
Криптографическая служба Российской Федерации: история создания и развития в XX в. (к 100-летию образования)

Василий Христофоров, Юлия Гусева

**The centenary of the Cryptographic service of the Russian Federation:
creation and development during the 20th century**

*Vasiliy Khristoforov (Russian State University for the Humanities;
Institute of Russian History, Russian Academy of Sciences, Moscow),
Yulia Guseva (Moscow, Russia)*

DOI: 10.31857/S086956870014467-4

Национальная безопасность напрямую зависит от многих факторов, среди которых важнейшей традиционно считается степень боеготовности и боеспособности вооружённых сил. В XXI в. всё большее значение приобретает также комплексная системная защита информации, составляющей государственную тайну. Возрастание роли криптографической службы¹ связано с активным внедрением разветвлённых систем связи, современных технологий обработки информации, широким использованием новейшей техники. В этих условиях проблема защиты информации как никогда актуальна, так как информационное противоборство становится одним из ключевых элементов локальной и глобальной политической повестки.

Академическая актуальность нашего исследования связана с изучением истории становления российской криптографии как части научно-технической политики СССР. В более узком смысле данная тема позволяет рассмотреть историю шифровального дела, вопросы защиты информации и обеспечения информационной безопасности, сотрудничества на этом поприще представителей научно-технической элиты страны и специалистов органов госбезопасности, взаимодействия подразделений, занимавшихся дешифровкой сообщений иностранных государств, и контрразведки.

Научные и научно-популярные издания, посвящённые истории криптографии в России, немногочисленны, но заслуживают внимания. Среди них особый интерес представляет книга Т.А. Соболевой — первое монографическое исследование на эту тему². Среди исследователей необходимо также отметить Л.С. Бутырского, Ю.И. Гольева, Д.А. Ларина, Е.А. Тришина, Г.П. Шанкина и др.³ Книга Б.Ю. Анина, много лет проработавшего в КГБ СССР, посвящена

© 2021 г. В.С. Христофоров, Ю.Н. Гусева

¹ Под криптографической службой понимается совокупность общегосударственных и ведомственных органов, осуществляющих разработку и эксплуатацию шифровых средств для передачи секретной информации по каналам связи, а также добывание информации путём её перехвата, дешифровки и анализа.

² Соболева Т.А. История шифровального дела в России. М., 2002.

³ Гольев Ю.И., Ларин Д.А., Тришин Е.А., Шанкин Г.П. Криптография. Страницы истории тайных операций. М., 2008; Бутырский Л., Ларин Д., Шанкин Г. Криптографический фронт Великой Отечественной. М., 2012; Ларин Д. Криптографическая служба России. Очерки истории. М., 2017; Ларин Д.А. Организация шифрованной связи во время конференций лидеров союзных государств

истории мирового радиоэлектронного шпионажа — разновидности шпионской деятельности, заключающейся в получении секретной информации из каналов связи. В ней содержится масса неизвестных фактов об операциях спецслужб иностранных государств и о работе КГБ⁴. В книгах А. Клепова⁵ и Г.А. Куренкова⁶ рассматриваются разносторонние вопросы защиты информации, в том числе вопросы её шифрования в партийных организациях. В книге М. Малиновской и Л. Эйтингона показано противоборство советских и американских спецслужб в сфере криптографии⁷.

В следующую группу входят труды, посвящённые вкладу научных и научно-исследовательских организаций СССР в победу в Великой Отечественной войне⁸, а также исследования о политических репрессиях среди научных работников⁹ и инженерно-технического персонала, изучению организации труда заключённых (конструкторов, инженеров, учёных и вольнонаёмных специалистов) в системе спецслужб в 1930—1950-х гг.¹⁰ Деятельность Особых технических бюро ОГПУ—НКВД—МВД СССР, 4-го спецотдела НКВД, а также различного рода спецтюрем-«шарашек», в которых использовался принудительный труд репрессированных, исследовали С.П. Стрекопытов¹¹, М.Ю. Моруков¹², А.И. Кокурин¹³ и др.¹⁴

Указанные научные и научно-популярные работы позволяют составить общее представление об истории криптографической службы в России в 1921—

в 1943—1945 годах // Великая Победа: в 15 т. / Под общ. ред. С.Е. Нарышкина, А.В. Торкунова. Т. XIV. Не стереть из памяти. М., 2015. С. 273—278.

⁴ Анин Б.Ю. Радиоэлектронный шпионаж. М., 2000.

⁵ Клепов А. Шифраторы и радиоразведка. Щит и меч информационного мира. Т. 1. Записки криптографа. М., 2015.

⁶ Куренков Г.А. От конспирации к секретности. Защита партийно-государственной тайны в РКП(б)—ВКП(б). 1918—1941. М., 2015.

⁷ Малиновская М., Эйтингон Л. На предельной высоте. О парашютистке и разведчице Музе Малиновской и генерале государственной безопасности Науме (Леониде) Эйтингоне. Великие Луки, 2009. С. 171—174.

⁸ Академическая наука — фронту. К 70-летию победы в Великой Отечественной войне 1941—1945 / Сост. В.И. Васильев, А.А. Макося; под ред. В.Е. Фортова. М., 2015; Вклад в Победу научно-исследовательских организаций СССР 1941—1945. Сборник документов. Т. 1: Эвакуация 1941—1942 / Сост. Л.Ю. Покровская, В.Н. Парамонов, О.Н. Солдатова, М.К. Сурина. Самара, 2016.

⁹ Репрессированная наука (библиографический указатель литературы за 1988—2008 гг.) / Сост. О.В. Кузьмина, И.Л. Сабельникова, О.Н. Солдатова, Е.Л. Храмова. Самара, 2009. С. 449—619.

¹⁰ Солдатова О.Н. Изобретатели и изобретательская деятельность в развитии научно-технического прогресса промышленности советского государства (1917—1956 гг.). Самара, 2013; Солдатова О.Н. Деятельность репрессированных учёных и изобретателей в годы Великой Отечественной войны (1941—1945 гг.) // Телескоп: научный альманах. Самара, 2005. С. 178—182.

¹¹ Стрекопытов С.П. История научно-технических учреждений в России (вторая половина XIX — XX вв.). Учебное пособие. М., 2002. С. 248—266.

¹² Моруков М.Ю. Особое техническое бюро // МВД России: энциклопедия. М., 2002. С. 371—374; Моруков М.Ю. Особые технические бюро ОГПУ—НКВД—МВД СССР // Исторические чтения на Лубянке. 2000 год. Отечественные спецслужбы накануне и в годы Великой Отечественной войны 1941—1945. М., 2001. С. 127—134.

¹³ Кокурин А.И. Организация и деятельность 4 спецотдела НКВД—МВД СССР (1939—1953 гг.) // Телескоп. Самара, 2008. С. 47—68.

¹⁴ Зимин В.А. Репрессированные учёные-связисты (по документам филиала РГАНТД) // Телескоп. Самара, 2008. С. 33—39; Христофоров В.С. Тюремно-морская «одиссея» инженера Н. Лапина // Там же. С. 135—146; Парамонов Р.Н. «Шарашки» как уникальный институт советского общества // Политические репрессии первой половины XX века в судьбах технической интеллигенции России. Материалы всероссийской конференции. Самара, 2009. С. 183—193.

1991 г., проанализировать основные направления разработки и производства специальной и шифровальной техники.

Большинство документов по данной проблематике сохраняют актуальность и потому находятся на секретном хранении до 2044 г. Наше исследование базируется на комплексе рассекреченных документов государственных и ведомственных архивов: ГА РФ, РГАСПИ, Центрального архива ФСБ России и архивов УФСБ по Архангельской, Курской и Орловской областям, Центрального архива Министерства обороны Российской Федерации (ЦА МО РФ). Документы ГА РФ позволяют реконструировать процесс создания Спецотдела при ВЧК, установить его основных сотрудников, исследовать причины межведомственной конкуренции и т.д. Документы ведомственных архивов (ФСБ и Минобороны) свидетельствуют, сколь важное значение придавалось шифровальному делу, какое влияние имели органы госбезопасности на другие структуры и ведомства в процессе организации и деятельности криптографической службы, как взаимодействовали шифровальные службы различных ведомств.

Среди публикаций источников обратим внимание на сборник «Органы государственной безопасности СССР в Великой Отечественной войне» в 6 томах и 11 книгах, документы которого свидетельствуют, что радиоконтрразведка и дешифровальная служба НКВД с первых дней войны вели перехват и контроль переписки частей и соединений германских и японских вооружённых сил и разведывательных органов¹⁵. В документах содержатся сведения об обнаружении радиостанций противника и отправке оперативно-розыскных групп для их деактивации, об использовании в радиоиграх захваченных агентов-радиостанций противника¹⁶. Опубликованные в сборнике «Курская битва глазами Лубянки» документы спецслужб свидетельствуют, что в период сражения дешифровальщики успешно вскрывали сообщения немецкого разведотдела армейской группы¹⁷. В 4—5 томах многотомного издания «Оборонно-промышленный комплекс СССР накануне и в годы Великой Отечественной войны» опубликованы документы об использовании труда заключённых специалистов, а также об улучшении работы радиопромышленности, форсировании оснащения армии радиоустановками по обнаружению самолётов, приёмопередающими радиостанциями. Кроме того, несомненный интерес представляют материалы о совершенствовании системы подготовки кадров¹⁸. Важное значение имеют постановления ГКО об обеспечении войск средствами связи, о плане производства и поставках основных средств связи для Главного управления связи Красной армии, о восстановлении и развитии заводов электровакуумной промышленности наркомата электропромышленности¹⁹. Некоторые документы

¹⁵ Органы государственной безопасности в Великой Отечественной войне. Т. 6. Победа (1 января — 9 мая 1945 г.) / Сост. В.П. Ямпольский, И.К. Белик, В.И. Кочанов, О.Б. Мозохин, Е.В. Шумилова, О.М. Тупицын. М., 2014.

¹⁶ Архив УФСБ России по Архангельской области, д. 259, л. 14; Органы государственной безопасности СССР в Великой Отечественной войне. Т. 3. Кн. 2. М., 2003. С. 245—246; Т. 4. Кн. 1. М., 2008. С. 429—430.

¹⁷ ЦА ФСБ России, ф. 40, оп. 24, д. 6, л. 258—258 об.; «Огненная дуга»: Курская битва глазами Лубянки / Сост. А.Т. Жадобин, В.В. Марковчин, В.С. Христофоров. М., 2003. С. 307.

¹⁸ Оборонно-промышленный комплекс СССР накануне Великой Отечественной войны (1938 — июнь 1941): сборник документов / Под ред. А.К. Соколова. Т. 4. М., 2015. С. 238—240, 254—255, 271, 302, 323—326, 409—410, 562—565.

¹⁹ Оборонно-промышленный комплекс СССР в годы Великой Отечественной войны (июнь 1941—1942). Т. 5. М., 2020. С. 145—146, 270—272, 602—609.

о кадрах КГБ при Совете министров (СМ) СССР и результатах проведения операций по негласному копированию шифрбллокнотов посольств иностранных государств опубликованы в сборнике «Политбюро и органы государственной безопасности»²⁰.

Наконец, важную информацию предоставляют источники личного происхождения. О Марфинской лаборатории («Марфинской шарашке»), созданной в Отделе оперативной техники МГБ СССР с целью разработки аппаратуры засекречивания телефонных переговоров гарантированной стойкости, писали в воспоминаниях А.И. Солженицын²¹, Л.З. Копелев²², Д.М. Панин²³, К.Ф. Калачёв²⁴. Бывший председатель КГБ СССР В.А. Крючков дал подробную оценку деятельности шифровальных и дешифровальных подразделений ведомства²⁵. Генерал-майор В.Н. Удилов, длительное время работавший на руководящих должностях в контрразведке, рассказал об уникальных операциях советских спецслужб по проникновению в иностранные посольства и снятию копий с их шифрбллокнотов, что позволяло читать переписку дипломатических представительств и разведок²⁶.

Становление криптографической службы Советской России. События 1917 г. парализовали работу имперской школы криптографии, погребённой под обломками государственного аппарата. Специалисты оказались по разные стороны баррикад: значительная их часть присоединилась к Белому движению, усилив его позиции. Ими широко использовались традиции и техническая база шифровальной службы, многие важные документы Временного правительства, документация командующих фронтами царской армии, шифры и коды. Создавались также новые коды, использовались буквенно-слоговые равнозначные таблицы замены. В распоряжении Белого движения были не только опытные кадры, но и значительная часть средств радиоперехвата, с помощью которых дешифровывались радиограммы между командованием Красной армии об операциях на Восточном и Туркестанском фронтах, переговорах в Брест-Литовске, работе ВЧК. Определённую поддержку оказывали зарубежные правительства и спецслужбы. Особенной активностью в этом направлении отличалась британская разведка. Часть опытных криптографов царской России, эмигрировавших в Лондон, привлекалась к работе по вскрытию советских шифров. В результате англичане провели операцию по перехвату дипломатической переписки делегации РСФСР с немцами о заключении мира в Брест-Литовске, в 1920 г. дешифровали значительную часть советско-английских торговых переговоров. В августе 1920 г. через газету «The Times» англичане фактически признали факт перехвата и чтения советских дипломатических депеш²⁷.

Пришедшие к власти бывшие революционеры-подпольщики прекрасно осознавали необходимость защиты партийных и государственных секретов. Для этого требовалось фактически заново построить систему технической передачи

²⁰ Политбюро и органы государственной безопасности. Сборник документов / Сост. О.Б. Мозохин. М., 2017. С. 728, 738—745.

²¹ Солженицын А.И. В круге первом. М., 1990.

²² Копелев Л.З. Утоли мои печали. М., 1991.

²³ Панин Д.М. Лубянка—Экибастуз. Лагерные записки. М., 1990.

²⁴ Калачёв К.Ф. В круге третьем (Воспоминания и размышления о работе Марфинской лаборатории в 1948—1951 гг.). М., 1999.

²⁵ Крючков В.А. Личное дело: в 2 ч. Ч. 1. М., 1996.

²⁶ Удилов В.Н. Записки контрразведчика (Взгляд изнутри). М., 1994.

²⁷ Куренков Г.А. От конспирации к секретности... С. 119—120.

и защиты информации, приступить к созданию специальной техники, шифров, кодов и организации шифрработы на государственном уровне. В условиях Гражданской войны эта задача оказалась невыполнимой: требовались новые структуры, кадры и подходы. Решение отказаться от дореволюционных шифров не принесло желаемого результата. 20 августа 1920 г. нарком иностранных дел Г.В. Чичерин направил В.И. Ленину записку, в которой обращал внимание на то, что советская система шифрования известна многим эмигрантам (бывшим царским чиновникам и военным), и это приводит к утечке информации. Почти все сообщения Красной армии и советской дипломатии, зашифрованные при помощи таблиц «Республика», «Москва» и «Секунда», успешно читались не только «белыми», но и иностранными государствами (Великобритания, Польша, Швеция). Даже новые, более стойкие шифры («Пулемёт», «Агитатор», «Советский») не повысили сохранность информации²⁸.

В первые годы советской власти шифровальное дело развивалось весьма хаотично: единой структуры, отвечавшей за сохранение важной информации, не существовало. Так, в августе 1920 г. появилось Шифрбюро Секретариата ЦК РКП(б) из семи человек, созданное для секретной переписки с партийными органами и зарубежными коммунистическими партиями, но оно плохо справлялось с поставленными задачами. 28 января 1921 г. при ВЧК был организован Специальный отдел, занимавшийся шифровальной и дешифровальной работой, однако это не решало вопроса защиты информации. Требовалось принятие организационных и административных решений и реорганизация государственного аппарата.

Впервые вопрос о подразделении, которое бы занялось такой работой во всероссийском масштабе, обсуждался на заседании СНК 12 апреля того же года. В итоге решили «поручить начальнику Шифровального отдела ВЧК принять меры к осуществлению надзора, контроля и руководства шифровальным делом в Республике и представить в Малый Совет соответствующий проект постановления, согласовав его с наиболее заинтересованными ведомствами в первую голову». Дальнейшие дискуссии выявили столкновение интересов ВЧК и наркомата юстиции, потребовалась череда согласований межведомственных позиций. 22 апреля, выполняя поручение правительства, начальник шифровального отдела ВЧК Г.И. Бокий направил в Малый Совнарком четыре экземпляра проекта постановления об образовании при ВЧК «Специального отдела». Заседание Малого СНК состоялось 25 апреля, однако решение принято не было, так как Бокий, понадеявшись на авторитет ВЧК и чрезвычайную важность обсуждаемого вопроса, не согласовал текст документа с заинтересованными ведомствами (иностранных и внутренних дел). Лишь 5 мая по итогам слушания вопроса СНК постановил: «1. Организовать при ВЧК “Специальный отдел”, начальником которого мог быть только член Коллегии ВЧК. 2. Специальный отдел при ВЧК объединяет все шифровальные органы РСФСР, контролирует и направляет всю деятельность таковых органов. 3. Все распоряжения и циркуляры Специального отдела при ВЧК по всем вопросам шифровального и расшифровального дела являются обязательными к исполнению всеми ведомствами РСФСР»²⁹.

Так было положено начало созданию советской криптографической службы. Её задачами стали: изучение шифров и выработка рекомендаций по повыше-

²⁸ Ларин Д. Красные и белые шифры // ФСБ: за и против. 2017. № 6. С. 53—55.

²⁹ ГА РФ, ф. 130, оп. 5, д. 87, л. 191—196.

нию их стойкости, разработка системы шифров и составление кодов различных ведомств; разработка специальных кодов для наркоматов внешней торговли, иностранных дел и штаба Красной армии, обследование шифрорганов; разработка инструкций, циркуляров и указаний для шифрорганов и контроль за их работой; организация подготовки и переподготовки специалистов-криптографов, дешифровка переписки иностранных государств и перлюстрация дипломатической почты. Работа Спецотдела изначально проходила в тесном взаимодействии с ЦК РКП(б) и его секретными подразделениями. Практически с первых дней ЦК уделял особое внимание организации шифровальной службы, повышению её статуса в системе спецслужб. В дальнейшем именно это позволяло отделу длительное время избегать постоянных реорганизаций, характерных для советского аппарата.

В своей работе отдел использовал опыт Российской империи и иностранных государств. Его сотрудники во второй половине 1921 — начале 1922 г. проанализировали 95 различных готовых шифрсистем, из которых только 36 признали криптографически стойкими и рекомендовали для использования в военном, внешнеполитическом и внешнеторговом ведомствах. На основе этого анализа и особенностей шифрпереписки в наркоматах и ведомствах создавались новые шифры (буквенные и буквенно-слоговые) и коды (алфавитные и неалфавитные). Их использовали в повседневной работе, в частности, малым кодом активно пользовалась советская делегация на Генуэзской конференции. Отдел постепенно расширял возможности и масштабы шифровального дела, контролировал деятельность шифрорганов РСФСР. В полномочных представительствах (ПП) ГПУ—ОГПУ создавались спецотделения, положения о которых утвердил приказ № 242/96 от 9 декабря 1927 г. Их основными задачами являлись: организация секретного и шифровального делопроизводства во всех учреждениях, расположенных на территории ПП ОГПУ как местного, так и союзного значения; разработка шифров и обеспечение ими всех учреждений на территории ПП, за исключением тех, которые пользовались шифром, установленным Спецотделом; контроль за порядком ведения и хранения мобилизационных и шифровальных материалов; учёт лиц, ведавших секретной перепиской в советских учреждениях³⁰.

Подготовка криптографов началась на шифровальном отделении курсов ВЧК (срок обучения 2—6 месяцев, руководитель В.Д. Цибизов). Среди преподавателей были как «царские» специалисты (И.А. Зыбин, В.И. Кривош-Неманич (Кирпичников)), так и советские. Кадры готовились не только для Спецотдела, но и для шифровальных отделений ЦК ВКП(б) и наркоматов, а также дипломатических и торговых представительств СССР за границей. В январе 1931 г. начали работу объединённые дешифровальные курсы по подготовке криптографов дипломатического и военного направлений с ежегодным выпуском 25 человек, годом позже — Центральные курсы по подготовке дешифровальщиков при дешифровально-разведывательной службе (ДРС) штаба РККА. Подготовка кадров для вскрытия дипломатической шифрпереписки до 1940 г. также проводилась на краткосрочных курсах при 7-м отделе (шифровальная работа) НКВД СССР. Большое значение имели учебные пособия и сборники, которые разрабатывались Спецотделом, а также преподавателями специальных учебных

³⁰ Спецтехника на защите государства (История становления и развития спецслужб и их технического обеспечения). М., 2004. С. 11.

заведений³¹. Однако краткосрочные курсы не могли удовлетворить потребность в специалистах ни в количественном, ни в качественном отношении³².

Несмотря на усилия по предотвращению утечки информации, спецслужбы иностранных государств перехватывали секретную информацию, циркулировавшую по каналам шифрсвязи. Так, к примеру, для англичан большой интерес представляла переписка советского правительства и дипломатов с Ближним Востоком и организациями в Великобритании. Её перехват и чтение в Лондоне продолжались до конца мая 1927 г. Затем правительственный комитет опубликовал избранные места из неё, чтобы оправдать разрыв дипотношений с СССР. После этого порядок изменили: отныне шифрование и расшифровка секретных сообщений велись путём применения односторонних шифроблокнотов. В итоге вплоть до середины 1940-х гг. английские криптоаналитики не могли дешифровать советскую дипломатическую переписку³³. С середины 1920-х гг. стали также применяться коды с гаммированием, использующиеся до настоящего времени в качестве резервных средств шифрования. В 1927 г. на вооружение Спецотдела поступили разработанные П.Н. Куксенко (выдающимся радиоспециалистом, работавшим в НИИ связи РККА) устройства многократного приёма для радиостанций.

Тем временем центральный аппарат ОГПУ начал подвергаться реорганизации. С 1 декабря 1929 г. в его структуре находились Спецотдел (начальник Боккий) и Центральное шифровальное бюро (начальник В.М. Колосов). В 1936—1941 гг. происходили новые структурные трансформации, в ходе которых менялись составы и наименования отделов, занимавшихся шифровальным делом, а также изготовлением оперативной техники. После разделения ведомства в феврале 1941 г. в структуре НКВД осталось Особое техническое бюро (начальник В.А. Кравченко), а также появилось 6-е отделение (ведение шифрованной переписки; начальник А.А. Солодянников). В новообразованный наркомат государственной безопасности «ушли» два отдела: 4-й (опертехника, начальник Е.П. Лапшин) и 5-й (шифровальный, начальник А.И. Копытцев).

При содействии и помощи Спецотдела создавалась армейская дешифровально-разведывательная служба. Долгое время она находилась в его оперативном подчинении. Лишь в 1939 г., после постановления Комитета обороны при СНК от 4 июля и приказа наркомата обороны (НКО) от 16 июля, началась организация ДРС при 5-м управлении Разведывательного управления Генерального штаба РККА. Впрочем, службы НКВД и ДРС, их подразделения на местах поддерживали тесное взаимодействие в работе, добыче информации, подготовке кадров.

В 1929—1930 гг. при отделах и ПП ОГПУ в Ленинградском военном округе независимо друг от друга появились отдельные радиолобатории. В соответствии с циркуляром ВСНХ и ОГПУ от 15 мая 1930 г. в их работе использовались специалисты, арестованные за «контрреволюционную деятельность».

³¹ Там же. С. 14, 35.

³² 50 лет Институту криптографии, связи и информатики (Исторический очерк) / Отв. ред. Б.А. Погорелов. М., 1999. С. 12.

³³ Куренков Г.А. Организация защиты информации в структурах РКП(б)—ВКП(б) 1918—1941 гг. Автореф. дис. ... канд. ист. наук. М., 2010. С. 20; Лайнер Л. «Венона». Самая секретная операция американских спецслужб. М., 2003. С. 262.

Эту дату можно считать днём рождения «шарашек»³⁴. Разработкой секретной телефонии занимались будущие академики В.А. Котельников и А.Л. Минц, профессора К.П. Егоров, В.К. Виторский. Точкой отсчёта стал 1930 г., когда к работе в наркомате почт и телеграфа приступил Котельников. В 1938—1939 гг. в ЦНИИ наркомата связи под его руководством появились две лаборатории — по засекречиванию телеграфной и телефонной информации. К концу 1930-х гг. секретной телефонией занимались уже несколько предприятий: НИИ наркомсвязи, НИИСТ Красной армии, завод им. Коминтерна, завод «Красная Заря» (Ленинград), НИИ связи и телемеханики Военно-морского флота, НИИ № 20 наркомата электропромышленности, а также лаборатории НКВД³⁵. В 1938 г. создана Центральная лаборатория оперативной техники (ЦЛОТ) в составе двух отделений³⁶.

С начала 1930-х гг. в 8-м управлении Генштаба РККА велась работа по созданию шифровальной аппаратуры. Одной из них стала громоздкая и не очень надёжная ШМВ-1 (шифрмашина И.П. Волоска). Она работала по принципу наложения гаммы (случайной последовательности знаков) на комбинацию знаков открытого текста, что в итоге создавало неразборчивую криптограмму, взломать которую по тем временам было практически невозможно. В 1934 г. разработали и запустили в производство шифрмашину В-4. В 1939 г. инженер Н.М. Шарыгин провёл серьёзную модернизацию В-4, создав по сути новый аппарат — М-100 «Спектр». В нём реализован шифр гаммирования, заключавшийся в непосредственном наложении на знаки открытого текста знаков гаммы, наперфорированных на бумажную ленту по двузначному коду. М-100 активно использовалась во время боевых действий в районе Халхин-Гола (1939) и советско-финляндской войны (1939—1940)³⁷. Через некоторое время создали более совершенную машину М-101, а к 1941 г. — К-37 (шифровальный аппарат для среднего звена), работавшую на многоалфавитном шифровании и частично заменившую применявшийся в армии командирский код.

До начала Великой Отечественной войны шифраппаратуру изготавливал 69-й отдел завода № 209 наркомата судостроительной промышленности, в котором числились около 160 рабочих и инженерно-технических работников (из них 8 конструкторов) и около 100 единиц станков. Им проектировалась и изготавливалась аппаратура кодирования телеграфных сообщений для Генштаба и Главного управления связи РККА: С-308 для аппарата Бодо, С-309 для советского телеграфа СТ-35, С-307 (полевая шифрующая приставка к телеграфному аппарату с питанием от аккумулятора), С-306 для присоединения к классическому аппарату Морзе (питание от сети), К-37 (компактный аппарат, работающий на многоалфавитном шифровании), 1001 (шифрмашина правительственной связи), СТ-35 (ленточный стартостопный³⁸ телеграф).

³⁴ В сентябре 1938 г. в структуре НКВД для использования заключённых, имевших специальные технические знания, при выполнении научно-исследовательских и опытно-конструкторских работ был создан Отдел особых конструкторских бюро (4-й спецотдел).

³⁵ *Калачёв К.Ф.* В круге третьем...

³⁶ Спецтехника на защите государства... С. 39.

³⁷ Шифровальная техника Советского Союза. Русские «Энигмы». Ч. 5 (URL: <https://topwar.ru/151854-shifrovalnaja-tehnika-sovetskogo-sojuza-russkie-jenigmy-chast-5.html>).

³⁸ Название принципа работы появилось из-за того, что механизмы передатчика и приёмника пускались в ход одновременно при передаче каждого знака телеграммы, после чего останавливались. При передаче следующего знака они запускались вновь. Пуск в ход это «старт», остановка — «стоп».

Активные меры по развитию системы защиты информации, развитию науки и техники, а также деятельность политической и научно-технической разведки по добычанию научно-технической информации заложили фундамент системы шифрования и дешифрования. Однако всё же ощущалось отставание разработок от уровня Англии, Германии, США, связанное прежде всего с тем, что в советских структурах не имелось высококвалифицированных математиков³⁹.

Советская криптография в период Великой Отечественной войны. Война явилась серьёзным испытанием для подразделений шифрования и дешифрования, обеспечения правительственной связи и защиты информации. Особое внимание уделялось сокрытию мероприятий Генерального штаба Красной армии и Ставки Верховного Главнокомандования (ВГК) по планированию, подготовке и ведению стратегических операций. Эффективность этой деятельности, её влияние на ход и исход событий на фронтах во многом зависели от оперативности разведки, полноты, достоверности и своевременности получения информации.

Соответствующие подразделения НКВД и ГРУ обеспечивали Ставку, Генштаб, командование фронтов безопасной связью и важной информацией о намерениях противника. В структуре НКВД работали спецотделы: 2-й (оперативной техники, начальник Е.П. Лапшин), 4-й (особое техническое бюро, ВЧ-связь, начальник В.А. Кравченко), 5-й (шифровальный, начальник И.Г. Шевелев). 3 ноября 1942 г. на базе 5-го спецотдела было создано 5-е (шифровальное) управление НКВД. В состав 4-го спецотдела вошли три радиолaborатории (со штатом 356 человек и всем лабораторным оборудованием), созданные ещё в 1929—1931 гг. для обеспечения оперативной и специальной техникой подразделений органов безопасности⁴⁰: в пос. Кучино, занимавшаяся разработкой и изготовлением радиопеленгаторных, радиоприёмных и звукозаписывающих устройств (210 человек); в Москве (на ул. Спиридоновка), занимавшаяся разработкой и изготовлением агентурных приёмопередающих станций и аппаратурой для спецслужб литер «Н» и «М» (110 человек); в Ленинграде (эвакуированная в Свердловск), занимавшаяся той же тематикой, что и предыдущие (36 человек). Их вскоре объединили в единую Центральную радиолaborаторию (ЦРЛ) (7-е отделение 4-го спецотдела НКВД, начальник Ф.Ф. Железов). С 1941 г. в ней работал талантливый инженер Л.С. Термен.

Для подготовки криптографов в августе 1940 г. при 7-м отделе ГУГБ НКВД была создана одногодичная криптографическая школа особого назначения, после начала войны переведённая в Уфу. В 1942 г. на базе школы и 3-го учебного отделения Высшей школы Генштаба организована Специальная школа 5-го управления НКВД с 10-месячным сроком обучения. Кроме того, появились четыре школы по подготовке радиоспециалистов: в Ленинграде (на 1 200 человек), Москве, Горьком и Воронеже (на 1 тыс. человек каждая). В армии вводился запрет на использование связистов не по специальности. Командирам частей и соединений предписывалось в 5-дневный срок возратить квалифицированных связистов (инженеры, техники, радисты-слухачи и операторы, телеграфисты, работавшие на аппаратах Бодо, СТ-35 и др.) в профильные части.

В октябре 1941 г. лабораторию Котельникова эвакуировали в Уфу, значительную часть документации и макетов уничтожили. В 1941—1946 гг. лаборатория несколько раз реорганизовывалась, передавалась в различные ведомства,

³⁹ 50 лет Институту криптографии, связи и информатики... С. 14.

⁴⁰ Спецтехника на защите государства... С. 60.

что оказывало негативное влияние на её работу. Несмотря на это, по итогам 1942 г. за разработку новой аппаратуры связи руководителя и инженеров наградили Сталинской премией.

Для объединения усилий шифровальных и дешифровальных подразделений армии и органов госбезопасности в ноябре 1942 г. на основе 5-го спецотдела НКВД и дешифровальной службы⁴¹ военной разведки Красной армии организовали 5-е управление (шифровально-дешифровальное) НКВД. Из НКО туда перевели опытных криптографов М.С. Одноробова, Н.В. Пишенина, В.С. Полина, Г.И. Пондопуло, М.И. Соколова, А.Ф. Яценко и др.

Накануне и в годы войны важнейшим средством связи являлись телеграфные аппараты Бодо⁴², допускались переговоры и телеграммы открытым текстом, но с применением при этом кодированных карт и таблиц позывных. Первые дни и недели ведения боевых действий показали, что управление войсками ведётся неудовлетворительно, работа связи организована плохо, телефонная связь ненадёжна. В огромном потоке документов, часто не имевших оперативного значения, тонули важнейшие приказы, директивы и распоряжения, с большим опозданием (на 8—10 часов) попадавшие в подчинённые штабы, что зачастую приводило к срыву намеченных операций. 23 июля 1941 г. вышел приказ НКО № 0243 «Об улучшении работы связи в Красной армии»⁴³, в соответствии с которым командирам и комиссарам частей и соединений, военным советам армий и фронтов предписывалось немедленно обеспечить полное использование радиосредств для управления войсками с обязательным соблюдением секретности передачи данных. Однако первое время части и соединения РККА, ВМФ, НКВД и НКГБ не имели достаточного количества радиостанций, телефонных и телеграфных аппаратов⁴⁴. Постановление ГКО от 9 августа 1941 г. «Об обеспечении Красной армии средствами связи» дало соответствующие поручения ряду наркоматов⁴⁵. Однако и эти меры не смогли решить проблему⁴⁶. Поэтому постановлениями ГКО в 1942 г. регулярно регламентировались следующие вопросы: организация правительственной высокочастотной связи между Москвой и штабами фронтов, производство аппаратуры ВЧ-связи, войсковых радиостанций, телеграфных аппаратов Бодо и автоматики Бодо, производство и поставки средств и имущества связи для различных ведомств, 5-го (шифро-

⁴¹ С 23 ноября 1942 г., согласно приказу НКО СССР № 00222 о реорганизации ГРУ Генштаба Красной армии, дешифровальная служба военной разведки и восемь отдельных радиодивизионов особого назначения передавались в состав НКВД.

⁴² Бодо — телеграфный аппарат, изобретённый в 1872 г. французом Ж.Э. Бодо. Аппарат позволял по одной линии вести передачу нескольких телеграмм одновременно, причём получение данных происходило уже не в виде точек и тире (до того все подобные системы базировались на азбуке Морзе), а в виде букв латинского и русского (после тщательной доработки отечественными специалистами) языка. Аппарат Бодо и другие созданные по его принципу устройства получили название стартопных. В 1940-х гг. в СССР использовались аппарат Бодо и буквопечатающее устройство типа 2БД-41 двукратного телеграфирования.

⁴³ ЦА МО РФ, ф. 4, оп. 11, д. 65, л. 165—169.

⁴⁴ Так, обеспеченность радиосетей Генштаба аппаратами Бодо составляла 69%, СТ-35 — 35%, телефонными аппаратами — 47% (Оборонно-промышленный комплекс СССР в годы Великой Отечественной войны. Т. 5. Ч. 1. С. 61).

⁴⁵ Там же. С. 145—146.

⁴⁶ На 1 декабря 1941 г., когда шла битва за Москву, войска связи Западного фронта были обеспечены телефонным кабелем на 36%, аппаратами СТ-35 — на 35—58% и Бодо — на 85% (Там же. С. 61).

вального) управления НКВД⁴⁷. В 1943 г. ГКО обращал внимание на необходимость обеспечения высококачественными проводами для ВЧ-связи Ставки со штабами фронтов и армий⁴⁸. Тогда же неоднократно принимались постановления об оснащении радиоаппаратурой и имуществом связи 5-го (шифровального) управления НКГБ⁴⁹.

В 1942 г. сотрудники подразделений дешифровальной службы ГРУ вскрыли основные немецкие и японские системы общевоинских, политических и дипломатических шифров, а также 75 шифров немецкой разведки и воинских соединений противника. В результате удалось прочесть более 50 тыс. телеграмм противника, что позволило установить места дислокации свыше 100 штабов соединений и раскрыть нумерацию 200 отдельных батальонов и других частей германской армии. В период Сталинградской битвы удалось получить информацию о составе группировки германских войск (6-й полевой и 4-й танковой армий), действовавших перед Юго-Западным, Донским и Сталинградским фронтами. В числе трофеев битвы оказались 696 радиостанций и 933 телефонных аппарата противника, коды 6-й полевой армии, а также три шифратора «Enigma». Советские контрразведчики выявили среди военнопленных несколько разведчиков и шифровальщиков, которых привлекли к сотрудничеству. Вступление РККА в 1944 г. на территорию иностранных государств потребовало дополнительных усилий по обеспечению маскировки и затруднению прослушивания оперативных телефонных разговоров штабов фронтов, армий и корпусов. На территории, занятой советскими войсками, устанавливался контроль за телеграфно-телефонной линией, радио и почтовой связью⁵⁰.

К началу войны в ЦНИИС наркомата связи разработали и изготовили несколько образцов аппаратуры засекречивания телефонных переговоров, основанной на частотно-временных преобразованиях речевого сигнала. В лаборатории Котельникова к концу 1941 г. изготовили и испытали лабораторные макеты отдельных основных узлов аппаратуры «Соболь-П»: частотных перестановок с инверсией спектра, временных перестановок, шифратора на базе транзистора и пятирядной перфорированной телеграфной ленты, а также макет генератора, создающего гамму управления перестановками частотных полос и временных отрезков⁵¹. Совершенствование шифровальной техники привело к созданию электрической машины предварительного шифрования М-150 (1945), на основе которой были созданы машины М-152, М-153, М-161 для министерств иностранных дел и внешней торговли СССР. В общей сложности на линиях связи между Ставкой и командующими фронтами и армиями использовались более 2 тыс. аппаратов засекречивания.

Наряду с разработкой шифровальной аппаратуры велось совершенствование и средств связи. Так, в течение 1941—1942 гг. под руководством Термена разработана серия радиопередатчиков «Белка», «Набла», «Марс», «Тюлень», которые активно использовались в оперативных подразделениях и войсках НКВД, а также в партизанских отрядах. Различные варианты радиостанций —

⁴⁷ РГАСПИ, ф. 644, оп. 1, д. 24, л. 45—46, 93—103; д. 33, л. 27—42; д. 45, л. 169—196; д. 52, л. 52—55; д. 61, л. 108—134; д. 64, л. 25—33; д. 65, л. 80—82; д. 73, л. 54—55; д. 80, л. 8—39.

⁴⁸ Там же, д. 85, л. 46—63; д. 127, л. 149—152.

⁴⁹ Там же, д. 121, л. 143—144; д. 212, л. 5—8.

⁵⁰ Там же, д. 214, л. 123—128; д. 301, л. 114—115; д. 324, л. 121; д. 397, л. 140—145; д. 387, л. 89—90.

⁵¹ Калачёв К.Ф. В кругу третьем...

чемоданный, десантный, унифицированный — оказались настолько надёжны и удобны, что их заказывали Центральный штаб партизанского движения, ГРУ⁵². Новое направление оперативной связи появилось в ЦРЛ — система «Интеграл» для городской радиотелефонной связи из легковой автомашины и радиостанция «Стрела» с дальностью связи до 3 тыс. км для связи правительственных поездов с Москвой. Эта аппаратура обеспечила высоконадёжную радиосвязь во время проведения Тегеранской конференции и в оперативных поездках на Северный Кавказ. Виднейшие советские военачальники высоко оценивали работу правительственной связи.

Таким образом, нападение Германии на Советский Союз стимулировало развитие шифровальной и специальной техники, средств правительственной связи и новых технологий. Для этого были объединены усилия шифровальных и дешифровальных подразделений РККА и отечественных органов госбезопасности, а также представителей шифровальной службы НКВД—НКГБ и коллективов разработчиков аппаратуры шифрования. По окончании войны в целях использования передового опыта радиотехнической и электропромышленности Германии и Австрии и для создания современной производственной базы на советских заводах, занимавшихся изготовлением шифровальной аппаратуры и радиостанций, по программе репарации с предприятий, научно-исследовательских институтов и складов вывозились оборудование связи, образцы новейшей радиотехнической аппаратуры, материалы, технические архивы и библиотеки⁵³. Так, в соответствии с постановлениями ГКО 1945 г. из Германии вывезли: на завод № 672 — оборудование по производству телеграфной аппаратуры с немецкого телеграфного завода фирмы «Лоренц» (Кюстрин); оборудование по производству телеграфной аппаратуры с завода «Верне Верке Т» фирмы «Сименс Гальске» в Берлине (Хозельхорст) (498 ед.); на завод № 697 — оборудование по производству аппаратуры дальней связи с телефонного и приборостроительного заводов в Берлине (Сименсштатт); на завод № 203 — оборудование по производству танковых и пехотных радиостанций с завода концерна «АЕГ-Саксен Верке» в районе г. Дрездена (Нидрезедлиц); на завод № 210 — оборудование по производству радиоаппаратуры с завода фирмы «АЭГ» (Берлин)⁵⁴.

Шифровальное дело в 1950—2000-х гг. Во второй половине 1940-х гг. Сталин предпринял ряд мер, направленных на ослабление влияния ведомства госбезопасности. Первым шагом стало выделение в мае 1947 г. из структуры МГБ политической разведки, объединение её с военной разведкой⁵⁵ и образование на их основе самостоятельного ведомства — Комитета информации при СМ СССР (1947—1949, в 1949—1951 — Комитет информации при МИД СССР)⁵⁶. Осенью 1949 г. из ведения МГБ изъята шифровально-дешифровальная служба. 19 октября Политбюро ЦК ВКП(б) приняло решение о коренной перестройке Специальной (шифровальной) службы МГБ СССР и создании Главного управления специальной службы (ГУСС) при ЦК ВКП(б), в состав

⁵² РГАСПИ, ф. 644, оп. 1, д. 165, л. 29—39; ГА РФ, ф. 9401, оп. 3, д. 93, л. 66—99; Спецтехника на защите государства... С. 60—62.

⁵³ РГАСПИ, ф. 644, оп. 1, д. 378, л. 10, 112; д. 401, л. 144—146; д. 406, л. 44—45; д. 414, л. 74—76; д. 421, л. 27—30; и др.

⁵⁴ См.: Тихонов С.Г. Оборонные предприятия СССР и России. Т. 1—2. М., 2010.

⁵⁵ В 1949 г. военная разведка вернулась в систему Минобороны.

⁵⁶ В 1951 г. разведывательная работа из МИД была возвращена в МГБ.

которого вошли бывшие 6-е управление МГБ и ДРС Генштаба. ГУСС заложило основы исследований и теории проектирования шифровальных систем широкого профиля, способствовало развитию экспериментальной и производственной базы для выпуска аппаратуры засекречивания: появились новые идеи и методики, давшие значительный эффект при дешифровании дисковых шифраторов с использованием как специализированных ЭВМ, так и ЭВМ общего назначения.

После смерти Сталина задачи развития шифровального и дешифровального дела замкнул на себя КГБ. В его структуре появились: в 1954 г. — 8-е главное управление (шифрование и дешифрование), в 1973 г. — 16-е управление (радиоэлектронная разведка и радиоперехват). В 1959 г. на базе 2-го (применение оперативной техники), 3-го (изготовление средств тайнописи, экспертиза документов), 4-го (радиоконтрразведка), 5-го (изготовление оперативной техники) и 6-го (перлюстрация почтовой и телеграфной корреспонденции) спецотделов создали Оперативно-техническое управление (ОТУ), которое просуществовало вплоть до расформирования КГБ в конце 1991 г. Оно являлось головным подразделением по проектированию, разработке, производству и эксплуатации специальных технических средств. В нём сосредоточивались достижения научной мысли, высочайших технологий, уникальные технические решения. ОТУ внимательно присматривалось к новинкам в области создания специальной техники за рубежом и стремилось использовать всё наиболее ценное. Среди его продукции было сравнительно немного технических средств, разрабатывавшихся и производившихся большими партиями, сериями. Часто они представляли собой единичные изделия, предназначенные для решения строго определённых оперативных задач. Продукция этого управления носила сугубо секретный характер. Утечка информации приводила к тому, что противник разрабатывал меры противодействия и тем самым лишал эффективности технические возможности КГБ. В то же время ОТУ делилось своими новинками с гражданскими отраслями промышленности, не требуя ничего взамен: коммерческой практики в те времена не существовало. Без его изделий ни разведка, ни контрразведка, ни другие подразделения Комитета, ни пограничные войска не могли решать стоявшие перед ними задачи⁵⁷.

26 апреля 1967 г. коллегия КГБ приняла решение «О внедрении электронных вычислительных машин для механизации и автоматизации аналитической работы в системе КГБ». Началось создание автоматизированной системы информационного обеспечения (АСИО) органов и войск КГБ, а также формирование в оперативных подразделениях группы разработки и группы управления разработками задач. Для решения указанных проблем в 1969 г. в ОТУ создали специальный Научно-исследовательский институт (НИИАИ). Началось построение, проектирование и исследование автоматизированных систем КГБ, а также изучение и применение математических методов в информационно-аналитической работе⁵⁸.

20 ноября 1967 г. 2-й отдел ОТУ выделили в самостоятельный 12-й отдел КГБ (прослушивание телефонов и помещений). Речь идёт о слуховом техническом контроле, используемом органами госбезопасности при проведении оперативно-розыскных мероприятий. О работе этого отдела ходило много домыслов, его работу преподносили как «тотальный контроль» органов госбез-

⁵⁷ Крючков В.А. Личное дело. Ч. 1. С. 343.

⁵⁸ См.: 50 лет Институту криптографии, связи и информатики... С. 66—67.

опасности над советскими гражданами и иностранцами. Однако технические возможности отдела в конце 1980-х гг. ограничивались контролем одновременно не более 2 тыс. абонентов.

Необходимо обратить внимание на организованное взаимодействие сотрудников 2-го и 8-го главных и 16-го управлений КГБ. Так, посты радиоэлектронной разведки⁵⁹ 16-го управления за рубежом фиксировали и обрабатывали не только «открытые» сообщения, но и шифровки иностранных внешнеполитических ведомств и разведок. Криптографы 8-го ГУ взломали многие используемые иностранными дипломатическими ведомствами шифросистемы. В годовом отчете КГБ, адресованном Н.С. Хрущёву и датированном началом 1961 г., говорится, что в 1960 г. управление расшифровало 209 тыс. дипломатических телеграмм, посланных представителями 51 государства. В структуры ЦК (главным образом, несомненно, в международный отдел) переданы не менее 133 200 перехваченных телеграмм. К 1967 г. КГБ смог раскрыть 152 шифра, использовавшихся 72 странами⁶⁰. Подразделения, занимавшиеся дешифровкой сообщений иностранных государств, активно использовали результаты деятельности советских контрразведывательных подразделений, которые проникали в шифровальные комнаты иностранных посольств, вскрывали там сейфы и добывали секретные документы, в том числе снимали копии с шифрблокнотов посольских резидентур⁶¹.

Перед советскими контрразведчиками ставились задачи по добыванию шифров разведок США, стран, входивших в НАТО, Франции, Японии, Китая и Израиля. Например, генерал В.Н. Удилов, работавший заместителем начальника 2-го ГУ КГБ, подробно описывает, как в 1960-х гг. контрразведчики при содействии болгарских коллег проводили уникальные операции по проникновению в посольство Италии в Софии и снятию копий с шифрблокнотов «Калабрия» и «Сардиния», одна из систем которых обслуживала отдел информации НАТО⁶². Итоги работы контрразведки изложены в докладе, направленном в ЦК КПСС в мае 1968 г. КГБ смог добыть шифры семи капиталистических стран, а также внедрил радиотехнику прослушивания на 36 объектах, представляющих интерес для разведки. Его работники добыли шифры и коды 11 посольств капиталистических стран, что позволило дешифровать их переписку. Специальная служба КГБ осуществляла перехват шифрованной переписки более 2 тыс. действующих радиостанций из 115 стран мира. Радиоконтрразведывательные подразделения разрабатывали 24 радицентра разведывательных органов капиталистических стран, которые обеспечивали связь со 108 агентурными точками.

Всего в 1967 г. вскрыто 11 шифрсистем, дешифровано более 188 тыс. телеграмм. Криптографами КГБ создано для министерств и ведомств Советского Союза 217 кодов и других средств ручного шифрования, изготовлено более 1,2 млн ключевых и перешифровальных блокнотов, около 30 тыс. экземпляров

⁵⁹ Подробнее о постах радиоразведки за рубежом см.: Структура центрального аппарата КГБ СССР (URL: <https://bezpekapiv.com/struktura-tsentralnogo-apparata-kgb-sssr/>).

⁶⁰ Там же.

⁶¹ Во время одной из таких тайных операций, проникнув в шифровальную комнату и вскрыв сейфы, сотрудники КГБ увидели, что блокноты имеют спецзащиту от постороннего вскрытия — особую вышивку по краям. Взяв один, они вернулись в резидентуру, где в течение дня учились делать такую же вышивку. На следующую ночь пришлось снова пробираться в посольство, вскрывать блокноты, копировать содержимое и сшивать их заново (*Удилов В.Н.* Записки контрразведчика... С. 93, 112—114).

⁶² Там же. С. 96—99.

кодов и кодовых таблиц и более 305 тыс. экземпляров других спецдокументов⁶³. По утверждению агента британской разведки, бывшего сотрудника 16-го управления КГБ СССР В.Б. Макарова, с 1980 по 1986 г. в число европейских государств, дипломатическая переписка которых расшифровывалась с той или иной частотой, входили Греция, Дания, Италия, Финляндия, Франция, ФРГ, Швеция и Швейцария. Ежедневно подборку наиболее интересных сообщений читали Л.И. Брежнев и несколько членов Политбюро, а также начальники 1-го и 2-го управлений КГБ. По оценкам отдельных западных экспертов, Москва частично или полностью могла читать дипломатическую переписку примерно 70 стран мира⁶⁴.

8-е ГУ КГБ осуществляло шифрованную переписку центра с местными органами, а также разведки с зарубежными резидентурами. Оно располагало технической и научной базой, отработанной системой шифрсвязи, которая полностью гарантировала секретность и бесперебойную круглосуточную работу на любом удалении от центра. Получить доступ к шифрованной переписке можно только агентурным путём. Особенно тяжёл труд радистов и шифровальщиков за рубежом. Один, два, максимум три человека обеспечивали связь с центром в любое время суток на любой удалённости. Условия работы были нелёгкими, а жизнь — полной неудобств и лишений из-за необходимости соблюдения строгого режима, поскольку к шифровальщикам иностранные разведки проявляли повышенный интерес⁶⁵.

21 июня 1973 г. из состава 8-го ГУ выделилось самостоятельное 16-е управление (электронная разведка, радиоперехват и дешифровка), обладавшее наибольшим интеллектуальным потенциалом для решения технических и научных задач. Оно занималось съёмом открытой и закрытой информации, решало сложнейшие задачи по проникновению в интересующие Советский Союз объекты других стран. На счету специалистов управления немало изобретений высочайшего уровня. В нём работали крупные специалисты, составлявшие гордость советской науки и техники. Подразделение имело широкие связи с промышленностью, научными учреждениями, использовало их потенциал и помогало последним решать научно-технические задачи. Это было одно из подразделений Комитета, искавших оптимальные пути к разгадке научно-технических головоломок для обеспечения безопасности СССР в условиях холодной войны⁶⁶. В подчинении у начальника управления находились посты радиоэлектронной разведки КГБ, размещённые за рубежом. Большинство из них находились на территории дипломатических миссий и подчинялись резидентам внешней разведки. Основная задача таких постов заключалась в перехвате с помощью специальных технических средств сообщений, передававшихся по закрытым каналам местной связи. Все добытые таким образом данные сотрудники постов радиоэлектронной разведки передавали в управление, которое занималось их дальнейшей обработкой. Посты радиоэлектронной разведки работали в связке с 16-м отделом 1-го ГУ КГБ, который специализировался на вербовке иностранных шифровальщиков и проникновении в шифровальные органы⁶⁷.

⁶³ Политбюро и органы государственной безопасности. С. 738—749.

⁶⁴ См.: Структура центрального аппарата КГБ СССР.

⁶⁵ Крючков В.А. Личное дело. Ч. 1. С. 337.

⁶⁶ Там же. С. 337—338.

⁶⁷ Структура центрального аппарата КГБ СССР.

Конечно, для столь напряжённой работы требовались квалифицированные кадры. 10 сентября 1946 г. приказом МВД СССР в составе 4-го спецотдела организовывалась лаборатория специальной техники. Для её укомплектования подбирали 15 высококвалифицированных специалистов из числа арестованных (спецконтингент). Они проектировали оборудование, размещение отраслевых лабораторий в главном корпусе, разрабатывали вопросы, связанные с тематикой основных работ по оснащению органов и войск МВД спецаппаратурой. Рабочей площадкой для лаборатории стали переданные ей здания и территория Марфинской детской колонии (Ростокинский район Москвы)⁶⁸. В историографии лаборатория получила наименование «Марфинская шарашка». Для ремонтно-строительных работ отобрали 150 человек из числа военнопленных и интернированных немецких специалистов. Они также использовались для разбора архивов берлинских лабораторий «Philips»⁶⁹. Для подготовки к установке в цехах лаборатории и в помещениях отраслевых лабораторий производственного оборудования сформировали техническую группу из 10 вольнонаёмных техников и механиков. В главном корпусе на время выполнения ремонтных работ организовали лагерь заключённых строителей численностью 450—500 человек⁷⁰. На строительные работы МВД израсходовало 2 млн руб., в 1947 г. в лабораторию из Германии завезли часть лабораторного и производственного оборудования.

Однако в результате межведомственной борьбы 21 января 1948 г. СМ СССР принял постановление, в соответствии с которым Марфинская лаборатория со всем оборудованием, измерительной техникой, хозяйственным инвентарём, наличным составом сотрудников и заключённых передавалась в ведение МГБ (Отдел оперативной техники)⁷¹. Уже в конце 1948 г. специалисты Марфинской лаборатории создали систему шифрования импульсов речи. Разработку шифраторов для таких систем, которые могли производиться только криптографическими методами, могли вести только специалисты-криптографы, однако таковых в лаборатории не оказалось. В связи с этим в марте 1949 г. на временную работу туда перевели И.Я. Верченко, Н.А. Тюрина и Л. Дайчика, работавших над конструированием и оценкой стойкости шифраторов⁷².

Одновременно с созданием ГУСС в октябре 1949 г. при нём создали Школу криптографов. Это был первый и единственный в СССР вуз такого профиля⁷³. В ней велись теоретическое обучение и практические занятия с использованием телеграфных аппаратов Бодо и СТ-35, трофейной машины «Enigma» и шифровальной приставки «Wegner», а также отечественных шифрмашин. Кроме того, для обеспечения специалистами по разработке и производству специальной аппаратуры на всесоюзном уровне готовились инженерные кадры в высших и средних специальных учебных заведениях. На старших курсах втузов формировались группы подготовки специалистов по шифрующей, засекречивающей

⁶⁸ ГА РФ, ф. Р-9401с, оп. 1, д. 761, л. 204.

⁶⁹ Об использовании немецких специалистов в Марфинской лаборатории см.: *Копелев Л.З.* Утоли мои печали. Гл. 1: Марфинская шарашка.

⁷⁰ ГА РФ, ф. Р-9401сч, оп. 1сч, д. 2706, л. 316—317.

⁷¹ Там же, ф. Р-5446, оп. Зас, д. 68, л. 70—71.

⁷² *Калачёв К.Ф.* В кругу третьем...

⁷³ В 1953 г. школу преобразовали в Высшую школу криптографов 8-го управления МВД СССР, в 1954 г. — в Высшую школу криптографов 8-го Главного управления КГБ при СМ СССР, в 1960 г. — в факультет специальных технических служб Высшей школы КГБ, в мае 1962 г. — в Технический факультет Высшей школы КГБ. С 1992 г. это Институт криптографии, связи и информатики.

и маскирующей аппаратуре для министерств промышленности средств связи и госбезопасности⁷⁴. Для этого были разработаны фундаментальные учебники криптографии⁷⁵.

С учётом возрастающего использования достижений науки и техники в деятельности разведок ведущих иностранных государств руководство КГБ принимало меры по укреплению кадрами своих оперативно-технических служб. В 1961—1962 гг. в них приняли на работу почти 2 тыс. специалистов из различных областей знания. Большая группа сотрудников без отрыва от работы проходила обучение в высших и средних технических учебных заведениях, заочных аспирантурах и на различных курсах повышения квалификации. В январе 1963 г. в оперативно-технических службах КГБ работало 36 кандидатов наук, свыше 1 500 инженеров, математиков и других высококвалифицированных специалистов⁷⁶.

В 1950—1960-х гг. развитие подразделений шифрования и дешифрования, создание и использование оперативной техники и правительственной связи вышло на новый уровень. Усовершенствовались технические средства, выпускалось новое оборудование, разрабатывались новые методики. В Марфинской лаборатории разработали телефонную шифровальную аппаратуру гарантированной стойкости (АГС) М-803-5 и временной стойкости мозаичного типа на временных и частотных перестановках отрезков речевой информации (АВС) М-503-2. Она обеспечила защиту переданной информации на некоторый интервал времени, в течение которого противник мог осуществить восстановление шифрованной информации за счёт подбора перетасованных в соответствии с работой шифратора отрезков телефонной информации, что обеспечило защиту большого количества внутрисоюзных линий связи. В 1950-х гг. указанные типы аппаратуры доработали и приспособили для различных условий применения: АГС — «Ландыш», «Восток», С-32, М-32, П-32, «Лагуна», «АВС-Алмаз», «Лиана», «Сирень», «Прибой».

Первые типы аппаратов предварительного шифрования (АПШ) строились в виде дисковых шифрмашин, реализующих шифр колонной замены знаков алфавита: М-125 («Фиалка»); М-130 («Коралл»); М-131 («Гвоздика»). В 1950-х гг. разработаны типы аппаратуры для различных условий применения. В числе засекречивающей аппаратуры с реализацией шифра колонной замены: М-13, ТС-25, ТС-26, Т-201, Т-202. Синхронная засекречивающая телеграфная аппаратура с оригинальной конструкцией дисков для быстрой смены ключей: Т-204 и Т-205. Фототелеграф: «Рулон» и «Старт». В 1961 г. завершена разработка электронной телеграфной аппаратуры шифрования Т-206, ставшей родоначальником класса такого рода устройств, действующего до настоящего времени. В дальнейшем в связи с изменением элементной базы разработана аппаратура М-208. Различные виды аппаратуры модифицировались для различных условий применения: радиослуховая (Т-620, Т-225, Т-600 и Т-228); электронная автоматизированная аппаратура шифрования и передачи телеграфной информации и команд боевого управления с полуавтономным шифратором для связи

⁷⁴ В 1949/50 учебном году в таких группах подготовлено 10 специалистов, а начиная с 1951 г. — 30 специалистов ежегодно.

⁷⁵ Учебник криптографии. Ч. 1. *Соколов М.И.* Курс раскрытия шифров замены, гаммирования и перестановки. М., 1954; Ч. 2. Курс раскрытия кодированных текстов и их усложнений / Под ред. Б.А. Аронского. М., 1954.

⁷⁶ Политбюро и органы государственной безопасности. С. 728.

с береговыми командными пунктами, надводными и подводными кораблями с учётом мер радиоэлектронной борьбы (Т-605). Для защиты командно-программной, телеметрической и специальной информации в 1960—1970-х гг. использовалась шифровальная аппаратура космических радиолиний: «Ветер», «Грим», «Дуб», «Муравей-М».

В 1970-е гг. началось активное применение интегральных микросхем (ИМС), что подтолкнуло разработку нового поколения АПШ с криптографическими алгоритмами «Уран» и «Фиалка», отличавшейся меньшей массой и энергопотреблением шифратора при одновременном увеличении функциональных возможностей и надёжности. Шло массовое перевооружение министерств и ведомств, использующих АПШ, аппаратурой нового поколения: М-171, М-201, М-21, М-205 (аппаратура типа «Уран», М-424(М), М-425 («Фиалка-5»), а также М-125 («Фиалка-3»)). Телеграфная аппаратура шифрования строилась на интегральных микросхемах средней степени интеграции, отличавшихся меньшими габаритами и стоимостью. В 1980-х гг. на смену ИМС малой и средней степени интеграции стали поступать большие интегральные схемы частотного применения, что позволило усилить тематические качества АПШ, расширило его функциональные возможности и повысило потребительские качества. В эксплуатацию введена новая перспективная криптографическая схема — аппаратура М-204М («Стратегия-2м»).

В конце августа 1991 г. началась коренная реорганизация советских спецслужб, существенным образом затронувшая и структуры, занимавшиеся вопросами организации правительственной связи, шифрованием, дешифрованием, радиоразведкой. 29 августа на базе Управления правительственной связи, 8-го ГУ и 16-го управления КГБ был создан Комитет правительственной связи при Президенте СССР (председатель А.В. Старовойтов). После образования на основе бывших подразделений шифрования, дешифрования и правительственной связи КГБ Федерального агентства правительственной связи и информации (ФАПСИ) при Президенте РФ вопросами шифровальной и специальной связи в контрразведке занималось Управление шифровальной и специальной связи ФСК—ФСБ России (1993—2003). Указом президента № 308 от 11 марта 2003 г. «О мерах по совершенствованию государственного управления в области безопасности Российской Федерации» ФАПСИ было упразднено, все его функции, личный состав, техника и имущество распределялись между ФСБ, Службой внешней разведки и Службой специальной связи и информации при Федеральной службе охраны. В структуре ФСБ появились Управление специальной связи Научно-технической службы и Центр безопасности связи, которые в 2007 г. объединились в Центр защиты информации и специальной связи (8-й Центр) ФСБ.

Тем временем в 1990-х гг. состоялся переход с микросхем на жёсткой логике на микропроцессорную элементную базу. Это позволило существенно уменьшить габариты и вес аппаратуры, размещать её непосредственно у абонентов. На её основе для работы в стационарной сети и сети подвижной радиосвязи создан комплекс аппаратуры линейного и абонентского шифрования «Разбег», обеспечивавший высоконадёжное шифрование и высококачественное преобразование речи. В качестве речепреобразующего устройства использовался вокодер с линейным предсказанием. Тем временем бурное развитие информационных технологий в автоматизированных системах управления и связи вызвало необходимость сопряжения АПШ со средствами автомати-

зации (ПЭВМ, локальные сети), а также с каналобразующей аппаратурой. В конце 1990-х — начале 2000-х гг. появилась аппаратура М-207 («Артист»), М-280 («Юрист»), М-427 и М-428 («Дервиш»), М-227 («Засека-АКШ»), М-229 («Шпага»), которая применяется на линиях связи в настоящее время, а также миниатюрные АПШ, предназначенные для эксплуатации оперативными сотрудниками силовых ведомств (ФСБ, ГРУ) вне помещений шифровальных органов. Изготовлением спецтехники в 1993—2004 гг. занималось Управление научно-технического обеспечения ФСК—ФСБ, с 2004 г. — Центр специальной техники ФСБ, имеющий большое будущее при одном условии — вбирать отечественный и зарубежный опыт, находиться в поиске научных и технических решений всякий раз на более высоком уровне.

Подводя итоги, отметим, что история становления и развития отечественных специализированных криптографических структур, обеспечения их кадрами и техникой демонстрирует тесную взаимосвязь с тенденциями развития органов госбезопасности и направлениями государственной научно-технической политики. Созданный для обеспечения режима секретности в реализации линии партии Специальный отдел при ВЧК сохранял привязку к аппарату «боевого отряда партии», успешно отбивая атаки в межведомственных боях. Однако попытки выстроить слаженно работающую структуру часто наталкивались на кадровые проблемы и технические сложности, не позволявшие показывать высокие результаты. 1930-е гг. и период Великой Отечественной стали для развития криптографической службы переломными: привлечение талантливых специалистов из числа репрессированной технической интеллигенции, определённые успехи советской разведки и контрразведки в деле перехвата шифров и радиogramм, ознакомление с зарубежными технологиями после победы в войне сыграли значительную роль в преодолении ресурсных проблем. Всё это создало предпосылки для дальнейшего интенсивного развития отрасли в 1950—1970-х гг.

При этом пример Марфинской лаборатории МВД показывает, что органы государственной безопасности не являлись монополистами в вопросах организации научно-технической деятельности в области криптографии. Напротив, послевоенный период явно демонстрирует их подчинённую роль по отношению к ЦК партии. Успешное окончание войны и послевоенные репрессии не привели к значительному расширению влияния МГБ. Межведомственная конкуренция, ярко проявившаяся в истории с «шарашкой», оставалась одной из ключевых характеристик работы советского государственного аппарата.