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.