

высказывание маршала А. Василевского: «В чём причины столь крупного просчета этого опытного и дальновидного государственного деятеля (Сталина — *Авт.*)? Прежде всего в том, что наши разведорганы, как справедливо отмечает в своих воспоминаниях Г. К. Жуков, не смогли в полной мере объективно оценивать поступавшую информацию о военных приготовлениях фашистской Германии и честно, по-партийному, докладывать ее И. В. Сталину. Я не буду касаться всех аспектов такого положения, они в основном известны. Остановлюсь лишь на том, что в этом, видимо, сыграла свою роль и некоторая обособленность разведуправления от аппарата Генштаба. Начальник разведуправления, являясь одновременно и заместителем наркома обороны, предпочитал выходить с докладом о разведанных непосредственно на Сталина, минуя начальника Генштаба. Если бы Г. К. Жуков был в курсе всей важнейшей развединформации... он, наверное, смог бы делать более точные выводы из неё и более авторитетно предоставлять эти выводы И. В. Сталину и тем самым в какой-то мере повлиять на убеждение И. В. Сталина, что мы в состоянии оттянуть сроки начала войны, что Германия не решится воевать на два фронта — на Западе и на Востоке»¹⁶⁹.

С началом Великой Отечественной войны было проведено мобилизационное развёртывание дешифровальной службы по штатам военного времени и организационное построение её применительно к условиям фронта. Военная обстановка потребовала перегруппировки и сосредоточения сил на главных направлениях. 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. При определении главных объектов

разработки внимание службы радиоперехвата и дешифровальных подразделений было, прежде всего, обращено на линии шифрованной связи верховного командования вооруженных сил Германии со штабами армий, корпусов и дивизий. Было установлено, что основными шифрами на этих линиях связи являлись шифрмашин «Энигма» и «Вернер-101», которые, как показал анализ, были наиболее стойкими шифрсистемами того времени. С первых дней войны советские дешифровальщики активно включились в боевую работу, уже на 20-й день войны был вскрыт один из действующих немецких шифров¹⁷⁰.

В течение войны успешно читалась переписка сетей военной полиции Германии, которая применяла такие же системы шифров, как и в войсковых радиосетях, с той лишь особенностью, что с введением суточного блока ключей немецкая полиция применяла ежедневно только два-три различных блока ключей. Одним из них переписывались подразделения полиции, находившиеся на оккупированной территории СССР, другим — на западе Европы и внутри Германии и третьим — на Балканах. Это давало возможность набирать необходимое количество радиogramм для их дешифрования. Дешифрованные материалы по немецкой полиции представляли определенную ценность для командования фронтов, органов госбезопасности и Центрального штаба партизанского движения. По этим материалам можно было судить о боевых действиях отдельных воинских частей и их дислокации, о действиях полицейских полков против партизан, о побегах военнопленных из лагерей и организации их розыска. В силу нехватки резервов немецкое командование часто вводило в боевые действия полицейские части. В таких случаях в полицейской шифрпереписке находила отражение информация военного характера¹⁷¹.

Битва за Москву

Большой вклад советские дешифровальщики внесли в победу под Москвой, «...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 ещё даже не началась!). Аналогичные сведения были получены С. С. Толстым путем дешифрования переписки линий связи высших эшелонов власти Японии»¹⁷². В качестве примера приведем сообщение, отправленное 27 ноября 1941 года

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.*)»¹⁷³. Эта информация была подтверждена и другими источниками, в частности, донесениями нашего знаменитого разведчика Р. Зорге (о его криптографической деятельности будет рассказано в следующей книге). Таким образом, руководство СССР убедилось, что Япония в ближайшее время не нападет на нашу страну и пошло на переброску войск с Дальнего Востока и из Сибири. 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.

Напряженный труд работников дешифровальной службы в годы войны был высоко отмечен партией и правительством. В газете «Правда» № 94 (8865) от 4 апреля 1942 года был опубликован Указ Президиума Верховного Совета СССР «О награждении работников НКВД Союза ССР за образцовое выполнение заданий Правительства» от 3 апреля 1942 года 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 Москвой¹⁷⁴.

Рассмотрим биографии знаменитых советских криптоаналитиков более подробно. Аронский Борис Алексеевич (1898–1976) родился 25 (12) апреля 1898 года в Москве в семье служащего. С 1907 года учился и в 1916 году окончил Московскую Практическую Академию Коммерческих наук (так в те годы именовалось одно из средних учебных заведений). В мае 1917 года призван на военную службу и направлен в Петергофскую (юнкерскую) Школу прапорщиков. После Октябрьской революции Аронский был призван в Красную Армию на военно-хозяй-

ственные курсы. С 1918 по 1922 годы проходил службу в системе военных комиссариатов Поволжья и Урала, где впервые познакомился с шифрработой. В 1922 году был откомандирован на службу в Спецотдел ВЧК. Постоянно заботясь о своём самообразовании, Борис Алексеевич постепенно стал знатоком русской и западной литературы, овладел французским, английским, немецким, итальянским, финским, японским и рядом других языков. Правда, эти знания были специфическими — в совершенстве он знал язык и стиль дипломатической переписки, что в сочетании с природным аналитическим даром сделало Бориса Алексеевича блестящим «взломщиком» кодов. Под кодом криптографы тогда понимали весьма распространенный шифр, представляющий собою обширный словарь, в котором каждому слову, знаку препинания или даже устойчивой группе слов приданы кодовые обозначения. В 1930 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 трудоёмкая. 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 всём комплекте. В связи с отсутствием в те годы специальной техники всё 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»¹⁷⁵.

Во время гражданской войны в Испании 1936–1939 дешифрование сообщений франкистов велось в Москве под руководством Б. А. Аронского. Вот лишь один из примеров их успешной работы. Из дешифрованной телеграммы советским специалистам стало известно о том, что франкисты намерены потопить советский корабль, который должен был выйти из французского порта Марсель в один из испанских портов. На борту этого судна находилось большое количество советских лётчиков, тан-

кистов и других военных специалистов, а также бойцов интербригад, следовавших на помощь республиканцам. Франкисты собирались выделить для перехвата этого корабля значительные силы флота и авиации. Сведения об этом были переданы капитану советского корабля, его выход из Марселя был задержан, а маршрут изменён. Так благодаря работе советских дешифровальщиков судно удалось благополучно добраться до порта назначения¹⁷⁶.

Как известно, в 1937–1938 годах волна репрессий прошла и по сотрудникам НКВД. Борис Алексеевич по воспоминаниям Л. А. Кузьмина рассказывал: «что эта участь миновала его, по-видимому, потому, что в то время он не являлся членом ВКП(б), а был всего лишь „рядовым спецом“. В партию же он вступил только в тяжёлое время войны»¹⁷⁷.

В 1939–1940 годах Аронский участвовал в советско-финской войне. За боевые заслуги Б. А. Аронский был награжден орденами Красного Знамени и Знак Почета, а во время Великой Отечественной — дважды орденом Ленина и орденом Трудового Красного Знамени. Трудно переоценить заслуги Б. А. Аронского и в Великой Отечественной войне. Позже Борис Алексеевич рассказывал, что работал в те годы неделями без сна и отдыха и был счастлив, поскольку своим трудом добывал материалы, нужные Верховному командованию для организации победы над фашизмом.

После войны по существовавшему тогда положению о выслуге лет он был награжден вторым орденом Красного Знамени. Окончил войну начальником отдела 5 Управления НКГБ СССР. После войны Б. А. Аронский преподавал криптографию на курсах в Спецшколе и в Высшей школе криптографов ГУСС. Вот что об этом вспоминал Л. А. Кузьмин: «После войны Борис Алексеевич передавал свой опыт молодежи в стенах Высшей школы криптографов (выросшей теперь в Институт криптографии, связи и информатики), слушателем которой в 1951 году стал и я. Занятия Б. А. Аронского состояли в раскрытии целой тетради составленных им „перехваченных кодированных телеграмм послов некоего государства в европейских столицах“ (на русском языке, поскольку он был уверен, что другие языки нам пока неподвластны). Он подталкивал нас к „легким местам“ этой переписки, мы постепенно надписывали карандашами над кодовыми знаками их смысловые эквиваленты и всё более уверенно находили всё новые и новые их

продолжения. Скажу прямо — это было захватывающим занятием, по сравнению с которым разгадывание кроссвордов стоит несколькими „этажами“ ниже. Курс лекций заканчивался экзаменом, состоявшим в раскрытии „новой перехваченной“ кодотелеграммы (у каждого своей). Так Борис Алексеевич наглядно проиллюстрировал технологию своего легендарного успеха времен начала войны. Фактически же его задача в военные годы была значительно труднее, поскольку первичный кодовый текст в то время уже перешифровывался еще каким-либо шифром. Принципиальные возможности „снятия“ такой перешифровки составляли содержание его последующих лекций. Мне довелось после окончания Школы, в 1953–1956 годах, работать с Борисом Алексеевичем в одной комнате и узнать из первых рук многие подробности его успехов военных лет, так что в достоверности вышесказанного у меня сомнений нет»¹⁷⁸.

Как опытный специалист Б. А. Аронский часто направлялся на наиболее важные и трудные участки дешифровальной работы. В 1954 году он был направлен в Специальную службу военно-морского флота, где и закончил военную службу в звании полковника в 1958 году. Б. А. Аронский скончался 15 февраля 1976 года и похоронен на Даниловском кладбище в Москве¹⁷⁹.



Рис. 9. Б. А. Аронский

Толстой Сергей Семенович (1899–1945) родился 5 октября (22 сентября) 1899 года в селе Старо-Захаркино Петровского уезда Саратовской губернии в семье служащего в Саратовском имении графов Толстых. Когда Сергею было 8 лет, семья с шестью детьми осталась без отца, а в 1916 году и без матери. В 1913 году С. С. Толстой окончил сельское училище и поступил на службу писмоводителем в Старо-Захаркинское волостное управление, а затем перешел на службу в штаб одной из воинских частей. С декабря

1917 года по август 1919 года принимал активное участие в организации Советов солдатских и крестьянских депутатов в родном селе. Организовал там волостной Комитет РКП(б), несколько раз участвовал в подавлении кулацких восстаний. В августе 1919 года был мобилизован в Красную Армию и в мае 1920 года, будучи писарем Штаба 34-й дивизии Красной Армии, впервые познакомился с шифровальной работой. В сентябре того же года был откомандирован в распоряжение специального отдела Реввоенсовета Республики. В 1921 году окончил специальные курсы ВЧК. С 1922 года работал в Специальном отделе ГПУ–ОГПУ.

В Спецотделе проявил себя талантливым специалистом. Его авторитет среди сотрудников Спецслужбы постепенно стал огромным. Талант С. С. Толстого особенно раскрылся в трудные предвоенные годы и годы Великой Отечественной войны. Не расставаясь с Москвой, С. С. Толстой оказывал действенную помощь испанским республиканцам в борьбе с генералом Франко. В 1940 году старший лейтенант госбезопасности Толстой, в связи с успешным завершением финской кампании, был награжден первым своим орденом — «Знак Почёта». В течение многих лет был ведущим специалистом в 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»¹⁸⁰. Таким образом, успешные результаты по чтению зашифрованной японской дипломатической переписки позволили сделать вывод о том, что Япония не намерена начинать военные действия против СССР. Это дало возможность перебросить большое количество сил на советско-германский фронт.

Вышеупомянутый Указ о награждении советских дешифровальщиков свидетельствует о том, что успехи С. С. Толстого в криптоанализе были очень весомы. Во время Отечественной войны С. С. Толстой был ещё раз награжден

орденом Ленина, орденами Красного Знамени и Трудового Красного Знамени и орденом Знак Почёта. Уже одно то, что даже непосредственные начальники Толстого и Аронского не имели стольких наград, говорит о важности дешифрованной ими информации для Верховного командования. Окончил войну С. С. Толстой полковником, заместителем начальника отделения 5 Управления НКГБ СССР. В качестве почётного гостя вместе с дочерью Ольгой он был приглашен на исторический Парад Победы.

Сергей Семёнович активно участвовал в обучении криптографов на курсах и в Специальной школе. Нельзя не отметить и тот факт, что С. С. Толстой в соавторстве с Б. А. Аронским, С. Г. Андреевым и А. И. Копытцевым (последние двое упомянутым Указом выше были отмечены орденами Трудового Красного Знамени) в 1939–1940 годах написали один из первых советских учебников криптографии¹⁸¹. Полковник Толстой умер 23 июля 1945 года от обширного кровоизлияния в мозг прямо на рабочем месте. Видимо, сказалось громадное нервное напряжение четырёх военных лет, а в июле для ведущего дешифровальщика война была еще в самом разгаре. Бывшие сослуживцы и помощники рассказывали, что он был одержим работой, о его характере и аналитических способностях сложены легенды.



Рис. 10. С. С. Толстой

В упоминавшемся выше Указе Президиума ВС СССР 1942 года в список награжденных включены полковник Михаил Николаевич Нестеренко и подполковник Давид Михайлович Трусканов, которые в своей работе показали, что разрекламированный критерий стойкости шифра — огромное количество ключей к нему — не всегда гарантирует невозможность его вскрытия.

По ленд-лизу было получено несколько экземпляров американского шифратора М-209 (ли-

цензионная копия шифратора С-38 знаменитой фирмы «Хагелин»), которые возможно были использованы в качестве прототипов для создания своих собственных шифрмашин, хотя об их применении на практике ничего достоверно не известно¹⁸². Не исключено, что американцы допустили намеренный недосмотр, «забыв» снять эти машинки с кораблей, поставляемых нашей стране по ленд-лизу в 1942–1944 годах, чтобы навязать

нам их широкое применение. Однако наши спецслужбы на эту удочку не попались, своевременно нащупав несколько способов дешифрования этой шифрмашинки, тем не менее сделавшей её создателя Бориса Хагелина миллионером. Обнаруженные слабости американских шифрмашин М-209, наряду с их широким распространением достаточно долго позволяли снабжать руководство СССР полезной информацией¹⁸³.

Радиодивизионы особого назначения

7 мая 1895 года русский ученый А. С. Попов выступил с публичным докладом на заседании физического отделения русского физико-химического общества, в ходе которого продемонстрировал первый в мире радиоприемник. Уже первые испытания беспроводного телеграфа на флоте доказали превосходство радио над другими средствами связи. Одновременно с опытами по радиосвязи на флоте подобные работы стали проводиться и в армии. Началом таких опытов нужно считать 1898 год. Именно с этого времени в них участвовал целый ряд армейских телеграфных специалистов.

Радиоразведка родилась в России. Первые опыты по перехвату иностранных радиogramм были проведены моряками Балтийского флота летом 1902 года под руководством изобретателя радио Александра Степановича Попова. В 1903 году на российском флоте началось регулярное ведение радиоразведки, что нашло отражение в одном из важнейших флотских документов — «Своде военно-морских сигналов»¹⁸⁴. Практический опыт ведения радиоразведки оказался востребован уже во время русско-японской войны 1904–1905 годов. Россия стала пионером в новых видах боевых действий — радиоразведке и радиоэлектронной борьбе. Приоритет в использовании этих новых видов боевых действий принадлежит российскому военно-морскому флоту. Фактически, русские моряки начали войну в новом измерении — радиоэфире¹⁸⁵.

Опыт боевого применения средств радиосвязи в 1904–1905 годах ознаменовало собой появление нового вида боевого противоборства — радиовойны. Получение сведений о вероятном противнике с помощью радио значительно расширяло разведывательные возможности. Но для этого нужна была эффективная служба

наблюдения. В проекте закона «Об императорском российском флоте» 1911 года в 27-й статье так определено содержание и направление дальнейшего развития службы наблюдения и связи: «Побережье Балтийского, Черного морей и Тихого океана должны быть оборудованы сооружениями для наблюдения за прилегающим водным пространством и для связи с флотом соответствующим числом береговых наблюдательных постов и радиотелеграфных станций»¹⁸⁶.

Радиоразведка получила развитие в последующие годы. Так во время учебных походов кораблей Балтийского флота в 1911–1913 годах ведение радиоразведки было одной из приоритетных задач и осуществлялся активный перехват иностранных радиogramм. В это время были созданы специальные контрольные, а затем и разведывательные станции. Первые были предназначены для наблюдения за радиообменом своих сил в целях пресечения нарушений установленного порядка радиопереговоров. Вторые — имели задачей перехват и дешифрование радиопередач противника. Такие станции, созданные на Балтийском и Черном морях, в комбинации с береговыми радиопеленгаторами в течение Первой мировой войны давали неоценимую информацию о содержании радиопереговоров противника и позволили провести ряд успешных боевых операций. Во время гражданской войны в России радиоразведку вели обе стороны и белые и красные¹⁸⁷.

После окончания гражданской войны ведение радиоразведки начало восстанавливаться лишь в 1929–1930 годах. Для руководства радиоразведкой и централизованной обработки сведений в состав Разведывательного управления в 1930 году была введена секция радиоразведки, которую возглавил бригадный инженер