УДК 003.26
DOI 10.33764/2618-981X-2023-5-25-32

В. А. Гашенко[1*]

Становление и развитие криптографической службы в России

[1] Сибирский государственный университет путей сообщения, г. Новосибирск, Российская Федерация
* e-mail: furibo@yandex.ru

Аннотация. Автор работы акцентирует внимание на периодах возникновения и дальнейшего развития (до середины 40-х годов XX века) отечественных государственных органов, обобщенно именуемых криптографическими службами. В статье показано, что российская криптография впервые появилась в XIV веке в монастырских рукописях в виде «затеи» церковных писарей, однако на «государеву службу» она поступила в XVI веке, выступая в качестве средства зашифровки царской переписки с различными корреспондентами. Автор статьи выделяет два периода в своем исследовании: досоветский и советский. В первом периоде анализируется процесс создания и деятельности таких царских органов, как Посольский приказ, Коллегия иностранных дел, секретная служба перлюстрации («черные кабинеты») МИД и др.; во втором – Шифровальный отдел НКИД, Центральный шифротдел штаба РККА, Специальный отдел ВЧК, Техническое отделение Оперативного отдела ОГПУ, Спецотдел ГУГБ НКВД и др. Автор статьи приходит к выводу, что криптографические службы России, пройдя долгий путь становления и развития в рассмотренный период, соответствовали своему предназначению, в целом были технически оснащены в соответствии с требованиями того времени и успешно решали ответственные задачи по обеспечению информационной безопасности государства.

Ключевые слова: криптография, шифрование, дешифрование, шифровальная машина, перлюстрация, правительственная связь

V. A. Gashenko[1*]

Establishment and development of the cryptographic service in Russia

[1] The Siberian Transport University, Novosibirsk, Russian Federation
* e-mail: furibo@yandex.ru

Abstract. The author focuses on the periods of the emergence and further development (until the mid-40s of the twentieth century) of domestic state agencies, generically referred to as cryptographic services. This article shows that Russian cryptography first appeared in the 14th century in monastery manuscripts as an "idea" of church scribes, but that it entered the "sovereign's service" in the 16th century, serving as a means for ciphering tsarist correspondence with various correspondents. The author of this article identifies two periods in her research: pre-Soviet and Soviet. The first period analyses the process of creation and activity of such tsarist bodies as the Ambassador's office, the Foreign Affairs Collegium, the secret service of perlustration ("black offices") of the Foreign Ministry, etc.; the second period includes the cipher department of the NKVD, the Central cipher department of the Red Army staff, the Special department of the Cheka, the Technical department of the Operative department of the OGPU, the Special department of the Main secret police of the NKVD, etc. The author concludes that cryptological services of Russia, having passed a long way of formation and development during the considered period, corresponded to their purpose, in general were technically equipped in accordance with requirements of that time and successfully solved important tasks of providing information security of the state.

Keywords: cryptography, encryption, decryption, encryption machine, perlusion, government communications

Введение

Анализ литературы и других источников, отражающих историю криптографических служб нашей страны, дает основание утверждать, что она до сих пор не исследована в полном объеме. Главной причиной этого, по-видимому, является большой объем исследуемого материала и его невероятная «запутанность». Так, во многих работах основной акцент делается на рассмотрении результатов криптологической деятельности наших соотечественников, т.е. рассматривается история появления разного рода шифров, шифровальных машин, биографии их создателей, принципы шифрования и т.д. Между тем, сам процесс создания криптографической службы в общем понимании этого слова, способствовавший появлению системы разнообразных государственных органов, рассматривается, как правило, в «фоновом» режиме. В этой связи возникает необходимость систематизации накопленного материала и его хронологического упорядочивания с целью воссоздания общей картины становления и развития структур, связанных с шифровальным и дешифровальным делом (криптографией и криптоанализом) в нашей стране. С учетом ограниченного объема статьи, ее автор хотел бы рассмотреть вопросы создания и развития основных криптологических служб в России с период с XVI века до 1945 года. Именно эти рубежи, на взгляд автора, можно считать наиболее интересными и знаменательными в истории становления и развития крипторграфической службы в России.

Обсуждение

По мнению некоторых исследователей [1], российская криптография как тайнопись впервые появилась в XIV веке в монастырских рукописях в виде «затеи» церковных писарей (например, в Смоленском Псалтыре 1395 года). Однако другие историки считают, что на «государеву службу» криптография поступила в XVI веке, выступая в качестве средства зашифровки царской переписки с различными корреспондентами [2].

Первые криптографы, в современном понимании этого слова, появились в Посольском приказе, созданном царем Иваном IV в XVI веке. [2]. Они были заняты разработкой шифров и ключей дешифрования («азбуки», «цифири», «цифры»), которые использовались в дипломатической переписке. Однако указанные лица не занимали конкретно созданных для этого должностей. Поэтому к первым официально утвержденным государственным органам, выполнявшим функции криптографической службы, большинство историков относят Походную посольскую канцелярию, созданную царем Петром I в XVIII веке. Ее главной задачей было ведение дипломатической переписки с использованием тайнописи [3]. Эта канцелярия позже стала называться Посольской канцелярией, а ее сотрудники занимались работой, связанной с усовершенствованием шифров, а также шифрованием и дешифрованием переписки Петра I и приближенных к нему лиц с разнообразными корреспондентами (европейскими монархами, российскими князьми, губернаторами, министрами, военачальниками и др.).

После смерти Петра I, при императрице Елизавете Петровне, продолжается развитие криптографической службы в форме создания так называемых «черных кабинетов», которые занимались перлюстрацией (негласным просмотром) корреспонденции, поступавшей в Россию и уходившей за границу. Эти кабинеты создавались, как правило, при почтовых отделениях, через которые пересылались письма [4].

При императоре Александре I создается Министерство иностранных дел, при котором существовал ряд криптографических подразделений: Первая цифирная (шифровальная) служба; Вторая цифирная (дешифровальная) служба; Третья цифирная (перлюстрационная) служба. [1].

В конце XIX века, с развитием технических устройств, многие государственные органы начинают использовать средства связи, нуждающиеся в криптографическом обеспечении. Так, в 1853 году телеграфом начинает пользоваться русская армия, в 1911 году вводится шифр в гвадейских частях России. В 80-е годы XIX века создаются криптографические службы в Министерстве внутренних дел, в Военном министерстве, Министерстве торговли. Главная задача этих служб заключалась в защите ведомственных и государственных секретов [4].

После изобретения радиосвязи, в 1895 году создаются соответствующие криптографические подразделения, которые занимаются, главным образом, кодированием передаваемой информации, особенно в военном деле.

Делая глобальное обобщение, досоветский период развития отечественной криптографической службы можно представить в виде следующей последовательности государственных органов, связанных с тайнописью: Посольский приказ, Походная канцелярия, Коллегия иностранных дел, секретная служба перлюстрации («черные кабинеты») МИД, «цифирный комитет» МИД, Особенная канцелярия Военного министерства, секретные экспедиции Департамента внешних сношений, «цифирная экспедиция» МИД, «секретные отделения» МВД, Особый отдел Департамента полиции.

После распада Российской империи в 1917 году и основания российской советской республики, криптогорфическая служба создается в нашей стране, по сути, заново, т.к. царские криптографы либо эмигрировали за границу, унеся с собой секретные коды и ключи, либо пошли на службу в белую армию. Сознательно на службу к большевикам шли единицы криптографов [1]. В этой связи, уже в декабре 1917 года в структуре Народного комиссариата ино**с**транных дел (НКИД) России появился «Отдел шифровальный и печатный», который 29 апреля 1918 года был реорганизован в самостоятельный Шифровальный отдел. После реорганизации НКИД в августе 1918 года, когда Канцелярия НКИД по делам Запада была переименована в Отдел Запада, в него вошло также и шифровальное отделение [1].

В структуре Рабоче-Крестьянской Красной армии в начале мая 1918 года обязанности по шифрованию и дешифрованию телеграмм были возложены на Общее отделение Военно-статистического отдела Оперативного управления Всероссийского главного штаба (ВГШ) РККА. [1].

13 ноября 1918 года издается Приказ РВС РСФСР № 217 о создании шифровального отделения во Всероссийском Главном штабе в составе 14 человек. Так появляется первый советский военный криптографический орган, который тогда был призван обеспечивать тайну проведения наступательных операций Красной армии на фронтах борьбы с международной интервенцией и внутренней контрреволюцией.

В 1920 году штатные шифровальные органы были введены во всех штабах военных округов, фронтов, армий и дивизий, а в 1921 году – во всех штабах, до бригады включительно. Тогда же начала создаваться система шифровальных органов РККА, ставшая сегодня основой службы защиты государственной тайны ВС РФ [4].

В дальнейшем шифровальный орган советских Вооруженных сил неоднократно менял свое название и организационно-штатную структуру. Так, в период с 1921 по 1941 годы существовали его следующие наименования: Центральный шифротдел штаба РККА (1921 г.); Шифровальный отдел при РВС СССР (1924 г.); Шифровальный отдел УД НКВМ (Управление делами Наркомата военмора) (1926 г.); 2-й отдел УД НКВМ и РВС (1929 г.); 7 отдел штаба РККА (1929 г.); 8-й отдел штаба РККА (1931 г.); 8-й отдел Генерального штаба РККА (1934 г.); Отдел шифровальной службы Оперативного управления Генерального штаба Красной Армии (1939 г.); 8-й отдел Оперативного управления Генерального штаба Красной Армии (1940 г.); Шифровальный отдел Генштаба Красной Армии (1941 г.) [4].

Вслед за созданием армейской криптографической службы, 5 мая 1921 года при Всероссийской Чрезвычайной Комиссии (ВЧК) создается Специальный отдел (8-й спецотдел при ВЧК), который занимался шифрованием, дешифрованием и созданием шифровальной техники [5]. В результате деятельности этого отдела в 1932 году появляется первая советская шифровальная машина ШМВ-1, а в последующие годы – шифровальная машина М-100 «Спектр» (1938 г.) и первая дисковая шифрмашина К-37 «Кристалл» (1939 г.) [6].

В 30-40-е годы XX века происходит дальнейшее совершенствование криптографических подразделений как в спецслужбах, так и в вооруженных силах страны. Так, в период с начала 1930-х годов и до начала Великой Отечественной войны шифровальные подразделения в органах госбезопасности носили следующие наименования: Спецотдел ГУГБ НКВД СССР (с 10.07.1934 г.); 9-й отдел ГУГБ НКВД СССР (с 25.12.1936 г.); Спецотдел НКВД СССР (с 09.06.1938 г.); 7-й отдел ГУГБ НКВД СССР (с 29.09.1938 г.); 5-й отдел НКГБ СССР (с 26.02.1941 г.) [4].

С началом Великой Отечественной войны крептографические функции были сосредоточены в руках сотрудников 5-го спецотдела НКВД СССР (с 31.07.1941 г.), затем – 5-го управления НКВД СССР (с 03.11.1942 г.), потом – 5-го управления НКГБ СССР (с 14.04.1943 г.) [4].

В военный период (1941–1945 гг.) криптографические органы советских спецслужб решали следующие основные задачи: повышение криптологической стойкости шифров, используемых для связи с агентами, подпольщиками и пар-

тизанами; проведение радиоигр с разведкой врага с использованием захваченных у него радиостанций; организация шифрованной связи во время переговоров и конференций лидеров союзников-участников антигитлеровской коалиции; разведывание новых каналов связи, перехват, анализ и чтение шифрованной корреспонденции, проходящей через дипломатические, военные сети, а также сети разведывательных и контрразведывательных служб антисоветских государств, их союзников и стран, придерживавшихся нейтралитета, с целью предоставления ее советскому руководству для принятия правильных стратегических решений; создание новых криптографических подразделений и специализированных лабораторий, а также решение проблем их кадрового укомплектования [7, 8, 9, 10, 17, 18].

Отдельно хочется остановиться на истории создания и развития Правительственной связи (так называемой ВЧ-связи) и Войск правительственной связи.

Необходимость использования указанного вида связи возникла в конце 1920-х годов. В указанный период телефонные переговоры руководителей государства с главами партийных и советских органов власти в республиках и других регионах СССР осуществлялись через сети связи общего пользования, которые находились в ведении Наркомата почт и телеграфов, причем скрытность телефонных разговоров руководящих работников практически не обеспечивалась [11]. В этой связи, в 1928 году И.В. Сталин поручил руководству ОГПУ организовать службу секретной телефонной связи для членов высшего политического, военного и хозяйственного руководства страны. В результате выполнения этого поручения, 1 июня 1928 года было создано 5-е (техническое) отделение Оперативного отдела ОГПУ, одной из задач которого было обслуживание абонентов высокочастотной телефонной связью с помощью станций ВЧ-связи, расположенных в Москве, Ленинграде, Ярославле и других крупных городах СССР. Для засекречивания этой связи использовалась аппаратура засекречивания (ЗАС) типа ЕС-1, МА-5 и МА-3. К началу 1939 года в СССР работали 62 станции правительственной связи, обслуживавшие 337 важных абонентов [11]. Особенностью довоенного периода использования ВЧ-связи было то, что ее работа обеспечивалась не только органами госбезопасности (ОГПУ, НКВД), но и органами гражданской связи (Наркоматом связи), а также военным ведомством (Наркоматом обороны).

С началом Великой Отечественной войны И.В. Сталиным была поставлена задача обеспечить устойчивой ВЧ-связью советское правительство с командованием армий и фронтов на огромном пространстве от Баренцева до Черного морей. В связи с этим, в августе 1941 года вышло постановление ГКО СССР об учреждении института уполномоченных по правительственной связи на местах. В рамках реализации данного постановления, в октябре 1941 года в структуре НКВД СССР было создан Отдел правительственной связи, на который была возложена задача технического обеспечения управления на уровне «Ставка-фронт-армия».

Как вид войск, войска правительственной связи (войска правительственной ВЧ-связи НКВД СССР) были созданы в начале 1943 года. В течение всего 1943

года шел процесс становления их организационной структуры, отрабатывались вопросы взаимодействия с командованием фронтов Красной армии [19].

30 января 1943 года Государственным Комитетом Обороны СССР было принято постановление, согласно которому строительство, восстановление, обслуживание и охрана всех магистральных линий, используемых для нужд правительственной ВЧ-связи, возлагались на НКВД СССР [11].

Управление связи Главного управления внутренних войск НКВД СССР, которое было создано 31 января 1943 года, приняло на себя функции линейной службы ВЧ-связи. В феврале 1943 года руководство войсками правительственной связи было передано Управлению войск правительственной связи.

В апреле 1944 года общая численность войск правительственной связи составляла 38148 человек, а к середине 1944 года – более 42000 человек [19, С. 218]. В марте 1945 года численность войск правительственной связи составляла уже 52574 человек [5].

В 1943–1945 годах Войска правительственной связи решали многочисленные задачи по обеспечению секретной связью военное руководство страны во всех наступательных и оборонительных операциях Красной армии на советско-германском фронте, а также в ходе боевых действий против милитаристской Японии на восточных рубежах нашей Родины [11, 12, 13, 14, 15, 16].

Таким образом, за военный период органы криптографической службы СССР различной ведомственной принадлежности предоставили советскому руководству большой объем важной информации, позволившей одержать победу в стратегически-значимых сражениях Великой Отечественной войны (сражение под Москвой, Сталинградская битва и др.). Советские криптологи добывали, перехватывали и дешифровывали шифры и переписку спецслужб, вооруженных сил и дипломатических органов Германии и ее союзников. Кроме того, в годы войны была значительно расширена сфера научных криптографических исследований, созданы новые виды шифровальной и дешифровальной техники, а также подготовлено большое количество способных ее эксплуатировать специалистов.

Заключение

Как разновидность тайнописи криптография появилась и развивалась в России по двум основным направлениям. Первое было связано с теоретической разработкой и созданием шифров, а также аппаратуры для их применения. Второе направление заключалось в практическом использовании шифров и шифровальной техники государственными органами для решения стоявших перед ними задач.

В досоветский период основным местом средоточения криптографических служб были органы, отвечавшие за развитие международных отношений. Со временем эти службы появились в органах внутренних дел, спецслужбах, а также в военных и гражданских ведомствах. В советское время происходили аналогичные процессы, однако наблюдалась тенденция выделения криптографических служб в самостоятельные структуры и даже виды войск.

Можно утверждать, что криптографические службы России, пройдя долгий путь становления и развития в рассмотренный период, соответствовали своему назначению, в целом были технически оснащены в соответствии с требованиями того времени и успешно решали задачи по обеспечению информационной безопасности государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гребенников В. В. Криптология и секретная связь. Сделано в СССР. – М. : Алгоритм, 2017. – 480 с.

2. Токарева Н. Н. Об истории криптографии в России // Прикладная дискретная математика. – 2012. – № 4 (18). – ISSN 2071-0410. – С. 183–185.

3. Соболева Т. А. История шифровального дела в России / [Электронный ресурс]. Режим доступа: https://www.universalinternetlibrary.ru/book/26603/ogl.shtml (дата обращения: 05.05.2023).

4. Шифровальная служба СССР и России / [Электронный ресурс]. Режим доступа: https://yarovan.ru/shifrsluzhba-sssr-rossii/ (дата обращения: 05.05.2023).

5. Ларин Д. А. Криптографическая служба России. Очерки истории: Монография. – М. : Гелиос АРВ, 2017. – 384 с.

6. Великая Победа: в 15 т. / под общ. ред. С.Е. Нарышкина, А.В. Торкунова; Моск. гос. ин-т междунар. отношений (ун-т) МИД России, Центр военно-политических исследований. Т. 10: Война в эфире. – М. : МГИМО–Университет, 2015.– 356 с.

7. Бутырский Л. С., Ларин Д. А., Шанкин Г. П. Криптографический фронт Великой Отечественной. – М. : Гелиос АРВ, 2017. – 688 с.

8. Ларин Д. А. Защита информации советских партизан и подпольщиков в годы Великой Отечественной войны / Д.А. Ларин // Безопасность информационных технологий. – 2011. – №3 (Т. 18). – ISSN 2074-3176. – С. 91–101.

9. Сколько битв выиграли криптоаналитики? // Север А. Лаврентий Берия. О чем молчало Совинформбюро. – М. : Алисторус, 2015. – 410 с.

10. Великая Победа: интернет-проект. Радиофронт VII. Криптографы вступают в бой / Под общ. ред. С. Е. Нарышкина, А. В. Торкунова; Ред. совет: А. Н. Артизов и др.; Московский гос. ин-т международных отношений (Ун-т) МИД России; Российское военно-историческое о-во. – 2015 / [Электронный ресурс]. Режим доступа: https://histrf.ru/uploads/media/artworks_object/0001/25/0d0945718c36be3438bb3b6afe9c314cbec548b7.pdf (дата обращения: 05.05.2023).

11. Чернышева Н.А., Коробицын А. С. Правительственной междугородной связи – 85 лет / [Электронный ресурс]. Режим доступа: https://vvprf/special/kreml-9/pravitelstvennoy-mezhdugorodnoy-svyazi-85-let.html (дата обращения: 05.05.2023).

12. От внутренней стражи Российской империи к войскам национальной гвардии Российской Федерации. 2-е изд. М. : Ред. журнала «На боевом посту» внутренних войск МВД России, 2019. – 160 с.

13. Бунин С. В., Марценюк Ю. А., Беркутов А. С., Климов А. А., Ченцов А.С. Войска НКВД в Великой Отечественной войне: в 3 томах. Том 3. Войска НКВД в третий период Великой Отечественной войны и в советско-японской войне (1944–1945). – М. : Ред. журнала «На боевом посту» внутренних войск МВД России, 2015. – 416 с.

14. Феськов В.И., Калашников К.А., Голиков В.И. Красная армия в победах и поражениях 1941–1945 гг. – Томск: Изд-во Том. ун-та, 2003. – 620 с.

15. Войска национальной гвардии Российской Федерации. Исторический очерк. – М.: Ред. журнала «На боевом посту» внутренних войск МВД России, 2018. – 448 с.

16. Ландер И.И. Негласные войны. История специальных служб 1919-1945: в двух книгах. Книга вторая. – Одесса: Изд-во «Друк», 2007. – 643 с.

17. Ларин Д.А. Советская шифровальная служба в годы Великой Отечественной войны / Д.А. Ларин / [Электронный ресурс] // Известия Уральского государственного университета. Серия 1: Проблемы образования, науки и культуры. – 2011. – Т. 86, № 1 – С. 69–80. Режим доступа: https://www.elibrary.ru/download/elibrary_15665372_85920693.pdf (дата обращения: 05.05.2023).

18. Прочти меня, если сможешь. Советские «тьюринги» и криптография времен Великой Отечественной Войны // Бессмертный полк. Москва: электронная кн. Памяти / [Электронный ресурс]. Режим доступа: https://www.polkmoskva.ru/articles/machines/prochti-menya-esli-smozhesh/ (дата обращения: 05.05.2023).

19. Краткая история внутренних войск. – М.: Ред. журнала «На боевом посту» внутренних войск МВД России, 2015. – 432 с.

20. Макаров В.Г. Лучшие спецоперации СМЕРШа. Война в эфире. – М.: Яуза; Эксмо, 2009. – 384 с.