Д. А. Ларин

О ВКЛАДЕ СОВЕТСКИХ КРИПТОГРАФОВ В ПОБЕДУ ПОД МОСКВОЙ

Одним из важных методов защиты информации являются криптографические. В победе советских войск в битве за Москву огромную роль сыграла отечественная криптографическая служба. Разработчики шифров и шифрмашин, шифровальная служба обеспечили безопасность советских линий связи. Радиоразведчики и дешифровальщики успешно перехватывали и дешифровывали криптограммы фашистской Германии, ее европейских союзников, милитаристской Японии.

В довоенные годы советское руководство приняло решение о создании радиодивизионов особого назначения (ОСНАЗ). Они входили в состав Главного разведывательного управления (ГРУ) Генштаба Красной Армии и во время войны вели перехват открытых и шифрованных сообщений немцев и их союзников в прифронтовой полосе, занимались пеленгацией вражеских передатчиков, создавали радиопомехи, участвовали в операциях по дезинформации противника. В каждом батальоне было от 18 до 20 приемников перехвата и 4 пеленгатора [1. С. 282]. Подготовка персонала для этих подразделений началась в 1937 г. в Ленинграде. Этим занимались на инженерном радиотехническом факультете Военной электротехнической академии связи имени С. М. Буденного. В июле 1941 г. первые выпускники этого потока были эвакуированы в Подмосковье, где был создан специальный учебный центр. Вот что вспоминал один из руководителей советской радиоэлектронной разведки генерал-лейтенант П. С. Шмырев: «В учебном центре изучали организацию радиосвязи в немецко-фашистской армии, в пределах того, что знали сами преподаватели. Тренировались в приеме на слух, изучали общевойсковые дисциплины» [2. С. 15].

Первым серьезным экзаменом для радиоразведки стало ее участие в битве под Москвой, где ей удалось совместно с другими видами разведки вскрыть создание немцами ударных группировок для наступления на Москву в самые драматические дни октября 1941 г. Бывший начальник разведки Западного фронта генерал Т. Ф. Корнеев так вспоминал о том периоде: «К 23 сентября 1941 года разведка фронта точно установила, что противник готовится к наступлению и создал для этого крупную группировку войск перед Западным и Резервным фронтами. Главную роль в обнаружении наступательных группировок выполнила радиоразведка Западного фронта. К тому времени значительно более эффективными стали авиационная и другие виды разведки, но первенство во вскрытии оперативных и тактических резервов противника принадлежит радиоразведке» [3].

В сентябре 1941 г. из Ташкента в Москву был переброшен 490-й радиодивизион, который стал радиодивизионом ОСНАЗ Ставки Верховного Главнокомандования. Дивизион успешно выполнял задачи по радиоразведке действий немецкой бомбардировочной авиации, устанавливал, с каких аэродромов какие самолеты и в каком количестве поднимаются в воздух для налетов на Москву. Эта информация представляла высокую ценность для сил ПВО нашей столицы.

Радиоразведчики сумели добыть сведения о сроке возобновления немецкого наступления на Москву в ноябре 1941 г., благодаря чему, как писал в своих воспоминаниях маршал Советского Союза В. Д. Соколовский, удалось своевременно (за двое суток) предупредить об этом войска. К концу ноября радиоразведчики доносили о понесенных противником больших потерях в живой силе и технике под Тулой, о нехватке оружия и боеприпасов под Волоколамском, о повсеместном дефиците горючего. Эти данные имели важное значение при определении сроков нашего контрнаступления под Москвой [3, 4].

Активно работали и советские дешифровальщики: «…Уже в первые дни войны Б. А. Аронским (с помощью своих помощников и переводчиков) были дешифрованы кодированные донесения послов ряда союзных Германии стран в Японии. По поручению Императора Японии послы докладывали

своим правительствам о том, что Япония уверена в их скорой победе над Россией, но пока сосредоточивает свои силы на юге Тихого океана против США (а ведь эта война тогда еще даже не началась!)» [5. С. 83].

В 1930-е годы Б. А. Аронский вскрыл ряд кодов иностранных государств. Вот что об этом писал ветеран советской криптографической службы Л. А. Кузьмин: «Дешифрование кода — работа чрезвычайно сложная и трудоемкая. Она предполагает тщательный отбор по внешним признакам из массы шифрперехвата комплекта криптограмм, — относящихся к данному коду, затем проведение очень скрупулезного статистического анализа, который должен отразить частоту появления, места и "соседей" каждого кодобозначения во всем комплекте. В связи с отсутствием в те годы специальной техники все это делалось вручную несколькими помощниками основного криптографа-аналитика. Тем не менее, многомесячная работа такого коллектива зачастую приводила к аналитическому вскрытию значительной доли содержания кодовой книги и возможности оперативного чтения очередных перехваченных кодированных телеграмм. Это и определило успех группы Аронского, сыгравшей огромное значение в исходе битвы за Москву» [5. С. 84].

Аналогичные сведения были получены С. С. Толстым путем дешифрования переписки линий связи высших эшелонов власти Японии [5. С.84]. В течение многих лет С. С. Толстой был ведущим специалистом в дешифровальной службе и внес большой вклад в развитие криптографии. Им лично и под его руководством было раскрыто много сложных шифров иностранных государств. Созданная им методика раскрытия ряда систем ручного и машинного шифрования имела большое практическое значение. В предвоенные годы С. С. Толстой возглавлял японский отдел дешифровальной службы НКВД. Одним из самых крупных успехов накануне войны было дешифрование группой специалистов во главе с Толстым японских шифрмашин, известных под названиями, данными им американцами: «оранжевая», «красная» и «пурпурная» [1, 5].

В качестве примера приведем сообщение, отправленное 27 ноября 1941 г. из Токио в посольство в Берлине, дешифрованное советскими специалистами: «Необходимо встретиться с Гитлером и тайно разъяснить ему нашу позицию в отношении Соединенных Штатов. Объясните Гитлеру, что основные усилия Японии будут сконцентрированы на юге (против США и Англии. — Б. А. и А. П.) и что мы предполагаем воздержаться от серьезных действий на севере (против СССР. — Б. А. и А. П.)» [1. С. 280]. Эта информация была подтверждена и другими источниками, в частности донесениями нашего знаменитого разведчика Р. Зорге. С началом войны разведчик и члены его группы прилагали все свои силы для получения конкретной информации, которую советское правительство считало жизненно важной для успешного продолжения войны и фактически для самого существования страны. Намерена ли Япония совершить нападение на СССР, чтобы «пожать руку» Германии на Урале, или она займется осуществлением давно разработанного плана захвата Малайи и голландской Восточной Индии, богатых каучуком и нефтью? Япония сделала свой выбор 2 июля 1941 г. в обстановке глубочайшей секретности на заседании кабинета, на котором присутствовал японский император. По мере того как сведения об этом выборе постепенно становились достоянием все более широкого круга лиц в правительстве Японии, группа Зорге наращивала объем пересылаемой в СССР информации. В течение лета, когда войска немцев неуклонно продвигались по направлению к столице СССР, Зорге передавал в Москву информацию о дальнейшем наиболее вероятном развитии событий на Дальнем Востоке. В конце концов, Зорге получил исчерпывающие сведения о решении Японии наступать в южном направлении и не начинать пока войну с Советским Союзом. Поэтому в начале октября 1941 г. Зорге передал свое окончательное заключение по этому вопросу: «Вступление Японии в войну против СССР не ожидается, по крайней мере, до весны следующего года» [6. С. 241]. Информация в Центр передавалась по радио. Шифрование осуществлялось с помощью характерного для советской разведки шифра разнозначной замены с перешифровкой книжной гаммой. Подробнее о криптографической деятельности Р. Зорге можно прочитать в статье [7].

При этом следует отметить, что окончательное решение по переброске войск с Дальнего Востока и из Сибири под Москву руководством СССР было принято после появления успешных результатов по чтению зашифрованной японской дипломатической переписки, которые позволили сделать вывод о том, что Япония не намерена начинать военные действия против СССР. Как раз в это же самое время немцы предприняли решительное наступление с целью захвата Москвы до начала зимы. Советское военное командование, не опасаясь удара в спину со стороны Японии, постепенно уменьшило свою Дальневосточную армию на 15 стрелковых и 3 кавалерийские дивизии, на 1700 танков и 1500 самолетов [6. С. 241]. Эти силы были вовремя переброшены на запад, к Москве. Они сыграли существенную роль в обороне столицы и контрнаступлении, завершившемся разгромом немцев.

Напряженный труд работников дешифровальной службы в начальный период войны был высоко отмечен партией и правительством. В газете «Правда» № 94 (8865) от 4 апреля 1942 г. был опубликован Указ Президиума Верховного Совета СССР «О награждении работников НКВД Союза ССР за образцовое выполнение заданий Правительства» от 3 апреля 1942 г. — 54 специалиста были награждены орденами и медалями Советского Союза, в том числе орденом Ленина награждены два капитана государственной безопасности Аронский и Толстой, орденом Трудового Красного Знамени 6 человек, орденами Красной Звезды и «Знаком почета» — 13 человек и медалями «За трудовую доблесть» и «За трудовое отличие» — еще 33 человека. Так советское правительство оценило вклад дешифровальщиков в победу под Москвой [5. С.83].

При рассказе о деятельности советских криптоаналитиков во время Великой Отечественной войны, разумеется, нельзя обойти тему знаменитого немецкого шифратора «Энигма». Именно во время битвы за Москву в 1941 г. первые два шифратора этого типа были захвачены нашими войсками, один из них — в начале декабря 1941 г., во время наступления на Клин. Также в этом году в советский плен попали несколько немецких шифровальщиков. Исследования машины «Энигма» велись по нескольким направлениям, и это дало свои результаты. В конце 1942 г. научные сотрудники специальной группы дешифровальной службы ГРУ с помощью агентуры выявили возможность дешифрования немецких криптограмм, зашифрованных «Энигмой», и приступили к конструированию специальных механизмов, ускоряющих процесс дешифрования. Советские специалисты сумели построить математическую модель немецкого шифратора, выявили слабости, которые могли способствовать процессу дешифрования. Кстати, эта информация была использована при совершенствовании советских шифрмашин, недостатки, присущие «Энигме», были исключены в принципе. Заслуги отечественных криптоаналитиков отражены в представлении к награждению орденами группы офицеров дешифровальной службы военной разведки, которое было подписано начальником ГРУ генералом И. И. Ильичевым 29 ноября 1942 г. К наградам были представлены 14 офицеров. Однако дешифровать удалось только старые радиоперехваты потому, что в январе 1943 г. немцы ввели ряд дополнительных уровней защиты. Преодолеть эти новинки советские криптоаналитики не смогли из-за отсталости электронной техники. При этом следует отметить, что от определения того, можно ли вообще дешифровать роторную шифрмашину, до практических результатов — дистанция огромного размера. Возможно, удавалось эпизодически вскрывать некоторые сообщения, однако о массовом чтении «Энигмы» в СССР говорить нельзя. Но это было закономерно, так как наши криптографы не обладали той исходной информацией, которая имелась у англичан, а также из-за отсутствия достаточных человеческих и материальных ресурсов и слабого развития «машинных» средств обработки информации. А теперь самое главное — огромный массив информации, касающейся дешифрования англичанами «Энигмы», в первую очередь содержание дешифрованных криптограмм, советское руководство получало по линии агентурной разведки. Исходя из этого разумно предположить, что руководители СССР и отечественных дешифровальных служб решили не тратить наши весьма ограниченные силы на «Энигму», так как в данном случае за нас всю необходимую работу делали англичане [8].

Иногда англичане передавали информацию, полученную из дешифрованных немецких криптограмм, официальным путем. Приведем пример. В начале февраля 1942 г. англичане дешифровали приказ верховного немецкого командования, в котором войскам, отступавшим на Восточном фронте, предписывалось не допустить попадание в руки противника новейшего вооружения, в особенности секретных бронебойных снарядов новой конструкции. Эту информацию передали в СССР. Только что закончилась битва под Москвой, советские войска захватили много немецкой техники и вооружения. Среди трофеев оказались и новые снаряды. Выяснилось, что их сердечник изготовлен из самого прочного в те времена материала — карбида вольфрама. Месторождений вольфрама на территории Германии и ее союзников не было, а значит, он поставлялся из нейтральных стран. Эту информацию сообщили англичанам и американцам, их спецслужбы провели ряд оперативных мероприятий и сумели перекрыть каналы поставки вольфрама в Германию, лишив ее военную промышленность ценного сырья [9].

Захватывали шифры у немецкой агентуры и сотрудники советской контрразведки. Заметим, что само наличие шифра у подозреваемого в военное время обычно служит доказательством его работы на противника. Вот один из примеров (октябрь 1941 г.): «Сержант Павлов, возвращаясь с дежурства в комендатуре, заметил женщину с большим узлом в руках, которая пробиралась огородами, часто оглядывалась и следила за мчавшимися по шоссе военными машинами. Поведение незнакомки показалось Павлову подозрительным. Он остановил ее и спросил, куда и зачем она идет. Женщина ответила, что ушла из села, которое заняли немцы, едва успев собрать все необходимое. Однако из узла торчал угол какой-то картины в раме, которую вряд ли можно было счесть за крайне нужную в пути вещь. Бдительный сержант предложил женщине следовать за ним в комендатуру. Подозрение подтвердилось. В узле при тщательном обыске были обнаружены **шифровальные таблицы** (выделено мной — Д.Л.) и адреса явок, куда "беженке" предстояло передавать собранные сведения» [10].

В заключение приведем оценку работы советских дешифровальщиков, данную бывшим генеральным директором ФАПСИ 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» [5. С. 85]. 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. *Анин Б. А., Петрович А. И.* Радиошпионаж. М.: Международные отношения, 1996.
2. *Бурнусов И.* Мэтр радиоэлектронной разведки // Независимое военное обозрение. 2009. № 3. С. 15.
3. http:// www. ww2history.ru.
4. *Шмырев П.* Часовые эфира (об истории радиоразведки) // Газета «Красная Звезда». 18 марта 2004 г. URL: http://offline.computerra.ru.
5. *Кузьмин Л. А.* Не забывать своих героев // Защита информации. Конфидент. 1998. № 1. С. 83–85.
6. *Кан Д.* Война кодов и шифров. М.: РИПОЛ КЛАССИК, 2004.
7. *Бутырский Л. С., Ларин Д. А., Шанкин Г. П.* Криптографический фронт Великой Отечественной. Разведка и контрразведка // Защита информации. INSIDE. 2010. № 2. С. 84–96; № 3. С. 80–88.
8. *Куличенко В.* Русские против «Энигмы» // Независимое военное обозрение. 2004. № 40. С. 7.
9. *Васильев В., Рощупкин В.* Вольфрам для фюрера // Независимое военное обозрение. 2004. № 46. С. 7.
10. *Сыромятников Б.* Неоценимый вклад. Военные контрразведчики в битве под Москвой // Независимое военное обозрение. 2006. № 44. С. 7.