КРИПТОГРАФИЧЕСКАЯ СЛУЖБА МИД РОССИЙСКОЙ ИМПЕРИИ В ПЕРИОД ПЕРВОЙ МИРОВОЙ ВОЙНЫ

Дмитрий Ларин*

В этом году исполняется 100 лет с начала Первой мировой войны (1) (1914-1918), одного из крупнейших военных конфликтов в истории человечества. В данной статье будет рассмотрена криптографическая деятельность российских спецслужб, в первую очередь шифровальщиков и дешифровальщиков МИД, при этом следует отметить, что все российские криптографы (такая деятельность велась еще в МВД и военном ведомстве) тесно сотрудничали между собой, криптографы МИД и МВД часто командировались к военным и помогали вести дешифровальную работу, а некоторые специалисты иногда одновременно числились в штате разных ведомств. При этом МИД (2) был все же главной организацией в области криптографии в стране в описываемый период.

Первая мировая война произвела революцию в военном деле, во время этого конфликта в массовом порядке были применены совершенно новые средства вооруженной борьбы: боевые самолеты и дирижабли, бронеавтомобили и танки, подводные лодки, и наконец, оружие массового поражения – отравляющие газы.

Во время Первой мировой войны ключевым моментом стало широкомасштабное применение противоборствующими сторонами радиосвязи для управления войсками. Радиосвязь оказалась дешевле и мобильнее проводной. Появилась возможность активизировать связь между военными подразделениями, устанавливать связь с подвижными объектами (автомобили, самолёты, корабли). Но имелась и другая сторона использования радиосвязи. Вопрос перехвата радиосообщений в техническом смысле не представлял принципиальных проблем.

Интересно отметить, что первым, кто высказал идею о возможности радиоперехвата, был автор знаменитого «Маугли» английский писатель Редьярд Киплинг. В 1902 году он опубликовал рассказ «Беспроволочный телеграф», в котором была описана возможность добычи информации подобным методом. Правда, процесс радиоперехвата в этом рассказе «уподоблялся спиритическому сеансу – те же «обрывки посланий, долетающие невесть откуда, отдельные слова, а в целом ничего не разберешь» [10. С. 7].

Первые реальные опыты по перехвату иностранных радиограмм были проведены моряками Балтийского флота летом 1902 года под руководством изобретателя радио Александра Степановича Попова. В 1903 году на российском флоте началось регулярное ведение радиоразведки, что нашло отражение в одном из важнейших флотских документов – «Своде военно-морских сигналов» [8]. Во время русско-японской войны 1904-05 годов впервые в мире начала применятся радиоразведка (наблюдение за радиосетями противника, перехват и дешифрование вражеских радиограмм) и радиоэлектронная борьба (постановка помех с целью срыва радиосвязи противника).

* Ларин Дмитрий Александрович, кандидат технических наук, историк криптографии.

Приоритет в использовании этих новых видов боевых действий принадлежит российскому военно-морскому флоту. Фактически, русские моряки начали войну в новом измерении – радиоэфире.

Теперь работа дешифровальщиков облегчилась, так как информацию, передаваемую по радио, защитить физически не представлялось возможным. Защищающаяся сторона, естественно, осведомленная о таком положении дел, иногда отказывалась от эффективной радиосвязи и использовала проводной телеграф, а нередко и отправку специальных курьеров. Резко возросли требования к помехоустойчивости шифров, поскольку радиоканал порождал значительно более серьёзные искажения, чем проводная связь. Значительно более актуальным стал вопрос об имитостойкости сети засекреченной связи.

Резкое расширение объёмов секретных зашифрованных передач и сравнительная простота радиоперехвата сообщений подтолкнули криптографов-дешифровальщиков к мысли о том, что исследование отдельной перехваченной криптограммы необходимо связать с анализом всего массива перехвата, в котором появилась эта криптограмма. Этот путь оказался весьма плодотворным. Как справедливо отмечает американский историк Д. Кан, телеграф создал современное шифровальное дело, радио — современный криптоанализ [6].

Исходя из вышесказанного, перед криптографической службой МИД России стояли 2 основные задачи. Во-первых, обеспечить защиту собственных линий связи (а специалисты дипломатического ведомства разрабатывали шифры и для военного ведомства, для МВД и ряда других ведомств, таких как таможня, пограничная стража, министерство финансов, министерство путей сообщения и т.п.). Подробнее о работе криптографов МИД во второй половине XIX –начала XX века можно прочитать в статье [4]. Во-вторых, дешифровальщики МИД должны были добывать информацию из дешифрованной переписки наших потенциальных, а после начала войны и реальных противников. На этом поприще имелись существенные успехи. В 1913-1914 годов они раскрыли 2 939 телеграмм из переписки государств из коалиции противника, в том числе: австрийских - 569, германских - 171, болгарских - 246, турецких - 181 [9. С. 283-284].

С 1910 по 1916 год министром иностранных дел Российской Империи являлся Сергей Дмитриевич Сазонов, именно он 1 августа 1914 года принял от германского посла ноту об объявлении войны. С.Д. Сазонов был женат на сестре жены знаменитого государственного деятеля России П.А. Столыпина и, став премьер министром, Петр Аркадьевич пригласил Сазонова на пост министра иностранных дел в своем правительстве. Однако на такой шаг Столыпина подвигли отнюдь не родственные связи. С.Д. Сазонов закончил Императорский Александровский Лицей, с 1883 года находился на службе в МИД на различных должностях (перед тем как стать министром занимал должность товарища (по современному, заместителя главы МИД), этот человек был полиглотом, музыкантом, знатоком истории и политики. Именно он курировал работу криптографов МИД в предвоенный и военный период.

Следует отметить, что сроки действия ключей были очень длительными. Некоторые ключи, введенные в середине XIX века, действовали и в начале XX века. Такой длительный срок использования ключей, разумеется, снижал стойкость шифров. К тому же биклавные шифры (3) не подходили для шифрования информации, передаваемой по телеграфу. Начальник 1-й экспедиции шифровального департамента отдела МИД (так тогда называлась наша шифровальная служба) К.Ф. Таубе писал в начале XX века: «Система биклавная не применима в настоящее время ввиду смешанной передачи буквами и цифрами, не допускаемой телеграфными конвенциями» [9. С. 229]. Однако некоторое количество шифров биклавного типа применялось для зашифрования секретной почтовой корреспонденции и в начале XX века.

К сожалению, российские шифры иногда становились объектами кражи. Особенно крупная утрата шифров произошла в русском посольстве в Пекине 19 августа 1888 года. Несмотря на компрометацию, ключи продолжали использоваться, что совершенно недопустимо! Например, ключ № 356, украденный в Пекине, был выведен из употребления лишь на некоторое время. В начале 1890-х годов его вновь ввели в действие, но уже в Европе. В 1898 году произошла еще одна компрометация этого шифра: один экземпляр его был утрачен начальником Адриатической эскадры. Только после этого действие ключа было прекращено окончательно. В Пекине также был украден русский ключ № 361. Его окончательно вывели из действия лишь в 1903 году, но и

после этого барон Таубе писал: «Ключ № 361 может применяться как временный в специальных случаях, кроме Дальнего Востока» [9. С. 222].

В 1913 году К.Ф. Таубе было присвоен чин тайного советника, что приблизительно соответствует армейскому званию генерал-лейтенанта. За работу по совершенствованию отечественной криптографической службы К.Ф. Таубе награжден российскими орденами Святого Владимира 3 и 4 степени, а также орденом Станислава 1 степени.

Начавшаяся война показала, что шифровальная служба Российской Империи не сумела предвидеть опасность проблемы по своевременному вводу новых специальных шифров и кодов на военный период по линии МИД. Уже к концу 1914 года стало ясно, что действующие шифры и коды не обеспечивают в достаточной мере тайну государственной, дипломатической и военной переписки и вместе с тем не позволяют ускорить скорость процесса шифрования и расшифрования.

Руководством МИД была поставлена задача по изготовлению новых шифров и кодов для снабжения своих подразделений в России и за рубежом.

Чиновникам МИД была поставлена задача срочно изготовить:

1) особые кодовые книги в 10 тысяч знаков, наборные и разборные, которые включали дипломатический русский код, дипломатический французский код, два восточных кода и консульский код.

2) словарные наборные и разборные таблицы с особыми вертикальными шифрами (очевидно, речь идет о кодовых книгах с перешифровкой шифром вертикальной перестановки);

3) особые ключи для перешифрования.

Однако через два года, осенью 1917-го, в докладе, представленном руководством шифровального отдела уже Временному правительству, констатировалось, что выполнение, намеченное к началу 1915 году, этой программы провалилось и что пришлось в качестве временных мер вводить более слабые шифры - «трехзначные словари» (напомним, что так в то время назывались коды – Д.Л.)» [9. С. 345].

Коды широко использовались в описываемый период для шифрования дипломатических сообщений как в России, так и в других странах, кстати заметим, что подобные системы шифрования применялись дипломатами разных стран даже после окончания Второй Мировой войны.

Что касается отечественных кодовых систем периода Первой Мировой войны, используемых в МИД, то практика их применения была такой: для одних кодов перешифровка была обязательной, для других — в случаях передачи особо секретных сообщений. Чиновники, которые, создавали шифры в МИД Российской Империи, хорошо понимали, что простые коды могут быть сравнительно легко дешифрованы противником, с другой стороны, перешифровка занимала дополнительное время на операции по шифрованию и расшифрованию. Приходилось искать разумный компромисс.

Тем не менее, в случаях, если из МИД России в какое-либо из наших посольств, консульств или из них передавался какой-то текст, известный или возможно становившийся известным потенциальному противнику, то этот текст необходимо было передавать, в обязательном порядке, используя сочетание специальных кодов и перешифровок. Так, например, в 1916 году «для этой цели использовались «Французский (4) общий малый дипломатический ключ № 431» и «Английский малый дипломатический ключ № 407» с обязательным перешифрованием» [9. С. 240].

К сожалению, ряд шифров, разработанных в МИДе и переданным военному ведомству, был вскрыт противником. Причина этого, в основном, заключалась даже не в слабости предложенных шифров, а в неправильной их эксплуатации. Чтение российской военной переписки австрийцами и немцами позволило им принимать эффективные решения при ведении боевых действий. Подробный рассказ об этих событиях выходит за рамки данной статьи. Об этом можно, в частности, прочитать в книгах [5] и [6].

Определенные проблемы были и в организации шифрованной связи непосредственно в недрах внешнеполитического ведомства, так, например, сведения о скомпрометированных шифрах, поступали не своевременно, из-за чего эти шифры продолжали употребляться и после компрометации. Вот что пишет об этом Т.А. Соболева: «Так, 6 февраля 1915 г. помощник начальника канцелярии МИД И. Базили сообщал в политический отдел: «Ввиду обнаружившейся несомненной скомпрометированности наших ламных словарных ключей (номера 335, 371, 374, 379, 382 и 391), из коих некоторые, как ключ 379 (Шпейера), прямо захвачены неприятелем, оказывает-

ся совершенно необходимым изъять все эти ключи из употребления...» [9. С. 356]. Тем не менее, как было отмечено выше, специалисты МИД всячески старались обеспечить секретность правительственной, дипломатической и военной переписки Российской Империи.

Теперь обратимся к дешифровальной работе специалистов МИД России в ходе войны. Разумеется, главной целью их работы были шифры, противостоящих России стран. Здесь были достигнуты значительные успехи, как отмечает российский историк Т.А. Соболева: «Дешифровальная служба МИД России непосредственно перед войной и во время войны довольно успешно работала над раскрытием шифров и кодов и читала переписку многих иностранных государств и, в первую очередь, стран, находившихся в состоянии войны с Россией. За 1914—1916 гг. (данные на 22 апреля 1916 г.) было дешифровано 588 австрийских телеграмм, 60 германских, 606 болгарских, 225 турецких, 457 итальянских и т. д. Можно отметить снижение числа дешифрованных телеграмм по ряду государств, что объясняется, в первую очередь, резким сокращением передачи таких телеграмм по радио. Так, за время с июля 1915 года по март 1916 года Германия и Австро-Венгрия совсем перестали пользоваться радиотелеграммами для сношения со своими миссиями в Балканских странах и пользовались для этой цели исключительно телеграфом. Дешифрование указанных сообщений проводилось не только с помощью добытых разведкой шифров и кодов, но и за счет аналитической дешифровальной работы» [9. С. 348-349].

Разумеется, добываемая дешифровальщиками информация была очень полезна российскому руководству. При этом следует отметить, что дешифровальная служба МИД Российской Империи проявляла интерес и к шифрпереписке союзников России и нейтральных государств.

Как уже было отмечено выше, сотрудники дешифровальной службы МИД России в ходе войны прикомандировывались к соответствующим подразделениям вооруженных сил и МВД (здесь основная задача была борьба с вражеской, в первую очередь германской агентурой, практически все разведчики противника использовали шифры). Специалисты-криптографы МИД оказали большую помощь нашим военным и сотрудникам правоохранительных органов. Помощь со стороны МИД не осталась не оцененной. Приведем лишь один пример: «22 февраля 1916 г. приказом командующего Балтийским флотом вице-адмирала Канина прикомандированный к станции особого назначения Южного района службы связи статский советник Эрнест Феттерлейн «за выполнение особого поручения, имеющего важное боевое значение» был награжден орденом Святой Анны 2-й степени. Примерно в то же время два других сотрудника шифротдела МИД надворный советник Юрий Павлович и дворянин не имеющий чина, Борис Орлов, работавшие там же, были награждены орденом Святого Станислава соответственно 2-й и 3-й степени» [9. С. 349-350]. Это лишь один из примеров работы чиновников МИД в интересах военного ведомства, специалисты внешнеполитического ведомства в течение всего периода войны постоянно помогали военным криптографам в дешифровании вражеской шифрпереписки.

Кстати, дешифровальная служба Российского флота, особенно на Балтике, достигла существенных успехов в осуществлении перехвата и дешифрования шифрованных радиограмм германского флота, что позволило провести ряд успешных операций против ВМС Германии, а на Черном море против ВМС Турции, подробнее об этом можно прочитать в частности в книге [1].

Российские моряки фактически переломили ход Первой Мировой войны. В августе 1914 года наскочил на мель в восточной части Балтийского моря у острова Оденсхольм немецкий легкий крейсер «Магдебург». Русские моряки сумели достать с этого крейсера кодовые книги ВМС Германии. Захваченными на «Магдебурге» кодовыми книгами русские поделились со своими союзниками — англичанами. Эта информация легла в основу успехов английской дешифровальной службы во время Первой мировой войны. Американский историк криптографии Д. Кан назвал этот эпизод важнейшим событием в истории криптографии [6]. А теперь покажем, как оценивает захват немецких кодовых книг на «Магдебурге» в своих мемуарах У. Черчилль. Вот какую цитату из книги [11] приводит Д. Кан: «В начале сентября 1914 г. на Балтийском море был потоплен немецкий легкий крейсер «Магдебург». Несколько часов спустя русские выловили из воды тело утонувшего немецкого младшего офицера. Окостеневшими руками... он прижимал к груди кодовые книги ВМС Германии, а

также разбитые на мелкие квадраты карты Северного моря и Гельголандской бухты. 6 сентября ко мне с визитом прибыл русский военно-морской атташе. Из Петрограда он получил сообщение с изложением случившегося. Оно уведомляло, что с помощью кодовых книг русское Адмиралтейство в состоянии дешифровать по меньшей мере отдельные участки немецких военно-морских шифртелеграмм. Русские считали, что Адмиралтейству Англии, ведущей морской державы, следовало бы иметь эти книги и карты. И если бы мы прислали корабль, то русские офицеры, в ведении которых находились книги, доставили бы их в Англию. Мы незамедлительно отправили такой корабль, и октябрьским вечером принц Луи и я получили из рук наших верных союзников слегка попорченные морем бесценные документы» [6. С. 265]. Подробнее о захвате шифрматериалов на «Магдебурге» рассказано, в частности, в книгах [5] и [6].

Предоставленные материалы позволили англичанам читать секретную переписку немецкого военно-морского флота и одержать ряд побед. Но самое главное, англичане выяснили, что немецкие дипломатические коды созданы на основе военно-морских. Благодаря этому английским дешифровальщикам удалось вскрыть телеграмму министра иностранных дел Германии А. Циммермана послу Германии в Мексике, в которой предписывалось принять меры по организации нападения мексиканцев на США, а также в ней сообщалось, что Германия начинает неограниченную подводную войну, в том числе против кораблей нейтральных стран, в первую очередь США. Публикация этой информации в американских СМИ и впоследствии докладе в Конгрессе, привела к вступлению США в Первую Мировую войну на стороне Антанты. Подробнее об этом можно прочитать, в частности, в книгах [6].

Более широкую и масштабную работу по дешифрованию вражеской шифрпереписки во многом не удавалось провести из-за недостаточного количества средств радиоперехвата и острой нехватки специалистов-криптографов. Как мы отмечали выше, объемы только радиоперехвата с началом войны возросли в разы, а ведь были еще перехваченные телеграммы и бумажные сообщения агентуры противника. Тем не менее, специалисты-криптографы МИД, а также их коллеги из МВД и военного ведомства продолжали поставлять руководству Российской Империи важную информацию из дешифрованных сообщений врага.

К сожалению, общая ситуация в стране стремительно ухудшалась, надвигалась революция. Многие неудачи отечественной криптографии заключительного периода Первой Мировой войны «обусловлены в первую очередь и главным образом не ее низким теоретическим и практическим уровнем, а разладом всей государственной машины в целом и, как следствие, разладом в самой организации криптографической службы, в ее координации, финансировании, снабжении и т. д. Инициатива и предложения рядовых сотрудников и руководителей среднего звена управления разбивались о бездействие «высшего эшелона» [9. С. 350].

Скоро грянула Октябрьская Революция и криптослужба МИД России, как и все государственные институты, на время прекратила свое существование. Хотя следует отметить, что во время Гражданской войны в России активную криптографическую деятельность вели и красные, и белые, подробнее об этом можно прочитать в статье [7].

Уже 5 мая 1921 года отечественная криптографическая служба была возрождена в виде Спецотдела при ВЧК (подробнее о нем в серии статей [3]) и до настоящего времени успешно решает задачи по обеспечению информационной безопасности нашей Родины.

ПРИМЕЧАНИЯ

(1) Отметим, что это название стало использоваться лишь после начала Второй мировой войны в 1939 году, до этого Первую мировую называли Великой войной, после революции в России, эта война получила название «империалистической» или «германской».

(2) Напомним, что штатная шифровальная служба была образована в России в составе Посольского Приказа, первый профессиональный дешифровальщик Х. Гольдбах, 18 марта 1742 именным указом Императрицы Елизаветы Петровны был назначен на «особливую должность в Коллегии Иностранных дел» [9. С. 118] Успешная работа российских дешифровальщиков шла всю вторую половину XVIII века и продолжилась в XIX-ом.

(3) Подробно эти шифры, разработанные в 1840-х годах руководителем криптографической службы России, действительным статским советником, бароном Н.Ф. Дризеном, описаны, в частности, в статье [2].

Литература:

1. Алексеев М. Военная разведка России. Первая мировая война. Кн.III, ч.2. М., 2001.
2. Бабаш А.В., Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Криптографические идеи XIX века. Русская криптография // Защита информации. Конфидент. №3, 2004.
3. Бабиевский В.В., Бутырский Л.С., Ларин Д.А. История Спецотдела ВЧК – ГПУ- ОГПУ. Части 1-5. // Защита информации. INSIDE. №3-6, 2011, №1-2, 2012.
4. Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П. Научно-технический прогресс и криптографическая деятельность в России XIX века. // Защита информации. INSIDE. №2, 2005.
5. Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П. Криптография: страницы истории тайных операций. М., 2008.
6. Кан Д. Война кодов и шифров. М., 2004.
7. Ларин Д.А. Криптографическая служба в годы Гражданской войны в России // Проблемы отечественной истории. Выпуск 11. М., 2009.
8. Партала М.А. Имя А.С. Попова в истории отечественной радиоразведки // Защита информации. INSIDE. № 4, 2010.
9. Соболева Т.А. История шифровального дела в России. М., 2002.
10. Сырков Б. Прослушка. Предтечи Сноудена. М., 2013.
11. Черчилль У. Мировой кризис. М. – Л., 1932.

THE CRYPTOGRAPHIC SERVICE OF THE RUSSIAN EMPIRE'S MINISTRY FOR FOREIGN AFFAIRS DURING WORLD WAR I

This year commemorates the 100th anniversary of the beginning of one of the greatest conflicts in the human history – World War I (1914-1918). This article is devoted to the cryptographic activity of the Russian special services, first of all cryptographers, during that period. It is worth noting that all Russian cryptographers belonging to different services worked in close cooperation with some of them being assigned to the Ministry for Internal Affairs and the Ministry for Foreign Affairs simultaneously. But the Ministry of Foreign Affairs was considered as the leading cryptographic organization at that time.

D.A. Larin. Candidate of Science (Technical sciences), Cryptography history expert

Ключевые слова:
Первая Мировая война, криптографическая служба МИД, дешифрование.

Keywords:
Word War 1, cryptography service of the Russian Ministry for Foreign Affairs, cryptanalysis.

References:

1. Alekseev M. Voennaya razvedka Rossii. Pervaya mirovaya voina. [Russian military Intelligence. World War I] Book III, part 2. M., 2001.
2. Babash A.V., Gol'ev J.I., Larin D.A., Shankin G.P. Kryptograficytskie idei XIX veka. Russkaya kriptografia [Cryptographic ideas of XIX century. Russian cryptography]// Zaschita informacii. Konfident. [Information Security. Konfident] Vol. 3, 2004.
3. Babievskiy V.V., Butyrsky L.S., Larin D.A. Istoriya Specotdela VCHK-GPU-OGPU [History of Spesial Department Soviet Secret Servis]] Part 1-5// Zaschita informacii. INSIDE [Information Security INSIDE] Vol. 3-6, 2011, №1-2, 2012.
4. Gol'ev J.I., Larin D.A., Trishin A.E. Shankin G.P. Nauchno-tehnicheskiy progress i kriptograficheskaya deyatelnost' v Rossii XIX veka [Scientific-technical progress and the cryptographic operations in Russia in XIX century] // Zaschita informacii. INSIDE [Information Security INSIDE] Vol. 2, 2005.
5. Gol'ev J.I., Larin D.A., Trishin A.E. Shankin G.P. Kriptografiya. Stranici istorii taynih operaciy [Cryptography: pages from the history of covert operations]. M., 2008.
6. Kahn D. Voina kodov i shifrov [War of codes and ciphers]. M. 2004.
7. Larin D.A. Kriptograficheskaya slugba v godi gragdanskoy voyni v Rossii [Cryptographic servis in the years civil war in Russia] // Problemi otechestvennoy istorii [Russian history problems]. Vol. 11. M. 2009.
8. Partala M.A. Imya A.S. Popova v istorii otechestvennoy radiorazvedki [The name of A.S. Popov in history Russian radiointelligence] // Zaschita informacii. INSIDE [Information Security INSIDE] Vol. 4, 2010.
9. Soboleva T.A. Istoria shifroval'nogo dela v Rossii [History Russian cryptography] M., 2002.
10. Syrkov B. Proslushka. Predtechi Snowdena [Wiretapping. The Forerunner Of Snowden]. M. 2013.
11. Churchill W. Mirovoy crisis [World Crisis]. M.-Leningrad, 1932.