*D.A. Larin*

**About The Soviet Cryptographs' contribution to the Great Patriotic War Victory**

*Key words: Great Patriotic war, cipher, cryptanalyst, the soviet cryptographs.*

This article deals with the unknown facts of the soviet cryptograph activity during Great Patriotic War. The specialists of our Cryptographic Service were able to provide the secret connection between the political and military members of the governing body and get access to very important information thought their deciphering work, which was used during the planning and implementing operations.

*Д.А. Ларин*

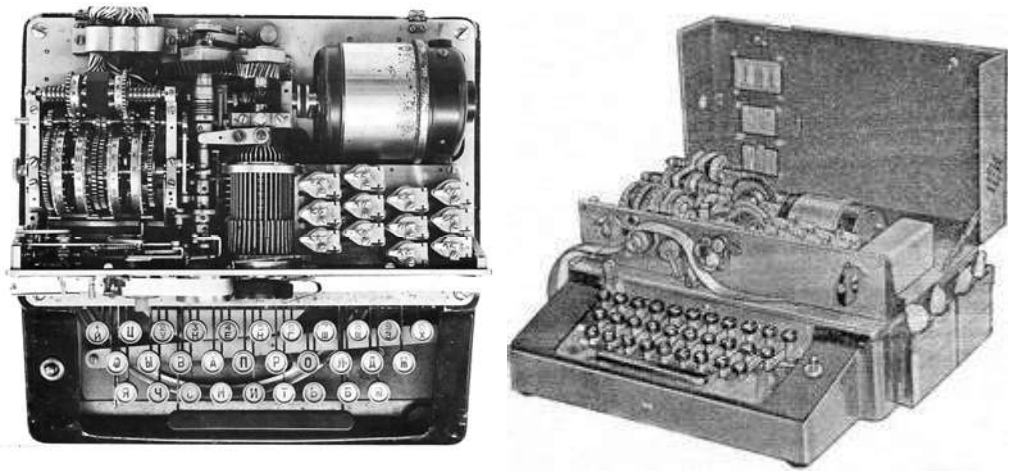
# О ВКЛАДЕ СОВЕТСКИХ КРИПТОГРАФОВ В ДОСТИЖЕНИЕ ВЕЛИКОЙ ПОБЕДЫ

В этом году исполняется 70 лет Великой Победе СССР над фашисткой Германией и ее союзниками. Огромный вклад в Великую Победу внесла советская криптографическая служба, специалисты по созданию шифров сумели обеспечить надежную секретную связь политического руководства страны с действующей армией и обмен зашифрованными сообщениями между группировками войск на фронте и тылу, в свою очередь наша дешифровальная служба в ходе войны обеспечила важнейшей информацией Ставку Верховного Главнокомандующего, командующих фронтов, армий, корпусов и других командиров нашей армии.

В период Великой Отечественной войны для закрытия самых важных сообщений высшего политического и военного руководства СССР применялись шифрмашины – электромеханические устройства, автоматически преобразующие открытый текст в шифрованный очень сложным образом, при этом шифровальщику достаточно просто набрать открытый текст на клавиатуре и получить шифрованный текст. Использование шифрмашин значительно ускоряло процесс шифрования и расшифрования.

Две модели шифрмашин, использовавшихся в СССР во время войны, были созданы в конце 1930-х годов коллективом под руководством блестящего инженера Ивана Павловича Волоска. Боевое крещение они прошли во время боев на Халхин-Голе (1939) и в Финляндии (1939-40).

И.П. Волосок (послевоенное фото)



Первые отечественные шифрмашины

Всего к началу войны в СССР имелось более 250 шифрмашин, а к исходу войны – уже 396. Эта техника позволила существенно повысить скорость обработки шифртелеграмм, при этом сохраняя стойкость передаваемых сообщений. На машинную шифрсвязь в годы войны легла основная нагрузка при передаче секретных телеграмм. Так за период с 1941 по 1945 годы было обработано свыше 1,6 миллиона шифрсообщений.

С самого начала войны фашистские дешифровальщики пытались прочесть перехваченные советские криптограммы, зашифрованные машинными шифрами. Но все их попытки были тщетны! Специалисты-шифровальщики с честью справились с возложенными на них задачами, обеспечивая машинной шифрсвязью Ставку ВГК, Генеральный штаб, управления Наркомата обороны, действующую армию. Важную роль сыграли шифрмашины в обеспечении связи советских делегаций на Тегеранской, Ялтинской и Потсдамской конференциях. За создание и внедрение шифрмашин И.П. Волоску и его коллегам П.А. Судакову и В.Н. Рытову в 1943 году были присуждены Сталинские премии. Орденами были награждены и другие создатели советских шифрмашин: Н.М. Шарыгин, М.С. Козлов, П.И. Строителев и Н.И. Гусев. Кроме того, И.П. Волоску была присвоена ученая степень «кандидат технических наук» (без защиты диссертации [3]).

В более низких звеньях военного управления применялись ручные шифры. В основном это были коды, коды с перешифровкой, а также шифры перестановки, многоалфавитной замены и гаммирования. Отметим, что в годы войны в войска было направлено порядка 3,2 млн. комплектов шифров.

Отдельным направлением в шифровальном деле является шифрование речи. Здесь используются принципы, отличные от шифрования текстовой информации, из-за иной физической природы речевого сигнала. При этом совершенно очевидно, что ручное шифрование телефонных переговоров невозможно в принципе, поэтому речевые шифраторы изначально были электромеханическими. Кстати, первой шифрмашиной, созданной в СССР, был именно речевой шифратор, это произошло в 1927 году.

Огромный вклад в создание отечественной техники шифрования речи внес Владимир Александрович Котельников. В.А. Котельников – знаменитый советский ученый, академик АН СССР, дважды Герой Социалистического Труда, лауреат многочисленных премий. В.А. Котельников опубликовал фундаментальные труды в области радиотехники, теории помехоустойчивой связи, радиолокации, радиоастрономии. Впервые в мире он сформулировал и доказал фундаментальную теорему дискретизации, на которой основана вся цифровая обработка сигналов. Параллельно с К. Шенноном В.А.

Котельников математически формализовал требования к стойкости шифров. Что касается телефонных шифраторов, то в лаборатории Котельникова в 1930-е годы был создан ряд образцов подобной аппаратуры. Эта работа продолжалась и в годы Великой Отечественной войны.

В.А. Котельников

Данная техника позволила обеспечить оперативную засекреченную связь политического и военного руководства страны с действующей армией, а также организации телефонной связи непосредственно в районах боевых действий.

Особо следует отметить шифратор «Соболь II». Это было самое сложное из разрабатываемых в стране средств засекречивания передаваемой информации, не имевшая аналогов в мире. Первые два аппарата сразу, даже не закончив испытаний, направили в Сталинград для обеспечения связи нашей группировки в городе со штабом на другом берегу Волги, проводная связь между которыми была разрушена во время боёв. Тогда в армии для связи такого уровня пользовались в основном проводными телефонными линиями, а «Соболь II» позволил устанавливать связь посредством радиоканала. Это сыграло положительную роль в организации управления войсками, участвующими в Сталинградской битве. К началу 1943 года было налажено производство усовершенствованной серии аппаратов «Соболь II». Как вспоминали ветераны, применение этих шифраторов в ходе решающих боев на Курской дуге в значительной степени определило успешный исход битвы. Они обеспечивали шифрование речи при передаче по радио. Шифраторы практически не поддавались взлому, это оказалось не по зубам даже лучшим немецким дешифровальщикам. По сведениям советской разведки, Гитлер заявлял, что за одного криптоаналитика, способного их «взломать», он не пожалел бы три отборные дивизии.

За создание телефонных шифраторов В.А. 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. Так, на премию, полученную В.А. Котельниковым, был построен танк. Впоследствии «Соболь II» активно использовался для связи Ставки Верховного Главнокомандования с фронтами. После окончания Второй мировой войны она получила 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 и для связи с Москвой нашей делегации

во время принятия капитуляции Германии в мае 1945 года. Работа над усовершенствованием шифровальной аппаратуры продолжалась до последних дней войны и даже после её окончания. За дальнейшие разработки в этой области В.А.Котельникову и группе специалистов в 1946 году была присуждена вторая Сталинская премия I степени. Так же большой вклад в разработку и внедрение аппаратуры засекречивания речевого сигнала внесли Ю.Я. Волошенко, М.Л. Дайчик, Г. Двойневский, А.Я. Захарова, К.Ф. Калачев, Н.Н. Коробков, Р. Лейтес, В.А. Малахов, В.Н. Мелков, А.П. Петерсон, Н.А. Тюрин, В.Б. Штейншлегер и др. [4].

Отметим, что шифровальная служба не позволила противнику получить сведения о наших замыслах и действиях. Вот как оценивают работу советских шифровальщиков прославленные полководцы Великой Отечественной. Г.К. Жуков: «Хорошая работа шифровальщиков помогла выиграть не одно сражение» [Цит. По 2 стр. 318]. А.М. Василевский: «Ни одно донесение о готовящихся военно-стратегических операциях нашей армии не стало достоянием фашистских разведок» [Цит. По 2 стр. 318]. Подобные оценки работы нашей шифрслужбы дали и многие другие знаменитые военачальники. Объем статьи не позволяет привести их все, но их можно найти в мемуарах И.С. Конева, И.Х. Баграмяна, К.К. Рокоссовского и др. [2, с. 319-320].

Оценил работу советской шифрслужбы и противник. Приведем выдержку из допроса советской контрразведкой начальника штаба при ставке верховного главнокомандования немецких вооруженных сил генерал-полковника А. Йодля от 17 июня 1945 года: «…нам никогда не удавалось перехватить и расшифровать радиограммы вашей ставки, штабов фронтов и армий» [Цит. По 2 стр. 318].

Но криптография – это не только создание шифров, а еще и дешифрование шифров противника. Перехват и дешифрование вражеских сообщений является важнейшим источником информации о противнике. К началу Великой Отечественной войны наши дешифровальщики уже имели боевой опыт участия в войне в Испании, конфликтах в Китае и на Халхин-Голе, а также в советско-финской войне. Серьезные успехи по дешифрованию иностранной шифрпереписки были достигнуты советскими специалистами во второй половине 1930 годов. С осени 1939 года перехватывалась и дешифровывалась дипломатическая переписка Италии, Японии, Турции и некоторых других государств, содержавшая сведения о подготовке агрессии против СССР. С началом войны активизировалась работа по вскрытию шифров Германии и ее союзников. Основной упор в дешифровальной работе по военной линии был сделан на разработку шифрпереписки войсковых сетей немецкой армии, органов военной разведки и войск СС, а также переписки немецкой полевой полиции и жандармерии. Так, уже на 20-й день войны был вскрыт один из действующих немецких шифров.

Огромный вклад советские дешифровальщики внесли в победу под Москвой. Напомним читателю, что группа дешифровальщиков под руководством Сергея Семеновича Толстого вскрыла ряд японских шифрмашин, что позволило читать шифрпереписку высшего политического и военного руководства Японии.

С.С. Толстой

Б.А. Аронский (послевоенное фото)

Японская «пурпурная» (американское обозначение) шифрмашина

В это же время группа Бориса Алексеевича Аронского дешифровала немецкие дипломатические коды. В результате успехов наших дешифровальщиков была получена информация колоссальной важности. Удалось выяснить, что несмотря на все уговоры немцев, Япония в 1941 году не нападет на СССР. Но это еще не все. Япония готовится к нападению на США и английские колонии в Юго-Восточной Азии, и поэтому нападение на СССР в ближайшее время невозможно. Таким образом, руководство СССР пошло на переброску войск с Дальнего Востока и из Сибири, не опасаясь удара в спину. Именно эти соединения сыграли решающую роль в ходе победоносного наступления. Вообще, в течение последующих нескольких лет одной из главных задач для советских дешифровальщиков стало наблюдение за военной и политической деятельностью Японии в связи с сохраняющейся опасностью нападения с её стороны.

В битве за Ленинград наибольших успехов радиоразведчики и дешифровальщики добились в борьбе с немецкой авиацией и дальнобойной артиллерией. Выход немецко-фашистских войск на ближайшие подступы к Ленинграду лишил нашу ПВО возможности своевременно предупреждать истребительную авиацию, зенитную артиллерию и население города о подходе вражеских бомбардировщиков. Задача обнаруживать немецкие самолёты с момента их взлета с аэродромов и засекать артиллерийские позиции была возложена на радиоразведку и успешно решена. В дальнейшим, читая немецкую и финскую шифрпереписку, наши дешифровальщики поставляли командованию важную информацию о численности, дислокации, планах и намерениях противника.

К исторической Сталинградской битве радиоразведчики и дешифровальщики подошли, обладая бесценным опытом. В оборонительный период битвы радиоразведка сумела, в частности, вскрыть выход итальянских и румынских частей к Дону, нащупав, таким образом, потенциально слабые места в группировке войск противника. С началом контрнаступления советских войск радиоразведка постоянно освещала положение в гитлеровской армии, перехватывала открытые, подчас панические донесения немцев, что позволяло советскому командованию быстро принимать соответствующие решения.

Дешифровальщики внесли заметный вклад в победу под Курском. Накануне Курской битвы буквально за сутки до начала сражения наши криптоаналитики вскрыли шифрованный приказ Гитлера о наступлении. Непосредственно в ходе сражения под Курском советские специалисты продолжили успешную работу. Так, удалось установить создание на Орловском выступе ударной группировки противника за счёт переброски туда целой полевой армии. В самый кульминационный момент Курской битвы дешифровальщикам удалось добыть важные данные об изменении направления главного танкового удара немцев с Обояни на Прохоровку. Командующий Воронежским фронтом Н.Ф. Ватутин, убедившись в достоверности этих данных, отменил переброску 5-й гвардейской танковой армии на Обоянское направление. Эта армия встретила противника под Прохоровкой и сорвала его планы, что и предрешило победу под Курском.

Эффективно работали советские дешифровальщики и в дальнейшем. Помимо военных шифров, советские специалисты вскрыли большое количество дипломатических шифров и кодов Германии и ее союзников, что позволило снабдить советское руководство ценной информацией политического характера. В дешифровальной службе в период войны работали В.Х. Бадальян, Ф.А. Бахшиян, М.Н. Нестеренко, И.В. Матвеев, Г.С. Погосов, В.С. Полин, Г.И. Пондопуло, М.И. Соколов, Д.М. Трусканов, Г.И. Чуриков и многие другие специалисты.

В ходе Берлинской наступательной операции наши радиоразведчики и криптоаналитики узнали состав и расположение немецкой группировки, а также сумели распознать, передаваемую немцами по радиоканалам дезинформацию о наличии крупных

резервов, которых на самом деле не было. При этом отметим, что накануне битвы за Берлин Г.К. Жуков приказал всю информацию, касающуюся предстоящего наступления, передавать по проводам или с курьерами, радиостанции во всех подразделениях были опечатаны. Это было сделано для того, чтобы исключить малейшую вероятность утечки информации [1], [2].

В заключение приведём оценку работы советских дешифровальщиков, данную одним из бывших руководителей уже российской криптографической службы генералом армии А.В. Старовойтовым: «Нам была доступна информация, циркулирующая в структурах Вермахта (почти вся!). Я полагаю, нашим маршалам была оказана существенная помощь в достижении перелома в ходе войны и, наконец, окончательной победы. Наши полевые центры дешифрования работали весьма успешно. Войну в эфире мы выиграли» [Цит. По 2 стр. 383]. Ценная информация, добытая героями невидимого криптографического фронта, позволила сохранить жизни тысяч и тысяч наших солдат и офицеров, сыграла значительную роль в победе над врагом.

## СПИСОК ЛИТЕРАТУРЫ:

1. Болтунов М.Е. «Золотое ухо» военной разведки. М.: Вече 2011. // http://read24.ru/fb2/mihail-boltunov-zolotoe-uho-voennoy-razvedki/ (дата обращения 20.04.2015).
2. Бутырский Л.С., Ларин Д.А., Шанкин Г.П. Криптографический фронт Великой Отечественной. Монография. М.: Гелиос АРВ, 2013. С. 318-320, 383.
3. Дадуков Н.С., Репин Г.А., Скачков М.М., Филин Ю.П. Советская шифровальная техника. Ленинградский период: 1935 – 1941 // Защита информации. INSIDE. №1-6, 2006.
4. Калачев К. В круге третьем. Воспоминания и размышления о работе Марфинской лаборатории в 1948-1951 годах. М.: Элиас рекордз, 2000.
5. Ларин Д.А. О вкладе советских криптографов в победу под Москвой // Безопасность информационных технологий. №4, 2011. С. 42-45.

## REFERENCES:

1. Boltunov M.E. «Zolotoe uho» voennoy razvedki. M.: Veche 2011 // http://read24.ru/fb2/mihail-boltunov-zolotoe-uho-voennoy-razvedki/
2. Butyrsky L.S., Larin D.A., Shankin G.P. Kriptograficheskij front Velikoy Otechestvennoi. Monografia. M.: Gelios-ARV, 2013. P. 318-320, 383.
3. Dadukov N.S., Repin G.A., Skachkov M.M., Filin U.P. Sovetskaja shifrovalnaja tehnika. Leningradskiy period: 1935 – 1941 // Zaschita informacii. INSIDE №1-6, 2006.
4. Kalachev K. V kruge tret'em. Vospominania i razmyshlenija o rabote Marfinskoy laboratorii v 1948-1951 godah. M.: Elias records, 2000.
5. Larin D.A. O vklade sovetskih kriptografov v pobedu pod Moskvoy // Bezopasnost informacionnyh tehnologiy №4, 2011. p. 42-45.