\dots;\theta_{n_N}|+ \\ +\frac{1}{2^{M(WT)}}\sum_{n_1,\dots,n_N}\big(1-\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)\big)|?\rangle\langle?|. \tag{29}$$

При больших WT нельзя сконструировать статистический ансамбль, построенный из более чем $2^{M(WT)}$ ортогональных $(N=WT)$-фотонных состояний. Классическая информация, которая может быть закодирована в ансамбль $\rho\big(M(WT)\big)$ и извлечена из $\rho(T)$ (29), дается величиной $\chi\big(\rho(T)\big)$, следующей из фундаментального неравенства, полученного впервые А.С. Холево (см. подробности в [52]). Поскольку состояния $|\theta_{n_1};\dots;\theta_{n_N}\rangle$ и $|?\rangle$ являются чистыми, то $\chi\big(\rho(T)\big)$ совпадает с энтропией фон Неймана для $\rho(T)$, отсюда имеем

$$\chi\big(\rho(T)\big)=-\mathrm{Tr}\left\{\rho(T)\log\rho(T)\right\}= \\ =-\sum_{n_1,\dots,n_N}\frac{\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)}{2^{M(WT)}}\times \\ \times\log\left(\frac{\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)}{2^{M(WT)}}\right)- \\ -\sum_{n_1,\dots,n_N}\left(\frac{1-\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)}{2^{M(WT)}}\right)\times \\ \times\log\left(\frac{1-\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)}{2^{M(WT)}}\right). \tag{30}$$

Пропускная способность в единицу времени определяется пределом, который аналогичен формуле (15) для классического случая. С учетом того, что вклад второй суммы в (30) стремится к нулю, получим

$$C=\lim_{T\to\infty}C_T,\qquad C_T=\frac{\log\left(2^{M(WT)}\right)}{2T}=\frac{M(WT)}{2T}=W. \tag{31}$$

Источник генерирует во временно́м окне $(N=WT)$-фотонные состояния так, что число фотонов на выходе источника в единицу времени $\sim W$ и энергия на один фотон $\sim\hbar W$. Соответственно, число фотонов во временно́м окне $(-T,T)$ равно WT (именно число, а не среднее число фотонов, поскольку состояния $|\theta_{n_1};\dots;\theta_{n_N}\rangle$ в (22) являются собственными векторами оператора числа фотонов, отвечающих собственному числу частиц $N=WT$)[5]. Мощность на выходе источника постоянна и пропорциональна $(\hbar W)W$. Минимальность источника в квантовом случае означает, что число ортогональных одночастичных амплитуд $\theta_n(t)$, из которых строится симметричная по перестановкам частиц $(N=WT)$-фотонная амплитуда, равно WT, и число фотонов — WT, т.е. число заполнения в пересчете на отдельную одночастичную амплитуду равно 1.

Информация в классическом случае кодируется в значения амплитуд (грубо, в число фотонов) в ортогональных модах, в квантовом же случае — в различные ортогональные многофотонные состояния [53]. Последние из-за тождественности фотонов принципиально являются запутанными внутри каждого временно́го окна $2T$. Такое кодирование квантового источника можно рассматривать как квантовый аналог теоремы В.А. Котельникова об отсчетах, когда числа заполнения одночастичных мод доведены до однофотонного уровня.

Удивительным является то, что пропускная способность в единицу времени на одну степень свободы в классическом случае (15), следующая из теоремы В.А. Котельникова об отсчетах, "буквенно" совпадает с аналогичной пропускной способностью в квантовом

[5] Строго говоря, всюду под WT нужно понимать целую часть $[WT]$.

случае (31). Однако способы кодирования в классическом и квантовом случаях оказываются разными.

В заключение следует отметить, что появление новых направлений в области конфиденциальной передачи информации является естественным логическим развитием идей, возникших в работах основателей данной области.

Список литературы

1. Котельников В А, Отчет (1941)
2. Shannon C E "Communication theory of secrecy systems" *Bell Syst. Technol. J.* **28** 656 (1949)
3. Vernam G S "Cipher printing telegraph systems for secret wire and radio telegraphic communications" *J. Am. Inst. Elect. Eng.* **55** 109 (1926)
4. Wiesner S *SIGACT News* **15** (1) 78 (1983)
5. Diffie W, Hellman M "New directions in cryptography" *IEEE Trans. Inform. Theory* **IT-22** 644 (1976)
6. Rivest R L, Shamir A, Adleman L "A method for obtaining digital signatures and public-key cryptosystems" *Commun. ACM* **21** 120 (1978)
7. Bennett C H, Brassard G "Quantum cryptography: public-key distribution and coin tossing", in *Proc. of IEEE Intern. Conf. on Computers Systems, and Signal Processing, Bangalore, India, December 1984* (New York: IEEE Press, 1984) p. 175
8. Wootters W K, Zurek W H "A single quantum cannot be cloned" *Nature* **299** 802 (1982)
9. Bennett C H *Phys. Rev. Lett.* **68** 3121 (1992); Bennett C H, Brassard G, Mermin N D *Phys. Rev. Lett.* **68** 557 (1992)
10. "Информационная технология. Криптографическая защита информации. Функция хэширования", Государственный стандарт Российской Федерации, ГОСТ Р 34.11-94 (Дата введения 01.01.95)
11. Bennett C H, Brassard G, Crépeau C, Maurer U M "Generalized privacy amplification" *IEEE Trans. Inform. Theory* **41** 1915 (1995)
12. Carter J L, Wegman M N "Universal classes of hash functions" *J. Comput. Syst. Sci.* **18** 143 (1979)
13. Muller A, Breguet J, Gisin N *Europhys. Lett.* **23** 383 (1993); Muller A, Zbinden H, Gisin N *Nature* **378** 449 (1995); *Europhys. Lett.* **33** 335 (1996)
14. Marand Ch, Townsend P D *Opt. Lett.* **20** 1695 (1995); Townsend P D *Nature* **385** 47 (1997); *IEEE Photon. Technol. Lett.* **10** 1048 (1998)
15. Hughes R J et al., in *Advances in Cryptology — CRYPTO'96: 16th Annual Intern. Cryptology Conf., Santa Barbara, Calif., USA, August 1996. Proc.* (Lecture Notes in Comput. Sci., Vol. 1109, Ed. Koblitz) (Heidelberg: Springer, 1996) p. 329; Hughes R J, Morgan G L, Peterson C G *J. Mod. Opt.* **47** 533 (2000)
16. Sun P C, Mazurenko Y, Fainman Y *Opt. Lett.* **20** 1062 (1995); Mazurenko Yu T, Giust R, Goedgebuer J P *Opt. Commun.* **133** 87 (1997); Молотков С Н *ЖЭТФ* **114** 526 (1998)
17. Grosshans F et al. *Nature* **421** 238 (2003)
18. Stucki D et al. *New J. Phys.* **4** 41 (2002); quant-ph/0203118
19. Bennett C H et al. *J. Cryptology* **5** 3 (1992)
20. Hughes R J, Morgan G L, Peterson C G *J. Mod. Opt.* **47** 533 (2000)
21. Kosaka H et al. *Electron. Lett.* **39** 1199 (2003); quant-ph/0306066
22. Kimura T et al. *Jpn. J. Appl. Phys.* **43** L1217 (2004); quant-ph/0403104
23. Bethune D S, Risk W P *New J. Phys.* **4** 42 (2002)
24. Bethune D S, Navarro M, Risk W P *Appl. Opt.* **41** 1640 (2002); quant-ph/0104089
25. Elliott C, Pearson D, Troxel G, quant-ph/0307049
26. Rarity J G et al. *New J. Phys.* **4** 82 (2002)
27. Hughes R J et al. *New J. Phys.* **4** 43 (2002); quant-ph/0206092
28. Kurtsiefer C et al. *Proc. SPIE* **4917** 25 (2002)
29. Acín A, Gisin N, Scarani V *Phys. Rev. A* **69** 012309 (2004); quant-ph/0302037
30. Mayers D, Yao A, quant-ph/9802025
31. Biham E et al., quant-ph/9912053
32. Shor P W, Preskill J *Phys. Rev. Lett.* **85** 441 (2000); quant-ph/0003004
33. Tamaki K, Koashi M, Imoto N *Phys. Rev. A* **67** 032310 (2003); quant-ph/0212161
34. Lütkenhaus N *Phys. Rev. A* **61** 052304 (2000)
35. Brassard G et al. *Phys. Rev. Lett.* **85** 1330 (2000)
36. Gilbert G, Hamrick M "Practical Quantum Cryptography: A Comprehensive Analysis (Part I)", Mitre Technical Report, MTR00W0000052 (McLean, VA: Mitre Corporation, 2000); quant-ph/0009027
37. Beveratos A et al. *Phys. Rev. Lett.* **89** 187901 (2002); quant-ph/0206136
38. Молотков С Н *ЖЭТФ* **126** 771 (2004)
39. Боголюбов Н Н, Ширков Д В *Введение в теорию квантованных полей* (М.: Наука, 1973)
40. Landau L D, Peierls R *Z. Phys.* **69** 56 (1931) [Ландау Л Д, Пайерлс Р, в кн.: Ландау Л Д *Собрание трудов* Т. 1 (М.: Наука, 1969) с. 56]; Landau L D, Peierls R *Z. Phys.* **62** 188 (1930) [Ландау Л Д, Пайерлс Р, в кн.: Ландау Л Д *Собрание трудов* Т. 1 (М.: Наука, 1969) с. 33]
41. Bohr N, Rosenfeld L *Kgl. Danske Vidensk. Selskab. Math.-Fys. Medd.* **12** (8) 3 (1933) [Бор Н, Розенфельд Л *Собрание научных трудов* Т. 1 (М.: Наука, 1969) с. 39]
42. Jaffee A M *Phys. Rev.* **158** 1454 (1967)
43. Hegerfeldt G C *Phys. Rev. D* **10** 3320 (1974); Hegerfeldt G C, Ruijsenaars S N M *Phys. Rev. D* **22** 377 (1980)
44. Киржниц Д А *УФН* **90** 129 (1966)
45. Винер Н, Пэли Р *Преобразование Фурье в комплексной области* (М.: Наука, 1964)
46. Bialynicki-Birula I *Phys. Rev. Lett.* **80** 5247 (1998)
47. Newton T D, Wigner E P *Rev. Mod. Phys.* **21** 400 (1949)
48. Fleischhauer M, Lukin M D *Phys. Rev. Lett.* **84** 5094 (2000)
49. Котельников В А, в сб. *Всесоюзный энергетический комитет. Материалы к I Всесоюз. съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности* (М.: Управление связи РККА, 1933) с. 1–19; переизд.: *О пропускной способности "эфира" и проволоки в электросвязи* (М.: Институт радиотехники и электроники МЭИ (ТУ), 2003)
50. Slepian D, Pollak H O *Bell Syst. Tech. J.* **40** 43 (1961); Slepian D "Some asymptotic expansions for prolate spheroidal wave functions" *J. Math. Phys.* (Cambridge, Mass.: MIT) **44** 99 (1965)
51. Ландау Л Д, Лифшиц Е М *Статистическая физика* Ч. 1 (М.: Физматлит, 1995)
52. Холево А С *Проблемы передачи информации* **8** (1) 63 (1972); **15** (4) 3 (1979); *УМН* **53** (6) 193 (1998); *Введение в квантовую теорию информации* (Сер. Современная математическая физика. Проблемы и методы, Вып. 5) (М.: Изд-во МЦНМО, 2002)
53. Молотков С Н *Письма в ЖЭТФ* **78** 1087 (2003)

PACS numbers: **01.60.+q**, **84.40.–x**

В.А. Котельников и его роль в развитии отечественной космической радиоэлектроники

Б.Е. Черток

Вклад Владимира Александровича Котельникова в космонавтику, в космическую технику вообще и в космическую радиотехнику в частности, настолько велик, что на эту тему можно писать очень подробно и много. Здесь же я коротко перечислю основные работы сделанные в этой области под его руководством и позже созданной им школой. Кроме того, остановлюсь на некоторых человеческих особенностях Владимира Александровича как великого ученого, с которыми мне приходилось сталкиваться в процессе очень длинной многолетней работы на этом поприще.

Дело в том, что Владимир Александрович очень часто упрекал меня в том, что это я втянул его в работу в области космонавтики. Делал он это очень вежливо и тонко, так что я и не понимал, действительно ли он этим недоволен или таким образом делает мне комплимент.

А началось все с того, что 13 мая 1946 г. Сталиным было подписано историческое постановление о создании в Советском Союзе ракетной отрасли промышленности, техники и науки.

В соответствии с этим постановлением, несмотря на тяжелейшее состояние, в котором тогда, после войны, находилась страна, создавались базовые институты, которые росли буквально, как грибы. В частности, был создан головной институт по ракетной технике Научно-исследовательский институт Министерства вооружения в Подлипках, вошедший в историю под именем НИИ-88, ныне всем известные Центральный научно-исследовательский институт машиностроения (ЦНИИМАШ) и Ракетно-космическая корпорация (РКК) "Энергия" им. С.П. Королева. Я был заместителем главного инженера НИИ-88 по системам управления.

В один прекрасный день, в начале апреля 1947 г., в институт для ознакомления с его работой приехал президент Академии наук СССР Сергей Иванович Вавилов. Сергей Иванович был тем ученым, который понимал, что прорыв в такую новую область требует объединения усилий промышленности с академической наукой и потенциальными возможностями научных кадров высших учебных заведений.

В НИИ-88 С.И. Вавилов приехал не со свитой академических ученых, а с директором Московского энергетического института (МЭИ) Валерией Алексеевной Голубцовой.

Встреча Вавилова и Голубцовой с руководством НИИ-88, участником которой я был, явилась началом интенсивного процесса вовлечения академических и вузовских ученых в новую область человеческой деятельности — ракетно-космическую.

Одним из судьбоносных результатов этой встречи было привлечение Владимира Александровича Котельникова к творческой деятельности в ракетной технике.

Ознакомившись с проблемами, которые тогда требовали активного участия ученых разных направлений, Вавилов высказал мысль о необходимости создания в системе Академии наук специального Института — будущего Института космических исследований (ИКИ) и обещал принять решение о непосредственном участии академических институтов в работе НИИ-88.

В.А. Голубцова, в свою очередь, предложила, чтобы я — заместитель главного инженера НИИ-88, бывший студент и аспирант МЭИ, приехал в свой родной институт и рассказал ученым института о наших проблемах.

Буквально на следующий день (тогда тянуть было нельзя — не такое было время) я приехал в МЭИ. Там была собрана группа ученых, возможно, Ученый совет, который вела сама Валерия Алексеевна. Я рассказал об основных проблемах, которые стояли перед нами, хотя мы сами мало еще понимали, в чем эти проблемы, дело было еще только на стадии становления. На следующий же день Голубцова еще раз вызвала меня и посадила в компанию, в которой находился в качестве руководителя, как я понял, заведующий кафедрой "Основы радиотехники" В.А. Котельников. И тогда я рассказал, что для нас сегодня самое важное — это иметь возможность с помощью радиотехнических средств непрерывно в реальном времени получать параметры ракеты. С помощью обычного локатора противовоздушной обороны у нас ничего не получалось. То ли из-за того, что у этих локаторов не достаточная точность измерений, то ли они в принципе не годятся для тех параметров движения, которые имели запускаемые ракеты.

Владимир Александрович Котельников и Борис Евсеевич Черток на сессии Российского научно-технического общества радиотехники, электроники и связи им. А.С. Попова. (Москва, Дом ученых, май 2003 г.)

Всего через 10 дней после нашей встречи в кабинете Голубцовой, 27 апреля 1947 г., вышло постановление правительства, подписанное Сталиным, о создании в МЭИ совершенно секретного Сектора специальных работ для выполнения НИР в интересах реактивного вооружения. Даже для нас, привыкших к оперативным решениям правительства, столь быстрая и эффективная реакция была впечатляющей.

Руководителем Сектора специальных работ был назначен Владимир Александрович Котельников.

Котельников был тогда деканом радиотехнического факультета и заведующим кафедрой "Основы радиотехники". Он только в январе 1947 г. защитил докторскую диссертацию. Однако во время войны в 1943 г. он получил Сталинскую премию 1-й степени, а в 1946 г. — вторую Сталинскую премию 1-й степени за создание систем специальной связи. По тем временам Владимир Александрович относился к поколению молодых ученых в области радиотехники. В научном мире он получил признание и уважение не только за секретные изобретения. Он разработал фундаментальные теоретические основы передачи информации, и показал практические методы их использования. Еще в 1933 г. им была опубликована так называемая теорема выборок, которая явилась ключевым элементом цифровых коммуникационных технологий. Суть теоремы Котельникова в том, что она предсказывает, что исходный сигнал передатчика информации может быть восстановлен без ошибок по значениям дискретных выборок. Он впервые показал, что аналоговую информацию можно передавать импульсами, говоря по-современному, в цифровом коде и восстановить после передачи. Во всем радиотехническом и связном мире Котельников стал широко известен после создания теории потенциальной помехоустойчивости. Это и было темой его докторской диссертации, защищенной в 1947 году.

С постановления о создании Сектора специальных работ МЭИ собственно и началось "втягивание" Владимира Александровича в космическую радиотехнику.

В.А. Котельников и Б.Е. Черток с группой сотрудников и гостей ОКБ МЭИ. В первом ряду сидят (слева направо): М.Е. Новиков, М.Н. Мешков, А.Л. Зиновьев, А.Ф. Богомолов, К.А. Победоносцев, В.А. Котельников, Б.Е. Черток. (Москва, ОКБ МЭИ, 1997 г.)

Именно это и явилось причиной, по которой мы с ним встречались; потом уже многие десятки раз, и он шутил, что я втянул его в эту историю. А деятельность его на протяжении последующих лет в этой области действительно исключительна и по объему, и по тому, что он вносил в нее как человек и ученый. Иногда одним только своим присутствием и участием в этой работе, даже не изобретая и не открывая ничего нового, он словно вносил освежающую струю в ситуациях, когда приходилось ставить проблему с головы на ноги.

Молодой коллектив Сектора МЭИ, сплотившийся вокруг Котельникова, работал с необычайным энтузиазмом. И огромной исторической заслугой Владимира Александровича является то, что Сектор превратился в школу. По существу, именно им, Котельниковым, была заложена основа и создано теперь уже широко известное Особое конструкторское бюро (ОКБ) МЭИ — очень мощная, высококвалифицированная организация, работающая и создающая радиотехнические системы целенаправленно для ракет и космических аппаратов.

Котельников вошел в закрытое общество ракетчиков, возглавляемое С.П. Королевым, как ученый и инженер. С нами, ракетчиками, он делил трудности первых лет полигонной жизни, а условия тогда были такие, что мы буквально "спали под одной шинелью". Владимир Александрович очень быстро завоевал большой авторитет у бывалых боевых генералов и главных конструкторов. Его чувство юмора и неиссякаемый оптимизм зачастую сглаживали обострение отношений между главными конструкторами в ситуациях, когда ракеты летели "за бугор". Участие Котельникова и его сотрудников было столь значительным, что и работа, и летные испытания уже не мыслились дальше без систем, разработанных сначала Сектором специальных работ МЭИ, а затем уже без аппаратуры, которая создавалась ОКБ МЭИ и далее шла в большое серийное производство. Все первые полеты, вошедшие в историю ракетной космической техники и обусловившие приоритет нашей страны, проходили с непременным использованием радиотехнических устройств, созданных школой Котельникова. Имеется в виду и бортовая, и наземная радиотехническая аппаратура, которая контролирует полет ракеты, ее траекторию и в режиме реального времени дает представление об орбитах космического аппарата. И что очень важно, — телеметрическая аппаратура, которая непрерывно посылает на землю все параметры, интересующие и разработчиков, и тех, кто эксплуатирует космические аппараты.

В.А. Котельников добился независимости от промышленных министерств при изготовлении разрабатываемых систем, создав при МЭИ свои опытные мастерские — впоследствии завод с законченным циклом. Свою аппаратуру и системы им приходилось создавать в острой конкурентной борьбе с мощными промышленными организациями за право оснащения первых межконтинентальных ракет и космических аппаратов. Сейчас много говорят, что в нашей старой системе, нашей старой экономике не было конкуренции. Ничего подобного — конкуренция была, может быть, даже более жесткая, чем при экономике так называемого свободного рынка. Потому что промышленные министерства считали, что это их исключительное право разраба-

тывать подобного рода системы. В частности, на этом настаивали министерство промышленности средств связи, министерства радиотехники и электроники. А тут, понимаете, какой-то спецсектор, ОКБ при высшем учебном заведении. Котельникова все знали и уважали, но он подчинялся министру высшего образования. А это вызывало большую ревность. И было много комиссий, в которых я принимал участие, когда надо было решать, чью разработку принимать в эксплуатацию и на вооружение. И, как правило, все эти конкурсные соревнования, несмотря на ведомственные давления, выигрывала школа Котельникова.

Первыми разработками, которые В.А. Котельников со своим коллективом создали для ракетной техники, были системы "Индикатор-Д" и "Индикатор-Т". Этими системами оснащались первые ракеты Р-2 Главного конструктора Королева при летных испытаниях начиная с 1950 г.

Система "Индикатор-Д" впервые позволила точно воспроизвести траекторию полета ракеты по наблюдениям с наземных радиопунктов.

"Индикатор-Т" был первой радиотелеметрической системой, созданной в МЭИ. С 1953 г. начали серийный выпуск бортовой аппаратуры систем радиоконтроля траекторий полета ракет. В 1955 г. была создана фазометрическая система контроля орбит "Иртыш".

Дальнейшие модификации систем внешнетраекторных измерений "Рубин" и "Алмаз" изготовлялись большими сериями и являлись обязательной принадлежностью при летных испытаниях всех типов ракет и большинства космических аппаратов.

В начале 1950-х годов коллектив Котельникова создал знаменитую радиотелеметрическую систему "Трал". Эта разработка не менее чем на 10 лет опередила уровень соответствующих мировых и отечественных разработок. В условиях чрезвычайно ограниченной и отстающей от американской элементной базы была создана эффективная система, использующая времяимпульсный код при оригинальных схемо-технических решениях, обеспечивавших высокую надежность. "Тралы" бортовые изготовлялись крупными сериями. Система "Трал" была основным инструментом при отработке первой межконтинентальной ракеты Р-7, пилотируемых космических кораблей и летно-конструкторских испытаниях основных ракет нашего ракетно-ядерного щита. На территории Советского Союза были построены десятки наземных измерительных пунктов, связанных в единый командно-измерительный комплекс. Обязательной принадлежностью этих пунктов являлись телеметрические станции "Трал" и станции контроля орбит "Кама", разработанные Сектором специальных работ МЭИ и серийно освоенные радиопромышленностью.

В 1957 г. телеметрическая система, разработанная МЭИ, впервые выходит в космос на втором искусственном спутнике Земли, а для третьего искусственного спутника коллектив создает комплекс траекторных и телеметрических измерений.

В 1953 г. академическое сообщество избирает Владимира Александровича Котельникова действительным членом — академиком Академии наук Советского Союза, минуя традиционную ступень члена-корреспондента. Он назначается заместителем директора вновь созданного академического Института радиотехники и электроники (ИРЭ). В 1954 г. академик Котельников сменил академика Акселя Ивановича Берга на посту руководителя этого института. В 1955 г. он вынужден был оставить должность главного конструктора в МЭИ. Инженерную научно-техническую школу МЭИ возглавил будущий академик Алексей Федорович Богомолов. Великолепный творческий коллектив, созданный Котельниковым, продолжил свою работу в Особом конструкторском бюро МЭИ, образованном по постановлению правительства на основе Сектора. В 1961 г. ОКБ МЭИ награждается орденом Трудового Красного Знамени за участие в создании и запуске первого пилотируемого космического корабля "Восток" с космонавтом Ю.А. Гагариным. Главный конструктор ОКБ МЭИ Алексей Федорович Богомолов стал полноправным членом Совета главных конструкторов Королева, а впоследствии Янгеля и Челомея. Коллектив ОКБ МЭИ прославился также созданием высокоэффективных наземных антенн и ретрансляционных пунктов для систем космической связи и телевидения. Всего на территории СССР и за рубежом было сооружено 160 антенных систем, которые позволили миллионам людей пользоваться космической связью и телевидением. В 1950–1954-х годах Котельников вместе с доцентом МЭИ А.М. Николаевым написали блестящий двухтомный труд *Основы радиотехники*. Еще до избрания в Академию наук Котельников, возглавляя всегда перегруженный ракетно-космическими проблемами Сектор специальных работ, оставался деканом радиотехнического факультета МЭИ и не прекращал своей педагогической деятельности в качестве заведующего кафедрой "Основы радиотехники".

В Институте радиотехники и электроники Академии наук, который Котельников возглавлял до 1987 г., собрался цвет радиоэлектронной науки Советского Союза. Здесь получили развитие фундаментальные исследования по важнейшим научным направлениям радиотехники и электроники.

Котельников организовал в ИРЭ новое космическое направление — планетную радиолокацию и исследование радиоизлучения планет. Под руководством Котельникова проведена радиолокация Венеры, Меркурия, Марса, Юпитера. За эти работы в 1964 г. он был удостоен Ленинской премии.

По инициативе и под научным руководством Котельникова был создан сложнейший радиотехнический комплекс, включающий мощные передатчики, большие остронаправленные антенны, приемные устройства высокой чувствительности и сложнейшую систему автоматической обработки планетных измерений.

В годы руководства ИРЭ Котельников заложил фундаментальные основы радиотехнической планетологии.

Котельникову принадлежит идея использования научного, технического и производственного потенциала отечественной радиотехники и космонавтики для картографирования Венеры. Фундаментальные идеи и методы этого уникального эксперимента разрабатывались в ИРЭ, Институте прикладной математики АН СССР, ОКБ МЭИ под научным руководством Котельникова.

В ОКБ МЭИ была разработана радиолокационная аппаратура для межпланетных станций "Венера-15" и "Венера-16", которые построил Научно-исследовательский центр им. Г.Н. Бабакина.

На Земле для приема и регистрации информации были оборудованы две крупнейшие в Советском Союзе антенны. Одна из них с диаметром зеркала 70 м в настоящее время оказалась за рубежом, а другая диаметром 64 м — в Медвежьих озерах под Москвой: до сих пор является собственностью и гордостью ОКБ МЭИ. В 1983–1984 гг. с помощью радиолокационной аппаратуры, установленной на межпланетных станциях "Венера-15" и "Венера-16" впервые в истории человечества было осуществлено картографирование закрытой непрозрачной атмосферой поверхности планеты Венера. Опыт, полученный в этом эксперименте, позволил разработать для модуля "Природа" орбитальной станции "Мир" радиолокатор бокового обзора и сверхширокодиапазонный радиометрический комплекс.

В кратком сообщении нет возможности перечислить всю массу радиокосмических проблем, в решение которых внес творческий вклад Котельников. Под редакцией Котельникова в 1989 г. был создан атлас поверхности Венеры. Сотни ученых и инженеров из нескольких десятков организаций принимали участие в этом межпланетном эксперименте. Академик Котельников практически доказал, насколько эффективным может быть объединение научных потенциалов высшей школы и Академии наук. Деятельность ОКБ МЭИ и ИРЭ АН СССР, получившая мировое признание, является тому блестящим примером. С 1969 г. по 1988 г. В.А. Котельников являлся вице-президентом Академии наук СССР, причем с 1975 г. — первым вице-президентом. На этом ответственном посту он внес огромный вклад в формирование государственной политики в развитии важнейших научных направлений.

И хотя Владимир Александрович больше не входил, как раньше, в бытность свою главным конструктором Сектора специальных работ МЭИ, в Совет главных конструкторов, он часто помогал, когда возникали серьезные проблемы. В процессе эксплуатации космических аппаратов приходится решать очень много чисто радиолокационных задач. Аппаратура там очень сложная, и поэтому трудно обеспечить высокую надежность. Порой возникают внештатные ситуации, аварии и так далее. Особенно это серьезно, когда такое происходит с пилотируемыми системами, скажем, с системой сближения и стыковки транспортного корабля с орбитальной станцией. В таких случаях Военно-промышленная комиссия при Совете министров тут же создает аварийную комиссию. Обращаются к президенту Академии наук М.В. Келдышу: "Необходима помощь Академии наук, кого Вы включите в эту комиссию?" И, конечно, включают в эту комиссию В.А. Котельникова. Мне в такого рода комиссиях очень много приходилось с ним встречаться и работать. Что его характеризовало и чем он нам помогал: он старался притушить разгоравшиеся страсти на тему "кто виноват" и, прежде всего, вникнуть в проблему физической сущности системы и понять, в чем физика отказа. Предлагал в этом разобраться. И, как правило, это удавалось сделать. Надо сказать, Владимир Александрович обладал исключительной интуицией. Иногда я поражался, каким образом он, не имея всей истории разработки, быстро находил, если не саму причину в деталях, то, по крайней мере, путеводную нить, которой надо было воспользоваться, чтобы понять причины неприятности, которая у нас происходила. И вместе с ним мы очень быстро находили предложения по "лечению" тех неприятностей, которые у нас появлялись.

Значительную долю своей не только научной, но и организационной деятельности он отдавал космонавтике. Многие годы он возглавлял научный Совет АН СССР по проблемам "Радиоастрономия", Совет АН СССР по международному сотрудничеству в области исследования и использования космического пространства. На руководителя Совета "Интеркосмос" были возложены не только научно-технические, но и общественно-политические задачи международного сотрудничества в области космонавтики. Пожалуй, теперь уж трудно восстановить перечень различных комитетов и экспертных комиссий, председателем или членом которых был Котельников. В одной из таких комиссий в 1989 г. мне вместе с Владимиром Александровичем была поручена задача привлечения французской науки и промышленности для создания глобальной спутниковой системы связи и непосредственно телевидения на базе использования нашей сверхтяжелой ракеты-носителя "Энергия". При переговорах в Париже мы не обнаружили энтузиазма с французской стороны и, чтобы "отвести душу", вдвоем с Котельниковым отправились в Лувр. В Лувре я не только наслаждался созерцанием великих произведений искусства, но еще и удивился эрудиции Владимира Александровича, который мне советовал, где и что смотреть. Он сказал, что если попытаетесь обойти весь Лувр, то потом не о чем будет вспомнить. Даже в такой, казалось бы, далекой от его деятельности области, он умел найти, увидеть и, как я убедился, получить эмоциональное удовлетворение от общения с великими произведениями человеческого гения.

За свою научную деятельность Котельников был удостоен многих наград — высоких правительственных, академических в СССР и России и международных. В 2000 г. за фундаментальный вклад в теорию связи профессор Брюс Айзенштайн (США) так оценил научные заслуги Котельникова: "Академик Котельников — выдающийся герой современности. Его заслуги признаются во всем мире. Перед нами гигант радиоинженерной мысли, который внес самый существенный вклад в развитие радиосвязи". В период 1973–1980 гг. Котельников был Председателем Верховного Совета РСФСР. В наше время об этом следует вспомнить еще и потому, что в те годы государство по достоинству оценивало науку как производительную силу, обеспечивавшую экономическое и оборонное могущество страны.

В связи с 95-летием академика Владимира Александровича Котельникова Президент Российской Федерации В.В. Путин 21 сентября 2003 г. подписал указ о его награждении орденом "За заслуги перед Отечеством" I степени. Он стал четвертым в России кавалером этого ордена.

Научно-техническая школа, созданная академиком Котельниковым, в настоящее время интенсивно внедряет новейшие радиотехнические разработки в мировую космонавтику.

Мы вправе гордиться, что вместе с крупнейшим ученым России состояли в Российской ассоциации членов Международной академии астронавтики.