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 30-х годах прошлого столетия 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 временные перестановки 100-миллисекундных отрезков речи. Управление частотными и временными 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-временных 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. Другими словами, любое открытое сообщение может быть зашифровано в любое шифрованное. Для «совершенной зашифровки» требуется, чтобы число различных шифрующих отображений, называемых шифрами, было не меньше числа возможных открытых сообщений, сами шифры не повторялись, и допускался любой закон их чередования.

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.

Из вероятностной модели, определяющей «совершенную секретность», вытекают требования, аналогичные требованиям «совершенной зашифровки».

В частности, требуется, чтобы число шифрующих отображений было бы не меньше числа открытых сообщений и вероятности таких отображений все должны быть отличны от нуля.

Таким образом, отмечая идейную близость понятий «совершенной секретности» и «совершенной зашифровки» следует признать, что модель стойкого шифрования К. Шеннона является математическим уточнением пионерской модели В.А. Котельникова.

Следует отметить, что системы шифрования, удовлетворяющие свойствам как «совершенной зашифровки», так и «совершенной секретности», существуют и используются в практике засекречивания информации. 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 50-х годах прошлого столетия. 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 50-х годов прошлого века 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 профилей, преемником которого сейчас является Институт криптографии, связи и информатики Академии ФСБ России. 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 90-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 научных работников, имеющих ученые степени докторов и кандидатов наук и являющихся высококвалифицированными специалистами в своей области знаний.

В этих условиях с одобрения Президента Российской академии наук Указом Президента РФ в 1992 г. была создана государственная Академия криптографии Российской Федерации как государственное научное учреждение, осуществляющее фундаментальные и важнейшие прикладные научные исследования в области криптографии и связанных с нею областях. 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 16 томов, в которых опубликованы статьи как членов Академии криптографии, так 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 ФСБ России в 2006 г. были учреждены две стипендии имени В.А. Котельникова.

В Академии криптографии свято чтят 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.