Декабрь 2025 г. *Том 195, № 12*

УСПЕХИ ФИЗИЧЕСКИХ НАУК

К 80-летию ПОБЕДЫ В ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЕ

КОНФЕРЕНЦИИ И СИМПОЗИУМЫ

Труды академика В.А. Котельникова (период 1932 – 1946 гг.) — основа научных направлений шифрования, криптографии и потенциальной помехоустойчивости *

С.А. Никитов, Л.Е. Назаров

Рассмотрены научные и прикладные исследования академика В.А. Котельникова в предвоенный и военный период (1932 – 1946 гг.) по разработке и созданию систем шифрованной телефонной связи, по созданию криптографически стойкой аппаратуры на основе исследований по дискретизации речевых сигналов, по созданию теории потенциальной помехоустойчивости при передаче информации по каналам с шумами.

Ключевые слова: шифрование, криптография, помехоустойчивость

PACS numbers: **01.60.+q**, **01.65.+g**, **89.70.–a** DOI: https://doi.org/10.3367/UFNr.2025.05.039981

Содержание

1. Введение

Невозможно переоценить вклад поколения советских учёных и инженеров в дело Победы над фашизмом в Великой Отечественной войне. В этом ряду достойное место занимает академик РАН Владимир Александрович Котельников — выдающийся учёный, организатор, педагог, общественный деятель. Его научные труды обогатили мировую науку, стали классическим фундаментом создания и развития новых научных направлений [1].

В.А. Котельников считается одним из основоположников теории и практических приложений статистической радиотехники, радиофизики, криптографии, инфор-

С.А. Никитов [(1, *)], **Л.Е. Назаров** [(2, †)]
[(1)] Институт радиотехники и электроники им. В.А. Котельникова РАН, ул. Моховая 11, корп. 7, 125009 Москва, Российская Федерация
[(2)] Фрязинский филиал Института радиотехники и электроники им. В.А. Котельникова РАН, пл. Введенского 1, 141190 г. Фрязино, Московская обл., Российская Федерация
E-mail: [(*)] nikitov@cplire.ru, [(†)] levnaz2018@mail.ru

Статья поступила 14 июля 2025 г.

Владимир Александрович Котельников

* Обзор написан на основе доклада, представленного к Научной сессии Отделения физических наук Российской академии наук (ОФН РАН) **"К 80-летию Великой Победы: вклад отечественных физиков"** 14 мая 2025 г. (см. *УФН* **195** (12) ii (2025)).

матики, радиолокационной астрономии, широкомасштабного исследования космического пространства [1 – 3]. Результаты, полученные при создании и развитии этих направлений, актуальны и востребованы для решения современных проблем цифровой обработки сигналов, организации надёжной и высокоскоростной передачи информации по радиолиниям с шумами с использованием адаптивных методов передачи/приёма, развития отечественной криптографии.

Среди широкого круга его научных и прикладных достижений особое место занимают направления по разработке и созданию систем шифрованной связи [3], по созданию криптографически стойкой аппаратуры на основе исследований по дискретизации речевых сигналов [4, 5], по созданию теории потенциальной помехоустойчивости при передаче информации по каналам с шумами [6], выполненные в предвоенное и военное время (1932 – 1946 гг.).

Следует отметить параллельные разработки иностранных учёных, выполнявших исследования по аналогичным направлениям, в частности, исследования американского математика К. Шеннона (1916 – 2001 гг.) [7]. К. Шеннон занимался вопросами теоретической стойкости криптографических шифров и создания теории пропускной способности каналов передачи с шумами. По результатам исследований в 1946 г. представлен закрытый отчёт "Математическая теория криптографии". В 1948 г. напечатана его книга *Математическая теория связи* [8], в которой изложены переоткрытые с существенной временно́й задержкой основные результаты В.А. Котельникова в части представления аналоговых сигналов в дискретном виде и оптимальной обработки сигналов при передаче по каналам с шумами.

В статье рассматриваются выполненные в этот период научные и прикладные исследования В.А. Котельникова по приведённым направлениям, составляющие фундаментальные основы для различных областей науки.

2. Основные вехи творческой биографии В.А. Котельникова

В.А. Котельников родился в 1908 г. в городе Казани. Его дед, Пётр Иванович Котельников (1809 – 1879), — математик, профессор Казанского университета. Отец, Александр Петрович Котельников (1865 – 1944), — математик, механик, также профессор Казанского университета [3].

Творческий путь В.А. Котельникова начался с 1927 г. После окончания 1-го курса МВТУ им. Н.Э. Баумана работал в Нижегородской радиолаборатории. Это было время, когда радиотехника была на начальном этапе своего создания и развития.

1930 г. — окончание Московского энергетического института (МЭИ), получение диплома инженера-электрика (специальность "радиотехника"), распределение в Научно-исследовательский институт (НИИ) связи Красной армии. Далее учёба в аспирантуре МЭИ (1931 – 1933 гг.), параллельно работа в НИИ связи Народного комиссариата связи. В этот период им выполнен анализ проблемы "дружных" замираний сигналов при их многолучевом распространении по радиолиниям коротковолнового (КВ) диапазона.

В 1932 г. выполнена фундаментальная работа «О пропускной способности "эфира" и проволоки в электросвязи» (теорема отсчётов Котельникова).

В 1938 г. В.А. Котельникову присуждена учёная степень кандидата технических наук без очной защиты диссертации, в 1946 г. — защита докторской диссертации по тематике потенциальной помехоустойчивости при передаче сигналов по каналам с шумами и создания нового научного направления — статистической радиотехники.

В 1953 г. избран действительным членом Академии наук СССР, минуя степень члена-корреспондента.

1954 – 1987 гг. В.А. Котельников являлся директором Института радиотехники и электроники РАН, оставаясь почётным директором до конца жизни.

Ниже приведён более детальный обзор результатов научной деятельности В.А. Котельникова, которые представляют базис теоретической разработки и технического исполнения информационных систем различного назначения, например, современных систем подвижной связи сотового формата наземного и спутникового базирования. Основной состав этих информационных систем включает шифрование речи, криптографическое преобразование информационного потока, а также приём сигналов с учётом искажений за счёт шумов с применением оптимальной обработки с целью обеспечения потенциальной помехоустойчивости.

3. Направление аналогового шифрования речи

Исходная задача аналогового шифрования речи решалась при разработке и технической реализации радиолинии КВ-диапазона Москва – Хабаровск (1936 – 1941 гг.), действие которой включает многолучевое распространение сигналов за счёт отражения от околоземной ионосферы и от земной поверхности. На рисунке 1 дан пример двухлучевого распространения сигналов с выхода передающего устройства (Прд) по радиолинии КВ-диапазона.

На вход приёмника (Прм) поступает реализация $\hat{s}(t)$ в виде суммы l копий сигналов

$$s(A_i, t_i, t) = A_i \cos\left(2\pi f(t + t_i) + \varphi(t)\right)$$

с различными амплитудами A_i и временны́ми задержками t_i (возможно до $l = 2 \ldots 6$ лучей распространения)

$$\hat{s}(t) = \sum_{i=1}^{l} s(A_i, t_i, t)\,, \qquad (1)$$

f, $\varphi(t)$ — несущая частота и фаза передаваемых сигналов.

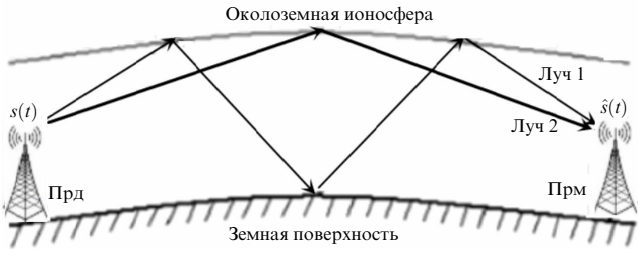

Рис. 1. Схема двухлучевого (луч 1, луч 2) распространения сигналов по ионосферной радиолинии КВ-диапазона (Прд — передающее устройство, Прм — приёмное устройство).

За счёт деструктивного сложения речевых сигналов $s(A_i, t_i, t)$ с частотной полосой в интервале (0,3...3 кГц) наблюдаются "дружные" (частотно-неселективные) замирания амплитуд сигналов $\hat{s}(t)$, снижающие надёжность телефонных переговоров по этим каналам [9, 10].

Выше отмечен выполненный В.А. Котельниковым анализ каналов передачи этого типа. Для компенсации искажающего влияния многолучевого канала разработан метод на основе разнесения p приёмных антенн (Прм) для временно́й декорреляции сигналов $\hat{s}_p(t)$ и их комбинации при формировании обрабатываемой реализации при приёме, например, выбор сигнала из множества $\hat{s}_p(t)$ с максимальной амплитудой [9 – 13].

Одновременно при разработке и создании этой информационной системы решалась проблема шифрования телефонной речи для защиты от несанкционированного прослушивания, что для В.А. Котельникова являлось новой прикладной областью. Шифрование речевой информации аналогового типа обеспечивалось специальными устройствами — маскираторами. Известный в то время подход при создании устройств такого типа был основан на инверсии частотного спектра $S(f)$ речевого сигнала с дополнительной модуляцией несущей высокой частотой $f_т$ [3]. Этот подход и соответствующая аппаратура не могли обеспечить требуемую защиту содержания перехваченных переговоров.

В сложных условиях военного времени в лаборатории В.А. Котельникова был разработан и испытан принципиально новый телефонный шифратор частотно-временно́го (мозаичного) типа (аппаратура "Соболь П"). На рисунке 2 приведена его функциональная схема. Шифратор "Соболь П" выполняет частотно-инверсное преобразование речевого сигнала $s(t)$ (взаимное перемещение низких и высоких частот сигнала относительно центральной частоты f_0), представление преобразованного сигнала временны́ми отрезками длительностью не менее 100 мс и их случайную перестановку и дополнительную модуляцию результирующего сигнала высокой частотой $f_т$ в диапазоне 10,6 – 38,4 кГц (ВЧ-модуляция). Приёмное устройство выполняет последовательность обратных операций.

В 1942 г. опытные образцы аппарата шифрования "Соболь П" приняты на вооружение. Для технических средств данного времени дешифрация двумерного (частота – время) информационного потока представлялась крайне трудной задачей. Командованию Германии был представлен доклад о невозможности прослушивания и раскрытия шифрованных речевых телефонных сообщений [3].

Аппаратура шифрования "Соболь П" использовалась для связи Ставки Верховного Главнокомандования с делегацией СССР во время подписания капитуляции Германии в мае 1945 г. [3]. Аппараты аналогового шифрования "Соболь П" продолжительное время работали на линиях Москва – Хельсинки, Москва – Париж, Москва – Вена при проведении переговоров по заключению мирных договоров по окончании Второй мировой войны. Свидетельством высокого качества работы этой аппаратуры является тот факт, что вследствие невозможности прослушивания телефонных переговоров применялся метод их разрушения посредством создания помех в каналах передачи [3].

За работу по созданию и совершенствованию аппаратуры "Соболь П" коллектив авторов отмечен Сталинской премией 1-й степени (1943 г.), в 1946 г. В.А. Котельникову была присуждена вторая Сталинская премия 1-й степени [3].

4. Направление дискретного шифрования речи

С развитием технических средств обработки сигналов (анализаторы спектра речевых сигналов и др.) требовалось дальнейшее повышение эффективности шифрования речи. Для развития этого направления В.А. Котельниковым сформулирован принципиально новый подход — дискретное шифрование речи.

Суть предложенного подхода дискретного шифрования речи заключается в использовании передачи телеграфного типа, включающей [2, 3]:

— аналого-цифровое преобразование речевого сигнала, т.е. дискретизацию аналогового речевого сигнала с использованием теоремы отсчётов, квантование и кодирование дискретных отсчётов;

— криптографическое кодирование цифровых отсчётов речевого сигнала.

На рисунке 3 приведена блок-схема метода дискретного шифрования речи, предложенного В.А. Котельниковым (1941 г.).

Блок n-разрядного аналого-цифрового преобразования (АЦП) в составе передающего устройства осуществляет дискретизацию речевых сигналов в соответствии с теоремой отсчётов Котельникова, квантование дискретных отсчётов на 2^n уровней и их кодирование [13]. Каждый из n двоичных разрядов АЦП суммируется в поле $GF(2)$ с двоичными символами криптографической последовательности [14, 15], результирующие двоичные символы поступают на модулятор сигналов $\hat{s}(t)$, передаваемых по каналу. В приёмном устройстве выполняются вычислительные операции, обратные операциям передающего устройства, выход блока цифро-аналогового преобразования (ЦАП) $\hat{s}(t)$ является выходом системы с дискретным шифрованием речи [13].

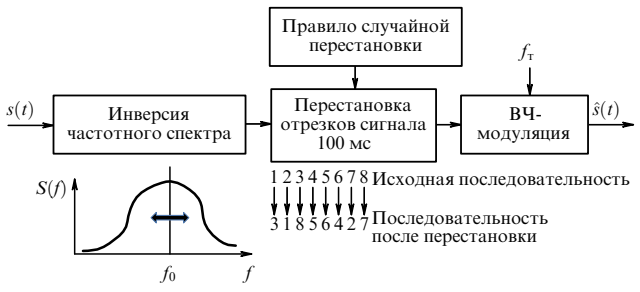

Рис. 2. Функциональная схема аналогового шифрования "Соболь П".

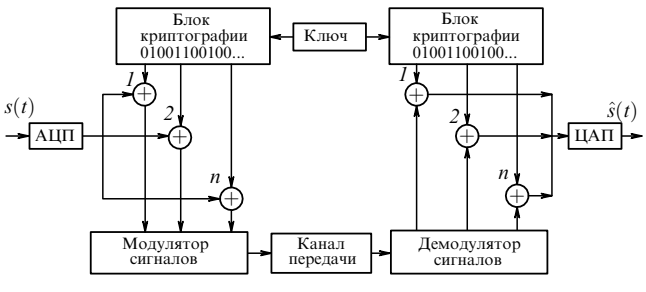

Рис. 3. Блок-схема дискретного шифрования речевого сигнала.

Анализ теоремы отсчётов Котельникова. Блок АЦП реализует представление в цифровом формате аналоговых сигналов $s(t)$ с ограниченной частотной полосой W аппроксимационным рядом Котельникова $\hat{s}(t)$ с временны́ми отсчётами $s(i\Delta t)$ с частотой дискретизации $f_д \geqslant 2W$ (период дискретизации $\Delta t \leqslant 1/2W$) [10, 13]

$$\hat{s}(t) = \sum_{i=-\infty}^{\infty} s(i\Delta t)\,\mathrm{sinc}\left(\frac{\pi(t - i\Delta t)}{\Delta t}\right), \qquad (2)$$

где $\mathrm{sinc}\,(x) = \sin(x)/x$.

В литературе отмечаются особенности аппроксимационного ряда (2):

— медленная сходимость ряда [16];

— представление сигналов $\hat{s}(t)$ суммированием дискретных отсчётов с весовыми коэффициентами входит в класс плохо обусловленных задач [17];

— приближённое вычисление сигналов $\hat{s}(t)$ вследствие ограничения длительности сигналов $s(t)$ [16];

— сходимость аппроксимационного ряда в евклидовой метрике L_2 [18, 19].

Несмотря на эти особенности, ряд Котельникова является базисом цифровой обработки сигналов и одним из основных фундаментов цифровой техники, интенсивно развиваемых в последние десятилетия [13, 20].

Теория вокодера. Требуемая информационная скорость потока с выхода дискретного шифратора, реализованного в соответствии с блок-схемой на рис. 3, достаточно высока, что является ограничивающим условием для его технической реализации. Существенное понижение требуемой скорости потока дискретного шифратора (на порядок и более) при практически эквивалентном качестве передачи обеспечивается при использовании вокодера — устройства сжатия частотной полосы речевого сигнала [20]. Исследование и разработка вокодера инициированы В.А. Котельниковым в 1941 г., однако с началом войны работы по совершенствованию вокодера были приостановлены и возобновлены лишь в 1948 г. [3]. Исходная информационная скорость дискретного шифратора, выполненного с участием В.А. Котельникова, равнялась 64 кбит $с^{-1}$, с включением вокодера требуемая информационная скорость снизилась до 4,8 кбит $с^{-1}$ [3].

Основу современной теории вокодера составляет модель линейного предсказания CELP (Code Exited Linear Prediction) на основе авторегрессионного соотношения [21–23]

$$\hat{s}(n) = \sum_{i=1}^{N} a_i s(n-i) + qw(n)\,. \qquad (3)$$

Значение дискретного отсчёта $\hat{s}(n)$ речевого сигнала вычисляется с использованием предыдущих N отсчётов $s(n-i)$ с весовыми коэффициентами a_i и текущего значения основного тона $w(n)$ с амплитудой q (рекомендованное значение $N = 10$, частота дискретизации 10 кГц [21]).

Особенностью голосового аппарата является практическая стационарность статистических характеристик случайного процесса речевого сигнала $s(n)$ для интервалов времени до 10–40 мс. С использованием этого свойства разработаны вычислительные процедуры оценивания весовых коэффициентов **a** и амплитуды основного тона q [22, 23].

На вход приёмного устройства передаются лишь квантованные и кодированные значения вектора весовых коэффициентов **a** и характеристики основного тона, что позволяет существенно сократить требуемую частотную полосу канала передачи W' по отношению к исходной частотной полосе W.

Критерии криптографической стойкости шифрования. В это же время проблема криптографического кодирования рассматривалась американским математиком К. Шенноном. Его исследования по данной тематике приведены в отчёте "A Mathematical Theory of Cryptography" (1946 г.) и опубликованы в статье (1948 г.) [8].

На основе результатов исследований, выполненных В.А. Котельниковым и К. Шенноном, определены критерии криптографической стойкости дискретного шифрования:

а) ключ блока криптографии известен лишь легитимным пользователям;

б) длина ключа не меньше длины сообщения;

в) ключ генерируется случайным образом;

г) ключ используется в режиме одноразового блокнота.

При выполнении указанных критериев передаваемое и зашифрованное сообщения статистически независимы. Основная проблема при реализации криптографических систем с ключами в режиме одноразового блокнота заключается в выполнении критерия а. Один из перспективных подходов к решению этой проблемы основан на методах квантовых вычислений, интенсивно исследуемых и разрабатываемых в настоящее время [24, 25].

Для эффективной работы информационных систем различного назначения, включая системы связи с аналоговым и дискретным шифрованием речи, требуются решения относительно выбора сигналов $s(t)$ и их обработки при приёме с учётом искажающего влияния физических каналов передачи [26]. Ниже приведены результаты исследований В.А. Котельникова по данным направлениям.

5. Теория потенциальной помехоустойчивости

К осени 1946 г. В.А. Котельников подготовил диссертационную работу на соискание учёной степени доктора наук по теме "Теория потенциальной помехоустойчивости", в 1956 г. текст диссертации опубликован в виде книги [6]. Данная работа является основой научного направления статистической радиотехники, включающего теорию проверки статистических гипотез относительно приёма и различения цифровых сигналов с различными видами манипуляций (фазовая, частотная) и теорию оценивания параметров сигналов (частоты, начальной фазы, амплитуды, времени обнаружения и др.) [9, 11, 12, 16, 19, 26, 27]. Используемый подход при решении комплекса рассматриваемых задач на основе применения методов теории вероятностей и математической статистики являлся совершенно новым для исследователей и инженеров того времени, в опубликованной книге [6] приведена единственная ссылка.

Направление статистической радиотехники имеет связь с теорией передачи дискретных сообщений (общая блок-схема приведена на рис. 3) относительно использования и анализа цифровых сигналов $s(t)$ и определения алгоритмов обработки реализаций с вы-

хода канала передачи, приводящих к оптимальному выбору решений с учётом статистических критериев качества [26].

Общая формулировка задачи потенциальной помехоустойчивости заключается в следующем: для реализации $x(t)$ с выхода канала передачи, задаваемой соотношением

$$x(t) = \mu s(\boldsymbol{\lambda}, t) + n(t)\,, \quad t \in [0, T]\,, \tag{4}$$

требуется определить правило отображения $x(t) \to \to s(\boldsymbol{\lambda}_0, t)$, минимизирующего искажающее действие аддитивного шума $n(t)$ [6, 26]. Здесь μ — коэффициент передачи канала, полагаемый известным; $\boldsymbol{\lambda}$ — информационный вектор. Для систем передачи дискретных сообщений, использующих ансамбль цифровых сигналов $s(\lambda_i, t)$ с объёмом M, значения элементов информационного вектора дискретны, $i = 1, 2, \ldots, M$. Для сигналов с непрерывными информационными параметрами соответствующие элементы вектора $\boldsymbol{\lambda}$ входят в состав подмножеств L евклидова пространства [6, 26].

Приём сигналов в системах передачи дискретных сообщений представляет проверку статистических гипотез [19, 26]. В этом случае при условии равновероятности передачи сигналов $s(\lambda_i, t)$ оптимальное правило приёма, реализующее статистический критерий минимального байесовского риска, формулируется следующим образом: присутствует сигнал $s(\lambda_m, t)$, если для всех $j \neq m$ выполняется условие [26]

$$\int_0^T V_{mj}(t) x(t)\,\mathrm{d}t \geqslant \frac{1}{2}\int_0^T V_{mj}(t)\big[s(\lambda_m, t) + s(\lambda_j, t)\big]\,\mathrm{d}t\,, \tag{5}$$

где $V_{mj}(t)$ — решение неоднородного линейного интегрального уравнения

$$\int_0^T B(t-u) V_{mj}(u)\,\mathrm{d}u = s(\lambda_m, t) - s(\lambda_j, t)\,, \quad t \in [0, T]\,, \tag{6}$$

где $B(t)$ — корреляционная функция аддитивного канального шума.

Условие (5) эквивалентно вычислению апостериорных вероятностей $\Pr\left(s(\lambda_i|x(t))\right)$, $i = 1, 2, \ldots, M$ и выбору максимального значения для λ_m.

В диссертационной работе рассмотрена модель канала передачи с аддитивным белым гауссовым шумом (АБГШ) $n(t)$ с односторонней спектральной плотностью N_0. Эта модель не лишена недостатков, в частности, корреляционная функция шума представляется обобщённой дельта-функцией $B(t) = (N_0/2)\delta(t)$ [26], т.е. мощность шума неограниченна. Вместе с тем предложенная модель принята научным сообществом в качестве базовой и интенсивно используется при анализе информационных систем различного назначения (системы связи, навигации, радиолокации, др.) [16, 19, 26, 27].

Для модели канала АБГШ решение интегрального уравнения (6) имеет вид $V_{mj}(t) = (2/N_0)[s(\lambda_m, t) - s(\lambda_j, t)]$. В этом случае условие (5) приводится к следующему виду [6, 26]:

$$\int_0^T \big[\mu s(\lambda_j, t) - x(t)\big]^2\,\mathrm{d}t \geqslant \int_0^T \big[\mu s(\lambda_m, t) - x(t)\big]^2\,\mathrm{d}t\,. \tag{7}$$

На рисунке 4 приведена блок-схема алгоритма (7) оптимального приёма (различения) равновероятных дискретных сигналов $s(\lambda_j, t)$, $j = 1, 2, \ldots, M$ для канала АБГШ. Принимается решение относительно передаваемого сигнала с параметром λ_m при условии минимума евклидова расстояния между $\mu s(\lambda_m, t)$ и $x(t)$.

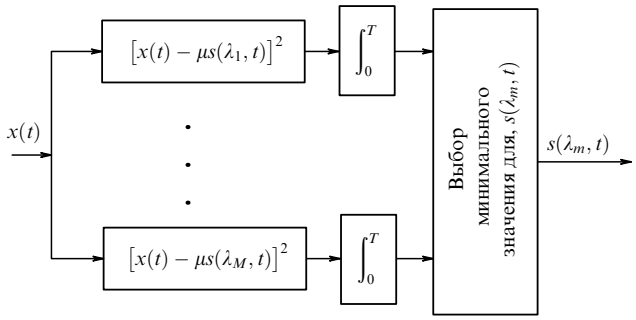

Рис. 4. Блок-схема алгоритма оптимального приёма (7) равновероятных дискретных сигналов $s(\lambda_j, t)$, $j = 1, 2, \ldots, M$, для канала АБГШ.

В.А. Котельниковым рассмотрено обобщение модели стационарного аддитивного гауссова шума с частотно-зависимой спектральной плотностью мощности $N(f)$ ("окрашенный" шум) и с соответствующей корреляционной функцией $B(t)$ [6]. В этом случае предложено применять алгоритм оптимального приёма (7) с включением обеляющего (инверсного) фильтра для реализации $x(t)$ на входе решающего устройства. Развитие такого подхода представляет собой вычислительный алгоритм обработки входной реализации $x(t)$, задаваемый соотношениями (5) на основе решения неоднородного линейного интегрального уравнения (6).

Рассмотрение "окрашенного" шума в диссертационной работе составило основу самостоятельного научного направления по разработке моделей для ряда более сложных каналов передачи со свойствами частотно-селективного замирания, с дисперсионными свойствами (ионосферные, атмосферные, гидролокационные каналы передачи) [10, 16, 19, 26, 28].

Оценки непрерывных параметров m-размерного вектора $\boldsymbol{\lambda}$ сигналов $s(\boldsymbol{\lambda}, t)$ с использованием критерия максимального правдоподобия задаются как решения системы уравнений [26]

$$\int_0^T \frac{\partial}{\partial\lambda_i} V(\boldsymbol{\lambda}, t)\big[x(t) - s(\boldsymbol{\lambda}, t)\big]\,\mathrm{d}t = 0\,, \quad i = 1, \ldots, m\,, \tag{8}$$

где $V(\boldsymbol{\lambda}, t)$ — решение неоднородного линейного интегрального уравнения

$$\int_0^T B(t, u) V(\boldsymbol{\lambda}, u)\,\mathrm{d}u = s(\boldsymbol{\lambda}, t)\,, \quad t \in [0, T]\,. \tag{9}$$

Для модели канала АБГШ, рассмотренной в диссертационной работе В.А. Котельникова, решение $V(\boldsymbol{\lambda}, t) = (2/N_0)s(\boldsymbol{\lambda}, t)$ и система уравнений (8) упрощается

$$\int_0^T \frac{\partial}{\partial\lambda_i} s(\boldsymbol{\lambda}, t)\big[x(t) - s(\boldsymbol{\lambda}, t)\big]\,\mathrm{d}t = 0\,, \quad i = 1, \ldots, m\,. \tag{10}$$

В диссертационной работе В.А. Котельникова выполнен анализ передачи дискретных сообщений по каналу с аддитивным белым гауссовым шумом с использованием ряда сигналов. В частности, для ансамблей ортогональных сигналов с объёмом M доказано выражение относи-

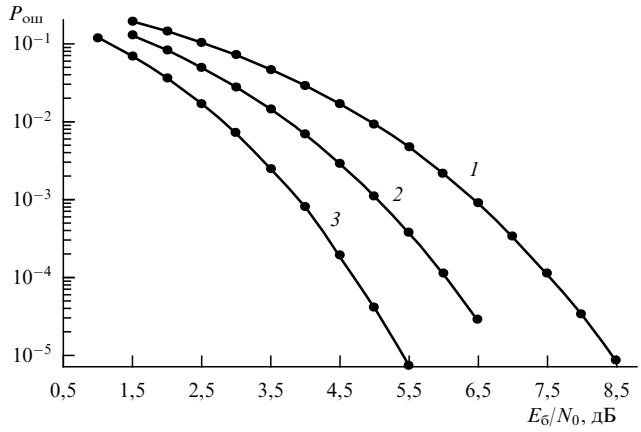

Рис. 5. Зависимости вероятности ошибки $P_{\text{ош}}$ от отношения $E_б/N_0$ для ансамблей ортогональных сигналов с объёмом $M = 8$ (кривая *1*), $M = 32$ (кривая *2*), $M = 256$ (кривая *3*).

тельно вероятности ошибочного приёма $P_{\text{ош}}$ при использовании алгоритма (7) [6]

$$P_{\text{ош}} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left(-\frac{x^2}{2}\right) \times \left[1 - F\left(x + \sqrt{2E_б \log_2 M/N_0}\right)\right]^{M-1} \mathrm{d}x, \qquad (11)$$

где

$$F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp\left(-\frac{y^2}{2}\right) \mathrm{d}y,$$

$E_б$ — энергия сигналов на бит.

На рисунке 5 даны зависимости вероятности ошибки $P_{\text{ош}}$ от отношения $E_б/N_0$, вычисленные с использованием соотношения (11) для ансамблей ортогональных сигналов с объёмом $M = 8$ (кривая *1*), $M = 32$ (кривая *2*) и $M = 256$ (кривая *3*). Видно, что вероятность $P_{\text{ош}}$ является монотонно убывающей функцией от M при постоянном значении $E_б/N_0$.

Замечательным свойством рассматриваемых сигналов при увеличении объёма M является пороговый эффект относительно $P_{\text{ош}}$ [27]

$$\underset{M\to\infty}{P_{\text{ош}}} = \begin{cases} 1, & \dfrac{E_б}{N_0} < \ln 2, \\ 0, & \dfrac{E_б}{N_0} > \ln 2, \end{cases} \qquad (12)$$

т.е. использование ансамблей ортогональных сигналов обеспечивает безошибочную передачу при условии $M \to \infty$ и ограничении $E_б/N_0 > \ln 2$, при этом требуется неограниченная частотная полоса канала [27].

Предельное соотношение (12) имеет особое значение для теории информации, определяющей пропускную способность Шеннона C и возможность организации безошибочной передачи с информационной скоростью, достигающей C [7, 8],

$$C = W \log_2 \left(1 + \frac{S}{N_0 W}\right) \text{ [бит с}^{-1}\text{]}, \qquad (13)$$

S — мощность сигнала, W — частотная полоса канала.

Следует отметить, что в работе К. Шеннона не даётся конструктивных рекомендаций о выборе сигналов, использование которых обеспечивает достижение вероятностно-энергетических характеристик, определяемых пропускной способностью C.

При доказательстве соотношения относительно пропускной способности C (13) К. Шеннон (1948 г.) переоткрыл теорему об отсчётах (позднее В.А. Котельникова на 16 лет) и основные положения теории потенциальной помехоустойчивости В.А. Котельникова.

При увеличении частотной полосы W выражение (13) имеет вид

$$\underset{W\to\infty}{C} = \frac{E_б}{N_0 \ln 2}, \qquad (14)$$

оно определяет минимальное значение сигнал/шум $E_б/N_0 > \ln 2$, при котором теоретически возможна безошибочная передача информации без ограничений на используемые сигналы с частотной полосой W.

Пороговые эффекты относительно параметра сигнал/шум, задаваемого соотношениями (12) и (14), тождественны. Вместе с тем в работе В.А. Котельникова предложен конкретный класс сигналов, с использованием которых теоретически возможна безошибочная передача информации по каналам с предельным отношением сигнал/шум. Таким образом, при разработке теории потенциальной помехоустойчивости В.А. Котельниковым сделаны начальные шаги по созданию теории информации, развитой впоследствии К. Шенноном [8, 9]. Разрабатываемое в настоящее время направление корректирующего кодирования, применяемое при разработке систем передачи дискретных сообщений с характеристиками, близкими к характеристикам пропускной способности для каналов передачи, основано на применении методов теории потенциальной помехоустойчивости [9, 10, 16, 19].

6. Заключение

Научные и прикладные работы В.А. Котельникова по аналоговому и дискретному шифрованию речи, по развитию отечественной криптографии и созданию теории потенциальной помехоустойчивости внесли весомый вклад в Победу, составляют основу многих научных направлений и востребованы современным научным сообществом.

За научные заслуги В.А. Котельников имеет 31 государственную награду, среди которых две Государственные премии (Сталинские премии 1-й степени). Знаменательно, что его именем названа малая планета № 2726 и имя "Владимир Котельников" присвоено судну размагничивания ВМФ РФ.

Международный научный фонд Эдуарда Рейна (Германия) в 1999 г. наградил В.А. Котельникова за впервые доказанную в аспекте коммуникационных технологий теорему отсчётов (в англоязычной научной литературе известна как теорема Уиттекера – Котельникова – Шеннона). Это свидетельствует об уважении и международном признании вклада Владимира Александровича в науку.

Список литературы

1. "К 100-летию со дня рождения академика В.А. Котельникова (Совместная научная сессия Отделения физических наук Российской академии наук и Отделения нанотехнологий и информационных технологий Российской академии наук, 17 сентября

2008 г.)" *УФН* **179** 201–224 (2009); "Commemoration of the centenary of the birth of Academician V A Kotel'nikov (Joint scientific session of the Physical Sciences Division of the Russian Academy of Sciences and the Division of Nanotechnologies and Information Technologies of the Russian Academy of Sciences, 17 September 2008)" *Phys. Usp.* **52** 183–205 (2009)
2. *В.А. Котельников. Судьба, охватившая век* В 2 т., Т. 1 *Воспоминания коллег* (Сост. Н В Котельникова) (М.: Физматлит, 2011)
3. *В.А. Котельников. Судьба, охватившая век* В 2 т., Т. 2 *Н.В. Котельникова об отце* (Под ред. А С Прохорова) (М.: Физматлит, 2011)
4. Котельников В А, в сб. *Всесоюзный энергетический комитет. Материалы к I Всесоюзному съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности, 1932, Москва* (М.: Управление связи РККА, 1933) с. 1
5. Котельников В А *УФН* **176** 762 (2006); Kotel'nikov V A *Phys. Usp.* **49** 736 (2006)
6. Котельников В А *Теория потенциальной помехоустойчивости* (М.– Л.: Госэнергоиздат, 1956)
7. Шеннон К *Работы по теории информации и кибернетике* (М.: ИЛ, 1963)
8. Shannon C E *Bell Syst. Tech. J.* **27** 379 (1948)
9. Галлагер Р *Теория информации и надежная связь* (М.: Советское радио, 1974); Пер. с англ. яз.: Gallager R G *Information Theory and Reliable Communication* (New York: Wiley, 1968)
10. Скляр Б *Цифровая связь. Теоретические основы и практическое применение* (М.: Вильямс, 2003); Пер. с англ. яз.: Sklar B *Digital Communications: Fundamentals and Applications* (Upper Saddle River, NJ: Prentice-Hall PTR, 2001)
11. Миддлтон Д *Введение в статистическую теорию связи* Т. 2 (М.: Советское радио, 1962); Пер. с англ. яз.: Middleton D *An Introduction to Statistical Communication Theory* (New York: McGraw-Hill, 1960)
12. Миддлтон Д *Введение в статистическую теорию связи* Т. 1 (М.: Советское радио, 1961) оригинал на англ. яз. см. [11]
13. Рабинер Л, Гоулд Б *Теория и применение цифровой обработки сигналов* (М.: Мир, 1978); Пер. с англ. яз.: Rabiner L R, Gold B *Theory and Application of Digital Signal Processing* (Englewood Cliffs, NJ: Prentice-Hall, 1975)
14. Шнайер Б *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си* (М.: Триумф, 2002); Пер. с англ. яз.: Schneier B *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (New York: Wiley, 1996)
15. Сачков В Н *УФН* **176** 775 (2006); Sachkov V N *Phys. Usp.* **49** 748 (2006)
16. Proakis J G, Salehi M *Digital Communications* 5th ed. (Boston: McGraw-Hill, Higher Education, 2008)
17. Тихонов А Н, Арсенин В Я *Методы решения некорректных задач* 2-е изд., перераб. и доп. (М.: Наука, 1979); Пер. на англ. яз. 1-го изд.: Tikhonov A N, Arsenin V Ya *Solutions of Ill-Posed Problems* (Washington, DC: Halsted Press, 1977)
18. Колмогоров А Н, Фомин С В *Элементы теории функций и функционального анализа* (М.: Наука, 1972); Пер. на англ. яз.: Kolmogorov A N, Fomin S V *Introductory Real Analysis* (New York: Dover Publ., 1975)
19. Балакришнан А В и др. *Теория связи* (М.: Связь, 1972); Пер. с англ. яз.: Balakrishnan A V (Ed.) *Advances in Communication Systems* (New York: Academic Press, 1965)
20. Арманд Н А *УФН* **176** 770 (2006); Armand N A *Phys. Usp.* **49** 744 (2006)
21. Gibson J D "Speech compression" *Information* **7** (2) 32 (2016) DOI:10.3390/info7020032
22. Markel J D, Gray A H (Jr.) *Linear Prediction of Speech* (Berlin: Springer-Verlag, 1976)
23. Makhoul J *Proc. IEEE* **63** 561 (1975)
24. Nielsen M A, Chuang I L *Quantum Computation and Quantum Information* 10th anniversary ed. (Cambridge: Cambridge Univ. Press, 2010)
25. Молотков С Н *УФН* **176** 777 (2006); Molotkov S N *Phys. Usp.* **49** 750 (2006)
26. Левин Б Р *Теоретические основы статистической радиотехники* Кн. 2 (М.: Советское радио, 1975)
27. Витерби Э Д *Принципы когерентной связи* (М.: Советское радио, 1970); Пер. с англ. яз.: Viterbi A J *Principles of Coherent Communication* (New York: McGraw-Hill, 1966)
28. Назаров Л Е, Батанов В В *Радиотехника и электроника* **67** 1133 (2022); Nazarov L E, Batanov V V *J. Commun. Technol. Electron.* **67** 1388 (2022)

Academician V.A. Kotelnikov's works (1932–1946) — the basis of research fields in encryption, cryptography, and potential noise immunity *

S.A. Nikitov [(1, *)], **L.E. Nazarov** [(2, †)]
[(1)] *Kotelnikov Institute of Radioengineering and Electronics, Russian Academy of Sciences, ul. Mokhovaya 11, kor. 7, 125009 Moscow, Russian Federation*
[(2)] *Fryazino Branch of the Kotelnikov Institute of Radioengineering and Electronics, Russian Academy of Sciences, pl. Vvedenskogo 1, 141190 Fryazino, Moscow region, Russian Federation*
E-mail: [(*)] *nikitov@cplire.ru*, [(†)] *levnaz2018@mail.ru*

We consider the scientific and applied research work of Academician V.A. Kotelnikov in the pre-war and wartime periods (1932–1946) focused on the development and creation of encrypted telephone communication systems, the creation of cryptographically secure equipment based on research in the sampling of speech signals, and the development of a theory of potential noise immunity when transmitting information through noisy channels.

* This review is based on the report presented at the Scientific Session of the Physical Sciences Division of the Russian Academy of Sciences (PSD RAS) "On the 80th Anniversary of the Great Victory: Contribution of Russian Physicists" on May 14, 2025 (see *Uspekhi Fizicheskikh Nauk* **195** (12) ii (2025); *Physics–Uspekhi* **68** (12) (2025)).

Keywords: encryption, cryptography, noise immunity

PACS numbers: **01.60.+q**, **01.65.+g**, **89.70.–a**

Bibliography — 28 references *Received 14 July 2025*

Uspekhi Fizicheskikh Nauk **195** (12) 1282–1288 (2025) *Physics–Uspekhi* **68** (12) (2025)

DOI: https://doi.org/10.3367/UFNr.2025.05.039981 DOI: https://doi.org/10.3367/UFNe.2025.05.039981