Physics – Uspekhi **49** (7) 725 – 765 (2006)

CONFERENCES AND SYMPOSIA PACS number: 01.10.Fv

Scientific session of the Division of Physical Sciences of the Russian Academy of Sciences, in commemoration of Academician Vladimir Aleksandrovich Kotel'nikov (22 February 2006)

The scientific session of the Division of Physical Sciences of the Russian Academy of Sciences (RAS), devoted to the memory of Academician Vladimir Aleksandrovich Kotel'nikov, was held on February 22, 2006 in the conference hall of the P N Lebedev Physics Institute, RAS. The following reports were presented at the session:

(1) **Gulyaev Yu V** (Institute of Radioengineering and Electronics, RAS) "Vladimir Aleksandrovich Kotel'nikov (Opening address)";

(2) **Kotel'nikova N V** "Vladimir Aleksandrovich Kotel'nikov: the life's journey of a scientist";

(3) **Armand N A** (Institute of Radioengineering and Electronics, RAS) "V A Kotel'nikov and his role in the development of radiophysics and radio engineering";

(4) **Sachkov V N** (Academy of Cryptography of the Russian Federation) "V A Kotel'nikov and encrypted communications in our country";

(5) **Molotkov S N** (Institute of Solid State Physics, RAS, Chernogolovka, Moscow region; Academy of Cryptography of the Russian Federation; M V Lomonosov Moscow State University Department of Computational Mathematics and Cybernetics) "Quantum cryptography and V A Kotel'nikov's one-time key and sampling theorems";

(6) **Chertok B E** (Russian Space Corporation 'Energiya') "V A Kotel'nikov and his role in the development of space radio electronics in our country";

(7) **Pobedonostsev K A** (Special Design Bureau of the Moscow Power Engineering Institute) "V A Kotel'nikov as outstanding engineer and his role in the coming of age of the Special Design Bureau of the Moscow Power Engineering Institute".

An abridge version of the first six reports is given below.

Vladimir Aleksandrovich Kotel'nikov
(06.09.1908 – 11.02.2005)

PACS number: **01.60.+q**
DOI: 10.1070/PU2006v049n07ABEH006046

Vladimir Aleksandrovich Kotel'nikov
(Opening address)

Yu V Gulyaev

It is a year ago that Academician Vladimir Aleksandrovich Kotel'nikov, an outstanding scientist in radio engineering, radiophysics, and informatics, passed away. His name is inseparable from an entire era in the development of these crucially important fields of science and technology, beginning with communication systems and computers and ending with large-scale studies of space. The Kotel'nikov (sampling) theorem is 'engraved into the alphabet' of the education of any engineer in the fields of communications and informatics; the theory of potential noise immunity elaborated by Kotel'nikov lies at the foundation of all modern communications systems, radar, radionavigation, and remote control. His work in radar astronomy rightfully belongs to the science and technology hall of fame.

I was exceptionally lucky in being able to work with Vladimir Aleksandrovich for more than 45 years. Allow me to briefly outline the main events in the life of this illustrious person.

Kotel'nikov, a brilliant scientist, graduated from the Moscow Power Engineering Institute (MEI in Russ. abbr.) in 1930, having majored as a radio engineer, and began his

Uspekhi Fizicheskikh Nauk **176** (7) 751 –792 (2006)
Translated by V I Kisin and E N Ragozin; edited by A Radzig

career as an engineer at the Communications Research Institute of the Red Army, then enrolled as a postgraduate at MEI (1931). After graduation (1933) he moved to the Research Institute of the People's Commissariat of Communications. The data communication facilities at the time were quite crude and the problem of noise resistance in wired communication systems demanded that a drastic solution be rapidly found. In the initial phase of his research career, Kotel'nikov searched to improve the efficiency of the communication facilities. In 1933, he wrote and published a fundamental work "On the transmission capacity of 'ether' and wire in electric communications", in which he formulated for the first time the theorem (known in radio engineering as the Kotel'nikov theorem, or sampling theorem) on exact representation of a function with a band-limited spectrum by a set of its reading taken at separately selected points. It is important to stress here that later this theorem formed the basis of digital processing and transmission of signals and of the creation of digital computers, and is widely used to analyze a number of phenomena in radiophysics and optics. Kotel'nikov was the first to realize the profound importance of the technological consequences implied by this theorem and in fact imparted a profound physical meaning to it.

During the Great Patriotic war (1941 – 1945), Kotel'nikov designed specialized communication equipment and was twice awarded the State Prize for this work (in 1943 and 1946). In 1947, he submitted and defended his doctoral dissertation in which he presented the theory of potential noise immunity and established for the first time the threshold constraints on the sensitivity of radio receivers imposed by noise, and also the theoretical foundations of extracting useful signals from background noise. His monograph *The Theory of Potential Noise Immunity* became widely known and was published both in this country and abroad. The theory of noise immunity still remains one of the main tools the world over for designing communication radar and remote control systems, as well as other radio engineering facilities. These achievements in their totality brought Kotel'nikov world renown.

Kotel'nikov's election to full membership in the USSR Academy of Sciences and his appointment to the post of Director of the Institute of Radioengineering and Electronics (IRE) of the RAS started a new phase in which his talents as an outstanding scientist, science organizer, and science manager of a large research body could manifest their brilliance. He directed all his energy and talent at searching for interesting and promising approaches to solving various scientific problems and to formulating and advancing fundamental research: in long-distance tropospheric propagation of ultrashort radiowaves, in waveguide communication systems, in extracting weak signals from background noise, in processing and transmission of information, and in the generation, amplification, and reception of signals in the centimetric and decimetric wave bands. He put great organizational effort into incorporating into the Institute the best and most talented distinguished physicists, together with the groups that crystallized around them.

Today we can only marvel at Kotel'nikov's sagacity and intuition, which we see in his formulation of new fundamental challenges to current-day radio electronics. For instance, it was under his guidance and with his close participation that progress was achieved in the following fields: moving into new radio-frequency bands (millimetric, submillimetric, optical, and ultralow-frequency wave bands); statistical radiophysics; remote sounding of the atmosphere and of terrestrial and planetary surfaces; that new avenues of research were created: planetary radar and radar investigation of planets using space probes, and work on waveguide and fiberglass broadband communication systems was pioneered. [Detailed results of these studies can be found in the review paper by V A Kotel'nikov and K I Palatov: "Radioengineering and electronics research at the IRE of the USSR Academy of Sciences from 1953 to 1978", in *Problems in Contemporary Radioengineering and Electronics* (Ed. by V A Kotel'nikov) (1980).] Kotel'nikov actively supported investigations into the theoretical foundations of microelectronics, optoelectronics, superconducting electronics, semiconductor electronics, acoustoelectronics, magnetoelectronics, crystal physics, and the automatization of scientific research; he paid special attention to these programs. His contribution to each of these fields did not stop with science management — he always took a very active part in solving the most difficult problems. As Chairman of the Interkosmos Board for many years, he was a permanent science supervisor of many programs on radar investigation of planets in the Solar system and deep space. Numerous results of this research served as a basis for designing various radio devices and systems by factories and plants of the former Ministries of Radio Industry, Electronic Industry, Electrotechnical Industry, Defense Industry, and Communication Facilities Industry, as well as by factories and plants of the Ministry of Communications and some others.

Owing to the efforts of Kotel'nikov and his students and colleagues, the relative accuracy of measuring distances in radar astronomy was improved to 10^{-8} of the quantity measured. Consequently, we know the size of the Solar system much better now and deeper understand the factors influencing the trajectories of planets. On Kotel'nikov's initiative, the antenna and transmitter of the Long-Range Cosmic Communications Center were used for planetary radar, which made it possible to receive weak reflected signals from Venus, Mercury, Mars, and Jupiter, as well as signals reflected by Halley's Comet and some of the larger asteroids.

Kotel'nikov actively supported the program of interplanetary flights of space vehicles. Together with his colleagues, he pioneered in improving the accuracy of the astronomical unit, which was necessary to achieve the required accuracy of control over space vehicles. After the completion of a number of fundamental research projects (1984 – 1992), the cartography of the northern part of the planet Venus was carried out, above 30° north latitude, for the first time ever, over an area of about 115 mln km^2 at a resolution of about 1 – 2 km, using automatic interplanetary stations 'Venera-15' and 'Venera-16', while the atmosphere and ionosphere of Venus were also studied in the framework of the 'Vega' program. The accuracy of the relativistic theory of planetary motion was investigated and a program to study solar wind, near-terrestrial space, and the terrestrial surface was started using space probes and round-the-earth satellites.

The election of Kotel'nikov as Honorary Member of the International Institute of Electrical and Electronics Engineers (IEEE), member of the International Union of Radio Science, member of the academies of sciences of Poland, Czechoslovakia, Mongolia, Bulgaria, and Germany (former GDR) is evidence of the international recognition of his scientific standing.

For his outstanding services to the progress of radio engineering, electronics, and radio astronomy of the mother-

land, as well as for scoring big successes in training new generations of scientists and for his personal achievements, Kotel'nikov was twice awarded the title of a Hero of Socialist Labor, received the Badge of Honor, two Orders of the Red Banner of Labor, six Orders of Lenin, the Order of the October Revolution, the Order of Honor, the Second Class Order of Merit for the Fatherland, and numerous medals. On his 95th birthday he received the Russian Federation First Class Order of Merit for the Fatherland.

He was also awarded, jointly with his corps of co-workers, two State Prizes and one Lenin Prize.

In 1993, the International Institute of Electrical and Electronics Engineers awarded Vladimir Aleksandrovich Kotel'nikov with the Hernand and Sosthenes Behn Prize from the IEEE "for fundamental contribution to communication theory and practice, and pioneering research and leadership in radar astronomy," and with the Alexander Graham Bell Medal "for fundamental contribution to signal theory" in 2000. The Eduard Rhein Foundation (ERF, Germany) awarded in 1999 Kotel'nikov with the Eduard Rhein Basic Research Prize for the first theoretically exact formulation of the sampling theory. Kotel'nikov's tremendous creative contribution to fundamental studies of communications theory and radar investigations of planets was marked in 1974 by the A S Popov Gold Medal of the USSR Academy of Sciences.

The Presidium of the USSR Academy of Sciences awarded Kotel'nikov with the highest distinctions of the Academy — the M V Lomonosov Large Gold Medal, and the M V Keldysh Gold Medal.

Vladimir Aleksandrovich was a quiet, even-tempered man, who treated everyone, from a factory worker to an academician, a general or a government minister, with equal kind-hearted attention. In his enormous erudition, obligatoriness, and desire to get to the bottom of each issue — whether it was a problem in science, or in the Institute's internal politics, or a matter connected with the Presidium of the Academy of Sciences, or just a complication in the life of a concrete collaborator — Kotel'nikov was invariably attentive to each individual and tried to help in any way open to him. He created in the IRE a rather specific, very friendly atmosphere. We practically never suffered from squabbles among the staff.

We, the people who worked at the IRE RAS, deeply respected and loved Vladimir Aleksandrovich. We consider it our obligation and moral duty to sustain the creative atmosphere that he built up in our Institute and to try and follow his principles in our daily lives.

PACS numbers: **01.60.+q**, **01.65.+g**
DOI: 10.1070/PU2006v049n07ABEH006047

Vladimir Aleksandrovich Kotel'nikov: the life's journey of a scientist

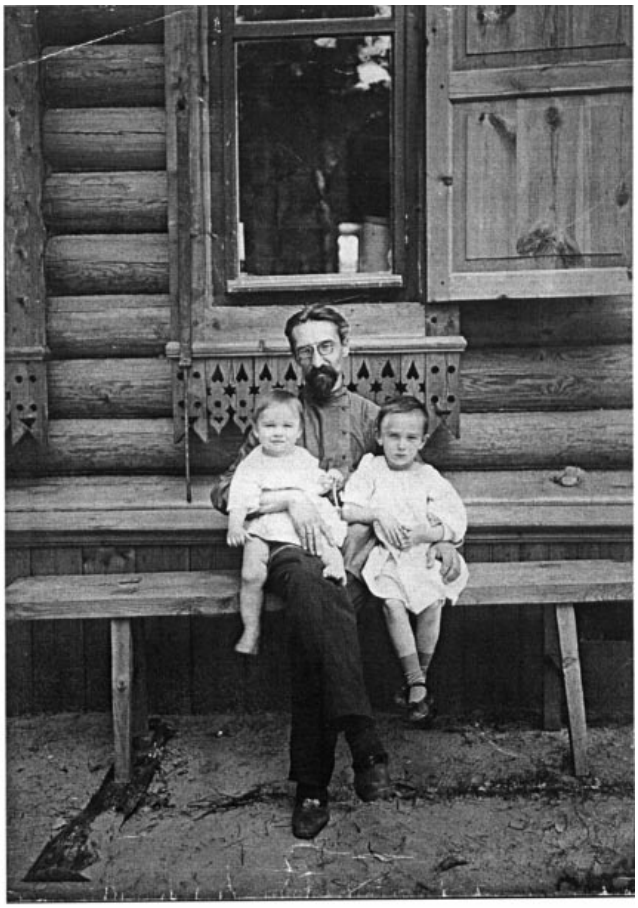
N V Kotel'nikova

In this talk we will outline some of the least known pages of V A Kotel'nikov's biography, covering his 'pre-academic' life. We describe his childhood and the path that led him to science, and also characterize the main stages of his creative life. Our guiding principle in this endeavor is to "tell it like it was". The text is based on Vladimir Aleksandrovich's reminiscences noted down by relatives and friends, on documents in the family archive, and on certain publications.

Childhood. Vladimir Aleksandrovich Kotel'nikov was born on September 6, 1908 in the city of Kazan' into the family of Kazan' University Professor Aleksandr Petrovich Kotel'nikov (1865–1944) and Varvara Petrovna Kotel'nikova (Litvinenko) (1878–1921), who was born and grew up in Kiev and graduated from a Kiev girl's school (gymnasium). The family had three children — Tatiyana, Vladimir, and Vsevolod, with three-year gaps between them.

The Kotel'nikovs, a minor nobility family, never rich, can be traced back to 1622. The line produced military officers, an office employee, lower-rung salaried persons, engineers, and scientists. Vladimir Aleksandrovich's great-great-great-grandfather — Semen Kirillovich Kotel'nikov (1723–1806), a mathematician, was only the seventh Russian scientist elected to full membership in the Russian Empire Academy of Sciences (1751).

His grandfather — Petr Ivanovich Kotel'nikov (1809–1879), mathematics Professor at Kazan' University, Dean of the Department of Physics and Mathematics — was the closest assistant to Nikolai I Lobachevsky. He was the only mathematician in the world who, during Lobachevsky's lifetime, not only understood his geometry but was openly his staunch supporter, posing a challenge to the entire scientific community at the time when Lobachevsky was vehemently vilified. Petr Ivanovich was the only person from whom Lobachevsky received public recognition of his merits as the creator of a new science.



Aleksandr Petrovich Kotel'nikov with son Vladimir (left) and daughter Tatiyana at the dacha in the village of Arakchino near Kazan' (1909).

Vladimir Aleksandrovich's father was Aleksandr Petrovich Kotel'nikov, also a professor at Kazan' University. He was an outstanding mathematician and mechanic, the creator of screw calculus, and one of the founders of the mechanics of a non-Euclidean space and spacetime geometry.

The happy and cloudless childhood of the boy Vladimir was spent mostly in Kazan' and lasted until the age of six (until the World War I). The Kotel'nikovs' home was frequented by friends and colleagues from the university and had lots of books and music. The adults were engrossed in work. As the children grew up, they were taught to play the piano and speak German. At the age of six, Vladimir learned to read and write and knew basic arithmetic, elementary algebra, and geometry, but for some reason he 'got stuck' on trigonometry. He was a great reader, set up interesting physical experiments under his father's guidance, and designed various mechanisms. Aleksandr Petrovich was a keen photographer and Vladimir observed the entire process, from preparing the photographic emulsion for photographic plates to printing the photographs. They attended exhibitions and even saw a genuine airplane. The father used to bring his son to the university where he showed him the mathematics study he himself created, with mathematical models of his own making. Much later this room and its rich library became the launching pad for the Mathematics and Mechanics Research Institute of Kazan' University [1].

In the summer of 1914 the parents made plans to move to Kiev, the city where the mother was born. She just could not get used to living in Kazan's climate and was frequently ill. At last she was able to persuade her husband to agree to an offer of professorship at the chair of mathematics at Kiev University. Aleksandr Petrovich was to start work at his new post in September. But suddenly their entire life was turned upside down — the World War I began. The family arrived in Kiev in August 1914 on the day when the frontline collapsed and the German army broke through; there was terrible panic, triggering an exodus of the population from the city. That was the beginning of the Kotel'nikovs' ordeal. It was with enormous difficulty that they were able to leave Kiev the next day and ultimately reach Kazan'. It then happened that the family found itself at the center of horrendous events near Kazan', then in Kazan' itself, and since the autumn of 1918 again in Kiev. Aleksandr Petrovich had to return to work in Kiev, which was terribly difficult. There was some hope that life in the new hetman republic would return to normal and the university would reopen. The matter is that the lectures in Kazan' University stopped when the university was evacuated to Saratov. In 1917, the university was closed, Aleksandr Petrovich lost his job and at the end of 1918 the Kotel'nikovs relocated to Kiev again. Vladimir Aleksandrovich recalled that their life in Kiev resembled very closely Mikhail Bulgakov's description in the novel *The White Guard* — the same period, the same place and the same circumstances. "It was a great year and a terrible year, the 1918th after Christ was born, but the year 1919 came to be even more terrible...." The city was a constant battleground, continually changing hands, and anarchy and destruction reigned. The times were terrible and hunger loomed. No money, nothing to

Petr Ivanovich Kotel'nikov (1809 – 1879), Vladimir Aleksandrovich Kotel'nikov's grandfather.

Aleksandr Petrovich Kotel'nikov (1865 – 1944), Vladimir Kotel'nikov's father.

sell — how could one feed a family? The professor boiled soap using recipes and ingredients that his friends and former colleagues would procure for him. The children would unravel covers and curtains and roll the thread into balls. The mother would bake buns from produce and additives that friends would provide... And the father would sell all this at the market. However, each evening Aleksandr Petrovich would sit at his desk and work late into the night. It is probable that the father's example, the passion of the scientist, his habit of permanent immersion in his work instilled in Vladimir the desire and ability to work on his own. Books and textbooks, which in this family were treated as living essentials, travelled with the owners from town to town. Reading them was exciting, and he digested 'science' on his own. Of course, he could ask his father for explanations of difficult points but this was not necessary.

In 1920, Aleksandr Petrovich was invited to work at the Kiev Polytechnic Institute, the very first higher education establishment to restart after all the 'perturbations'. Life seemed to slowly start improving. But misfortune struck: the entire family, with the single exception of Vladimir, who was miraculously spared, fell ill with typhus in 1921. Thereupon the great distress overtook their family — the mother and aunt Liza, the father's sister, died of typhus. All domestic chores and children's upbringing fell on Aleksandr Petrovich's shoulders. The older siblings — Tatiyana and Vladimir — greatly helped. Their tasks were to keep the house in order, cook dinner, help father with the vegetable garden, which was the main source of food, and take care of the younger brother Seva — he was to play the role of 'emergency helper'.

School. Institute. University. Vladimir entered school in 1922, directly into the 5th grade. Learning was easy, since he already knew so much. Physics was taught by an instructor of the Polytechnic Institute. His lectures were invariably very interesting and often took place in the institute's building where excellent experiments were demonstrated in a large lecture-hall. The mathematics teacher was a student of the same institute. As far as problem solving was concerned, Vladimir was his equal. Pupils published a hand-written newspaper ('wall paper') and children wrote articles about exciting achievements in science and engineering. Boys would only write about airplanes: this was the time of explosive progress in aviation. But Vladimir decided to write about radio. He believed he more or less knew the essentials of aviation but radio remained a total mystery.

He saw, or rather heard, a signal of a radio station for the first time in Kazan' in 1918 from either 'the reds' or 'the whites' during the battle for the city. His father explained that messages are sent via radio waves that we cannot hear or see. His son's question: "How does it work?" met with the answer: "This is something you cannot understand yet." After an answer like that, Volodya would typically try to think up his own explanation for the incomprehensible phenomenon or device and he usually succeeded. In this case, however, he failed miserably. Radio was awe-inspiring!

He did write that article. In fact, it required rapidly learning trigonometry which was not yet taught at school. However, this was insufficient for being truly able to read and understand papers in the radio engineering journal *Wireless telegraphy and telephony* that his father brought home on his request. (No popular magazines yet existed for the science concerned with radio engineering, which was only making its first steps.) That was when he decided that radio would be his field of serious work.

Volodya Kotel'nikov: "How in the world does radio function?"

In 1924, the family moved to Moscow. Kiev was the scene of intense 'Ukrainization'. Administrators demanded that professors deliver lectures in Ukrainian. Aleksandr Petrovich decided to take the children to Moscow. For some time already he had been invited to take up professorship at the Moscow Higher Technical School (MVTU in Russ. abbr.). Vladimir graduated from a secondary school in Moscow in 1925. All in all, he had spent three years in school but, as he always studied much himself, his level was sufficiently high for trying to enroll in a higher educational institution or university. Radio engineering as a major subject — Vladimir dreamed about it — was also taught at the MVTU but it accepted only people with worker or peasant roots, and only after they graduated from the so-called *rabfak* (workers' faculty pre-training schools). He had to enroll in a communications technical school. A year later, in 1926, he did get into MVTU — bars to enrolling were removed that year. Learning was a pleasure, and it was interesting. He attended only the lectures that he considered cognitive and useful and dealt with the rest by gaining an understanding from relevant textbooks. In parallel, he attended lectures at Moscow State University and covered the entire curriculum of the Physics and Mathematics Department of the University (it was at the time housed right in the center, on Mokhovaya street, where the Institute of Radioengineering and Electronics (IRE RAS) now resides).

Postgraduate courses. The Kotel'nikov theorem. In 1930, Vladimir graduated from the Moscow Power Engineering Institute (MEI), which by that time had separated from MVTU, and was, against his wishes, sent to the postgrad-

uate course. His dream was to join the Central Radio Laboratory (TsRL), the name of the former Nizhnii Novgorod Radio Laboratory after it was transferred to Leningrad. As a student, Kotel'nikov had practice terms there twice, after the first and third years, under B A Ostroumov's supervision. The results obtained during the first practice term allowed Vladimir to publish his first research paper "A triple characterograph (automatic recorder for volt – ampere characteristics)" in the proceedings of the Nizhnii Novgorod Radio Laboratory *Wireless telegraphy and telephony* (No. 46, 1928). However, at the dean's office he was told that, being the best graduate of the year, he should stay at the MEI. Kotel'nikov refused — he wished to do science. Teaching was not attractive for him at the time. While negotiations dragged on — MEI tried to persuade him and he refused — all vacancies at TsRL were filled. Only the dullest positions were still open — sheer supervision and maintenance work in other establishments. Kotel'nikov feverishly tried to figure out what to do with his life. He was not ready yet to give up on his dream. A way out was suddenly suggested by Professor I G Klyatskin, who ran into Vladimir in the corridor of the institute and offered him a position in his laboratory at the Communications Research Institute of the Red Army (NIIS RKKA). The decision was made. Alas, three months later the MEI administration learned about his place of work. A terrible scandal ensued, Klyatskin was accused of unprincipled behavior ... it couldn't be helped, Vladimir had to bow to fate and return to MEI. There he was immediately made postgraduate as of January 1931 (without any exams) and at the same time given the job of senior laboratory assistant. As a senior laboratory assistant, Vladimir was responsible for setting students' laboratory practice going. He was later promoted to assistant professor.

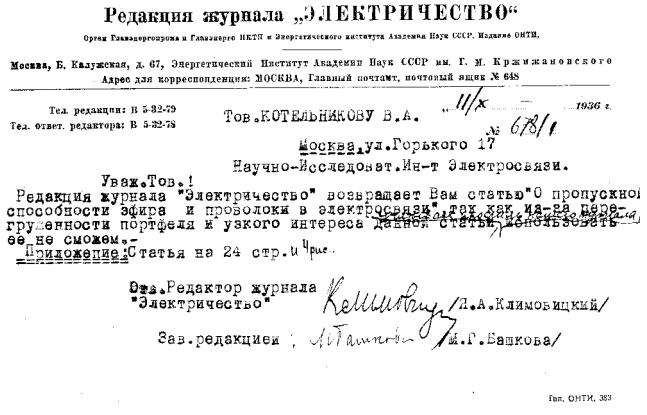
Author of the Kotel'nikov theorem.

It was within the precincts of the laboratories that he first met his future love and wife, Anna Ivanovna Bogatskaya (1916 – 1990). They got married in 1938, brought up three children, and led a life of love and devotion until the end of their days.

The postgraduate course at MEI in those years was cardinally different from what we know now. Postgraduates were their own bosses: no science advisors, no tutoring, no research tasks assigned. The only obligatory learning courses were philosophy and a foreign language; other subjects were selected by the postgraduate student himself. Vladimir decided that since he could not change the framework, he would do his research on his own. He carefully scrutinized pressing problems of radio communication and wire communication. As a result, he prepared in 1932 three papers, one of which — "On the transmission capacity of 'ether' and wire in electric communications" — was submitted as a report to the anticipated 1st All-Union Congress on the Technical Reconstruction of Communication Facilities and Progress in the Low-Currents Industry. The congress was cancelled but contributions to it were published in 1933 (Kotel'nikov's report was accepted for publication in November 1932) [2]. Completing his postgraduate term, Vladimir presented his results to the Learned Council of the department. The presentation was approved but the paper "On the transmission capacity of 'ether'..." and the significance of the sampling theorem proved in it were not understood by the council members — "sure, appears correct, but sounds more like science fiction". More is the pity! The work was outstanding in two aspects. First, it was a well-reasoned program document that cut off blind paths and pointed to promising and feasible approaches to the expansion of radio communication in the aspects of overcoming "overcrowding in the ether and wires". Among other things, the paper outlined a promising technique of transmitting radio waves "on one sideband". Time proved that the predictions by the young Kotel'nikov were right. He himself was advancing unflinchingly along a chosen path together with his laboratory at the Research Institute of Communications of the People's Commissariat of Communications (NIIS NKS) and then with his much later creation — the Institute of Radioengineering and Electronics of the USSR Academy of Sciences (IRE AN SSSR). Second, this work was future-oriented. For the first time there, it was a substantive discussion of the information aspect of communications problems. Vladimir built a mathematical foundation for the prediction of digital data transmission (he proved what in the future became the famous Kotel'nikov theorem). His idea formed the basis for today's information theory. In this aspect, the work was ahead of its time by at least 15 years. It was fully appreciated only at the end of the 1970s when it became possible to replace the analog system of data transmission with that of a digital one [3].

No science degrees were given to people in the early 1930s. On the initiative of the Leningrad Electrotechnical Institute (LETI), the candidate's degree in technical sciences (an equivalent to a PhD) was formally conferred on Kotel'nikov in 1938 without a viva voce procedure.

The subsequent history of the Kotel'nikov theorem, also known as the sampling theorem, formulated and proved by a 24-year-old 'unsupervised' postgraduate, reads very much like a detective story. Vladimir fully understood its signifi-



Редакция журнала „ЭЛЕКТРИЧЕСТВО"

Орган Главэнергопрома и Главэлектро 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

Тов. КОТЕЛЬНИКОВУ В.А. 11/X 1936 г. № 678/1

Москва, ул. Горького 17
Научно-Исследоват. Ин-т Электросвязи.

Увaж. 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, использовать ее не сможем.
Приложение: Статья на 24 стр. и 4 рис.

Отв. Редактор журнала "Электричество" /А.А. Климовицкий/

Зав. редакцией /М.Г. Башкова/

Тип. ОНТИ, 383

Letter from the editorial board of the journal *Electricity* rejecting the paper with the Kotel'nikov theorem (handwritten insert into the typed letter: "...in view of the specific profile of our journal, ...").

cance and tried to publish an article in 1936 in a journal *Elektrichestvo* (Electricity) (the official publication of the Energy Institute of the USSR Academy of Sciences) more widely read by professionals but the manuscript was rejected! "OK, rejected, so be it! People who need to know will read it in 'Conference proceedings' ", — was his decision and he continued to work, completely forgetting this episode. He only recalled it almost seventy years later, when he was shown the rejection letter that survived in his archive (see the figure above).

Fifteen years later (1948) Claude Shannon formulated his sampling theorem [4]. Ideas do hang in the air, and similar theorems did appear at different points on the globe, spread over time and differing in the rigor of proof of the theorem. Because this theorem is of supreme importance in information theory, experts in the field focused their attention on it, especially in the 1970s when progress in electronics made it technically possible to implement the digital transmission and recording of data. In 1977, when the discoverer's priorities were realigned, it was proposed to refer to it as the WKS-theorem, namely, the Whittaker–Kotelnikov–Shannon theorem [5, 6]. Ultimately, in 1999, the Eduard Rhein Foundation, summarizing the results of the most outstanding scientific discoveries of the 20th century, awarded its Prize in the nomination 'for fundamental work' to Russian scientist Vladimir Aleksandrovich Kotel'nikov "for the sampling theorem first rigorously formulated and published", the theorem which is the cornerstone of all modern (now digital) radio engineering and computation engineering.

In an article preceding Kotel'nikov's nomination for this prize, Hans Dieter Lüke wrote about the article "On the transmission capacity of 'ether' and wire in electric communications" that as this brilliant paper was never published in internationally accessible journals, publications of the sampling theory in theoretically exact formulation appeared in the literature on communications systems independently of each other [6]. In view of the fact that this work continues to be of great interest even today, albeit from a historical point of view, *Physics Uspekhi* publishes it for the first time in an 'internationally accessible journal' in the present issue of our journal in the Supplement to this presentation.

Research Institute of Communications of the People's Commissariat of Communications. (Later renamed TsNIIS NKS by adding 'The Central'.) Having graduated from the postgraduate course in 1933, Vladimir Kotel'nikov, continuing to teach at MEI (first as lecturer, then as assistant professor), began working at the NIIS NKS (engineer, chief radio engineer of the institute, head of a new laboratory). In 1936, Kotel'nikov published two pioneering papers in nonclassified publications [7, 8] in which he, as one of the first to achieve it, made use of probability theory to analyze the efficiency of multichannel systems for signal diversity reception and proposed a general analytical method for studying a nonlinear distortion of signals in various devices. Progress in such methods was achieved in the late 1940s in the work of outstanding Soviet and Western scientists [9]. In 1935–1936, the government finalized the strategy of building trunk lines of short-, mid-, and long-range radio communications. In the framework of this directive, NIIS began to develop new equipment for such communication lines. From his days at MEI, Kotel'nikov 'carried' the firm conviction that the wonderful idea of "analog transmission on one sideband" [2] can and must be implemented. Having overcome the resistance of his superiors, he and his team succeeded in implementing this idea and created unique equipment. The industry refused to accept the order for manufacturing the devices designed: "Impossible to produce as no one has ever built it anywhere". "We'll do it ourselves" was Kotel'nikov's decision, and the team succeeded. The equipment was installed on the Moscow–Khabarovsk trunk line (1939). This was an outstanding project for the time. However, the unique radiotelephone circuit, though ready and tested, was not certified for service; the reason was: "too easy to intercept". It was necessary to find a way out, and in a very short time. Kotel'nikov had never worked in cryptography before and had no access to the relevant literature and experts. After a careful analysis, he came to the conclusion that the problem could be handled. The team urgently accepted a challenge. They started from scratch. They had to solve numerous scientific and technical problems as the new equipment would be of an absolutely unknown type. Having read a paper by H Dudley [10] that appeared in October 1939, Kotel'nikov immediately understood the excellent potential advantages of the vocoder (artificial voice generator), described there as a promising device for basing the necessary voice encoding equipment. The first vocoder in the USSR was already working in the laboratory at the beginning of 1941. Kotel'nikov worked under the enormous pressure of deadlines, and had to figure out the main problems of cryptography. He presented his arguments in the report "Fundamentals of automatic encoding", which was submitted just three days before the Great Patriotic war broke out, on June 19, 1941. The report had for the first time "given clear formulation of requirements that a mathematically non-decipherable system must meet, and proof was given of the impossibility of its deciphering" [11]. This work laid the basis for the development of cryptography in the USSR. Unfortunately, not many people know about this work — it was never published in the open media. Four years later, C Shannon described approaches to building deciphering-resistant systems in a classified report dated September 1, 1945. This report was declassified and published in 1949 [4].

The war years. The arrival of the war forced Kotel'nikov and his group to interrupt their research projects and urgently begin designing pilot samples of new equipment. They worked almost around the clock. Soon, with the war front approaching Moscow, NIIS was disbanded and all staff dismissed. Only Kotel'nikov's laboratory was left working

Staff of Kotel'nikov's laboratory (Ufa, April 1943). Standing (left to right): E Kunina, E L Gavrilov, V N Melkov, N N Naidenov. Sitting (left to right): A M Trakhtman, D P Gorelov, Kotel'nikov, I S Neiman, V B Shteinshleger.

as it conducted classified work on radio telephony that was urgently needed at the front. The instruction was: receive the money and pay off all discharged employees of the institute; burn the documentation except the most important; prepare the equipment of the laboratory for evacuation, and if the German army broke through to Moscow, blow up the building of the institute. The first three instructions in the order were implemented. Luckily, there was no need to blast the building. On October 17, 1941, the following entry appeared in Kotel'nikov's personal work-book: "Dismissed from work in view of going on vacation". And the 'vacations' did begin: step by step, the laboratory was evacuated to the town of Ufa in the Bashkiriya in October and November. There was a complication in resuming the work on the equipment: most of the design documents had been destroyed. Despite this, several units of secret radiotelephonic apparatuses were produced by autumn 1942 and were immediately sent to the Transcaucasian front, which had no communication with the center during the battle of Stalingrad (the armies were then using wire communication lines). As a result, it became possible to restore communications via the radio channel. By the beginning of 1943, production lines for this equipment were functioning and the Armies in the Field started using it. This saved the lives of many Soviet soldiers and constituted a huge contribution to the ultimate victory. At the time, this was the most advanced system of secret radiotelephone communications, virtually 'crack-proof'. This same equipment was used to connect Moscow to the Soviet delegation at the signing of Germany's capitulation in May 1945. The staff of the laboratory received awards for this work — First Class Stalin Prizes (1943). The money was donated to meet the needs of the war effort. Kotel'nikov's prize money went into building a tank.

Experts believe that no efficient algorithms for deciphering messages encoded with modernized systems of this type were available until the early 1970s [12].

Return to Moscow. The Moscow Power Engineering Institute. In the spring of 1943, Kotel'nikov's laboratory was relocated from Ufa back to Moscow and transferred to the disposal of the People's Commissariat of Internal Affairs (NKVD) of the USSR. There it was bandied from department to department... At that very moment Kotel'nikov was found by V A Golubtsova — the new Rector of MEI. The war was

Kotel'nikov (center) in the laboratory room of RTF MEI (1946).

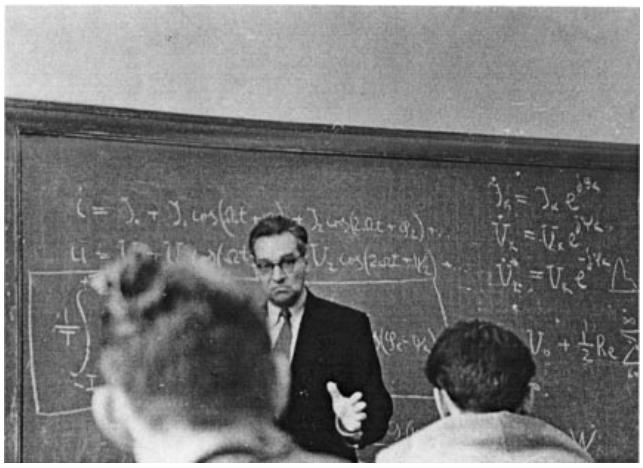
still on but the country was beginning to reconstruct the national economy ruined by the enemy. MEI required rebuilding too — the country needed engineers. Having outlined MEI's problems and prospects for expansion, Golubtsova suggested that Kotel'nikov return to MEI. Kotel'nikov was only too glad to oblige. He preferred to do science in a nonmilitary establishment, and even more so in his alma mater. Incidentally, Golubtsova's husband was G M Malenkov, First Secretary of the Central Committee of the Communist Party of the Soviet Union. It is probable that this was the decisive factor that made it possible for Kotel'nikov, in his position as head of a top-secret project, to escape from the NKVD system to MEI. The order finalizing the transfer to MEI to a position of Head of the Chair of Fundamentals of Radio Engineering (ORT) that he was yet to create at the Radio Engineering Department (RTF) was signed on November 1, 1944. Some time later Kotel'nikov was also elected Dean of the RTF. He is regarded as one of the founders of RTF. His multifaceted efforts at MEI built the 'V A Kotel'nikov scientific and pedagogical school' that advanced along three main directions: further expansion of the ideas of the theory of potential noise immunity that he had created; research related to the theory of the electromagnetic field and expansion into yet unconquered ranges of the electromagnetic spectrum (millimeter, submillimeter, infrared, and optical wave bands), and engineering applications of the theory [12].

Kotel'nikov was firmly convinced that the main task of a training program was to impart a good knowledge of physics and mathematics and to teach the future specialists to think independently. He was the first to introduce theoretical physics into the MEI curriculum. Kotel'nikov's courses on 'Fundamentals of radio engineering' and 'Electrodynamics' (he always conducted them himself) were tremendously popular. They were attended by students and lecturers not only from the Radio Engineering Department but from other

departments as well. Kotel'nikov was known as Reformation Dean. While he held this post, a number of important transformations took place in the department; for instance, he introduced a new speciality for study — radiophysics [13].

At the same time he continued to supervise and consult his former laboratory on the main problems of secret telephony.

Theory of potential noise immunity. One day in the spring of 1946 Golubtsova called Kotel'nikov to her office and stated quite decisively: "Vladimir Aleksandrovich, you absolutely must maintain a thesis for doctorate of sciences". OK, so be it. This had not been a point he had been thinking about earlier. He had no concrete ideas about the subject of his thesis. A legend exists that a draft of a future DSc thesis on potential noise immunity was scribbled on scraps of paper in the difficult years of evacuation but was unfortunately lost on the way back to Moscow. Not true. One suitcase was indeed stolen but no rough copy of the thesis was in it. No thesis existed at the time. The most valuable object in the suitcase was a loaf of bread. In the summer Kotel'nikov took his usual holiday, packed the family off to the summer cottage and started creating the "Theory of potential noise immunity" — that was the title he gave to his thesis. Completing the writing during the holiday weeks proved impossible and he had to finalize the text in the evenings after work. The thesis was ready by autumn. However, the dissertation presentation and its defense ran into a snag. It was not easy to find official opponents because nobody understand the essence of the work presented. "For the science community, the theory emerged virtually 'from thin air'" [14]. The author could not even cite anyone. This work was ahead of its time by about ten years. Academician Nikolai D Papaleksi was invited to write a review of the doctoral dissertation. Papaleksi took a look at the thesis and concluded that he failed to understand anything. To make matters worse, there were no references to other publications and the competitor had no supervisor — he stood all by himself. Papaleksi refused to act as opponent. Ultimately, the official opponents were found and the thesis was defended in January 1947. Witnesses recalled that the impression was that hardly anyone was able to understand much, even the opponents. But everyone had the feeling that right then and there "something very important was being born". It became clear later that what was born on that day was one of the two mutually complementing branches of the information theory. The other branch, C Shannon's work,



"That's how it is...very simple...." (Giving a lecture at MEI (1947).

At a demonstration in a red-letter day, with wife and daughter Nataliya (1948).

appeared in 1948 [4]. In his work Kotel'nikov analyzed for the first time the main problems of communications from the standpoint of probability theory. It provided a powerful impetus for the advance of the statistical theory of message transmission, statistical synthesis of optimal methods of signal processing, and development of efficient algorithms for signal receivers [15]. The author only published a single short paper "Problems of noise immunity in radio communications" (1947) [16] on the topic of his thesis. The second copy of the thesis was duly submitted to the V I Lenin State Library in Moscow for archiving. The work was never published in full at the time. Kotel'nikov probably understood that the situation was no different from what he faced in the case of the previous paper "On the transmission capacity of 'ether' and wire in electric communications". Given that even Academician Papaleksi failed to understand the work, what hope was there of publishing it? "Whoever needs to will find and read it at the Lenin Library", was his decision. Kotel'nikov's monograph *The Theory of Potential Noise Immunity* [17] was published only in 1956, after the first papers devoted to this topical problem began to appear in Western journals. The publication created a huge stir in the entire 'radio engineering world'. Kotel'nikov became world famous!

In 2005, a list of "Printed works of V A Kotel'nikov. 1950" was discovered in Kotel'nikov's archive. The relevant line reads: "*The Theory of Potential Noise Immunity* — a monograph of 12 printer's sheets [1], manuscript, prepared for publication by Svyaz'izdat". It is hardly possible for those who knew Kotel'nikov to imagine that he 'delayed' the realization of a pre-planned job by six years. It is likely that this work was also declined by the publisher.

The Marfino Laboratory or "Third Circle". Alexander Solzhenitsyn's *The First Circle* and K F Kalachev's memoirs *The Third circle* [18] describe events that took place at the

[1] *Translator's note*: 1 printer's sheet comprised 40,000 typographical units, roughly 4000 words.

Two times First Class Stalin Prize (State Prize) laureate (1946).

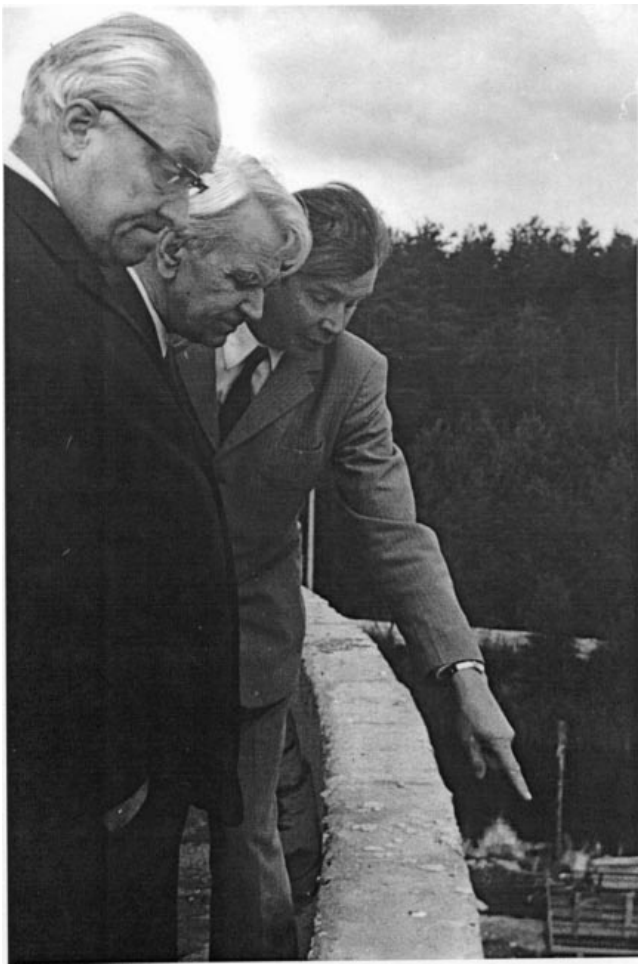
same time and in the same place — the Marfino Laboratory. Both authors worked there but their stations in life, feelings, visions, and reactions were inevitably different. Solzhenitsyn's 'First circle' is a circle of hell for an imprisoned engineer. For Kalachev, a 'free' expert, the 'third circle' is the third stage in the work on secret telephony. The principal scientists and designers of the Marfino Laboratory came from Kotel'nikov's former laboratory which became subordinated to the NKVD technical department after their return from evacuation. Kalachev also worked on Kotel'nikov's team but that was before the war. At the time the Marfino Laboratory was created, Kotel'nikov had already returned to work at MEI.

In 1947, the Ministry of Internal Affairs (MVD) and the Ministry of State Security (MGB) of the USSR decided to establish a Specialized Laboratory for developing the equipment for 'absolutely security-restricted' telephone conversations over governmental radio-frequency communication lines. In view of the top importance of the tasks assigned to the laboratory, it was decided that it must be headed by a brilliant scientist, a well-known expert in the field. There was every reason to consider Kotel'nikov the founding father of secret telephony [11, 18].

One day (in 1947) Kotel'nikov was called to the office of the Minister for the USSR State Security V S Abakumov. The conversation proceeded in a polite and respectful manner. Having outlined what sort of Specialized Laboratory he needed, Abakumov suggested that Kotel'nikov be its head. Kotel'nikov declined the offer. The Minister was surprised to the extreme — he was not in the habit of being turned down. His 'proposal' normally meant 'order'. Abakumov asked what the reason for the refusal was. Kotel'nikov calmly explained that he wished to be engaged in scientific research. Abakumov tried to win the stubborn scientist over by promising numerous perks and privileges. Kotel'nikov stood his ground. "Well, that's a pity ..." concluded the Minister, and the meeting ended.

On his way back to MEI, Kotel'nikov mulled over the resulting situation and what kind of aftermath this "that's a pity..." may bring. Back at MEI, he went straight to the Rector Golubtsova and described for her the visit to MGB. Having heard him out, she asked what he himself wanted. The answer was: "To work at MEI". To which she replied: "Then continue to work calmly as before".

From Special Sector to Special Design Bureau (OKB) of MEI. Having created the ORT Chair at the MEI RTF Department, Kotel'nikov surrounded himself with a team of highly talented scientists and engineers. In 1944 – 1947, they developed telemetric equipment for airplanes, which was found to be excellent. In 1947, exciting new projects were launched in the USSR in the framework of the Missile and Space Program, which MEI actively joined. A Sector of Special Tasks was set up by direction of the USSR Government to carry out research and development studies for the needs of rocket weapon (Special Sector). The Special Sector was mostly based on the (substantially expanded) staff of the

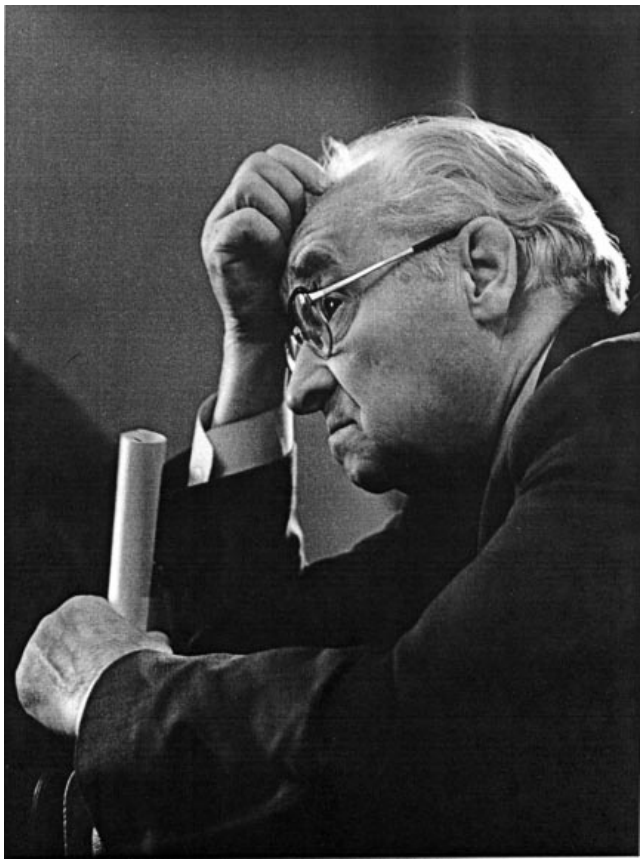


It is clearer if seen from the height of the antenna (Medvezh'i lakes). Left to right: Kotel'nikov, M V Keldysh, A F Bogomolov.

ORT Chair. It did not take long time for the sector to become one of the leading organizations of the missile and space industry and was later renamed OKB MEI. It was headed by Kotel'nikov. Under his guidance a large-scale research, design, and development program was implemented to develop integrated radio engineering systems on different scales and to vigorously expand the missile and space industry. In a number of cases the Special Sector took on itself the problems that an industry rejected as too difficult or problematic. Kotel'nikov in his capacity of Chief Designer of the Special Sector was a member of the interdepartmental Council of Chief Designers, headed by Sergei P Korolev. The presence of every chief at every systems test, not to mention a missile launch, was a *conditio sine qua non* — "to have someone responsible in case something went wrong". At the time when the Missile and Space Program was in its infancy, life at the 'raketodromes' (proving grounds) was quite rough. Like many other expert technicians, those of the Special Sector lived in mud-huts excavated right in the steppe, not far from the missile testing grounds. Bosses were allotted 'more comfortable' quarters — in some sort of a small house close to the Kapustin Yar railway station, or in railway carriages of a train parked in a dead end. They would be taken to the testing area by cars. Kotel'nikov preferred to live in a mud-hut with the 'crowd', and would use a joke to deflect suggestions to move to 'bosses apartments': "Too far to drive to the workplace". Missiles were launched around the year, regardless of the weather — in terrible heat, in the rain, in freezing weather, during a snowfall... Everybody worked with great enthusiasm, notwithstanding the difficulties. Note that Kotel'nikov continued to be the Dean of RTF, and continued to carry out his duties at the ORT Chair, as its Head and lecturer.

Kotel'nikov headed the Special Sector until 1955 when he handed the 'reins of government' to his highly talented pupil A F Bogomolov (a future academician). However, his connection to the Special Sector (under a new name OKB MEI) was not broken. In 1983 – 1984, the two bodies built by him, IRE AN SSSR and OKB MEI, worked successfully 'hand in hand' throughout the entire stage of preparation and implementation of the brilliant project that he thought up and headed — the radio-cartographic scanning of the surface of Venus. The experiment proved a success and produced unique and spectacular results!

The USSR Academy of Sciences. The Institute of Radioengineering and Electronics. In 1953, in late summer or early autumn (Kotel'nikov was not sure about the date), Academician Aksel' Ivanovich Berg invited Kotel'nikov to the Central Research Institute of Radio Engineering (TsNIRTI), which he was Director of at the time. Berg told him that an idea was being discussed of establishing within the Academy an institute that would have for its main task theoretical studies and engineering in the field of radio engineering and electronics, and asked for help in composing consitutative documents. Kotel'nikov was only too happy to help. He felt great respect toward Berg. They had known each other since way back. In pre-World-War years (1933 – 1937) Berg, then Head of the Research Institute of Naval Communications, visited NIIS NKS and read a report to the staff. He remembered a young engineer Kotel'nikov who was very active and asked well-informed questions, of the sort we say hit the bull's-eye. After the report, the two continued to discuss for a long time various problems in radio engineering. The paths of the two 'radio men' kept crossing.



Auditioning interesting report.

Immediately after the war they were organizing the A S Popov Society, followed each other as Chairman of the Organizing Bureau of the Society, worked together on the State Commission on assessing the work of the Marfino Laboratory and the equipment it developed (1950 and 1952).

Kotel'nikov arrived at TsNIRTI in the evenings and 'composed' documents in Berg's study. The academician himself was too busy. The relevant directions and other constituent documents for the institute, which was to have the title 'The Institute of Radioengineering and Electronics', were soon prepared, debated and approved. All the resolutions involved were passed in September 1953 and the IRE AN SSSR had 'arrived'. Academician Berg was given an assignment as its Director. The same autumn Kotel'nikov was invited by the Academician-Secretary of the Division of Technical Sciences B A Vvedensky and was informed: "We wish to propose your candidature for Full Member of the Academy, any objections?" Much surprised, Kotel'nikov gave his agreement and Vvedensky added that if Kotel'nikov was elected, the Division planned to offer him the directorship of the Institute of Automation and Telemechanics, where the Academy faced problems with its director. Kotel'nikov was indeed elected Full Member of the USSR Academy of Sciences in October 1953 (bypassing the first stage of Corresponding Membership). It appears that his candidature was seconded by Academicians Berg and Vvedensky. (Kotel'nikov took no part in the election campaign.) Immediately after the election Berg suggested that the new academician start the process of creating the just enacted IRE, in the position of the First Deputy to its Director. Kotel'nikov agreed. To create such an Institute! Marvelous!

In November 1953, Kotel'nikov was transferred to his new position of Vice Director of IRE, which still existed on paper only, and became its Director in 1954. (Berg had already been promoted to Deputy Minister of the USSR Ministry of Defense in 1953.) Berg was known as an incomparable strategist and kept his plans well hidden until the right time. He jokingly remarked some time later that he could already discern in Kotel'nikov the directorship of the Institute. Enormous work has begun on the establishment of the institute: the selection of personnel, definition of the subjects of research, searching of premises for the institute, their putting in order, setting up the design bureau, etc. In a very brief space of time, IRE AN SSSR turned into the leading institute in the field of radiophysics, radio engineering and electronics not only in this country but also the world over.

Kotel'nikov was not only Director of the Institute but at the same time the initiator, scientific leader and immediate executor of numerous scientific and technical projects whose realization yielded unique scientific results. All those who collaborated with Kotel'nikov noted his exceptional erudition, scientific intuition, ability of inquiring into the heart of the matter, and the possession of enormous capacity for work.

Vladimir Aleksandrovich Kotel'nikov was forty five years of age at the instant of his election as Full Member of the USSR Academy of Sciences and the onset of establishing IRE. Next fifty one years of his active and successful creative life were ahead of him.

References

1. Putyata T V et al. *Aleksandr Petrovich Kotel'nikov. 1865 – 1944* (Moscow: Nauka, 1968)
2. Kotel'nikov V A "O propusknoi sposobnosti 'efira' i provoloki v elektrosvyazi" ("On the transmission capacity of 'ether' and wire in electric communications"), in *Vsesoyuznyi Energeticheskii Komitet. Materialy k I Vsesoyuznomu S'ezdu po Voprosam Tekhnicheskoi Rekonstruktsii Dela Svyazi i Razvitiya Slabotochnoi Promyshlennosti. Po Radiosektsii* (The All-Union Energy Committee. Materials for the 1st All-Union Congress on the Technical Reconstruction of Communication Facilities and Progress in the Low-Currents Industry. At Radio Section) (Moscow: Upravlenie Svyazi RKKA, 1933) pp. 1 – 19
3. Vitushkin A G, in *Matematicheskie Sobytiya XX Veka* (Events in Mathematics in the XXth Century) (Editorial Commission: V I Arnold et al.) (Moscow: FAZIS, 2003); "Nikolai Nikolaevich Bogolyubov: mathematician by the grace of God", in *Mathematical Events of the Twentieth Century* (Eds A A Bolibruch, Yu S Osipov, Ya G Sinai) (Berlin: Springer; Moscow: PHAZIS, 2006)
4. Sloane N J A, Wyner A D (Eds) *Claude Elwood Shannon: Collected Papers* (New York: IEEE Press, 1993) Pt. A [Translated into Russian (Moscow: IL, 1963)]
5. Abdul J *Proc. IEEE* **65** 1585 (1967)
6. Lüke H D *IEEE Commun. Mag.* **37** (4) 106 (1999)
7. Kotel'nikov V A *Nauchno-tekh. Sbornik Leningradskogo Elektrotekh. Inst. Svyazi* (11) (1936)
8. Kotel'nikov V A *Nauchno-tekh. Sbornik Leningradskogo Elektrotekh. Inst. Svyazi* (14) (1936)
9. Bykhovskii M A, in *Tvortsy Rossiiskoi Radiotekhniki. Zhizn' i Vklad v Mirovuyu Nauku* (Creators of Radio Engineering in Russia. Life and Contribution to the World Science) (Ser. Istoriya Elektrosvyazi i Radiotekhniki (History of Electric Communications and Radio Engineering Series), Issue 3, Ed. by M A Bykhovskii) (Moscow: Eko-Trendz, 2005) p. 67
10. Dudley H *Bell Labs Record* **XI** 122 (1939)
11. Andreev N N et al. *Radiotekh.* (8) 8 (1998)
12. Udalov N N *Radiotekh.* (11) 37 (1998)
13. Zinov'ev A L *Elektrosvyaz'* (9) 3 (1998)
14. Sokolov A V, Filippov L I *Radiotekh.* (8) 48 (1998)
15. Fleishman B S *Konstruktivnye Metody Optimal'nogo Kodirovaniya dlya Kanalov s Shumami* (Design Methods of Optimal Encoding for Noisy Channels) (Moscow: Izd. AN SSSR, 1963)
16. Kotel'nikov V A, in *Radiotekhnicheskii Sbornik* (Moscow – Leningrad: Gosenergoizdat, 1947)
17. Kotel'nikov V A *Teoriya Potentsial'noi Pomekhoustoichivosti* (The Theory of Potential Noise Immunity) (Moscow-Leningrad: Gosenergoizdat, 1956); reprint (Moscow: Radio i Svyaz', 1998) [Translated into English (New York: McGraw-Hill, 1960)]
18. Kalachev K F *V Kruge Tret'em: Vospominaniya i Razmyshleniya o Rabote Marfinskoi Laboratorii v 1948 – 1951 Godakh* (The Third Circle: Reminiscences and Reflections on the Work of the Marfino Laboratory in 1948 – 1951) (Moscow: Mashmir, 2001)

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

DOI: 10.1070/PU2006v049n07ABEH006160

Supplement

All-Union Energy Committee

Materials prepared for the 1st All-Union Congress
on the Technical Reconstruction
of Communication Facilities and Progress
in the Low-Currents Industry

For consideration at the Radio Section

On the transmission capacity of 'ether' and wire in electric communications *

V A Kotel'nikov, Engineer

Both in radio and in wire communication technology, every transmission requires a certain frequency range rather than some single frequency. This has the effect that only a limited number of radio stations (broadcasting different programs) can operate simultaneously. Along one pair of wires it is also impossible to transfer at once more than a certain number of transmissions, because the frequency band of one transmission should not overlap with the band of another one, for such an overlap would lead to mutual interference.

To increase the transmission capacity of 'ether' and wire (this would be of enormous practical significance, especially in view of the rapid development of radio engineering and such broadcasts as television) necessitates narrowing somehow the frequency range required for a given broadcast, without degrading its quality, or inventing a way of separating broadcasts not on the basis of frequency, as has been done up till now, but on some other basis. [1]

Presently, no contrivances in these realms have made it possible to increase, even theoretically, the transmission

* The paper of 1933 is reproduced from the edition published on the 70th anniversary of the Kotel'nikov theorem and the 95th birthday of Vladimir Aleksandrovich Kotel'nikov by the Institute of Radioengineering and Electronics of the Moscow Power Engineering Institute (Technical University) in 2003 under the supervision of its Director N N Udalov. Minor alterations have been made in the reproduction: formulas have been written in the format adopted by *Phys.-Usp.*, the page numbering of footnotes replaced with a continuous one, the orthography and the syntax brought into agreement with modern standards. The author's style has been retained.

[1] True, this can sometimes be effected with directional antennas, but here we will consider only the case when this cannot be done with antennas for some reason or other.

capacity of 'ether' and wire to a greater degree than is allowed by transmitting 'on one sideband'.

This brings up the question of whether this can be done at all. Or is it that all attempts in this area will be equivalent to attempts to construct a 'perpetuum mobile'?

This radio engineering problem is topical nowadays in view of the 'tightness in the ether', which is growing year after year. It is important to now elucidate this question in connection with the planning of scientific research, because in the planning it is vital to know what is possible and what is absolutely impossible to do, so as to mount efforts in the right direction.

In the present work I tackle this problem and prove that there exists a quite specific, minimally necessary frequency band for television and the transmission of images with all their half-shadows, as well as for telephone communication. This frequency band can in no way be narrowed without degrading the rate and quality of transmission. It is also proven that for these broadcasts there is no way of increasing the transmission capacity of either 'ether' or wire by applying nonfrequency selection of any kind or any other means (with the exception, of course, of the selection by directions employing directional antennas). The maximum achievable transmission capacity for these broadcasts may be obtained in the transmission 'on one sideband', and basically this is quite attainable at present.

For such transmissions as telegraphy or the image transmission and television without penumbra, etc., in which the transmitted object may assume only definite values known in advance and not vary continuously, it is shown that the requisite frequency band can be reduced by an arbitrarily large factor without impairing the quality of transmission or its rate, this being achieved by increasing the power and complexity of the equipment. One method for such a frequency band reduction is pointed out in this paper, and it is shown what increase in power is required for this purpose.

Therefore, no theoretical limit is imposed on the transmission capacity of 'ether' and wire for broadcasts of this kind; the problem is only one of technical implementation.

In the present work, the above propositions are proven without reference to a broadcast technique on the following basis: in all kinds of electric communication, the transmitter can send and the receiver can bring in only signals being some function of time which cannot be absolutely arbitrary, because the frequencies it consists of and may be resolved into must be confined to certain ranges. In a radio broadcasting, this function is the current intensity of the transmitting antenna, which is perceived by the receiver more or less accurately; in a wire communication, this is the electromotive force at the origin of the line. In either case, the transmitted functions would comprise frequencies from a limited range because, first, very high and very low frequencies would not reach the receiver due to propagation conditions and, second, ordinarily the frequencies that are beyond a prescribed narrow range are purposely suppressed, so as not to be a hindrance to other broadcasts.

The inevitability of transmission with the help of time functions that contain only a limited frequency range entails, as shown below, quite a definite restriction on the transmission capacity.

To prove the stated propositions, we address ourselves to the study of functions consisting of a definite frequency range.

Functions consisting of frequencies from 0 to f_1

Theorem I. Any function $F(t)$ consisting of frequencies from 0 to f_1 cycles per second can be represented as a series

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

where k is an integer, $\omega_1 = 2\pi f_1$, and D_k are constants depending on $F(t)$.

And vice versa, any function $F(t)$ represented as a series (1) consists of only the frequencies from 0 to f_1 cycles per second.

Proof. Any function $F(t)$ subject to the Dirichlet conditions (a finite number of maxima, minima, and discontinuity points on any finite segment) and integrable between the limits from $-\infty$ to $+\infty$, which is always the case in electrical engineering, can be represented as a Fourier integral [2, 3]:

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

i.e., as the sum of an infinite number of sinusoidal oscillations with frequencies from 0 to ∞ and the frequency-dependent amplitudes $C(\omega)$ and $S(\omega)$. In this case, one obtains

$$\begin{aligned} C(\omega) &= \frac{1}{\pi} \int_{-\infty}^{+\infty} F(t) \cos \omega t \, \mathrm{d}t\,, \\ S(\omega) &= \frac{1}{\pi} \int_{-\infty}^{+\infty} F(t) \sin \omega t \, \mathrm{d}t\,. \end{aligned} \tag{3}$$

In our case, when $F(t)$ consists of only the frequencies from 0 to f_1, evidently one finds

$$\begin{aligned} C(\omega) &= 0\,, \\ S(\omega) &= 0 \end{aligned}$$

for

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

and $F(t)$ can therefore be represented according to Eqn (2) as follows:

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

The functions $C(\omega)$ and $S(\omega)$, like any other ones, may always be represented as Fourier series on the interval

$$0 < \omega < \omega_1\,.$$

In this case, these series may, at our will, consist of only cosines or only sines, provided the double length of the interval is taken as the period, i.e., $2\omega_1$ [4]. Therefore, one has

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

[2] See, for instance, V I Smirnov, *Course of Higher Mathematics Vol. II*, 1931 publ., p. 427.

[3] In what follows we also consider only the functions satisfying the Dirichlet conditions.

[4] See, for instance, V I Smirnov, *Course of Higher Mathematics Vol. II*, 1931 publ., p. 385.

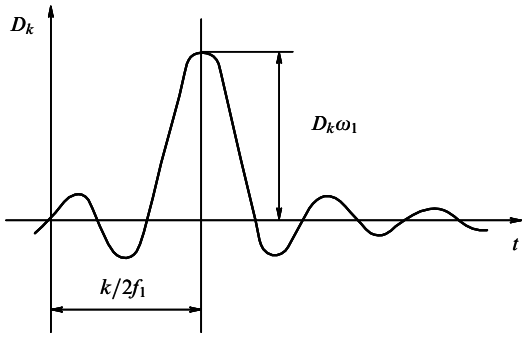


Figure 1.

and

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

We introduce the following notation

$$\begin{aligned} D_k &= \frac{A_k + B_k}{2} \,, \\ D_{-k} &= \frac{A_k - B_k}{2} \,; \end{aligned} \tag{6}$$

formulas (5a) and (5b) can then be rewritten as

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

On substituting expressions (7) into formula (4), on some rearrangements and integration (see Appendix I) we obtain Eqn (1), i.e., prove the first part of Theorem I.

To prove the second part of the theorem, we consider the special case of $F(t)$ when the spectrum of its constituent frequencies falls in the range 0 to f_1 and is expressed in the form of Eqn (7) in which all D_k, with the exception of one, are equal to zero. This $F(t)$ will evidently consist of a single term of series (1). And vice versa: when $F(t)$ consists of a single, arbitrary term of series (1), its entire spectrum is confined to the range 0 to f_1. And therefore the sum of any individual terms of series (1), i.e., series (1) itself, will consist of frequencies confined to the range 0 to f_1, which proves the statement.

All terms of series (1) are similar and differ by only the shift in time and the factors D_k. One of the terms with a subscript k is plotted in Fig. 1; it peaks for $t = k/(2f_1)$ and possesses a gradually decreasing amplitude in both directions.

Theorem II. Any function $F(t)$ consisting of frequencies from 0 to f_1 can be continuously transmitted with an arbitrary accuracy with the aid of numbers which follow one after another $1/(2f_1)$ seconds apart. Indeed, by measuring the value of $F(t)$ for $t = n/(2f_1)$ (n is an integer), we will obtain

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

Since all terms of series (1) vanish for this value of t, with the exception of the term with $k = n$, which, as is easily obtained by removing ambiguity, is equal to $D_n\,\omega_1$, in every $1/(2f_1)$th second we will be able to learn the next D_k. By transmitting these D_k one after another at $1/(2f_1)$-second intervals, from them we will be able, according to Eqn (1), to reconstruct $F(t)$ with an arbitrary accuracy.

Theorem III. It is possible to continuously and uniformly transmit arbitrary numbers D_k with a rate of N numbers per second by means of a function $F(t)$ with arbitrarily small items at frequencies greater than $f_1 = N/2$.

Indeed, on receiving every number we will construct the function $F_k(t)$ such that

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

and transmit their sum $F(t)$. Should be $T = \infty$, the resultant function $F(t)$ would consist only of frequencies lower than f_1, because in this case we would have obtained the series (1), but unfortunately such infinite series of terms are impossible to construct, and we will therefore restrict ourselves to finite T. We will prove the following: the longer T, the lower are the amplitudes at frequencies $f > f_1$, and these amplitudes can be made as small as desired. To this end, we will find the amplitudes $C(\omega)$ and $S(\omega)$ for function (9) by substituting it into Eqn (3). We obtain

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

Upon integration (see Appendix II) we will have

$$\begin{aligned} C(\omega) &= \frac{D_k}{\pi} \cos \omega \, \frac{k}{2f_1} \bigl[\mathrm{Si}\, T(\omega + \omega_1) - \mathrm{Si}\, T(\omega - \omega_1)\bigr] \,, \\ S(\omega) &= \frac{D_k}{\pi} \sin \omega \, \frac{k}{2f_1} \bigl[\mathrm{Si}\, T(\omega + \omega_1) - \mathrm{Si}\, T(\omega - \omega_1)\bigr] \,. \end{aligned} \tag{11}$$

In this expression, Si denotes integral sine, i.e., the function

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

The values of this function were calculated and tabulated [5], and it is graphically displayed in Fig. 2.

As may be seen from Fig. 2, $\mathrm{Si}\, x$ tends to $\pm\pi/2$ as $x \to \pm\infty$.

We now consider the value of the expression in square brackets in expression (11). Its graphic representation for $T = 3/(2f_1)$ is given in Fig. 3a, for $T = 6/(2f_1)$ in Fig. 3b, for $T = 24/(2f_1)$ in Fig. 3c, and for $T = \infty$ in Fig. 3d.

As is evident from these plots, with increasing T the expression in square brackets in expression (11) tends to the

[5] See, for instance, E Jahnke und F Emde, *Funktionentafeln mit Formeln und Kurven.*

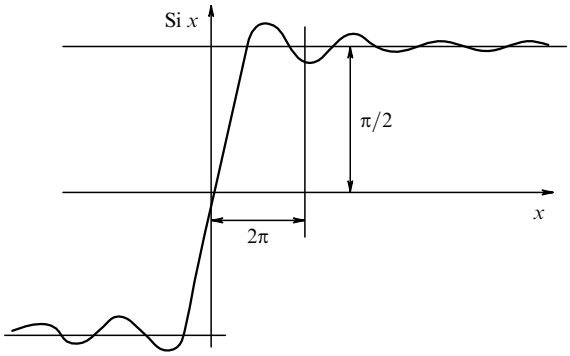


Figure 2.

limits in Fig. 3d, namely

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

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

This is also clear directly from expression (11): with increasing T, it is as if the scale of ω increases and Si becomes a rapidly decaying function.

Therefore, the resultant sum of $F_k(t)$ will possess arbitrarily low amplitudes at frequencies $f > f_1$ provided T is taken sufficiently long.

On receiving the $F(t)$ function it is easy to recover the D_k numbers transmitted: at $t = n/(2f_1)$ all terms vanish with the exception of the term for which $k = n$, which is equal to $D_n\,\omega$.

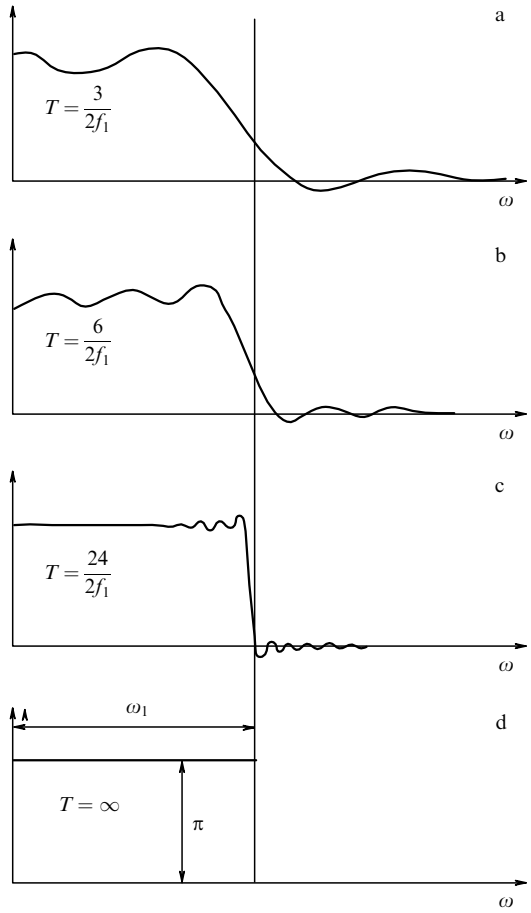


Figure 3.

And so

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

Therefore, from our function we will be able, by measuring its value at $t = k/(2f_1)$, to recover every $t = 1/(2f_1)$th second the value of a new D_k and to obtain $N = 2f_1$ transmitted numbers per second, which proves the statement.

Functions consisting of frequencies from f_1 to f_2

Let us prove a theorem.

Theorem IV. Any function $F(t)$ consisting of frequencies from f_1 to f_2 may be represented as

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

where $\omega_1 = 2\pi f_1$, $\omega_2 = 2\pi f_2$, while $F_1(t)$ and $F_2(t)$ are some functions consisting of frequencies from 0 to $f = (f_2 - f_1)/2$. And vice versa: if $F_1(t)$ and $F_2(t)$ in Eqn (13) are arbitrary functions consisting of frequencies from 0 to $f = (f_2 - f_1)/2$, then $F(t)$ consists of frequencies from f_1 to f_2.

If $F(t)$ consists only of frequencies from f_1 to f_2, clearly $C(\omega)$ and $S(\omega)$ for this function may then be represented as follows:

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

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

or, introducing once again the notation

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

we arrive at

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

$$\text{for} \quad \omega_1 < \omega < \omega_2$$

and

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

By substituting Eqn (14) into Eqn (2), upon integration and some rearrangement (see Appendix III) we obtain

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

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

or, denoting

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

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

and taking into account that the spectra of $F_1(t)$ and $F_2(t)$ must, according to Theorem I, necessarily consist of frequencies from 0 to $f=(f_2-f_1)/2$, because series (16) and (17) differ from series (1) in only the notation, the first part of Theorem IV may be considered proven.

Since any functions $F_1(t)$ and $F_2(t)$ consisting of frequencies from 0 to $f=(f_2-f_1)/2$ may, according to Theorem I, be represented by series (16) and (17) and since no constraints are imposed on the coefficients D_k that appear in these series, evidently the second part of Theorem IV is also valid.

We now prove two theorems which are a generalization of Theorems II and III.

Theorem V. Any function $F(t)$ which consists of frequencies from f_1 to f_2 may be continuously transmitted with an arbitrary accuracy by means of numbers transmitted one after another at $1/[2(f_2-f_1)]$-second intervals.

Indeed, for $t=k/(f_2+f_1)$ (k is an integer) we obtain according to formula (13):

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

because for this value of t the cosine is equal to unity, and the sine to zero. When $t=(k+1/2)/(f_2+f_1)$, by the same reasoning we obtain

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

Therefore, every $1/(f_2+f_1)$th second we will be able to learn the values of $F_1(t)$ and $F_2(t)$ one by one. From these values we will be able to reproduce the $F_1(t)$ and $F_2(t)$ functions themselves, because from so frequent a succession of numbers it is, according to Theorem II, possible to reproduce the functions consisting of frequencies from 0 to $(f_2+f_1)/2$, whereas the $F_1(t)$ and $F_2(t)$ functions consist only of frequencies from 0 to $(f_2-f_1)/2$.

Each of the functions thus obtained may, as a function consisting of frequencies from 0 to $(f_2-f_1)/2$, be transmitted, according to Theorem II, by numbers that follow one after another $1/(f_2-f_1)$ seconds apart; while evidently these two functions may be simultaneously transmitted by numbers that follow one after another $1/[2\,(f_2-f_1)]$ seconds apart. By first reconstructing $F_1(t)$ and $F_2(t)$ from these numbers, we will then be able to reconstruct $F(t)$ itself by formula (13).

Theorem VI. It is possible to continuously and uniformly transmit arbitrary numbers D_k with a rate N numbers per second by means of a function $F(t)$ that possesses arbitrarily small terms at frequencies $f>f_2$ and $f<f_1$ (i.e., is practically devoid of them) if

$$N = 2(f_2-f_1)\,. \tag{19}$$

Indeed, according to Theorem III we may transmit N numbers per second using two functions $F_1(t)$ and $F_2(t)$, each having arbitrarily small terms at frequencies above $(f_2-f_1)/2$.

The same functions may be continuously transmitted by the function $F(t)$ with arbitrarily small terms at frequencies $f>f_2$ and $f<f_1$. Indeed, from the functions $F_1(t)$ and $F_2(t)$ we will, according to Eqn (13), obtain $F(t)$, by the transmission of which we will be able, as noted above, to reconstruct $F_1(t)$ and $F_2(t)$ from it and thereby the numbers being transmitted.

To prove the last theorem, which states that there is no way to transmit infinitely much with the aid of a function comprising a limited frequency range, we will prove the following lemma.

Lemma. There is no way to transmit N arbitrary numbers with the aid of M numbers if

$$M < N\,. \tag{20}$$

Let us assume that this is possible to do.

Then, it is apparent that M numbers $m_1,\ldots,m_M$ are some functions of N numbers $n_1,\ldots,n_N$, namely

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

and we evidently should, with only the knowledge of the M numbers $m_1,\ldots,m_M$, and, of course, of the functions $\varphi_1,\ldots,\varphi_M$, manage to recover the numbers $n_1,\ldots,n_N$ from them.

But this is equivalent to the solution of M equations (21) with N unknown quantities, which is impossible to do when the number of equations is smaller than the number of unknowns, i.e., when inequality (20) holds.

Theorem VII. It is possible to continuously transmit arbitrary numbers which uniformly follow one after another with a rate of N numbers per second and M arbitrary functions $F_1(t),\ldots,F_M(t)$ with frequency ranges of widths $\Delta f_1,\ldots,\Delta f_M$ by means of numbers which continuously follow one after another with a rate of N' numbers per second and by means of M' functions $F_1'(t),\ldots,F_{M'}'(t)$ with the frequency ranges $\Delta f_1',\ldots,\Delta f_{M'}'$ if

$$N + 2\sum_1^M \Delta f_k \leqslant N' + 2\sum_1^{M'} \Delta f_k'\,. \tag{22}$$

And this cannot be done by any means when

$$N + 2\sum_1^M \Delta f_k > N' + 2\sum_1^{M'} \Delta f_k'\,. \tag{23}$$

The first part of this theorem is proved on the basis of Theorems V and VI.

Indeed, by virtue of Theorem V we can transmit our N numbers per second and M curves by means of P numbers per

second when

$$P = N + 2\sum_{1}^{M} \Delta f_k \,. \tag{24}$$

And these P numbers per second may be partly transmitted by means of N' numbers per second and partly by means of the curves $F_1'(t), \ldots, F_{M'}'(t)$ on the strength of Theorem VI if equality (22) is correct.

The second part of the theorem will be proved by contradiction, on the basis of the lemma.

Assume that it is required to transmit P arbitrary numbers per second; according to Theorem VI this can be done by transmitting N numbers per second and the functions $F_1(t), \ldots, F_M(t)$ with the frequency ranges $\Delta f_1, \ldots, \Delta f_M$ if equality (24) is valid.

Were the second part of the theorem not valid, these functions and numbers would be possible to transmit by means of functions $F_1'(t), \ldots, F_{M'}'(t)$ and N' numbers per second. But the latter numbers and functions may, according to Theorem V, be transmitted by means of P' numbers per second if

$$P' = N' + 2\sum_{1}^{M'} \Delta f_k' \,. \tag{25}$$

In other words, we would be able to continuously transmit P numbers per second by means of P' numbers per second, although according to equalities (24) and (25) and inequality (23) we have

$$P > P' \,.$$

Therefore, the assumption that the second part of Theorem VII is invalid leads us to an inadmissible, according to the lemma proven, result.

Transmission capacity in the telephone communication

A conversation, music, and other objects of telephone communication are arbitrary functions of time, which comprise a frequency spectrum whose width is quite definite and depends on how adequately we wish to transmit the sound.

When transmitting this function by wire or by radio, we transform it into another time function which is actually transmitted. In this case, the latter function should necessarily, according to Theorem VII, possess a frequency spectrum of width not smaller than the sound frequency band we would like to transmit.

Therefore, a continuous telephone communication cannot occupy in ether or wire a narrower frequency range than the width of the sound frequency spectrum required for a given broadcast. This is true irrespective of the method of transmission, and it is impossible to contrive a method that would enable occupying a narrower frequency range for continuous transmission.

As is well known, such a minimal frequency spectrum may be afforded even at present by one sideband transmission.

The reservation about 'continuous transmission' is of paramount importance, because it is possible to transmit some sounds, say music, off and on and thereby occupy a narrower frequency range than the width of the sound spectrum we would receive in this case. To do this it would suffice first to record the transmitted music on phonograph records and then to broadcast from them by rotating them, say, two times slower than during the recording. Then, all frequencies will be two times lower than the regular ones and we will manage to occupy a two-fold narrower frequency range during transmission. Such a broadcast may also be reconstructed by means of a phonograph. Clearly, such a broadcast cannot increase the transmission capacity, because the 'ether' or wire will be occupied all the time, while the broadcast will proceed interrupted.

This is not at variance with Theorem VII, either, for its formulation contains reservations: there is no way of transmitting an 'arbitrary function' and of doing this 'continuously', while in the above broadcast we can either transmit off and on an arbitrary function or transmit uninterruptedly a function not quite arbitrary but possessing breaks known beforehand.

From Theorem VII it also follows that the transmission capacity cannot be increased by employing some selections of a nonfrequency nature (excluding directional antennas) or something else of the kind.

Indeed, if this could be done, then by applying these methods it would be possible to transmit from one place to another, say, n telephone broadcasts simultaneously with the frequency spectra of width Δf each, occupying for this purpose a frequency range narrower than $n\Delta f$.

However, in the course of this transmission the field intensities (or currents in the wire) of different broadcasts would be mixed up into some single function of time with the frequency spectra narrower than $n\Delta f$, which will be perceived by receivers. The result would be that we have managed to transfer n time functions with the frequency ranges of width Δf by means of one function with a frequency range narrower than $n\Delta f$, which is strictly prohibited by Theorem VII.

It is clear from the aforesaid that the ether transmission capacity for a telephone may be increased only by resorting to directional antennas or by broadening the operating frequency range through the use of ultrashort (metric) waves.

Transmission of images and television with all half-shadows

In the transmission of images and in television it is required to transfer the degree of blackness of N elements per second, which is equivalent to the transmission of arbitrary numbers with a rate of N numbers per second. If we want to do this by means of a time function, as is always done, according to Theorem VII it has to occupy a frequency range not narrower than $N/2$ periods per second. Therefore, it is immediately evident that in this case, too, the frequency band cannot be reduced more than is allowed by one sideband transmission. True, even its realization can encounter serious technical difficulties due to phase distortions which may occur during such a transmission.

The frequency band cannot be narrowed by means of some 'grouped image scan' (scanning not over individual elements), either, because with this scan, too, one will have to transfer, although by some other means, the degree of blackening of the same N elements per second, i.e., N arbitrary numbers per second, which is impossible to do with a decreased frequency range.

In this case, too, nonfrequency selection techniques (excluding directional antennas) cannot be helpful for the same reasons as in the telephone communication.

Telegraph transmission and image transmission without half-shadows or with their limited number

In telegraph transmission, as well in the transmission of images without half-shadows or with quite definite preas-

Table

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

signed half-shadows, once again we are dealing with the transmission of a kind of N elements per second, which is equivalent to the transmission of N numbers per second. However, the number of these elements and hence the magnitude of numbers may assume quite definite preassigned values rather than be quite arbitrary. That is why the above-deduced theorems are not directly applicable to these transmissions, for they deal with the transmission of arbitrary numbers which are absolutely unknown beforehand.

True, it is possible to narrow the frequency range required for these transmissions by an arbitrarily large factor and hence increase, at least theoretically, the transmission capacity also by as many times as desired.

To do this we may proceed as follows: we are to transmit, say, with a rate of N elements per second the elements which may assume the values 0 or 1 and in doing this occupy a frequency range of a width of $N/4$ (in lieu of $N/2$ by Theorem VII). For this purpose, we will transmit two such elements by means of one element (or number), for instance, according to the following table, in which column I gives the value of the first element, column II the value of the second, and column III the value of the element intended for their transmission.

In this way we will be able to transmit N two-valued elements per second by means of $N/2$ four-valued elements per second, which can, according to Theorem VII, be transmitted employing a frequency range of a width of $N/4$.

In practice, this replacement of two elements with one may be effected, for instance, by the scheme of Fig. 4, where F_1 and F_2 are two photoelectric cells or two telegraph apparatuses. In this case, F_1 actuates modulator M_1 which sends into the line an amplitude equal to unity, while F_2 operates with modulator M_2 which sends an amplitude equal to 3. In the simultaneous operation of F_1 and F_2, both modulators are actuated and, since they are engaged in opposition, an amplitude equal to 2 is sent. During reception, the signal is fed to three receivers. The first, R_1, is actuated by the amplitude 1, the second, R_2, by the amplitude 2, and the third, R_3, by the amplitude 3. The first receiver R_1 actuates L_1, the second one actuates L_2, and the third one, on arrival of the amplitude equal to 3, denies access to L_1 for the first receiver. By means of this circuit we will obtain the above narrowing of the frequency band.

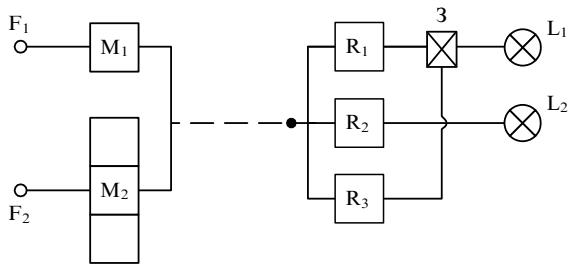


Figure 4.

In the course of such a transmission it is required to distinguish four gradations of the signals under detection instead of two, which evidently generates the need for raising the transmitter power by a factor of $3^2 = 9$ in comparison with conventional transmission.

In a similar way, it is also possible to narrow the frequency band by a factor n by transmitting n elements that may assume two values each with the use of a single element which should evidently be able to assume 2^n values (in accordance with the number of combinations of n elements that may assume two values). Such a transmission calls for a $(2^n - 1)^2$-fold rise in power.

In the transmission of images with a certain number of preassigned half-shadows, every element should be able to assume several, say m (in this case, $m > 2$), values. To narrow the frequency band by a factor n in this transmission, it is possible to replace n transmitted elements with one which should be able to assume m^n values (in accordance with the number of possible combinations of n elements possessing m possible values each). In this case, evidently, the power is to be raised by a factor of $[(m^n - 1)^2]/[(m - 1)^2]$.

One can see that such-like narrowing of the frequency band calls for an enormous increase in power.

Furthermore, the methods described above would fail in transmission at short wavelengths due to fading.

For wire communication, this method of frequency band narrowing may be of practical significance even now, because the powers required in this case are small and there are no fast changes in reception strength.

Appendix I

We substitute expression (7) in Eqn (4) to obtain

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

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

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

or, upon integrating and replacing ω_1 with $2\pi f_1$ in parentheses, we arrive at

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

Appendix II

In the expression

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

we make a substitution

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

then

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

In passing through the zero, the integrand of the second integral changes its sign, while retaining its magnitude, and therefore the second integral is equal to zero.

With $-u$ in place of u, the integrand of the first integral remain invariable, and therefore this integral may be taken between the limits 0 and T and then multiplied by a factor of two. So, one finds

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

or

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

In the first integral we make the following change

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

and in the second one

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

to obtain

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

The integrals in square brackets cannot be taken. Clearly, they are some functions of the upper limit. These functions are commonly referred to as integral sines. On introducing this notion we obtain

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

Doing precisely the same operations on $S(\omega)$, we arrive at Eqn (11).

Appendix III

We substitute equations (14) into Eqn (2) to obtain

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

The limits were taken to be equal to ω_1 and ω_2, because

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

for

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

Upon trigonometric rearrangement, one finds

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

By replacing the difference of sines with a product and performing simplifications, we obtain

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

or, grouping together the terms with even and odd k, we arrive at Eqn (15).

Conclusions

(1) In view of the present-day 'tightness in the ether' and in connection with the further rapid progress of radio engineering, especially with the development of short-wavelength telephone communication and image transmission, the task of searching for ways to increase the transmission capacity of 'ether' should be set before research institutes as a burning problem.

The problem of increasing the transmission capacity of wire is also of great economic significance and, therefore, should also be brought under study.

(2) Since there are no ways to increase the transmission capacity of 'ether' or wire during image transmission and telephone communication (for instance, by narrowing the frequency bands of separate broadcasts or by using some methods to separate the broadcasts with overlapping frequencies, etc.) to a greater degree than is allowed by the ordinary transmission with one sideband, all attempts in this area are unrealizable and should be abandoned.

(3) For telegraphy and image transmission without half-shadows or with their limited number, the transmission capacities may theoretically be made as high as desired, but this is associated with a major increase in power and complicated equipment. It is therefore believed that in the near future this frequency band narrowing may find use only in wire communications, where this problem should be explored.

(4) As regards the first category of transmissions (telephone and the transfer of images with half-shadows), all efforts should go into the development of methods of reception and transmission on one sideband as the methods which permit the most efficient use of 'ether' and wire.

The purpose of this development is to improve and simplify the equipment, which is quite complicated at the present time.

(5) An investigation should be made into the problem of increasing the transmission capacity of 'ether' by means of directional antennas, both receiving and transmitting antennas.

(6) The operating frequency range in 'ether' should be broadened by employing, where possible, ultrashort waves and by studying this frequency range.

(7) There is a need to examine the feasibility of improving the frequency stability of radio stations, which will allow a greater compactness in 'ether'.

PACS numbers: **89.70.+c**, 95.85.Bh, 96.30.Ea
DOI: 10.1070/PU2006v049n07ABEH006048

V A Kotel'nikov and his role in the development of radiophysics and radio engineering

N A Armand

1. Introduction

It is not an easy task to write about V A Kotel'nikov's role in the development of radiophysics and radio engineering. This difficulty stems both from the fact that he was involved in the making and development of a diversity of areas and from the scientific results, part of which were obtained more than 70 years ago and which appear 'obvious' from the modern point of view. The difficulty is also related to the fact that Kotel'nikov was not a 'publication-lover'. In particular, his famous theorem was never published properly at all, and his classic work on potential noise immunity was not published until 1956, ten years after its completion.

2. Theorem

In 1932–1933, the 25-year-old engineer Kotel'nikov conceived the idea of whether it is possible to transmit without distortions a signal in a frequency band which is narrower than is allowed by transmission 'on one sideband'. In the modern view, this signifies the possibility for distortion-free transmission of signals through a channel whose spectral transmission capacity is narrower than the spectral width of the signal. To us, this sounds absurd, but at that time (1933), when the problems of spectral filtration were not quite clear to engineers, such a formulation of the problem appeared reasonable. In this connection, mention should be made of the debate at that time about whether an amplitude-modulated signal is a sinusoidal oscillation with a slowly varying amplitude or a set of spectral components. The findings of Kotel'nikov's investigation were formulated in the form of a report ''On the transmission capacity of 'ether' and wire in electric communications'' prepared for the 1st All-Union Congress on the Technical Reconstruction of Communication Facilities and Progress in the Low-Currents Industry. The Congress was never held, but the materials submitted to the Organizing Committee were published [1], which served as official confirmation of Kotel'nikov's priority of proving the famous sampling theorem.

The work in fact contained seven theorems, but all of them were to an extent the development of the principal theorem which states that any function $f(t)$ with a limited spectrum of width B is representable in the form of a series

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

The theorem states in essence that any function is completely representable by the collection of its values selected at discrete points in time $t_n = n/2B$. If ultrashort pulses are emitted with amplitudes equal to the values of the function at the above discrete points in time, a receiver possessing a low-pass filter of spectral width B will generate oscillations of the form $\operatorname{sinc}(x)$ and the sum of these oscillations will once again exhibit the undistorted function $f(t)$. This procedure of signal transmission and reception is explained in Fig. 1. Since the bandwidth of the low-pass receiver filter should not be smaller than the spectral width of the signal, attempts to narrow this band for an undistorted signal transmission are similar to endeavors to make a *perpetuum mobile* as warned by Kotel'nikov [1] in the formulation of the problem.

Interestingly, in 1936 Kotel'nikov tried to publish his theorem in the journal *Elektrichestvo* (Electricity). However, he was denied publication because the journal was overloaded with papers and his paper was only of narrow interest. If only those who turned him down knew what they were saying! What actually happens is that the theorem has more profound importance than the problem that led to its proof. In essence, it pointed the way for the representation of continuous functions in digital form and thereby came to be one of the theoretical foundations of numerical technology which has been rapidly advancing during the last decades. In the formulation of the problem of the digital representation of continuous functions, first of all there arises the question of how frequently the values of a function should be sampled to adequately represent its form. The first and naive answer is: the more frequently, the better. This signifies that the undistorted transmission of any message calls for rather frequent sampling. However, in communication systems we deal with signals of limited spectral width. Such signals cannot exhibit arbitrarily rapid variations in time. That is why the signal samples taken within too short a time interval may turn out to be little different from one another, and the use of their total collection is unnecessary. A function with a limited spectrum may significantly vary only within time intervals not shorter that the reciprocal of its spectral bandwidth. This was recognized by H Nyquist who was presumably one of the first to express the idea that the samples of a signal should be differed by time intervals equal to approximately the reciprocal of its spectral bandwidth [2]. Not infrequently this gives grounds, especially for Western scientists, to use the term 'Nyquist sampling rule'. However, Nyquist applied his reasoning to the problem of undistorted transmission of a telegraph (digital) signal. This problem is different from the problem of the undistorted transmission of an analogue signal, although they have much in common as pointed out by Professor D Lüke in his paper concerning the origin of the sampling theorem [3]. He noted that ''V A Kotel'nikov was presumably the first scientist who rigorously formulated the sampling theorem and applied it to the theory and technology of communications''. This statement gave grounds to award the Eduard Rhein Foundation prize 1999 for basic research to Kotel'nikov.

A similar theorem had been known to mathematicians. In particular, in 1915 E Whittaker proved it when investigating the approximation problem for entire functions of finite

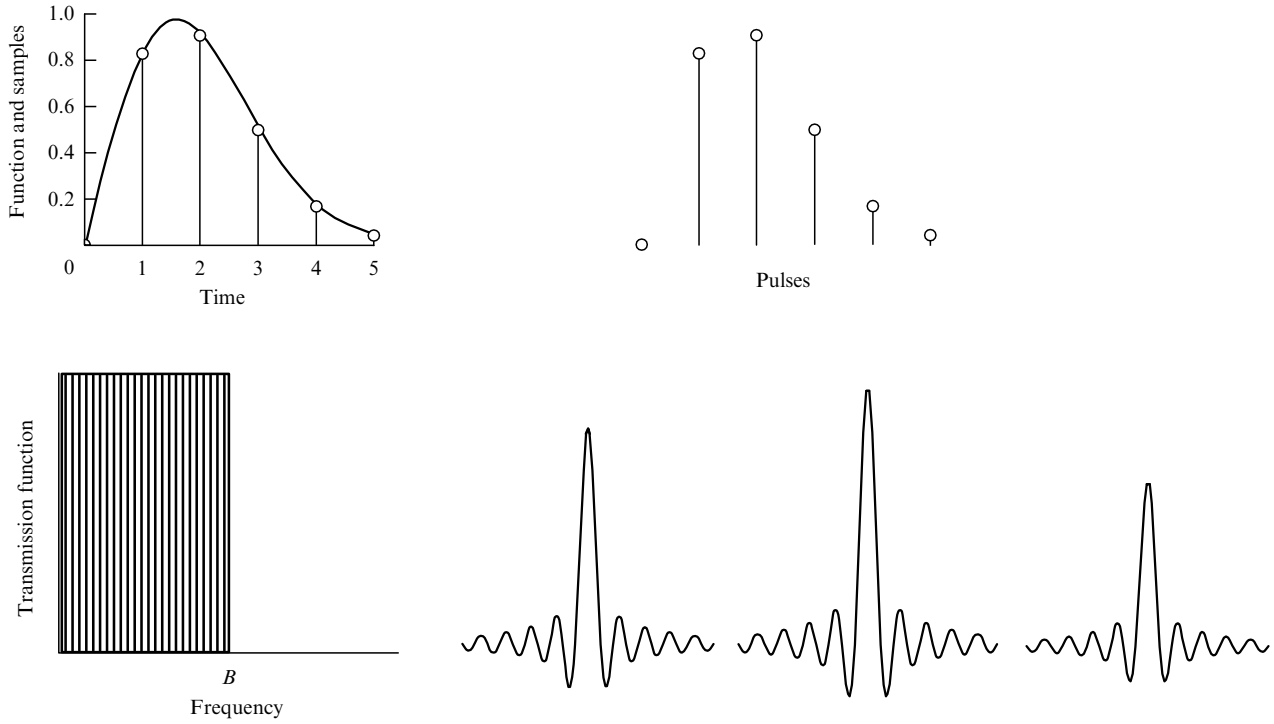


Figure 1. Schematic diagram highlighting the sampling theorem.

degree [4]. Kotel'nikov was not familiar with that work. However, in mathematics this is just one of many ordinary theorems. In communication theory and digital technology this theorem is central, and the credit for its proof undoubtedly goes to Kotel'nikov. Unfortunately, the problems with the publication of his theorem prevented the members of the broad scientific community from familiarizing themselves with it. It was not until C Shannon proved the sampling theorem anew in 1948 [5] that it became widely known. At present, this theorem is frequently referred to as the Whittaker–Kotelnikov–Shannon sampling theorem [6].

The Kotel'nikov theorem can be extended to any functions possessing limitations in some space [7]. There is an adjoint theorem which pertains to functions limited in time [8]. In particular, it is possible to produce short pulses by generating oscillations at discrete frequencies. The antenna directivity pattern is the Fourier transform of the currents whose spatial distribution is bounded by the antenna aperture. On these grounds, the directivity pattern can also be represented as a discrete series [9]. In the processing of images a demand arises for digitizing them, and in this case Kotel'nikov's theorem is one of the most important instruments for effecting this operation.

An interesting example is provided by a somewhat unexpected application of the theorem to the description of signal dispersion [10]. As is well known, this effect occurs in wave propagation through media where the phase velocity is frequency-dependent and manifests itself in that the shape of signals is distorted in their propagation. Figure 2a shows an undistorted signal produced by linear frequency modulation in a band B. It possesses the shape of sinc (ξ) and is therefore represented by one Kotel'nikov component. During propagation in plasma, the signal shape is distorted to assume the form plotted in Fig. 2b. This distorted signal now possesses many Kotel'nikov components, their number and amplitudes reflective of the degree of signal distortion. From their parameters it is possible to recover the signal shape [10].

3. Theory of potential noise immunity

In this section we dwell on the next classic Kotel'nikov work concerned with the limiting sensitivity of receiving systems. At the end of the 1930s there arose a crisis in the improvement of noiseproof feature of communication systems. Technical contrivances of all kinds ran across some limit which hindered further increases in receiver sensitivity. This brought up the natural question: did it result from the insufficient resourcefulness of engineers or did there exist some basic reasons that impose a limit on the noise immunity of the systems involved? The answer to this question was provided in Kotel'nikov's doctoral dissertation "The theory of potential noise immunity" written in 1946 and successfully defended in 1947. The aim of the work was "to elucidate whether it is possible to lessen the influence of interference by improving receivers for the existing types of signals. Can noise abatement benefit from a change in the signal form? What signal forms are optimal for the purpose?" [11].

Much in the work under discussion was radically new and unusual to the practising engineers of that time. First of all, there was the introduction of orthonormal time functions $C_k(t)$ in terms of which the signal could be expanded. The signal $A_j(t)$ is represented as a sum:

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

Different signals differ by the a_{jk}-coefficient set. In the case of a limited number of basis functions $C_k(t)$, this expansion would be referred to as the signal representation in the finite-dimensional Euclidean space (Hilbert space) [12]. The signals may be treated as the vectors in this space. An example of such geometric representation is given in Fig. 3. It is pertinent to

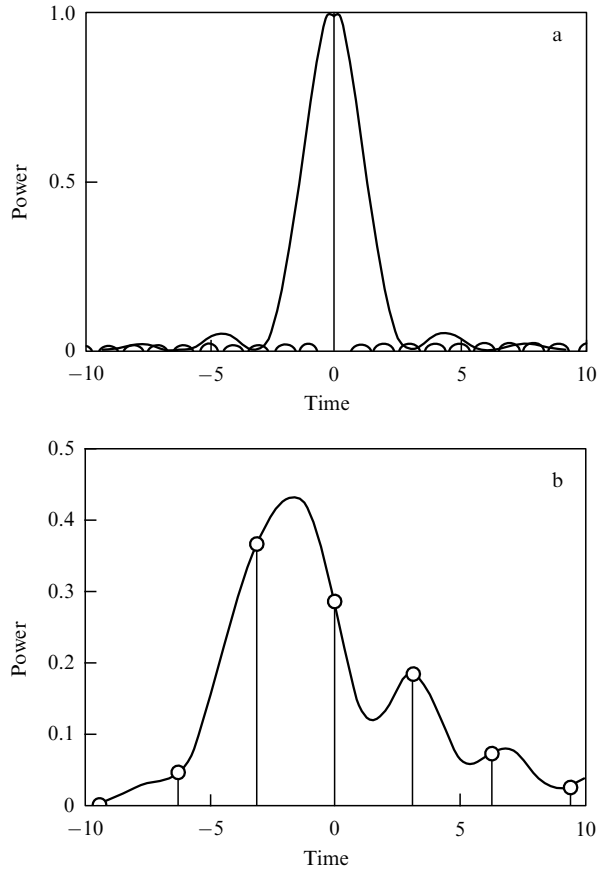


Figure 2. Sampling theorem and signal dispersion.

note that the illustrations like those in Fig. 3 are absent from the thesis although its author quite frequently addresses himself to the geometric representation of the signal. In practical calculations, Kotel'nikov took advantage of Fourier series, which is a natural tribute to the conventional spectral representation of the signal.

The first problem considered in the work was that of signal identification. Its essence is represented in simplified form in Fig. 3. A mixture of signal and noise **X** arrives at the receiver input. What should be the response at the receiver output — is this signal $\mathbf{A}_1$ or $\mathbf{A}_2$? Clearly, the answer will be $\mathbf{A}_1$

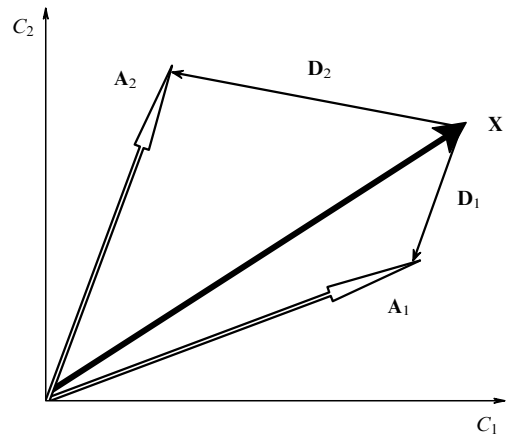


Figure 3. Geometric representation of signals.

if the inequality $|\mathbf{D}_1| < |\mathbf{D}_2|$ is valid for Euclidean distances. However, the validity or invalidity of this inequality is statistical in nature, because some possibility exists that the inequality under discussion is not fulfilled due to random noise behavior. It is therefore reasonable to expect that correct signal extraction against the noise background is probabilistic in nature. Hence follows the concept of an ideal receiver as yielding the minimal number of incorrectly reproduced messages upon noise induction. Potential noise immunity is characterized by the least possible distortions. It is equal to the probability of incorrect reproduction and in the case of Gaussian noise with a uniform spectrum is defined by the ratio between the specific energy and the noise intensity σ^2:

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

Here, T is the signal duration. This relation takes on quite a simple form in the typical case for radar, when $\mathbf{A}_2(t) = 0$:

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

where Q is the energy of the signal. In this case, "the potential noise immunity is defined only by the energy of the signal and is absolutely independent of its form" [11]. Modern radar experts would say that the parameter α is the signal-to-noise ratio which defines the probability of false alarm. For a high signal-to-noise ratio, the probability of correct signal extraction is close to unity, and the probability of false alarm tends to zero. More recently (1948), Shannon obtained the corresponding results for a broader class of noise. It is significant that the decisive role in potential noise immunity is played by the energy of a signal rather than its power. This circumstance is not universally recognized by everyone. Modern techniques of signal production are quite often reliant on its moderate power, while the signal extraction procedure itself involves compression (optimal filtration) in the receiving device [8]. The final answer to the question posed in the first pages of the Kotel'nikov's thesis reduces to the following statement: to improve the noiseproof feature of a communication system requires increasing the signal-to-noise ratio which turns out to be the crucial parameter defining the probability that the signal is correctly extracted against the noise background.

In the following parts of the work, the signal identification problem discussed in the foregoing was supplemented with the problems of parameter assessment and filtration. Thereby addressed were the main problems of statistical radio engineering. This underlies the statement about the fundamental character of Kotel'nikov's doctoral dissertation.

It is pertinent to note that mathematicians had obtained several basic results in the probability theory and the theory of random processes, which were of prime importance to the filtration theory, the parameter assessment theory, the theory of statistical solutions, etc., by the time Kotel'nikov wrote his work. Here, we are faced with a situation that is similar to the situation with the sampling theory. The results obtained by mathematicians did not find their way to the consumer, and the efforts of different specialists were called for to give them practical significance. In 1998, S Verdu published a paper dedicated to the fiftieth anniversary of Shannon's theory [13]. It said, in particular, that the greatest contribution to the introduction of the theory of random processes into the

toolkit of communication engineers had been made by Wiener [14] and Rice [15]. However, Wiener's paper, published in 1949, could not have been familiar to Kotel'nikov in 1946. As regards Rice's work, it was published in 1944, and it was the only paper referred to in Kotel'nikov's thesis for doctorate. There were no other references, because there were no predecessors. That is why it is fair to say that Kotel'nikov should be regarded as one of the founders of statistical radiophysics and radio engineering. For some reason, this outstanding role of his is not broadly reflected in the scientific literature. The fact that the statistical views were not widespread among radio engineers is shown by the mode of Kotel'nikov's work presentation itself. Despite the fact that it constantly deals with random processes, the terms correlation, spectral density, etc. are not encountered, although they are implicitly present. The procedure of decision making itself is based on the Bayes strategy, but this is not mentioned in the text, and the formula for the *a priori* probability is derived simply from 'reasonable' considerations.

As already noted, *The Theory of Potential Noise Immunity* was published only in 1956, when the works of many other authors had gained wide recognition. That is why this work is well known to only those who are 'well informed' and in recent years has been sometimes cited primarily by Russian scientists. And this comes as no surprise. Science is advancing.

4. Planetary radar

Planetary radar is another outstanding achievement in Kotel'nikov's scientific work. In the 1960s, progress in rocket and space technology opened up the possibility of launching space vehicles to other planets of the Solar system. To control the flight of such a spacecraft required a sufficiently thorough knowledge of planet locations. The astronomical observations performed by that time provided reliable data about the relative dimensions of the Solar system. However, successful interplanetary navigation called for a good knowledge of the absolute dimensions of the system. The main scale quantity characterizing the dimensions of the Solar system is the astronomical unit (AU), which is equal to the major semiaxis of the elliptic orbit of the Earth, or the average distance from the Earth to the Sun (about 150 million km). It can be calculated if the distance between two planets is known. Radar exactly furnishes this possibility. The team supervised by Kotel'nikov took on the task of its implementation. In this case, Kotel'nikov proved to be a remarkable organizer, and not only an outstanding scientist. At that time, a long-range space communication center was being built in Evpatoriya (the Crimea), which consisted of a high-power transmitter (≈ 10 kW) at a wavelength of 39 cm, as well as the large transmitting and receiving antennas ADU-1000 with an effective area of about 1000 m^2. To successfully implement the radar required devising a wide range of equipment for filtering signals and measuring their spectrum, frequency, etc. It is worth mentioning that there were no computers at the beginning, and many algorithms could not be realized by software-based techniques. The only way was to make the corresponding facilities on one's own.

That planetary radar was an intricate matter at that time was evidenced by foreign experience. The first attempts of Venus's radar location were undertaken in the USA (1958) [16] and England (1959) [17]. However, the results of these experiments turned out to be erroneous. This was also confirmed by the first experiment of Kotel'nikov's group. Early in the work the capabilities of the radar set were so low that extracting the signal required accumulating it for several hours. However, as the technology developed (which involved increasing the transmitter power, equipping the receiver with low-noise paramagnetic amplifiers, introducing linear frequency modulation, improving the methods of signal extraction, etc.), they succeeded in realizing a relative measurement accuracy of about 10^{-8} for interplanetary distances. This afforded determination of the astronomical unit with an accuracy on the order of 1 km. This accuracy is thousands of times higher than that attained by astronomical methods. At the XVIth General Assembly of the International Astronomical Union (1967) it was accepted that $1\ \mathrm{AU} = 149{,}597{,}870 \pm 2$ km for a speed of light $c = 299{,}792{,}558 \pm 1.2\ \mathrm{m\ s^{-1}}$. The time of radio wave propagation was determined so accurately that the accuracy with which the speed of light was known turned out to be significant in the time–distance translation. It is noteworthy that planetary radar investigations were simultaneously pursued in the USSR and the USA. Competition existed between scientific teams and, naturally, many results were similar.

Apart from Venus, radar measurements were made of Mars, Mercury, and Jupiter. These measurement data were also used to make more precise the astronomical unit. The high precision of the radar measurements permitted constructing the theory of planetary motion, which was more exact than the theory relying on optical data. To construct this theory, account had to be taken of the effects of the general relativity theory. Planetary radar thereby came to be one of the means of verifying the implications of general relativity.

Radar observations also enabled revising other parameters of the planets. This is especially true for Venus whose radius, period, and sense of rotation were refined. In particular, the rotation of Venus was found to be of opposite sense (relative to the sense of its orbital motion around the Sun) and its period was measured at 243.04 days. Interestingly, this value is quite close to the synodic resonance with a rotation period of 243.16 days, whereby the same side of Venus would be facing the Earth at every inferior conjunction. The results of planetary radar are described in greater detail, for instance, in Ref. [18].

5. Radar cartography of Venus

In the implementation of this work, which brought fame to the Soviet space program, V A Kotel'nikov was not its formal supervisor. However, the program of radar-assisted cartography of Venus could hardly have been realized without his active participation. In doing this there was a need to 'synchronize', apart from the Institute of Radioengineering and Electronics of the USSR Academy of Sciences, the work of the S A Lavochkin Research and Production Association, the Special Design Bureau of the Moscow Power Engineering Institute, and several other industrial and academic organizations. This was within the power of only such a prominent and authoritative personality as Kotel'nikov.

In 1983, the artificial satellites 'Venera-15' and 'Venera-16', each having aboard a radar with a synthetic aperture and an altimeter, were sent into Venus orbit. The radar enabled obtaining an image of the planet's surface, permanently screened by clouds and therefore invisible in the optical range. In this way, they succeeded in mapping the planet surface with a spatial resolution of 1–2 km, and the altimeter

provided data about the relief with a resolution of 230 m in altitude. And so for the first time humankind learned about the surface structure of the northern part of Venus over an area of 115 million km^2 (25% of the Venus total surface). Unquestionably, this was an outstanding achievement. Several years later this research was continued in the USA during the Magellan mission, when they managed to obtain images of almost the entire surface of Venus with a spatial resolution of about 100 m. This mission was planned with the inclusion of the results of the Soviet space program. The results of the Venera-15 and Venera-16 missions are described in greater detail in Ref. [19].

We emphasize that, apart from the radar survey itself, the radar data processing and the construction of planet images were also a problem. At that time, one of the most complicated operations was the Fourier analysis. The computers which were at the disposal of researchers were too weak to perform this operation in a reasonable time. It was not without reason that optical processors were still employed at that time to process the data from radars with synthetic aperture, in which the Fourier transform of a radar hologram was effected with a lens. The project participants devised and made a special-purpose Fourier processor which permitted increasing the SM-4 computer speed up to 5×10^7 operations per second by this algorithm and thereby performing the all-digital radar data processing and surface image construction. That was the USSR's first experience in the digital processing of radar image, which was subsequently taken into account in the production of the Almaz radar data processing programs.

6. Conclusion

In so brief a report it is hard to outline all the results of the activities of a personality like V A Kotel'nikov in scale and depth of thought. We have not, in particular, touched upon his basic works in the area of cryptography, his role in the design and implementation of the Moscow – Khabarovsk radio communication system in the pre-war years, his contribution to the theory of parametric amplifiers, his role in the making of the systems of communication with deeply submerged submarines, and many other things. It is pertinent to note that Kotel'nikov initiated time and again new lines of research performed both at the Institute of Radioengineering and Electronics of the Russian Academy of Sciences, which he directed for many years, and in other organizations. Special mention should be made of his role in the development of space research, which he played as Vice-President of the USSR Academy of Sciences and Chairman of the Interkosmos Council.

To summarize, it is valid to say that Vladimir Aleksandrovich Kotel'nikov was an outstanding scientist and engineer of the 20th century — one of the founders of digital signal processing technology, information theory, statistical radiophysics, radio engineering, and radar astronomy. This brief list alone makes it clear that we were dealing with a prominent personality in the history of our country and science, who made an enormous contribution to the progress of science.

References

1. Kotel'nikov V A, in *Vsesoyuznyi Energeticheskii Komitet. Materialy k I Vsesoyuznomy S'ezdu po Voprosam Tekhnicheskoi Rekonstruktsii Dela Svyazi i Razvitiya Slabotochnoi Promyshlennosti* (All-Union Energy Committee. Materials for the I All-Union Congress on the Technical Reconstruction of Communication Facilities and Progress in the Low-Currents Industry) (Moscow: Upravlenie Svyazi RKKA, 1933) pp. 1 – 19; reprint: *O Propusknoi Sposobnosti 'Efira' i Provoloki v Elektrosvyazi* (On the Transmission Capacity of 'Ether' and Wire in Electric Communications) (Moscow: Institut Radiotekhniki i Elektroniki MEI (TU), 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. Khurgin Ya I, Yakovlev V P *Metody Teorii Tselykh Funktsii v Radiofizike, Teorii Svyazi i Optike* (Methods of the Theory of Entire Functions in Radiophysics, Communication Theory, and Optics) (Moscow: Fizmatgiz, 1962)
8. Vainshtein L A, Zubakov V D *Vydelenie Signalov na Fone Sluchainykh Pomekh* (Extraction of Signals against Random Noise Background) (Moscow: Sovetskoe Radio, 1960) [Translated into English: Wainstein L A, Zubakov V D *Extraction of Signals from Noise* (Englewood Cliffs, NJ: Prentice-Hall, 1962)]
9. Minkovich B M, Yakovlev V P *Teoriya Sinteza Antenn* (Antenna Synthesis Theory) (Moscow: Sovetskoe Radio, 1969)
10. Armand N A *Radiotekh. Elektron.* **49** 1199 (2004) [*J. Commun. Technol. Electron.* **49** 1123 (2004)]
11. Kotel'nikov V A *Teoriya Potentsial'noi Pomekhoustoichivosti* (The Theory of Potential Noise Immunity) (Moscow: Radio i Svyaz', 1998) [Translated into English as *The Theory of Optimum Noise Immunity* (New York: McGraw-Hill, 1960)]
12. Levitan B M "Gil'bertovo prostranstvo" ("Hilbert space"), in *Matematicheskaya Entsiklopediya* (Encyclopedia of Mathematics) Vol. 1 (Moscow: Sovetskaya Entsiklopediya, 1977) p. 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. Kotel'nikov V A et al. "Razvitie radiolokatsionnykh issledovanii planet v Sovetskom Soyuze" ("Progress of radar investigations of planets in the Soviet Union"), in *Problemy Sovremennoi Radiotekhniki i Elektroniki* (Problems of Modern Radio Engineering and Electronics) (Ed. V A Kotel'nikov) (Moscow: Nauka, 1980) p. 32
19. Aleksandrov Yu N et al. "Vnov' otkrytaya planeta (radiolokatsionnye issledovaniya Venery s kosmicheskikh apparatov Venera 15 i Venera 16)" ["The planet discovered anew (radar investigations of Venus from the Venera-15 and Venera-16 spacecrafts)"], in *Itogi Nauki i Tekhniki* (Progress in Science and Technology) (Ser. Astronomy, Vol. 32) (Moscow: VINITI, 1987) p. 201

PACS numbers: **01.60.+q**, **89.70.+c**
DOI: 10.1070/PU2006v049n07ABEH006049

V A Kotel'nikov and encrypted communications in our country

V N Sachkov

Vladimir Aleksandrovich Kotel'nikov is one of the outstanding Russian scientists whose work and scientific activity enriched the world of science and are not only the classic heritage of our country, but are of worldwide scientific and cultural significance as well.

Among the broad spectrum of Kotel'nikov's achievements in many areas of science and engineering, a special place is occupied by his work in the development of secrecy communication systems in our country. He addressed himself to the problems of secret telephony and telegraphy in the 1930s in connection with the development of facilities for encrypting telegraph and telephone transmissions via the

short-wavelength Moscow – Khabarovsk communication line. At that time, several organizations were concerned with the scientific and technical problems related to the development of encrypting telephone equipment, whose activity resulted in the production of small batches of such equipment employed on communication lines.

That was mainly the so-called masking apparatus in which the vocal signal transformation consisted in inverting the vocal spectrum, which was as follows: the low frequencies of speech were inverted with the high ones and the remaining frequencies were shifted relative to the center of the spectral band. Under this transformation, open speech recovery in the case of unauthorized interception of the secret transmission did not present a major technical problem for an enemy.

To Kotel'nikov's credit, he proposed the application of more complicated but technically feasible transformations of the vocal signal in encryption telephone equipment. Along with the rearrangement of frequency bands with inversion, he proposed the employment of the temporal rearrangement of 100-millisecond vocal intervals. A coder controlled the frequency and time rearrangements during transmission and reception of messages. In the context of the limited capabilities of contemporary equipment which underlay the efficient methods for unauthorized transformed-speech recovery, the method for encrypting telephone transmissions proposed by Kotel'nikov was sufficiently immune.

Two laboratories were set up in the Central Research Institute of Communications of the People's Commissariat of Communications (TsNIIS NKS in Russ. abbr.) with the aim of developing equipment for encrypting telephone and telegraph communications, including the use of the transformation algorithms proposed by Kotel'nikov. Kotel'nikov was appointed scientific supervisor of these laboratories.

In 1940, in Kotel'nikov's laboratory a start was made on the development of encryption telephone equipment, badly needed by the armed forces of the country at that time. Owing to the selfless labor of laboratory staff members it was possible to produce and test the laboratory prototypes of some of the main units of encryption equipment within approximately three months after the Soviet Union entered the war. Under the dreadful wartime conditions, among them evacuation of the laboratory to Ufa, test-pieces of encryption telephone equipment were made to be 'baptized by fire' in 1942, when the wire lines of communication with the Transcaucasian front were broken during the battle of Stalingrad. This equipment was subsequently applied to encrypt the short-wavelength communication channels employed by the Supreme Commander Headquarters for communicating with the fronts. Later on, the equipment for encrypting telephone transmissions was also used on diplomatic communication lines between Moscow and Helsinki, Paris, and Vienna in the course of negotiations on concluding peace treaties after the termination of the Second World War, as well as during the Tehran, Yalta, and Potsdam Conferences of the leaders of three countries.

The systems for encrypting telephone information on the basis of frequency-temporal transformations of a vocal signal by their nature could not guarantee information protection under the conditions of a significant increase in the capabilities of computer technologies and the development of techniques for deciphering encrypted telephone messages. Devising equipment to ensure the guaranteed encryption of vocal information required invoking the discretization principle in the signal transmission via a communication channel and developing a way of unbreakable information encryption in a digital form. Kotel'nikov made a significant contribution to the solution to the first problem even in 1933, when he published his paper "On the transmission capacity of 'ether' and wire in electric communications", in which he formulated a theorem which defines the function discretization conditions and which now bears his name.

Of fundamental importance to the development of a telephone coder with guaranteed unbreakability against unauthorized access was the development of a vocoder which narrowed the speech-representing spectrum by a factor of several dozen. Kotel'nikov immediately recognized the promise of using the vocoder for encrypted telephony, and his laboratory pursued active research aimed at developing a domestic vocoder. The first sample of such a vocoder, which was far from perfect, was made in 1941. Its design was subsequently improved, resulting in the development of a vocoder with acceptable technical characteristics.

Aside from the discretization problem of a vocal signal and its compression in a communication channel, making the corresponding high-speed digital-type encryption device was required in the development of encryption telephone equipment with guaranteed unbreakability against unauthorized access. Kotel'nikov outlined the principles underlying such an encryption device in his typewritten paper "Basic principles of automated encryption", which he signed on 18 June 1941. In this work, Kotel'nikov introduced the notion of 'perfect encryption' as a way of encoding whereby it is impossible, proceeding from the intercepted encoded text, to limit the set of open messages to which the open message transferred in encoded form belongs.

In 1945, C Shannon introduced the notion of 'perfect secrecy' using a probabilistic approach. An encoding system possesses 'perfect secrecy' when the conditional probability of any open message for a given encoded text coincides with the absolute probability.

It is noteworthy that there exist encryption systems that satisfy two above definitions (both of 'perfect encryption' and of 'perfect secrecy'). An example is provided by the encryption system in which the alphabets of open and encrypted texts coincide, the cipher consists in the realization of a random, equally probable sequence of independent tests in the same alphabet, and the length of messages is fixed. In the encoding, the sign of the text in cipher is obtained by summation of the absolute values of the sign of the open text and the sign of the encoding sequence.

In the 1950s, cryptographically unbreakable equipment for encoding telephone information was produced, which took advantage of the research into vocal signal discretization and vocoder design. At that time, Kotel'nikov moved to the Moscow Power Engineering Institute and took up other scientific problems. However, not only did he continue to advise the designers of new encryption telephone equipment, but he also participated in the work of the State Commission for the formal acceptance of pilot samples, which produced recommendations for manufacturing pilot batches of the equipment by the industry.

Beginning in the 1950s, domestic cryptography as a science advanced considerably. At that period, several well-known scientists and experts in the realms of mathematics, physics, and computer technology participated in the solution of cryptographic problems. Under their scientific supervision new lines of research formed, which provided the theoretical basis for practical implementation of the solutions found in

the area of information encryption. The teams of specialists in cryptography were substantially reinforced with young graduates from the leading higher educational institutions of our country.

A special branch was set up at the Mechanics and Mathematics Department of Moscow State University for training future experts in mathematics and cryptography. A higher educational institution was simultaneously organized for training cryptographers and specialists in mathematical, physicotechnical, communications, and related areas; its successor is now the Institute of Cryptography, Communications, and Informatics. For several decades, the graduates of these educational institutions, along with the graduates of other higher educational establishments, formed a highly qualified body of scientists and practising engineers who drove the successful development of domestic cryptography and the cryptography-based immunity of the state, military, and economic communication lines in this country. By the early 1990s, the cryptographic service of our country had accumulated substantial scientific potential and scientific and technical schools had taken shape, where scientists and specialists carried out research at contemporary scientific and technical levels. Based on the results of this research, a system was established for upholding doctoral and candidate's dissertations. As a result, the cryptographic service has come to embrace a substantial contingent of highly qualified researchers with doctor's and candidate's degrees.

Under these circumstances, the State Academy of Cryptography of the Russian Federation was established with the approval of the President of the Russian Academy of Sciences by decree of the President, Russian Federation in 1992. At present, the Academy of Cryptography conducts about 100 research works per year, which are performed by up to 1000 scientists and experts from over 40 scientific organizations in our country, including the Russian Academy of Sciences, M V Lomonosov Moscow State University, etc. Jointly with the RAS, the Academy of Cryptography publishes *Trudy po Diskretnoi Matematike* (Proceedings in Discrete Mathematics). Since 1997, eight volumes have been published, which contain unclassified papers of the members of the Academy of Cryptography and young mathematician-cryptographers.

Kotel'nikov's creative collaboration with the cryptographic service of the country continued on and off throughout all his life. An active phase of this cooperation dates to 1992, when the Academy of Cryptography of the Russian Federation was set up. Kotel'nikov played a crucial role in the establishment of the Academy of Cryptography and actively provided support for it at all stages of its formation and development. Together with five other members of the Russian Academy of Sciences, he was among its founders and would subsequently participate directly in the scientific and scientific-organizational activity of the Academy of Cryptography. The talks and discussions between Academy members and Kotel'nikov about different cryptographic problems, including discussions on various ways of constructing 'perfect encryption' devices, were interesting and fruitful for the interlocutors.

To perpetuate Kotel'nikov's memory, the Presidium of the Academy of Cryptography of the Russian Federation instituted in 2006 two V A Kotel'nikov scholarships for postgraduates of the Institute of Cryptography, Communications, and Informatics of the Academy of the Federal Security Service.

The Academy of Cryptography piously reveres the memory of those who have participated in the formation and development of the modern cryptographic service of the country, who worked hard and made a major contribution to the development of domestic cryptography. The name Vladimir Aleksandrovich Kotel'nikov is one of the highest on the list of these names.

PACS numbers: 03.67.Dd, **89.70.+c**
DOI: 10.1070/PU2006v049n07ABEH006050

Quantum cryptography and V A Kotel'nikov's one-time key and sampling theorems

S N Molotkov

Quantum cryptography constitutes a new avenue in the development of the means of confidential information transmission. To be more precise, quantum cryptographic systems are systems for secret key distribution between spatially separated (remote) legitimate users. Affording secret key distribution over such users is of crucial importance in cryptography. If there existed a way of distributing (transferring) secret keys from one legitimate user to another via a public (nonsecret) communication channel with an assurance that the keys would remain unknown to the eavesdropper in the course of transfer, it would be possible to transfer messages ciphered with the aid of these keys, which in principle cannot be deciphered (broken) by a third person. Suchlike fundamentally nondecipherable systems are referred to as absolutely unbreakable, or cipher systems in a one-time pad mode. More recently, these ciphers have come to be known as perfect.

First we briefly touch upon the history of the problem.

The first rigorous substantiation of the fact that one-time key cipher systems are absolutely unbreakable was given in Vladimir Aleksandrovich Kotel'nikov's work. This work, which had been completed a few days before the Soviet Union entered the Great Patriotic war, was part of a classified report [1] and has never been published in the open press.

At the same time, the problems of theoretical cipher immunity were independently studied by C Shannon. The findings of his investigations were presented in the classified report "A mathematical theory of cryptography", which dates to 1 September 1946. Following the war this report was declassified[1] and published in 1949 as the paper "Communication theory of secrecy systems" [2], which became a well-known classic work on theoretical cryptography.

An idea quite close to the idea of the one-time pad cipher mode was advanced in G S Vernam's work "Cipher printing telegraph systems for secret wire and radio telegraphic communication" [3] back in 1926. He stated, although without any mathematical reasoning, that running key ciphers would be perfectly secure: "If, now, instead of using

[1] Here, there is good reason to mention the opinion of W Diffie, one of the founders of public-key cryptography. In his view, Shannon's work might conceivably have been declassified by mistake [see the preface to B Schneier's monograph *Applied Cryptography* (John Wiley & Sons, Inc., 1996)].

English words or sentences, we employ a key composed of letters selected absolutely at random, a cipher system is produced which is absolutely unbreakable".

Thanks to Kotel'nikov's and Shannon's research, there emerged a clear and rigorous understanding as to what criteria an absolutely unbreakable cipher should satisfy.

Informally, a cipher is absolutely unbreakable when:

(i) the key is secret — is known to only the legitimate users;

(ii) the key length in bits is no shorter than the message length;

(iii) the key is random, and

(iv) the key is employed only once.

In this case, the message in cipher is statistically independent of the initial message.

The fundamental problem in the realization of one-time key cryptosystems consists in the transfer (distribution) of secret keys to remote legitimate users.

The key has to be transferred to such users by way of some physical signal via a public (i.e., accessible to eavesdropping) communication channel. From the standpoint of classical physics, in this case there is no prohibition against measuring the transmitted signal without its perturbing. That is why it is in principle impossible to guarantee the secrecy of the key in its distribution.

The situation is radically different and more interesting when the key transfer is effected by means of quantum states. Quantum cryptography, based on the basic prohibitions imposed by quantum mechanics, opens the door to key transfer with the aid of quantum states, the secrecy being ensured by the basic laws of nature. Quantum cryptography therefore makes it possible to realize absolutely unbreakable cipher systems with one-time keys, which can be traced to the works of Vernam, Kotel'nikov, and Shannon. Properly speaking, the idea of quantum cryptography is aimed precisely at solving the central cryptographic problem — the problem of secret key distribution.

The idea of invoking quantum mechanics for information protection was first stated by S Wiesner in 1973 (the idea of 'quantum' money) but published [4] only a decade later. Interestingly, the ideas of applying quantum mechanics to information protection were conceived earlier than classical public-key cryptography [5, 6].

The advent of quantum cryptography is associated with the publication of a remarkable paper by Bennett and Brassard in 1984, who came up with the first cryptographic protocol BB84 which later became classic [7].

Quantum cryptography, or secret key distribution, permits, in principle, realizing absolutely unbreakable (not decipherable by an eavesdropper even theoretically) one-time key cipher systems. The secrecy of keys in quantum cryptography relies on the fundamental quantum-mechanical prohibitions: (i) an unknown quantum state cannot be cloned (the no-cloning theorem [8]); (ii) a pair of observables to which there correspond noncommuting Hermitian operators cannot be simultaneously distinguished with confidence, which stems from the Heisenberg uncertainty relation [9], or, to be more formal, noncommuting operators cannot posses common eigenvectors. The density matrices of the information states corresponding to the classical 0 and 1 bits fulfill the function of observables in quantum cryptography. For pure states, the simultaneous unobservability (certain indistinguishability) of the density matrices is equivalent to the nonorthogonality of information quantum states [9]. The aforesaid signifies that there are no measurements which allow distinguishing one of the pair of nonorthogonal states with the probability 1 and in doing this retain the initial (unperturbed) state of the system.

Therefore, any measurement that yields information about the transmitted states is bound to disturb them, which permits detecting any attempts at eavesdropping in the communication channel. In other words, the eavesdropping (accordingly, the perturbation of the transmitted states) cannot help but change the statistics of measurement data at the receiving end in comparison with the statistics of the measurement data covering unperturbed states. A quantum state distortion takes place in a nonideal quantum channel, which is also responsible for a change in the statistics of measurement data. In quantum cryptography it is in principle impossible to distinguish whether the data statistics change in comparison with that in the ideal case due to noise in the channel or due to the actions of an eavesdropper, and therefore any changes in statistics are to be attributed to an eavesdropper's action.

If the laws of quantum mechanics allowed revealing merely the very fact of perturbation of transmitted states, this would be of little interest for the purposes of cryptography, more specifically for the transfer of keys. *Quantum mechanics permits not only detecting the state perturbation, but also relating the change in measurement data statistics to the amount of information which might be obtained by an eavesdropper for the observed change in counting statistics in comparison with the statistics in the ideal case*.

Apart from a quantum communication channel (in real conditions, this is either optical fiber or open space) employed for transferring quantum states in quantum cryptography, also required is a public, classical communication channel. The latter is required by legitimate users to reveal the changes in counting statistics and error correction in the primary key transmitted via the quantum communication channel.

The only requirement imposed on the classical communication channel is that the classical information transmitted openly and accessible to anyone, including an eavesdropper, cannot be altered by the eavesdropper, thus being intact (the so-called unjammable channel) [7]. This unjammable channel is, of course, a mathematical idealization. In real conditions, to retain the integrity of the publicly transmitted classical data advantage should be taken of data authenticity and integrity verification procedures. These procedures, in turn, require a secret key. When use is made, for instance, of the Internet as the unjammable channel, the Hellman – Diffie key generation scheme [5] may be employed for authenticity verification purposes. However, when the unjammable channel makes use of the same optical fiber line as for the quantum channel, the Hellman – Diffie key generation scheme for authenticity verification obviously turns out to be unacceptable due to the so-called 'man in the middle' attack.

In this situation, a small start-up key is required once during the first communication session. In the succeeding sessions this key is discarded, and a part of the key generated via the quantum channel during the previous exchange session is employed to verify the authenticity and integrity of data transmitted via the classical channel. The remaining greater part of the key obtained via the quantum channel is intended for transmitted information ciphering itself. When use is made of GOST R 34.11-94 procedures [10] to verify the authenticity and to retain integrity of the data, the start-up key length equals 256 bits. In this case, a new secret key (much longer than the initial one) may be

transferred during several seconds of exchange via the quantum channel.

Of course, the start-up key may be used for ciphering a new key and transferring it to the second legitimate user. However, in doing this the absolute secrecy of the new key is guaranteed only when its length does not exceed the length of the key employed to cipher the new key, i.e., there is no way of obtaining a longer key than the initial one. In quantum cryptography, the start-up key is not employed directly to transfer a new key, which is generated via the quantum communication channel. In this case, the number of open information bits transferred via the unjammable channel per one bit of the new secret key can be made smaller than unity, and a key expansion is therefore possible.

The approach involving a small start-up key is preferable to the approaches relying on asymmetric public-key cryptography algorithms, because it permits minimizing the number of sessions of exchange via the public communication channel in the course of key privacy amplification and 'purification'.

The main task of the theory reduces to elucidating the length of the secret key which can be obtained for observed changes in the statistics of the measurement data at the receiving end in comparison with the statistics covering unperturbed states. As a rule, the quantity which characterizes the departure of the measurement statistics from the ideal ones is the observed error probability at the receiving end, or more precisely, the probability that the transferred 0 bit was recorded as 1, and vice versa. This situation takes place in the widely used BB84 protocol, although other criteria of a statistics change are possible, which employ several parameters. Prior to error probability elucidation, via a public channel there occurs a comparison of the bases at the receiving and transmitting sides (for the BB84 protocol [7]) or disclosing the positions at the receiving side, where measurements yielded an indefinite result (for the B92 protocol [9]). The error probability is evaluated by comparing, via the public communication channel, a part of the sequence obtained via the quantum information channel with the corresponding part of the initial one; the disclosed part is subsequently discarded.

The next step of any quantum cryptographic key-distribution protocol consists in error correction in the undisclosed part of the sequence for legitimate users by way of information exchange via the public information channel. Legitimate users are commonly given the names Alice and Bob, while the eavesdropper is referred to as Eve. As a result of error correction, Alice and Bob retain bit sequences of shorter length that are already similar. In this context, 'similar' signifies that the sequences coincide with a probability arbitrarily close to unity: $1 - 2^{v}$ (for instance, $1 - 2^{-200} \sim 1 - 10^{-70}$; we recall that the number of atoms in the Universe is estimated at 10^{77}). The parameter v is selected by legitimate users.

Upon 'purifying' the primary key, the eavesdropper has a string of bits or a register of quantum memory with the states, or both. The last step in obtaining the final secret key consists in privacy amplification [11] — in the compression of the 'purified' key with the aid of the so-called 2-universal hash function [12], which is a random function by itself for the already similar sequences with Alice and Bob. The randomly selected hash function is openly conveyed by one of legitimate users via the public communication channel and is considered to be known to all, including the eavesdropper. For legitimate users, the compressed bit sequence is the common secret key, with the assurance that the eavesdropper has an arbitrarily small amount of information about the key according to some secrecy parameter prescribed by Alice and Bob.

The natural requirement imposed on the error correction and key privacy amplification procedures is that the number of bits conserved in the final key should be as large as possible. Yet another requirement consists in the minimization of the number of exchange sessions involving the public communication channel in terms of one bit in the final secret key.

In the error correction in the primary key, the task of the legitimate users is not only to correct the errors, but also to estimate the upper limit of the amount of information which the eavesdropper can gain from exchanges via the public communication channel. To correct errors, advantage can be taken of different procedures, including the well-elaborated classical error-correcting codes.

We now turn our attention to the discussion of experimental realizations of quantum cryptographic systems.

Research in the area of quantum cryptography and realization of different quantum cryptosystems is pursued in many universities in all developed countries and nearly all leading telecommunication companies. During the last five years, quantum cryptography has walked its way from purely theoretical investigations to their practical realization and the fabrication of the first commercial prototypes.

The existing prototypes of quantum cryptosystems employ primarily the following principles of coding classical information into the states of quantum systems.

(1) Coding the information about the key into polarization degrees of freedom [13].

(2) Phase coding with the aid of a Mach – Zehnder interferometer, in which the information is coded into the phase difference between the receiving and transmitting interferometer arms [14, 15].

(3) Coding on the basis of frequency modulation of the carrier frequency [16].

(4) Quantum cryptography on coherent states employing homodyne detection at the receiving end [17].

The greatest progress has been achieved in cryptosystems with phase coding and self-compensation [18] employing Faraday reflectors. The first laboratory prototype of a quantum cryptosystem was made in the IBM Research Center in 1989, and the length of its quantum communication channel measured 1 m [19]. Laboratory versions of a cryptosystem based on a time division Mach – Zehnder interferometer were implemented using a 30-km long optical fiber communication line in the research laboratory of British Telecom in 1995 [20] and optical fiber communication lines of total length 48 km in the Los Alamos Laboratory [21]. These schemes relied on the principle of phase coding. The NEC research laboratory extended the range to 100 km in 2003 [21], and to 150 km in 2004 [22]. These schemes exhibit a sophisticated development of the idea of phase coding with self-compensation by the use of Faraday reflectors. The aforementioned cryptosystems, particularly the schemes with phase coding and self-compensation, are rather complicated to realize. The theoretical research of a group at Geneva University resulted in the implementation of a quantum cryptosystem with a 23-km long optical fiber cable laid on the bottom of Lake Geneva between the cities of Nyon and Geneva. The line, which has been lengthened to 67 km to date, constitutes a complex optical-fiber interferometer with phase coding and self-compensation employing Faraday reflectors [18] (the first so-called plug&play quantum cryptographic

system). Active research is being pursued at the IBM research laboratory (Almaden) [23, 24]. The first local quantum cryptographic network in Boston has been approbated, which is intended for distributing secret keys between users spaced at 10 km (the project is being carried out under the auspices of the Defense Advanced Research Projects Agency) [25].

The MagiQ innovative company recently announced the first commercial version of a quantum fiber cryptosystem operating within a 120-km range, which relies on the phase coding principle. The scheme realizes the BB84 quantum cryptographic protocol.

In the opinion of experts of QinetiQ and Toshiba Research Europe (Great Britain), within three years a start will be made on the wide use of quantum cryptosystems, first and foremost by governmental institutions and banks.

There are known realizations of the prototypes of quantum cryptosystems that transfer secret keys via open space [26–28]. Judging by the published data [28], the record-long range amounts to 23.4 km, both in the daytime and night-time. Suchlike quantum cryptosystems are intended for the generation and transfer of secret keys between ground-based objects and low-orbit satellites (up to altitudes of 1000 km) or between ground-based objects via satellites. In the view of a project leader of QinetiQ, experiments are planned on the transfer of cryptographic keys to low-orbit satellites and with their aid it will be possible to convey secret keys to any point of the planet within seven years or so.

The following parameters of quantum cryptographic optical fiber communication lines are predicted for the near future:

(1) The number of errors not exceeding several percent for an effective rate of information transfer via an optical fiber quantum channel.

(2) A length of about 100–150 km for a quantum optical-fiber communication channel.

(3) 8–16 subchannels in the wavelength multiplexing.

Despite the impressive progress in the understanding of the cryptographic unbreakability (secrecy) of quantum cryptosystems, as well as in their implementation, these systems contain rather sophisticated optical-fiber, electronic, and software components, and operating them at the present time is more like conducting a subtle scientific experiment and demonstrating experimental skill rather than a practical activity involving conventional equipment in general use. Another significant circumstance which now limits the wide acceptance of quantum cryptosystems on the basis of phase coding is that the quantum cryptosystems so far are hardly compatible with standardized optical-fiber telecommunication technologies because they contain specific components (interferometers) requiring fine adjustments. Lastly, the fundamental point is that every quantum cryptographic protocol for secret key distribution in fact necessitates 'dark' optical fiber lines (vacant lines).

There are three basic protocols for secret key transfer, which are briefly termed BB84 [7], B92 [9], and BB84$(4+2)$ [29]. The BB84 protocol makes use of four quantum states: two orthogonal states for 0 and 1 in one basis, and two orthogonal states for 0 and 1 in the other. Between the bases, the states are nonorthogonal in pairs, which is needed to ensure secrecy. The B92 protocol makes use of a pair of any nonorthogonal quantum states corresponding to 0 and 1. The BB84$(4+2)$ protocol is a derivative of BB84 and differs from the latter in that the states inside the bases are also made nonorthogonal. Clearly, different exchange protocols necessitate different physical devices to produce the quantum states at the transmitting end and, accordingly, different devices to make quantum-mechanical measurements at the receiving end.

The cryptographic unbreakability (secrecy) of these protocols has been investigated in sufficient detail [29–36]. When account is taken of real parameters — the nonstrict single-photon nature of the source, the nonideality of avalanche photodetectors, and the optical-fiber communication line attenuation, the above protocols ensure the secrecy of key distribution up to a certain critical length of the optical-fiber communication line [29]. The B92 protocol is minimal in terms of the number of states involved and measurements but ensures secrecy up to distances of only $\sim 15-20$ km [33]. The most thoroughly studied BB84 protocol, which uses four quantum states, is more complicated in realization and maintains secrecy up to distances of ~ 50 km [29]. Finally, the BB84$(4+2)$ protocol makes use of four states nonorthogonal in pairs. This protocol is still more complex in realization and optical-fiber interferometer adjustment, but 'survives' up to distances of ~ 150 km from the viewpoint of secrecy [29].

Experimental realization of quantum cryptosystems calls for single-photon sources. We emphasize that from the standpoint of theory it is not necessary that the quantum states used for key transfer be single-photon states. In a multiphoton case, however, quantum-mechanical measurements taken at the receiving end to detect attempts at eavesdropping and changing the quantum states should formally be realized as projectors on the corresponding vectors of multiphoton quantum states. Such measuring devices so far do not exist, although there are no theoretical prohibitions against the realization of these quantum-mechanical measurements. That is, the use of precisely single-photon quantum states is caused by the existing detectors (actual detectors are gated avalanche photodetectors with Peltier cooling).

It is pertinent to note that superconductor-based photodetectors have already been devised; these, unlike heterostructure-based avalanche photodetectors, distinguish states with a different number of photons.

Single-photon (more precisely, quasi-single-photon) quantum states are obtained by way of strong attenuation of a coherent state — laser radiation, which contains multiphoton components even after arbitrary attenuation.

The nonstrict single-photon nature of the source in combination with the attenuation in the quantum communication channel have the effect that the distributed-key secrecy is guaranteed only when the channel length does not exceed some critical value.

The negative role of attenuation (for a nonstrictly single-photon source) in the quantum communication channel consists in the fact that, beginning with some degree of attenuation, it is no longer possible to guarantee the transferred-key secrecy (which is most important) rather than that the attenuation evidently lowers the rate of key transfer, because not all photons reach the receiving end. The attenuation in optical-fiber communication lines depends on the length of the communication channel. However, the critical length up to which the system retains secrecy is still not strictly known. Its estimates range from dozens of kilometers to 150 km [29].

Efforts are underway to employ radiation sources in quantum cryptography, which are built, for instance, around diamond nanoparticles that approach single-photon sources by their parameters [37].

When the main quantum cryptographic protocols and the proofs of their secrecy in a channel with attenuation are analyzed (BB84 and B92 are the main protocols, while the remaining ones are their derivatives of one kind or another), it becomes evident that *a priori* information is required (and employed explicitly or implicitly) about the error stream (Quantum Bit Error Rate, QBER) arising from the attenuation. For instance, if the attenuation in the communication channel varies during the key transfer protocol, the error stream also changes (even in the absence of an eavesdropper). Moreover, if the protocol implies the QBER constancy, no secrecy of the key transfer may be assured whatsoever. While the attenuation in optical-fiber quantum cryptosystems may be treated as being constant (for a single-mode optical fiber it is equal to $0.17-0.25$ dB km^{-1} at a wavelength of 1550 nm), in the transfer via open space this is clearly not so, because the state of the atmosphere is impossible to control. It is therefore desirable to have key distribution protocols that are immune to and guarantee key secrecy under variations of attenuation in the communication channel during the protocol time and whose secrecy would be independent of the *a priori* knowledge of attenuation strength. This problem, in our view, is serious enough and calls for a solution, because otherwise the absolute secrecy of quantum cryptography (the secrecy which is fully ensured by the fundamental quantum-mechanical prohibitions rather than by the technically limited capabilities of the eavesdropper) may be thrown into doubt.

All the aforementioned difficulties are related to the fact that the protocol secrecy is actually based only on the geometric properties of the state vectors of a quantum system in the Hilbert space $\mathcal{H}$. More precisely, on the impossibility of cloning (the no-cloning theorem [8]) an unknown quantum state and the principal certain indistinguishability of nonorthogonal quantum states (the Bennett theorem [9]). Roughly speaking, these protocols are formulated in the Hilbert space $\mathcal{H}$. The fact that all measurements and the distribution of quantum states occur in space – time is in no way used explicitly. In the distribution of a quantum state, attenuation takes place in space – time rather than in the Hilbert space. That is why to eliminate the problem of attenuation-caused secrecy loss requires involving other additional *basic* limitations that stem from the properties of quantum states and gaining information about them in space – time. The limitations stemming from only the geometric properties of quantum states in the Hilbert space have supposedly been exhausted with relation to the construction of quantum cryptographic protocols.

These additional basic and natural limitations are dictated by the special relativity theory. Furthermore, photons represent truly relativistic massless particles (the massless quantized field states) which travel at a maximum permissible speed. That is why in the development and realization of quantum cryptography in open space it would be unnatural to take no advantage of the additional possibilities offered by nature.

Below we briefly discuss quantum cryptosystems for key transfer via open space, which take advantage of the additional prohibitions stemming from special relativity, in addition to the limitations on the measurability of quantum states, stemming from quantum mechanics.

Since the fact of distribution of quantum states (*the key*) *in space – time is explicitly taken into account in the quantum cryptosystems discussed below, it is required to know beforehand the length of the quantum communication channel between the transmitting and receiving parts.*

Relativistic quantum cryptosystems retain secrecy for any attenuation in the communication channel. The magnitude of attenuation lowers only the key transfer rate but has no effect on its secrecy. Moreover, the key secrecy is guaranteed even for non-single-photon states. The scheme remains secret for an arbitrary average number of photons in the quantum state. According to calculations (for details, see Ref. [38]), the highest efficiency is achieved when the average number of photons is small, viz. $\mu = 1-3$. For these average occupation numbers, idle sendings are virtually absent (the vacuum component fraction in the coherent state is low). This signifies that the key generation rate is at least an order of magnitude higher than in schemes entirely based on the geometric properties of quantum states, which require attenuating laser radiation down to $\mu = 0.1-0.3$. An additional increase in the rate arises from the fact that the limitations from the side of the special relativity theory permit us to employ even orthogonal states, which does not require verifying the reconciliation of measurement bases, as in the BB84 protocol. Furthermore, since all actions of participants (both of the legitimate ones and the eavesdropper) are effected in space – time and the states are orthogonal, collective measurements of the eavesdropper do not offer him any advantages in comparison with individual measurements in every sending. Lastly, the system guarantees key secrecy even for an error level close to 50% in the received binary sequence (for details, see Ref. [38]). It is pertinent to note that the secrecy, for instance, for the BB84 protocol is ensured up to an error level of only 11% [30, 32].

Recall that error-free information transfer, actually error correction in the limit of asymptotically long sequences in a classical binary symmetric channel, is theoretically possible when the error probability does not exceed 50%. *In relativistic quantum cryptography, for an error level close to* 50% *it is possible not only to correct errors, but also to guarantee the secrecy of information* (*keys*) *transmitted by means of quantum states via open space.*

The only additional requirement imposed on relativistic quantum cryptosystems in comparison with nonrelativistic quantum cryptosystems based on nonorthogonal states is the knowledge of the length of the quantum communication channel, which, in our opinion, is a small penalty for those advantages which may be offered by relativistic quantum cryptography.

In quantum cryptosystems, the revelation of any attempts at eavesdropping is guaranteed by the following two basic, closely related quantum-mechanical prohibitions.

(1) Impossibility of the process

$$\begin{aligned} &|\varphi_0\rangle \otimes |A\rangle \mapsto |\varphi_0\rangle \otimes |\varphi_0\rangle \otimes |A_0\rangle\,, \\ &\qquad\qquad\qquad\qquad \langle\varphi_0|\varphi_1\rangle \neq 0\,. \\ &|\varphi_1\rangle \otimes |A\rangle \mapsto |\varphi_1\rangle \otimes |\varphi_1\rangle \otimes |A_1\rangle\,, \end{aligned} \qquad (1)$$

This prohibition against cloning an unknown quantum state is termed the no-cloning theorem.

(2) Impossibility of gaining information about one of the nonorthogonal states without their perturbation, i.e., forbid-

ding of the following process:

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

where $|A\rangle$ is the state of the observer's device, and U is some unitary operator which describes the joint evolution of the state under investigation and the state of the device. These prohibitions are in essence one of the manifestations of the basic Heisenberg uncertainty principle relating to the impossibility of simultaneously measuring the observables to which there correspond noncommuting operators.

For orthogonal states, there are no prohibitions on their cloning or information extraction without their perturbation. In the framework of nonrelativistic quantum mechanics, to the observables $\rho_0 = |\varphi_0\rangle\langle\varphi_0|$ and $\rho_1 = |\varphi_1\rangle\langle\varphi_1|$ there correspond commutative measuring operators, which are orthogonal projectors $\mathcal{P}_{0,1} = |\varphi_{0,1}\rangle\langle\varphi_{0,1}|$ ($[\mathcal{P}_0, \mathcal{P}_1] = 0$). Restrictions (1) and (2) are in essence the geometric property of the state vectors $|\varphi_{0,1}\rangle$ of the quantum system in the Hilbert space of states. Unless some additional basic restrictions on the measurability of orthogonal quantum states are employed, they cannot be used for the purposes of quantum cryptography owing to certain distinguishability. The restrictions on the measurability of quantum states imposed by special relativity represent such additional basic restrictions.

For orthogonal states, there is no prohibition against certain distinguishing without their perturbation [9], or to be more precise, the theorem [9] states nothing about it. The statement that an orthogonal state 'passes' through an auxiliary system $|A\rangle$, interacts with it during the passage, and changes its state, which is frequently made in the interpretation of this theorem, does not correspond to the contents of the theorem. The theorem contains nothing of the kind, in the sense that it is purely geometric in nature and states that the state vector of the auxiliary system $|A\rangle$ may be unitarily turned, depending on the input vector $|\varphi_{0,1}\rangle$, and transferred to a new state $|A_0\rangle$ or $|A_1\rangle$ with no change of the input vector. In this case, it is implicitly assumed that the input vector $|\varphi_{0,1}\rangle$ is accessible as an integral object — that is, to perform the unitary transformation U requires having access to the entire space $\mathcal{H}_{\varphi_{0,1}}$ of states, in which the state carrier is nonzero, otherwise the transformation will not be unitary. The fact that in the proof there appears only the state vector as an integral object $|\varphi_{0,1}\rangle$ without inner coordinate 'filling' just means that the state vector participates 'as a whole' in the transformation.

For any real physical system, the Hilbert space $\mathcal{H}_{\varphi_{0,1}}$ is inevitably attached to the Minkowski space–time, in which a state possesses amplitude (the smoothing wave function). Therefore, access to the Hilbert space of states implies access to that domain of space–time, in which the state amplitude (the wave function) is nonzero. If only a part of such a domain is accessible, then even orthogonal states are impossible to reliably clone or distinguish. This is more or less obvious, since no process, including cloning or distinguishing, may have a higher outcome probability than the fraction of state normalization, which is gathered within the accessible spatio-temporal domain and thereby automatically in the accessible part of the Hilbert space. Roughly speaking, to clone with certainty and distinguish orthogonal states, they are required entirely and at once.

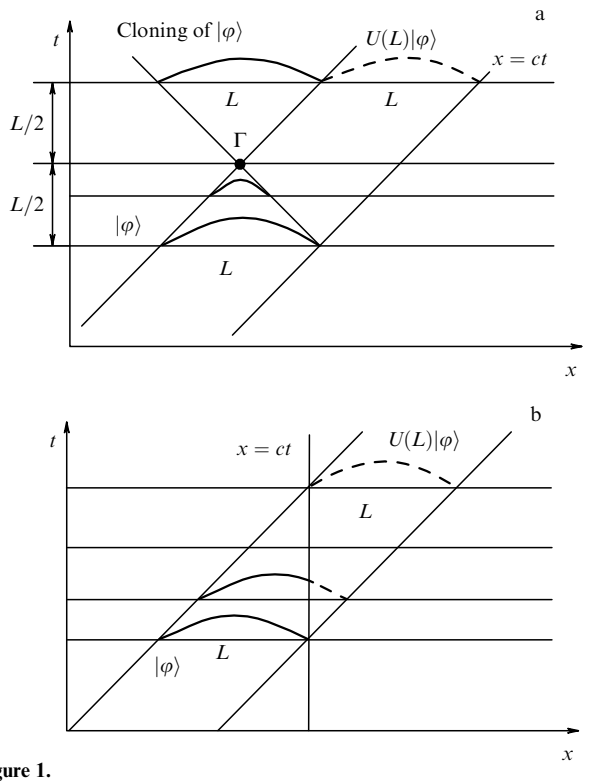


Figure 1.

So, when the amplitude of a state is nonzero in some finite domain of space–time, the words that the state is entirely accessible signify access to this domain. In nonrelativistic quantum mechanics, which imposes no restrictions on the limiting speed, access to any finite domain may be instantly obtained. In quantum field theory, which imposes restrictions on a limiting speed, access to the state as a whole may be obtained only when the lengthy state is preliminarily unitarily transformed to a state with an amplitude which is nonzero in only an arbitrarily small spatial domain. After that, advantage can be taken of the theorem [9]. According to the relativistic causality principle [39], this unitary transformation of the state defined in a finite spatio-temporal domain to a state localized in an arbitrarily small spatial domain may be effected in a finite time only. The minimum requisite time is determined from the condition that a part of the light cone relevant to the 'past' covers the initial spatial domain in which the state amplitude was nonzero (Fig. 1a). The vertex of a light cone resides in an arbitrarily strongly localized domain (at a point) to which the initial state amplitude is unitarily transformed. Each of the pairs of orthogonal states unitarily transformed to ('collected in') a localized domain may thereafter be cloned with certainty or distinguished. Since we are dealing with massless states of a quantized field (photons), which propagate at the maximum allowable speed, this unitary transformation and the subsequent cloning will result in a shift (delay) of the states in space–time relative to those in the case of their free evolution (propagation). This circumstance makes it possible to detect any attempts at eavesdropping. It is pertinent to note that the restrictions imposed on measurements in the relativistic domain were first investigated by L D Landau and R Peierls [40] and subsequently by Niels Bohr and L Rosenfeld [41].[2]

[2] The problem of state localization in the relativistic domain is of significance (in this connection see Refs [42–47]).

In other words, for orthogonal states of the massless quantized field, the no-cloning theorem looks like this. Orthogonal states may be cloned with a probability arbitrarily close to unity. The cloning results in production of states with amplitudes of the same form but being shifted (translated in space – time). That is, a weaker process than in the nonrelativistic case is allowed in expression (1). Therefore, we have

$$\begin{aligned} &|\varphi_0\rangle \mapsto \big(U_L|\varphi_0\rangle\big) \otimes \big(U_L|\varphi_0\rangle\big)\,, \\ &|\varphi_1\rangle \mapsto \big(U_L|\varphi_1\rangle\big) \otimes \big(U_L|\varphi_1\rangle\big)\,. \end{aligned} \tag{3}$$

Here, U_L is the translation operator along the branch of the light cone in space – time, $L = \Delta(x - t)$ is the dimension of the domain in which the state amplitude is nonzero [for brevity we assume that both states are nonzero in the same spatio-temporal domain but differ in amplitude form $\varphi_{0,1}(x - t)$].

Similarly modified is the theorem of Ref. [9] about distinguishing orthogonal states — only a weaker process in comparison with that in the nonrelativistic case (2) is allowed:

$$\begin{aligned} &|\varphi_0\rangle \otimes |A\rangle \mapsto \big(U_L|\varphi_0\rangle\big) \otimes |A_0\rangle\,, \\ &|\varphi_1\rangle \otimes |A\rangle \mapsto \big(U_L|\varphi_1\rangle\big) \otimes |A_1\rangle\,, \end{aligned} \qquad |A_0\rangle \neq |A_1\rangle\,. \tag{4}$$

The aforesaid is conveniently exemplified by the diagrams given in Fig. 1.

Since the amplitude of massless quantized field states propagating in one direction of the x-axis depends only on the difference $x - t$, it is possible to fix the time and treat the coordinate as a variable, or vice versa. We consider both cases. These two cases exhaust all the situations. Assume that one of the orthogonal states with an amplitude $\varphi(x - t)$ is given, and they propagate at the speed of light ($c = 1$; the subscript standing for the state 0 or 1 is for the moment omitted for brevity). Let the state be concentrated in the domain L in the sense that $\int_L \big|\varphi(x - t_0)\big|^2 \,\mathrm{d}x \approx 1$, where $\varphi_{0,1}(x - t_0)$ is the amplitude at the time section t_0.

To obtain *at once all values of the state amplitude for all x at a point in time t_0* in the domain where it is nonzero requires effecting a unitary transformation of the whole state at once. Let the unitary transformation of the state amplitude be $U\varphi_{0,1}(x - t_0) = \tilde{\varphi}_{0,1}(x' - t)$ $(t > t_0)$, then the new state amplitude $\tilde{\varphi}(x' - t)$ may be nonzero in a smaller spatial domain. The minimal domain dimension in x' by the point in time t is dictated, in essence, by the relativistic causality principle which was formulated in its final form by N N Bogolyubov [39]. The matrix elements of the unitary operator are nonzero only when the points (x, t_0) and (x', t) lie within the 'past' part of the light cone emanating from the point Γ and covering the domain in which the state amplitude is nonzero at the point in time t_0. By a point in time no earlier than L, the amplitude of the initial state may be unitarily transformed to a state with an amplitude arbitrarily strongly localized about Γ. It is basically significant that this will be *another* state, a state different from the initial one $\varphi(x - t_0)$. Accessible by the point in time Γ are the values of state amplitude for all x at once (instantaneously). It is now possible to instantaneously obtain the measurement outcome and have complete (with the probability 1) information about the state. If the pair of initial states is orthogonal, by means of a unitary transformation it is possible to obtain also a pair of orthogonal states by the point in time Γ and, therefore, reliably distinguish one from the other (it is now possible to take advantage of the theorem of Ref. [9] about the certain distinguishability of orthogonal states). We emphasize once again that these orthogonal states are *different* from the initial ones. The 'recovery' or cloning of the state may also be realized through the inverse unitary transformation 'directed' forward in time. The state with an amplitude of the same form as the initial one may be obtained by a point in time no earlier than the point defined by relativistic causality. The amplitude of the state with the same form as the initial one is located in the forward part of the light cone emanating from the point Γ. The resultant state is also *different* from the initial one in the sense that it is retarded in time relative to the initial state, which would have travelled forward along x by the point in time L by precisely the value of L had there been no attempts to clone it or obtain information about it (see Fig. 1a). So far we have been dealing with gaining information with the probability 1 about states in the channel. The same reasoning applies to gaining information with a probability lower than unity. The delay will be shorter than L in this case (see Fig. 1).

Similar reasoning also applies to the nonrelativistic case. If the restrictions of the special theory of relativity are neglected, in the previous consideration one should discard that part which appeals to the light cone. In this case, the unitary transformations may formally be effected instantaneously, and even the explicit presence of a coordinate can be eliminated from consideration, retaining implicitly only the fact that the states are entirely accessible under a unitary transformation (the entire spatial region is instantaneously accessible).

Similar reasoning may be employed when a state is unitarily transformed to the state of an auxiliary localized system. An example of such a unitary transformation is provided by the 'stopping' of light [48]. This unitary transformation transfers the photon field state to a vacuum state due to its masslessness and the impossibility of possessing the zero propagation velocity, while the state of an atomic system is transformed to some new state. Being unitary, the transformation also requires access to all values of the photon packet amplitude at the point of atomic system localization. This access is achieved in the natural way during propagation of the wave packet at the speed of light and its arrival at the localized atomic system ('entry' of the whole packet into the atomic system). Where obtaining a result with the probability 1 is involved, this process also requires a time L (the single-photon packet should completely 'enter' the atomic system). As this takes place, the photon field finds itself in a *different — vacuum — state*, while the auxiliary system finds itself in a new state, depending on the input photon state. By the point in time L with the probability 1 it is possible to find out what state it is and prepare the same one with a delay L, which is inevitable in this case, unlike the case of free propagation of the initial wave packet (see Fig. 1b).

Therefore, any acquisition of information about one of the orthogonal states inevitably leads to their modification — translation in space – time (*delay*).

For the subsequent discussion it is significant that no evolution of a massless quantized field interacting with the environment (other quantum and classical degrees of freedom in the communication channel) can result in state 'squeezing' in the sense that the state normalization would be accumulated in a spatial domain going beyond the light cone and being smaller than that in the free propagation (see Fig. 2). As

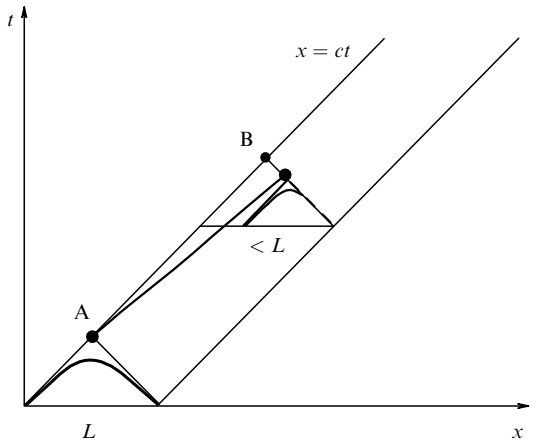


Figure 2.

a rule, this interaction will have the effect that the state will be mixed, but the carrier of the density matrix in space–time cannot be 'squeezed' and drawn out of the light cone (see Fig. 2). Otherwise, that would allow conveying of information by means of quantum states at a supraluminal speed. Indeed, let there be one of a pair of orthogonal quantum states (see Fig. 2). Participant A may extract classical information from the quantum state no earlier than at the point in time defined by the constraint that a part of the light cone relevant to the 'past' covers the state amplitude. After that he can transmit the now-classical information to participant B. This transmission cannot be effected faster than the speed of light [the observers are connected by a branch of the light cone (see Fig. 2)]. Were the quantum state in the channel able to 'squeeze' in the course of its evolution in such a way that, on covering the state by a part of the light cone relevant to the 'past', the vertex of a cone found itself in the domain spatially like to the light cone with a vertex at point A, with one of the cone branches passing through point B, then the observer at point B would be able to extract classical information from the quantum state earlier than participant A could transmit it with the speed of light, because the vertex of a light cone covering the 'squeezed' quantum state went out into a spacelike domain.

From the standpoint of cryptography, the aforesaid signifies that the noise in the channel does not permit the eavesdropper to either clone or gain information about the state earlier than it is dictated by the restrictions imposed by relativistic causality and quantum mechanics (*actually, the quantum field theory*).

Invoking new fundamental physical principles in quantum cryptography enables formulation of a new approach to assuring key transfer secrecy, which eliminates the difficulties encountered in nonrelativistic quantum cryptography (for details, see Ref. [38]). Suchlike quantum cryptosystems would naturally be termed relativistic ones.

We briefly consider here the theoretical limit of the secret key generation rate attainable in quantum cryptography [3] via a quantum communication channel with a finite transmission bandwidth W.

[3] As of now, the key distribution rate in quantum cryptography is determined not by fundamental limitations but by the technology level, or more specifically, by the time it takes an avalanche photodiode to revert to the initial state upon recording a photon, and by effects.

In the classical case, when a signal is described by a time function $x(t)$, the number of information bits transferable via a channel with a finite frequency bandwidth is, according to the famous Kotel'nikov sampling theorem proven in 1933 [49] (see the Supplement to N V Kotel'nikova's report in this issue), determined by the number of independent degrees of freedom of the signal, in whose value it is possible to encode the information transmitted. In our digital age, the sampling theory 'operates' in any facility that processes or transmits information in a digital form.

A classical signal with a finite frequency band is described by a time function $x(t)$. In a finite time interval $(-T, T)$, the signal $x(t)$ is, as first shown by Kotel'nikov [49], defined by $2WT$ degrees of freedom in the sense that in the expansion in terms of the orthogonal system of functions:

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

it would suffice to restrict the series to $2WT$ terms, for which

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

For basis functions $\theta_n(t)$, Kotel'nikov employed the so-called reference functions [49]

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

The basis of reference functions possesses a remarkable property: the expansion coefficients x_n in terms of this basis are equal to the values of the signal $x(t)$ itself at the reference points in time. This has the following implication: to describe a continuous signal at any point in time it would suffice to know its values at only $2WT$ points in time.

Below we will conveniently employ other basis functions. The number of these functions localized primarily in the window $(-T, T)$ remains the same in this case. Moreover, these functions also emerge in the quantum case, where they play the part of single-particle amplitudes (wave functions) for photons which are most strongly localized in the time window $(-T, T)$.

The orthogonality of basis functions with the carrier in a finite frequency band W leads to the condition

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

The basis functions are orthogonal if they satisfy the following integral equation

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

The eigenvalues depend only on the product WT and form an infinite series

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

The degree of localization of the nth function squared in the time window $(-T, T)$ is determined by the eigenvalue

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

The integral equation (9) defines the so-called prolate spheroidal functions [50]. The eigenvalues possess the remarkable property that for large WT ($WT \gg 1$) they break up into two groups: one with numbers $n < 2WT$, for which $\lambda_n(WT) \approx 1$, and the other with numbers $n > 2WT$, for which $\lambda_n(WT) \approx 0$. The passage from one behavior to the other occupies a domain which measures $\approx \ln(4\pi WT)$ in number, i.e., for any $\varepsilon > 0$, one has

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

This signifies that for large WT there exist no more than $2WT(1-\varepsilon)$ orthogonal (distinguishable) functions whose contribution to the temporal window $(-T, T)$ tends to unity. When use is made of more than $2WT(1+\varepsilon)$ degrees of freedom, among them there will be states which make a vanishingly small contribution to the temporal window $(-T, T)$. For large WT, the signal $x(t)$ in a finite frequency band is described on a finite time interval by no more than $2WT$ independent (orthogonal and distinguishable) degrees of freedom and may by defined by $2WT$ independent expansion coefficients x_n.

When a classical source with a finite frequency band W generates signals localized in the time window $(-T, T)$ in such a way that the expansion coefficients are prescribed in accordance with a given probability distribution $p(x_n)$ on the set of these coefficients x_n (the values of signal amplitudes), the source entropy is defined by the quantity

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

Furthermore, when these signals are transmitted via a perfect (noise-free) physical communication channel, for instance, having the same transmission frequency band W, the source entropy (12) coincides in essence with the mutual information between the input and output of this communication channel. Then, the transmission capacity per unit time (source + physical communication channel + receiver) is defined as

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

We will need the following qualitative considerations to compare the classical and quantum cases. In the framework of classical physics there are no formal prohibitions against variations in the expansion coefficients x_n [the amplitudes of orthogonal basis functions $\theta_n(t)$] with an arbitrarily small discreteness (continuously). Since the classical signal intensity x_n^2, for instance, for an electromagnetic field, in every separate mode $\theta_n(t)$ is, correct to a factor $\approx \hbar W$, the number of photons in this mode, changes in signal level may take place with a finite discreteness. To encode information into x_n values requires at least two values ($x_n^2 \propto N_{\max}$, $N_{\max}$ is the highest number of possible x_n^2 values). The total number of different values for all modes equals $(\sqrt{N_{\max}})^{2WT}$. If every value is selected with equal probability, the source entropy (12) is given by

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

The transmission capacity (8) per unit time for the lowest signal level ($N_{\max} = 2$) is defined as

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

Formula (15), *which is in essence an alternative representation of Kotel'nikov's sampling theorem, defines the amount of information in bits per one degree of freedom that can be transmitted per unit time*.

Strictly speaking, the formulas are inapplicable when the mode occupation numbers are small.

In the subsequent discussion our concern will be with the transmission capacity in the single-photon regime (the mode occupation numbers are equal to unity). It is precisely this quantity that will define the key generation rate in quantum cryptography via a channel with a finite frequency band W.

The above reasoning was needed to qualitatively compare the classical and quantum cases. Our task will actually reduce to calculating for a source with a finite frequency band W the number of possible orthogonal multiphoton states localized in the time window $(-T, T)$. First we consider single-photon states at the source output, which then travel in one direction ($k > 0$) and have a carrier in a finite frequency band W ($k \in [0, W]$). The polarization degrees of freedom will be ignored in the encoding into different forms of state amplitudes, again for the sake of a closer analogy with the classical case. For simplicity of calculations we put $c = \hbar = 1$. Then we have

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

where $\varphi(k, k)$ ($k > 0$) and $\varphi(\tau)$ are the respective amplitudes of a single-photon packet in the momentum and spatio-temporal representations:

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

For a massless field, $\tau = x - t$ depends only on the difference between the coordinate and time; and so if a measurement result was obtained in the neighborhood of a point x at an instant of time t, the same result may be obtained at a point x' at the instant of time $t' = t + (x' - x)$. Below, when mentioning a time window, we will bear in mind that $(-T, T)$ signifies $[-(x-t), (x-t)]$.

We have to select the amplitude (wave function) of a single-photon packet with a carrier in a finite frequency band W in such a way as to maximize its normalization in the spatio-temporal domain, namely, in the $(-T, T)$ window. Formally, the degree of localization is described by the measurement in this window. Any measurement on the single-photon packet made in the temporal window is described by expansion of unity in the single-particle sub-

space, which is of the form

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

In view of expressions (12) and (13), the operator corresponding to the temporal window $(-T, T)$ is represented as

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

The functions $\theta_n(k)$ themselves are the eigenfunctions of an integral equation which differs from Eqn (9) only in that the integration is performed over the segment $[0, W]$. The number of functions localized in the temporal window $(-T, T)$ will equal WT. The vectors $|\theta_n\rangle$ are in essence the eigenvectors of the operator $I^{(1)}(T)$ — the operator is diagonal in the basis of these vectors. Any measurement on the initial state, when the outcomes in only the temporal window are accessible, is equivalent to measurements on the effective density matrix:

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

Here, we introduced the formal state $|?\rangle$ which is orthogonal to all states and describes the outcomes beyond the temporal window. These outcomes correspond to a situation wherein the equipment did not actuate inside the window whatsoever. Taking into account these outcomes, to which an inconclusive result should be assigned, the effective density matrix possesses a unit spur. For large WT, it is possible to select one of WT orthogonal (distinguishable) single-photon states, which is localized in the $(-T, T)$ window with a probability arbitrarily close to unity [$\lambda_n(WT) \approx 1$] and which possesses in this window the effective density matrix

$$\rho_n(T) = \lambda_n(WT)|\theta_n\rangle\langle\theta_n| + \big(1 - \lambda_n(WT)\big)|?\rangle\langle?|\,, \qquad 1 \leqslant n \leqslant WT\,. \tag{21}$$

Let the source generate in the working temporal window the $(N = WT)$-photon states of the form

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

where the generalized basis vectors are completely symmetric with respect to particle permutations:

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

where the symbol $\{j\}$ implies that summation is performed over all permutations. Let us now construct the $(N = WT)$-photon density matrices. In this case, the occupation number of each single-particle mode is equal to unity. The set of vectors in expression (17) with different indices is made up of the eigenvectors of the operator $I^{(N)}(T)$ in the $(N = WT)$-photon subspace, similarly to the single-photon case. We have

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

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

Let us calculate the number of orthogonal $(N = WT)$-photon states. Were $N = WT$ photons distinguishable, the number of orthogonal $(N = WT)$-photon vectors in the time window $(-T, T)$, localized in it with a nearly unit probability, would be equal to N^N (neglecting the polarization degrees of freedom). By the boson (photon) identity principle, the number of such vectors, which is conveniently denoted as $2^{M(WT)}$, is equal to the number of distributions of $N = WT$ identical particles over $N = WT$ states. Therefore, we arrive at [51]

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

and for large N, in view of the Stirling formula ($N! \approx (N/e)^N\sqrt{2\pi N}$), we obtain

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

Let the source generate with equal probability one of the $2^{M(WT)}$ orthogonal $(N = WT)$-photon states in every working time window. If the source operates for a sufficiently long time, the statistical ensemble, into which classical information may be encoded, is described by the density matrix

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

The von Neumann ensemble entropy is highest for an equiprobable sampling of vectors. The information in the finite time window $(-T, T)$ is extracted from the effective density matrix

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

For large WT, it is impossible to construct a statistical ensemble comprising more than $2^{M(WT)}$ orthogonal $(N = WT)$-photon states. The classical information which may be encoded into the ensemble $\rho\big(M(WT)\big)$ and extracted from $\rho(T)$ (29) is given by the quantity $\chi\big(\rho(T)\big)$ which follows from the fundamental inequality first derived by A S Kholevo (for details, see Ref. [52]). Since the states $|\theta_{n_1};\ldots;\theta_{n_N}\rangle$ and $|?\rangle$ are pure, $\chi\big(\rho(T)\big)$ coincides with the von Neumann entropy

for $\rho(T)$, we find that

$$\begin{aligned}\chi\bigl(\rho(T)\bigr) &= -\mathrm{Tr}\left\{\rho(T)\log\rho(T)\right\}\\ &= -\sum_{n_1,\ldots,n_N}\frac{\lambda_{n_1}(WT)\ldots\lambda_{n_N}(WT)}{2^{M(WT)}}\\ &\quad\times\log\left(\frac{\lambda_{n_1}(WT)\ldots\lambda_{n_N}(WT)}{2^{M(WT)}}\right)\\ &\quad-\sum_{n_1,\ldots,n_N}\left(\frac{1-\lambda_{n_1}(WT)\ldots\lambda_{n_N}(WT)}{2^{M(WT)}}\right)\\ &\quad\times\log\left(\frac{1-\lambda_{n_1}(WT)\ldots\lambda_{n_N}(WT)}{2^{M(WT)}}\right). \qquad (30)\end{aligned}$$

The transmission capacity per unit time is defined by the limit similar to formula (15) applied in the classical case. Taking into account that the contribution of the second sum in expression (30) tends to zero, we obtain

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

During the time window, the source generates $(N=WT)$-photon states in such a way that the number of photons at the source output per unit time equals $\sim W$, and the energy per photon $\sim\hbar W$. Accordingly, the number of photons in the time window $(-T,T)$ is equal to WT (precisely the number and not the average number of photons, because the states $|\theta_{n_1};\ldots;\theta_{n_N}\rangle$ in expression (22) are the eigenvectors of the operator of the number of photons that correspond to the particle eigenvalue $N=WT$).[4] The power at the source output is constant and proportional to $(\hbar W)W$. The source minimality in the quantum case signifies that the number of orthogonal single-particle amplitudes $\theta_n(t)$, which make up the particle-permutation symmetric $(N=WT)$-photon amplitude, amount to WT, and the number of photons are WT, i.e., the occupation number in terms of an individual single-particle amplitude is equal to 1.

In the classical case, information is encoded into the values of the amplitudes (roughly, into the number of photons) in orthogonal modes, and in the quantum case into different orthogonal multiphoton states [53]. The latter are, by virtue of photon identity, fundamentally entangled inside every temporal window $2T$. This quantum source coding may be regarded as the quantum analog of Kotel'nikov's sampling theorem, when the single-particle mode occupation numbers are brought to the single-photon level.

The surprising thing is that the transmission capacity per unit time per one degree of freedom in the classical case (15), which follows from Kotel'nikov's sampling theorem, 'literally' coincides with the similar transmission capacity in the quantum case (31). However, the ways of encoding turn out to be different in the classical and quantum cases.

In summary, it is pertinent to note that the emergence of new avenues in the realm of confidential information transmission is a natural, logical development of the ideas conceived by the founders of this realm.

References

1. Kotel'nikov V A, Classified Report (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. "Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Funktsiya kheshirovaniya" ("Information technology. Cryptographic information protection. Hash function"), Gosudarstvennyi Standart Rossiiskoi Federatsii (State Standard of the Russian Federation), GOST R 34.11-94 (Introduced 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. Proceedings* (Lecture Notes in Comput. Sci., Vol. 1109, Ed. N Koblitz) (Heidelberg: Springer-Verlag, 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); Molotkov S N *Zh. Eksp. Teor. Fiz.* **114** 526 (1998) [*JETP* **87** 288 (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. Molotkov S N *Zh. Eksp. Teor. Fiz.* **126** 771 (2004) [*JETP* **99** 669 (2004)]

[4] Strictly speaking, by WT is everywhere meant its integral part $[WT]$.

39. Bogolyubov N N, Shirkov D V *Vvedenie v Teoriyu Kvantovannykh Polei* (Introduction to the Theory of Quantized Fields) (Moscow: Nauka, 1973) [Translated into English (New York: John Wiley, 1980)]
40. Landau L D, Peierls R *Z. Phys.* **69** 56 (1931) [Translated into Russian, in Landau L D *Sobranie Trudov* (Collected Works) Vol. 1 (Moscow: Nauka, 1969) p. 56]; *Z. Phys.* **62** 188 (1930) [Translated into Russian, in Landau L D *Sobranie Trudov* (Collected Works) Vol. 1 (Moscow: Nauka, 1969) p. 33]
41. Bohr N, Rosenfeld L *Kgl. Danske Vidensk. Selskab. Math.-Fys. Medd.* **12** (8) 3 (1933) [Translated into English, in *Quantum Theory and Measurement* (Eds J A Wheeler, W H Zurek) (Princeton, NJ: Princeton Univ. Press, 1983) p. 470; translated into Russian, in Bohr N *Sobranie Nauchnykh Trudov* (Collected Scientific Works) Vol. 1 (Moscow: Nauka, 1969) p. 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. Kirzhnits D A *Usp. Fiz. Nauk* **90** 129 (1966) [*Sov. Phys. Usp.* **9** 692 (1967)]
45. Paley R E A C, Wiener N *Fourier Transforms in the Complex Domain* (New York: American Mathematical Society, 1934) [Translated into Russian (Moscow: Nauka, 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. Kotel'nikov V A, in *Vsesoyuznyi Energeticheskii Komitet. Materialy k I Vsesoyuznomy S'ezdu po Voprosam Tekhnicheskoi Rekonstruktsii Dela Svyazi i Razvitiya Slabotochnoi Promyshlennosti* (All-Union Energy Committee. Materials prepared for the I All-Union Congress on the Technical Reconstruction of Communication Facilities and the Progress in Low-Currents Industry) (Moscow: Upravlenie Svyazi RKKA, 1933) pp. 1 – 19; reprint: "O propusknoi sposobnosti 'efira' i provoloki v elektrosvyazi" ("On the transmission capacity of 'ether' and wire in electric communications") (Moscow: Institut Radiotekhniki i Elektroniki MEI (TU), 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.* **44** 99 (1965)
51. Landau L D, Lifshitz E M *Statisticheskaya Fizika* (Statistical Physics) Pt. 1 (Moscow: Fizmatlit, 1995) [Translated into English (Oxford: Pergamon Press, 1980)]
52. Kholevo A S *Problemy Peredachi Informatsii* **8** (1) 63 (1972); **15** (4) 3 (1979) [*Probl. Inf. Transm.* **15** 247 (1980)]; Holevo A S *Usp. Mat. Nauk* **53** (6) 193 (1998) [*Russ. Math. Surv.* **53** 1295 (1998)]; Kholevo A S *Vvedenie v Kvantovuyu Teoriyu Informatsii* (Introduction to Quantum Information Theory) [Ser. Sovremennaya Matematicheskaya Fizika. Problemy i Metody (Modern Mathematical Physics. Problems and Methods) Issue 5] (Moscow: Izd. MTsNMO, 2002)
53. Molotkov S N *Pis'ma Zh. Eksp. Teor. Fiz.* **78** 1087 (2003) [*JETP Lett.* **78** 597 (2003)]

PACS numbers: **01.60.+q**, **84.40.–x**
DOI: 10.1070/PU2006v049n07ABEH006051

V A Kotel'nikov and his role in the development of space radio electronics in our country

B E Chertok

Vladimir Aleksandrovich Kotel'nikov's contribution to astronautics, to space technology in general, and to space radio engineering in particular is so huge that one can elaborate on this subject for a long time and in great detail. Here, I briefly list the main investigations in this area, performed under his supervision and more recently by the school he created. Furthermore, I will enlarge on some of his personal traits as a great scientist, who I met during my work of very many years in this field.

Kotel'nikov and Chertok at a session of the A S Popov Russian Scientific-Technical Society of Radio Engineering, Electronics, and Communications (Moscow, House of Scientists, May 2003).

The matter is that Kotel'nikov quite often reproached me for drawing him into work in the area of astronautics. He would do this very politely and subtly, so that I could not understand whether he was really displeased with this or was paying me a compliment in this way.

Everything commenced when Stalin approved on 13 May 1946 the historic resolution on the creation of the rocket branch of industry, engineering, and science in the Soviet Union.

In line with this resolution, despite the hard postwar time the country was enduring, base institutions were established and were growing quickly. In particular, they established a leading research institute for rocket technology, the Scientific Research Institute of the Ministry of Armaments in Podlipki, which went down in history as NII-88, the now universally known Central Scientific Research Institute of Machine Building (TsNIIMash in Russ. abbr.), and the S P Korolev Rocket and Space Corporation (RKK) 'Energiya'. I was Deputy Chief Engineer responsible for control systems.

One fine day, early in April 1947, the President of the USSR Academy of Sciences Sergei Ivanovich Vavilov came to the Institute to familiarize himself with its work. He was that kind of scientist who realized that a breakthrough in this new area called for combining the efforts of industry and academic science with the potentialities of personnel of higher education establishments.

Vavilov arrived at NII-88 with Rector of the Moscow Power Engineering Institute (MEI in Russ. abbr.) Valeriya Alekseevna Golubtsova rather than with a retinue of academic scientists.

The meeting of Vavilov and Golubtsova with the governing body of NII-88, in which I participated, marked the beginning of the process of drawing academic scientists and the scientists from institutes of higher education in a new area of human activity — rocket and space exploration.

One of the outcomes of the utmost significance of this meeting was drawing Vladimir Aleksandrovich Kotel'nikov into creative activity in the area of rocket technology.

On familiarizing himself with the problems which then called for the active participation of scientists of different expertise, Vavilov came up with the idea of establishing

V A Kotel'nikov and B E Chertok with a group of staff members and guests of the Special Design Bureau (OKB) of MEI. Sitting in the first row (from left to right) are M E Novikov, M N Meshkov, A L Zinov'ev, A F Bogomolov, K A Pobedonostsev, Kotel'nikov, and Chertok (Moscow, OKB MEI, 1997).

within the Academy a specialized institute — which was to become the Institute of Space Research (IKI) — and promised to oblige academic institutes to directly participate in this NII-88 activity.

Golubtsova in turn suggested that I — Deputy Chief Engineer of NII-88, a former student and postgraduate student of MEI — should come to my native institute and tell the scientists there about our problems.

Already the next day (one could not afford to linger in those days) I went to MEI. There assembled a group of scientists, maybe the Scientific Council, with Golubtsova herself presiding over the meeting. I outlined the main problems we were facing, although we lacked the understanding of what these problems consisted in, because the business was still early in the making. The next day Golubtsova called me once again and I found myself in a group, among which was Kotel'nikov as the supervisor and Head of the Chair of Fundamentals of Radio Engineering. And then I told them what was most important to us at that time — to be able to continuously monitor rocket parameters in real time by radio engineering aids. Attempts to do this with the help of conventional air-defense radar had not met with success. It was either that the radar measurements were insufficiently precise or that they were basically unsuitable for the parameters of motion of the rockets launched.

Only 10 days after our meeting in Golubtsova's study, on 27 April 1947 the Government passed a resolution, which was approved by Stalin, about setting up at MEI a top-secret Special Sector for carrying out specialized research in the interests of jet armament. So prompt and efficient a reaction was impressive even to us, who were accustomed to timely decisions by the Government.

Kotel'nikov was appointed scientific leader of the works of the Special Sector.

At that time Kotel'nikov was the Dean of the Radio Engineering Department at MEI and the Head of the Chair of Fundamentals of Radio Engineering. It was not until January of 1947 that he defended his doctoral dissertation. However, during the war with Hitlerite Germany in 1943 he was awarded a First Class Stalin Prize, and in 1946 a second First Class Stalin Prize, for the development of special communication systems. At that time, Kotel'nikov was regarded as belonging to the generation of young scientists in the field of radio engineering. He had gained the recognition of the scientific community not only for his secret inventions; he had developed the theoretical foundations of information conveying and showed practical ways of using them. Back in 1933 he published the so-called sampling theorem which proved to be the key element of digital communication technologies. The gist of Kotel'nikov's theorem is that it predicts the conditions when the initial signal of an information transmitter may be recovered error-free from the values of discrete samples. He was the first to show that analogue information may be transmitted by pulses, to state it in modern terms, in a digital code and may be recovered upon transmission. Kotel'nikov became well known to the radio engineering and communication community after the construction of the theory of potential noise immunity. This was the subject of his thesis for Doctorate of Sciences defended in 1947.

Kotel'nikov's 'involvement' in space radio engineering commenced with issuing the Government's Resolution on establishing the Special Sector at MEI. This was precisely the reason we met; later on, we would meet dozens of times, and he would say in jest that I had involved him in this affair. His activity in this area during subsequent years was really exceptionally fruitful, both in the volume and the content of what he contributed as a personality and a scientist. Sometimes his mere presence and participation in the work, even without inventing anything new, seemed to be a breath of fresh air in situations where the problem had to be completely revised.

The young team of the MEI Special Sector rallied round Kotel'nikov and worked with great enthusiasm. To his historical credit, the Sector turned into a scientific school. In essence, it was precisely he, Kotel'nikov, who laid the groundwork for and set up the now widely known Special Design Bureau (OKB in Russ. abbr.) at MEI — a powerful and highly qualified organization which designs and makes radio-engineering systems intended for missiles and spacecraft.

Kotel'nikov entered the closed community of rocketeers, which was led by S P Korolev, as a scientist and engineer. He shared with us, rocketeers, the difficulties of the first years of life in the proving ground, and the conditions were such that we literally 'slept under a common overcoat'. Kotel'nikov quickly gained authority over worldly-wise combatant generals and chief designers. His sense of humor and inexhaustible optimism would smooth over tensions between chief designers in situations where missile launches failed. The participation of Kotel'nikov and his collaborators was so substantial that both the work and flight tests could no longer be thought of without the systems developed by the MEI Special Sector and, more recently, without the equipment which was designed by the OKB MEI and then went into major serial production. All the first flights, which went down in the annals of space rocket technology and underlay the priority of our country, were made with the inevitable use of radioengineering devices created by Kotel'nikov's school. The case in point is rocket-borne and ground-based radioengineering equipment which monitors the flight of a rocket and its trajectory, as well as providing an impression of the spacecraft orbit in real time, not to mention, which is very important, remote measuring equipment which continuously transmits to the Earth the values of all the parameters of interest to both the developers and those who operate the spacecraft.

Kotel'nikov achieved independence from the industrial ministries in the production of the systems under development; at MEI he set up an experimental workshop — subsequently a plant with a closed cycle. They had to make their equipment and systems in cut-throat competition with powerful industrial organizations for the right to equip the first intercontinental rockets and spacecrafts. Nowadays it is quite often said that there was no competition in our previous system, our former economy. Nothing of the kind: there was competition, maybe even more severe than in the so-called free-market economy. Because industrial ministries believed that it was their exclusive right to develop systems of this kind. In particular, the Ministry of Industry of Communication Facilities and the Ministries of Radio Engineering and Electronics insisted on that. And now, some special-purpose department, an OKB at a higher education establishment! Everybody knew and respected Kotel'nikov, but he was subordinate to the Minister of Higher Education, and this aroused intense jealousy. And there were many committees, in which I had to participate, to decide whose design was to be put into operation and added to the armory. Kotel'nikov's school won all these contests despite the departmental pressure.

The first systems developed by Kotel'nikov and his colleagues for rocket technology were 'Indikator-D' and 'Indikator-T'. The first R-2 rockets of Chief Designer Korolev were equipped with these systems in flight tests beginning in 1950.

The Indikator-D system enabled precise recovery for the first time of the rocket trajectory from the observations of ground-based radio posts.

Indikator-T was the first radio-telemetric system made at MEI. In 1953, a start was made on batch production of rocket-borne equipment for the radio monitoring of the trajectories of rocket flights. In 1955, a phase-metric Irtysh system was made for monitoring orbits.

The subsequent Rubin and Almaz modifications of external trajectory measuring systems were made in large batches and were an obligatory constituent in the flight tests of all types of rockets and the majority of spacecraft.

In the early 1950s, Kotel'nikov's team developed the famous radio-telemetric Tral system. This system outstripped the level of the corresponding foreign and domestic systems by no less than 10 years. In the conditions of extremely limited component types, which lagged behind the American one, they made an efficient system using a time-pulse code and ingenious circuit-technical solutions which ensured high reliability. On-board Trals were produced in large quantities. The Tral system was the main tool in the elaboration of the first intercontinental missile R-7 and crewed space vehicles, as well as the flight tests of the basic missiles of our nuclear-missile shield. Dozens of ground-based radio posts were constructed on the territory of the Soviet Union, which were united in a single control-measuring complex. The telemetric Tral stations and orbit control Kama stations, which were developed by the MEI Special Sector and quantity-produced by industry, were obligatory equipment in these posts.

In 1957, the telemetric system developed by MEI was first launched in space in the second artificial Earth satellite; for the third artificial satellite, Kotel'nikov's team developed a complex of trajectory and telemetric measurements.

In 1953, the academic community elected Vladimir Aleksandrovich Kotel'nikov a Full Member — an Academician — of the USSR Academy of Sciences, foregoing the traditional stage of Corresponding Member. He was appointed Deputy Director of the newly established academic Institute of Radioengineering and Electronics (IRE). In 1954, Academician Kotel'nikov superseded Academician Aksel' Ivanovich Berg as Director of this Institute. In 1955, he had to leave the post of Chief Designer at MEI Special Sector. The engineering scientific and technical school of MEI was subsequently headed by Academician-to-be Aleksei Fedorovich Bogomolov. The magnificent creative team formed by Kotel'nikov continued its work in the Special Design Bureau at MEI, established by the governmental resolution on the basis of the Sector. In 1961, OKB MEI was decorated with the Order of the Red Banner of Labor for participation in the creation and launch of the first crewed space vehicle 'Vostok' with the cosmonaut Yurii Gagarin. OKB MEI Chief Designer Bogomolov became a full member of Korolev's

Council of Chief Designers, and later of Yangel's and Chelomei's ones. The team of OKB MEI also became famous for the development of high-efficiency ground-based antennas and relaying stations for space communication systems and television. In all, 160 antenna systems were constructed on the territory of the USSR and abroad, which enabled millions of people to make use of space communications and television. In 1950 – 1954, Kotel'nikov, in collaboration with MEI Assistant Professor A M Nikolaev, wrote a brilliant two-volume work *Osnovy Radiotekhniki* (*Basics of Radio Engineering*). Prior to his election to the Academy of Sciences, Kotel'nikov, who as scientific leader of the Special Sector was always overloaded with rocket – space problems, retained the post of Dean of the Radio Engineering Department and continued his pedagogical activity as the Head of the Chair of Fundamentals of Radio Engineering.

The Institute of Radioengineering and Electronics of the USSR Academy of Sciences, which Kotel'nikov supervised until 1987, gathered the cream of the crop of the radioelectronic scientific community of the Soviet Union. There, basic research was conducted in the most important areas of radio engineering and electronics.

At IRE, Kotel'nikov pioneered a new avenue of space research: planetary radiolocation and investigations of planetary radio emission. The radar of Venus, Mercury, Mars, and Jupiter was carried out under his supervision. In 1964, he was awarded a Lenin Prize for this work.

On Kotel'nikov's initiative and under his scientific supervision, an extremely intricate radio engineering complex was brought into existence, which comprised high-power transmitters, large narrow-beam antennas, high-sensitivity receivers, and a sophisticated system of automated processing of planetary measurements.

During his time of supervising IRE, Kotel'nikov laid the foundations of radio-engineering planetology.

Kotel'nikov came up with the idea of using the scientific, technical, and industrial potential of domestic radio engineering and cosmonautics for the cartography of Venus. The basic ideas and techniques of this unique experiment were elaborated at IRE, the Institute of Applied Mathematics of the USSR Academy of Sciences, and OKB MEI under Kotel'nikov's scientific supervision.

OKB MEI developed the radar equipment for the Venera-15 and Venera-16 interplanetary stations which were made by the G N Babakin Research Center.

Two of the Soviet Union's largest antennas were equipped to receive and record information on Earth. One of them, with a mirror 70 m in diameter, is now abroad; the other, 64 m in diameter, is located near the Medvezh'i Ozera near Moscow and is the property of OKB MEI and is a source of pride. In 1983 – 1984, with the aid of the radar equipment mounted aboard the Venera-15 and Venera-16 interplanetary stations, for the first time in history it was possible to accomplish the cartography of the planetary surface of Venus shielded by its opaque atmosphere. The experience gained in that experiment permitted developing a side survey radar and an ultrabroad-range radiometric complex for the Priroda module of the orbital Mir station.

In a brief report it is impossible to show the wealth of radio-space problems which were solved with the creative contribution by Kotel'nikov. An atlas of the Venus surface, edited by Kotel'nikov, was made in 1989. Hundreds of scientists and engineers from several dozen organizations participated in this interplanetary experiment. Academician Kotel'nikov proved in practice how efficient the concerted effort of the institutions of higher education and of the Academy of Sciences can be. An excellent example is provided by the activities of OKB MEI and the IRE of the USSR Academy of Sciences, which gained worldwide recognition. From 1969 to 1988, Kotel'nikov was Vice-President of the USSR Academy of Sciences, and First Vice-President from 1975. While filling this post, he made a huge contribution to the formation of governmental policy in the development of the most important areas of science.

Although Kotel'nikov was no longer a member of the Council of Chief Designers as earlier when he was the Chief Designer of the MEI Special Sector, he would often render assistance when serious problems arose. A lot of purely radar problems had to be solved in the course of spacecraft operation. The corresponding equipment is extremely sophisticated, so that high reliability is hard to achieve. Sometimes there occur irregular situations, breakdowns, etc. This is especially dangerous in the case of crewed systems, say, when a failure occurs in the transport – orbital station approach-and-docking system. In these cases, the Military Industrial Committee under the Council of Ministers immediately set up an emergency commission. They addressed the Academy of Sciences President M V Keldysh: "Cooperation of the Academy of Sciences is required; whom do you include on this commission?" And, of course, Kotel'nikov was included. I quite often had to meet him during the work of these commissions. He was characterized by and helpful in the following: he tried to quench the debate on the 'who is to blame' subject and, above all, to thoroughly examine the physical essence of the system and grasp the physics of the failure. He suggested that this should be elucidated. And, as a rule, this was possible to do. It is worth noting that Kotel'nikov had an exceptional intuition. Sometimes I was astonished at how promptly he, not knowing the full story of the design, found, if not the very cause in detail, at least the guiding idea which had to be followed to understand the cause of the failure that had occurred. Together we would quickly hit upon the way to remedy the problems occurring.

A substantial part of his scientific and organizational activity was devoted to cosmonautics. For many years he presided over the 'Radioastronomy' Scientific Council of the USSR Academy of Sciences and the Council for International Cooperation in the Area of Investigation and Use of Space. The supervisor of the Interkosmos Council was entrusted not only with the scientific and technical tasks, but also with the social and political tasks of international cooperation in the area of cosmonautics. At the present time it would be hard to recollect the list of different committees and expert commissions which Kotel'nikov was president of or a member of. In one such commission in 1989 I was entrusted, together with Kotel'nikov, with the task of drawing the French science and industry into the deployment of a global satellite communication system and, directly, television on the basis of employing our Energiya giant rocket-carrier. During negotiations in Paris, the French side did not exhibit much enthusiasm and, to unburden ourselves, Kotel'nikov and I went to the Louvre. In the Louvre, I not only enjoyed contemplating the great works of art, but was also surprised by Kotel'nikov's erudition, with his advice on what to see and where. He explained that attempts to make the rounds of the whole Louvre would result in having nothing to recollect at a later time. Even in this field, seemingly distant from his activities, he could spot and contemplate the masterpieces of human

genius and in doing this gain, as I witnessed, emotional satisfaction.

For his scientific activity Kotel'nikov was honored with many awards — governmental, domestic academic, and international. In 2000, Professor Bruce Eisenstein (USA) thus praised the scientific merits of Kotel'nikov: ''Academician Kotel'nikov is an outstanding hero of the present. His merit is world-wide recognized. We are in the presence of a giant of radio-engineering thought, one who made some of the most significant contributions to the development of radio communications.'' From 1973 to 1980, Kotel'nikov was Chairman of the Supreme Soviet of the Russian Soviet Federative Socialist Republic (RSFSR). Today this should be remembered also for the reason that in those days the state estimated at its true worth science as a productive force, which ensured the economic and defense might of the country.

In connection with the 95th birthday of Academician Vladimir Aleksandrovich Kotel'nikov, on 21 September 2003 the President of the Russian Federation Vladimir V Putin signed a decree on decorating him with the First Class Order 'For Service to the Homeland'. He came to be Russia's fourth holder of this order.

At present, the scientific and technical school created by Academician Kotel'nikov is actively introducing the newest radio-engineering products into the cosmonautics world.

We have the right to pride ourselves in being members, together with this outstanding Russian scientist, of the Russian Association of Members of the International Academy of Astronautics.