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

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

В.А. Котельников и отечественная шифрованная связь

В.Н. Сачков

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

С.Н. Молотков

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

Сначала кратко коснемся истории вопроса.

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

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

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

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

Неформально, шифр является абсолютно стойким, если:

1) ключ секретен — известен только легитимным пользователям;

2) длина ключа в битах не меньше длины сообщения;

3) ключ случаен;

4) ключ используется только один раз.

В этом случае зашифрованное сообщение статистически независимо от исходного сообщения.

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

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

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

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

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

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

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