

тических методов. В целях организации и координации научных исследований и подготовки научных кадров в 1942 году в составе 5 Управления НКВД был создан Криптографический совет и редакция «Криптографического сборника», в состав которой вошли Б. А. Аронский, С. С. Толстой, А. В. Австриаков и другие.

За время войны Криптографический совет рассмотрел более 60 проблем и вопросов по основным направлениям специальной работы и подготовки кадров. В дальнейшем в «Криптографических сборниках» публиковались наиболее важные результаты криптографических исследований, материалы по обмену опытом и повышению деловой квалификации. Издавались учебные пособия для школы... Для укомплектования пятых (дешифровальных) отделений разведотделов фронтов в ноябре 1941 года туда были направлены все выпускники спецотделения Разведывательных (дешифровальных) курсов усовершенствования Высшей школы Генштаба. В декабре 1942 года на базе Школы особого назначения 5 Управления НКВД и 3-го учебного отделения Высшей школы Генштаба была организована Специальная школа 5 Управления НКВД в составе двух отделений с 10 месячным сроком обучения. Первое отделение этой школы готовило кадры криптографов для дешифрования военной переписки, а второе отделение — для дешифрования дипломатической переписки. Получаемые в школе специальные и языковые знания позволяли ее выпускникам быстро включаться в работу.

В годы Великой Отечественной войны криптографические подразделения дешифровальной службы пополнялись в основном за счет окончивших Специальную школу 5 Управления НКВД, в которой были подготовлены многие ведущие специалисты. Специальная школа, а также ряд криптографических подразделений, находящихся в Уфе, подчинялись А. И. Копытцеву.

Вместе с передачей 3-го отделения Высшей школы ГШ в состав Специальной школы из НКО были переведены в Специальную службу госбезопасности и опытные криптографы, в том числе М. С. Одноробов, Н. В. Пишенин, Г. И. Пондопуло, М. И. Соколов, А. Ф. Яценко и другие.



Рис. 12. Руководитель дешифровальной службы в годы войны генерал-майор А. И. Копытцев

Одновременно в подразделениях Специальной службы принимались меры для повышения квалификации работавших там специалистов. Была создана система различных курсов по криптографии и изучению иностранных языков. Почти каждый сотрудник, имевший отношение к разработке шифров, изучал криптографию и, в той или иной мере, иностранный язык. В этот период в криптографическую практику все активнее внедрялись научные методы анализа, основанные на использовании закономерностей языка. Поэтому при наборе в Службу отдавалось предпочтение лицам с физико-математическим образованием. Партийные органы энергично помогали Спецслужбе в подборе кадров. По решениям ЦК и МГК ВКП(б) на криптографическую работу в НКВД и НКО отбирались математики и лингвисты из научных учреждений и различных учебных заведений<sup>231</sup>.

## Работа ГРУ

В первые годы Великой Отечественной войны дешифровальной работой в СССР занимались органы государственной безопасности (о их деятельности см. выше), ГРУ Генерального штаба вооруженных сил СССР и дешифровально-разведывательная служба ВМФ. Расскажем о деятельности этих организаций подробнее.

Начнем с военных разведчиков. Выше уже отмечалось, что в 1941 году в состав ДРС РУ ГШ зачислена большая группа молодых ученых с основательной математической и технической подготовкой, выпускников ведущих вузов призванных в армию. К сожалению авторам не удалось найти сведения о всех этих людях.

Приведем краткие биографии В. С. Полина, Г. И. Пондопуло и М. И. Соколова.

Полин Владимир Степанович (1907–1975) Кандидат технических наук полковник В. С. Полин родился 19 июля 1907 года в Туле в семье потомственного оружейника. Перед Великой Отечественной войной успел защитить кандидатскую диссертацию в Московском педагогическом институте имени К. Либкнехта. Пришел в криптографическую службу после всеобщей мобилизации в июне 1941 года и вскоре стал конструктором и организатором применения вспомогательной техники криптоанализа. Его труд во время войны отмечен несколькими орденами и медалями. Позднее во время гонений на кибернетику как «буржуазную лженауку» Полин собирал коллектив единомышленников для создания ЭВМ общего и специального применения. В заслугу этому коллективу можно поставить разработку целого ряда компьютеров. В частности, одна из последних в Союзе ламповых машин «Иней» и одна из первых в стране ЭВМ 2-го поколения полупроводниковая «Весна» превосходили по ряду параметров широко известные отечественные М-20 и БЭСМ-6 и долго работали во многих отраслях науки и промышленности. За эти работы В. С. Полина, его соратникам и ученикам — в том числе и воспитанникам Школы криптографов — впервые в истории ГУСС была присуждена Ленинская премия.



Рис. 13. В. С. Полин

В. С. Полин преподавал в Высшей школе криптографов дисциплину о вспомогательной технике криптоанализа. Эта техника в то время представляла собой отдельные релейные или многоламповые устройства, облегчавшие криптографу трудоёмкие процессы статистического анализа шифрперехвата, однако было ясно, что вскоре ей предстоит занять в криптоанализе более важное место. Умер Владимир Степанович 20 августа 1975 года<sup>232</sup>.



Рис. 14. Г. И. Пондопуло

Георгий Иванович Пондопуло (1910–1994) родился 21 апреля 1910 года на юге России в семье фельдшера и учительницы. В 1928 году окончил Краснодарский педагогический техникум и затем три года проработал учителем в станице Смоленской. Там же был избран секретарем комсомольской ячейки. В 1932 году Г. И. Пондопуло поступил на механико-математический факультет МГУ им. Ломоносова, а в 1937 с отличием его окончил. Во время учебы в аспирантуре был избран секретарём комитета комсомола МГУ. К маю 1941 года он полностью подготовил к защите диссертацию, посвященную обтеканию решётки газом при больших скоростях. К этому времени он был призван в Спецслужбу Красной Армии. Однако в связи с тем, что все отзывы на его диссертацию уже были получены, а день защиты в Совете МГУ назначен, 26 июня командование в порядке исключения предоставило Георгию Ивановичу отпуск на полдня. Диплом кандидата наук он получил уже по окончании войны. В 1941–1942 годах Г. И. Пондопуло работал в Специальной службе Генерального штаба РККА. Приход в Службу Георгия Ивановича и других специалистов с основательной математической и технической подготовкой явился важным фактором активизации деятельности Службы, расширения фронта её работ, внедрения в её работу математических методов.

Ещё в апреле–мае 1941 года в отечественную криптографическую службу было направлено несколько десятков молодых математиков и физиков из МГУ и Военной академии связи. Они привнесли в криптографическую работу новые идеи. Вот что пишет о вкладе этих специалистов в Победу Л. А. Кузьмин: «Если „старики“ умели кропотливо, шаг за шагом накапливать сведения о ключе шифра противника, то математики, анализируя логику построения лишь частично известного ключа, находили алгоритмы его существенного пополнения. Инженеры и физики начали создавать и внедрять в анализ шифров вспомогательную технику. Эти два фак-

тора способствовали совершению качественного скачка в раскрытии часто изменяющихся ключей вермахта. Уже к началу Курской битвы такие методы стали приносить Ставке ценнейший материал о перегруппировках сил противника и его планах»<sup>233</sup>. Немалый вклад в становление этих методов внес Г. И. Пондопуло, вообще следует отметить, что в ходе войны он занимался исследованием наиболее сложных шифрсистем противника.

С 1942 по 1946 год Г. И. Пондопуло проходил службу в НКВД (НКГБ) на различных должностях от старшего оперуполномоченного до заместителя начальника отдела. В 1946–1950 годах он работал в МГБ СССР в должности заместителя начальника отдела. Георгий Иванович обладал высоким авторитетом среди советских математиков и механиков. Вполне закономерно, что когда в 1949 году для подготовки специалистов по криптографии было организовано закрытое отделение мехмата МГУ, его возглавил именно Г. И. Пондопуло. Он также являлся заместителем декана мехмата МГУ, при этом педагогической деятельностью Георгий Иванович занимался по совместительству без отрыва от основной службы. Обладая хорошей математической и криптографической подготовкой, Г. И. Пондопуло многое сделал для организации, становления и развития закрытого отделения, в частности он преподавал новые математические методы анализа современных шифров. Выпускники отделения имели глубокие математические знания и в значительной степени способствовали повышению научного уровня работы ГУСС (в 1949 году было создано Главное Управление Специальной Службы, основная криптографическая организация страны) и успешному решению стоящих перед ним задач. С 1950 по 1953 год Г. И. Пондопуло был начальником лаборатории в НИИ-1 ГУСС при ЦК ВКП(б). Пребывая на этих должностях, Г. И. Пондопуло продолжал научную работу по исследованию глубоких свойств современных шифров.

Г. И. Пондопуло совместно с И. Я. Верченко и Е. Ф. Баженовым принимал участие в становлении технического факультета Высшей школы КГБ. Заслуга в создании внутри чекистского вуза особой, неповторимой научной атмосферы, сочетавшей в себе высокую воинскую требовательность и дисциплину с глубоким уважением слушателей к своим педагогам, безусловно, принадлежит профессорам И. Я. Верченко и Г. И. Пондопуло. С мая 1953 по 1976 год Георгий

Иванович Пондопуло возглавлял кафедру криптографии на техническом факультете. Он внёс значительный вклад в подготовку специалистов для практических подразделений и уделял большое внимание подготовке научных кадров. Научные интересы Г. И. Пондопуло были связаны с изучением свойств дисковых шифраторов. Эти проблемы были весьма актуальны, ими занимались многие специалисты-криптографы (М. И. Соколов, Г. В. Чуриков, А. А. Блинов, В. И. Бобылев и многие другие).

Г. И. Пондопуло поддерживал тесный контакт с широким кругом представителей математической общественности СССР. Благодаря этому у слушателей и аспирантов имелась возможность посещать семинары крупных математиков: члена-корреспондента АН СССР Андрея Андреевича Маркова и академика (позже Героя Социалистического труда) Константина Константиновича Марджанишвили и др. Осуществлялось тесное взаимодействие с представителями практических подразделений. Тесное творческое общение с прекрасными специалистами и уже накопленный опыт позволили преподавателям и сотрудникам приступить к работе над учебными пособиями на новом уровне.

В 1965 году ВАК СССР утвердила Г. И. Пондопуло в звании профессора по кафедре прикладной математики, а Президиум Верховного Совета РСФСР 5 февраля 1975 года присудил почётное звание Заслуженного деятеля науки и техники (возможно, это единственный случай в Спецслужбе того времени). За свои заслуги перед страной Георгий Иванович награжден орденом «Знак Почета» и многими медалями, а также знаком «Почетный сотрудник госбезопасности». В отставку полковник Пондопуло вышел в 1976 году, после чего длительное время преподавал в Московском институте электронного машиностроения. Умер он 15 сентября 1994 года и похоронен на Хованском кладбище<sup>234</sup>.



Рис. 15. М. И. Соколов

Соколов Михаил Иванович (1914–1998) родился в Москве, детдомовец. В 1938 году с отличием окончил механико-математический факультет МГУ. Затем успешно окончил аспирантуру при НИИ Механики МГУ. В 1941 году М. И. Соколову была присвоена ученая степень кандидата физико-математических наук. С 1941 года работал в Специальной службе Генерального штаба Красной Армии, а затем в Специальной службе органов госбезопасности. Внес большой вклад в дешифрование шифрпереписки Германии и её союзников во время Великой Отечественной войны, а также подготовку молодых специалистов. После войны М. И. Соколов работал в криптографических подразделениях и продолжал преподавательскую деятельность.

М. И. Соколов был первым начальником кафедры криптографии в Высшей школе криптографов ГУСС. Он является автором многочисленных научных и учебно-методических работ. Так же М. И. Соколов работал ученым секретарём в НИИ-1 ГУСС, был редактором ряда научно-технических сборников. Был научным руководителем 6 аспирантов, которые успешно защитили диссертации. Доцент, старший научный сотрудник, полковник. М. И. Соколов награжден 2 орденами и 20 медалями<sup>235</sup>.

В 1942 году в состав Разведуправления Красной Армии входила и дешифровальная служба. Сотрудники этого вида разведки в 1942 году добились значительных результатов. Дешифровальной службой ГРУ было раскрыто 75 шифров немецких вооруженных сил и разведки, в результате чего прочитано свыше 25 000 немецких радиogramм. Полученные таким путем сведения о противнике позволили установить дислокацию свыше ста штабов соединений, раскрыть нумерацию двухсот отдельных батальонов и других частей немецкой армии. В период Сталинградской битвы радиотехническая разведка и дешифровальная служба ГРУ добились значительных успехов. К началу контрнаступления наших войск была вскрыта группировка войск противника перед Юго-Западным, Донским и Сталинградскими фронтами, где вели боевые действия 6-я армия и 4-я танковая армии немцев. В ходе контрнаступления радиоразведка фронтов достаточно полно освещала подготовку контратак противника, переброску резервов, а также потери в живой силе и технике. В 1942 году дешифровальная служба Разведуправления Красной

Армии вскрыла основные немецкие и японские системы общевойсковых, политических и дипломатических шифров, шифры немецкой разведки. Специалистам дешифровальной службы удалось прочесть более 50 тысяч шифртелеграмм противника<sup>236</sup>. В конце ноября, когда кольцо окружения немецко-фашистских войск в районе Сталинграда сомкнулось, радиоразведкой было установлено, что в окружении находились штабы 6-й полевой армии, 4, 8 и 51-го армейских корпусов, 11-го механизированного корпуса, 14-го танкового корпуса, а также шести танковых и механизированных дивизий и тринадцати пехотных дивизий противника, т. е. группировка окруженных немецких войск была вскрыта полностью. Победа под Сталинградом стала переломным моментом в ходе войны. При этом среди трофеев оказалось большое количество аппаратуры связи, советские войска захватили 696 радиостанций и 933 телефонных аппарата<sup>237</sup>.

В ноябре 1942 года, в самый разгар Сталинградской битвы, в соответствии с приказом НКО № 00222 от 23 октября 1942 года о реорганизации ГРУ ГШ КА в ГРУ КА и УВР ГШ КА дешифровальная служба военной разведки и 8 отдельных радиодивизионов ОСНАЗ переданы в НКВД, где созданы полевые управления специальной службы, а дивизионы переформированы в отдельные дивизионы спецслужбы, центральную и отдельную радиостанции войск НКВД<sup>238</sup>.

Криптоаналитики органов безопасности активно работали на победу. Так к весне 1942 года было дешифровано 50 тысяч только немецких телеграмм, не считая переписки Румынии и других стран гитлеровской коалиции. В 1942 году 5 отдел НКВД СССР помимо исследования и составления кодов, издания шифр-блокнотов для государственных учреждений и др. вел дешифровально-разведывательные работы не только по Германии, но и Англии, США, Италии, Испании, Франции, Бельгии, Турции, Ирану, Ираку, Афганистану, Китаю, Балканам, странам Скандинавии, Финляндии, Японии, Маньчжоу-Го. В 1942 году в НКВД из ГРУ Генштаба Красной Армии были переданы дешифровальная служба военной разведки и 8 отдельных радиодивизионов, а из Наркомата обороны переведены опытные криптографы Одноробов М. С., Пишенин Н. В., Полин В. С., Пондопуло Г. И., Соколов М. И., Яценко А. Ф. и другие<sup>239</sup>.

Одноробов Михаил Спиридонович (1910–1997). Окончил МГУ им. Ломоносова. В специальной службе с 1941 года по 1973 год. За 32 года своей работы внес заметный вклад в совершенствование советской криптографической службы и подготовку кадров для неё. М. С. Одноробов был криптографом военной мобилизации. Он внес немалый вклад в становление математических методов криптоанализа. М. С. Одноробов был участником Великой Отечественной войны, в 1943–1944 годах был заместителем начальника 7-го Полевого отдела (1-й Белорусский фронт). После войны неоднократно выполнял поручения Правительства по оказанию помощи дружественным странам в организации шифрованной связи. С 1951 по 1965 годы был начальником отдела 8 Главного управления КГБ СССР. С 1965 по 1973 годы был начальником Службы 8 Главного управления. М. С. Одноробов принимал активное участие в подготовке инженеров и специалистов для советской криптографической службы. В Высшей школе криптографов ГУСС Одноробов преподавал ряд дисциплин, в том числе «Основы криптографии». Вот что вспоминал Л. А. Кузьмин: «Лекции Михаила Спиридоновича состояли из двух частей. Первая содержала систематизированное описание классических шифров с анализом их слабостей и подходов к их взлому, вторая же знакомила с только что опубликованной в западной печати математической теорией стойкости секретных систем Клода Шеннона. Практические занятия по курсу состояли, как и следовало ожидать, в дешифровании всё более сложных шифров. Это было столь увлекательно, что добрая половина группы „заболела“ страстью раскрытия шифрпереписки, несмотря на заветы матерей, считавших, что „читать чужие письма — грешно!“. Однако успехи советских криптографов времен войны заставляли забыть материнский наказ, находились и слова классиков марксизма (особенно Энгельса), подтверждавшие необходимость такой работы. И хотя не все однокурсники в дальнейшем посвятили свою жизнь криптографии, думаю, что большинство „отступников“ покинули её не из-за твёрдости своих моральных устоев, а испугавшись тягот каждодневного напряженного умственного труда, не отпускавшего мозг полностью даже во сне»<sup>240</sup>. Почетный сотрудник госбезопасности, полковник М. С. Одноробов был награжден орденами Красного Знамени, Отечественной войны и Красной Звезды (дважды), а также 25 медалями<sup>241</sup>.



Рис. 16. М. С. Одноробов

Иногда из радиоперехвата вражеских сообщений выявлялись недостатки в организации ведения боевых действий советских войск, в качестве примера приведем следующий документ:

«СООБЩЕНИЕ ГУКР „СМЕРШ“ НКО СССР № 193/А В ГКО И ГЕНШТАБ РККА ОБ ОБНАРУЖЕНИИ ПРОТИВНИКОМ ПЕРЕГРУППИРОВКИ НАШИХ ВОЙСК НА УЧАСТКЕ 39-Й АРМИИ ВСЛЕДСТВИЕ НАРУШЕНИЯ ПРАВИЛ МАСКИРОВКИ

7 августа 1943 г.

По сообщению УКР „Смерш“ Калининского фронта, противник с воздуха обнаружил начавшуюся 25 июля сего года перегруппировку наших войск на участке 39-й армии.

Произошло это вследствие того, что передвижение войск происходило с нарушением маскировки. Во время движения, особенно в ночное время, раскладывались костры, автомашины двигались со светом, техника сосредотачивалась в большом количестве на открытой местности.

Обнаружив перегруппировку наших войск, авиация противника начиная с 27 июля сего года групповыми и эшелонированными налётами стала бомбить сосредоточение войск и техники на железнодорожной ст. Ломоносове и переднем крае, в то время как до этого налеты авиации противника на участке 39-й армии носили одиночный характер.

Кроме того, перехваты радиogramм противника за последние дни также дают основание полагать, что немцы обнаружили перегруппировку наших войск на участке 39-й армии.

26 июля сего года отдел „Смерш“ 39-й армии о фактах демаскировки и беспорядках при перегруппировке войск доложил Военному совету армии, который принял необходимые меры к восстановлению порядка.

Начальник ГУКР „Смерш“ НКО СССР  
Абакумов.  
ЦА ФСБ России»<sup>242</sup>.