ОСНОВОПОЛОЖНИК ОТЕЧЕСТВЕННОЙ ЗАСЕКРЕЧЕННОЙ ТЕЛЕФОННОЙ СВЯЗИ

Н. Н. Андреев, А. П. Петерсон, К. В. Прянишников, А. В. Старовойтов

Радиотехника, 1998 г., № 8, с. 8–12

Андреев Николай Николаевич, генерал-лейтенант,вице-президент Академии криптографии РФ

Необходимость обеспечения конфиденциальности телефонных переговоров привела несколько десятилетий назад к появлению телефонных шифраторов — устройств преобразования речевых сигналов в форму, существенно затрудняющую противнику, перехватившему телефонный сигнал, восстановление смысла разговора. В СССР у истока разработок таких систем стоял Владимир Александрович Котельников.

Простейшим преобразованием, затрудняющим восстановление смысла речевого сообщения по перехваченному телефонному сигналу, является инверсия спектра его частот. Речевой сигнал, подвергнутый такому преобразованию, становится неразборчивым, а на приеме аналогичная инверсия обеспечивает восстановление исходного сигнала. Аппаратно инверсия спектра реализуется с использованием модулятора и фильтра. Недостаток такого преобразования — возможность несанкционированного восстановления исходного сигнала с применением аналогичного инвертора. Использование модулятора с переменной частотой заметно усложняет преобразование и саму аппаратуру защиты информации, но не представляет серьезных затруднений для квалифицированного специалиста. Существенное усложнение преобразований возможно за счет использования перестановок отрезков речевого сигнала во времени.

Первый телефонный шифратор, сочетающий в себе частотные преобразования речевого сигнала с перестановками его отрезков по времени, разработан под руководством В. А. Котельникова. Этот шифратор был крупным шагом вперед по сравнению с существовавшей тогда техникой засекречивания телефонных переговоров. Реализуемые им преобразования речевого сигнала были динамическими, т. е. менялись во времени по случайному закону. Для того времени вскрытие таких преобразований представляло весьма серьезные затруднения даже для квалифицированных специалистов. Для разработки телефонного шифратора с высокой степенью стойкости в 1939 г. в Центральном научно-исследовательском институте связи была организована специальная лаборатория, численность которой в 1940 г. была 30 человек. Основной состав лаборатории был укомплектован молодыми специалистами — выпускниками Московского электротехнического института

связи. Главным конструктором и идейным организатором этих работ был В. А. Котельников.

В связи с тем, что разрабатывалась принципиально новая аппаратура, сразу возникло много научных и технических проблем. В частности, необходимо было определить параметры шифрующих преобразований таким образом, чтобы, с одной стороны, обеспечить их достаточную сложность, а с другой — сохранить качество речи при передаче по телефонным каналам и каналам армейских радиостанций.

Большие трудности возникли при создании блока запись-воспроизведение, необходимого для реализации перестановок отрезков речевого сигнала во времени. Магнитная запись речи в то время находилась на начальной ступени развития, поэтому применить что-либо готовое было невозможно. После длительных экспериментов был выбран вариант записи на ободе диска, изготовленного из специальной стали.

Начало войны заставило прервать научно-исследовательскую работу и перейти к проектированию образцов аппаратуры. За период с июня по октябрь 1941 г. при очень интенсивной, иногда почти круглосуточной работе удалось сконструировать и частично изготовить отдельные блоки аппаратуры. Однако 15 октября 1941 г. после прорыва немцев под Москвой было принято решение об эвакуации лаборатории в Уфу. К сожалению, при подготовке к эвакуации была уничтожена большая часть конструкторской документации, что в дальнейшем задержало продолжение этих работ. Эвакуация проводилась в три этапа в течение октября — ноября 1941 г. В Уфе лаборатория была размещена в эвакуированном еще летом 1941 г. Ленинградском институте № 56, работавшем на полную мощность и имевшем хорошо оборудованные производственные цеха. Интенсивная работа лабораториии с помощью института № 56 в производстве позволила к осени 1942 г. разработать, изготовить и отладить два образца аппаратуры, которые были немедленно отправлены на Закавказский фронт для использования в действующей радиосвязи Москва–Тбилиси. Некоторое время это была единственная связь с Москвой ввиду разрушения проводных каналов. Она работала до тех пор, пока не была построена новая проводная линия в обход территорий, занятых в 1942 г. немцами. Одновременно с этим изготавливалась небольшая партия аппаратов, причем изготовление сложного механического узла, включающего шифратор, магнитную запись, синхронный привод, было поручено заводу № 209, расположенному в блокадном Ленинграде. Помощь в освоении узла оказывалась приехавшими на завод разработчиками аппаратуры.

В 1943–1945 гг. аппаратура использовалась в войсках связи действующей армии, а также во время принятия капитуляции Германии для связи нашей делегации с Москвой. За создание аппаратуры В. А. Котельников и группа ведущих разработчиков были удостоены Государственной премии. Эта разработка положила начало развитию целого класса отечественных систем шифрования речи, которые для

своего времени надежно защищали телефонные переговоры от утечки информации.

Усложнение преобразований за счет уменьшения длительности переставляемых отрезков речи и ширины занимаемой ими полосы частот приводит к снижению качества восстановленной на приеме речи и возможно до некоторого предела, который определяется требованиями к качеству речи, а также технологией обработки сигнала. Вместе с тем в последующих разработках отечественных шифраторов удалось добиться довольно сложных преобразований при сохранении приемлемого качества речи. До начала 70-х годов не существовало эффективных алгоритмов дешифрования сообщений, зашифрованных с помощью наиболее сложных систем такого типа, и эти системы широко применялись на различных линиях и сетях связи в СССР. Их достоинствами являются относительно низкая стоимость и способность работать по каналам связи низкого качества, в том числе по коротковолновым. Однако использование такого типа систем непригодно для надежной защиты линий связи.

Альтернативой такому шифрованию, которое условно называют *аналоговым*, является дискретное шифрование. Дело в том, что последовательность букв или цифр можно зашифровывать достаточно надежно, т. е. так, чтобы гарантировать невозможность раскрытия смысла сообщения в течение десятков лет с помощью даже самой современной вычислительной техники с учетом тенденций ее развития.

Известно, что К. Шенон в своем секретном докладе, датированном 1 сентября 1945 г., изложил подходы к построению стойких систем шифрования. Эти результаты были впоследствии рассекречены и опубликованы [2]. Однако мало кому известно, что еще в 1941 г. В. А. Котельниковым сформулированы четкие положения о том, каким требованиям должна удовлетворять математически недешифруемая система, и дано доказательство невозможности ее дешифрования. Для таких систем предполагается, что множество шифруемых сигналов конечно. Поэтому для обеспечения наивысшего уровня конфиденциальности телефонных переговоров необходимо речевой сигнал преобразовать в цифровую последовательность, зашифровать которую уже не представляет принципиальной трудности. Такое преобразование должно допускать восстановление речевого сигнала на приеме с достаточно хорошим качеством.

Следующим шагом на пути к созданию телефонных шифраторов с гарантированной стойкостью была доказанная В. А. Котельниковым «теорема отсчетов», позволившая представить сигнал с ограниченной полосой частот в виде цифровой последовательности [1] [1]). Такое пред-

[1]) Впервые теорема отсчетов опубликована была в 1933 г. в Материалах к I Всесоюзному съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности.

ставление сигнала фактически открыло новую эру в технологии анализа и синтеза сигналов — эру цифровой обработки сигналов.

Созданный в начале 50-х годов телефонный шифратор на основе прямого преобразования речевого сигнала в цифровую форму с помощью импульсно-кодовой модуляции обладал очень высоким качеством речи и осуществлял дискретное шифрование с гарантированной стойкостью. Однако цифровой поток, который он вырабатывал, составлял 64 Кбит/с, поэтому его применение ограничивалось кабельными каналами, способными пропустить цифровой поток такого большого объема.

В октябре 1939 г. в американском акустическом журнале была опубликована статья Х. Дадли с описанием разработанного им аппарата искусственной речи, названного им *вокодер* (vocoder — от английских слов «voice» — голос и «coder» — кодирующее устройство) [3, 4]. Впоследствии это название закрепилось за определенным классом систем синтетической телефонии. Вокодер Дадли воспроизводил мгновенный спектр речевого сигнала. При этом форма сигнала не сохранялась, т. е. нарушались фазовые соотношения между его частотными компонентами при сохранении амплитудных соотношений. Основное достоинство вокодера — возможность сокращенного описания речевого сигнала, что открывало перспективы для цифровой передачи речи по узкополосным каналам связи.

В. А. Котельников оценил потенциальные свойства вокодера как перспективные для разработки на его базе аппаратуры шифрования речи и немедленно организовал работы по созданию аналогичного устройства. Уже в начале 1941 г. в лаборатории работал макет вокодера, построенного в соответствии с данными, приведенными в статье Х. Дадли. Вокодер воспроизводил достаточно разборчивую речь, но весьма низкого качества, совершенно непригодного для использования в аппаратуре связи. К сожалению, с началом войны работы по совершенствованию вокодера были почти полностью прекращены и возобновились в необходимом объеме лишь в 1948 г.

Для передачи цифровых сигналов по различным каналам связи используются специальные устройства — модемы, которые на передаче преобразуют цифровой сигнал — последовательность бит — в аналоговые с переменными параметрами, а на приеме по выделенным параметрам принятых сигналов восстанавливают исходный цифровой поток. При этом основная проблема — ограничение реальной пропускной способности канала связи шириной полосы его частот и помехами в канале. Для передачи речевого сигнала с исходной полосой частот 4 кГц в соответствии с теоремой отсчетов необходима частота дискретизации 8 кГц, при передаче одного отсчета восемью двоичными импульсами объем результирующего цифрового потока составит 64 Кбит/с. Пропускная способность реальных узкополосных каналов существенно меньше 64 Кбит/с, что приводит к необходимости сокращенного описания речевого сигнала, его «сжатия» с информационной

точки зрения. Принципиальная возможность такого сжатия становится очевидной, если сопоставить речь с соответствующим буквенным текстом, для передачи которого требуется менее 50 бит/с [5] при среднем темпе произнесения (80...100 слов/мин). Эта возможность реализуется в вокодерах, хотя до 50 бит/с даже современным вокодерам еще очень далеко. Речь человека состоит из последовательности звуков, представляющих собой основные лингвистические единицы — фонемы, которые можно упрощенно трактовать как акустические эквиваленты букв текста. Длительность фонем колеблется в пределах 10...300 мс. Экспериментально установлено, что речевой сигнал можно охарактеризовать совокупностью переменных параметров, значения которых можно передавать один раз в течение 10...30 мс. Речевой сигнал представляет собой сложный случайный процесс, модель которого можно описать с помощью линейной системы с переменными параметрами [6], имеющей на входе сигнал возбуждения. В качестве модели возбуждения для глухих фрикативных звуков (ф, с, ш и т. п.) используется широкополосный шум, а для вокализованных звуков (а, о, у и т. п.) — квазипериодическая последовательность сигналов с широким спектром, в простейшем случае — одиночных узких импульсов; временной интервал между этими сигналами — квазипериод — называют *периодом основного тона*. Спектр сигнала возбуждения в случае фрикативных звуков равномерен, а в случае вокализованных линейчатый с расстоянием между гармониками, обратным периоду основного тона. Для фрикативных вокализованных звуков (типа ж, з, в) возбуждение смешанное. Модель речевого тракта, являющаяся линейным фильтром с переменными параметрами, описывается огибающей спектра выходного сигнала. Таким образом, результирующий спектр $S(\omega)$ выходного сигнала $s(t)$ является произведением спектров возбуждения $U(\omega)$ и речевого тракта $A(\omega)$

$$S(\omega) = U(\omega)A(\omega).$$

При обработке речевой сигнал разбивают на интервалы анализа — кадры, на каждом их которых вычисляют параметры сигнала возбуждения и речевого тракта. Различные способы описания огибающей спектра порождают варианты вокодеров. Простейший способ — описание с помощью ступенчатой функции — используется в полосном вокодере, который был разработан еще Х. Дадли, и его варианты используются до сих пор. Формантный вокодер описывает спектральные области концентрации энергии — форманты, положение и форма которых фактически определяют фонемы.

Необходимо отметить, что определенные сложности представляет квантование параметров — преобразование последовательности значений параметров речевого сигнала в двоичную последовательность, которая передается с помощью модема по каналу связи. Это преобразование должно учитывать, что искажение значений различных параметров по-разному влияет на качество восстановленного на приеме речево-

го сигнала. В частности, для каждого параметра существует некая оптимальная точность и надежность представления, которая, с одной стороны, не вызывает излишних искажений из-за ошибок квантования и помех в канале, с другой — не требует излишнего расхода бит на передачу значения параметра.

Для принятой стандартной ширины полосы канала около 3 кГц и существующих в реальных каналах искажений и помех скорость передачи модемов составляла 2400 или 4800 бит/с. Для этих скоростей в СССР были разработаны телефонные шифраторы, основанные на вокодерных принципах.

Первая попытка создания в 1941 г. (СССР) макета полосного вокодера Дадли закончилась не совсем удачно из-за низкого качества восстановленной на приеме речи. Причина главным образом заключалась в том, что отсутствовали надежные методы выделения основного тона. Искажения основного тона были неприятными на слух. Научные изыскания привели к созданию так называемых «полувокодеров», которые и нашли первое практическое применение в отечественной шифровальной технике, появившейся в 1950 г. и работавшей на скорости 4500 бит/с. Затем на тех же принципах в 1955 г. была создана аппаратура с улучшенными массогабаритными показателями, за счет использования более современной технологии, на скорость 4800 бит/с. Для повышения качества восстановленной речи в этой аппаратуре низкочастотная часть речевого сигнала передается в непреобразованном виде. Однако даже на скорости 4800 бит/с качество речи остается довольно низким, голос обладает характерными «синтетическими» призвуками. Несмотря на использование передовых для того времени технологий, аппаратура весила сотни килограммов и занимала значительный объем.

Низкое качество отечественных каналов связи привело к необходимости дальнейшего снижения скорости передачи речи. Появление более надежных методов выделения основного тона речевого сигнала позволило использовать принцип полосного вокодера, что дало возможность сократить скорости передачи до 2400 и 1200 бит/с к концу 60-х годов. Однако и качество речи, и массо-габаритные показатели оставляли желать лучшего.

Развитие технологии сжатия речевого сигнала, сдерживаемое до начала 80-х годов отсутствием технических возможностей реализации сколько-нибудь сложных алгоритмов в реальном времени, получило мощный импульс в результате появления специализированных цифровых процессоров обработки сигналов, способных за один такт работы производить операции типа свертки векторов большой размерности, что стимулировало развитие подходов к анализу и синтезу речевых сигналов, использующих такие операции. Наиболее плодотворным оказался подход, использующий модель речевого сигнала на основе ли-

нейной авторегрессии:

$$s(t) = \sum_{r=1}^{n} a(r)s(t-r) + u(t),$$

где $a(r)$ — коэффициенты линейной авторегрессии; n — порядок модели, который варьируется обычно в пределах от 8 до 12; $u(t)$ — обновляющий процесс (роль которого играет сигнал возбуждения).

При этом огибающая спектра речевого сигнала представляется коэффициентами $a(r)$, которые определяются на каждом кадре — интервале анализа из условия минимизации средней квадратической ошибки предсказания. Такие вокодеры получили название липредеров (от английских слов linear prediction — линейное предсказание). Эта модель речевого тракта фактически представляется резонансной системой, и области резонанса соответствуют формантам.

Уже давно обнаружено, что сохранение формы речевого сигнала не является обязательным условием для передачи речи, и в низкоскоростных системах это обстоятельство используется. Однако наилучшее качество синтезированной речи все-таки достигается при сохранении формы речевого сигнала. Устройства и алгоритмы анализа-синтеза речевых сигналов, основанные на этом принципе, называют «кодерами речевой волны». В таких алгоритмах наряду с передачей информации об огибающей спектра кодируется информация о сигналах возбуждения $u(t)$. Такого типа алгоримы являются наиболее совершенными для анализа-синтеза речи, поэтому используются в современных речевых шифраторах. На скорости передачи 9600 бит/с можно достичь качества речи, практически не уступающего исходному, на скорости 4800 бит/с — сохранить его весьма высоким.

Можно констатировать, что развитие технологии шифрования речи и других видов информации в нашей стране и за рубежом в течение всего периода шло практически параллельно, паритет в области шифрования информации с экономически развитыми странами сохраняется до настоящего время.

Федеральное агентство правительственной связи и информации при президенте Российской Федерации активно использует новейшие исследования при внедрении современных информационных технологий. Так, завершена разработка и создаются сети специальной связи на базе телефонной шифровальной аппаратуры нового поколения, обеспечивающей высококачественную передачу речи и надежную защиту информации даже в экстремальных условиях. Аппаратура реализует самые современные методы цифровой обработки речевого сигнала при гарантированной защите информации, ее целостности и подлинности с возможностью аутентификации абонентов, устанавливающих связь.

На этапе разработки этой аппаратуры В. А. Котельников принимает непосредственное участие в развертывании программы работ по ее созданию. Будучи в курсе самых передовых достижений техниче-

ской мысли, он дает практические рекомендации по использованию новейших технологий в разрабатываемой отечественной специальной технике.

Технические параметры речепреобразующих устройств и модемов в современной телефонной шифровальной аппаратуре, ее высокие потребительские качества позволяют устанавливать надежную высококачественную телефонную связь даже для каналов связи общего пользования. При этом процесс эксплуатации аппаратуры предельно упрощен. Развернутые в настоящее время широкомасштабные работы по внедрению современной телефонной аппаратуры нового поколения уже показали возросшую эффективность функционирования сетей правительственной связи, существенный рост услуг, предоставляемых потребителям.

Вместе с тем остается сложная научно-техническая проблема совершенствования телефонных шифраторов, дальнейшего повышения их тактикотехнических характеристик, помехоустойчивости и функциональной устойчивости по отношению к используемым каналам связи. Ее решение потребует проведения объемных научных изысканий, анализа современных методов цифровой обработки сигнала, применения высокопроизводительной вычислительной элементной базы, внедрения научных достижений в различных дисциплинах, включая математику, лингвистику, электронику и др.

Ближайшие перспективы развития телефонных шифраторов обусловлены необходимостью их совершенствования без изменения принципов функционирования, а также увеличения парка этих шифраторов в связи с предстоящим расширением круга их пользователей, включая коммерческие организации. Необходимость работы по коротковолновым каналам требует создания аппаратуры, обеспечивающей высокое качество речи при низких скоростях передачи информации (1200 бит/с). Потребуется достичь постепенной унификации элементов телефонной аппаратуры для их взаимоувязывания в сетях специальной связи без потери качества предоставляемых услуг. Переход на новейшие цифровые процессоры обработки сигналов и на новый технологический уровень предприятий средств связи приведет к снижению массогабаритных характеристик аппаратуры и ее энергопотребления.

Отдаленные перспективы связаны *с* кардинальным снижением скоростей передачи систем синтетической телефонии при сохранении высокого качества синтезированной речи на основе других принципов анализа-синтеза. Повышение эффективности распознавания звуков слитной речи, оценки индивидуальных и эмоциональных характеристик голоса, а также совершенствование элементной базы в дальнейшем должны привести к созданию фонетических вокодеров, способных работать на скоростях 300…400 бит/с. Потребности в таких вокодерах обусловлены возрастающими объемами речевой информации, которую необходимо хранить и передавать по различным каналам связи. Такие вокодеры найдут применение в различных цифровых системах передачи

и хранения речевой информации, в том числе и не использующих шифрования.

История развития телефонной засекреченной связи в России, начало которой положено В. А. Котельниковым, не стоит на месте. На заложенных им теоретических основах базируется современная технология обработки сигналов, что позволяет успешно продвигаться вперед по пути технического прогресса.

Литература

1. *Котельников В. А.* Теория потенциальной помехоустойчивости. — М.: Госэнергоиздат, 1956.
2. *Шенон К.*Работы по теории информации и кибернентике: Пер. с англ. — М.: ИЛ, 1963.
3. *Dudley H. J.* Acoust. Soc. Am. 11, 1939, pp. 166–177.
4. *Dudley H.*The Vocoder. Bell Labs. Record 17, 1939, pp. 122–126.
5. *Флйнаган Дж. Л.* Анализ, синтез и восприятие речи. — М.: Связь, 1968.
6. *Рабинер Л. Р., Шафер Р. В.* Цифровая обработка сигналов. — М.: Радио и связь, 1981.

Поступила
в редакцию 2.04.98 г.