КРИПТОГРАФИЧЕСКИЙ ФРОНТ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ

АКАДЕМИК В.А.КОТЕЛЬНИКОВ И СТАНОВЛЕНИЕ ЗАСЕКРЕЧЕННОЙ ТЕЛЕФОННОЙ СВЯЗИ

Развитие средств связи к началу Великой Отечественной войны обусловило необходимость перехода от медленных систем предварительного шифрования текстовой информации к синхронному линейному засекречиванию телефонных переговоров непосредственно в процессе связи.

Перед войной для защиты отечественных проводных телефонных линий стали использовать так называемую ВЧ-связь (высокочастотную связь). Основная её идея заключалась в том, что по проводам передавался ток высокой частоты, модулированный звуковыми сигналами от мембраны телефона. Этот способ защиты предохранял содержание сообщения только от прямого подслушивания. Подслушивающий воспринимал лишь незначительно искаженный непрерывный писк. Такая защита могла быть преодолена подбором фильтра для «отцеживания» высокой частоты, после чего разговор становился внятно слышным.

Недостатком ВЧ-связи являлось ещё и то, что её воздушные линии располагались, как правило, вблизи железных и шоссейных дорог. Массированные артиллерийские удары или авианалеты противника, направленные на разрушение нашей транспортной инфраструктуры, уничтожали не только дороги, но и идущие вдоль них линии засекреченной связи. Кроме того, техника ВЧ-связи была очень громоздкой и устанавливалась, в основном, в крупных населенных пунктах в административных зданиях НКВД. Ни о какой мобильности связи даже между Ставкой ВГК и Генштабом со штабами фронтов говорить не приходилось.

Заместитель начальника Отдела правительственной связи НКВД СССР И.Я. Воробьев (слева) на Центральной ВЧ-станции

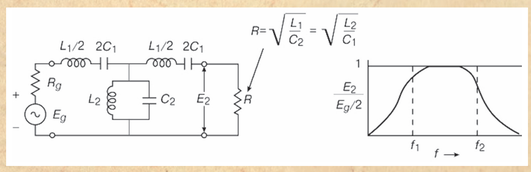
В этих условиях стало актуальным создание особой секретной телефонии, которая обеспечила бы надёжную защиту содержания перехваченного противником телефонного разговора.

Задача была решена коллективом специалистов под руководством начальника лаборатории и главного инженера по радио в Центральном научно-исследовательском институте связи Народного комиссариата почт и телеграфов (НИИС НКПиТ) **Владимира Александровича Котельникова**.

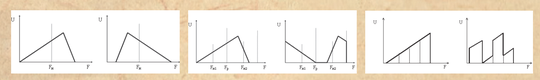
В сложнейших условиях военного времени в лаборатории был разработан и построен принципиально новый телефонный шифратор «мозаичного» типа «Соболь-П», не имевший аналогов в мире.

Шифратор осуществлял частотно-временные («мозаичные») преобразования речевого сигнала.

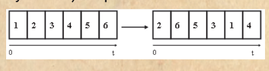
Частотные преобразования заключались в делении сигнала на три — четыре частотных поддиапазона посредством системы полосовых фильтров.



К некоторым из частотных поддиапазонов применялись частотные инверсии. Далее поддиапазоны случайным образом перемешивались.



Сигнал, полученный после частотных преобразований, делился на отрезки по 100 миллисекунд и задерживался для осуществления перемешивания отрезков во времени посредством записи на магнитный барабан. Перемешивание частотно-временных отрезков осуществлялось с помощью специального узла, управлявшегося посредством перфоленты, отверстия в которой проделывались случайным (непредсказуемым) образом.



Описанные преобразования надёжно защищали речевой сигнал не только от непосредственного подслушивания в канале связи, но и от попыток восстановить исходную речь доступными на тот момент техническими средствами и методами.

Уровень безопасности телефонных переговоров, обеспечиваемый аппаратурой «Соболь-П», для своего времени являлся беспрецедентным. По каналам связи, оборудованным аппаратурой «Соболь-П», разрешалась передача совершенно секретных донесений и приказов.

При создании аппаратуры коллективу разработчиков пришлось преодолеть сложности эвакуации. К концу 1941 года, когда Ленинград оказался в блокаде, цех ленинградского завода «Красная заря», где первоначально была организована база производства аппаратуры связи, был экстренно эвакуирован в Уфу. Туда же были переведены сотрудники лаборатории В.А. Котельникова. Здесь был создан завод № 697 Наркомата электропромышленности СССР, на котором к 1942 году были изготовлены первые образцы аппаратуры «Соболь-П». Наиболее сложные механические узлы, магнитные барабаны линии задержки, приходилось производить в блокадном Ленинграде на приборостроительном заводе № 209 им. А.А. Кулакова, обладавшем необходимой производственной базой. Для окончательной наладки шифраторов В.А. Котельников регулярно летал в блокадный город, не раз подвергался при этом вражеским обстрелам.

Готовые аппараты срочно отправляли на фронт. Их настоящее боевое крещение прошло в 1943 году. Ими были оборудованы магистральные радиотелефонные линии связи Москвы со и штабами 2-го Украинского, 1-го Белорусского и 2-го Прибалтийского фронтов, а также опытная линия связи с Хабаровском.

Возможность оперативного управления боевыми действиями непосредственно из Ставки Верховного Главнокомандования, обеспеченная новой аппаратурой шифрования, явилась одним из общепризнанных факторов победы советских войск на Курской дуге. Виднейшие военачальники периода Отечественной войны Г.К. Жуков, И.С. Конев, И.Т. Пересыпкин, А.Е. Еременко, В.И. Чуйков в ряде публикаций говорят о хорошей работе правительственной связи.

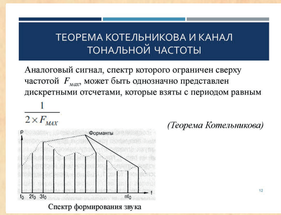
Спецслужбой не зафиксировано фактов дешифрования переговоров, засекреченных сложной шифрующей отечественной аппаратурой.

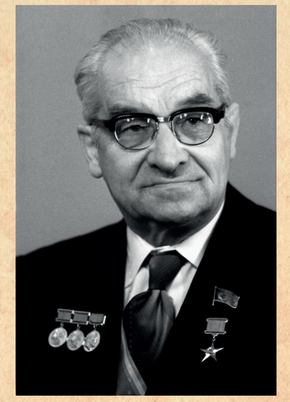
За создание шифраторов Котельников и его коллеги по лаборатории (И.С. Нейман, Д.П. Горелов, А.М. Трахтман, Н.Н. Найденов) получили в марте 1943 года Сталинские премии I степени. Деньги они передали «на нужды фронта». На премию, полученную В.А. Котельниковым, был построен танк.

В дальнейшем аппаратура «Соболь-П» активно использовалась для связи Ставки Верховного Главнокомандования с фронтами. Применялась она и для связи с Москвой нашей делегации во время принятия капитуляции Германии в мае 1945 года, в ходе Тегеранской, Ялтинской и Потсдамской конференций и на дипломатических линиях связи Москвы с Хельсинки, Парижем и Веной при проведении переговоров по заключению мирных договоров.

Работа над усовершенствованием шифровальной аппаратуры продолжалась до последних дней войны и после ее окончания. За дальнейшие разработки в этой области группе специалистов в том числе В. А. Котельникову в 1946 году была повторно присуждена Сталинская премия I степени.

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. Вклад в решение первой задачи был внесен В.А. Котельниковым еще в 1932 г., когда он опубликовал статью «О пропускной способности «эфира» и проволоки в электросвязи», в которой он сформулировал теорему, определяющую условия дискретизации функций и носящую теперь его имя.





В 1953 году Владимир Александрович Котельников был избран действительным членом АН СССР. Он, безусловно, заслужил это звание не только за неоценимый вклад в отечественную криптографическую науку, но и как выдающийся советский и российский учёный, инженер, педагог, организатор науки и образования, один из основоположников радиофизики, радиотехники, информатики и радиоастрономии.

Академик Котельников руководил лабораториями, создававшими устройства по заказу Министерства обороны и КГБ, возглавлял комиссии, контролировавшие качество новых изобретений других инженеров. В 1950–60-е годы он стал инициатором и вдохновителем создания ряда отечественных устройств шифрования информации. С 1954 по 1988 гг. В.А. Котельников работал директором Института радиотехники и электроники АН СССР.

Значимая фаза сотрудничества В.А. Котельникова и отечественной криптографической службы приходится на 1992 г., когда при его существенной поддержке была создана Академия криптографии Российской Федерации. Вместе с другими пятью членами РАН он вошел в число основателей Академии криптографии и в дальнейшем принимал непосредственное участие в её научной и научно-организационной деятельности.

Фонд содействия развитию безопасных информационных технологий

Наглядное пособие разработано в рамках проекта «Криптографический фронт Великой Отечественной», реализуемого НКО «Фонд содействия развитию безопасных информационных технологий» при поддержке гранта Президента Российской Федерации на развитие гражданского общества (Фонд Президентских грантов, договор №18–2–012576)

Более подробная информация о советской дешифровальной службе: v-otgrpi.ru/kfront2