08 мая 2009

Три дивизии за шифр

Судьба одного человека может определить, «направить судьбу целого народа или даже всего человечества», писал Стефан Цвейг. Думается, в минуты наивысшего драматического напряжения истории влияющих на неё личностей оказывается немало. К таким безусловно относится и **Владимир Котельников**, выдающийся учёный, чьи работы в области криптографии внесли огромный вклад в нашу победу в Великой Отечественной войне.
*При подготовке материала использованы фрагменты из готовящегося к печати очерка дочери учёного **Наталии Котельниковой** «Судьба, охватившая век».*

Справка STRF:
Котельников Владимир Александрович (1908—2005), академик АН СССР, один из основоположников отечественной радиофизики, радиотехники, радиоэлектроники, радиоастрономии и криптографии, инженер, педагог и организатор. Его пионерские работы повлияли также на становление информатики и цифрового метода передачи сигналов, статистической и космической радиофизики, планетной радиолокации и широкомасштабных исследований космического пространства.

Владимир Котельников: «Я слышал, что всякие шифры рассекречиваются. Решил разобраться, можно ли сделать абсолютно недешифруемый шифр. Ну, и разобрался. Доказал, что это возможно. Но шифр должен быть случайным и использоваться только раз»

Идею «недешифруемого шифра» Владимир Котельников сформулировал незадолго до войны:

— Я слышал, что всякие шифры рассекречиваются. Решил разобраться, возможно ли сделать абсолютно недешифруемый шифр. Ну, и *разобрался*. Доказал, что возможно. Но для этого шифр должен быть случайным и использоваться только один раз, — так учёный рассказывал об открытом им «условии одноразового ключа»[1].

Закрытый отчёт «Основные положения автоматической шифровки»[2], где было впервые представлено строгое обоснование того, что системы шифрования с одноразовыми ключами абсолютно стойкие, Владимир Котельников сдал за три дня до начала Великой

Отечественной войны. Не «*разберись*» он тогда, неизвестно, был бы создан «Соболь-II», была бы возможна надёжная закрытая связь Ставки с фронтом во время переломной Сталинградской битвы, остались бы живы те, кому удалось выжить?

Перед войной

Ещё в 1935 году перед советскими учёными была сформулирована проблема разработки систем защиты от прослушивания использовавшейся в то время для правительственной и военной коммуникации высокочастотной связи (ВЧ связи)[3]. Созданием специальной радиотелеграфной и телефонной аппаратуры для этих целей с середины 1936 года занимались сразу несколько лабораторий, исследования которых основывались преимущественно на принципе простой инверсии спектра передаваемого сигнала. В результате их деятельности появились образцы шифровальной аппаратуры «маскирующего» типа, которая делала невозможным «любительское» прослушивание, но не спасала от специального перехвата. Параллельно эту же проблему решал и Владимир Котельников с коллегами из Центрального научно-исследовательского института связи (ЦНИИС), в котором он руководил лабораторией. Учёные пытались обеспечить конфиденциальность передачи информации при помощи созданной ими уникальной аппаратуры многоканальной телефонно-телеграфной радиосвязи, установленной на магистрали Москва—Хабаровск.

— Сначала мы просто «перевёртывали спектр» (инвертировали), но быстро поняли, что это легко разгадать. Тогда стали разбивать речь на некоторые «отрезки» по частоте с инверсией спектра, и их «перепутывать»[4].

Под руководством Владимира Котельникова был разработан первый телефонный шифратор, сочетающий в себе частотные преобразования речевого сигнала с перестановками его отрезков по времени. Реализуемые им преобразования были динамическими, то есть периодически менялись по закону распределения случайных величин, и потому их вскрытие представляло весьма серьёзную задачу даже для квалифицированных специалистов.

> *К началу войны в лаборатории Котельникова была разработана самая совершенная на то время система защиты радиотелефонии — система шифрования мозаичного типа*

— Для того чтобы было труднее расшифровать передаваемую речь, было важно сделать «отрезки», на которые мы её разбивали, как можно короче. А это проблема потому, что тогда ухудшается качество передаваемой речи, — вспоминал Владимир Александрович. — Я стал думать, как бы передавать речь не всю полностью, а как-то сжать её спектр. Начал рассматривать спектр звуков, чтобы понять, какие частоты определяющие… В это время попалась на глаза ссылка на статью **Хомера Дадли**[5], опубликованную в октябре 1940 года, где говорилось, что он сделал преобразователь речи — «Вокодер». Бросился смотреть, а оказалось, что там ничего конкретного не написано. Но всё равно, это было очень полезно: идея у него та же, значит, мы на правильном пути. В общем, мы начали делать свой «вокодер». И перед самой войной у нас уже работал его опытный образец. Правда, пока он ещё «говорил» плохо, «дрожащим голосом».

Это был первый вокодер в СССР. Помимо него, в процессе «преодоления трудностей» появилось и немало других изобретений; но Котельников и его коллеги их не публиковали и не патентовали, во-первых, по причине секретности разработок, а, во-вторых, на это у учёных попросту «не было времени».

— Особенно патентование — жуткая волынка. Я как-то перед войной несколько раз этим занимался, но потом бросил, — так комментировал весьма актуальную для нынешних учёных тему Владимир Котельников.

Перед войной сотрудники лаборатории Котельникова разработали самую совершенную на то время систему защиты радиотелефонии — систему шифрования мозаичного типа. Когда же начались военные действия, перед учёными поставили срочную задачу — сделать аппаратуру для секретной правительственной связи[6].

Война

В середине лета 1941 года ситуация на фронте сложилась угрожающая, немцы продвигались к Москве. Началась эвакуация населения города, а позже и предприятий.

— Семьи большинства сотрудников лаборатории, в том числе и Нюсю (жену Владимира Александровича — Анну Ивановну Богацкую. — *здесь и далее прим. авт*.) с годовалым Шуриком (сыном), эвакуировали. Это произошло как раз в день первой бомбёжки Москвы. Привёз я их на вокзал, сели они в поезд. Пока шла посадка, началась воздушная тревога, поезд тронулся и укатил куда-то со станции… Тогда было непонятно, что с ними произошло, остались ли они целы? Только потом узнал, что, к счастью, их поезд остался невредим, и когда кончилась бомбёжка, отправился в Уфу.

А в Москве Владимира Александровича ждали напряжённые рабочие дни и тревожные ночи:

— Иногда, по очереди, чтобы не прерывать работу, на ночь уходили домой. Когда я возвращался на квартиру, в случае бомбардировок приходилось бежать не в бомбоубежище, как всем жильцам дома, а дежурить на чердаке и крыше. Немцы сбрасывали на город и тяжёлые взрывные бомбы, и зажигательные (их прозвали «зажигалками»), которые были небольшие и не разрушали взрывом дом, а пробивали крышу и обычно застревали на чердаке или на верхних этажах, где и загорались. И тут-то надо было их хватать такими большими щипцами, и тушить, засовывая в приготовленный специально для этого ящик с песком. Если не успевали, то тогда надо было тушить уже начавшийся пожар[7].

> *По сведениям советской разведки, за одного шифровальщика, способного «взломать» систему засекречивания передаваемой информации, созданную Котельниковым, Гитлер готов был отдать три отборные дивизии*

В октябре противник вплотную приблизился к Москве. Началась срочная эвакуация тех предприятий, которые ещё не выехали из города. Поступил приказ распустить ЦНИИС. «Все сотрудники были уволены. Оставили почему-то только мою лабораторию. Тогда было непонятно, почему оставили именно нас», — вспоминал Владимир Котельников. Дело в том, что ещё в самом начале войны Генеральный штаб Наркомата обороны направил в институт подписанную Георгием Жуковым директиву, извещавшую, что в случае объявления мобилизации сотрудники лаборатории Владимира Котельникова освобождаются от призыва в армию ввиду важности для обороны страны проводимых ими разработок. Вот что писал учёный об этих днях:

— Нам было приказано: получить деньги и расплатиться со всеми уволенными сотрудниками института. Мои ребята сходили в банк, принесли два мешка денег. Машин не было, так как все они уже были мобилизованы, поэтому тащились пешком с мешками

на плечах без всякой охраны. Хорошо, что жулики не знали, что в этих мешках! Выплатили сотрудникам деньги, и потом все уволенные разбрелись кто куда. Что же касается моей лаборатории, то мы занимались тем, что паковали свою аппаратуру для эвакуации, сжигали документы, чтобы немцам не достались, оставляли только самые необходимые. Ещё приходили к нам подрывники и инструктировали, как взорвать здание института в случае, если в город войдут немцы, чтобы им, как Наполеону, ничего не досталось. Куда потом надо «уходить», было непонятно, но у нас на работе наготове стояли у печки новенькие лыжные ботинки, а в углу — лыжи. Убегать не пришлось, а подошвы ботинок рассыпались на кусочки — пересохли.

Бежать не пришлось, зато пришлось эвакуироваться лабораторией в Уфу, и оставаться там до весны 1943 года[8].

— В Уфе мы продолжили работы над аппаратурой «закрытой радиотелефонии», начатые в Москве. Но они сильно осложнялись тем, что по приказу значительная часть конструкторской документации перед отъездом была уничтожена. Очень многое восстанавливали по памяти.

Несмотря на все трудности, уже к осени 1942 года сотрудники лаборатории Котельникова изготовили несколько образцов оборудования для секретной КВ-радиотелефонии под индексом «Соболь-II»[9]. Это была самая сложная из разрабатываемой в стране аппаратура засекречивания передаваемой информации, не имевшая аналогов в мире. Первые аппараты сразу направили под Сталинград для связи Ставки Верховного Главнокомандования со штабом Закавказского фронта, разрушенной во время боёв. (В то время в армии для связи такого уровня пользовались в основном проводными телефонными линиями. «Соболи-II» позволили установить связь посредством радиоканала.)

К началу 1943 года было налажено производство усовершенствованной серии аппаратов «Соболь-II». Сложные механические узлы уникальных шифраторов, разработанных в лаборатории Котельникова, изготавливались на одном из ленинградских заводов. Для окончательной наладки шифраторов Владимир Александрович регулярно летал в блокадный город, не раз подвергался при этом вражеским обстрелам. Готовые аппараты срочно отправляли на фронт. Как вспоминали ветераны Великой Отечественной войны, применение шифраторов Котельникова в ходе решающих боев на Курской дуге в значительной степени определило успешный исход битвы. Они обеспечивали систему кодирования речи для закрытой радиосвязи, которая практически не поддавалась вскрытию, это оказалось не по зубам даже лучшим дешифровальщикам вермахта. По сведениям советской разведки, Гитлер заявлял, что за одного шифровальщика, способного её «взломать», он не пожалел бы три отборные дивизии.

За создание шифраторов Котельников и его коллеги по лаборатории получили в марте 1943 года Сталинские премии I степени. Деньги они передали «на нужды фронта». В частности, на премию, полученную Владимиром Котельниковым, был построен танк.

После войны

Работа над усовершенствованием шифровальной аппаратуры продолжалась до последних дней войны и даже после её окончания. За дальнейшие разработки в этой области Владимир Котельников в 1946 году удостоился второй Сталинской премии I степени.

Аппаратура стойкого шифрования, разработанная в его лаборатории, положила начало развитию целого класса отечественных систем шифрования речи, которые для своего времени надёжно защищали телефонные переговоры от утечки информации. Эти системы широко применялись в СССР на различных линиях и сетях связи, и вплоть до начала 70-х годов не существовало эффективных алгоритмов дешифрования сообщений, закодированных с помощью наиболее сложных систем такого типа. Однако для «абсолютно надёжной» защиты коммуникаций они всё же не годились.

> *Послевоенные работы Владимира Котельникова в значительной степени определили лицо эпохи глобальной информатизации и покорения космического пространства*

На смену шифрованию, которое условно называют *аналоговым,* пришло *дискретное*. Котельников описал возможность создания аппаратуры стойкого засекречивания телефонных переговоров на базе вокодера и шифратора. Для этого компрессированный (с помощью вокодера) спектр речи необходимо преобразовать в последовательность дискретных импульсов (по теореме отсчётов Котельникова) и осуществить засекречивание, используя модель телеграфного шифрования (в соответствии с другой теоремой, сформулированной и строго доказанной Котельниковым, — об одноразовых ключах). Разработками такой аппаратуры занялись в Марфинской лаборатории, созданной для этих целей в 1948 году. Её костяк составили сотрудники бывшей лаборатории Котельникова, поэтому их исследования велись фактически в русле предвоенных работ лаборатории Котельникова, прерванных началом войны.

Работы Владимира Александровича уже мирного времени в значительной степени определили лицо эпохи глобальной информатизации и покорения космического пространства.

Его исследования в области радиофизики, вылившиеся в уже упомянутую теорему отсчётов («Теорему Котельникова»), а также теорию потенциальной неустойчивости и ряд других, положили начало теории информации, развитию цифровых систем передачи сообщений, управления, кодирования и обработки информации — практически всей современной теории связи. Владимир Котельников внёс весомый вклад и в создание компьютеров, цифровой радиоэлектроники, спутниковой и космической связи, современных радиотелескопов.

Под его руководством разработаны первая в мире система контроля траектории ракет и уникальная система телеметрии, открыто новое направление в радиоастрономии — планетная радиолокация. В результате осуществлённых Котельниковым и его сотрудниками уникальных экспериментов по радиолокации Венеры (1961—1964 годы), Меркурия (1962 год), Марса (1963 год), Юпитера (1963 год) с высокой точностью определено значение астрономической единицы, создана и экспериментально подтверждена новая теория движения внутренних планет Солнечной системы — Венеры и Меркурия. Данные исследования, опирающиеся на релятивистские уравнения небесной механики, а также общую теорию относительности, позволили повысить точность измерения размеров Солнечной системы более чем в 100 раз. Идеи Владимира Котельникова повлияли на дальнейшее развитие всех космических программ, они и по сей день используются при создании систем управления и контроля движения космических аппаратов.

[1] Теорема отсчётов (выборок) к тому времени была доказана (Владимир Котельников сформулировал её в 1932 году), но технически осуществить преобразование аналогового способа передачи информации в цифровой тогда было ещё невозможно, поясняет Наталья Владимировна Котельникова.
Из воспоминаний Владимира Котельникова: «Использование одноразового ключа полезно и для засекречивания в телефонии как проводной, так и радио. Только там все гораздо сложнее, и в случае аналоговой передачи спектра речи, не преобразуя его в цифровую, получить абсолютно стойкое засекречивание невозможно. Можно получить высокую степень стойкости, но не абсолютную. При мозаичном шифровании спектра, даже, если применяется одноразовый ключ, система остаётся уязвимой, поскольку каждый «кусочек», сам по себе, оказывается незашифрованным. Поэтому-то важно сделать интервалы и по возможности меньше, но при этом теряется качество передаваемой речи».

[2] Эта работа, к сожалению, малоизвестна, поскольку так и не вышла в открытой печати. Через пять лет **Клод Шеннон** изложил подходы к построению стойких систем шифрования в своём секретном докладе, датированном 1 сентября 1946 года. В открытой печати он появился в 1949 году.

[3] В докладной записке от 5 декабря 1936 года начальник оперативного отдела УГБ управления НКВД по Ленинградской области **Михаил Алёхин** подчёркивал: «Для создания решительного поворота в технике необходима организация в Москве и Ленинграде групп, работающих исключительно по наблюдению за научно-технической деятельностью в интересующих нас областях. <…>
Без ответственных только за это дело людей, без использования всех достижений техники, проходящих сейчас мимо нас, без привлечения к этому делу молодых талантливых сил поворота в сторону прогресса не добиться».

[4] Из воспоминаний Владимира Котельникова: «“Перепутывали” не просто так, как придётся, а определённым образом, с помощью шифратора. <…> Был у нас “барабан”, наполненный маленькими шариками, который крутился, и из него высыпались шарики на специальное устройство со штырьками и щелями так, что потом через эти щели шарики случайным образом попадали на две движущиеся телеграфные ленты, которые были наложены одна на другую через “копирку”. В результате получался на обеих лентах одинаковый рисунок — “дорожки” из случайно расположенных пятнышек. Затем по этим меткам ленты перфорировались. Одна лента оставалась на “передающем конце”, а вторую мы аккуратненько скручивали и упаковывали в пластмассовую коробочку, которую запаивали, чтобы никто не подсмотрел. Эту процедуру повторяли несколько раз. Таким образом получали два одинаковых набора шифров. Мы их пронумеровывали, и один из наборов отправляли на “пункт приёма”. А туда, во время сеанса связи секретно сообщали номер шифра, и таким образом на том конце знали, какую из коробочек надо распаковывать, чтобы использовать спрятанный там шифр».

[5] Записка, написанная Владимиром Котельниковым после просмотра статьи Хомера Дадли:
«Искусственная речь.
1. The Carrier Nature of Speech
H. Dudley. BSTJ. Oct. 1940
Вокодер. В приложении математическое выражение для речи. Но мало что дающее».

[6] Из воспоминаний Владимира Котельникова: «С началом войны нам (сотрудникам лаборатории в ЦНИИС — *прим. авт*.) пришлось прервать научно-исследовательскую работу и перейти к срочному проектированию образцов аппаратуры “закрытой

радиотелефонии”. Аппаратура, над которой мы начали работать, была, конечно, попроще той, которой мы занимались до начала войны, но многое из тех наработок мы здесь использовали».

[7] Из воспоминаний Владимира Котельникова: «С тушением “зажигалок” мы быстро освоились, а вот с тушением пожара первый раз, по неопытности, вышел казус. Когда загорелся чердак, один из дежурных побежал за пожарным шлангом, который лежал свёрнутый в положенном для него месте. Быстро подсоединил к пожарному крану, открыл воду и — шланг вздулся, зашевелился, как удав, стал разворачиваться, вода хлынула… Он схватил его, а дотащить не может — наполнившись водой, шланг стал тяжеленный. Тогда потащили все вместе. Пожар, слава богу, затушить успели. Уже потом, наученные горьким опытом, мы действовали правильно: один хватал шланг и бежал к месту возгорания, а второй включал воду».

[8] Записи в трудовой книжке Владимира Котельникова за 1941—1943 годы:
12.12.1941 г. Откомандирован в Инст-т №56.
16.12.1941 г. Зачислен нач. лаборат. №3 Инст №56.
16.02.1942 г. Зач. руководителя спец. группы 2 лаб. Инст №56.
11.11.1942 г. Переведён на должность. начальника лаборатории
1943 г. Откомандирован в распоряж. ОПС НКВД СССР

[9] Аппараты шифрования телефонных переговоров «Соболь-II», получившие боевое крещение в 1942 году под Сталинградом и в дальнейшем активно использовавшиеся для связи Ставки Верховного Главнокомандования с фронтами, после окончания Второй мировой войны получили применение и на дипломатических линиях связи Москвы с Хельсинки, Парижем и Веной при проведении переговоров по заключению мирных договоров, а также при проведении Тегеранской, Ялтинской и Потсдамской конференций глав трёх государств.

Подготовила Светлана Σ Синявская,
по материалам готовящегося к печати очерка Наталии Котельниковой «Судьба, охватившая век»