

Ларин Д.А., к.т.н.
Доцент кафедры ИТС МГТУ МИРЭА

Война не возможна без связи, а связь должна быть шифрованной. Опыт оборонительных и наступательных операций Красной Армии в первом периоде войны подтвердил необходимость укрепления структур правительственной связи в действующей армии. Совместный приказ Наркомата Обороны (НКО) и НКВД, подписанный 11.02.1943 г., «предусматривал передачу в распоряжение НКВД СССР сформированных НКО частей связи и основных магистральных линий с проводами для правительственной ВЧ-связи Ставки ВГК со штабами фронтов и армий...»¹. Таким образом, был сформирован новый род войск НКВД - войска правительственной связи. В первой половине 1943 г. был проведен ряд организационных мероприятий и изданы нормативные документы по улучшению функционирования правительственной связи, что положительно сказалось на организации управления войсками по линии Ставка ВГК - штабы фронтов и армий, ведущих боевые действия, и послужило импульсом к дальнейшему совершенствованию системы правительственной связи².

В марте 1943 г. были увеличены штаты отделов правительственной связи (ОПС) этих фронтов. Это мероприятие имело целью обеспечить бесперебойное действие высокочастотной (ВЧ) связи от Москвы до штабов фронтов. Для обеспечения командующего фронтом ВЧ-связью на наблюдательном пункте (НП) формировалась выездная группа фронтовой станции в составе старшего техника и техника, оснащенная засекречивающей аппаратурой телефонной связи (шифраторами) типа "Снегирь", несколькими телефонными аппаратами³.

Еще одним типом аппаратуры засекречивания телефонных переговоров, впервые в массовом порядке примененной в ходе решающих боев на Курской дуге, стала аппаратура повышенной стойкости "Соболь", созданная под руководством знаменитого ученого впоследствии – академика В.А. Котельникова⁴. Еще в 1938-39 годах в ЦНИИ связи Наркомата почт и телеграфа были организованы две лаборатории под его руководством по засекречиванию телеграфной и телефонной информации. В 1939 году В.А. Котельникову было поручено решение важной государственной задачи – создание шифратора для засекречивания речевых сигналов с повышенной стойкостью к дешифрованию. Аппаратура была создана к осени 1942 года и получила название "Соболь". Это была самая сложная из разрабатываемой в СССР аппаратура засекречивания передаваемой информации, не имевшая аналогов в мире. Первые аппараты сразу направили под Сталинград для связи Ставки Верховного Главнокомандования со штабом Закавказского фронта, проводная связь между которыми была разрушена во время боёв. В то время в армии для связи такого уровня пользовались в основном проводными

телефонными линиями, а «Соболь» позволил устанавливать связь посредством радиоканала. Это сыграло положительную роль в улучшении управления войсками, участвующими в Сталинградской битве.

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 Котельников регулярно летал в блокадный Ленинград, при этом не раз попадал под обстрелы и бомбардировки. 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 шифрование речи при передаче по радио, таким образом обеспечивалось оперативное управление войсками в ходе быстро меняющейся обстановки на театре военных действий. Шифраторы не поддавались взлому, они оказались «не по зубам» даже лучшим немецким дешифровальщикам. По сведениям советской разведки, Гитлер заявлял, что за одного криптоаналитика, способного «взломать» «Соболя», он не пожалел бы три отборные дивизии. За создание 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 фронта⁵.

Для шифрования текстовых сообщений советские связисты применяли шифрмашины М-100, М-101 (наложение гаммы) и К-37 (дисковый шифратор многоалфавитной замены), а также ручные шифры. Наиболее распространённой системой шифрования советских вооружённых сил во время Великой Отечественной войны были коды с перешифровкой. При этом была установлена следующая иерархия: пятизначные коды для шифрования стратегической информации; четырёхзначные для оперативного звена (уровень армия – фронт), трёхзначные для тактического звена до уровня бригады и наконец двухзначные, предназначались для низшего звена советских вооружённых сил. Полученный с помощью кодовой книги промежуточный шифртекст затем, как правило, (а высших звеньях обязательно) перешифровывался одноразовой гаммой⁶.

При этом также использовались и весьма простые, но эффективные методы защиты информации. Так все военачальники даже при ведении переговоров по зашифрованным каналам связи использовали псевдонимы, так И.В. Сталин, представлялся Ивановым, у А.М. Василевского был псевдоним Александров, у И.С. Конева – Степной, у Н.Ф. Ватутина – Николаев и т.д.⁷ Так же применялся режим радиомолчания, так выдвижение 5 гвардейской танковой армии генерал-лейтенанта П.А. Ротмистрова выдвигалась в район Прохоровки соблюдая полное радиомолчание что не позволило вычислить её прибытие радиоразведке противника, и только после сосредоточения для контрудара было разрешено использовать радио: «...2.

Начало атаки в 8.30 12.07.43 г. Начало артподготовки с 8.00. 3. Разрешаю пользоваться радио с 7.00 12.07.43 г. Командующий 5 гв. ТА генерал-лейтенант Ротмистров».⁸

Делая выводы о работе службы правительственной полевой связи в летних наступательных операциях 1943 г., начальник управления войск правительственной связи НКВД генерал-майор П.Ф. Угловский отмечал: "Опыт последних боевых операций показал, что правительственная ВЧ-связь стала основным средством связи для командования фронтов в звене фронт-армия... По телефону ВЧ практически разрешено вести не только секретные, но и сов. секретные переговоры. Одно уже это обстоятельство делает ВЧ-связь в глазах командования фронтов и армий **САМЫМ ЦЕННЫМ И НЕЗАМЕНИМЫМ СРЕДСТВОМ УПРАВЛЕНИЯ ВОЙСКАМИ**" (выделено авт. цитаты)⁹.

Теперь рассмотрим другую сторону работы криптографической службы – перехват и дешифрование сообщений противника. Имея достаточно объективную информацию от нашей радиоразведки и дешифровальной службы, а также военной разведки и контрразведки, о намерении противника провести летом 1943 г. операцию "Цитадель", Ставка Верховного Главнокомандующего (ВГК) в течение апреля-июня развернула работу по созданию в районе Курского выступа мощной, глубоко эшелонированной обороны.

Значительную роль в выявлении планов врага и разгрому противника в Курской битве сыграли наши радиоразведчики из радиодивизионов особого назначения (ОСНАЗ)¹⁰, криптоаналитики и сотрудники разведки. Накануне Курской битвы буквально за сутки до начала сражения наши криптоаналитики вскрыли зашифрованный приказ А. Гитлера о наступлении в районе Курска¹¹. Перехватив радиограмму, радиоразведчики опознали почерк радиста ставки противника и сделали вывод, что она содержит очень важный приказ. Дешифровальщики знали, что речь может идти о крупном наступлении фашистов и предположили, что в конце документа находится подпись Гитлера. С помощью атаки «открытый-шифрованный текст» криптограмма была раскрыта. Она подтвердила информацию из других источников, в том числе и сообщения от нашего знаменитого разведчика Героя Советского Союза Н.И. Кузнецова, назвавшего дату наступления немецких войск под Курском.

Советские радиоразведчики продолжали свою успешную работу и непосредственно в ходе сражения под Курском. Бывший в то время начальником отделения радиоразведки разведотдела Брянского фронта А.Ф. Соловьянов вспоминал, как в апреле 1943 г. в условиях строжайшего радиомолчания, введенного немцами в сухопутных войсках, нашей радиоразведке всё же удалось установить создание на Орловском направлении ударной группировки за счёт переброски туда целой полевой армии. Такой вывод наши радиоразведчики смогли сделать в результате наблюдения за радиообменом немецкой разведывательной авиации в

УКВ-диапазоне. Люфтваффе (ВВС Германии) обеспечивали каждую полевую армию одной разведывательной группой, самолёты которой регулярно вели воздушную разведку переднего края нашей армии, докладывая с борта информацию о положении наших войск. Так было и на Орловском направлении, где дислоцировалась 2-я полевая армия немцев. Но в апреле здесь появилась новая разведывательная авиагруппа, самолёты которой вели разведку исключительно южнее Орла в узкой полосе. Был выявлен ещё ряд признаков, позволивших утверждать, что южнее Орла сосредоточена новая полевая армия, переброшенная для удара на Курск. Удалось установить количество корпусов и дивизий первого эшелона этой армии, определить разграничительные линии между ними. Спустя некоторое время данные радиоразведки получили дополнительное подтверждение воздушной и войсковой разведок¹².

В кульминационный момент Курской битвы 313 радиодивизион ОСНАЗ, которым командовал подполковник П.Т. Костин, добыл важные данные об изменении направления главного танкового удара фашистов с Обояни на Прохоровку. Командующий Воронежским фронтом генерал армии Н.Ф. Ватугин, 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. Впоследствии упомянутый выше радиодивизион был награжден орденами Красного Знамени и Богдана Хмельницкого.¹³

Для проведения операции, на флангах Курского выступа были сосредоточены 50 дивизий противника (в их составе были 10000 орудий и 2700 танков) и свыше 2000 самолётов 4 и 6 воздушных флотов. В дешифрованном приказе Гитлера указывалось, что наступление начнется в 5 часов утра. Советским командованием было принято решение нанести упреждающий удар в 2 часа 20 минут наши войска начали артиллерийскую контрподготовку, которая нанесла немцам, сосредоточенным на исходных рубежах, значительные потери и оказала на них глубокое психологическое воздействие.

В ходе грандиозного сражения на Курской дуге враг был разгромлен, потеряв большое количество живой силы и техники. Так, например, из-за больших потерь ВВС, понесенных под Курском, Германия вынуждена была впредь почти полностью отказаться от действий своей авиации по объектам нашего глубокого тыла. Успех радиоразведчиков и криптографов стал одним из весьма важных факторов, приведших к победе под Курском. Об этом в своих мемуарах упоминают маршалы Советского Союза А.М. Василевский и Г.К. Жуков¹⁴. Впоследствии высоко оценили работу наших радиоразведчиков и криптоаналитиков под Курском и немцы. Вот что позднее было написано одним из офицеров 19-й танковой дивизии вермархта: «Как выяснилось позже, противнику задолго до начала был известен X-день, а также Y-время наступления, вплоть до последнего изменения в 10 минут»¹⁵.

Значительное количество информации о планах и намерениях немцев поступило по линии внешней разведки из Великобритании. Большой вклад в добывание английской криптографической информации внес член знаменитой «кембриджской пятерки» сотрудник МИД этой страны Д. Кернкросс. Наиболее ценными разведывательными материалами, переданными Кернкроссом, были сведения, связанные с операцией «Ультра» (дешифрованием английскими специалистами немецкого шифратора «Энигма»). Кернкросс имел к ним доступ с 1942 по 1944 гг., когда работал в дешифровальной службе Великобритании, располагавшейся в поместье Блетчли-парк. Весной 1943 г. от Кернкросса поступила информация о намерениях немцев начать наступление в районе Курска. При этом сообщались подробности предстоящей операции, число и номера дивизий, которые должны принять участие в операции, данные по укомплектованности немецких частей вооружением, боеприпасами, средствами материально-технического обеспечения, направления ударов немцев. Сам Кернкросс особенно гордился тем, что ключи к шифрам люфтваффе, которые он передал советскому командованию, позволили перед Курской битвой разбомбить значительную часть немецких самолетов на земле, и это стало предпосылкой господства советских ВВС в небе над Курском.¹⁶

Материалы «Ультра», переданные Кернкроссом, заметно дополнялись сведениями от сотрудника британской разведки Л. Лонга. С декабря 1940 г. он работал в британском министерстве обороны в отделе MI-14, в котором занимались сопоставлением и анализом разведывательной информации, полученной в результате дешифрования немецких шифров, в первую очередь «Энигмы». С секретными материалами британской дешифровальной службы, которая за время войны перехватила и дешифровала свыше 15000 немецких криптограмм, советская разведка имела возможность знакомиться через еще одного члена «кембриджской пятерки» Энтони Бланта¹⁷.

Подводя итог анализа деятельности советской криптографической службы в период подготовки и проведения Курской битвы, необходимо подчеркнуть, что на своем участке борьбы с противником она выполнила все стоящие перед ней задачи, а по ряду важнейших направлений его превосходила и тем самым внесла свой неоценимый вклад в общую победу СССР. Более подробно об этом можно прочитать в статье *Ларин Д.А. «Иванов» у аппарата // «Родина». Российский иллюстрированный исторический журнал. М.: 2013, №7 С. 12-14.*

Примечания

- ¹ Астрахан В.И., Павлов В.В., Чернега В.Г., Чернявский Б.Г. Правительственная электросвязь в истории России. Часть I (1917-1945). М., Наука, 2001. С. 207.
- ² Там же. С. 220-221.
- ³ Там же. С. 237.
- ⁴ Владимир Александрович Котельников (1908-2005) знаменитый русский 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 сформулировал и доказал фундаментальную теорему дискретизации, на которой основана вся цифровая обработка сигналов. Под его руководством в 1930 годы были созданы первые отечественные аппараты для шифрования речевого сигнала. Эта работа продолжалась и в годы Великой Отечественной войны. Параллельно с К. Шенноном В.А. Котельников математически формализовал требования к стойкости шифров.
- ⁵ Быховский М.А. и др. “В.А.Котельников и его влияние на научные исследования и разработки ученых НИИР”. Электросвязь, №11, 2003, Быховский М. “Пионеры информационного века. История развития теории связи”. М.А. Техносфера, 2006, Синявская С. “Три дивизии за шифр”. // Электронное издание “S&TRF — Наука и технология РФ”, 08.05.2009, <http://www.strf.ru>.
- ⁶ Подробнее о советских системах шифрования и организации шифрованной связи можно прочитать в Главе 4 книги Бутырский Л.С., Ларин Д.А., Шанкин Г.П. Криптографический фронт Великой Отечественной. Монография. М.: Гелиос АРВ, 2012.
- ⁷ Мощанский И.Б. Крупнейшие танковые сражения Второй мировой войны. Аналитический обзор. М.: Вече, 2011. С. 271-272.
- ⁸ Там же. С. 286.
- ⁹ Там же. С. 260.
- ¹⁰ Подробнее о создании дивизионов ОСНАЗ можно прочитать в главе 5 книги Бутырский Л.С. и др. Указ. соч.
- ¹¹ Таким образом, была подтверждена информация разведки, предоставившей этот приказ (по другим данным директиву (<http://ru.wikipedia.org>)), правда документ еще не был подписан Гитлером, советскому руководству весной 1943 года (<http://www.militera.lib.ru/memo/russian/mykoyan/04.html>). Предположительно эта информация была получена из Германии через советскую разведку в Швейцарии «Люси» (<http://ru.wikipedia.org>), подробнее о работе этих разведчиков, в том числе о криптографических аспектах их деятельности, можно прочитать в главе 6 книги Бутырский Л.С. и др. Указ. соч.
- ¹² Шмырев П. Часовые эфира (об истории радиоразведки). // Газета “Красная Звезда”, 18 марта 2004г. <http://offline.computerra.ru>.
- ¹³ Там же.
- ¹⁴ Василевский А.М. Дело всей жизни. М.: Политиздат, 1978. 552 с. // Жуков Г.К. Воспоминания и размышления. М.: Олма-Пресс 2002.
- ¹⁵ Ащеулов О.Е. Остановившие «тигров» и «пантер»: артиллеристы Воронежского фронта в оборонительных боях Курской битвы // Военно-исторический архив. М., 2012, №7 (151), С. 60.
- ¹⁶ Более подробную информацию о добывании английских криптографических секретов Д. Кенкроссом и другими членами «кембриджской пятерки» можно получить, в частности, из книги Бутырский Л.С. и др. Указ. соч. Глава 6.
- ¹⁷ Лекарев С., Порк В. Радиоэлектронный щит и меч // Независимое военное обозрение №2, 2002, с.7.