СЕРИЯ «ДОСЬЕ»

Татьяна Соболева

ИСТОРИЯ ШИФРОВАЛЬНОГО ДЕЛА В РОССИИ

Москва
«ОЛМА-ПРЕСС»
2002

ББК 63.3(2)6
С 54

Соболева Т. А.

С 54 История шифровального дела в России. — М.: ОЛМА-ПРЕСС-Образование, 2002. — 511 с.: ил. — (Досье)

ISBN 5-224-03634-8

В книге прослеживается история становления отечественной криптографической службы, которое происходило на протяжении нескольких веков Принципы и основы этой работы, ее формы и методы, приемы и способы вырабатывались несколькими поколениями русских криптографов, начиная с эпохи Петра Великого и до начала Второй мировой войны Обо всем этом автор рассказывает, опираясь на большой документальный материал

ISBN 5-224-03634-8

ПРЕДИСЛОВИЕ

Каждое государство стремится тщательно хранить свои секреты. При этом в разряд секретных попадает и деятельность государственных служб, призванных тем или иным способом осуществлять эту охрану. Криптографическая служба исключения не составляет.

В секретных инструкциях государственных органов России всегда подчеркивалось, что все документы, касающиеся деятельности криптографической службы, составляют государственную тайну, подлежат особому хранению и при определенных условиях уничтожаются. Эти правила российская криптографическая служба строго соблюдала. К разряду секретных до последнего времени относились и материалы, связанные с историей самой криптографической службы.

В то же время мировая историческая наука вопросы истории криптографической службы различных государств исследовала весьма основательно, естественно, без ущерба для современных государственных интересов заинтересованных сторон.

Наиболее фундаментальным трудом на эту тему является книга Дэвида Кана «Взломщики кодов», выпущенная издательством «Макмиллан» (David Kahn. The Codebreakers. — N. Y., 1967). Автор кни-

ги, известный журналист, президент американской ассоциации криптографов, сделал попытку, и, надо сказать, весьма удачную, осветить в общедоступной форме, приводя многочисленные примеры, мировую историю криптографической деятельности с древнейших времен до конца 50-х годов XX в. Одна глава в книге Д. Кана, к сожалению весьма краткая и носящая лишь обзорный характер, посвящена истории криптографии в России.

Между тем история криптографической службы является неотъемлемой частью истории Российского государства и уже с середины XIX века вызывала значительный интерес у исследователей. Одной из первых отечественных научных публикаций на эту тему явилась работа Г. Попова «Дипломатическая тайнопись эпохи царя Алексея Михайловича» (в «Записках Археологического общества». Т. V. СПб., 1853). В той или иной степени этого вопроса касались в своих работах такие крупные ученые, как академики А. И. Соболевский, М. Н. Сперанский и некоторые другие, однако, как правило, лишь в палеографическом аспекте.

Становление отечественной криптографической службы происходило на протяжении многих десятилетий и даже веков. Принципы и основы этой работы, ее формы и методы, приемы и способы вырабатывались несколькими поколениями русских криптографов, их трудом, опытом, порой мучительными поисками истины. В этой истории, как и в истории любой науки, всякого вида человеческой деятельности, были свои победы и поражения, успехи и неудачи, великие и трагические страницы. Все они — наше национальное достояние, наша память, гордость и боль. И обязанность отечественной исторической науки — открыть эти страницы. Сделать их доступными для широкой общественности.

Перед читателем второе издание книги, в которой автор впервые в отечественной исторической науке

делает попытку на базе найденных архивных документов, существующих исторических исследований и других материалов воссоздать более полную картину становления и развития криптографической службы России, критически осмыслить накопленный исторический опыт, рассмотреть роль этой службы в истории нашего государства в целом, познакомить читателя с ранее неизвестными историческими фактами, событиями, именами.

Кроме прочих источников в работе использованы некоторые материалы специальных архивов, ссылки на которые не приводятся.

ВВЕДЕНИЕ

«Криптография» — слово греческое, в переводе означает тайное, скрытое (крипто) письмо (графия), или тайнопись. Наукой не установлен точный исторический период, когда появилась криптография, каковы были ее первоначальные формы и кто был ее создателем. Американский криптограф Л. Д. Смит подчеркивает, что криптография по возрасту старше египетских пирамид. Другой американец — Флетчер Пратт в своей книге «История шифров и кодов» дает такое определение криптографии: «Криптография— искусство шифрования — это процесс выражения слов, передающих смысл только немногим лицам, которым известен этот секрет». Из подобного определения следует, что всякое письмо, написанное на неизвестном для того или иного человека языке, является шифрованным письмом, то есть любой алфавит может стать шифром. Следует предположить с большой долей вероятности, что как только человечество достигло определенного уровня цивилизации и возникла письменность, тотчас же появилась и криптография.

Уже в исторических документах древних цивилизаций — Индии, Египта, Месопотамии — имеются сведения о системах и способах составления шифрованного письма.

В древнеиндийских рукописях приводится более 60 способов письма. Среди них есть и такие, которые можно рассматривать как криптографические, то есть обеспечивающие секретность переписки. Так, встречается описание системы замены гласных букв согласными, и наоборот. В этих рукописях упоминается о тайнописи как об одном из 64 искусств, которым должны овладеть и женщины.

Один из самых старых шифрованных текстов Месопотамии представляет собой табличку, написанную клинописью и содержащую рецепт изготовления глазури для гончарных изделий. Автор этой клинописи, стремясь скрыть содержание написанного, использовал редко употребляемые знаки, игнорировал некоторые гласные и согласные, вместо имен употребил цифры.

Использовалась тайнопись и в рукописных памятниках Древнего Египта. Здесь шифровались религиозные тексты и медицинские рецепты.

Сохранились достоверные сведения о системах шифров, применявшихся в Древней Греции. Известно, что в Спарте в V—IV веках до н. э. существовала тайнопись. Образованные греки того времени применяли шифровальный прибор «Сцитала». Он представлял собой два цилиндра одинакового диаметра. Каждая из переписывающихся сторон имела у себя один из цилиндров. Шифрование осуществлялось следующим образом: на цилиндр наматывали узкую полоску пергамента; текст, подлежащий зашифрованию, выписывали на ленту вдоль цилиндра, затем ленту сматывали и отправляли корреспонденту. Он, обернув лентой свой цилиндр, читал сообщение. Это был первый шифр, осуществляющий перестановку букв в тексте, где буквы шифруемого (открытого) текста переставлялись и отстояли друг от друга на длину окружности цилиндра. Сохранение в тайне диаметра цилиндров обеспечивало секретность переписки. Вместо специальных цилиндров приме-

нялись жезлы, рукоятки мечей, кинжалов, копий и др. Известен также и метод дешифрования данного шифра, приписываемый Аристотелю. Предлагалось сделать длинный конус и, обернув его у основания полоской перехваченного пергамента, сдвигать пергамент к вершине конуса. Там, где диаметр конуса совпадал с диаметром «Сциталы», буквы на пергаменте сочетались в слоги и слова.

Другим шифровальным прибором времен Спарты был прибор, называемый «табличка Энея». На небольшой табличке горизонтально располагался алфавит, а по ее боковым сторонам имелись выемки для наматывания шнура. Для зашифрования текста шнур закрепляли у одной из сторон таблички и наматывали на нее. При этом на шнуре делали отметки в местах, которые находились напротив букв алфавита, соответствующих буквам шифруемого текста. По алфавиту можно было идти только в одну сторону, то есть делать по одной отметке на каждом витке. После зашифрования шнур сматывали и отсылали корреспонденту. Этот шифр есть шифр замены букв открытого текста знаками, которые передавали расстояния на шнуре между отметками. Размер таблички, а также порядок расположения букв на ней обеспечивали секретность.

В Древней Греции криптография широко использовалась в разных областях деятельности. Так, Плутарх сообщает, что жрецы хранили в форме тайнописи свои прорицания. Однако наиболее широкое применение криптография получила в государственной сфере. Во все времена криптография была одним из основных орудий в межгосударственной борьбе, надежным средством сокрытия политических, дипломатических, экономических и иных секретов государства, с одной стороны, и средством проникновения в секреты государства-противника — с другой.

Эней в своем сочинении «Об обороне укрепленных мест» предложил использовать для шифрования

военной переписки книжный шифр, в котором буквам открытого текста соответствуют буквы, находящиеся на определенных местах в являющемся ключом книжном тексте. Эта система шифра установила рекорд долголетия: она применялась даже в середине XX века, в период Второй мировой войны.

Полибий предложил систему шифра, вошедшего в историю как «квадрат Полибия», и представлявшего собой замену каждой буквы парой чисел — координатами буквы в квадрате, где написан весь алфавит. О криптографии упоминается и в «Илиаде» Гомера.

Криптография сыграла значительную роль в укреплении могущества Римской империи. В частности, особая роль в обеспечении государственной тайны принадлежит новому способу шифрования, изобретенному Юлием Цезарем и изложенному им в «Записках о галльской войне» (I в. до н. э.). «Шифр Цезаря» представляет собой замену букв в соответствии с подстановкой, нижняя строка которой — алфавит открытого текста, сдвинутый на три буквы влево.

Во всеобщей истории почти не нашла отражения криптографическая практика в мрачные годы средневековья. В этот период искусство шифрования, и тем более дешифрования, сохранялось в строжайшей тайне. Известно, например, что в годы крестовых походов составители шифрованных писем, служившие у папы римского, после года работы подлежали физическому уничтожению — так сохранялась тайна применявшегося шифра.

В эпоху Возрождения в итальянских городах-государствах параллельно с расцветом культуры и науки активно развивается криптография. Торговля, мореплавание, войны требовали развития шифрованной связи внутри государств, между государствами, а также отдельными лицами, принадлежавшими к различным политическим и религиозным партиям. Так, нередко ученый зашифровывал свои гипотезы, что-

бы не прослыть еретиком и не подвергнуться преследованиям инквизиции.

Научные методы в криптографии впервые появились, по-видимому, в арабских странах. Арабского происхождения и само слов «шифр». О тайнописи и ее значении говорится даже в сказках «Тысячи и одной ночи». Первая книга, специально посвященная описанию нескольких систем шифров, появилась уже в 855 году, она называлась «Книга о большом стремлении человека разгадать загадки древней письменности». В 1412 году издается 14-томная энциклопедия, содержащая систематический обзор всех важнейших областей человеческого знания, — «Шауба аль-Аща». Ее автор Шехаб аль-Кашканди. В этой энциклопедии есть раздел о криптографии под заголовком «Относительно сокрытия в буквах тайных сообщений», в котором приводятся семь способов шифрования. Здесь же дается перечень букв в порядке частоты их употребления в арабском языке на основе изучения текста Корана, а также приводятся примеры раскрытия шифров методом частотного анализа встречаемости букв.

Важность криптографии подчеркивается в книге знаменитого флорентийца Николо Макиавелли «О военном искусстве». В XIV веке появляется книга о системах тайнописи, автором которой был сотрудник тайной канцелярии папской курии Чикко Симонетти. В этой книге приводятся замены, в которых гласным буквам соответствует несколько значковых выражений, дается описание значкового шифра, в котором гласные получают несколько значений. Эти описания свидетельствуют о том, что папская курия была осведомлена о дешифровании шифров простой замены.

В XV веке появляется книга «Трактат о шифрах», написанная Габриелем де Левиндой — секретарем папы Клементия XII, из которой явствует, что криптография в те годы стояла уже на довольно высокой

ступени развития. Автор приводит целый ряд шифров, в том числе дает описание шифра пропорциональной замены, в котором каждой букве ставится в соответствие несколько числовых или значковых значений пропорционально частоте встречаемости буквы в открытом тексте. Кроме того, предлагается заменить имена, названия должностей, географические наименования условными группами. В этот же период в Милане был предложен шифр, получивший название «миланский ключ», который представляет собой значковый шифр пропорциональной замены, где гласным буквам ставилось в соответствие пять знаков шифруемого алфавита.

В 1466 году известный философ, живописец, архитектор Леон Альберти также представил в папскую канцелярию трактат о шифрах. Этот труд явился этапным в развитии криптографической мысли. В нем дается анализ повторяемости букв и обсуждаются пути предотвращения раскрытия шифров, рассматриваются различные системы шифров, такие как замена букв, их перестановка в словах, расстановка точек под буквами маскировочного текста. Работу свою автор завершает собственным шифром, который он назвал «шифром, достойным королей» и который, по его мнению, был недешифруем. Это шифровальный диск, положивший начало целой серии так называемых многоалфавитных шифров.

Шифровальный диск представляет собой пару полудисков: внешний — неподвижный, на котором выписаны буквы алфавита в их обычной последовательности, и внутренний — подвижный, где буквы даны с некоторой перестановкой. Шифровать следовало так: буквам открытого текста на внешнем диске ставились в соответствие буквы шифрованного текста на внутреннем диске. После шифрования нескольких слов внутренний диск сдвигался на один шаг. Секретность переписки обеспечивалась ключом — начальным угловым положением внутреннего диска.

Поскольку с каждым новым угловым положением внутреннего диска вступает в действие новый шифралфавит, то это и есть многоалфавитный шифр.

Позднее Альберти изобрел код с перешифровкой. Для этого на внешний диск он вписал цифры от 1 до 4, составил из этих цифр упорядоченные наборы по две, три и четыре цифры и использовал их в качестве кодовых групп небольшого кода на 336 величин. Числа шифровались на диске как буквы открытого текста. Изобретение Альберти намного опередило свое время. Главные державы мира стали применять код с перешифровкой лишь спустя четыре столетия.

В XV веке в Европе широкое распространение получили так называемые диаграмматические шифры. Зашифрованные ими послания легко скрывались в картинах, картах и т. п. С помощью таких шифров текст изображался в виде геометрических фигур (точек, прямых и изогнутых линий, треугольников и т. д.). К этим шифрам примыкают шифры простой замены, в которых буквы алфавита расположены в различных геометрических фигурах.

В то время как в Италии, Франции, Испании криптография быстро развивалась, во многих государствах Европы она не продвигалась дальше «шифра Цезаря». Связано это прежде всего со строжайшей тайной, которая всегда сопровождала криптографическую деятельность.

В XV веке в некоторых государствах Европы вместо шифров стали использоваться так называемые жаргонные коды. В основном их применяли послы, постоянно проживавшие, согласно введенным законам, в том или ином государстве. К применению жаргонных кодов их вынуждало то отношение, которое проявлялось в то время к шифрованной переписке: одно обнаружение написанных тайнописью посланий могло привести к дипломатическому скандалу. Поэтому

в случае необходимости послать секретное сообщение посол составлял письмо совершенно невинного содержания, а его секретарь писал второе письмо на имя какого-нибудь «друга» или «знакомого», в котором все продиктованные послом секретные сведения передавались в аллегорической форме. Так, например, французский посол в России с помощью своего секретаря-мехоторговца послал в Париж письмо такого содержания: «Волчий мех сейчас очень моден в Петербурге, Я слышал, что герр Еммерих из Германии послал заказ на 30 тыс. кротовых шкурок, хотя его денежное положение неважное. Интересно, где он возьмет деньги на их оплату». Согласно имевшемуся и у этого посла, и в Париже жаргонному коду, «волком» здесь называется австрийский посол, «кротовым мехом» — английские войска и т. д. Письмо в Париже было расшифровано так: «Россия и Австрия собираются заключить союз; ходят слухи, что прусский король попросил у Англии 30 тыс. солдат, но что он испытывает трудности в связи с их получением, так как у него нет денег».

Жаргонные коды широко применялись в Англии, Голландии, Дании, некоторых других государствах Северной Европы. Свое развитие они получили от воровского жаргона, распространившегося в то время в Англии, и от разговорной формы иносказания — эвфемизма, принятого в высшем свете. В XV веке в Англии был даже учрежден специальный орган, занимавшийся изучением воровского жаргона и составлением специальных жаргонных кодов для дипломатических и торговых представителей.

В это же время в качестве одного из способов передачи секретных сообщений начинает использоваться трафарет-решетка, впервые примененная неким Флейснером: в некоторые места письма невинного содержания, определенные вырезами в особом трафарете-решетке, вписывались слова секретного сообщения.

В XVI столетии наблюдается быстрое развитие шифровального дела. К этому времени почти все государства Европы начали применять сложные системы шифров, широкое распространение получили шифры пропорциональной замены.

Быстро развивалось в этот период и искусство дешифрования. Дешифровальные службы тогда еще созданы не были, и дешифрованием занимались отдельные люди, в некоторых случаях это были видные ученые и политические деятели. Помимо работы дешифровальщиков, вызванной необходимостью читать дипломатическую и другую секретную переписку, практика дешифрования становилась для некоторых образованных людей своего рода развлечением и забавой.

В 1518 году в развитии криптографии был сделан еще один шаг вперед. Этому способствовало появление в Германии первой печатной книги, посвященной тайнописи, которая носила название «Полиграфия». Ее автором был Иоганнес Третемий — аббат, настоятель монастыря в Вюрцбурге, автор множества теологических сочинений. В этой книге дается описание шифра, названного автором «Аве Мария». В шифре каждой букве соответствует слово духовного содержания, например букве «А» — слово «Бог». Тогда любому открытому тексту соответствует текст духовного содержания. Кроме того, Третемий в своей книге развил идею многоалфавитного шифра, введя квадратную таблицу, состоявшую из алфавита, сдвинутого на один шаг, алфавита, сдвинутого на два шага, и т. д.

Следующая ступень в развитии криптографии связана с именем Джованни Беллазо, который в своей небольшой книге «Шифр сеньора Беллазо», вышедшей в Италии в 1553 году, предложил использовать для многоалфавитного шифра легко запоминающийся ключ. Автор назвал его «паролем». Пароль выписывается над открытым текстом, буква, стоящая над буквой открытого текста, означает номер алфавита

(т. е. номер строки в таблице замены), по которому осуществляется замена. При этом автор отмечал, что разных корреспондентов можно снабжать различными паролями, и если пароль оказывался украденным, то его можно было заменить.

В начале XVI века криптограф папы римского Матео Ардженти изобрел буквенный код — самый сложный шифр замены, в котором буквы, слоги, слова и целые фразы заменялись группами букв. Необходимым количеством словарных величин в коде в то время считалось 1200. Числами словарные величины в коде стали обозначаться с 1586 года. Это изобретение приписывается Триентеру Копцилю.

В 1563 году итальянский естествоиспытатель, член научного общества, в которое входил Галилей, автор многих научных трудов и литературных произведений Джованни де ла По́рта опубликовал книгу «О тайной переписке». В ней имеются разделы о древних шифрах, о шифрах современных, дается их анализ, описываются лингвистические особенности в раскрытии шифров.

Среди «современных» систем в книге был впервые представлен биграммный шифр, в котором две буквы обозначены единым символом, де ла Порта привел классификацию шифров (шифры, связанные с изменением порядка, формы, значения букв), описал различные системы шифров, привел примеры раскрытия шифров простой замены, если в шифрованном тексте нет разделения на слова. Кроме того, рассуждая о дешифровании, де ла Порта привел списки слов, наиболее вероятных для текстов любовного содержания и для военных текстов.

В своей книге де ла Порта предложил новую систему шифра периодической лозунговой замены. В применении к русскому языку он выглядел так:

1. А а б в г д е ж з и й к л м н о п
   Б р с т у ф х ц ч ш щ ъ ы ь э ю я

2. В а б в г д е ж з и й к л м н о п
   Г с т у ф х ц ч ш щ ъ ы ь э ю я р

3. Д а б в г д е ж з и й к л м н о п
   Е т у ф х ц ч ш щ ъ ы ь э ю я р с

4. Ж а б в г д е ж з и й к л м н о п
   З у ф х ц ч ш щ ъ ы ь э ю я р с т

5. И а б в г д е ж з и й к л м н о п
   Й ф х ц ч ш щ ъ ы ь э ю я р с т у

6. К а б в г д е ж з и й к л м н о п
   Л х ц ч ш щ ъ ы ь э ю я р с т у ф

7. М а б в г д е ж з и й к л м н о п
   Н ц ч ш щ ё ы ъ э ю я р с т у ф х

8. О а б в г д е ж з и й к л м н о п
   П ч ш щ ъ ы ь э ю я р с т у ф х ц

9. Р а б в г д е ж з и й к л м н о п
   С ш щ ъ ы ь э ю я р с т у ф х ц ч

10. Т а б в г д е ж з и й к л м н о п
    У щ ъ ы ь э ю я р с т у ф х ц ч ш

11. Ф а б в г д е ж з и й к л м н о п
    Х ъ ы ь э ю я р с т у ф х ц ч ш щ

12. Ц а б в г д е ж з и й к л м н о п
    Ч ы ь э ю я р с т у ф х ц ч ш щ ъ

13. Ш а б в г д е ж з и й к л м н о п
    Щ ь э ю я р с т у ф х ц ч ш щ ъ ы

14. Ъ а б в г д е ж з и й к л м н о п
    Ы э ю я р с т у ф х ц ч ш щ ъ ы ь

15. Ь а б в г д е ж з и й к л м н о п
    Э ю я р с т у ф х ц ч ш щ ъ ы ь э

16. Ю а б в г д е ж з и й к л м н о п
    Я я р с т у ф х ц ч ш щ ъ ы ь э ю

Шифрование производится при помощи лозунга. Лозунг пишется над открытым текстом, по первой букве лозунга отыскивается алфавит (большие буквы в начале строк), в верхнем или нижнем полуал-

фавите отыскивается первая буква открытого текста и заменяется соответствующей ей буквой из верхней или нижней строки.

Пример:
Лозунг: ф и л о с о ф и я ф и л о с о ф и я ф и л...
Открытый текст: п е р и о д и ч е с к и й ш и ф р д е л я...

Шифртекст: щ щ л я ц ы т г ф з ю з р а я к м у я я в...

Несмотря на то, что за этот шифр де ла Порту позднее стали называть отцом современной криптографии, в то время его система не была признана итальянскими криптографами и не нашла широкого применения. Причиной этого были сложность шифрования и необходимость постоянно иметь при себе всю таблицу шифра.

Живший в одно время с де ла Портой французский посол в Риме де Виженер многому научился от итальянцев в деле шифрования и дешифрования открытых писем.

Система шифра де ла Порты поразила его оригинальностью, но не простотой использования. Наблюдая в Риме замечательное искусство дешифрования, демонстрируемое главным настоятелем собора св. Петра, который в течение нескольких часов раскрыл турецкие шифры, несмотря на незнание турецкого языка, де Виженер стал сам изобретать шифры, не уступавшие по стойкости шифру де ла Порты. Написав большой труд о шифрах, де Виженер изложил свою систему шифра периодической лозунговой замены, которая явилась первым великим открытием в криптографии со времен Юлия Цезаря. Квадратный «шифр Виженера» на протяжении почти 400 лет не был дешифрован.

«Шифр Виженера», переложенный на современный русский алфавит, выглядит так:

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
А	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
Б	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а
В	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б
Г	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в
Д	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г
Е	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д
Ж	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е
З	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж
И	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з
Й	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и
К	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й
Л	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
М	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л
Н	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м
О	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
П	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о
Р	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
С	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
Т	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
У	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т
Ф	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
Х	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
Ц	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
Ч	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
Ш	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
Щ	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
Ъ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
Ы	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
Ь	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы
Э	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь
Ю	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
Я	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю

Шифрование с помощью «таблицы Виженера» производится следующим образом: над шифруемым текстом, в котором все цифры и знаки препинания пишутся прописью, надписывается какое-то условное слово-лозунг. Пользуясь горизонтальным и вертикальным алфавитами таблицы как системой координат, находят первый знак лозунга в верхнем алфавите, а первый знак шифруемого текста — в вертикальном алфавите (или наоборот), и соответствующую этим

координатам букву выписывают как первую букву шифрованного текста.

«Шифр Виженера» не нашел широкого распространения в дипломатической переписке, но зато активно использовался как военный шифр.

Мы уже говорили о том, что искусство шифрования развивалось быстрее, чем искусство дешифрования. Но второе всегда подталкивало первое к прогрессу. Шифровальная и дешифровальная службы всегда вели между собой борьбу. Криптографы-шифровальщики старались как можно лучше скрыть открытый текст с помощью шифра, а криптографы-дешифровальщики, базируясь на знании множества систем шифров, на опыте их раскрытия, стремились отыскать новые и усовершенствовать старые методы дешифрования. Мы назвали несколько имен криптографов, которым удалось либо дешифровать ту или иную систему шифра, либо изложить методы дешифрования на бумаге, оставив таким образом свой след в истории криптографии. Однако эти люди работали чаще всего по своему собственному призванию и своими успехами были обязаны самим себе.

Организация первых дешифровальных органов в Европе относится к середине XVI столетия, когда разведка и контрразведка в большинстве стран начинают оформляться в специальные службы, бюро, отделы.

Оливер Кромвель, основатель разведывательной службы в Англии (1530 г.), утверждал, что «управлять — значит предвидеть», а предвидеть можно только тогда, когда глава государства своевременно и хорошо информирован. Исходя из этих посылок, в Англии была создана разведывательная служба «Интеллидженс сервис», в которой на правах отделения — так называемого «черного кабинета» — была сформирована специальная дешифровальная служба.

В бытность на английском престоле дочери Генриха XVIII королевы Елизаветы (1558—1603) английская разведка и особенно дешифровальная служба сыграли огромную роль в разоблачении заговора претендовавшей на английский престол Марии Шотландской и ее приверженцев. В то время начальником «Интеллидженс сервис» был Фрэнсис Волсингхэм, а его правой рукой — начальник «черного кабинета» Кристофор Марло. Заговорщики вели переписку с помощью шифра пропорциональной замены, усложненного «пустышками». Кристофору Марло и работавшим с ним дешифровальщикам удалось прочесть перехваченные письма и представить их как обвинительные документы.

В начале XVII века аналогичное разведывательное бюро было создано во Франции. Его организатором стал кардинал де Ришелье, о котором справедливо заметили: он сделал слишком много хорошего, чтобы говорить о нем плохо, и слишком много плохого, чтобы говорить о нем хорошо.

В 1626 году Ришелье создал французское дешифровальное отделение при следующих обстоятельствах. Принц Конде, командовавший армией Людовика XIII, осаждал город Реанмольд, где засели гугеноты. Королевская армия была деморализована бесплодными попытками овладеть крепостью. Принц хотел уже снять осаду, когда случайно у одного из пленных было найдено письмо, написанное на условном языке. Это была длинная и неумело сочиненная поэма. Ни одному из офицеров не удалось понять ее тайный смысл. Тогда был приглашен писец Антуан Россиньоль. После нескольких часов исследования ему удалось прочитать поэму. Оказалось, что это шифрованное письмо, в котором осажденные уведомляли своих сообщников о том, что остались без боеприпасов. Вернув осажденным шифрованное письмо, Конде добился капитуляции города Реанмольда.

Кардинал Ришелье осыпал Антуана Россиньоля почестями и назначил начальником «счетной части» — дешифровального отделения. Россиньоль до глубокой старости занимал этот пост. Его работа сводилась в основном к дешифрованию, которое он производил столь блестяще, что во Франции до сих пор способ, при помощи которого открывается ключ шифра, называется «россиньоль».

Этому великому криптографу принадлежит доктрина, согласно которой стойкость военно-полевого шифра должна быть такой, чтобы обеспечить секретность шифрдонесения до получения его армейским подразделением и выполнения приказа. Дипломатический же шифр должен быть таким, чтобы раскрытие его заняло несколько десятков, а может быть, и сотен лет, так как в дипломатии зашифрованный документ часто должен оставаться секретным еще очень продолжительное время после его зашифрования.

Антуан Россиньоль знал, конечно, шифры системы де ла Порты, Виженера, Жерома Кардано и др. Когда ему поручили составить шифр для дипломатической переписки, Россиньоль изобрел такой шифр, который не был дешифрован на протяжении двух столетий и получил название «великого шифра».

В Германии начальником первого дешифровального отделения — «криптографической лаборатории» был граф Гронсфельд, создавший один из вариантов усовершенствования «шифра Виженера». Вместо буквенного лозунга Гронсфельд взял цифровой, состоявший из нескольких цифр, порядок которых было легко запомнить. Вместо большого квадрата использовался только один алфавит с правильным расположением букв. При шифровании знаки открытого текста выписывались под буквами алфавита, цифровой лозунг воспроизводился в памяти и не выписывался. Буква шифруемого текста заменялась буквой алфавита, отстоявшей от нее вправо на количество букв, равное соответствующей цифре лозунга.

Таким образом в конце XVI—начале XVII века в главных европейских государствах появились службы перлюстрации — «черные кабинеты» — с дешифровальными отделениями. Специалисты всегда считали дешифрование и наукой, и искусством. Как всякая наука, оно базируется на определенных законах, а как искусство опирается на интуицию дешифровальщика. Дешифрование всегда было весьма трудным делом, которое требовало хорошего знания иностранного языка, большой практики, громадного терпения, упорства, наблюдательности и, наконец, интуиции.

Глава первая

ДРЕВНЕРУССКАЯ ТАЙНОПИСЬ

Письменные традиции

Традиции русского тайнописания уходят своими корнями в средние века. Подобно другим древним и всем славянским письменностям, уже древнерусская письменность обладала этим особым применением. Термин «тайнопись» получил распространение в славянской научной литературе в XIX в. В более раннее время одного общего названия для тайнописи, по-видимому, не существовало. Отдельные же ее виды имели свои особые названия. Так, известна «цифровая» тайнопись, носившая название «хвиоть» или «фиоть» в XVI—XVII вв. Есть название «еффата» применительно к цифровой же загадке — акростиху в южно-славянской рукописи XVII в. Тайнопись в широком смысле может считаться довольно распространенным явлением в древнерусских рукописных памятниках в XIV в., хотя известны случаи и более раннего ее употребления. Обычное место тайных надписей или записей в рукописях — в виде послесловий или приписок на особых местах — в основном в начале или конце рукописи, часто на внутренней стороне переплета. Обычно за тайнописью скрывается имя писца, имя владельца рукописи, какое-либо замечание и т. п.

Уже в середине XIX в. многие отечественные ученые-филологи начали проявлять в той или иной

степени интерес к вопросам тайнописания в южнославянских и русских рукописях. Среди них мы встречаем имена таких извеетных языковедов, как А. Х. Востоков, И. И. Срезневский, А. И. Соболевский, Е. Ф. Карский, В. Н. Щепкин. Все, ставшие классическими, труды названных ученых, посвященные палеографии*, содержат разделы о тайнописании. Наиболее глубоко исследовал эту проблему академик М. Н. Сперанский. В своем фундаментальном труде «Тайнопись в юго-славянских и русских памятниках письма» [1], созданном на базе скрупулезного изучения многочисленных рукописных памятников, находившихся не только в России, но и в многочисленных европейских книгохранилищах, автор детально описал ряд систем славянской и русской тайнописи.

Рассмотрим системы тайнописи, которые употребляли писцы в древнерусских письменных памятниках, подробнее, опираясь, в основном, на выводы М. Н. Сперанского и используя его терминологию.

Виды древнерусской тайнописи

Наиболее ранней из известных по древнерусским памятникам письменности систем тайнописи является система «иных письмен». В этом виде тайнописи буквы кирилловского алфавита заменяются буквами других алфавитов: глаголицы, греческого, латинского, пермской азбуки.

В употреблении глаголицы в качестве тайнописи хронологически следует различать два периода: древнейший (XI—XIII вв.), когда глаголицей в кириллическом тексте пишут только отдельные буквы и слова, и позднейший (XV—XVI вв.), когда глаголицей пишутся целые фразы. Однако относительно первого периода возникают некоторые сомнения в том, что глаголица использовалась именно как тайнопись.

* Палеография — историко-филологическая дисциплина, изучающая памятники древней письменности с целью установления места и времени их издания.

Письменные источники повествуют о том, что «устроенное» славянское письмо создали около 863 г. просветители братья Кирилл-Константин и Мефодий, греки, родом из Болгарии. Предназначали они новую письменность для принявшего христианство славянского княжества Моравии.

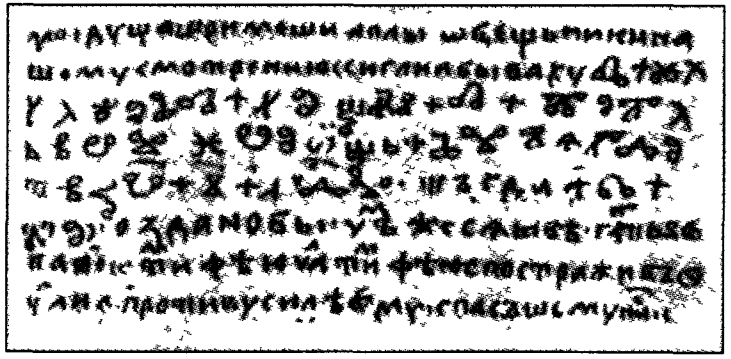
В самой Болгарии (а как известно, Первое Болгарское царство, где официальным был греческий язык, но основную массу населения составляли славяне, возникло в Подунавье в VII в.) христианства еще не было, оно там было введено около 865 г. Официальный греческий язык стал после этого и церковным. На нем велась церковная служба по греческим книгам.

После смерти Мефодия (885 г.) славянское богослужение в Моравии было запрещено (Кирилл-Константин умер еще раньше, в 869 г.). Последователи славянских первоучителей нашли приют в Болгарии. Не прошло и десяти лет, как в 893—894 гг. в Первом Болгарском царстве произошло событие большого политического и культурного значения: в качестве официального и церковного языка был объявлен славянский. Использовавшаяся в богослужении греческая литература заменялась славянской.

Подлинники славянских книг от указанного времени не сохранились. Правда, сохранились позднейшие копии книг, которые, по мнению ученых, были написаны на славянском языке в конце IX — начале X в. Вокруг них ведутся споры о виде славянского письма, каким они были первоначально написаны, — глаголице или кириллице. Например, по мнению болгарского ученого академика Ив. Гошева, в конце IX — начале X в. еще не существовало сложившегося письма типа кириллицы. Он считает, что

применительно к этому времени можно говорить лишь о «первокириллице», состоявшей из 24 греческих букв, дополненных 14 глаголическими для передачи славянских звуков. Впоследствии эти глаголические буквы приобрели «кириллический» облик. По мнению Ив. Гошева, процесс складывания кириллицы еще полностью не завершился в X в., негреческие буквы сохраняли известную графическую связь со своими глаголическими прообразами.

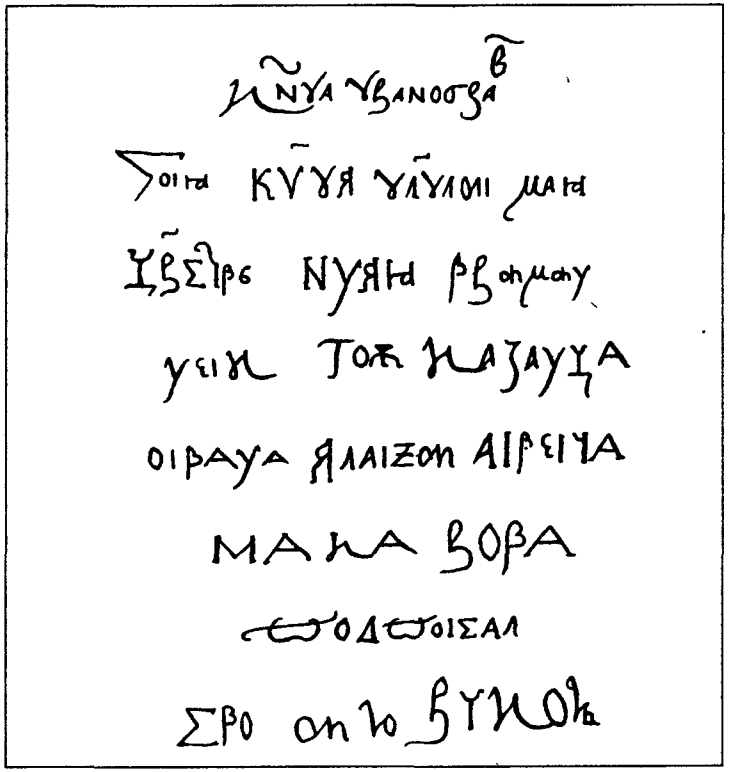
Глаголицу древнерусские писцы хорошо знали, они ее умели читать и копировали в своих текстах, чему есть множество примеров. Поэтому в древнейший период глаголица не была на Руси чем-то особенным, и употребление ее в кириллических памятниках, вероятно, лишь отражает стремление писца обратить особое внимание на какое-то место в тексте. Но к концу XV в. глаголица была уже на русской почве основательно забыта и в рукописях использовалась исключительно как тайнопись. Возможно, этот новый интерес к глаголице объясняется вторым южно-славянским влиянием. Мы приводим пример тайнописи глаголицей в сборнике № 95 Собраний Большой Патриаршей библиотеки, на листе 2 в Слове, приписанном Иоанну Златоусту.



Чтение этого места на кириллице таково: «Си глаголана бываху даже не создано(=ъ) бысть адамо(=ъ)

перьвиА(=е) вообразися плоть христова и апостоли тогда адамо(=ъ) создано(=ъ) бысть».

К XV—XVI вв. относится употребление в русских рукописях греческого алфавита в целях тайнописи. При этом все писцы обнаруживают знание произношения греческих букв и буквосочетаний и даже иногда пытаются изобразить греческими буквами русские звуки, отсутствующие в греческом языке (ч, ж, ц, ю, я). В этом случае они или ставят греческую букву, приблизительно выражающую русский звук, или сочиняют какое-то особое начертание. Примером для второго случая может являться запись на Царственном Летописце из собрания Государственного исторического музея (2291), где внизу по л. 1—25 читается:



Интересно, что раскрытие этой тайнописи дано в самой рукописи на верхних полях страниц параллельно самой тайнописи.

"Сиа книга глглемаю цр҃ственнаю временник тои казанца Ивана Але҆еевича Макарова, подписал своею роукою, книга гранографа ".

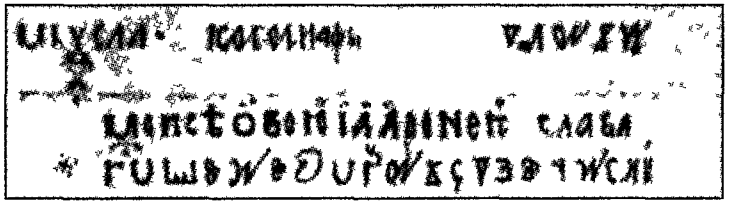
Употребление греческой тайнописи связывают с определенной модой, которая прошла к концу XVI в. Появление же этого способа тайнописи было обусловлено, с одной стороны, вторым южно-славянским влиянием, несшим кое-какие навыки и греческого письма, более близкого югу славянства, чем Руси, а с другой — оживлением начавшихся с конца XIV в. сношений Московской Руси с греками.

Употребление латинской азбуки в качестве тайнописи относится к более позднему времени и обусловлено усилившимся западноевропейским влиянием. В распространении этого вида тайнописи, встречающегося в рукописях XVI и XVII вв., вероятно, известную роль играла школа с ее латинским языком преподавания.

Несколько обособленное место среди других алфавитов в применении к тайнописи занимает пермская азбука. Изобретенная, по преданию, просветителем зырян епископом пермским Стефаном, создавшим ее на основах современного кирилловского и греческого алфавитов, азбука эта не привилась на практике и уже в XV в., как малоизвестная, получила значение тайнописи. Но и в этом качестве она не была широко распространена. М. Н. Сперанский по разным источникам составил сводную таблицу пермской азбуки, которую мы и приводим (см илл. на вкладке).

Второй после системы «иных письмен» системой тайнописи, известной по русским рукописным памятникам, является система «измененных знаков», зафиксированная уже в XIV в. Выделяют две ее разновидности: а) систему знаков, измененных «путем прибавок» к обычным начертаниям, б) построенную на принципе, сходном с греческой тахиграфией, когда вместо буквы пишется лишь часть ее. Первую разновидность такой тайнописи М. Н. Сперанский открыл в замечательной, по его выражению, Смоленской Псалтыри 1395 г. По свидетельству ученого, эта Псалтырь Онежского Крестного монастыря хранилась в свое время в Архангельском местном отделении Церковно-Археологического комитета. Ее писец, смолянин инок Лука, прекрасно владевший искусством письма, любил, видимо, и тайнопись. В этой рукописи он применил три вида тайнописи: одна — измененных начертаний, вторая — цифирь счетная, третья — система вязи (о двух последних мы скажем ниже).

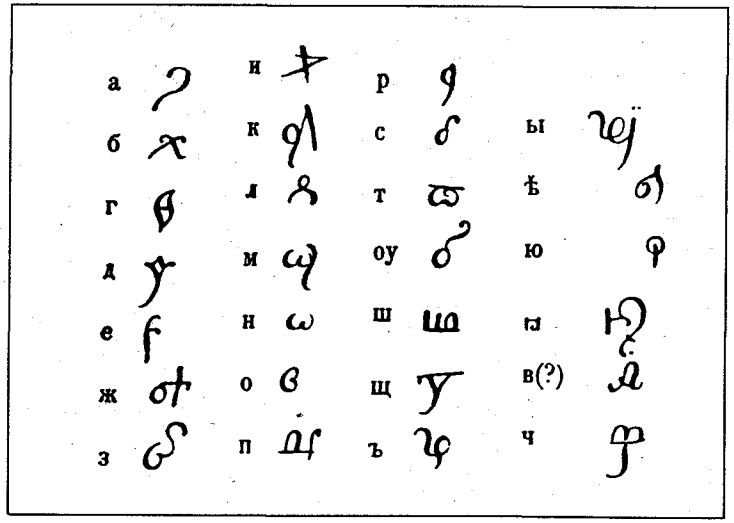
Присматриваясь к манере изменения обычных письменных знаков, можно выделить такие приемы у писца: одни начертания он переворачивает вниз головой или в обратную сторону, прибавляя к ним черточки, другие он деформирует, затушевывая таким образом обычный облик букв или избирая для букв совершенно особые начертания. Мы приводим тайнопись, содержащуюся на л. 72 об. этой рукописи, которая расшифровывается так. «Господи, помози рабу своему Луце».



Ярко выраженный принцип изменения начертаний обычных букв, притом с примесью греческого алфавита, представляет запись в Евангелии 1527 г., писанном под Вязьмой (рукопись ГПБ им. М. Е. Салтыкова-Щедрина, Q. 1. № 21). Читается она (в переводе на современный язык) так: «Владыко-человеколюбец, слава тебе, что сподобил меня, раба своего Сидора, написать сию книгу...»

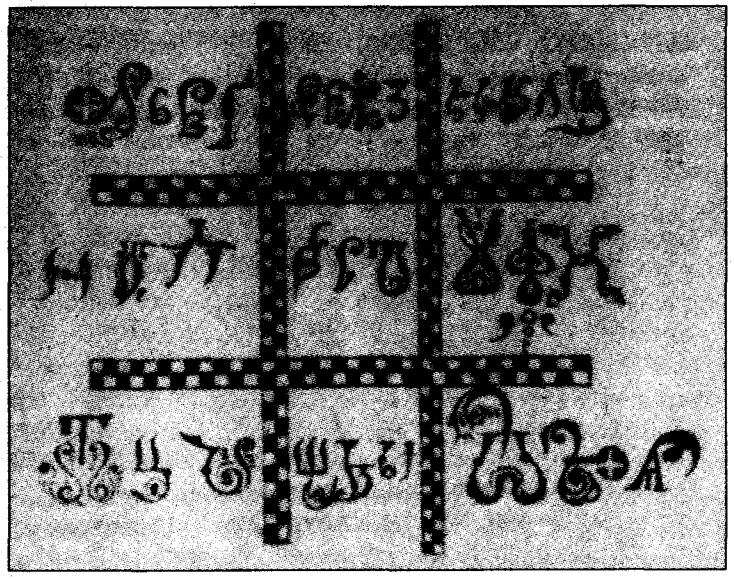
Использовали писцы древних рукописей и систему условных алфавитов. Как правило, в их основе лежали уже известные: греческий, глаголический, кирилловский, в которые привносились какие-то изменения или дополнения. Однако встречаются в рукописях и оригинальные условные алфавиты, построенные либо по какому-то определенному принципу, либо совершенно произвольных начертаний.

Для первой группы условных алфавитов характерен пример из рукописного собрания Н. П. Никифорова, № 3801 (ГИМ), где тайнопись читается так: «А сию книгоу писа многогрѣшный рабъ бжеи в(?)орошня лѣта 7098 (1590) бже щедрыи».



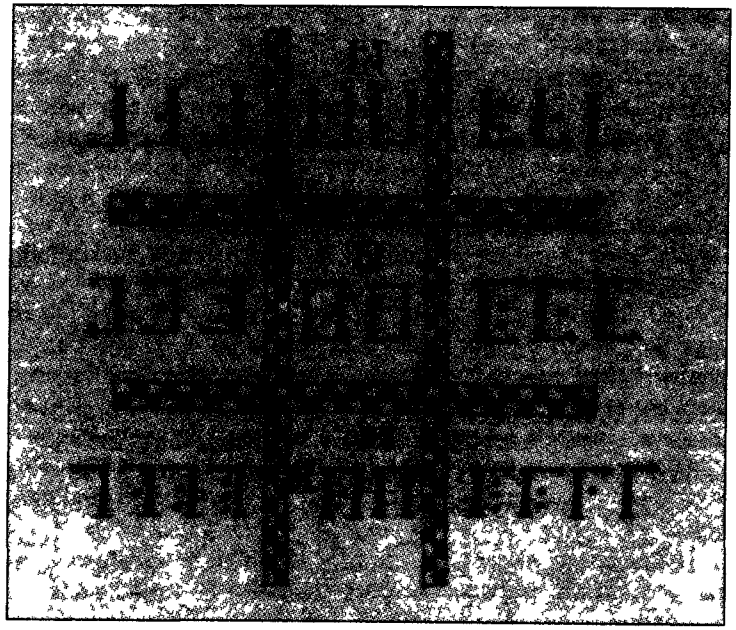
М. Н. Сперанский извлек из этой записи условный алфавит, использованный писцом. Для него характерны такие принципы затемнения обычных начертаний: деформация (е, л, п, ш и др.), переворачивание (р), специально придуманные знаки, а кроме того использован принцип замены: для некоторых букв (г, н) взято начертание, заимствованное из греческого алфавита (см. рис. на с. 30).

Образцом алфавита, придуманного специально для тайнописи, притом по особому принципу, может служить ключ к тайнописи, изображенный на отдельном листе второй половины XVII в. (Собрание Большой Патриаршей библиотеки, № 93). Он весьма прост, как это видно из снимка самой тайнописи и ключа к ней.



Здесь тайнопись состоит в замене обычных букв угольниками и четырехугольниками, заимствованными из решетки, составленной из двух параллельных линий, пересеченных двумя такими же линиями под

прямым углом. В полученных клетках помещено по четыре и по три буквы в порядке азбуки: в тайнописи буквы заменяются, при этом первая — простым угольником, а следующие — тем же угольником с одной, двумя или тремя точками, смотря по месту буквы в нем. Так как при таком размещении букв в клетках вся азбука не могла уместиться, то в этой тайнописи не оказывается знаков для таких букв кириллицы: ш, ь и др.



Следующая система тайнописи, которая использовалась писцами в русских рукописях, — это «система замен». Выделяют два вида такой тайнописи: «простую литорею» (т. е. простое риторское письмо) и «мудрую литорею», а также как вариант этой последней — тайнопись «в квадратах».

«Простая литорея», особенно часто встречаемая, весьма не сложна. Она состоит в том, что каждая из десяти по порядку азбуки согласных, поставленных

в одном ряду, при письме литореей заменяется соответствующей ей буквой во втором таком же ряду, состоящем из остальных десяти согласных, идущих в обратном (справа налево) порядке и обратно; гласные и бывшие редуцированные ъ, ь остаются на своих местах, греческие буквы, как известно, также входившие в состав кириллицы, исключены и заменяются созвучными. Ключ к «простой литорее» таков:

б	в	г	д	ж	з	к	л	м	н
щ	ш	ч	ц	х	ф	т	с	р	п

Старейший образец этого вида тайнописи представлен в известном Шенкурском Прологе 1229 г., принадлежавшем в свое время профессору Московского университета Баузе и сгоревшем в Москве во время пожара 1812 г. Тайнописная запись, имевшаяся в этом Прологе, приводилась П. И. Кеппеном по списку К. Ф. Калайдовича, державшего в руках эту рукопись в таком виде: «мацъ щыл томащсь нменсышви нугипу ромълтую като хе и нилед топгашви тъпичу лию. аринъ.», что значит: «рад быс корабль преплывши пучину морьскую тако же и писець кончавши кънигу сию. аминъ». Однако вызывает сомнение тот факт, что эта запись современна рукописи. Дело в том, что по-настоящему распространен этот вид тайнописи был в конце XIV—XV вв. и поэтому весьма вероятно, что приписка тайнописью была сделана в древней рукописи позднее. Мода же на этот вид тайнописи не прекращалась до XVIII в. включительно.

Для «мудрой литореи», где одни буквы кириллической азбуки, включая гласные, также заменялись другими из той же азбуки, в рукописях существует множество примеров. К этому же виду тайнописи относится использовавшаяся в XVI—XVII вв. тайнопись «в квадратах», где таблицы замены букв выписывались в виде квадратов.

Цифровая система тайнописи или, как ее еще называют, «счетная» или «цифирная», основанная на

употреблении букв в качестве цифр и на различных практических действиях с ними, является весьма распространенной, и притом с довольно раннего времени. Однако, прежде чем мы перейдем к описанию этой системы тайнописи, сделаем небольшой экскурс в историю складывания цифровой системы у восточных славян.

В 1923 г., историк математики М. Н. Марчевский писал: «У нас в России до введения христианства цифр не было никаких. Только знакомство с греками, сношения с Византией после принятия христианства и перевод священных книг на славянский язык имели своим последствием появление церковно-славянской буквенной нумерации, представляющей подражание греческой системе нумерации в алфавитном порядке». Не касаясь здесь вопроса о знакомстве восточных славян с цифрами в дохристианский период, обратимся к тому, что представляла собой византийская цифровая система. В ее основе лежат знаки греческого 24-буквенного алфавита. Они были дополнены тремя цифровыми знаками 6, 90 и 900. Вместе эти три знака называют эписемами. Младшая эписема в средневековых текстах (византийская шестерка) часто выглядит наподобие латинской буквы «эс» (S), такую же примерно форму имел вариант греческой буквы, которую ставили только в конце слова, — «конечная сигма». Средняя эписема, обозначавшая 90, встречается в различных вариантах, именующихся общим словом «коппа». Старшая эписема (900) также известна в нескольких начертаниях, объединенных названием «сампи».

24 греческие буквы вместе с эписемами образовывали 27-знаковую цифровую систему, которую в литературе часто именуют «алфавитной» или «буквенной». Такое название для средневековья является условным, так как три входящих в нее цифры — эписемы — тогда не являлись буквами.

Византийские цифры делились на три группы по девять знаков в каждой. Одна группа выражала единицы, вторая — десятки, третья — сотни. В этой системе можно было обозначать числа от 1 до 999.

Числа записывались слева от старшего разряда к младшему. Например, число 325 выражалось знаками TKE. Здесь T=300, K=20, E=5. Если нужно было выразить число порядка нескольких тысяч, то перед разрядом сотен располагали соответствующую цифру единиц. Например, число 6325 записывалось STKE. Здесь S — шестерка (младшая эписема). Цифре на месте разряда тысяч обычно придавался элемент в виде наклонной черты — «тысячный знак». В таком случае указанное выше число будет выглядеть как /STKE. Чтобы числовую запись не путать с буквенной, она выделялась в тексте точками с обеих сторон (по две или по три), одной или несколькими горизонтальными линиями сверху.

С конца X — начала XI в. дошло до нашего времени несколько болгарских каменных надписей на славянском языке, выполненных кириллицей. Встречающиеся в этих текстах числа записаны в византийской нумерации. Причем она здесь имеет особенности, которые могли возникнуть на болгарской почве. Это новый вариант младшей эписемы, наподобие скорописного «Г», и инверсия в записи чисел второго десятка $\overrightarrow{\text{аі}}$, $\overrightarrow{\text{бі}}$, ... (по сравнению с типичным византийским порядком: $\overrightarrow{\text{іа}}$, $\overrightarrow{\text{іб}}$, ...).

Восточные славяне еще до X в. имели тесные контакты с Византией и греческими колониями Крыма и Северного Причерноморья. О возможном знакомстве восточных славян с византийской нумерацией в X в. говорят письменные источники. Важнейшими из них являются договоры древнерусских князей с греками. Уже в договоре князя Олега (911 г.) употребляется византийская нумерация.

После принятия Русью христианства произошли существенные перемены в жизни страны. Коренным

образом изменился культурный уклад, обусловленный небывалой до того ролью в духовной жизни Руси церковной литературы на старославянском языке, заимствованном из Болгарии. Древнерусские писцы воспринимали и те изменения, которые внесли в византийскую цифровую систему южные болгары.

Как в дальнейшем развивались цифровые представления на Руси? Древнерусские письменные источники XI—XII вв. показывают, что примерно столетие спустя после своего появления на Руси старославянские цифровые черты (шестерка в форме скорописного «Г» и запись чисел второго десятка типа аї, бї...) постепенно закрепляются в древнерусской практике. Однако и в XII в. на Руси не исчезает младшая эписема византийского начертания и встречается иногда византийский порядок в записи чисел второго десятка. Характерным для периода XII—XIII вв. оказывается начертание средней эписемы типа получервь. В это время стреловидная форма «сампи» (900) уступила место сходной по начертанию кириллической букве «юс малый».

Таким образом, в этот период на Руси существовало цифровое «двуязычие»: на практику применения византийской нумерации в чистом виде накладывались старославянские цифровые отклонения.

О дальнейшей судьбе древнерусской нумерации можно сказать следующее. После татаро-монгольского нашествия около 1240 г., когда нарушились традиционные культурные связи с Византией и южными славянами, древнерусская цифровая система продолжала развиваться в прежнем направлении — замена греческих знаков на сходные кириллические. Так, появившийся в ней в конце XIII в. новый знак «от» (800) заменил сходную по виду «омегу». В конце XIV — начале XV в. на Руси в качестве 900 стал использоваться знак «цы». Вместо 900 «юс малый» стал выражать 1000, правда, он нашел ограниченное применение: «юс малый» в значении 1000 стал применяться только в тайнописи. В XVI в. средняя эписема (90) приобрела облик буквы «че» [2].

Возвращаясь к вопросу цифровой тайнописи, следует сказать, что в древнерусских рукописных памятниках встречаются различные ее виды: простая цифровая система, сложная цифровая система, описательная система, система особенного применения арабских цифр, значковая система, т. е. с использованием различных значков для обозначения цифр-букв. Цифровая тайнопись существовала на Руси уже в самом начале XIV в. Здесь нет необходимости подробно рассматривать все ее виды, поэтому мы остановимся на главных.

Простая цифровая тайнопись состоит в том, что для каждой цифры-буквы, соответствующей желательной в обычном письме букве, дается два или несколько большей частью одинаковых слагаемых. Таким образом, чтобы получить нужную букву, надо произвести сложение, а полученная сумма, изображенная соответствующей цифрой-буквой, и будет искомой буквой. Реже сумма слагается из различных цифр-букв, причем каждая группа цифр-слагаемых отделяется каким-либо знаком или пробелом от соседних. Буквы, не имеющие цифрового значения, остаются неизменными.

Старший образец такой тайнописи находится в псковском Апостоле 1307 г. (Собрание Большой Патриаршей библиотеки, № 722):

"а γ҃лъ.в҃.в҃.нк.кк.дд. вв.ъ рекше.дв҃дъ.органъ.мыслъ.истина..."

Произведя сложение попарно стоящих цифр (2+2=4, 50+20=70, 20+20=40, 4+4=8, 2+2=4), получим: д о м и д, т. е. имя Домид. Такая система тайнописи была популярна на Руси долгое время: с XIV по XVII в. Именно отсюда она проникла на славянский юг. Однако само появление цифровой системы тайнописи у славян следует поставить в зависимость от Византии, где она была известна уже в VII—VIII вв.

Греческим по происхождению является и описательный вид цифровой тайнописи. Примером ее может служить тайнописный текст из рукописного собрания Кирилло-Белозерского монастыря XV в.: «Аще хощеши увъдати имя писавшаго книгу сию, и то ти написую: «Десятерица сугубая (10+10=20) и пятерица четверицею (5×4 = 20, сумма 40) и единъ (1); десятерица дващи (10×2 = 20) и един (1); десятья четыре сугубо и четырежди по пяти (10×2×4 + 4×5 = 100); дващи два съ единемъ (2×2 + 1 = 5); единица четверицею сугубо (1×4×2 = 8); в семъ имени словъ седмерица, три столпы и три души, царь. И всего же числа в семъ имени РОЕ (175)». Отгадка: «Макарей», где сумма букв-цифр действительно 175 и семь букв, из которых три гласные и три согласные и одна (й) полугласная. Использованы здесь количественные числительные и сумма. Последняя часть служит как бы проверкой для всей задачи.

Арабские числа стали использоваться в качестве тайнописи лишь с того времени, как они начали входить в употребление в русской письменности, т. е. со второй половины XVI в. на русском юго-западе и с начала XVII в. на северо-востоке.

В рукописном собрании Большой Московской Синодальной типографии № 199 на л. 8—33 внизу идет такая запись 1641 г. (приводим фрагмент):

3 Ѣ 3 І 7 І 4 9 3 7 4 4=лѣта 7І49 и т.д.

Ключ к записи прост: буквы-цифры от 1 до 9 (а — 0), пишутся просто арабскими цифрами, от 10 до 90 (— ч) — теми же цифрами и обозначаются значком над ними, от 100 и до 900 — та же, с другим значком над ними, тысячи — со значком под цифрой; буквы, цифрового значения не имеющие, пишутся просто.

К прочим системам тайнописи, известным по древнерусским рукописям, принадлежат монокондил (т. е. лигатура), различные приемы образного и фигурного

письма, а также акростих*. На этом последнем виде тайнописи, принципиально отличном от описанных выше, нам хотелось бы остановиться особо. Акростих — типичный для европейской средневековой письменной культуры прием организации поэтического текста — входил в арсенал художественно-изобразительных средств древнерусских авторов уже с конца XI в. В поэзии прошлых веков, начиная с самых ее письменных истоков и вплоть до середины XIX в., акростих занимал настолько большое и важное место, характеризовался таким богатством форм и функций, что его с полным основанием относят к числу важнейших компонентов древнейшей и средневековой поэтики.

Истоки техники акростиха уходят в глубь веков, в старейшие письменные культуры Востока. В псалмах Ветхого завета уже встречается акростих, его фрагменты исследователи находят в эпопеях Гомера. Однако большинство ученых квалифицируют их как спонтанные. Согласно Диогену Лаэртскому (конец II — начало III в.), изобретателем акростиха считается Эпихарм Сиракузский, известный древнегреческий комедиограф, философ и врач, живший около 550—460 гг. до н. э. Диоген сообщал, что уже в самом начале одной из функций акростиха была фиксация в тексте имени автора. Именной акростих размещался чаще всего в начале или в конце произведения.

Своеобразной областью применения акростиха были эпитафии, в которых с помощью этого приема сообщалось имя покойного, иногда имя составителя надписи или поставившего надгробие. Здесь встречается акростих, составленный не только по начальным буквам строк, но и по начальным слогам строк, использовался прием повторения в акростихе слова текста или строфы. В русской традиции акростишная

* Акростих — стихотворение, в котором начальные буквы стихов (строк) образуют слово или фразу (часто имя автора или адресата).

эпитафия отмечена в надписи на надгробии патриарха Никона, причем это именно именной акростих — «Герман писа», принадлежащий, по всей вероятности, поэту-гимнографу XVII в. монаху Герману [3].

Другим излюбленным наполнением акростиха было божественное имя, «nomen sacer». Идущая от античных времен, эта традиция во времена христианства нашла выражение в частом обращении в акростишном тексте к имени Христа, Богородицы, святых апостолов или небесного покровителя автора — одноименного святого или великомученика.

На Русь акростих проник из Византии и получил вначале в соответствии с византийской традицией широкое распространение в русских литургических, гимнографических текстах, а позднее и в оригинальных произведениях. В «Словаре названий молитвословий пъснопъний церковныхъ» дается такое определение акростиха: «Краегранесие, краестрочие, иначе акростих (от акрос — край и стихос — стих, строка. — *Т. С.*), есть начальные буквы в песнопениях, из которых букв составлено одно или многия речения. Так, канон мясопустной недели имеет на греческом языке в начальных буквах троичных и Богородичных тропарей краестрочия, например в каноне св. Дмитрию Царевичу краегранесие: «Хвалю славу Царевича Димитрия» [4].

Современный исследователь древнерусской поэтики А. А. Гогешвили указывает на то обстоятельство, что акростих с древнейших времен рассматривался не как чисто формальный тайнописный прием, а как «своеобразная эстетическая и даже онтологическая категория, квинтэссенция истины и гармонии» [5]. Уже в одном из старейших памятников русской письменности — «Повести временных лет», в той ее части, где под годом 6477 (969) сообщается о смерти княгини Ольги и воздается ей хвала как первой христианке и предтече христианства на Руси, реконструируется акростишное чтение:

1 Си бысть предътекущия крестьяньствеи земли,
2 аки деньница предъ солнцемь
3 и аки зоря предъ свътомъ.
— — — — — — — — — — — —
4 Си бо съяше аки луна в нощи, такои си
в неверныхъ человецехъ светящеся;
5 аки бисеръ в калъ кальни бо беша грехомъ,
6 не омовени крещеньемъ святымъ.
7 Си бо омыся купелью святою,
и съвлечеся греховною одежевъ ветхаго человека
Адама
8 и въ новыи Адамъ облечеся,
9 еже есть Христосъ.
— — — — — — — — —
10 Мы же рцемъ къ неи:
11 радуися, руское познанье къ богу,
12 начатокъ примирению быхомъ.
13 Си первое вниде въ царство небесное отъ Руси,
14 аки началницю сию бо хвалят рустии сынове,
15 ибо по смерти моляще бога за Русь.

В состав Похвалы включается также «строфа», помещенная в «Повести временных лет» под 6463 (955) годом:

16 Си бо от вьзраста блаженая Ольга искаше мудростью все въ светъ семь,
17 налезе бисеръ многоценьныхъ,
18 еже есть Христосъ.
— — — — — — — — —

Реконструкция акростишного чтения в Похвале княгине Ольге такова: «Сиаи сиане сие мрна сиаи сине», т. е.: «Сияй, сиянье сие мирно, сияй, сыне» [6].

Русский акростих, переживший свой расцвет в разнообразных краегранесиях монаха Германа, справщика Савватия, Симеона Полоцкого, Кариона Истомина, Мих. Собакина и многих других стихотворцев XVII — начала XVIII в., был еще весьма распространен и в 20-е годы XX в. в творчестве В. Брюсова, Н. Гумилева, С. Городецкого и других известных поэтов «серебряного века» русской поэзии.

Глава вторая

НАЧАЛО

Дипломатическая тайнопись

Долгое время государственная тайнопись в трудах отечественных ученых, в той или иной степени изучавших ее, именовалась «дипломатической тайнописью». Впервые термин «дипломатическая тайнопись» был введен А. Н. Поповым, который в 1853 г. опубликовал работу «Дипломатическая тайнопись времен царя Алексея Михайловича с дополнением к ней» [1]. Следом за А. Н. Поповым и другие исследователи русской тайнописи стали называть переписку при российском дворе «дипломатическим тайнописанием», а шифры, которыми она велась, «дипломатическими». Следует, однако, отметить, что тайная дипломатическая переписка составляла лишь часть, правда, бóльшую, шифрованной переписки при дворе, которая наряду с дипломатическими, касалась военных вопросов, а также внутригосударственных дел. Но именно в области дипломатии, с присущими ей специфическими чертами и свойствами, в России почти на протяжении двух столетий проходило основное становление криптографии как государственно значимого дела. Политическая борьба, политическая игра — словом, ведение «большой политики» немыслимо без соблюдения государственной тайны.

На развитие способов защиты письменной информации большое влияние оказывает состояние средств связи. В то время была почта. До конца XV в. послания отправлялись со специальным курьером — гонцом. С начала XVI в. стала распространяться так называемая ямская гоньба, однако тайные письма пересылались все равно со специальными гонцами. Для защиты посланий использовались особые печати. Такие печати с надписью «ДЬНЕСЛОВО», что переводится как «скрытое, тайное слово», были у киевских князей Святополка Изяславича, Мстислава Владимировича, Александра Невского и других.

Первый международный акт о перевозке корреспонденции, подписанный Россией, — это соглашение между Москвой и Варшавой 1634 г. По этому акту гонцам обеих сторон разрешалось иметь при себе шестерых провожатых. В 1665 г. была организована международная почтовая связь между Москвой и Ригой, позднее аналогичное соглашение было подписано со Швецией.

И все же ни физическая охрана гонцов, ни специальные печати не могли сохранить тайну письменной информации: почту часто перехватывали в пути, печати ломали, письма читали. Поэтому криптографические методы защиты письменной информации начинают применяться более активно.

Появление в России первых специалистов-тайнописчиков, находящихся на государственной службе, следует отнести к 1549 г., к моменту образования Посольского приказа, осуществлявшего общее руководство внешней политикой страны. Кроме того, Приказ ведал выкупом и обменом пленными, управлял рядом территорий на Юго-Востоке страны и некоторыми категориями служилых людей. Вся эта деятельность с необходимостью требовала осуществления довольно интенсивной шифрованной переписки. На службе в Посольском приказе и находились лица, создававшие шифры или, как их называли тогда, «цифири», «цифры» или «азбуки».

Во времена царствования Ивана IV Грозного (1530—1584) осуществлялись крупные дипломатические и военные акции — покорение Казанского и Астраханского ханств, Ливонская война, установление торговых связей с Англией и некоторыми другими государствами, присоединение Сибири. Все это, естественно, оказало влияние на дальнейшее становление тайнописного дела.

В наказе царя Федора Иоанновича (1557—1598) — сына Ивана Грозного, — данном в 1589 г. послу Николаю Воркачу, ему поручалось «писать письма мудрою азбукою, чтоб оприч Царского величества никто не разумел». В предписываемой ему для письма азбуке каждая буква заменялась своим причудливым знаком.

С конца XVI в. русские посланники за рубежом получают шифры в виде таблиц замены или «на память», — т. е. задание «вытвердить гораздо памятно» дипломатический шифр.

С началом правления Романовых (1613 г.) укрепляются основы феодального строя. В 1619 г. из польского плена возвращается отец царя Михаила Федор, постриженный Борисом Годуновым в монахи под именем Филарета. Еще при Лжедмитрии II он был наречен патриархом, теперь к этому был добавлен титул «великого государя». Больной и малоспособный царь Михаил предоставил отцу управление страной (до 1633 г., а затем боярам). Филарет соединил в своих руках верховную, светскую и духовную власть. Он лично заведовал иностранными делами и сам разрабатывал тайные азбуки. Используемые в это время шифры были, естественно, самого простейшего вида — простые замены и простейшие перестановки. Так, известно, что русский посол в Грузии К. П. Савин в 1597—1598 гг. употреблял шифр перестановки, при котором текст сообщения (мы будем в дальнейшем называть его открытым текстом) разбивался на слоги и осуществлялась перестановка букв в слогах.

При усилении центральной власти в годы правления царя Алексея Михайловича (1629—1676) шифры получают более широкое распространение. Сам царь, человек весьма образованный для своего времени, в своей частной переписке также использовал шифры. Послы и резиденты всегда снабжались шифрами. Известен, например, такой факт. В 1673 г. резидентом в Речь Посполитую был назначен полковник В. М. Тяпкин. По дороге в Вильно его догнал царский гонец и вручил ему «знаки тайнописи и повеление царское пользоваться ими для донесений».

Однако через некоторое время царь Алексей Михайлович заметил, что корреспонденция его резидента из Варшавы сильно запаздывает. Причина выяснилась очень просто. Когда В. М. Тяпкин явился с жалобой к королю Яну Собескому, тот, в свою очередь, упрекнул резидента в том, что он писал «ссорные и затейные письма» к царю. Следовательно, поляки перехватывали и дешифровали послания Тяпкина.

В государственной криптографии получают развитие и некоторые другие способы тайнописи, известные по древним русским рукописям, например, такие, как «мудрая литорея». Этим способом, в частности, зашифрован текст, отлитый на большом колоколе Саввино-Сторожевского монастыря под Звенигородом. Зашифрование текста, по предположению ученых, произвел сам царь Алексей Михайлович. Дешифрован он был филологами М. Ф. Калайдовичем, А. И. Ермолаевым, князем П. П. Лопухиным и ротмистром М. С. Суридиным. А. И. Ермолаев по поводу этого обстоятельства высказался так: «Сия надпись во многих отношениях достойна особенного внимания. Представляя нам любопытный образец русской тайнописи (стеганографии) XVII в., она доказывает, что в России в старину шифры были пригодны не для одних дипломатических переписок или для внесения в книги разных обстоятельств, которые затейливые люди того

времени ухитрялись сделать непонятными для многих из своих современников, долженствовавших быть видимыми народом...»

Первые организаторы и руководители криптографической службы России

И все же первым из российских государей, который предельно ясно осознал важность шифрования депеш и развития шифровального дела для обеспечения безопасности государства, был Петр Великий (1672—1725). Эпоха его правления характеризуется усилением Российского государства, всех его управленческих структур, а также структур исполнительной власти. Петр Великий осуществил ряд важнейших преобразований: организацию мануфактур, строительство горных и оружейных заводов, развитие торговли, включая межгосударственную, создание Сената — высшего органа власти по делам законодательства и государственного управления, создание коллегий. Для удобства управления страной он разделил ее на губернии, организовал строительство флота, крепостей, каналов, возвел новую столицу — Петербург. Он открыл учебные заведения, Академию наук, ввел практику посылки молодых дворян для учебы за границу, приглашение иностранных ученых и специалистов для работы в России. Все эти реформы и преобразования привели к усилению внешнеполитической деятельности государства, развитию экономики и науки в стране, что способствовало становлению и последующему развитию криптографической деятельности России на государственном уровне.

Уже в самом начале XVIII в. Петром Великим была учреждена Походная посольская канцелярия, сосредоточившая в своем ведении важнейшую политическую переписку. Создание ее было вызвано частыми поездками Петра. Походная канцелярия явля-

лась преимущественно личной канцелярией императора: отсюда исходили его важнейшие распоряжения по всем отраслям управления, сюда стекались на его решение дела из всех ведомств. Но главной ее функцией было ведение дипломатических дел, почему и к названию ее прибавлялось слово «посольская».

Первое определенное упоминание в документах о Походной канцелярии относится к 1702 г. В это время царь отправился «в поход» в Архангельск. В поездке его сопровождал и начальник продолжавшего существовать Посольского приказа, первый министр Ф. А. Головин. Несмотря на то, что все государственные дела продолжали проходить через Посольский приказ, а «печатанье государственной печатью грамот» должно было далее находиться под контролем бояр, «которым Москва приказала», наиболее важные дела уже решались в Архангельске у Петра Великого. Туда же, в место пребывания царя и его первого министра, был перенесен и центр управления иностранной частью Приказа. В 1705 г. в Походной канцелярии уже присутствуют: тайный секретарь (П. П. Шафиров), два переводчика, два подьячих малороссийского приказа, «да по вся годы посылаются в Свейский (шведский. — *Т. С.*) поход старый подьячий Василий Степанов и три молодых».

К 1710 г. Походная посольская канцелярия окончательно обосновывается в Петербурге и из временного учреждения обращается в постоянное, причем с 1709 г. ее называют просто Посольской канцелярией. Именно здесь теперь сосредоточивается вся работа по зашифрованию и расшифрованию переписки Петра и его приближенных с различными корреспондентами, а также по созданию шифров и рекомендаций по их использованию.

В период между 1710 и 1718 гг. эта Канцелярия становится главным органом внешних сношений России. Компетенция ее расширяется в ущерб оставшемуся в Москве Посольскому приказу. Растет лич-

ный состав Канцелярии. В 1709 г. граф Г. И. Головкин, заступивший место Ф. А. Головина, назначается государственным канцлером, а П. П. Шафиров — вице-канцлером. Именно эти первые лица государства руководят деятельностью постепенно обретающей опыт криптографической службы. Канцлер и вице-канцлер дают указания о создании новых шифров, замене устаревших, по обеспечению шифрами корреспондентов — дипломатов, военачальников, других государственных деятелей. Непосредственно им докладываются отчеты о создании новых шифров, о добыче шифров иностранных. Руководство криптографической службой со стороны канцлера и вице-канцлера вошло в традицию в России, которая сохранялась почти на протяжении полутора веков.

Имена первых руководителей криптографической службы России мало знакомы современному читателю. Между тем все эти люди были выдающимися государственными деятелями, чьи труды на благо Отечества по достоинству ценили современники. Именно их самоотверженное служение государственным интересам позволило Петру Великому выделить этих своих сподвижников среди прочих и поставить на самый верх государственной иерархической лестницы.

Указом от 18 февраля 1700 г. во главе Посольского приказа и принадлежавших к нему приказов был официально поставлен выдающийся деятель и дипломат раннего периода петровского времени Федор Алексеевич Головин (1650—1706). Он сменил здесь думного дьяка Е. И. Украинцева, который в 1699 г. был отправлен послом в Константинополь на русском корабле, впервые явившемся в водах Босфора. При своем назначении Головин получил звание «начального президента государственной посольской канцелярии». Как генерал-адмирал Головин одновременно управлял флотом, возглавлял оружейную палату, монетный двор, малороссийский приказ. Кроме личного участия в переговорах с иностранными государствами и заключения договоров с ними, Головин руководил деятельностью русских послов за границей, оказывал большое влияние на внешнюю политику России в период Северной войны. Под непосредственным наблюдением Головина работало цифирное отделение.

Знатность рода, образованность, недюжинные способности помогли ему занять высший государственный пост. Ф. А. Головин приобрел известность в 1689 г. заключением Нерчинского договора с Китаем. Под Азовом мы видим его в чине генерала наряду с иностранными сотрудниками царя Лефортом и Гордоном. В 1697 г. Головин был уже одним из ближайших сподвижников Петра I, пользовался его большим доверием и расположением. Впервые отправляясь за границу, царь назначил его вторым после Лефорта полномочным послом со званием «генерала, воинского комиссария и наместника сибирского». После смерти Лефорта Головин получил звание генерал-адмирала, в тот же период при учреждении 10 марта 1699 г. ордена Св. Андрея Первозванного он был пожалован первым его кавалером. 16 ноября 1702 г. первым из русских получил графское Римской империи достоинство. Умер Ф. А. Головин 2 августа 1706 г. на пути в Киев, в Глухове. О смерти его Петр I так извещал Ф. М. Апраксина: «Сей недели господин адмирал и друг наш от сего света отсечен смертью в Глухове; того ради извольте которые приказы (кроме Посольского) он ведал, присмотреть и деньги и прочия вещи запечатать по указу. Сие возвещает печали исполненный Петр».

Преемником Ф. А. Головина стал Гавриил Иванович Головкин (1660—1734). Являясь родственником Петра I по материнской линии, Головкин начал свою службу при дворе с детства. Получив в шестнадцать лет звание постельничего, он носил его до назначения канцлером. Головкин принимал активное учас-

тие в борьбе за власть на стороне Нарышкиных, после падения царевны Софьи (1689 г.) он ведал Казенным двором. В начале Северной войны Головкин находился при царе и исполнял самые важные его поручения, руководил внешней политикой России. 17 мая 1703 г., на следующий день после основания Петербурга, Головкин стал кавалером ордена Св. Андрея Первозванного. В 1706 г. он возглавил Посольский приказ, 1 мая 1707 г. Петр пожаловал его графским достоинством.

По случаю Полтавской победы Петр I указом, подписанным 16 июля 1709 г. в местечке Решетиловке близ Полтавы, назначил графа Г. И. Головкина канцлером. По этому же указу он занял место президента вновь образованной Коллегии иностранных дел. С учреждением коллегий (1718 г.) Головкин был назначен президентом Коллегии иностранных дел.

Граф Головкин смог удержаться у власти при всех переменах, которые последовали за смертью Петра Великого, и сохранил до конца своих дней звание канцлера. С учреждением Верховного тайного совета он был назначен одним из его членов и примкнул к партии А. Д. Меншикова. При вступлении Анны Иоанновны на престол он поддержал ее и тем сохранил свое положение при дворе. С учреждением кабинета он был сделан членом его и сенатором. Умер Г. И. Головкин 20 января 1734 г.

Петр Павлович Шафиров (1669—1739) начал свою службу в 1691 г., сопровождал Петра I в его заграничной поездке и в 1703 г. назначен был «тайным секретарем» при Походной посольской канцелярии, где переводчиком работал его отец. Знания П. П. Шафирова в иностранной политике, постоянная близость к царю помогли ему приобрести то значение, на которое он по рождению не мог рассчитывать. После смерти Ф. А. Головина, 23 сентября 1706 г. П. П. Шафиров был назначен в помощь Г. И. Головкину. Одним указом с Головкиным 16 июля 1709 г. Шафиров

назначается Петром I подканцлером с чином тайного советника. По указу он занял место вице-канцлера вновь образованной Коллегии иностранных дел. 30 мая 1710 г. Шафиров получил баронское достоинство, в 1711 г. он вел переговоры с турками во время Прутского похода, затем в 1712 г. в Константинополе, где был посажен в тюрьму, но по освобождении успешно заключил договор с Турцией 13 июня 1713 г. Возвратившись в Россию, Шафиров сыграл большую роль в восстановлении и расширении Северного союза, участвовал в заключении Амстердамского договора 1717 г. с Францией. Эта плодотворная деятельность Шафирова вскоре была прервана вследствие столкновений его с канцлером Головкиным и обер-прокурором Сената Скорняковым-Писаревым. Взаимные отношения двух министров царя, Головкина и Шафирова, никогда не были дружественными. Возможно, этому способствовала не только сословная неприязнь, но и различие их характеров. Осторожный, сухой и скупой Головкин был полной противоположностью щедрому, часто несдержанному в обращении Шафирову. Даже в наружности они были контрастны: Головкин высок и очень худ, а Шафиров при очень маленьком росте едва мог двигаться от полноты.

Уже в 1712 г. Шафиров, находясь в Турции, обвинял канцлера в недоброжелательном к нему отношении. В 1719 г. отношения обоих настолько обострились, что привели к открытой ссоре. 19 мая 1719 г. на заседании Коллегии канцлер предложил, чтобы по именному указу царя дела слушались, решались и подписывались всеми членами Коллегии. Шафиров возразил на это, что с присутствующими членами подписывать не будет, причем асессора Курбатова назвал креатурой канцлера. Затем он сказал: «Я с ушниками и бездельниками дел не хочу делать», в сердцах встал и вышел вон, но, остановившись в дверях, закричал канцлеру: «Что ты мнишь и ста-

вишь себя высоко? Я и сам такой же». Канцлер ему отвечал: «Как ты моей старости не устыдишься такими словами мне кричать!» Несдержанный характер Шафирова вызвал другое резкое столкновение его с обер-прокурором Сената. Осенью 1722 г. на заседании Сената, когда царь был в Персидском походе, Шафиров назвал Скорнякова-Писарева вором и грозил убить его и графа Головкина. В 1723 г. Шафиров был обвинен в крупных хищениях и злоупотреблениях по службе. Петр I по возвращении в Петербург созвал «вышний суд», который осудил Шафирова на смертную казнь. 15 февраля 1723 г. его возвели на эшафот, однако казнь была заменена ссылкой в Сибирь. Петр освободил своего бывшего подканцлера и от этого наказания, сослав его в Новгород, где он жил под самым строгим надзором. В ссылке Шафиров оставался недолго: Екатерина I вернула его в марте 1725 г. в Москву, милостиво приняла и назначила президентом Коммерц-коллегии, но прежнего влияния он уже не приобрел. Год спустя Шафиров был своим заклятым врагом Меншиковым командирован в Архангельск для надзора за китовым промыслом, но остался в Москве под предлогом болезни. При Анне Иоанновне в августе 1730 г. он был отправлен в Гилян, а в марте 1737 г. назначен полномочным послом на Немировском конгрессе. Умер П. П. Шафиров 1 марта 1739 г.

Корреспонденты шифрованной связи

В условиях напряженной деятельности правительства, вызванной реформами, Северной войной и войной со Швецией, от Посольского приказа, Посольской канцелярии, а затем и Коллегии иностранных дел потребовались «новые орудия действия», которые создавались под руководством Головкина и Шафирова. Важнейшим шагом в этом направлении явилось уста-

новление постоянных русских миссий за границей и западно-европейских в России. Это обстоятельство ясно осозналось уже после первой поездки Петра за границу. В 1701 г. Россия имела шесть постоянных миссий в Западной Европе (в Польше, Голландии, Швеции, Дании, Австрии и Турции). В 1719 г. кроме них были созданы миссии во Франции (барон Шлейниц), в Пруссии (граф А. Г. Головкин), Англии (резидент Ф. Веселовский), Меклебурге (М. Салтыков), Гамбурге (резидент Беттигер), Венеции (агент П. Беклемишев), Курляндии (генерал-комиссар П. М. Бестужев), наконец, в Бухаре (агент Флорио Беневени). Можно сказать, что это были первые корреспонденты первых внешних шифрованных сетей связи России. Все они обязательно имели шифры для переписки с царем и Посольской канцелярией. Кроме упомянутых миссий, постоянных или чрезвычайных, Россия имела за границей еще специальных агентов «для предостережения интересов Его Царского Величества», как указывалось в официальном документе. Это были первые российские консулы, причем все — иностранцы. В 1707 г. мы встречаем только одного такого агента Иоганна фон дер Бурга в Амстердаме. В 1719 г. их было уже несколько: три в Голландии, по одному в Париже, Вене, Антверпене и Люттихе. Со всеми этими лицами организовывалась также тайная шифрованная переписка. Одновременно с увеличением числа русских миссий за границей росло число иностранных миссий в России.

В декабре 1712 г. Петр I сделал первые предварительные распоряжения об учреждении коллегий, и в том числе Коллегии иностранных дел. В 1716 г. в Посольской канцелярии был установлен коллегиальный порядок решения дел. Дело в том, что в начале XVIII в. Посольская канцелярия не имела права рассматривать важнейшие политические дела, поскольку это право принадлежало Сенату. Члены Сената — «господа тайные советники» — обычно на своих за-

седаниях слушали изготовленные в Посольской канцелярии рескрипты русским представителям за границей. Тайные советники собирались иногда в присутствии царя в доме канцлера «на конференцию» о наиболее серьезных вопросах иностранной политики. Окончательное устройство Коллегии иностранных дел последовало в 1720 г. 13 февраля царь прислал канцлеру графу Головкину подписанное и скрепленное резолюцией «быть по сему» «Определение Коллегии иностранных дел». Это «Определение» преследовало две цели: установить личный состав Коллегии с распределением между ним подлежащих ее ведению дел, и указать обязанности ее главных должностных лиц. На первом месте поставлены президент и вице-президент: канцлер граф Головкин и вице-канцлер барон Шафиров. «Когда важные дела,— написано далее в «Определении» рукой Петра I,— то призывать всех или несколько, по качеству дела, тайных советников действительных, и от всех надлежит быть совету на письме, и потом докладывать о решении».

После президента и вице-президента «Определение» касается канцелярии советников. На эту должность назначены были два лица: Андрей Остерман (будущий вице-канцлер) и Василий Степанов, притом первый со званием тайного канцелярии советника. Обязанности их заключались в составлении наиболее важных грамот к иностранным государям, рескриптов к русским министрам за границей, деклараций и резолюций, в надзоре за исполнением дел, поручаемых секретарям. Секретари по «Определению» ведали отделами или, как их называли, «экспедициями» Коллегии. Секретарями являлись И. Веселовский, П. Голембовский, Флорио Беневени и др. Для нас особый интерес представляет Первая экспедиция (иностранные дела на русском языке), секретари которой, а их было два, заведовали приемом и отправкой иностранных представителей

в России и русских за границей, всей перепиской с последними.

Становлению криптографии в этот период способствовало также развитие печатного дела. При Петре Великом начала выходить газета «Ведомости», был введен гражданский шрифт, продолжалась деятельность по переводу, а впоследствии изданию астрономических календарей. Увлечение астрологией, переводы и издание астрологических календарей, календарей-альманахов (в том числе широко известного Брюсова календаря) способствовали оживлению интереса к естественным наукам и, в первую очередь, к астрологии, медицине, физико-математическим наукам. Кстати, переводил календари в Посольском приказе еще в конце XVII в. П. П. Шафиров. Им, в частности, переведен календарь с предсказаниями, озаглавленный так: «Математических хитростных тонкостей календарь на 1697 лето от Р. Х. Сочинен впервые от Павла Генкена, математического художника... письменного и сочинительного мастера графа Букстегуда. А переведен с немецкого языка на славянский в государственном Посольском приказе переводчиком Петром Шафировым в нынешнем 205 (1697) г. в ноябре месяце» [2].

Глава третья

СЕКРЕТНАЯ ПЕРЕПИСКА В ПЕТРОВСКУЮ ЭПОХУ

Виды шифров

Внимание исследователей неоднократно обращалось к шифрованной переписке в России петровского времени. Уже непосредственно с конца XVIII в. стали появляться в печати публикации шифрованных текстов и шифров — так называемых «цифирных азбук» или «ключей» к тайному письму.

Первым, кто опубликовал шифр, который использовался внутри страны для переписки правительства с наместниками и военачальниками (о Булавине и восстании на Дону), был И. И. Голиков [1]. К. Я. Тромонин поместил в «Достопамятностях Москвы» в первой половине XIX в. шифрованное письмо 1711 г. Петра Великого к бригадиру П. И. Яковлеву [2] М П. Погодин напечатал в «Москвитянине» три шифрованных письма Петра к бригадиру Ф. Н. Балку и приложил шифр для них В «Материалах для истории Гангутской операции» напечатаны расшифрованные письма и четыре шифра 1713—1714 гг. [3]. Наиболее полно шифрованная переписка петровской эпохи представлена в многотомном издании «Письма и бумаги императора Петра Великого» (1887—1956), редакторами которого были А. Ф. и И. А. Бычковы. На этом труде (который мы для краткости в дальнейшем будем называть «Письма и бумаги») нам хотелось бы остановиться особо.

Академик Иван Афанасьевич Бычков неизменно работал над изданием источников эпохи Петра Великого с начала 80-х гг. XIX века. Вначале он проводил эту работу под руководством своего отца — академика А. Ф. Бычкова, а после смерти последнего в 1899 г. продолжил ее самостоятельно. Издание было приостановлено в 1918 г., когда к печати готовился уже 2-й выпуск 7-го тома. В последующие годы своей жизни И. А. Бычков не переставал работать над подготовкой к изданию последующих томов «П. и Б.». Издание 2-го выпуска 7-го тома было поставлено в издательский план АН СССР на 1944 г. Принять участие в этой работе И. А. Бычкову не удалось: 23 марта 1944 г. в возрасте 85 лет он скончался, завещав АН СССР собранные им материалы для последующих томов.

С мая 1943 г. в Институте истории была образована специальная группа, сначала под руководством академика Ю. В. Готье, а с сентября 1943 г. — под председательством доктора исторических наук А. И. Андреева, работающая над изучением петровской эпохи. После смерти И. А. Бычкова издание «Писем и бумаг» было поручено Институтом этой группе.

А. Ф. и И. А. Бычковы в своем издании «Писем и бумаг» опубликовали не только расшифрованную ими корреспонденцию, но также и некоторые шифры и зашифрованные письма целиком, если их не удалось прочесть. Заметим, кстати, что такой же материал А. Ф. Бычков поместил в сборнике Русского исторического общества, выпущенном в 1873 г. [4]. Работу Бычковых по опубликованию шифров Петра I продолжил во 2-м выпуске 7-го тома указанного издания А. И. Андреев, но в дальнейшем печатание шифров Петра I в этом издании было приостановлено.

Шифрованная переписка начала XVIII в. дает богатый материал для наблюдений за шифрами, употреб-

лявшимися в России в это время. А. Ф. Бычков в комментариях к своему изданию неоднократно останавливается на вопросах расшифрования наиболее трудных в этом смысле, по его мнению, текстов.

Российские «цифирные азбуки» и ключи 1700—1720-х гг. представляют собой уже знакомые нам по древнерусским рукописным памятникам шифры замены, где элементы открытого текста, которые мы в дальнейшем будем называть шифрвеличинами, заменяются условными обозначениями — шифробозначениями. Тексты, подлежащие зашифрованию, писались на русском, французском, немецком и даже греческом языках. В различных шифрах шифрвеличинами выступали отдельные буквы, слова и стандартные выражения. В качестве шифробозначений использовались элементы как правило специально составлявшихся с этой целью алфавитов, которые могли представлять собой буквы кириллицы, латиницы, других азбук (например, глаголицы), цифры, особые значки. Часть из таких значков, имевших порой весьма причудливые очертания, были, как нам кажется, нейтральны по значению, другие же являлись символами, к нашему времени почти совершенно забытыми и известными лишь узкому кругу лиц, а в ту далекую эпоху несли определенную смысловую нагрузку. К этим последним относятся символы планет, одновременно являвшиеся символами металлов и дней недели:

☾ — Луна — серебро — понедельник

☿ — Меркурий — ртуть — среда

♀ — Венера — медь — пятница

☉ — Солнце — золото — воскресенье

♂ — Марс — железо — вторник

♃ — Юпитер — олово — четверг

♄ — Сатурн — свинец — суббота

В шифрах петровской эпохи употреблялись только индо-арабские цифры, что явилось, вероятно, следствием того, что именно Петром I в начале XVIII в. была выведена из употребления архаическая буквенная кириллическая нумерация, употреблявшаяся до этого. Реформировал Петр и кириллическое письмо, введя новые виды шрифтов, которые определяют современный облик русской письменности. Однако старые графемы продолжают использоваться в качестве тайнописи.

Употреблялись как шифробозначения и буквенные сочетания. Таким образом, в то время в России использовались однобуквенные, двубуквенные, цифровые, буквенно-слоговые шифры замены.

Первые государственные шифры были шифрами простой или взаимно-однозначной замены, в которых каждой шифрвеличине соответствует только одно шифробозначение, и каждому шифробозначению соответствует одна шифрвеличина.

В российские шифры рассматриваемого периода, как правило, вводятся «пустышки» — шифробозначения, которым не соответствует никакого знака открытого текста. Хотя обычно для этого использовалось всего пять—восемь шифрвеличин в качестве пустышек, очевидно, что введение их в шифртекст, получающийся в результате замены элементов открытого текста шифробозначениями, отражает стремление создателей шифров осмыслить дешифрование шифрпереписки. Эти пустышки разбивают структурные лингвистические связи открытого текста и, в определенной мере, изменяют статистические закономерности, то есть именно те особенности текста, которые используют в первую очередь при дешифровании шифра простой замены. Кроме того, они изменяют длину передаваемого открытого сообщения, что усложняет привязку текста к шифрсообщению. Поэтому, видимо, не случайно, по сведениям Д. Кана, первый такой русский шифр был де-

шифрован англичанами лишь в 1725 г. Кроме того, в некоторых шифрах шифробозначения-пустышки могли использоваться для зашифрования точек и запятых, содержавшихся в открытом тексте. Как правило, это особо оговаривалось в кратких правилах пользования шифром, которые помещались в этих случаях в шифры.

Внешне шифр Петровской эпохи представляет собой лист бумаги, на котором от руки написана таблица замены: под горизонтально расположенными в алфавитной последовательности буквами кириллической или иной азбуки, соответствующей языку открытого сообщения, подписаны элементы соответствующего шифралфавита. Ниже могут помещаться пустышки, краткие правила пользования, а также небольшой словарь, называвшийся «суплемент» и содержащий некоторое количество слов (имен собственных, географических наименований) или каких-то устойчивых словосочетаний, которые могли активно использоваться в текстах, предназначенных для зашифрования с помощью данного шифра.

Самый ранний из исследованных нами пятидесяти с лишним шифров описанного типа представляет особый интерес.

Это — «цифирная азбука» 1700 г. для переписки Коллегии иностранных дел с российским послом в Константинополе Петром Толстым [5] (см. илл. на вкладке).

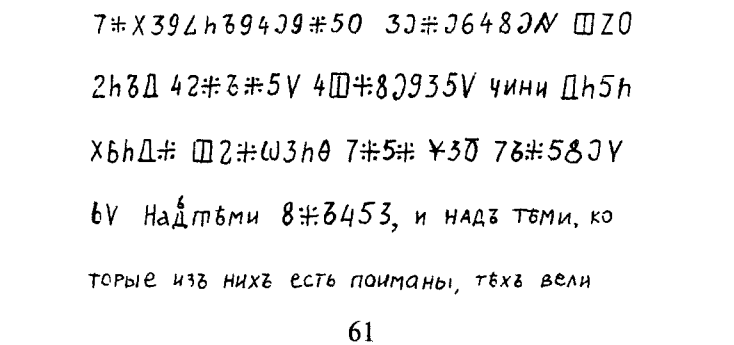
Она представляет собой шифр простой замены, в котором кириллической азбуке соответствует специально составленный алфавит. Здесь же имеются две записи. Первая из них: «Список с образцовой цифирной азбуки, какова написана и послана в Турскую землю с послом и стольником с Толстым сими литеры». Вторая особенно интересна: «Такову азбуку азволнил (изволил. — *Т. С.*) во 1700 г. написать своею рукою Великий государь по друго диво еси

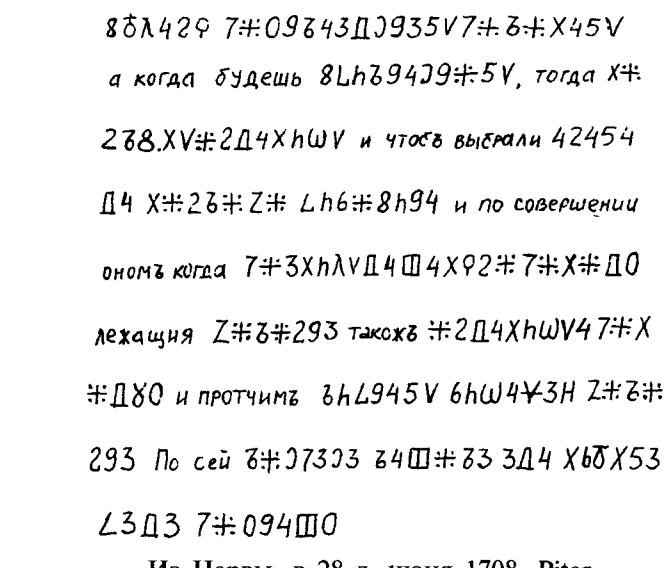
же». Из этого следует, что автором данной цифири был сам Петр Великий.

Очень похожий шифр для переписки И. А. Толстого с князем В. В. Долгоруким сохранился в подлинном письме Петра князю Долгорукому. Копия с этого шифра воспроизведена А. Ф. Бычковым.

Приводит А. Ф. Бычков и зашифрованное этим шифром письмо, написанное Петром I собственноручно. Вот его текст:

«Господин маеоръ. Письма ваши до меня дошли, из которых я выразумел, что вы намърены оба полка, то есть Кропотовъ драгунской и пъшей из Кіева, у себя держать, на что отвътствую, что пъшему, ежели опасно пройтить въ Азовъ, то удержите у себя, а конной, не мъшкавъ, конечно отправьте на Таганрогъ. Также является изъ вашихъ писемъ нъкоторая медленіе, что намъ не зело пріятна, когда дождетесь нашего баталіона и Ингермонланского и Билсова полковъ, тогда тотчас.





Зашифрованный текст читается так: «Поди къ Черкаскому и, сослався з губернаторомъ азовскимъ, чини немедленно съ Божіею помощію промыслъ надъ тъми ворами, и которые изъ нихъ есть поиманы, тъхъ вели въшать по украинскимъ городамъ. А когда будешь в Черкаскомъ, тогда добрыхъ обнадежь и чтобъ выбрали атамана доброго человека; и по совершении ономъ, когда пойдешь назадъ, то по Дону лежащие городки такожъ обнадежъ, а по Донцу и протчим речкамъ лежащие городки по сей росписи разори и над людми чини по указу».

В Государственном архиве Татарстана находится собственноручное письмо Петра I И. А. Толстому, в котором он, в частности, говорит, что посылает ему цифирь для корреспонденций. Текст письма издавался несколько раз, но А. Ф. Бычков сообщает, что цифирь, которая была послана при этом письме, не сохранилась уже к концу XIX в. Бычков воспроизводит ее по изданию Голикова [6].

А	Б	В	Г	Д	Е	Ж	З	И	К	Л
ме	ли	ко	ин	зе	жу	ню	о	пы	ра	су
М	Н	О	П	Р	С	Т	У	Ф	Х	Ы
ти	у	хи	от	ца	чу	ше	ам	з	ъ	от
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Ъ	Ю	Я	
ь	ъ	ю	я	ф	а	бе	ва	гу	ди	

Этот шифр имел правила пользования: «Сии слова без разделения и без точек и запятых писать, а вместо точек и запятых и разделения речей вписывать из нижеписанных букв...» Имелся здесь и небольшой словарь с именами некоторых государственных деятелей и наименованиями нескольких воинских подразделений и географическими наименованиями. Это обстоятельство также нашло отражение в правилах пользования, где говорится: «Буде же когда случится писать нижеписанных персон имяна и прочее, то оныя писать такими знаки, какия против каждой отмечено, однакож писать все сплош, нигде не оставливая, а между ими ставить помянутыя буквы, которыя ничего не значат».

Письмо Петра I было такого содержания:

«Господин губернатор! Понеже вы уже известны о умножении вора Булавина и что оный идет внизъ; того ради, для лучшаго опасения сихъ нужныхъ местъ, послали мы к вамъ полкъ Смоленский изъ Киева, и велели ему на спехъ иттить; а сего поручика нашего господина Пескарского послали к Вамъ, дабы уведать подлинно о вашемъ состоянии и нътъ ли какой блазни у васъ межъ солдаты. Также (от чего Боже сохрани, ежели Черкаскъ не удержится) имеешь ли надежду на своихъ солдатъ, о чемъ о всемъ дай немедленно знать чрезъ сего посланного, съ которымъ послана к вамъ цифирь для корреспонденции к намъ. Также другой ключъ для корреспонденции съ господиномъ маеромъ (гвардии Долгорукимъ), который посланъ на техъ

воровъ съ воинскими людьми, прочее наказано оному посыльному словесно.

Piter».

Нами найден другой шифр этого же времени, почти полностью повторяющий утраченную, по свидетельству А. Ф. Бычкова, цифирь 1708 г. [7]. Назовем первый шифр «цифирь А», а второй шифр — «цифирь Б». Отличия в шифробозначениях, соответствующих буквам кирилловской азбуки, отсутствуют совсем, но все же это разные шифры. Их различия сводятся к следующему: в «цифири Б» пустышек на одну больше, здесь же значительно обширнее и «суплемент».

Характер словарных величин, помещаемых в суплемент каждой данной цифири, обычно позволяет судить о том, каким темам могут быть посвящены сообщения, шифруемые с помощью этой цифири. Так, небольшой словарь в «цифири А» содержит величины, связанные с перепиской по восстанию Булавина (Булавин, губернатор Азовский, войсковой атаман и казаки и др.). И действительно, в приведенном выше письме Петра I, зашифрованном «цифирью А», отражена эта тема. В словарь же «цифири Б» включены величины, характерные для военной переписки, и не вообще, а необходимые для переписки о событиях на вполне определенном театре военных действий (графъ Фризъ, Речь Посполитая, князь Примасъ, гетманъ Огинский, Сапега, прусы польские, Литва, Великопольша и др.).

В томе IV «Писем и бумаг» опубликованы тексты белового и чернового писем, писанных собственноручно Петром I по-французски к князю Н. И. Репнину 29 января 1706 г. Частично это письмо было шифрованным. Подлинник не сохранился. Сохранился лишь сделанный у генерала Ренна перевод этого письма, причем у корреспондентов не оказалось ключа для расшифрования письма царя и шифрованные места остались не дешифрованы. В этом виде опубликовали

текст письма и издатели «Писем и бумаг». Относительно отсутствия ключей генерал Ренн писал Петру:

*«Пресветлейший, державнейший царь, великомилостивейший Государь. Во всепокорность Вашему пресветлому Величеству доношу: вчерашняго дня получил я личбу цифрами чрез посланного от Вашего пресветлого Величества смоленских полков прапорщика, по которой с господином генералом князем Никитой Ивановичем (*Репниным — *Т. С.) будем вразумляться. Только мое несчастие, что той личбы ключи отосланы в обозе. Благоволи, Ваше пресветлое Величество, приказать прислать ключи, а мы и без ключей покамест, как можно мыслить и по указу Вашего пресветлого Величества поступать будем, также и друг друга покидать не будем...»* [8].

Не менее интересным для нас является и блокнот с шифрами, которыми переписывался Петр I [9]. Он представляет собой тетрадь, листы которой скреплены веревкой. Размер тетради 20×16 см. На каждой ее странице записано по одному шифру, всего их шесть: 1) шифр Петра I, который был ему прислан из Коллегии иностранных дел во Францию в 1720 г. для переписки «от двора ко двору»; 2) шифр «для писем к графу Г. и барону П.»; 3) к князю Григорию Федоровичу Долгорукому; 4) к князю А. И. Репнину (1715 г.); 5) «азбука, которая была прислана от двора его царского величества при указе №..., а полученная 30 июля 1721 г.»; 6) «азбука цифирная, какову прислал Дмитрий Константинович Кантемир в 1721 г.».

Последний шифр с русским алфавитом отличается от предыдущих тем, что в качестве шифробозначений в нем использованы не буквы какого-либо алфавита, а числа.

Рассмотрим еще несколько шифров раннего типа, использовавшихся в эпоху Петра.

«Азбука, данная из государственной коллегии иностранных дел 3 ноября 1721 г. камер-юнкеру Михаи-

лу Бестужеву, отправленному в Швецию» [10], предназначалась для шифрования писем Бестужева к Петру I и в Коллегию иностранных дел. Алфавит в этом шифре русский, простая буквенно-цифирно-значковая замена. Усложнений нет. Эта и многие другие азбуки хранятся в современных им конвертах, на которых имеются надписи о том, для каких целей предназначается данный шифр. Изучение этих надписей позволяет установить, что шифры для переписки с государем или Коллегией иностранных дел в обязательном порядке вручались всем, кто направлялся за границу с государственным поручением. Это могли быть как дипломаты, так и не дипломаты. Например, сохранилась «азбука для переписки с господином бригадиром и от гвардии майором Семеном Салтыковым, который отправлен к его светлости герцегу Мекленбургскому. Дана Салтыкову 1 декабря 1721 г.» [11].

Сохранились и шифры канцлера Г. И. Головкина. Так, шифры, которыми пользовался канцлер в 1721, 1724 и 1726 гг. для переписки с различными государственными деятелями, подшиты в одну тетрадь [12]. У корреспондентов Головкина были первые экземпляры этих шифров, у канцлера — вторые. В эту тетрадь включено 17 шифров. Среди них «Азбука Алексея Гавриловича Головкина», «Азбука князя Бориса Ивановича Куракина», «Азбука Алексея Бестужева», «Азбука губернатора астраханского господина Волынского», «Азбука Флорио Беневени» и др. Все эти шифры построены одинаково, хотя и имеют некоторые особенности. Так, в «Азбуке А. Г. Головкина» (см. вкладку) русский алфавит, где каждой согласной букве соответствует по одному шифробозначению, а гласной — по два, одно из которых — буква латиницы, а другое — двузначное число или два двузначных числа. Есть тринадцать пустышек (буквы кириллицы), как помечено: «пустые между слов дабы растановок не знать». Кроме того, есть особые, также буквенные обозначения для запятых и точек. Таких обозначений пять.

«Азбука Алексея Бестужева» имеет десять двузначных цифровых шифробозначений для точек и запятых, в этой же функции в этом шифре выступает число 100. Алфавит в этом шифре — кириллица, шифробозначения — однозначные и двузначные числа и буквы латиницы.

«Азбука Флорио Беневени» не имеет пустышек, для обозначения точек использовались десять двузначных чисел.

В целом можно констатировать, что именно этот тип шифров простой замены был самым распространенным в государственной переписке России, по крайней мере до конца 20-х годов XVIII столетия.

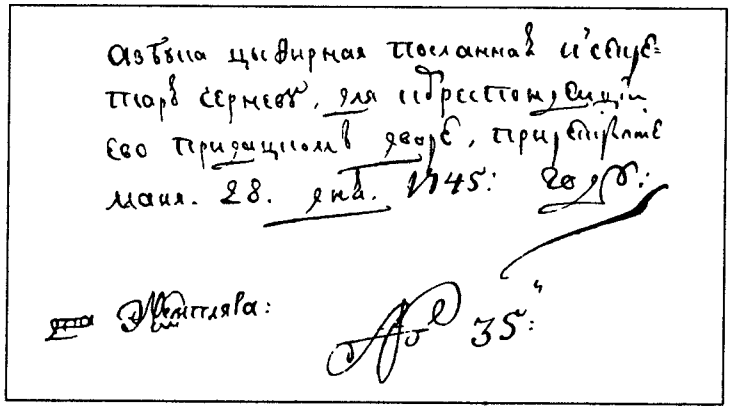
Организация шифрованной связи

Итак, документы свидетельствуют, что в Петровскую эпоху центром, где создавались шифры, где они вручались или откуда они рассылались корреспондентам, был вначале Посольский приказ, затем Посольская походная канцелярия, а в дальнейшем Первая экспедиция Коллегии иностранных дел. Вся деятельность по изготовлению шифров проводилась под непосредственным руководством самого императора, канцлера и вице-канцлера. Как в будущем в Коллегии иностранных дел, уже в Посольском приказе существовал специальный штат, которому поручалось зашифровывать и расшифровывать переписку. Текст, подлежащий зашифрованию, переписывали надлежащим образом дьяки Посольского приказа, а затем переводчики и секретари Коллегии иностранных дел [13]. Они же производили расшифровку писем.

В деловых бумагах нередко употребляется слово «перевод», когда речь идет о расшифрованных письмах, и упоминаются «переводчики» — лица, занимающиеся не только собственно переводом корреспонденции, но и расшифрованием ее. В Посольском

приказе, например, переводчиком польских писем являлся Голембовский. Он же «переводил», т. е. расшифровывал, письма, написанные тайнописью, приходившие из Польши. П. П. Шафиров, отсылая Г. И. Головкину письма польских министров, писал: «А цифирь такая, чаю, есть у Голембовского» [14].

Ключ к шифру вручали непосредственно тому лицу, с кем предстояло переписываться. Однако части ключа могли пересылаться с нарочными. Для этого их упаковывали в конверт, который опечатывался несколькими сургучными печатями. На конверте иногда писалось имя нарочного.



Так, в 1709 г. Я. В. Полонскому было поручено следить за движением войска старосты бобруйского и не допускать его до соединения с корпусом шведского генерала Крассау. Полонскому вменялось сноситься шифром. «При этом посылаем к Вам ключ, — писал Петр, — и ежели сей посланный здорово с ним поедет, и о том к нам отпиши, дабы мы впредь нужные письма могли тем ключем писать и посылать». Выражения «здорово» — дошло, «невредно» — получено означали, что шифр или письмо дошли благополучно.

Сообщения корреспондентов, полученные Коллегией иностранных дел, просматривались секретаря-

ми экспедиции при получении их с почты, написанные шифром разбирались ими или подчиненными им нотариусом-регистратором, канцеляристом и копиистами. После этого секретари были обязаны, если президента и вице-президента в Коллегии не было, посылать эти реляции к ним на дом, а во время заседаний Коллегии о них докладывать, записывать последовавшие на них резолюции и сочинять ответные рескрипты. Эти рескрипты прочитывались на следующем заседании, причем, согласно указу от 5 апреля 1716 г., и черновые их списки, и переписанные набело подписывались всеми членами Коллегии и скреплялись подписью секретаря. Затем текс рескрипта зашифровывался и направлялся в соответствующий адрес с курьером. Вся работа Коллегии была строго регламентирована. Вход в ее апартаменты был строго ограничен служащими там лицами. Инструкция от 11 апреля 1720 г., в которой было установлено устройство Коллегии иностранных дел, заканчивалась предписанием, как хранить государственные печати и цифирные азбуки.

Для сохранения письма в тайне предпринимались предосторожности. Так, письмо Петра I к Огильви от 17 февраля 1706 г. сопровождалось следующей записью: «Февраля в 17 день цыфирью Реновою. А посланы в 22 день; замешкались за тем, что азбуку переписывали и в пуговицу вделывали. Посланы с маером Вейром».

Кроме цифирных азбук, полученных из Коллегии иностранных дел, государственные деятели России и сами создавали шифры для своей переписки. Так, например, сохранилась подлинная цифирная азбука, созданная известным поэтом и дипломатом Дмитрием Кантемиром [15]. На азбуке надпись: «Азбука цифирная, какову послал князь Дмитре Костянтинович Кантемир в 1721 г. ». Это такой же, как и описанные выше, шифр простой замены, в котором буквы кириллицы заменяются на цифры и другие буквы кириллицы. Шифр содержит небольшой «суплемент»:

Царское Величество российский государь;
Королевское Величество французский государь;
Султанское Величество турецкий государь;
резидент французский Правоте;
князь Василий Лукич Долгорукий;
князь Антиох Кантемир;
князь Дмитрий Кантемир.

Сохранились некоторые цифирные азбуки, созданные и другими государственными деятелями России. Так, например, на одном из пакетов с шифром написано: «Такова азбука послана от резидента Алексея Бестужева при реляции ево № 88, полученной в Москве октября 8-го дня 1722 г., в которой он доносит, что прежняя пропала» [16]. На самом же шифре надпись: «Азбука в государственную Коллегию иностранных дел из Копенгагена от А. Бестужева отправлена сентября 8/19-го 1722». Сохранилось два экземпляра этого шифра. Очевидно, по приезде в Россию, Бестужев в соответствии с установленным порядком сдал в Коллегию и свой экземпляр ключа.

Сохранилась в Архиве внешней политики Российской империи (АВПРИ) и цифирь, которую сделал и в 2-х экземплярах прислал 9 ноября 1722 г. в Коллегию князь Куракин. Это шифр того же типа, но алфавит — латиница.

Посылались в Коллегию такие азбуки в конвертах, которые опечатывались красными сургучными печатями, уже не государственными, а личными — отправителей азбук, как в случаях с Бестужевым и Куракиным.

Пересылали шифры довольно часто, ведь срок их действия был ограничен, и вышедшие из действия документы направлялись в Коллегию иностранных дел. Например, в одном из своих писем в Коллегию Иван Неплюев перечислял шифры, ставшие недействительными.

Новые шифры готовились в Коллегии заранее и направлялись адресатам. Но бывали и другие случаи. Так, например, на одном из шифров есть надпись: «Азбука цифирная, присланная от генерала графа Вейсбаха, которою он велел до указа корреспонденцию чинить с господином оберштальмейстером, отправленным из Киева в Полшу, генералитету» [17]. А вот другая надпись: «Такова надпись написана по приказу его сиятельства графа Андрея Ивановича (Остермана. — *Т. С.*) и отослана к его сиятельству на двор секретарем фон Келлерманом апреля 11 дня 1734 года» [18].

С кем же царь и Коллегия иностранных дел вели шифрованную переписку? Постоянно такая переписка осуществлялась с дипломатическими представителями России за границей, в том числе: при венском дворе — П. А. Голицыным, И. Х. Урбихом, П. И. Беклемишевым, А. П. Веселовским; при прусском дворе — с Альбрехтом Литом, а затем с А. Г. Головкиным. Специальные шифры для переписки с русским двором имели: А. А. Матвеев — посол в Англии, Голландии, Австрии; Б. И. Куракин — посол в Риме, Лондоне, Нидерландах, Ганновере, Париже, и многие другие дипломаты, чьи шифры сохранились.

Часто зашифровывались письма коронованных корреспондентов — польского короля Августа II, прусского короля Фридриха, хотя чаще эту переписку вели министры и вельможи союзных государств: саксонскую — И. Ф. Арнштедт, Я. Г. Флеминг, польскую — Ян Шембек, А. Н. Синявский, К. Ф. Шанявский, С. Денгоф, датскую — Юст Юль. Переписка эта касалась вопросов международной политики, заключения союзных договоров и военных вопросов. Шифрованная переписка прусского короля находилась в руках его министра И. Г. Кайзерлинга. Существовала секретная переписка России и Молдавии. Известны шифрованные письма господаря Михаила Раковицы, молдавского «посланца» Георгия Кастриота. Кратковременные дипломатические миссии также сопровождались вручением тайной азбуки лицу, направлявшемуся из России за границу.

Информация, которая содержится в шифрованной переписке государственных деятелей России Петровской эпохи, исследовалась Е. П. Подъяпольской [19].

Уже тогда русские послы широко практиковали взаимный обмен информацией, которую пересылали в шифрованном виде.

Матвеев, будучи в Лондоне, переписывался с Урбихом, русским послом в Вене. Куракин переписывался одновременно с несколькими русскими представителями за границей [20]. Г. Ф. Долгорукий и его племянник В. Л. Долгорукий держали друг друга в курсе политики двух союзных с Россией государств — Польши и Дании. Переписка эта шифровалась.

Высший командный состав армии и флота имел шифры для переписки с царем. Известны шифрованные письма Петра I к адмиралу Ф. М. Апраксину, однако сохранилось их немного. Почти все подлинные письма Петра к Апраксиным исчезли (по-видимому, погибли) и дошли до нас только в списках. Шифрованные письма Петра фельдмаршалу Г. Б. Огильви, фельдмаршалу Б. П. Шереметеву, фельдмаршалу-лейтенанту Гольцу и их шифрованные ответы опубликованы в уже упоминавшемся многотомном издании [21].

В своей переписке корреспонденты использовали шифры, предназначенные для шифрования переписки на разных языках. В основном в этот период применялись так называемые русские, немецкие и французские цифири, т. е. шифры, в которых в качестве шифрвеличин представлены буквы, слоги, слова, словосочетания соответственно русские, немецкие, французские. Петр I особенно часто употреблял французские шифры. В одном из писем Огильви жаловался Головкину, что не сумел прочесть присланных распоряжений Петра: «Французские цифирные грамотки нихто читать не может, тако не знаю, что на них ответствовать.. Прошу... извольте мне на все мои письма ответ учинить немецкою цифирью, ибо той францужкой нихто не разумеет». Такие же жалобы Огильви адресовал и Петру: «...никого здесь нет, который бы французское ваше мог разуметь, понеже Рен ключ от того потерял... Изволте ко мне через цифирь мою писать, чтоб я мог разуметь...» [22].

Петр объяснил, почему он перешел в переписке тайнописью с немецкого языка на французский язык: «Французскою азбукою к вам писали для того, что иной не было. А которую вы перво прислали, и та не годна, понеже так, как простое письмо, честь можно. А когда другую прислал, то от тех пор ею, а не французскою, к вам пишем. А и французский ключ послан» [23].

Вообще же известно, что Петр не доверял Огильви и прикомандировал к нему А. И. Репнина, который наблюдал за действиями фельдмаршала. В 1707 г. Репнин получил новое задание от Петра, для которого ему был дан особый шифр. «При сем,— писал Петр 28 мая 1707г.,— посылаетца вам азбука особливыми литерами и знаками имян изображенная, против которой изволте в нужное время ради снисения оною азбукою к нам писать» [24].

Через две недели Петр посылает Репнина срочно ехать под Быхов «чинить промысл» над генералом литовских регулярных войск Синицким, перешедшим на сторону Станислава Лещинского. На этот раз Репнину предписывалось взять шифр у Ф. Х. Боура, который уже свыше двух месяцев находился в лагере под Быховом, пытаясь заманить и арестовать Синицкого. Переписка с Боуром шифровалась с помощью немецкого шифра. «Немецкой цифирью» был и шифр в переписке с фельдмаршалом-лейтенантом Гольцем; в издании «Писем и бумаг» она расшифрована только частично [25].

Вручались шифры для тайной переписки и лицам, получавшим специальное военное задание от царя. Наиболее близким лицом Петра I, как известно, был А. Д. Меншиков, которого после Полтавской победы царь возвел в чин генерал-фельдмаршала. Но и до этого Меншиков пользовался почти безграничным влиянием на Петра I. В 1704—1706 гг. Петр назначил его своим официальным заместителем на фронте, что нашло отражение в специальной терминологии.

Так, в письмах Петр называл Меншикова «господин мой товарищ». Слово «товарищ», по аналогии с воеводским товарищем, означало в данном случае, как указывает Е. П. Подъяпольская, «заместитель» или «помощник», т. е. Меншиков являлся официальным заместителем царя.

Шифрованная переписка между Петром I и Меншиковым касалась чрезвычайно важных вопросов. Так, в январе 1708 г. Петр I послал Меншикову шифрованное «Рассуждение», которое рассматривалось на военном совете в Вильно 3 февраля, и просил Меншикова высказаться по данному вопросу. В другом случае Петр требовал, чтобы Меншиков со своей стороны прислал «Рассуждение» цифирью [26].

Меншиков еще не был генерал-фельдмаршалом, когда шла подготовка к Полтавскому сражению. Однако он получал руководящие «пункты» наравне, а нередко и раньше фельдмаршала Шереметева. «...Пункты... отдали мы господину генералу князю Меншикову, — писал Петр Шереметеву из Воронежа 1 апреля 1709 г., — и с тех для ведома... посылаем к вам копию, цифирью писанную. Подтверждаю, дабы вы чинили по тем пунктам, которые с Воронежа вам посланы, а писаны оныя цифирью, а таковыя даны и генералу князю Меншикову» [27].

В переписке Петра I и Меншикова затрагиваются не только важнейшие вопросы военных операций, но также и вопросы внешней политики и дела, касавшиеся царевича Алексея Петровича. Так, была зашифрована часть письма Меншикова к Петру от 29 ноября 1709 г. о поездке царевича в Саксонию.

Меншиков, в свою очередь, переписывался тайной азбукой и с дипломатами (В. Л. и Г. Ф. Долгорукими), и с подчиненными ему лицами — генерал-майором А. Г. Волконским, Р. Х. Боуром, Г. И. Кропотовым и другими (шифр для переписки с В. Л. Долгоруким см. на с. 77).

Комендант Полтавы А. С. Келин получил 19 июня 1709 г., т. е. за неделю до Полтавского сражения, шифрованное письмо Петра I, отправленное к нему в шести экземплярах. Царь писал: «Когда сии письма получите, то дайте в наши шанцы сегодня знак, не мешкав, однем великим огнем и пятью пушечными выстрелами рядом... что вы те письма получили» [28]. Таким образом, военная шифрованная корреспонденция сопровождалась еще условной сигнализацией. Сами письма пересылались в полых снарядах, так как осада шведами Полтавы не давала возможности сообщаться иным образом. Через два дня, 21 июня, А. С. Келин сумел дать знать Меншикову в шифрованном письме о наблюдавшейся в Полтаве тревоге в шведском лагере и о перегруппировке войск неприятеля в связи с переходом русской армии на правый берег Ворсклы [29].

Как правило, все доверенные лица Петра получали от него вместе с заданиями шифры для переписки. Такими доверенными лицами, кроме А. Д. Меншикова и А. И. Репнина, например, являлись бригадир Г. И. Кропотов, генерал-майор Я. В. Полонский, сержант Преображенского полка, позже поручик флота А. В. Кикин, адъютант Петра А. И. Румянцев, полковник П. И. Яковлев.

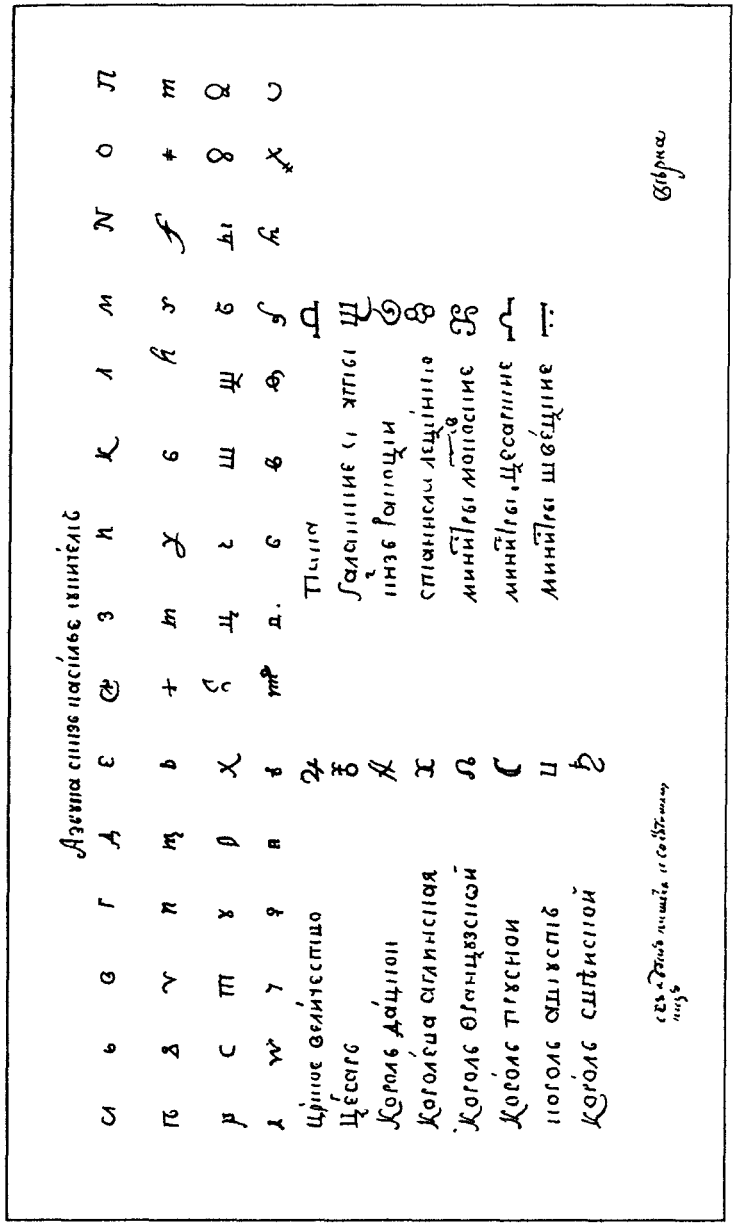
Бригадир Кропотов был отправлен в 1709 г. к крепости Каменец-Подольский, находившейся близ молдавской границы. Перед Кропотовым ставилась весьма ответственная задача — не пропустить Карла XII из Турции в Молдавию, откуда тот предполагал пробраться по горному проходу Кампулунг в Венгрию; вести секретные сношения с молдавским господарем Михаилом Раковицей, стремиться захватить на молдавской границе коронного стражника Стефана Потоцкого — сторонника Лещинского и Карла XII — и, что особенно важно, попытаться задержать самого Карла XII. Кропотов был обязан «о вышеописанных делах писать... цифирью». Переписка Кропотова с

Меншиковым сохранилась в архивном фонде последнего. Почти все письма Кропотова зашифрованы. Точно так же зашифрована переписка Кропотова и находившегося при нем переводчика А. Ботвинкина с М. Раковицей. Молдавский господарь жестоко поплатился за свою борьбу против турецкого гнета и за симпатии к России: он был низложен султаном, брошен в тюрьму и погиб в ней. Кропотов же, оставаясь на молдавской границе, и в 1710 г. продолжал посылать оттуда шифрованные письма.

Петр I использовал опыт генералов-иностранцев, но, не доверяя им, прикомандировал к каждому генералу своих людей из лейб-гвардии. Подобно тому, как к генерал-фельдмаршалу Огильви был приставлен Репнин, сообщавший сведения Петру шифрованными письмами, к генералу Георгу-Густаву Розену был прикомандирован в 1706 г. А. В. Кикин, носивший в то время скромный чин сержанта Преображенского полка. Генерал Розен имел немецкий шифр для переписки, этот же шифр имел и А. В. Кикин.

Торговые агенты, посылавшиеся за границу и получавшие нередко важные дополнительные поручения, имели шифры для письменных сношений. Сохранились азбуки для переписки с С. В. Рагузинским — агентом в Рагузе, Венеции, Средней Италии; с Осипом Соловьевым — агентом в Амстердаме и Ф. С. Салтыковым — морским агентом, известным автором различных проектов.

Переписка, касающаяся важных внутриполитических вопросов, также шифровалась. Мы уже писали о том, что специальный шифр был выработан для переписки о восстании на Дону в 1707—1708 гг. Ключ к этому шифру имели: Петр I, зорко следивший за ходом восстания, А. Д. Меншиков — командующий кавалерией, адмирал Ф. М. Апраксин, который вел строительство гаваней и флота на юге России, где развивалось восстание, подполковник Преображенского полка В. В. Долгорукий, назначен-



ный начальником всех вооруженных сил, выставленных против повстанцев, и азовский губернатор И. А. Толстой, на вверенной которому территории находился оплот от турецкой опасности — Азовская крепость, закладывались, строились новые крепости и гавани, сооружался молодой карабельный флот, причем всем этим начинаниям угрожало быстро ширившееся крестьянско-казацкое восстание. Восстание росло.

Против булавинцев на Дон были направлены гвардейцы, в том числе и Г. И. Кропотов. Меншиков писал ему: «...между тем временем как к нам, так и к господину маеору Долгорукому писать с нарочными курьерами, которых хотя шпигами или под видом переметчиков сквозь воровские войска посылать, ежели каким иным способом послать будет невозможно, и такие с ними письма писать цифирью» [30].

Секретная переписка, для которой имелись особые шифры, велась с администраторами пограничных районов и губерний — с киевским губернатором Д. М. Голицыным, с обер-комендантом Нарвы К. А. Нарышкиным.

В 1711 г. для внутреннего управления государством был создан Сенат. Очень скоро после этого Петр I начинает шифровать свои письма Сенату. Зашифрованные части этих писем обычно касались военных вопросов [31].

Таким образом, можно сказать, что правительственная, общегосударственная шифрованная переписка в Петровскую эпоху активно велась в области внешней политики и дипломатии, в военной деятельности, в области решения внутриполитических вопросов.

Один и тот же шифр без изменения использовали в разное время для переписки с различными лицами. Так, например, шифр, которым Петр I переписывался с Ф. Н. Балком в 1710—1711 гг., был дан позднее Д. М. Голицыну, в 1720 г. — князю Борису

Мещерскому. В 1715 г. шифр, которым до того переписывался П. П. Шафиров, был принят для переписки Г. И. Головкина и П. И. Ягужинского, а в 1716 г. его получил П. И. Беклемишев. Один и тот же шифр использовался в разное время и для переписки Коллегии с Я. В. Полонским, Н. Ю. Ифлантом, С. В. Рагузинским, С. Г. Нарышкиным. Подобное использование одних и тех же шифров, сданных ранее в Коллегию иностранных дел, практиковалось на протяжении всего XVIII столетия.

Глава четвертая

ДЕЛО ПРОДОЛЖАЕТСЯ

Преемники

С воцарением на российском престоле Екатерины I вице-канцлером России и, следовательно, руководителем ее криптографической службы становится А. И. Остерман (1686—1747). Вестфалец по рождению, Андрей Иванович (Генрих Иоганн Фридрих) Остерман в 1703 г. вступил на русскую службу к адмиралу Крюйсу, с которым и прибыл в Россию в октябре следующего года. В 1708 г. он был принят в число переводчиков Посольского приказа и служил в Походной канцелярии царя. В июле 1710 г. был послан к прусскому и датскому королям. По возвращении в Россию он назначается секретарем Посольской канцелярии. Остерман сопровождал царя в Прутский поход, причем 12 июля 1711 г. получил звание тайного секретаря, до этого пренадлежавшее П. П. Шафирову. В 1716 г. он был сделан канцелярии советником, в 1717 г. участвовал в Аландском конгрессе, а в 1721 г. заключил вместе с Брюсом Ништадтский мир, в награду за что получил баронское достоинство, деревни, деньги и чин тайного советника. В образованной в 1720 г. Коллегии иностранных дел он занял место тайного канцелярии советника. Первенствующее значение Остерман получает

при Екатерине I. Усидчивость, трудолюбие, дипломатическое искусство и знание в совершенстве четырех европейских языков сделали его незаменимым для императрицы. 24 ноября 1725 г. она пожаловала Остермана званием вице-канцлера с чином действительного тайного советника, а в начале следующего года он был назначен членом Верховного тайного совета. В ноябре 1726 г. Остерман стал главным начальником над почтами (почт-директором), а 1 января 1727 г. получил орден Андрея Первозванного. В Верховном тайном совете А. И. Остерман сначала держал сторону всесильного князя А. Д. Меншикова. Назначенный воспитателем при Петре II, со званием обер-гофмейстера, он продолжал оставаться сторонником Меншикова до его падения. Влияние Остермана на Петра II, значительное в начале царствования последнего, понемногу потеряло свою благотворную силу, перевешенное влиянием князей Долгоруких. После смерти Петра II Остерман только с виду присоединился к членам Верховного тайного совета, подписавшим условия ограничения самодержавной власти Анны Иоанновны, на самом деле действуя против них.

Поведение его в этом деле, после того как замысел верховников потерпел неудачу, снискало ему благоволение императрицы. 28 апреля 1730 г. Остерман был возведен в графское достоинство и получил земли в Лифляндии, а жена его была назначена статс-дамой к императрице С падением верховников и уничтожением Верховного тайного совета Остерман выдвинулся на первые роли вместе с немецкой партией. В учрежденном 10 ноября 1731 г. кабинете барон Остерман появляется рядом с графом Головкиным и князем Черкасским в звании второго кабинет-министра и в это время приобретает первостепенное влияние на дела, которого не могут у него оспаривать ни дряхлеющий Головкин, ни бездеятельный Черкасский.

После смерти канцлера Головкина Остерман получил звание первого кабинет-министра и, несмотря на обострившиеся отношения между ним и Бироном, сохранил прочное положение при дворе. Императрица Анна Иоанновна в затруднительных случаях спрашивала у него совета; современники называли его «оракулом» государыни, «душою» кабинета. После смерти Анны Иоанновны Остерман первое время держался в стороне от большой политической игры. 10 ноября 1740 г. он был произведен в генерал-адмиралы и оставался кабинет-министром, но не сохранил звания вице-канцлера. Вслед за падением Бирона первенствующее значение перешло к Миниху, но Остерман вместе с принцем Антоном-Ульрихом и графом Михаилом Головкиным вскоре добился того, что Миних принужден был уйти в отставку (1 марта 1741 г.). Остерман остался один, без соперников, почти полновластным вершителем судеб государства. Но не прошло и года, как он пал вслед за свержением с престола Иоанна Антоновича (25 ноября 1741 г.). Он был приговорен к смертной казни вместе с Минихом, Головкиным и другими. 18 января 1742 г. все осужденные были приведены к эшафоту на Васильевском острове против здания двенадцати коллегий. Приговор сначала прочитали Остерману. Он был возведен на эшафот и уже положил голову на плаху, когда секретарь Сената объявил, что по высочайшему повелению осужденному дарується жизнь, с заменой смертной казни ссылкой в Березов. Там он провел пять лет и умер 20 мая 1747 г.

Король Пруссии Фридрих II в своих «Записках» так писал об А. И. Остермане: «Искусный кормчий, он в эпоху переворотов самых бурных верною рукою управлял кормилом империи, являясь осторожным и отважным, смотря по обстоятельствам, и знал Россию, как Верней человеческое тело».

Говоря об А. И. Остермане, следует помнить, что он был одним из первых немцев, которые вслед за

Лефортом оказались на самом верху российской государственной иерархической лестницы, кто в бурные и переломные времена нашей истории сыграл значительную роль в ее судьбе. Известно, что вопрос о роли иностранцев, и в частности немцев, в судьбе России в том или ином контексте, неоднократно поднимался и в литературе, и в науке, и в обществе в целом. Исследуя историю криптографической службы России, и мы будем постоянно встречать немецкие фамилии среди тех, кто вносил в том или ином качестве свою лепту в ее развитие и совершенствование. Поэтому, на наш взгляд, здесь уместно напомнить слова выдающегося русского историка и философа XIX в. Н. И. Костомарова, который писал об Остермане: «Вестфалец родом, чуждый России по происхождению, по воспитанию и по симпатиям, которые привлекали его как немца в немецкой народности, этот иноземец более всех других иноземцев, привлеченных в Россию Петром Великим, понял, что, поселившись в чужой стране, надобно посвятить себя совершенно новому отечеству и сжиться с духом, нравами, особенностями того общества, среди которого будет течь новая жизнь... Это был человек замечательной честности, ничем нельзя было подкупить его — и в этом отношении он был истинным кладом между государственными людьми тогдашней России, которые все вообще, как природные русские, так и внедрившиеся в России иноземцы были падки на житейские выгоды, и многие были обличаемы в похищении казны. Для Остермана пользы государству, которому он служил, были выше всего на свете» [1].

При Остермане криптографы Коллегии иностранных дел продолжали работу в соответствии с уже установившимися традициями. Научная мысль не стояла на месте, постоянно велись поиски новых видов шифров.

Новые шифры

Сейчас трудно установить, что явилось причиной появления в начале 30-х годов XVIII в. в России совершенно новых тайнописных систем: были ли они плодом отечественной аналитической мысли или следованием иностранным образцам. Для нас важно отметить, что во всяком случае эти шифры — не плод слепого подражания, а составлены с полным знанием дела.

Такими новыми шифрами были сначала алфавитные, а затем неалфавитные коды. В этих кодах словарные величины помещались в несколько разделов: алфавит, слоги, суплемент, счеты, месяцы.

Алфавит в этих шифрах мог быть русский или латинский, в зависимости от того, на каком языке писалось сообщение. Слоги постоянны и характерны для каждого языка, поэтому эти разделы шифров для каждого языка были одинаковы. Например, для русских шифров это были:

ба бе би бо бу бы бя
ва ве ви во ву вы вя и т. д.

Суплемент был достаточно велик и включал не только необходимые имена царственных особ, государственных деятелей («персон») и географические наименования, как это было раньше, но и иную активную лексику. В этот раздел, например, могли входить слова: домогательство, склонность и т. д.

Раздел «счеты» или, как его еще называли, «исчисления», как правило, во всех кодах одинаков. Он включает в себя такие величины:

1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 00, 000, 0000, 00000, миллион.

Иногда этот раздел как-то дополнялся, например, могли быть добавлены числа 50 000 и 100 000.

Месяцы также перечисляются в особом разделе, и почти во всех шифрах это поясняется так: «Месяцы

для того особливыми литерами изображены, чтоб оные употреблять, когда в контексте нужда востребует, а инако в обыкновенном месте датума писать не надлежит» [2].

За редким исключением шифробозначения — это арабские цифры. Цифры-шифробозначения для разных частей словаря всегда имеют различия. Например, если для алфавита они могут быть одно-, дву-, трехзначные, то для суплемента только трех- или четырехзначные, а для иных частей (месяцы, счеты) только четырехзначные. Кроме того, могут быть и иные отличия. Так, если для алфавита и суплемента шифробозначениями могут быть различные числа, то для других разделов — лишь числа, оканчивающиеся нулями: 700, 750, 720, 4000 и т. п. Вообще для каждой последующей части словаря характерна все большая значность шифробозначений.

Эти шифры имеют большое количество пустышек, вводимых с целью усложнения шифра. Могут вводиться ложные дополнительные цифры, также не имеющие смысла, но и не входящие в число пустышек. В правилах пользования шифрами, хотя они еще весьма краткие, явно проступает тенденция к использованию при шифровании даже небольших текстов значительной части или даже большинства словарных величин. В качестве шифробозначений используются почти исключительно цифры, в отличие от шифров первой четверти века, когда в этой роли чаще выступали различные идеограммы. В новом типе шифров они употребляются крайне редко и только для обозначения «персон».

Однако наряду с этими шифрами продолжают активно использоваться и шифры старых образцов, в которых имеется лишь алфавит с шифробозначениями — цифрами, буквами или вычурными старинными идеограммами, такими, например, как в ранней цифирной азбуке для переписки с Григорием Волковым и князем Куракиным [3].

"король французский – , король английский – , король датский –  , король польский –  , король прусский –  , галанские статы –  , министры –  ".

Составители шифров в этот период уже знали, что частота употребляемости гласных букв в языке выше, чем согласных. Поэтому в 30—40-е гг. в новых шифрах гласным обязательно соответствует по нескольку шифробозначений, согласным же — одно-два. Наблюдаются попытки записи шифртекста без разделений шифробозначений точками (что раньше было абсолютно исключено) либо с разделением их фальшивыми точками. Способ расшифрования в правилах оговаривается заранее. Пример такого зашифрования дан в цифирной азбуке для переписки с государственным вице-канцлером графом Михаилом Илларионовичем Воронцовым [4].

Это шифр простой замены, где буквам кириллицы соответствуют двузначные цифровые шифробозначения, причем гласным придано по шесть шифробозначений, согласным — по два. В правилах сказано: «Сею цифирью писать двояким образом, без точек, и с фальшивыми точками, которые как бы расставлены не были, токмо для разбору всегда по два номера брать надлежит.

Пример 1.

2754493291301926...

Пример 2.

275. 449. 329. 1. 301. 926...»

Шифробозначения в этот период выбираются всегда по определенным порядковым алфавитным схемам, что, конечно, не способствовало надежности шифров. Например, в этой цифири мы находим:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	...
11	12	13	14	15	16	17	18	19	20	21	22	23	24	...
40	57	58	59	60	41	74	75	42	80	81	82	83	43	...
62	. . . . .				63	. . . . .		64	. . . . .				65	. . .
85	. . . . .				86	. . . .		87	. . . . .				88	. . .
99	. . . . .				98	. . . . .		97	. . . . .				96	. . .
56	. . . . .				55	. . . . .		54	. . . . .				53	. . .

Легко заметить здесь многочисленные закономерности в выборе шифробозначений. Эти закономерности, в каждом шифре свои, присутствуют в этот период всегда.

С начала 30-х годов в России наблюдается переход от алфавитных кодов к неалфавитным. В алфавитных кодах открытый текст и шифробозначения (собственно код) нумеруются параллельно друг другу. Отклонения от этого порядка хотя и были, но практически очень незначительные и мало влияли на повышение надежности или, как принято говорить, стойкости кода. По-видимому, составители шифров заметили, что такой параллелизм существенно облегчает восстановление открытого текста и самого кода, поскольку правильное угадывание некоторого числа шифробозначений позволяет упорядочить в алфавите шифробозначения других словарных величин. Ясно, что избежать такой слабости кода можно было путем перемешивания шифробозначений. В этих случаях для облегчения процессов зашифрования и расшифрования необходимо было составить «шифрант» и «дешифрант» — части кода, предназначенные соответственно для зашифрования и для расшифрования. В шифранте в алфавитном порядке располагались элементы открытого текста (шифрвеличины), т. е. буквы, слоги, слова, словосочетания, а в дешифранте — в порядке возрастания — шифробозначения, если они были цифровые, если же они были буквенные, то в дешифранте шифробозначения также располагались в алфавитном порядке. Однако в шифрах этого второго типа буквенные шифробозначения были крайне.

редки, они встречаются лишь иногда в отдельных частях шифров, например в суплементе.

Вместе с тем в это же время появляются первые попытки выделить отдельно артикли (для французских и немецких вариантов шифров) и слоги. Например, цифирная азбука для переписки Коллегии иностранных дел с графом Левенвольдом, направленным в Польшу в августе 1733 г. [5], имеет такой вид:

	Four Chiffrer	Four Dechiffrer
A	3	1 — E
B	81	2 — L
C	6	
D	01 и т. д.	01 — D и т. д.

Далее даны четыре величины:

que	94
et	95
de	96
la	97

В этот период у составителей шифров проявляется явное стремление придать каждой букве алфавита в шифре как можно больше шифробозначений. Однако все эти шифробозначения имеют один очень большой изъян: они пишутся подряд, что дает возможность легко их раскрыть. Так, например, цифирная азбука для переписки с бароном Кейзерлингом, отправленным в Польшу в декабре 1733 г. [6], имела такой вид:

A	11	12	13	14	15
B	16	17	18	19	20
C	21	22	23	24	25
.	.	.	.	.	.
Z	131	132	133	134	135

В небольшом суплементе этого шифра также каждой величине соответствуют по два шифробозначения, выбранных подряд в числовом ряду трехзначных цифр:

260 261 и т. д.

А в еще одном шифре камергера графа Левенвольда [7] каждой букве латинского алфавита соответствует даже по десять шифробозначений (примечателен особый 10-й столбец):

A	12	13	14	15	16	17	18	19	20	321
B	21	22	23	24	25	26	27	28	29	332
C	30	31	32	33	34	35	36	37	38	343 и т. д.

В небольшом суплементе два трехзначных цифровых шифробозначения, приданных каждой словарной величине, также выбраны подряд. Точкам и запятым соответствуют трехзначные шифробозначения. Таким образом, традиция выбора различных шифробозначений для разных частей шифра, сложившаяся в Петровскую эпоху, нашла свое продолжение в этом втором типе шифров XVIII в.

Однотипные по существу шифры рассматриваемого нами второго типа шифров XVIII в. внешне могли оформляться по-разному. Так, в одних случаях шифрант и дешифрант могли помещаться на одном развороте большого листа бумаги. В других случаях шифрант мог выделяться отдельно и представлял собой листы, сшитые нитками в тетрадь, а дешифрант писался на отдельном развернутом листе. В обоих случаях в шифрант шифрвеличины могли помещаться по-разному: либо в порядке алфавита с выделением пустых, точек и запятых отдельно в конце, либо по разделам (словарь, слоговая таблица, алфавит, числа — «счеты», календарь — «месяцы», пустые). В это же время начинают помещать в шифрант, а часто и в дешифрант правила пользования шифром. Эти правила поясняют те усложнения, те хитрости, которыми отличается данный шифр.

Рассмотрим некоторые наиболее характерные образцы таких шифров.

В 1735 г. резидент Алексей Вешняков прислал в Коллегию иностранных дел «цифры, которыми он корреспондует с генералитетом и министрами рос-

сийскими, обретающимися при чужестранных дворах» [8].

Цифирь оформлена в виде прошитой нитками тетради. На 1-й странице — заглавие: «Цифирь секретная, посланная к ея императорского величества господам министрам в Лондон и Дрезден». Вся страница разбита на три вертикальные графы. Первая графа озаглавлена «Алфавит для сложения». В эту графу помещены буквы русского алфавита, которым соответствуют двузначные цифровые шифробозначения (произвольные). Сюда же помещены в алфавитном порядке наиболее употребительные предлоги, местоимения, частицы: въ, изъ, как и т. д.

Вторая графа — «Разные знаменования» — содержит словарь шифра. Интересно, что наряду с тем, что каждому шифробозначению могут соответствовать, как обычно, по одной словарной величине (например, 100 — Ея Императорское Величество, 199 — двор Ея Императорского Величества), некоторым из шифробозначений соответствуют целые группы словарных величин, необходимые величины из которых выбираются в соответствии с контекстом (например: 198 — Английский король, двор, Англия).

Третья графа — «Для разбору» — дешифрант. На 2-м листе здесь приведены «Изъяснения для употребления сей цифири».

В «Изъяснениях» раскрыты хитрости этого шифра. В шифробозначениях цифири отсутствуют цифры 3 и 7, т. е. может быть 46, но не 47, 36 и т. д. Сами по себе любые двузначные или трехзначные цифры, содержащие 3 и 7, служат для обозначения запятых и точек. При этом рекомендуется: «Мешать оныя между всеми как в десятичных (двузначных. — *Т. С.*), так и в сотенных (трехзначных. — *Т. С.*), яко прибавкою оных число умножится. Следственно, знаменательное (значащее. — *Т. С.*) скроется так, что никакая комбинация открыть не может. Например: А — 29 можно представить: 729, 279, 297 или 329,

239, 293. Сим образом на всяку литеру, по малой мере, шесть номеров, которы знаемы будут токмо тому, кто ведает, что 3 и 7 ничего тут не значать. Следственно, яко оне бы не были; но едино 29 будет видеть».

Писать рекомендовалось все цифры и без вставок и со вставками подряд «без роставок буква от буквы и речь от речи (слово от слова. — *Т. С.*)». Особенно рекомендовал автор шифра вводить «смешения с 3 и 7» при зашифровании по буквам, где шифробозначения — двузначные («от большей части десятеричных надлежит мешать с пустыми»), ибо «когда в 10 строках один номер чаще найдется, то можно догадаться, что гласная буква или какое обыкновенное частое окончание, но расставливая всякой пятою на преди, в средине или на конце прибавлять. Как явствует в следующих двух примерах в цифири сей речи, сей образец есть неразборимый, ежели будет писана смешением пустых прилежно». И далее приводится пример на зашифрование, из которого следует вывод о том, что гласные легко выделить, «понеже оных токмо пять против двадцати нужно чаще употреблять. А когда будут смешаны с пустыми, то знающий оные иного опричь сих не увидит, ведая, что 3 и 7 ничего не знаменуют. А незнающему все различными номерами покажется, смешанные с пустыми, ибо ни один на другого походить не будет, и не однем, но разными те образы особливо в одной строке и ближних перемешивать надлежит».

А. Вешняков, как и многие другие государственные деятели России того времени, дипломаты и недипломаты, был человеком высокообразованным, знавшим несколько языков. Сохранились его греческие, французские, немецкие шифры. Так, например, его цифирь от 26 апреля 1739 г. [9] имеет заголовок: «Цифирь, которую ныне резидент Вешняков употребляет и статский советник Канионий» создана для

шифрования на французском языке. В ней есть примечание: «Все шифры (шифробозначения. — *Т. С.*) употребляются без разделения на точки и запятые, когда встречаются 0, 8 или 9, надо взять два шифра и так же для дешифрования».

Введение множества пустых в старые типы шифров свидетельствует об отчетливом понимании составителями цифирных азбук того влияния, которое имеет на раскрываемость зашифрованного текста частота употребления одних и тех же величин, особенно букв. По мере усложнения шифров количество пустышек, в них помещаемых, все увеличивается, порой объем их в словаре может превышать объем его значащих величин.

Так, например, немецкая цифирь от января 1744 г., «присланная от генерала барона Любераса для корреспонденций с ним наших министров при чужестранных дворах», имеет 165 пустышек, а в цифирной азбуке для переписки Коллегии с «Действительным камергером и чрезвычайным посланником (в Берлине — *Т. С.*) Петром Чернышевым от января 1745 года» [10], пустышек вообще великое множество. В обычной таблице пустышек дано 90 — от 1003 до 1093 (они конкретно перечислены), кроме того, в примечании написано: «Все нумера свыше 3015 служат тако ж пустыми, како пустыми употребляются и те нумеры, которые по порядку до 3015 не доставают». Значащих величин в данной цифири около 400, таким образом пустые значительно превышают это количество. В том же 1745 г. Чернышеву была послана еще одна цифирь, в которой конкретно перечислено 90 пустышек, а кроме того, указано: «Прочие числа все от 500 до 1000 и выше можно писать пустыми же, но каждое число... разделять точками. При употреблении сего ключа цифирного надо особливо того наблюдать, чтобы каждое число точками разделяемо было с частым при том вмешиванием пустых».

Еще одним примером того, что составители шифров стремились в этот период поместить в них как можно больше пустышек, может служить цифирь, посланная в 1747 г. в Берлин к действительному тайному советнику Кейзерлингу [11]. В этом небольшом по объему шифре для шифробозначений выбраны числа из разных, кроме первой, сотен, а также первой, шестой, седьмой, восьмой тысяч. А в качестве пустышек указаны такие числа: 1—100, 190—199, 243—299, 327—427, 442—549, 573—674, 682—789, 807—906, 921—1000, 5635—7009, 7043—10 000. Сохранился конверт, в котором доставили этот шифр в Берлин. Конверт был опечатан множеством сургучных печатей и на нем есть надпись о том, что доставлен он был лейб-гвардии поручиком Измайловым.

Тайнопись и разведка

Высокая активность России во всех сферах деятельности — политической, военной, экономической, дипломатической и других, характерная для XVIII в. в целом, а для его первой трети в особенности, повлекла за собой становление еще одного вида государственной деятельности, совершенно особенного, но неразрывно связанного с вышеназванными. Мы имеем в виду разведывательную деятельность, т. е. получение интересующей государство разнообразной информации с помощью специальных тайных агентов. Однако совершенно очевидно, что разведывательная деятельность теряет всякий смысл, если полученная информация не может быть передана заинтересованной стороне. И здесь важнейшее значение приобретает организация скрытых каналов передачи разведывательной информации, в том числе передачи ее в письменном виде с помощью шифров.

Изучая вопрос об источниках секретной информации, получаемой Россией, в первую очередь сле-

дует сказать о некоторых министрах иностранных держав. Сохранилось несколько шифров, по которым велась тайная переписка между этими лицами и теми русскими дипломатическими представителями за границей, кому они передавали соответствующие разведывательные данные.

При этом имена корреспондентов, с кем переписывался тот или иной российский дипломат, не назывались, в письмах и шифрах их именовали словом «приятель» и прибавляли идеограмму, которая скрывала имя секретного корреспондента.

Вот перед нами «Цифирь, данная приятелю Магрини, которою корреспондовать будет в Га(а)ге к графу Александру Г(авриловичу) Головкину. Прислана (в Коллегию. — *Т. С.*) при реляции... от 14 июня 1735 года» [12]. Этот шифр имеет следующий вид. На одном большом бумажном листе помещены четыре варианта шифра. Различаются они порядком расположения букв в латинском алфавите и шифробозначениями. Алфавиты построены так:

1. обычный порядок букв от A до Z;
2. S T U V X Y Z — M N O P Q R — F G H I K L — A B C D E;
3. M N O P Q R S T U V X Y Z — A B C D E F G H I K L;
4. F G H I K L — A B C D E — S T U V X Y Z — M N O P Q R.

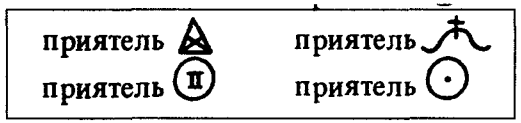
Другой сохранившийся шифр Магрини озаглавлен: «Цифры для корреспонденции и в нужном случае дается приятелю... или другому, кому поверено будет к высокому Ея Императорского Величества двору доносить или в Га(а)гу к его сиятельству Александру Гавриловичу Головкину». Цифирь была запечатана в конверт, на котором надпись гласила: «Цифирь приятелю X под литерой «F». Как видим, в данном случае имя Магрини и в названии шифра, и на конверте вообще отсутствует, оно обозначено идеограммой.

Шифр этот представляет собой большой лист бумаги, на котором на итальянском языке написан словарь на 400 величин, состоящий из букв, слогов

и слов. Каждой словарной величине соответствует по одному цифровому шифробозначению (двух- и трехзначному), кроме того, дано 40 пустышек. В конце словаря написано по-русски: «А для французского языка сие прибавляется» и даются французские слова, буквосочетания, артикли, их около ста. Дешифрант помещен на отдельный большой бумажный лист и озаглавлен: «Разборная цифирь приятеля X под литерой «F» [13]. Все подобные шифры обязательно в заглавии имели какую-то букву, цифру или знак, в данном случае это «F». Дело в том, что у каждого корреспондента, как правило, было по несколько шифров и, чтобы его адресаты знали, с помощью какого именно шифра написано то или иное сообщение, на каждой странице шифрованного текста эта литера шифра проставлялась несколько раз.

Подобные иностранные секретные корреспонденты или, если назвать более точно, агенты могли вести шифрованную переписку не только с российскими представителями за границей, но и непосредственно с Коллегией иностранных дел.

Важные для нас сведения содержатся в «Цифирной азбуке для переписки цесарского резидента Талмана с Российским двором, генералами и Вешняковым» от 2 августа 1735 г. [14]. Интерес представляет словарь шифра, который, с одной стороны, включая определенные географические наименования, словосочетания и т. п., позволяет в некоторой степени судить о содержании переписки (например: Республика Голанская, статы генеральные, крепость Святого Креста), а с другой стороны, — содержит несколько обозначений и секретных имен заграничных секретных агентов России. Например, в словаре этого шифра есть такие величины:



Некоторые идеограммы имеют пояснения:

– "секретарь голанского Риго"

– "Ергаки Ераки"

– "секретарь Афендия"

– "Андрей Магрини"

Сохранилась в архиве и цифирь упомянутого «приятеля» Ергаки Ераки. На ней надпись: «Цифирь приятеля Ергаки Ераки к российскому двору и генералам, присланная при реляции №... от 2 августа 1735 года» [15], а ниже приписка: «Сия же с приятелем Юргакием Хризоскомьевым, которого знак ☾+».

Наряду с описанным шифром для переписки с иностранными агентами русский дипломат А. Вешняков употреблял и другие. Так, для переписки с молдавским агентом он прислал из Константинополя большую шифровальную таблицу, представляющую собой шифр простой замены, словарь которого состоял из греческих букв, слогов, слов, а шифробозначениями были буквы греческого же алфавита или идеограммы. Много пустышек, обозначений для точек и запятых.

Сохранилась также цифирь, которую А. Вешняков вручил в январе 1737 г. для переписки аббату Косу, бывшему агентом российского двора [16]. На шифре надпись: «Цифирь с аббатом Косом, данная ему в Каменце от резидента Вешнякова при проезде его от Турской крепости в Россию». Этот шифр построен по принципу шифров 20-х годов: русский алфавит, каждой букве соответствуют одно-, дву- и трехзначные цифры. Правда, дано много пустышек — 85. Такой же шифр был вручен Вешняковым Косу и с латинским алфавитом.

Политическими агентами России были не только государственные иностранные деятели, но и иные

лица. Например, в Турции политическими агентами России в этот период являлись иерусалимские патриархи Досифей, а позже Хрисанф. Через Досифея шла переписка России с молдавским господарем. Патриарх Хрисанф предложил А. Г. Головкину тайную азбуку для переписки, которая была принята русским двором с некоторыми поправками, по поводу чего Хрисанф писал Головкину: «Приняли мы цифирь, которая прислана в дополнку нашей, и зело изрядна». Кроме того, Хрисанф предложил ввести в тайную переписку еще некоторые условности: «А чтоб нам чащей писать к Великому Государю и к Вашему Высочеству и безопасно, — писал он почтительно А. Г. Головкину, — сделали мы сию цифирь. Посылаем и образ печати. И как придет к вам какое письмо, в котором есть та печать, ведомо буди, что есть наше писание. А с лица печать какая-нибудь, только бы что была сия внутри. К тому же, которое письмо имеет с лица круг, то есть к Великому Государю; а которое имеет треугольный знак, есть к Высочеству Вашему. И сие всегда да будет за подлинное» [17].

Развитие русской разведки повлекло за собой активное становление института агентуры как за пределами государства, так и внутри него. Выделяется целая группа крупных государственных деятелей России изучаемого периода, специально занимавшихся этим вопросом. Кроме того, некоторые из них, такие как уже названные нами А. Головкин и А. Вешняков, выполняли и роль резидентов, которые вербовали агентов, руководили их работой, получали от них информацию.

И здесь, в первую очередь, мы должны назвать Ивана Ивановича Неплюева (1693—1773), чье имя, почти не известное нашим современникам, между тем занимает достойное место в отечественной истории.

И. И. Неплюев был видным дипломатом и крупным государственным деятелем, одним из «птенцов гнезда Петрова», активным проводником реформ

Петра I. Еще в 1721 г. он был назначен резидентом в Константинополь, где находился до 1734 г. В 1736—1742 гг. он работал в Коллегии иностранных дел и выполнял различные дипломатические поручения. В 1742—1758 гг. Неплюев был начальником Оренбургского края, где построил несколько укрепленных линий и более семидесяти крепостей. В 1760 г. И. И. Неплюев назначается сенатором.

Обнаруженные нами документы свидетельствуют о том, что И. И. Неплюев был одним из тех государственных деятелей России, кто стоял у истоков организации ее разведывательной и контрразведывательной службы. Именно Неплюеву удалось создать разветвленную агентурную сеть в некоторых регионах империи и за границей, «при иностранных дворах», в тех местах, которые представляли наибольший политический и, следовательно, разведывательный интерес для России.

В архивах сохранились некоторые шифры и письма И. Неплюева в Коллегию иностранных дел, к генерал-фельдмаршалу Г. Ф. Миниху, к другим корреспондентам. Эти письма проливают некоторый свет на деятельность русской разведки той поры. Вопросы, затрагиваемые Неплюевым, касаются агентов, которыми располагала Россия в том или ином регионе, задач, стоявших перед этими агентами, и многого другого. Известно, что в этот период Россия вела войну с Турцией и поэтому для нее особый интерес представляли разведывательные данные о главном военном противнике, о его возможных союзниках, а также о положении дел в сопредельных государствах и на сопредельных территориях.

В октябре 1739 г. И. Неплюев пишет Г. Ф. Миниху: «В Польше находящиеся корреспонденты по обращению дел ни к чему не способны. А в Молдавии и никого нет. Лупполь ушел с Господарем. Александр Дука и Контакузин в Яссах. А от Немирова при Днестре не токмо корреспондентов, но и людей ни-

каких нет». В этой связи тайный советник спрашивает генерал-фельдмаршала: «Не можно ли через знатных, обретающихся в Яссах, светских и духовных, внутри турецкого государства како надежно корреспонденции основать, к чему единый тот способ остается, что корреспондента из Каменца в Могилев перевести для того, что у поляков зимою с турками не без сношения будет, а через Хотин, когда он в наших руках, делать им того не можно...» На что Миних распорядился «поступать во всех случаях по благоизобретению» [18].

Чтобы поступать «по благоизобретению», очевидно, что Неплюев должен был подбирать агентов, причем тщательнейшим образом, внимательно изучая черты характера, биографии и т. д. всех возможных кандидатов на эти роли. Среди агентов Неплюева были: два брата Вуцино — «один в Яссах, другой при Гетмане коронном», Дыма, который находился в Каменце и, как писал в своем донесении Неплюев, выказывал «склонность вступить в службу российскую», а также другие. Наибольшим доверием со стороны Неплюева пользовался агент во Львове Юрья Томазин, по национальности грек.

В одном из писем Миниху Неплюев дает ему такую характеристику, раскрывая при этом и причины, побудившие Томазина стать агентом: «Юрья Томазин холостой, умом остр и из неубогих, на многих польских знатных вельможах долги имеет, но без протекции опасен, дабы его в Польше не погубили. Того ради желает быть в службе российской, дабы Ея Императорского Величества протекциею мог впредь те свои долги выбрать...» Юрья Томазин оказался очень ценным агентом. Он не только сам добывал разведывательные данные и передавал их Неплюеву, но поставлял Неплюеву лиц, которые также использовались как агенты, т. е. Томазин стал так называемым агентом-вербовщиком. При этом Неплюев поддерживал секретную связь только с

самим Томазином, другими же агентами руководил через него.

Братьев Вуцино, по-видимому, завербовал также Томазин. Одного из них, Биажжио, Неплюев решил направить с заданием в Турцию. В письме к Томазину он пишет: «Присланного от Вас сюда... Биажжио Вуцино я такова нашел, как Ваше благородие об нем писали, то есть способна с плодом служить, и потому, обнадежа его о моем за его труды признании по представлению Вашему, послал его в Царьград и приказал тамо жить, донде же верховный визирь с войском не выступит, за которым ему следовать в лагере приказал».

Однако чтобы агент работал надежно и преданно, его подкупали не только деньгами, порой решающую роль играли какие-то иные факторы, и Неплюев это хорошо понимал. Томазин, очевидно, имел большой опыт в подобных делах, так как Неплюев полностью на него полагался. Так, относительно Б. Вуцино он писал Томазину: «Я хотя его и не знаю состояния и можно ль в таких нужных делах на него положиться, но имел Вашу об нем рекомендацию и, уповая на Вас, столько ему доверил в надежде, что Вы его наивяще в том его доброжелательстве утвердите, дабы как Вам вреда, так и все напрасно не пропало» [19].

Нам бы хотелось обратить внимание читателя на подчеркнуто-уважительный тон, в котором выдержаны все письма Неплюева к Томазину. Это также свидетельствует о том, что тайный советник прекрасно понимал, что не только деньги определяют надежность работы агента. Конечно, за такой подход к этой проблеме Неплюеву следует отдать должное, особенно если задуматься о той пропасти в общественном положении, которая разделяла этих людей, — генерала, тайного советника и простого агента.

Агенты Неплюева прекрасно работали не только за границей. Так, тайному советнику стало известно об измене киевского воеводы, которого подкупили

турки. Секретарь же воеводы, некто Хелминский, был еще агентом князя В. Л. Долгорукого в бытность последнего киевским губернатором. Неплюев дает задание Томазину вновь использовать помощь Хелминского, при этом так инструктирует агента: «Секретарь Хелминский получал прежде сего от князя Долгорукого по сту по пятидесяти червонных и по одной паре соболей в год, что все я ему охотно дать готов, только б он так служил верно, как Вам обещался, и, ежели действительно ревность свою покажет, то можете его и большим награждением обнадежить, которое в действе скоро увидит. А ныне, ежели Вы то заблагорассудите, можно ему, Хелминскому, половину, то есть семьдесят червонных переслать». Помощь Хелминского была крайне необходима Неплюеву еще и потому, что ему стало известно о том, что кто-то из высших чинов русской армии также продался туркам и поставляет им секретные сведения. Об этом Неплюев писал Томазину: «Вашему благородию сообщаю, что есть у нас сумнение, что в минувшую кампанию некто из нашей армии чрез... воеводу киевского тайную корреспонденцию с секретарем бендерским продолжал, и понеже как сами рассудите, нам то весьма потребно и нужно открыть, того ради усильно Вас прошу чрез секретаря Хелминского, искусно и не давая о том ему знать, наведаться, ибо та корреспонденция необходимо на турецком языке продолжалась, следственно ему о том сведому быть надлежит. А что про сие секретное дело от него услышите, о том, уповаю, откровенное и ничего не опасаясь известие о том иметь».

Хелминский стал работать, и вскоре Неплюев получил от него «две польские копии с писем сераскера и салтана буджацкого к воеводе киевскому». С помощью Хелминского через переписку киевского воеводы Неплюев старался проследить за попытками Швеции и Польши вступить в союз с Турцией, и это с успехом удавалось сделать. Завербовал

Неплюев и одного из шведских агентов — капитана Болгорда. Болгорд выдал еще четырех шведских агентов, действовавших на территории Малороссии, сообщив также о данных им заданиях и связях.

Для переписки Неплюев снабдил Вуцино шифром («италианскою цифрою»), но письма свои тот должен был переправлять с помощью специальных «искусных» людей не Неплюеву, а, с целью конспирации, Томазину. На оплату курьеров и другие расходы Неплюев дал Вуцино денег.

Подобных Томазину, крупных агентов у Неплюева было несколько. С некоторыми из них велась шифрованная переписка, хотя в целом значение шифров еще явно недооценивалось. Это, по-видимому, связано с тем, что сам процесс шифрования был весьма трудоемким, трудности приводили к ошибкам, что искажало текст. В одном из писем Неплюев прямо пишет агенту: «Сие мое дружеское пишу к Вам по-русски, опасаясь, дабы по важности дел в цифрах не было ошибки... и Ваше благородие ответ на сие можете ко мне без цифры ж прислать, понеже я за тем нарочного курьера отправлю, чрез которого не так как эстафету верно дойти может...»

Как видим, для того чтобы оценить значение шифров, нужен был исторический опыт, пока же его явно не хватало. Но пройдет совсем немного лет и взгляды на этот вопрос изменятся коренным образом. Во многом этому будет способствовать перлюстрация иностранной корреспонденции и деятельность дешифровальной службы России.

Глава пятая

ВЕЛИКИЙ КАНЦЛЕР

Чтобы тайное не стало явным

Перелистаем некоторые страницы политической истории Российского государства XVIII в., связанные с добычей секретной переписки иностранных государств, и попытаемся проследить, какое значение имело знание ее содержания. Пусть нашим путеводителем будут только подлинные документы той далекой эпохи. Они сохранились в архивах, известные и малоизвестные, но крепко забытые. Проникнемся подлинным духом их текстов, стараясь не искажать их своими краткими пересказами. Подобные пересказы почти всегда обедняют содержание документов, а то и придают ему неправильный акцент.

1738 г. Россия ведет войну с Турцией. Русскими войсками в Крыму и Бессарабии командует Бурхард Христоф Миних (1683—1767) — генерал-фельдмаршал, немец по национальности, женившийся на графине Салтыковой и возвысившийся на русской службе в период кратковременного царствования юного самодержца Петра II. Императрица Анна Иоанновна в 1732 г. назначила его президентом Военной коллегии. Не обладавший особыми полководческими талантами, но преуспевший во многих политических интригах, Миних стремился добиваться

государственных, да и личных целей любыми средствами и любой ценой.

В условиях войны для России в тот период особую ценность имела информация о намечавшемся тайном союзе между Турцией и Швецией. Через секретную агентуру Ивана Неплюева Миниху стало известно, что в Турцию с важными документами направлен шведский гонец. Командующий принимает решение, перехватив гонца по дороге, добыть документы. Выполнить это задание поручается поручику Тверского драгунского полка Левицкому. Сохранилась подлинная инструкция Левицкому, написанная самим Минихом, датированная 23 сентября 1738 г.

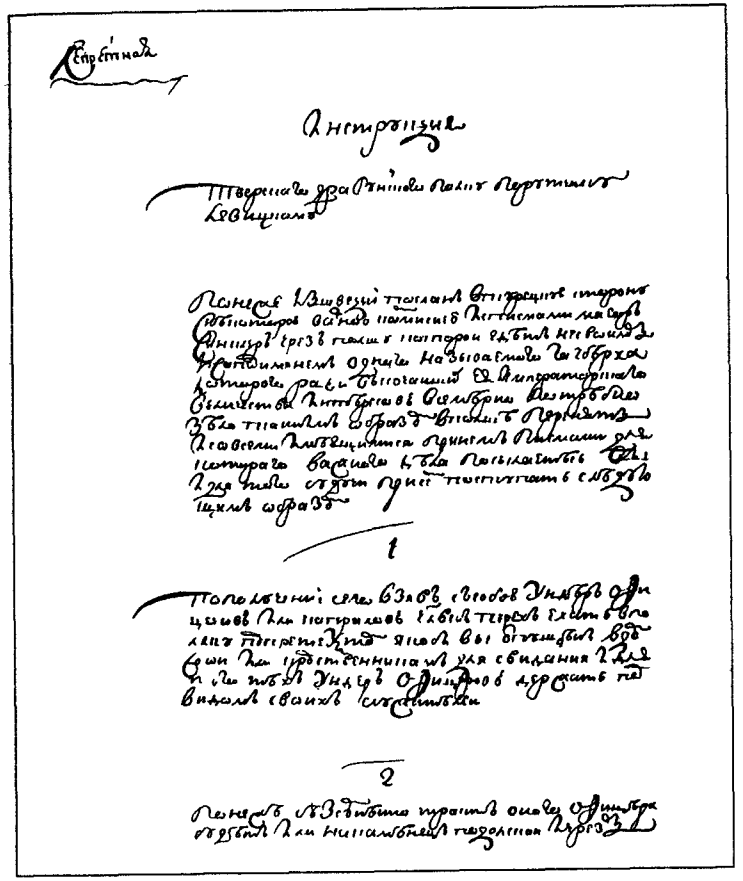
Вот ее текст:

«Понеже из Швеции послан в Турецкую сторону с некоторой важной комиссией и с письмами майор Синклер, который едет не под своим, а под именем одного, называемого Гогберх, которого ради высочайших Ея Императорского величества интересов всемерно потребно зело тайным образом в Польше перенять и со всеми имеющимися при нем письмами. Для которого важного дела посылаетесь Вы и для того будете при сем поступать следующим образом:

*1. При получении сего взять с собой унтер-офицеров или капралов человек трех, ехать в Польшу под претекстом (*под предлогом. — *Т. С.) якобы вы отпущены в дом свой или к родственникам для свидания. И для того же тех унтер-офицеров иметь под видом своих служителей.*

2. Понеже, без сомнения, тракт оного офицера будет или на Каменец-Подольский, или через Хотин, или через Сороку, того ради ездить Вам более по тем местам, кои по тракту к вышеописанным местам, и везде, будучи в разговорах, пристойным образом спрашивать об оном офицере тем именем, под которым он едет, объявляя, что он человек знакомый...

3. Ежели по вопросам о нем где уведаете, то тотчас ехать в то место и искать с ним случая компа-



Страница инструкции Миниха

нию свесть или иным каким образом его видеть. А потом наблюдать, не можно ли его на пути или в каком другом скрытом месте, где б поляков не было, постичь.

4. Ежели такова случая найдете, то стараться его умертвить или в воду утопить. А письма прежде без остатка отобрать, токмо при том таким образом поступать, чтобы никакого подозрения полякам не показать и ими то уведано не было.

5. И ежели оное благополучно исполнится, то тотчас ехать обратно. А письма, которые от него отобраны будут, везти во всяком бережении и сохранении. А по приезде обо всем подать ко мне обстоятельный рапорт.

В прочем, будучи при сем важном деле, поступать так, как надлежит Ея Императорского Величества верному рабу и искусному человеку, ожидая за исполнение того высочайшей Ея Императорского Величества милости и награждения, смотря при том, чтобы от подчиненных Ваших польским подданным никаких малейших обид, позлобления чинено не было... Миних» [1].

Поразительный документ, по сути своей приказ, подробный и четкий: добыть секретную информацию любой ценой, пускай даже ценой человеческой жизни. И все по пунктам и в деталях описано, как провести операцию по изъятию документов и скрыть все следы.

Перед отправлением в Польшу Левицкому от тайного советника Ивана Неплюева послали цифирную азбуку. Исполнил Левицкий все точно по приказу. А когда дело было сделано и Синклер убит, а почта, которую он вез, попала в руки Миниха, то и самого поручика Левицкого, и других, посвященных в эту тайну, да и не посвященных, а тех, кто лишь прикоснулся к ней, арестовали и сослали в Сибирь, в Тобольскую губернию. Там они благополучно провели пять лет. Чтобы тайна осталась тайной. Правда, за это время Левицкий получил следующий воинский чин и, вернувшись по отбытии срока ссылки, продолжил службу.

Интерес к секретной переписке противника стал проявляться постоянно, последовательным было стремление в любом удобном случае завладеть его шифрами и ключами. И всегда подобные действия, предпринимаемые по приказу высших лиц государства или с их ведома, держались в абсолютной тайне. Проникнуть в эти тайны удавалось порой спустя много лет, а некоторые из них так и затерялись в веках.

...В марте 1827 г. государственный канцлер Нессельроде предложил директору архива МИД России А. Ф. Малиновскому (брату В. Ф. Малиновского — директора Царскосельского лицея) разыскать во вверенном ему архиве документы, содержащие сведения о бывшем в 30-е годы XVIII в. в плену в России некоем Дюке де Фаллари, лицо которого в тюрьме будто бы скрывала железная маска.

Ф. А. Малиновскому удалось обнаружить документы, рассказывающие историю французского генерал-майора Дюка де Фаллари, который был направлен в Россию в 1739 г. Меклебург-Шверинским герцогом Карлом Леопольдом [2] с секретным поручением. Но, как сказано в документах, «российское министерство заранее предуведомлено было о неблагоприятных предложениях, Фалларию вверенных, и давно знало сего постыдными поступками обезглавленного негоциатора, то и предписало по приезде его в Россию арестовать» [3].

Фаллари, прибывший в Ригу 15 мая 1739 г., на третий день был взят под стражу и в препровождении майора Астраханского полка Федора Воейкова отправлен в Санкт-Петербург. Среди бумаг Фаллари был найден шифр, представляющий собой многозначную замену букв латинского алфавита на двух- и трехзначные числа. Каждой букве алфавита соответствовало 3 шифробозначения — трехзначных числа из второй сотни. С помощью этого шифра были прочитаны секретные инструкции и бумаги, которые Фаллари вез с собой. В одной из зашифрованных инструкций посланнику герцога приказывалось заботиться: 1) о возобновлении союза, заключенного Карлом Леопольдом в 1716 г. с Петром Великим, 2) через посредничество русского двора и лично императрицы Анны Иоанновны ходатайствовать у германского цесаря, чтобы тот «уничтожил все изданные в предостережение герцогу декреты и ввел бы его опять во владение меклебург-шверинских земель»

и, главное, 3) готовить почву для супружества дочери Карла Леопольда с сыном курляндского герцога Бирона. У российского двора на этот престол были, как известно, совершенно иные виды.

Императрица грамотой известила меклебургского герцога об аресте Фаллари. Однако Карл Леопольд решил отмежеваться от неудачливого посланника и в своем ответе Анне Иоанновне сообщил, что ничего общего с Фаллари не имеет и, напротив, «описав коварные замыслы сего аккредитованного им дипломата, назвал его злодеем и плутом, который старался у Папы обратить его в католическую веру», и даже просил императрицу, чтобы Фаллари был «предан по делам его наказанию».

Так оказался Фаллари в русской тюрьме, где провел много лет, а затем был сослан в Сибирь. Однако слухи о якобы надетой на него железной маске, что и вызвало интерес Нессельроде, документами не подтверждаются.

Добывали секретную информацию в то время и другими способами и путями. Нам, однако, важно отметить, что какой-либо системы в том не было, как не было и специального органа, который бы организовывал добычу и прочтение секретной переписки, в том числе и шифрованной.

«Черные кабинеты»

Среди специалистов бытует мнение, что, в отличие от стран Западной Европы, где служба перлюстрации — тайного вскрытия и копирования корреспонденции, в том числе и частной, существовала уже в XVII в., таковая в России была организована лишь в самом конце XVIII в. в период царствования императрицы Екатерины II [4]. Возможно, что эта неточность проникла в научные исследования из-за того, что еще в 1862 г. в «Чтениях Московского Общества истории и

древностей Российских» были опубликованы записки личного секретаря Екатерины II Храповицкого, в которых он говорит об особом интересе императрицы к перлюстрации почты иностранных дипломатов. Кроме того, именно в царствование Екатерины II в 1796 г. в Петербурге, Москве и Одессе были созданы органы цензуры, а при них организованы «черные кабинеты», — т. е. служба перлюстрации. Подробно деятельность этой службы описал в своей работе в 1873 г. Брикнер. В частности, исследователь пишет: «Перлюстрацией называлось чтение чужих писем и депеш, нарушение тайны писем; ею заменялись отчасти газеты и телеграммы нынешнего времени, она была важным орудием при управлении делами, потому что при помощи ее правительство знало о положении дел и о настроении умов, сколько в провинции, сколько за границей, о расположении министров и государей европейских держав, о намерениях и действиях аккредитованных при русском дворе иностранных дипломатов» [5].

Действительно, в царствование Екатерины II служба перлюстрации работала активно, именно в этот период была учреждена цензура. Однако «черные кабинеты» появились в России значительно раньше, и притом на целых пятьдесят лет. Как следует из найденных нами архивных материалов, перлюстрация переписки иностранных дипломатов была организована в России в начале 40-х гг. XVIII в. — в эпоху царствования дочери Петра I императрицы Елизаветы Петровны. Учреждение службы перлюстрации в первую очередь связано с именем Алексея Петровича Бестужева-Рюмина(1693—1766).

Об этом выдающемся государственном деятеле России XVIII в., к сожалению, мало известно современному читателю. Между тем он относится к числу тех лиц, которые сыграли заметную роль в судьбе нашего Отечества. Родился А. П. Бестужев-Рюмин 22 мая 1693 г. В 1708 г. он был отправлен по приказу

Петра I вместе с братом Михаилом за границу «для науки». В 1712 г. А. П. Бестужев становится дворянином посольства в Берлине, но год спустя поступает с разрешения Петра I на службу к Ганноверскому курфюрсту, впоследствии английскому королю Георгу I и в качестве его посланника приезжает в Петербург в 1714 г. В Англии Бестужев пробыл около четырех лет. В 1717 г. он возвращается на русскую службу, и в 1721 г. его назначают резидентом в Дании. Со вступлением на престол Анны Иоанновны Бестужева переводят резидентом в Гамбург, а через год он получает звание посланника в Нижнем Саксонском округе. В 1735 г. он был снова определен посланником в Данию, где оставался до 1740 г., когда был, наконец, вызван в Россию Бироном и 18 августа 1740 г. назначен кабинет-министром. Преданный Бирону, Бестужев принял деятельное участие в вопросе о назначении его регентом после смерти Анны Иоанновны. Вместе с Бироном он был арестован в ночь с 8 на 9 ноября 1740 г. и приговорен к четвертованию. Однако казнь его была заменена ссылкой в дальнюю деревню. В октябре 1741 г. Бестужев вновь был возвращен в Петербург и по вступлении на престол императрицы Елизаветы Петровны осыпан милостями. 12 декабря 1741 г. он был пожалован званием вице-канцлера, в марте 1742 г. назначен главным директором почт. 25 апреля 1742 г. вместе с отцом и братом А. П. Бестужев-Рюмин получил графское достоинство. Занимая при дворе все более влиятельное положение, он начинает активно проводить свою политику. Его система — это союз с Англией и Австрией против Франции и Пруссии. Французские дипломаты, аккредитованные в России, употребляли все старания к тому, чтобы свергнуть Бестужева, особую активность в этом вопросе проявлял французский посол маркиз Шетарди.

Как следует из найденных нами архивных материалов, перлюстрация переписки иностранных дипло-

матов была организована в России при деятельном участии А. П. Бестужева-Рюмина в начале 1742 г., т. е. как раз в тот период, когда он назначается главным директором почт.

Сохранились русские копии писем 1742 г.: от «голштинского в Швеции министра Пехлина к находящемуся в Санкт-Петербурге обер-маршалу голштинскому Бриммеру», «голландского в Санкт-Петербурге резидента Шварца к Генеральным штатам, к графине Фагель в Гаагу, к пансионерному советнику фон дер Гейму и пр.», «австро-венгерского в Санкт-Петербурге резидента Гогенгольца к великому канцлеру графу Ульфельду и к графу Естергазию, а также секретаря его Бослера к маркизу Вотте», «английского в Санкт-Петербурге министра Вейча к милорду Картерсту в Ганновер и к герцогу Ньюкастльскому», а также копии некоторых других документов [6].

От разных лет царствования Елизаветы Петровны сохранились копии писем иностранных дипломатов, снятые в черных кабинетах», все они сшиты в толстые дела и снабжены переводом. На некоторых, в том числе самых ранних, таких копиях есть пометы: «Ея Императорское Величество слушать изволила». Таким образом, содержание перлюстрированной переписки иностранных дипломатов докладывалось императрице уже в 1742—1743 гг.

Документально известно, что по установленному порядку канцлер или вице-канцлер делали доклады Елизавете Петровне о положении государственных дел несколько раз в месяц. Доклады эти, как правило, содержали сведения по двум-трем десяткам наиболее важных вопросов. При докладах обязательно присутствовал секретарь (в тот период им был Иван Пуговишников), который вел подробный протокол докладов-совещаний. Затем этот протокол переписывался набело, скреплялся в обязательном порядке подписями канцлера или вице-канцлера и подши-

вался в дела. Сейчас эти фолианты являются бесценным историческим источником, содержащим сведения о том, чем жило государство, какую политику проводило правительство в том или ином вопросе, а, в конечном итоге, по реакции императрицы на эти вопросы (а запротоколировано все, о чем она «изволила рассуждать») мы можем более четко представить себе ее облик, государственный и человеческий.

Изученные нами тома этих протоколов свидетельствуют о том, что императрица Елизавета Петровна отнюдь не была такой уж «неподготовленной к роли правительницы огромного государства» и «ленивой», как утверждают, например, Н. Б. Голиков и Л. Г. Кислягин в своей статье, помещенной в трехтомнике «Очерки русской культуры XVIII века» [7]. Елизавета Петровна весьма активно участвовала в обсуждении буквально всех докладываемых вопросов и «рассуждала» по ним вполне самостоятельно и обоснованно. Это же относится и к вопросам, связанным с перлюстрацией и чтением дипломатической переписки, которые также обязательно регулярно докладывались императрице.

О том, как была организована и действовала служба перлюстрации, можно судить по сохранившейся обширной переписке А. П. Бестужева-Рюмина с Ф. Ашем, которого он назначил на должность почт-директора в Петербурге и кому непосредственно и поручил осуществление перлюстрации дипломатической корреспонденции.

Дело перлюстрации писем оказалось чрезвычайно сложным, требовавшим терпения, внимания и особых навыков, которые приобретались отнюдь не сразу. Конверты следовало вскрывать аккуратно, по возможности не нарушая их целостности. Дипломатическое письмо обычно помещали в конверт, который прошивали ниткой и опечатывали печатями. Так упакованное послание могло вкладываться еще в один конверт, также прошиваемый и опечатываемый.

Вот письмо Ф. Аша А. П. Бестужеву-Рюмину (одно из многих подобных), в котором он описывает трудности, с которыми встречались перлюстраторы:

«Высокородный государственный граф, высокоповелевающий господин государственный вице-канцлер.

Милостивый государь!

29-го числа прошлого месяца купно с приложенною депешею от г-на барона Мардефельда (министр прусского двора в Санкт-Петербурге. — *Т. С.), вчерась пополудни я со всяким респектом получил. И не приминул по силе данного мне милостивейшего приказа оную депешу распечатывать, а в ней нашлось три пакета, а именно первый в придворный почтовый амт в Берлин от г-на барона Мардефельда самого, второй к финанц-советнику Магирусу в Кенигсберг от секретаря Варендорфа, а третий от господина Латдорфа* (работника прусской миссии в Санкт-Петербурге. — *Т. С.) к его брату в Ангальтбернбург. Последние два письма без трудности распечатать было можно, чего ради и копии с них при сем прилагаются. Тако ж де куверт в придворный почтовый амт в Берлин легко было распечатать, однако ж два в оном письма, то есть к королю и в кабинет, такого состояния были, что, хотя всякое удобовымышленное старание прилагалось, однако ж оных для следующих причин отворить невозможно было, а именно: куверты не токмо по углам, но и везде клеем заклеены, и тем клеем обвязанная под кувертом крестом на письмах нитка таким образом утверждена была, что оный клей от пара кипятка, над чем письма я несколько часов держал, никак распуститься и отстать не мог. Да и тот клей, который под печатями находился (кои я хотя искусно снял), однако ж не распустился. Следовательно же я к привеликому моему соболезнованию никакой возможности не нашел оных писем распечатать без совершенного разодрания куверт. И тако я оные паки запечатал и стафету в ея дорогу отправить принужден был...»* [8].

Если вскрывал и запечатывал письма лично почт-директор, то копировал их особый секретарь, переводил же особый переводчик. Так как письмам необходимо было придать их первоначальный вид, то есть заклеить, прошить ниткой и опечатать точно такими же печатями, какими они были опечатаны до вскрытия, то большое значение имело и мастерство человека, изготовлявшего печати. Этот мастер «печатнорезчик» также содержался в штате ведомства Аша. Работа его была тонкая и ответственная, ведь употреблялось великое множество печатей, личных и государственных, которыми дипломаты пользовались при опечатывании своих писем, направляемых в разные адреса. Оттиски таких печатей красного сургуча на старых конвертах от дипломатических писем сохранили тонкую, замысловатую резьбу с изображением фамильных и государственных гербов.

Аш лично проверял все изделия резчика печатей, делал замечания, а затем отправлял готовые образцы для оценки Бестужеву-Рюмину, который давал уже окончательное заключение. На этот предмет велась переписка.

Из письма Аша Бестужеву-Рюмину от 29 февраля 1744 г.: «Печатнорезчик Купи от своей болезни отчасти оправился и уже начало подделыванием некоторых штемпелей учинил, из которых он и сегодня два отдал, но один назад взять принужден был, дабы усмотренное мною в нем погрешение поправить, а другой, который барона Нейгауза (австрийского посла в России. — *Т. С.*) есть, я за нарочитой (подходящий. — *Т. С.*) нахожу и оной при чем посылаю...» [9].

Через несколько дней Бестужев-Рюмин пишет предписание: «Из Государственной коллегии иностранных дел санкт-петербургскому почт-директору господину Ашу.

На рапорт Ваш от 29-го февраля здесь в 6-е марта полученный в резолюцию объявляется... присланная от Вас печать барона Нейгауза при сем возвратно к Вам отправляется, дабы Вы, оную имев, столь меньшим трудом в распечатывании без формы исправляться могли. Рекомендуя, впрочем, резчику Купи оные печати вырезывать с лучшим прилежанием, ибо нынешняя нейгаузова не весьма хорошего мастерства» [10].

Итак, в 1742—1744 гг. резчиком печатей был некто Купи, возможно, француз по национальности. Однако в «Протоколах докладов Ея Императорскому Величеству Елизавете» нами найден и такой любопытный документ:

«В Санкт-Петербурге. 12 февраля 1745 года пополудни при докладе происходило:

...20. При сих же докладах Ея Императорское Величество о потребности в сделании печатей для известного открывания писем рассуждать изволила: что для лучшего содержания сего в секрете весьма надежного человека и ежели возможно было, то лучше из российских такого мастера или резчика приискать, и оного такие печати делать заставить не здесь, в Санкт-Петербурге, дабы не разгласилось, но разве в Москве или около Петербурга, где в отдаленном месте, и к нему особливый караул приставить, а по окончании того дела все инструменты и образцы печатей у того мастера обыскать и отобрать, чтоб ничего у него не осталось, и сверх того присягою его утвердить надобно, дабы никому о том не разглашал» [11].

Как видим, Елизавета внимательно следила за перлюстрацией документов и вникала в подробности ее организации, стремясь максимально защитить государственные интересы. У читателя может возникнуть вопрос: а как же моральный аспект? Можно ли ссылкой на государственные интересы оправдать чтение личной переписки? Конечно, этот вопрос вполне обоснован. И высшие лица государства

это прекрасно понимали, поэтому все, связанное с перлюстрацией, содержалось в глубочайшем секрете. Собственно говоря, именно так обстояло дело и во всех европейских державах, от которых Россия в организации службы перлюстрации отстала почти на два столетия.

Не следует думать, что в XVIII в. перлюстрации в России подвергалась исключительно дипломатическая переписка, а частная корреспонденция была избавлена от этого. Забегая несколько вперед, заметим, что уже при Екатерине II многие государственные и дипломатические деятели в своих письмах писали о вещах, которые могли заинтересовать не столько их адресатов, сколько правительство — так сильна была их уверенность в том, что эти письма будут вскрыты и прочитаны.

Создание дешифровальной службы

Итак, перлюстрированные в «черных кабинетах» письма иностранных дипломатов переводились и докладывались А. П. Бестужеву-Рюмину, а при необходимости и императрице. В этих сохранившихся в архиве переводах часто можно видеть такие пометы в каком-то месте текста: «Далее... страниц цифрами писано было...» Затем переводчик делает пропуск и дает следующий далее текст письма. Таким образом, вначале при перлюстрации писем зашифрованные их части просто пропускали и даже не копировали. Однако постепенно обнаруживается, что самые важные и интересные сведения содержатся, как правило, именно в этих зашифрованных частях писем. Естественным образом возникает настоятельная необходимость их дешифровать, а это значит организовать специальную дешифровальную службу. Сохранившиеся документы позволяют достаточно подробно восстановить связанные с этим события.

Первые успехи российских криптографов в дешифровании иностранных шифров связаны с именем тогда уже известного математика Христиана Гольдбаха (1690—1764).

Родился Х. Гольдбах в Кенигсберге. История приезда в Россию этого немецкого ученого такова. Задуманное и осуществленное Петром I дело реорганизации всей жизни страны не могло, конечно, ограничиться реформами лишь в военной и технической областях. Уже в первые годы своего царствования Петр ощутил огромную потребность России в образованных людях, способных осуществлять его планы, руководить, создаваемыми учреждениями, работать в промышленности и служить в преобразованной армии. Эта потребность вызвала к жизни «цифирные» (математические), а также специальные технические и военные школы. Петр также понимал, что для основательного развития его начинаний России нужна своя развитая наука, нужны ученые. Это понимание привело к созданию в России Академии наук.

24 января 1724 г. последовал императорский указ об организации Академии наук, а при ней — университета и гимназии. При участии немецкого философа и математика Вольфа, с которым Петр длительное время вел переписку относительно развития науки, в Россию были приглашены профессора. В их числе были и математики, подбор которых оказался поразительно удачным. Приехали Герман — ученик Якоба Бернулли, сыновья знаменитого Иоганна Бернулли — Николай и Даниил и, наконец, Христиан Гольдбах. В 1727 г. к ним присоединился один из самых замечательных математиков всех времен Леонард Эйлер.

В России Х. Гольдбах в течение 15 лет (1726—1740) исполнял обязанности конференц-секретаря Академии. Как математик он широко известен классическими трудами по теории чисел и математическому анализу. В первых томах «Коммен-

тариев Петербургской Академии наук» — первом научном российском журнале Гольдбах напечатал ряд статей об интегрировании дифференциального уравнения Риккати, о превращении расходящихся рядов в сходящиеся и другие.

Как известно, Х. Гольдбах с 1729 г. и до конца своих дней работал в тесном контакте с Леонардом Эйлером и вел с ним регулярную переписку. В одном из писем (1742 г.) Гольдбах высказал Эйлеру гипотезу, вошедшую в историю под названием «проблемы Гольдбаха», которая сводится к тому, что всякое целое число, большее или равное шести, может быть представлено в виде суммы трех простых чисел.

Есть основания предположить, что идея привлечь к дешифровальной работе в Коллегии иностранных дел математика, специалиста по теории чисел Х. Гольдбаха принадлежит А. П. Бестужеву-Рюмину.

Сейчас трудно сказать, почему выбор Бестужева-Рюмина пал на Гольдбаха. Возможно, это связано с тем, что по приглашению еще Остермана Гольдбах при дворе исполнял должность одного из воспитателей Петра II. Однако, как показывают дальнейшие события, совершенно очевидно, что Бестужев-Рюмин знал, какого именно профиля специалист необходим был для дешифровальной деятельности. Возможно, он использовал европейский опыт. Так или иначе, именной указ императрицы Елизаветы о назначении Гольдбаха на «особливую должность» датирован 18 марта 1742 г., а дело об этом в архиве МИД озаглавлено «Об определении в Коллегию иностранных дел бывшего при Академии наук профессора юстиц-рата Христиана Гольдбаха статским советником с жалованьем 1500 рублей, о выдаче недоданного ему в Академии наук жалованья и о выдаче ему вперед жалованья» [12].

С этого времени вся дальнейшая жизнь Гольдбаха была связана с дешифровальной службой. Однако успеха в своей деятельности он достиг не сразу, а лишь через год. На полях копии одного из писем барона Нейгауза из числа тех, что датированы июлем 1743 г., имеется надпись: «Разобраны с цифр искусством статского советника Гольдбаха; в цифрах имевшиеся места внесены, для знака линиями подчерчены и прочее малое число еще не разобранных цифров каждая тремя пунктами означены» [13]. Это значит, что в представляемых вице-канцлеру переводах перлюстрированных писем те места, которые дешифрованы, подчеркнуть, чтобы было ясно, какую именно информацию зашифровали. Шетарди, как и другие дипломатические представители, имел несколько шифров для переписки с разными лицами. Разобрав один его шифр, Гольдбах стал работать над другими.

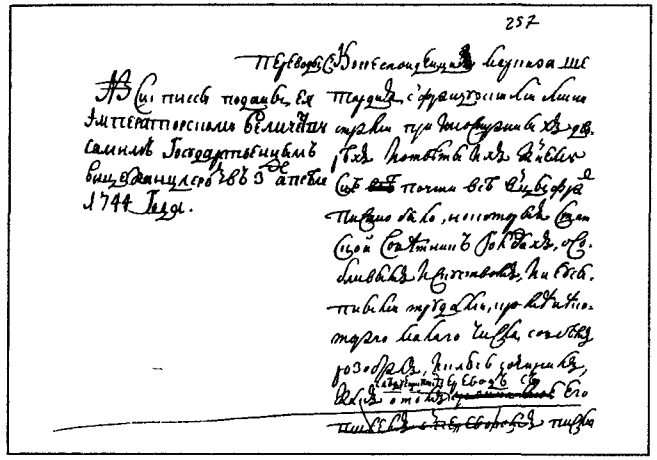
30 июля 1743 г. Гольдбах представил Бестужеву-Рюмину 5 дешифрованных писем, 2 августа — 5 писем, 10 августа — 2 письма, 20 августа — 5 писем, 27 августа — 2 письма, 30 августа — 2 письма... Всего с июля по декабрь 1743 г. им было дешифровано 61 письмо «министров прусского и французского дворов» [14]. Напомним, что это было в 1743 г. В своей книге историк криптографии Д. Кан пишет о том, что первое дешифрованное российскими криптографами письмо было показано Елизавете 16 июня 1744 г. Это было письмо посла Франции маркиза де ля Шетарди, в котором он неуважительно отозвался о русской императрице. Кан говорит о том, что Елизавета, «будучи ослепленной своими симпатиями к Франции, отказалась поверить этому письму, пока оно не было дешифровано в ее присутствии». В реальности дело обстояло иначе. Начиная с Петра Великого, все российские монархи в обязательном порядке имели шифры и вели по ним деловую переписку. Елизавета Петровна не являлась исключением и, более того, вопросам деятельности криптографической службы уделяла большое внимание. Как ука-

зывалось выше, с самого начала работы по перлюстрации корреспонденции иностранных дипломатов Елизавете докладывалось ее содержание канцлером и вице-канцлером, о дешифровальной деятельности Гольдбаха она также была прекрасно осведомлена. В январе 1744 г. с Гольдбахом был перезаключен договор о службе в России именно на основании его успехов в дешифровальной деятельности. Указ подписывала, естественно, Елизавета. Из протоколов докладов Елизавете от 3 января 1744 г.: «...18. Слушать же и всемилостивийше апробовать соизволила проект заключаемого статским советником Гольдбахом о вступлении его в российскую службу контракта. И при том по всеподданнейшему докладу, не соизволено ль будет ему, Гольдбаху, за прилежные его труды и особливое искусство в разбирании цифирных секретных писем в награждение до 1000 рублей пожаловать, Ея Императорское Величество на сие всемилостивийше соизволила» [15].

Что касается Шетарди, то чтение его переписки было лишь очередным этапом в дешифровальной деятельности Гольдбаха, а отнюдь не первым опытом, и потому дешифрованное письмо Шетарди никак не могло «поразить» прекрасно информированную императрицу. Это подтверждает деловая записка того времени:

«Переводы корреспонденции маркиза Шетардия с французскими министрами при иностранных дворах и ответы к нему.

Сие почти все в цифрах писано было, но которые статский советник Гольдбах особливым искусством и неусыпным трудом, кроме некоторого малого числа, соизволил разобрать и ключ сочинить, как о том следующей пиесе перевод с его письма гласит». На полях же рядом с этим текстом написано: «Сии пиесы поданы Ея Императорскому Величеству самим государственным вице-канцлером в 3 апреля 1744 года».



И текст записки далее: «Итако сие уже четвертая цифирь, которую помянутый статский советник разобрал, а именно сперва нейгаузову, потом далионову с французскими министрами при иностранных дворах, да его же с статским секретарем Амелотом и сие, шетардиеву. Понеже он уповает в кратком времени употребляемую и статским секретарем Амелотом и придворную цифирь маркиза Шетардия разобрать...» [16]. Таким образом, можно констатировать, что шифр Шетарди для переписки с другими французскими министрами был четвертым по счету из тех, что раскрыл Гольдбах.

Именно с момента появления Гольдбаха в штатах Коллегии иностранных дел Ашу начинают поступать распоряжения Бестужева-Рюмина тщательно копировать письма целиком, ни в коем случае не опуская в них шифртекста. Не доверяя рядовым копиистам, Бестужев-Рюмин приказал копировать в «черном кабинете» «цифрами писанные» части писем профессору математику Тауберту. По этому поводу Бестужев-Рюмин писал Ашу: «Усмотренные в переписываемых унтер-библиотекарусом Таубертом в цифрах писем неисправность причиною, что я Вам особли-

во рекомендовал, за нужно признать впредь списываемые им копии не токмо в речах, но и в цифрах все нумеры противу оригиналов сходны, с ним сличать и исправность оных прилежно наблюдать, ибо то необходимо потребно... Еще рекомендуется отсюда отходящие за границу иностранных министров письма прилежно рассмотреть и оные все верно списать... и того для не худо когда б и закрепленные иногда пакеты отворить возможно было, к чему благоволите приложить особливое старание» [17] .

И Аш старался, старался изо всех сил. Правда, трудности при этом он испытывал большие. Их он подробно описывал в своих докладах Бестужеву-Рюмину.

Из рапорта почт-директора Аша из Санкт-Петербурга от 29 февраля 1744 г.:

*«...Покорнейше доношу, что я не премину списываемые унтер-библиотекарием Таубертом копии с оригинальными письмами прилежно сличать и находящиеся иногда погрешности в письме или цифири переправлять... Не меньше ж я и пробу хотя делал, возможно ли заклеенные письма вскрыть, не повредя приметным образом куверта. Чего ради я подобно тот куверт сам заклеивал и оно, паки высушедши наперед, паки вскрыть старался, но как без мочения до того достигнуть нельзя, то бумага не токмо зело замаралась, но и со всякою уподобовымышленною субтильностью (*предосторожностью. — *Т. С.) однако ж таким образом вскрыть возможно не было, чтоб оной куверт по некоторым местам не изодрался. И тако по сей мне неудачной пробе заключать можно, что таковые заклеенные куверты без подания о том явных знаков вскрывать нельзя...»* [18].

Х. Гольдбах прекрасно понимал значение своей работы и стремился разъяснить вице-канцлеру ее сложность. Так, в январе 1744 г. он писал Бестужеву-Рюмину:

«Милостивый государь мой!

Принося Вашему сиятельству первые плоды третьяго цифирного ключа, надеюсь, что вместо нарекания мне какого-либо в том медления, паче моей поспешности удивляться причину иметь будут, ежели когда-нибудь соизволено будет сличать самой ключ с разобранными письмами и когда усмотрится, что потребно было каждое число или каждую цифру весьма прилежно свидетельствовать, нежели возможно было познать содержание хотя б одного письма. Но понеже сия работа уже сделана, то я в состоянии нахожусь, в день по одной пиесе разобрав, отдавать, ежели я, однако ж, другими делами от того отторгнут не буду.

Что же касается до четвертого и пятого ключей, от которого я еще несколько штук [писем] в руках имею, то оныя ключи несравненно труднее первых нахожу...» [19].

Сохранились раскрытые Гольдбахом и написанные его собственной рукой ключи к шифрам Нейгауза, Далиона, Вахмейстера, Кастеляна, Шетарди...

Надо ли было объяснять значение этой работы Бестужеву-Рюмину? Думаем, что нет. Он понимал ее важность и многочисленные вытекающие из этого последствия лучше, чем кто-либо. Почему же Гольдбах говорит в своем письме о том, что его работу вице-канцлер может считать слишком медленной? Для этого у него были основания. Бестужев-Рюмин конечно же торопил математика. И дело было прежде всего в том, что он сам лично был заинтересован в скорейшем получении дешифрованных текстов писем французских министров и, в частности, маркиза де ла Шетарди.

К середине XVIII в. дипломатические отношения России с Францией уже насчитывали около полутора столетий. Началом этих отношений можно считать приезд в Россию чрезвычайного посла

короля Людовика XIII. Постоянное французское посольство было учреждено в России с 1702 г. В 30-е годы XVIII столетия версальский кабинет назначил своим представителем в России маркиза де ла Шетарди, бывшего до того времени французским послом в Берлине. Деятельность этого дипломата оставила заметный и далеко не самый светлый след в истории русско-французских отношений. Исчезнув на некоторое время из России после восшествия на престол Елизаветы Петровны, в 1743 г. Шетарди вновь появился в Петербурге в качестве полномочного посла. Главной целью его деятельности было воспрепятствовать России сблизиться с Англией и Австрией, что означало бы ослабление отношений России с Францией. Для достижения этой цели Шетарди старался использовать любые возможные средства, включая и далеко не благовидные.

Являясь проводником политики, ориентированной на создание сильной независимой России, что связывалось в то время, в частности, с отходом от Франции и Пруссии и с усилением союза с Англией, вице-канцлер Бестужев-Рюмин был крайне неугоден французскому двору. Шетарди писал об этом в своих письмах весьма откровенно. Вот дешифрованный текст одного из них от мая 1744 г:

«Царица по индифирентности ее о делах привыкшая по мнениям вице-канцлеровым поступать, ему одному милость свою присвоила. То истинно есть, чтоб он тогда по оказании уже к нам довольно явственно своего недоброжелательства, всевозможные затруднения изыскал, дабы всякое согласие между Францией и Россиею отдалить» [20].

Против Бестужева-Рюмина французскими министрами проводилась большая клеветническая кампания, сопровождавшаяся тайными заговорами. Французы стремились как могли навредить вице-канцлеру,

они сумели удалить от двора его брата и единомышленника Михаила, во многом способствовали отправке в ссылку жены вице-канцлера, обвиненной в государственной измене.

Шетарди писал в шифрованном письме от 4 февраля 1744 г.: «Отдаление его брата его истинной помощи лишает. Мы и не одни, которые его, вице-канцлера, низвержения ищем: король прусский по меньшей мере тако же, как и мы оное видеть желает» [21].

Из письма Шетарди от 24 декабря 1743 г. королевскому казначею Монтартелю:

«...Еще не могу Вам о другом обстоятельстве, касающемся графа Бестужева — прежде бывшего обер-маршала и брата вице-канцлера, — таким образом сообщить, что неизвестность о его определении ныне уже миновалась, ибо Ея Величество Всероссийская, торжествуя в прошлое воскресенье день своего рождения, оного Бестужева своим полномочным министром в Берлин на место графа Чернышева назначить изволила» [22].

Днем раньше, 23 декабря 1743 г., вице-канцлер А. П. Бестужев-Рюмин пишет императрице Елизавете Петровне «просительное письмо», в котором просит защитить его от «мерзких нареканий и клеветы со стороны французских министров Далиона и маркиза Ланмари, их секретаря Мондамера, а также от тайного советника Лестока, генерал-прокурора князя Трубецкого и от голштинского обер-маршала Бриммера». При этом Бестужев-Рюмин прилагает выдержки из шифрованных писем указанных министров, а также из письма польского короля его резиденту Пецольду и английского министра Вейча тайному советнику Бреверну. Нам бы также хотелось привести их здесь.

Из письма французского посла в Стокгольме Ланмари Далиону в Санкт-Петербург 7 июля 1743 г.:

«Пока Бестужевы здешним двором править будут, мы никогда ничего доброго при них не достигнем, то

Ваше Превосходительство можете надежны быть, что я ничего во свете не пожалею для ссажения оных с высоты их великости».

30 июля 1743 г. Далион отвечал Ланмари:

«Мы здесь в весьма сильных движениях находимся, и я уже приближаюсь к тому моменту с долгою отдышкою увеселением насыщаться Бестужевых погубить или свергнуть... Сии два брата уже столько на своем счете имеют, что уже можно всякое совестное сомнение на сторону отложить, одним словом сказать, господа Бриммер и Лесток меня твердо обнадежили, что сие дело не совершенным оставлено не будет... И Вы, мой господин, можете уверены быть, что я прилежно тому следовать буду».

Еще Далион писал Ланмари 9 августа 1743 г.:

«В письмах обер-маршала Бестужева ничего ни против России, ни же персонально против царицы не имеется, но, невзирая на то, твердо постановлено, что как он, так и его брат чинов их лишены будут и от двора отдалены будут... Погубление сих людей таким для меня пунктом есть, который я ни на минуту из глаз не выпущу. Господа Бриммер, Лесток и генерал-прокурор Трубецкой, яко равномерно же в том интересованные, тем не меньше моего себя упражняют»...

Выписка из письма к английскому министру в России Вейчу из Лондона от милорда Картерста и из Стокгольма от английского министра там:

«Отправленные в Санкт-Петербург депутаты шведские от нынешнего министерства инструктированы: вначале через знатные оферты и великие обещания господ Бестужевых склонить к вступлению во французские виды, но ежели усмотрят, что сим способом в намерении своем успеха получить не могут, то всякие удобовымышленные интриги и до ста тысяч рублей, которые Франция заплатить хочет, употреблять имеют для повреждения сих министров...» [23].

Как говорится, комментарии тут излишни. Война против Бестужева-Рюмина велась не на жизнь, а на смерть. Для достижения своей цели французские министры образуют «заговорщицкий» союз с прусским послом бароном Мардефельдом. Вместе они стремятся найти себе союзницу в лице ангельдтцербстской принцессы.

*«Она за оказанную ей от барона Мардефельда и меня атенцию (*внимание. — *Т. С.), — писал Шетарди, — что мы ее здесь дожидались, и за толь ей потребную помощь, которую та потому в нас нашла, весьма особливое свое удовольствие засвидетельствовала...»* [24].

Для достижения своих целей Шетарди использует и подкуп различных лиц при российском дворе:

«Всемерно потребно, чтоб его величество король, апробуя то, что я к назначенному господину Лестоку подарку еще две ж тысячи рублей более присовокупил. На мою ревность к службе его в употреблении поручаемых мне здесь денег совершенно положиться изволил, да и подлинно, как я наперед объявить могу, кому я больше или меньше дам, потому что все от случаев зависит»,— писал он в одном из писем [25].

Шетарди выбирает в качестве своих осведомителей близких к императрице людей, в том числе и придворных дам, предлагая давать им регулярно взятки в виде «пенсий»: «Который их пенсионеров предпочтительнее есть, потому что сии пенсии тем персонам, о которых старание прилагается на нашу сторону преклонить, более прибавляется [денег]... Ту даму пенсиею по тысяче двести рублей ... я за потребно признал. К тому еще тысячу рублей прибавить той персоне я за благо рассужу, у которой господин Далион

на квартире стоял, о которой он Вам доносил, что весьма важно ей пенсию давать, оную шестьюстами рублями умножить...» От оплачиваемых им лиц Шетарди стремится получить наиболее полные сведения о российском дворе, включая самые сокровенные. И для этого он настойчиво и продуманно расставляет сети: «Дабы о том, что в сердце царицыном делается, сведать или паче ее суеверными предупредительными мнениями пользоваться, то всемерно и существительно потребно есть ее духовника и тех архиереев, которые Синод сочиняют, подкупить... В таком случае, каковы бы велики или малы издержки ни были, об оных сожалеть не надобно» [26].

И вот такого содержания письма попали в руки Бестужева-Рюмина. Понимая, что он борется за государственные российские интересы и одновременно за собственную жизнь, он пишет яростные письма Ашу, требуя от него вскрывать и перлюстрировать абсолютно всю корреспонденцию интересующих его министров соответствующих иностранных государств.

Гольдбах продолжает трудиться. Дешифруя переписку Шетарди, он стремится раскрывать все новые ключи. 20 марта 1744 г. он пишет Бестужеву-Рюмину: «Понеже я в четвертой цифири (шифре Шетарди для переписки с другими французскими министрами. — *Т. С.*) успех возымел, того ради я в состоянии буду Вашему сиятельству не токмо по пиесе на день из тех, которые Вы мне прислали, имею возвращать, но как скоро токмо Вы мне приказать изволите и цифирный ключ вручить, способом которого каждому, который по-французски разумеет, все, написанные той же цифирью пиесы дешифровать весьма легко сможет... В настоящее время я занимаюсь пятой цифирью, которая по своему виду гораздо важнее пиесы откроет. Но всепокорно Ваше сиятельство прошу мне по меньшей мере две недели сроку дать, дабы я себя в состояние привесть мог Вам такой опыт представить, который бы Вашей апробации достоин был. Вашему сиятельству существо подобного труда весьма известно, дабы мне сего дозволить, в которое я все свое возможное прилежание приложу, дабы Ваше сиятельство о моем безмерном желании повелением Вашим удовольствие показать...» [27].

Совершенно очевидно, что к этому периоду своей работы по дешифрованию секретной переписки Гольдбах выработал систему приемов и методов, которые позволяли ему добиваться успеха в столь короткий (две недели!) срок. Напомним, что раскрытие первых шифров у него потребовало значительно большего времени, а именно целого года.

Работа Гольдбаха на поприще дешифрования не оставалась без внимания и высоко ценилась императрицей. В 1744 г. она дает указание о выдаче ему впредь годового жалованья в 2000 рублей из статс-конторы. В 1760 г. Гольдбах был пожалован в тайные советники с ежегодным жалованьем в 4500 рублей. Это было одно из самых высоких званий в российском государстве, и награждались им дворяне за особые заслуги перед Отечеством. Заметим, кстати, что Леонарду Эйлеру, несмотря на его выдающиеся научные достижения и постоянное покровительство со стороны российского двора, указанное звание так и не было пожаловано. «Тайных советников у меня много, а Эйлер один», — так обычно отшучивалась императрица на прошения о пожаловании Эйлеру этого титула. Шутка шуткой, но не будем забывать, что принадлежала она императрице, которая, конечно же, знала, что делала.

Итак, приведенные документы достаточно подробно обрисовывают историческую картину, содержащую последовательность событий, связанных с первыми в России опытами по дешифрованию иностранной секретной корреспонденции. Они же свидетельствуют о колоссальном политическом значе-

нии этого научного достижения для российского государства. Императрица Елизавета и ее кабинет, возглавляемый А. П. Бестужевым-Рюминым, сразу же стали активно использовать получаемую информацию для проведения своей внешней и внутренней политики. Вот лишь один пример.

14 февраля 1744 г. в протоколах докладов императрице записано, что в тот день ей был подан «экстракт из письма от французского министра Ланмари из Стокгольма от 5 (16) июля 1743 г. в Санкт-Петербург к французскому же министру Далиону. Да из письма ж от него Далиона к французскому в Копенгагене министру Лемеру от 12 августа того ж года, писанного со учиненными при том ремарками для высочайшего Ея Императорского Величества усмотрения, каким образом от французского двора нынешние у Швеции с Данией дела в повреждение голштинскому дому интересов проектированы и как чаятельно потому оные и производятся. Который экстракт у себя Ея Императорское Величество оставить изволила».

А уже через неделю, 22 февраля, при докладе Елизавета «объявить изволила, что обретающемуся в Швеции российскому помощному корпусу до того времени тамо прибыть за благо рассужено, пока между Данией и Швецией нынешние несогласия без предосуждения голштинского дома интересов совершенно прекращены не будут, и что Ея Императорское Величество никогда от защищения интересов сего дому и восприемлемого в том участия отступить не соизволит и для написания такой резолюции соизволила ее императорское величество оное от собрания поданное рассуждение вице-канцлеру отдать».

Судя по этим документам, можно заключить, что успехи в дешифровании иностранных шифров раскрыли перед правительством России возможность получения «дополнительного знания», которое дало совершенно иное наполнение его политической деятельности.

Собрав достаточно материалов против Шетарди, Бестужев-Рюмин перешел к решительным действиям. Сохранилось его письмо к графу Михайлу Илларионовичу Воронцову от 3 апреля 1744 г. Вот его текст:

«Месье, включенный пакет с двумя известного автора письмами при удобном случае Ея Императорскому Величеству поднести всепокорно прошу. Из которого никогда чаятельную жестокую предерзость, что ни иным чем письма свои зачинает, как токмо оскорблением Величества всевысочайше усмотреть соизволит... Весьма нужно есть надлежащие рефлексии и благовременные предупредительные меры восприять. Ибо оный автор, как письма его явствуют, не токмо мужеска и женска полу подкупил и что у его сообщников адгеренты имеются, но уже и духовенство (по удачливости одному его конфиденту) подкупить старается. Не клонится ли сочиненный его план по отъезде Ея Императорского Величества в Киев какое зло учинить. Я о том ни рассуждать, ни что-либо присоветовать не в состоянци, дабы мне, яко обиженному, не причтено было в какое пристрастие. Того ради поручаю Вашему Превосходительству, яко Ея Императорского Величества верному рабу и сыну Отечества, по присяжной Вашей должности о чистой совести как пред ведущим ответ дать можете для предосторожности всевысочайшей славы, чести и интересу, яко же благополучия и целости любезного нашего Отечества принадлежащие, со всякою откровенностью Ея Императорскому Величеству представления всеподданнейше учинить. Ибо все оное в молчании оставить пред богом и пред Ея Императорским Величеством безответно будет...» [28].

О том, что было дальше, нам рассказывает Д. Кан: «Посол Франции де ла Шетарди определенно знал, что русские вскрывают его корреспонденцию. Одна-

ко текст его писем был зашифрован и, как все дипломаты, он чувствовал себя в безопасности, так как был уверен, что русские слишком глупы, чтобы вскрыть его шифр... В письме домой он неуважительно отозвался о царице, написав, что она «полностью находится во власти своих прихотей» и что она является «довольно фривольной и распутной женщиной»... Письмо было показано Елизавете. На следующий день, 17 июня 1744 г., когда Шетарди прибыл в свою резиденцию, ему была вручена нота, в соответствии с которой он должен был в течение 24 часов покинуть пределы России. Он заявил протест. Тогда русские стали зачитывать ему его же собственные письма. «Достаточно»,— сказал он и начал упаковывать свои вещи. Однако приведенные нами выше материалы показывают, что Кан во многом ошибся. Русской императрице дешифрованная переписка иностранных министров, в том числе и переписка Шетарди, начала докладываться задолго до июня 1744 г., с того самого времени, как первых успехов добился Гольдбах. По этой же причине Елизавета никак не могла не поверить информации о содержании переписки Шетарди и потребовать ее дешифрования в своем присутствии. Что же касается «глупости русских», о которой писал Шетарди, да и Кан, то оставим это утверждение на их совести и просто улыбнемся. Не так ли, читатель?

Что же касается интересующего нас предмета, то зададимся вопросом, был ли привлечен к дешифровальной работе помимо Гольдбаха другой крупнейший математик, работавший в России одновременно с ним, — великий Леонард Эйлер? Знал ли Эйлер о работе Гольдбаха? Как известно, Эйлер был приглашен в Россию в Академию наук в 1726 г., и к 1742 г. уже пятнадцать лет жил и работал здесь. При этом он неоднократно доказывал свою преданность императрице и российским интересам. С Гольдбахом Эйлер состоял в дружественной и научной переписке. Именно в одном из писем Эйлеру Гольдбах сформулировал свою знаменитую проблему, получившую впоследствии его имя. И все же мы считаем, что на интересующий нас вопрос следует ответить отрицательно, исходя из следующего. Во-первых, насколько нам известно, в архивах не сохранилось документов, которые прямо или косвенно подтверждали участие Эйлера в дешифровальной работе. Ни в одном из писем из переписки Эйлера и Гольдбаха нет и намека на какие-либо аспекты криптографической деятельности. Это свидетельствует о том, что Гольдбах тщательно сохранял в тайне свою работу на особливой должности в Коллегии иностранных дел. Во-вторых, можно привести следующий любопытный случай, свидетельствующий о том, что по крайней мере до 1744 г. Эйлер не имел никакого понятия о криптографическом анализе и криптографической стойкости даже простейших шифров. В 1744 г. Эйлер послал одному из своих друзей письмо-криптограмму, в которой было несколько омофонов (некоторые буквы имели несколько шифробозначений), выразив при этом уверенность, что дешифровать такое письмо невозможно. Это свидетельствует о том, что в криптографических вопросах он был даже наивнее большинства изобретателей шифров-самоучек. В то же время нам удалось найти документы, из которых следует, что один из сыновей Эйлера, Иван Эйлер, работал в секретной экспедиции Коллегии иностранных дел и составлял шифры. На некоторых из них сохранилось его имя.

Какие же последствия имела история с Шетарди? Французские послы были отозваны, и, таким образом, к середине XVIII в. отношения между Россией и Францией оказались весьма прохладными. Францию такое положение дел явно не устраивало. Она искала союза с Россией и Австрией для противодействия усиливающейся с каждым годом Пруссии, вступившей в союз с Англией. Англия, в свою оче-

редь, вела упорную борьбу против Франции за колониальное и морское преобладание.

Людовик XV, опасаясь официально предложить возобновить дипломатические отношения с Россией и обменяться послами из-за возможного отказа, что нанесло бы урон престижу французского двора, послал в Петербург послов тайных — шотландского дворянина Дугласа-Маккензи с якобы его племянницей, роль которой играл некий шевалье д'Эон де Бомон.

Ближайшим советником французского короля в российских делах выступал принц Конти, происходивший из рода Конде, который вел свое начало от младшей линии бурбонского дома и, следовательно, считался родственным королевской династии. Принц имел виды на польскую корону и поэтому был лично заинтересован в том, чтобы иметь в Петербурге, где главным образом должна была происходить развязка каждого возникавшего в Польше вопроса, преданных людей.

В 1866 г. в Париже тогдашним начальником императорских архивов Бутариком была издана секретная дипломатическая переписка короля Людовика XV. Эта переписка, которая охватывает двадцатилетний период, содержит материалы о том, что, по заведенному обычаю, по воскресеньям лица, управлявшие почтовой частью, сообщали королю все сведения, почерпнутые ими в «черном кабинете», где, как мы знаем, благонадежные чиновники занимались перлюстрацией корреспонденции. Проявляя интерес к чужим секретам, Людовик XV тайны своей дипломатической переписки стремился сохранить, скрывая ее даже от своих министров. У короля всюду были свои собственные корреспонденты, с которыми он переписывался сам.

Именно принц Конти в течение двенадцати лет заведовал секретной перепиской короля, причем лицам, получившим право вести такую переписку, заявлялось, чтобы они всегда считали ее главным для

себя руководством, а предписания министров — делом второстепенным.

Преподанные русскими уроки дешифрования переписки Шетарди не прошли для французов даром. Посланцы Людовика XV по приезде в Петербург были буквально нашпигованы шифрами и тайными бумагами. Самому Дугласу разрешалось отправить в Париж только одно шифрованное письмо. При этом он должен был перед шифрованием закодировать сообщение с помощью жаргонного кода. Поскольку по заготовленной заранее «легенде» Дуглас приехал в Россию как торговец мехами, то ему необходимо было интересоваться в первую очередь этим видом коммерции. Соответственно и шифр был составлен с учетом этого обстоятельства. Так, его условный код содержал такие замены: усиление влияния австрийцев обозначалось как «рысь в цене», где канцлер А. П. Бестужев-Рюмин был «рысью», ослабление влияния австрийцев кодировалось как «соболь падает в цене», «чернобурой лисицей» именовался посол Англии в России Вильямс Генбюри, выражение «горностай в ходу» означало усиление противников австрийской партии. Ключ от шифра де Бомон прятал в подошве собственного башмака. Уже в период пребывания французских агентов в Петербурге в силу определенных обстоятельств Конти отказался от дел и, согласно воле короля, передал все корреспонденции и шифры старшему королевскому секретарю по иностранным делам Терсье, с которым и привелось д'Эону вести большую часть секретной переписки из Петербурга.

При отправлении французских агентов в Петербург им было дано задание ознакомиться с внутренним положением России, с состоянием ее армии и флота, с ходом русской торговли, с расположением различных партий и отдельных придворных лиц к императрице. Особенно французов интересовал вопрос о степени доверия, каким пользовались у импе-

ратрицы канцлер Бестужев-Рюмин и вице-канцлер Воронцов, о фаворитах императрицы и о том влиянии, какое они имеют на министров. Некоторые задания касались специально д'Эона. Ему, в частности, поручалось войти в непосредственные отношения с самой Елизаветой Петровной и попытаться установить прямую корреспонденцию между ней и Людовиком XV. Отправляя д'Эона в Петербург, и король и принц рассчитывали прежде всего на помощь со стороны русского вице-канцлера М. И. Воронцова, обнаруживавшего, в противоположность А. П. Бестужеву-Рюмину, свои постоянные симпатии к французскому двору. Ему первому представилась «девица» д'Эон как племянница кавалера Дугласа.

Миссия Дугласа и д'Эона де Бомона завершилась успешно и больше всего потому, что у самих руководителей русской политики появились основания для сближения с Францией. Д'Эон успел до такой степени расположить русскую императрицу в пользу французского короля, что она написала Людовику XV самое дружелюбное письмо, изъявляя желание насчет посылки в Россию из Франции официального дипломатического агента. Вскоре французским поверенным в делах при русском дворе был назначен кавалер Дуглас, а д'Эон, в звании секретаря посольства, был дан ему в помощники.

В 1757 г. в Петербург прибыл официальный посол Франции маршал де Л'Опиталь. Однако д'Эон продолжал выполнять свою секретную миссию. Тому есть документальные подтверждения. В опубликованном в свое время седьмом томе Архива графа Воронцова имеются письма к нему Терсье. В одном из этих писем, от 15 сентября 1758 г., Терсье просит Воронцова призвать к себе д'Эона и сжечь в его присутствии как прежнее письмо Терсье, «купно с приложенными двумя цифирными ключами, так и сие, дабы он мог о том меня уведомить. Именем королевским наперед сего сообщенное Вам есть собственно

его секрет, и Его Величество не сомневается, что Ваше сиятельство оной так свято хранили, как я вас о том просил. Я прошу господина д'Эона, чтоб он ко мне отписал о том, что Вашему сиятельству по сему учинить угодно будет». В то же время в письме д'Эону от 16 сентября Терсье писал, что секретная переписка его с Воронцовым относилась к Курляндским делам, но что теперь дальнейшее ее ведение бесполезно, так как «господин граф Брюл негоциацию в России производит, чтобы герцогство курляндское дано было саксонцу принцу Карлу» [29].

Более чем через двадцать лет после этого, в 1779 г., д'Эон, который много лет состоял тайным агентом короля, но к тому времени потерял его доверие, вознамерился предать огласке секретную переписку Людовика XV. Король потребовал от д'Эона выдачи находившихся у него секретных бумаг. Д'Эон упорствовал. Для переговоров с ним в Лондон, где пребывал бывший тайный агент, направили знаменитого писателя Бомарше. После многих скандалов, получивших широкую огласку, д'Эон, за условленное денежное вознаграждение, согласился выдать Бомарше секретные бумаги.

В том же 1779 г. в своем письме к министру иностранных дел Франции графу Верженю д'Эон поведал ему обстоятельства передачи секретных документов Бомарше. При этом он подробно рассказал о переданной им в том числе книге Монтескье «L'Espit des Lois». Переплет этой книги состоял из двух картонных листов, между которыми были вложены секретные бумаги. Картон переплета был обтянут телячьей кожей, края которой подклеили бумагой с мраморным узором. Переплетенную таким образом книгу положили на сутки под пресс, после чего переплет получил такую плотность, что никакой переплетчик не в состоянии был догадаться, что между картонными листами заделаны бумаги. Именно в таком виде сочинение Монтескье было вручено

д'Эону для передачи императрице Елизавете Петровне секретных писем Людовика XV и секретной цифирной азбуки, при посредстве которой она и ее вице-канцлер граф Воронцов могли без ведома французских министров и посланника вести секретную переписку с королем. В переплет же книги была заделана другая цифирная азбука для переписки д'Эона с принцем Конти и Терсье. Когда же принц Конти удалился от дел, то д'Эон, находясь в Петербурге, получил новые шифры, один исключительно для переписки с королем, Терсье и графом Брольи (второе лицо, ведавшее секретной перепиской короля), а другой — для переписки с императрицей Елизаветой Петровной и графом Воронцовым. При этом д'Эону строжайшим образом внушалось, чтобы он хранил вверенные ему тайны как от версальских министров, так и от маршала де л'Опиталя.

В то же время Бестужев-Рюмин зорко следил за тем, чтобы официальная дипломатическая переписка французских дипломатов контролировалась. Вследствие этого Дуглас был вынужден покинуть Россию.

Кстати, именно с д'Эоном связана история с так называемым завещанием Петра Великого. Как известно, на Западе в 1812 г. во время войны с Наполеоном был опубликован текст некого «документа», который якобы являлся «Завещанием» императора Петра I, в котором излагалась фантастическая программа русского завоевания всей Европы и Азии. С тех пор на протяжении многих десятилетий, включая годы Второй мировой войны и послевоенное время, этот «документ» использовался дипломатией и публицистикой тех держав, которые находились во враждебных отношениях с Россией. Объективная научная экспертиза уже давно сделала заключение, что это фальшивка, что подобный документ не исходил и не мог исходить от Петра. Роль д'Эона в ее появлении состоит в том, как следует из его в свое время изданных мемуаров, что во время пребывания в русской столице он сумел похитить из секретного императорского архива в Петербурге копию завещания Петра I.

В конце XVIII в. дешифровальная служба России свободно читала французскую дипломатическую переписку. Этот результат был получен при сочетании аналитических методов раскрытия шифров, которыми пользовалась криптографическая служба, и работы агентов русской разведки, добывавших французские шифры. Российское посольство через секретаря посольства Мешкова завербовало к себе на службу в качестве секретного агента одного из чиновников Министерства иностранных дел Франции. Таким путем русский посол во Франции барон Смолин получал и пересылал в Петербург шифры и ключи к ним, которыми пользовались в своей переписке министр иностранных дел Франции граф Монморси и французский поверенный в делах в России Жене [30]. В результате Россия получала подробную разведывательную информацию в течение длительного периода, даже после того, как Смолин вынужден был покинуть революционную столицу Франции после неудачной попытки помочь увезти Людовика XVI из Парижа.

Глава шестая

НА СЛУЖБЕ ОТЕЧЕСТВУ, НАУКЕ И КРИПТОГРАФИИ

Франц Ульрих Эпинус

Успешная работа дешифровальной службы России XVIII в. связана с именем еще одного ученого — в свое время известного физика и математика Франца Ульриха Теодора Эпинуса (1724—1802). Эпинус вошел в историю науки своими трудами в области электричества и магнетизма. Он первым дал математическую трактовку электрических и магнитных явлений. Член Петербургской Академии наук (с 1756 года) Эпинус был привлечен к дешифровальной работе графом Н. И. Паниным. Руководитель Коллегии иностранных дел, по-видимому, учитывая успешный опыт работы на этом поприще Гольдбаха, после смерти последнего в 1764 г. решил продолжить традицию сотрудничества Коллегии с подобным же ученым. В 1769 г. Эпинус был «пожалован статским советником и определен при Коллегии иностранных дел при особливой должности». За успешную работу на поприще дешифрования в 1773 г. он получает чин действительного статского советника. Эпинус почти всю свою жизнь провел в России, которая стала для ученого вторым Отечеством. Он уехал в Дерпт лишь в 1798 г., за несколько лет до смерти. Все годы, проведенные в России, Эпинус посвятил преданному служению интересам Российского государства, развитию науки.

С именем Эпинуса связано начало сотрудничества Российской Академии наук с зарубежными академиями, в том числе с учеными Соединенных Штатов Америки. Так, к шестидесятым годам XVIII столетия относятся первые усилия американских ученых установить связи с коллегами в России. В 1765—1766 гг. Э. Стайлс и Б. Франклин предприняли попытку завязать научную переписку с М. В. Ломоносовым, И. А. Брауном и Ф. У. Т. Эпинусом.

Научный труд выдающегося политического деятеля и дипломата физика Бенджамина Франклина «Опыты и наблюдения над электричеством» вызвал в России восторженные отклики. В 1752 г. М. В. Ломоносов писал: «Внезапно чудный слух по всем странам течет, что от громовых стрел опасности уж нет» и высказал уверенность в том, что отныне можно отвести от «храмин наших гром» [1]. В России был проявлен огромный интерес к изучению электричества. В 1753 г. Академия наук по предложению М. В. Ломоносова обратилась к ученому миру с задачей: «Сыскать подлинной электрической силы причину и составить точную ея теорию». В трактате «Теория электричества и магнетизма», посвященном К. Разумовскому, Ф. Эпинус выражал уверенность в том, что с помощью электрической силы, «после того, как она будет в достаточной мере исследована, можно надеяться когда-либо раскрыть тайны самой природы» [2]. В этом трактате Ф. Эпинус дал количественную теорию электричества. Трактат высоко оценивали А. Вольта, Г. Кавендиш, П. Лаплас, Ш. Кулон. Эпинус разделял основные положения теории Б. Франклина, впервые перенесшего в 1751 г. в область электричества ньютоновскую концепцию «притягательных» и «отталкивательных» сил. Эпинус существенно продвинул эту теорию, снабдив ее количественным анализом. Он, как

и Франклин, считал, что электрические явления порождаются особой электрической жидкостью, частицы которой обладают способностью взаимоотталкивания. На одних принципах с теорией электричества строит Эпинус и теорию магнетизма. Сходство электричества и магнетизма он подтверждал опытами с турмалином, в которых впервые открыл дипольный эффект у наэлектризованных тел (существование у них двух полюсов, аналогичных полюсам магнитов). Закон взаимодействия электрических зарядов и магнитных полюсов подобен, по Эпинусу, гравитационному закону Ньютона.

О знакомстве Б. Франклина с работами Эпинуса свидетельствует его переписка. Так, в письме Стайлсу от 29 мая 1763 г. Франклин описывал эксперименты русских ученых по изучению воздействия сильного охлаждения на некоторые металлы, в том числе и ртуть. При этом он упоминал труд Эпинуса «Tentamen Theoriae Electricitatis et Magnetismi». Франклин отмечал, что Эпинус применил разработанную им самим теорию электричества для объяснения различных явлений магнетизма «с немалым успехом». Он сообщал Стайлсу, что может переслать через него работу Эпинуса, которая, вероятно, прилагалась к письму Стайлса, профессору Уинтропу из Гарвардского колледжа. В письме Стайлсу от 21 февраля 1764 г. Уинтроп писал, что возвращает работу Эпинуса о магнетизме и электричестве. Уинтроп называл Эпинуса «человеком светлой мысли, широкого пытливого ума, работа которого проливает новый свет на теорию магнетизма» [3].

Б. Франклин и Эпинус в течение многих лет поддерживали научную переписку. Несмотря на то что она частично уже была опубликована, мы не можем отказать себе в удовольствии познакомить здесь читателя с текстами двух сохранившихся писем. Эти письма свидетельствуют о высоких человеческих и моральных качествах двух выдающихся ученых. Они

наполнены искренней доброжелательностью, глубочайшим уважением к труду коллеги, научным бескорыстием.

Первое письмо принадлежит Б. Франклину. Написано оно в Лондоне, датировано 6 июня 1766 г. и адресовано члену Петербургской Академии наук Ф. У. Т. Эпинусу:

«Сэр. Когда я в первый раз был в Америке, я получил там вашу прекрасную работу о теориях электричества и магнетизма, которую, как я понял, вы удостоили чести послать мне. Я прочитал ее с бесконечным удовлетворением и удовольствием и прошу Вас принять мою величайшую благодарность и признательность, которые Вы по праву заслужили от всего ученого мира. Вместе с этим письмом я беру на себя смелость послать Вам свою небольшую работу, которая еще не опубликована, но должна появиться в очередном томе «Трудов королевского общества». Пожалуйста, примите ее как скромное свидетельство огромного уважения и почтения, с каким я, сэр, являюсь...» [4].

Второе письмо написал Б. Франклину Эпинус. Было это значительно позже, через семнадцать лет, в тот период, когда многолетняя борьба за независимость Североамериканских Соединенных Штатов увенчалась успехом и при активном участии Бенджамина Франклина в 1783 г. был заключен Версальский мирный договор, в соответствии с которым Великобритания признала независимость США.

В этом письме Эпинус формулирует свое научное и общественное кредо, пишет о величайшем в жизни предназначении — служении своему Отечеству:

«С.-Петербург. 1 [12] февраля 1783 г.

Милостивый государь.

Вы, без сомнения, простите мне ту поспешность, с какой я, пользуясь представившимся случаем — полученным здесь на днях важным известием [5], чтобы

напомнить Вам о себе: Ваша память всегда будет мне так же дорога, как было дорого одобрение, которым Вы в свое время соблаговолили удостоить мои труды на благо науки.

Я имею честь поздравить Вас, м-вый г-рь, не столько с тем, что потомки не перестанут с уважением и восхищением повторять Ваше имя: ведь для людей, подобных Вам, это не так уж важно, ибо то, что называют славой, не служит для них побудительным мотивом. Чтобы добиться поразительного результата, субстанция, обладающая собственным весом, не нуждается, как ружейная пуля, в дополнительном импульсе от сжатых паров, который придал бы ей некую скорость, способную в известной мере компенсировать ограниченность или, скорее, отсутствие собственной энергии и первоначального веса. Если я считаю уместным поздравить Вас, м-вый г-рь, то делаю это потому, что Вы имеете основания испытывать ныне искреннюю радость, будучи вправе сказать себе, что начали предначертанный Вам Провидением путь, пролив ослепительный и неожиданный свет на область человеческих знаний, занимающуюся раскрытием сил и законов, с помощью которых Всевышний управляет своим вечным и необъятным творением, одухотворяя его, а завершили эту блестящую карьеру, добыв и обеспечив свободу Вашей родной стране, — событие, благотворное воздействие которого на весь род человеческий будет сказываться и в грядущих веках.

С самыми искренними пожеланиями постоянного благополучия и с самым подлинным неизменным уважением имею честь ...

Эпинус

действительный статский советник Коллегии иностранных дел» [6].

Направленность политической деятельности Б. Франклина была особенно понятна и близка Ф. Эпинусу в связи с тем, что сам он принимал участие в разработке декларации о вооруженном нейтралитете, имевшей целью защиту нейтральной торговли от насильственных действий английского флота в войне Англии с боровшимися за свою независимость ее североамериканскими колониями и с примкнувшими к ним Францией и Испанией. Отклонив попытку Англии использовать русские силы в войне с ее колониями в Северной Америке, Россия оказала Северной Америке определенное содействие в борьбе за независимость.

Высокая духовность освещала жизнь и деятельность Эпинуса, ученых его типа. В его письмах, его трудах присутствуют следы некоего озарения, которое содержат сочинения древних философов всех времен и народов, песни великих поэтов, проповеди пророков. Лейтмотивом жизни Эпинуса и, естественно, всей его деятельности являлось глубокое понимание единства с окружающим миром, великой гармонии жизни, постижение истинного смысла человеческого существования, его высшего предназначения. Это понимание в свою очередь шло от широкой эрудиции, обширных, поистине энциклопедических познаний в различных областях науки, религии, философии.

Достоин всяческого уважения бескорыстный, движимый великой идеей познания истины труд всякого ученого. Но труд ученого, сумевшего передать свои знания, свои идеи ученикам, труд ученого, осознавшего важность подготовки научных кадров и сумевшего внести свой вклад в организацию науки, достоин уважения вдвойне. И здесь, обращаясь к архивам изучаемого нами времени, мы вновь встречаем знакомые имена.

В России XVIII в. со времени основания Академии наук и университета сложилась определенная система подготовки научных кадров. Состояла она в том, что при университете была основана гимназия, в которой на казенном содержании находились шесть-

десят учащихся. После окончания гимназии эта молодежь должна была пополнять ряды студентов университета. К середине 60-х годов эта система пришла в негодность. Дело в том, что дети, которым был уготован по тем или иным причинам «путь в науку» и определяемые для этого в гимназию, часто оказывались совершенно не способными и не подготовленными для этого занятия. Вследствие этого создалось трудное положение с кадрами для университета. И вот в этот период в полной мере проявились организаторские способности Эпинуса и отчасти известного уже нам Ивана Тауберта (того самого профессора-математика, который когда-то был приставлен А. П. Бестужевым-Рюминым наблюдать за правильной перлюстрацией писем).

Этими учеными было создано так называемое воспитательное училище при гимназии. К идее создания училища они пришли, незадолго до этого принимая участие в разработке регламента для российской Академии художеств, при которой также была создана детская воспитательная школа. Эту инициативу поддержал и президент Академии наук И. И. Разумовский. В своем письме из Ахена профессору Тауберту от 28 июля 1765 г. он писал: «Особливо рекомендую покрепче приняться за Университет и Гимназию. Тот департамент, будучи первейшей надеждой Академии; но ныне слабо себя оказывает, а причина тому не иная, как та, которую воспитательным училищем поправить можно.

Вследствие сего рассуждено собранием академическим вместо выключенных из гимназии за неспособностью к наукам и за негодными поступками набрать в комплект к положенным по штату на казенном содержании 60-ти гимназистам... хорошей надежды молодых людей и дать им прямое в благонравии воспитание» [7].

Создание училища началось с выработки программы, подбора преподавательских кадров. Затем про-

фессор Тауберт дал объявление в газетах о том, что «при академической гимназии создается учреждение к воспитанию малолетних детей, определяемых к высоким наукам, и чтоб желающие всякого чина, кроме крепостных, приводили в канцелярию академии своих детей не старее как от пяти до шести лет».

Узнав о работе Эпинуса и Тауберта по созданию училища, императрица направила в Академию наук для проверки обстоятельств дела Ивана Теплова. Тауберт и Эпинус, сославшись на приказ президента Академии, показали Теплову проект о новом учреждении, который они готовили. Теплов обо всем доложил императрице и поднес ей положение об учреждении училища. Однако, так как проект был весьма пространен, императрица отложила его рассмотрение на будущее.

Эпинус и Тауберт настойчиво продолжали начатое дело. Тем более, что желающих определить своих детей в училище оказалось предостаточно. Из всех возможных кандидатов было отобрано тридцать человек. Это были мальчики 5—6 лет из простых, непривилегированных семей: Василий Чанников — сын бывшего воеводы Петра Чанникова, Михайло Данауров — сын коллежского регистратора Ивана Данаурова, Аполлон Фирсов — сын секретаря Михайлы Фирсова, Андрей Чернышев — сын придворного музыканта Андрея Чернышева, Тимофей Соловцов — сын солдата Архангелогородского полка Никифора Соловцова, Александр Рукомойкин — сын подмастерья Ильи Рукомойкина, Дмитрий Беляев — сын придворной конюшной конторы живописного ученика Ивана Беляева и др. [8]. Вскоре начались занятия.

Императрица вновь направила в училище Ивана Теплова. В своем докладе императрице Теплов писал: «...вчерашнего числа по высочайшему повелению Вашего Величества ездил я в Академию и застал там с Таубертом профессора Эпинуса, которые мне по-

казывали в особливом при Академии доме (в котором и гимназия находится) учреждение воспитываемых малолетних детей... Я оное нашел не токмо по объяснениям Тауберта и Эпинуса, но и в самом деле учреждено точно с высочайшим намерением Вашего Величества сходно... Дети... все чисто одеты и прибраны; одним словом, все по наблюдению как в Академии художеств. Между тем нашел ту только отмену, что дети в первом с трех лет классе воспитываются в немецком, а не во французском языке...» Именно на это обстоятельство, отмеченное Тепловым, нам бы хотелось обратить особое внимание читателя. Вспомним, что в екатерининскую эпоху среди образованной, светской части общества все более широкое распространение получал французский язык. Поэтому естественное недоумение у Теплова вызвало введение в программу первого класса, а он был рассчитан на целых три года обучения, немецкого языка, а не французского. Как же объяснили это Эпинус и Тауберт? Создание училища ставит целью подготовку детей к научной деятельности («сии младенцы к высоким наукам будут приготовляться») и, чтобы оказаться на необходимом научном уровне, они обязаны будут со временем познать достижения передовой европейской научной мысли. Вся же европейская средневековая наука создавалась на латинском и немецком языках. Русским детям — будущим ученым необходимо было дать к этим научным знаниям ключ. Таким ключом являлись в то время немецкий язык и латынь. Именно изучение этих языков и было в первую очередь включено в программу училища. Эта глубокая и плодотворная мысль, заложенная когда-то трудами истинных организаторов науки Эпинуса и Тауберта, была успешно реализована в системе образования России, глубоко продуманной и принесшей со временем, как известно, прекрасные результаты.

В том же 1765 г. императрица Екатерина II поручила Ф. Эпинусу преподавание физики и математики наследнику престола (Павлу I). Состоя с 1782 г. членом Комиссии по учреждению народных училищ, Эпинус разработал проект организации системы среднего и низшего образования в России.

Вспоминая здесь Эпинуса и других ученых, было бы непростительной ошибкой, на наш взгляд, оценивать их жизнь и деятельность одномерно, а, обращаясь к предмету нашего исследования, судить о них лишь как о лицах, внесших свой вклад в становление какой-то специальной государственной службы. Эту мысль мы будем пытаться подкрепить примерами и в дальнейшем. Здесь же мы расскажем еще о двух выдающихся наших соотечественниках, внесших свою лепту в деятельность криптографической службы России XVIII столетия. Это Е. Н. и Ф. В. Каржавины.

Ерофей и Федор Каржавины

Ерофей Никитич Каржавин (1719—1772) родился в старообрядческой семье ямщиков, занимавшихся мелкой розничной торговлей в лесном ряду у Покровских ворот в Москве. Ерофей с детства помогал отцу, ездил с братьями для «торгового промысла» с кожевенным товаром в Петербург и на Украину. В 1738 г. во время русско-турецкой войны они числились «при российской армии для торгового же промысла сапогами». Юные годы Ерофея Каржавина прошли в отцовском доме, находившемся в Москве близ Яузы, в приходе церкви Ильи Пророка, что на Воронцовском поле. Начинания Петра I, открывшего широким слоям российской молодежи путь к знаниям, к европейской науке, не были забыты и после смерти великого императора. Не к «купеческой коммерции», а к служению обществу, к знаниям стремился и юный Е. Н. Каржавин. В 1748 г. он тайно, через костромского купца Андрея Кошелева, отправился во Францию. Там талантливый молодой

человек поступил в Сорбоннский университет. Ученый-лингвист и переводчик Е. Н. Каржавин в Париже был в тесном творческом общении со знаменитыми французскими учеными: Ж.-Н. Делилем, Ж.-Н. Бюашем, Ж.-Л. Барбо де Брюером. Последний из них в августе 1756 г. подал государственному министру Франции д'Аржансону, «покровителю наук», официальную записку о Ерофее Каржавине. 16 сентября 1760 г. Е. Н. Каржавину, «самовольно отлучившемуся за границу», было разрешено вернуться в Россию, где он начинает работать переводчиком и составителем шифров в Коллегии иностранных дел. Кроме того, он продолжает активно вести культурно-просветительскую работу, переводит различные литературные произведения. Ерофей Каржавин является первым переводчиком на русский язык «Путешествий Гулливера» Д. Свифта. По сохранившимся именным спискам можно установить, что коллегами Е. Н. Каржавина по ведомству иностранных дел являлись известные в дальнейшем писатели: Д. И. Фонвизин, Ф. А. Этин, В. Г. Рубан, И. Ф. Богданович. Здесь работали тогда переводчиками А. П. Курбатов и И. И. Челищев [9].

В бытность Е. Н. Каржавина в Париже в 1753 г. к нему приехал родной племянник, сын его брата Василия Федор Каржавин (1745—1812). В упоминавшейся нами выше записке Барбо де Брюера от августа 1756 г. д'Аржансону, касавшейся в основном Е. Н. Каржавина, говорится также о «блестящих успехах в латинской и французской грамматике и в экспериментальной физике его племянника, занимающегося на 6-м курсе колледжа Лизье». Обучение Федора Каржавина наукам в Париже продолжалось 13 лет. В это время он познакомился с трудами идеологов Просвещения. С мая 1763 г. Ф. Каржавин живет у русского посланника в Париже графа С. В. Салтыкова. В письме отцу он писал: «Я окончил мои занятия в колледже. Я там изучал французский язык,

латынь, латинскую поэзию, немножко древнегреческий язык, риторику, в которой заключено красноречие французское и латинское, философию, географию и опытную физику, которую я, могу похвастать, знаю лучше, чем французский язык; сейчас я учусь итальянскому и прохожу курс физики...»

В тот год Ф. Каржавин попадает под опеку чиновников парижской миссии, где получает работу переводчика. Именно там началась его многолетняя дружба с советником посольства Н. К. Хотинским. Федор Каржавин был купцом, литератором, путешественником. Он первым из русских побывал в США, на Кубе и Мартинике [10].

К нашему глубокому сожалению, имея иной предмет нашего исследования, мы здесь можем привести лишь отрывочные и краткие сведения о тех лицах, которые внесли вклад в развитие нашей криптографической службы. Мы надеемся, что заинтересованный читатель сможет самостоятельно расширить свои знания о названных нами людях. И все же, чтобы более отчетливо высветить фигуру Ф. В. Каржавина, нам хотелось бы процитировать некоторые его высказывания. Так, в письме из Америки родителям в Москву от сентября 1785 г. Каржавин, говоря о своих путешествиях, размышляя о своей дальнейшей судьбе, писал так о возможной смерти: «Умереть где бы то ни было все равно: из пыли мы вышли, живая пыль мы есмь и в пыль должны возвратиться (четыре элемента, составляющие махину, называемую человек, должны рассыпаться, и всяк из них присоединится своему начальному источнику. Химия то мне доказала)...» Но далее, укоряя отца в том, что тот проклял его за тайный отъезд за границу на учебу, в непонимании его трудов во имя науки, Федор Каржавин пишет о своей Родине, о своем человеческом достоинстве: «Вы лишили меня моих друзей, моего Отечества, моего государя, моего счастия, всю мою науку вы возвратили в ничто; вы у меня отня-

ли честь, следовательно, вы меня до основания разорили...» [11].

Вернувшись в Россию в 1788 г., Федор Каржавин так же, как до него Ерофей Каржавин, стал работать в Коллегии иностранных дел переводчиком и составителем шифров. Принимает он участие и в дешифровальной работе. Параллельно с этой секретной своей деятельностью Ф. В. Каржавин занимался литературным творчеством. Он опубликовал нескольких оригинальных прозаических произведений: литературную хрестоматию «Вожак, показывающий путь к лучшему выговору букв и речений французских» (СПб., 1794), нравоучительную книгу «Новоявленный ведун, поведующий гадание духов» (СПб., 1795), «Краткий исторический очерк о проникновении письменности в Россию» (в книге Е. Н. Каржавина «Заметки о русском языке и алфавите», СПб., 1791). Из-под пера Федора Каржавина вышел также целый ряд статей филологического, исторического, естественнонаучного характера.

Размышляя о Х. Гольдбахе, Ф. У. Т. Эпинусе, И. Тауберте, Е. Н. и Ф. В. Каржавиных, невольно приходишь к мысли о необходимости подробных исследований жизни таких людей. Ведь их судьбы проливают свет на общество, в котором они обитали, на его взгляды, на его ноосферу. Что определяло их успех или неудачи? Талант, благосклонность звезд, случайность, политическая игра или что-то иное? Кроме того, их карьера, их служба государственным интересам, научная, общественная и иная деятельность напрямую отражают взгляды, интеллектуальный уровень людей, стоящих на высших ступенях общественной лестницы, олицетворяющих собой государство.

Слишком многие имена забыты, скрыты от потомков тяжелыми пластами Времени.

Глава седьмая

ТАЙНОПИСЬ ЕКАТЕРИНИНСКИХ ВРЕМЕН

Шифры императрицы

С конца 40-х — начала 50-х годов начинают употребляться шифры совершенно нового для этого века, так называемого третьего типа. Именно этот третий тип шифров остается господствующим до самого конца XVIII в., хотя пытливая мысль разработчиков шифров ищет все новые и новые способы и приемы, которые еще более надежно могли бы скрывать письменную информацию. И хотя принципиально новые решения находятся, все же широкого распространения они пока не получают.

Этот третий тип шифров XVIII столетия представлен в архивах достаточно полно. Цифирные азбуки стали больше прежних по объему, в основном они включают 1000—1200 величин. Изредка встречаются шифры на 400—500 словарных величин, но строятся они по тем же принципам, что и большие цифири. Словарь этих шифров, как и прежде, включает буквы, слоги, наиболее употребительную в переписке лексику, географические названия, имена, месяцы, счеты. Как правило, все эти величины уже не выделяются в шифранте в отдельные разделы, а располагаются по алфавиту. Шифробозначения только цифровые. Как и прежде, особое внимание уделяет-

ся гласным буквам: им придается обязательно несколько шифробозначений, тогда как все другие величины имеют по одному-двум.

Основное внимание продолжает уделяться повышению криптографической стойкости шифров. Кроме огромного количества пустышек (их задают теперь тысячами), в этом типе шифров применяются и другие «хитрости», которые тщательно описываются в подробных и объемных правилах, которыми снабжается каждая цифирная азбука.

Так, о пустышках в правилах писалось следующее: «Пустые числа писать где сколько хочется, только чтобы на каждой строке было сих чисел не меньше трех или четырех» [1]..

«Не начинать пиесы (в данном случае шифртекста. — *Т. С.*) значащими числами, но пустыми, которых определяется тысяча чисел, начиная с 5001 до 5999. Но сколько можно между собой перемешивать оныя, например: 5010, 5772, 5384, 5832 и проч., стараясь употреблять оныя во всякой строке между значащими» [2].

Первым шифром нового типа была цифирь 1749 г., о которой в правилах пользования сказано: «Оная имеет употребляться в секретных на высочайшее Ея Императорского Величества имя реляциях и в письмах к канцлеру по таким материалам, кои Коллегии не принадлежат.

Оная ж с первыми куриерами и ко всем Ея Императорского Величества при других дворах министрам, с коими секретная корреспонденция производится, а именно: послу графу Головкину в Га(а)гу, к графу М. П. Бестужеву-Рюмину в Вену, к тайному советнику Ланчинскому, к графу Чернышеву в Лондон и к советнику канцелярии Грос(с)у в Берлин пошлется для равномерного ж употребления и для того, чтоб они между собою корреспондовать могли» [3].

Новым в шифрах данного типа было помещение в их словарь особых знаков, шифробозначения которых означали в шифрованном тексте, что при расшифровании определенные куски шифртекста обращались в пустышки. Эти особые знаки могли иметь различные значения.

Например, в одной из цифирей знак + (а ему соответствовало, естественно, несколько шифробозначений) означал, что следуюшее за ним в шифртексте шифробозначение не следует принимать во внимание, оно ничего не значит. Два таких знака (+ +) означали, что не следует читать два следующих за ними шифробозначения, три таких знака (+ + +) означали, что не следует читать три следующих за ними шифробозначения. По правилам этой же цифири употребление знака = означало, что не следует принимать во внимание все шифробозначения, стоящие за этим знаком в данной строке шифртекста, а знак = = уничтожал весь последующий шифртекст на данной странице. Здесь же знак * уничтожал предыдущее шифробозначение, два таких знака (* *) уничтожали два предыдущих шифробозначения, три знака (* * *) уничтожали три предыдущих шифробозначения.

В правилах к другой цифири указывалось: «Знаки × (а их было в цифири девять, т. е. им соответствовало девять различных шифробозначений. — *Т. С.*) такую силу иметь должны, что когда один поставится, то все за ним следующие пустыми сделаются, пока паки оное другим таким же знаком заключатся, и потому весьма нужно, чтоб сие как в начале, так и в окончании каждой пиесы или каждого параграфа наблюдаемо было». Иными словами, шифробозначения, соответствовавшие такому особому знаку, означали, что весь шифртекст между ними следовало не принимать во внимание при расшифровании.

В других цифирях были знаки, уничтожавшие шифртекст до начала следующего параграфа, а то и более. Все зависело от фантазии составителя шифра.

Таким образом, текст, шифрованный в результате применения многочисленных пустышек и написания ничего не значащих отрезков, оказывался значительно длиннее текста открытого. Расчет составителей шифров как раз и заключался в том, что шифртексты представляли собой огромные цифровые массивы, в которых, по их мнению, лишь знающий ключ мог отделить зерна от плевел, причем зерен было ничтожно мало в море плевел. Накручивался как бы клубок из шифробозначений, который в действительности был лишь мыльным пузырем.

Со временем этот тип шифров еще усложняется. В правилах появляются, например, такие пункты:

«Пред каждым числом из четырех цифр состоящих можно толь часто, сколь похочется, 5 (цифра могла быть и любая другая. — *Т. С.*) ставить, еже знаменование оных отнюдь не переменяется и тако значит 51871 то же, как и 1871, 51632 — как и 1632 и проч.». Естественно, что в правилах указывалось, из каких тысяч или сотен выбраны были шифробозначения для данной цифири.

Вот это направление поиска в отношении изменения значности шифробозначений особенно активно начинает разрабатываться в 60—70-е годы XVIII в. Некоторые составители шифров даже писали в правилах: «Можно с помощью этого шифра зашифровать другим способом так, что не узнают, что это тот же шифр». Для подобной маскировки авторы предлагали проводить такие манипуляции с шифробозначениями: «Для этого надо заменить все тысячи на сотни, добавив к десяткам и единицам нули, например, вместо 543, 351 писать 1543, 2351; вместо 1. 26 писать 001. 026, а вместо 1000. 2000. 3000 писать только 000 и без разделения точками, как можно более слитно, чтобы не было обнаружено, что они тройные. Нет необходимости знать, из какой тысячи они взяты: их значимость будет узнана по смыслу и как только увидят расшифровку. Но, чтобы не

было никаких трудностей, которые могут помешать опытному расшифровальщику, нашли удобным отмечать цифры первой тысячи точкой, второй — линией и оставить числа из третьей тысячи без пометок. Эти точки и линии можно было ставить над и под числами, в начале, середине и конце их, не соблюдая никакого порядка, чтобы лучше спрятать эти изменения в шифре, например: 276300000. Это можно расшифровать с той же легкостью, как и цифры, разделенные точками, надо только вспомнить, что они все тройные и из какой тысячи. Тогда будет видно, что 276 — из третьей тысячи и используется вместо 2276, что следующее число — из первой тысячи и точно 300, и что третье число из второй тысячи и стало быть 2000 и т. п.» [4].

В других правилах для сокрытия значения шифробозначений рекомендовалось такое изменение их значности (шифробозначения в данной цифирной азбуке от 6001 до 7000):

«В шифровании писем... всегда выпущать первые две цифры и писать 1. 2. 3. 31. 56, что в расшифровке будет значить 6001. 6002. 6003. 6031. 6056 и проч.

Так же от 6221 по 6999 как можно чаще в шифровании пиесы выпущать первую цифру 6 и писать 221. 356. 763 и проч., что в расшифровке будет значить 6221. 6356. 6763, чего, однако же, не делать с числами, имеющими в конце нули, как то: 6020. 6030. 6200. 6250 и проч.» [5].

Чрезвычайно существенным для шифров этого типа было продолжение в них традиции использования при зашифровании одного сообщения разных языков: как правило, все шифры третьего типа были двуязычными. Словарь их состоял из двух частей: русской и французской (реже немецкой). Открытый текст депеши составлялся на этих двух языках, при переходе в процессе зашифрования с одного языка

на другой ставились особые, заранее оговоренные в правилах числа, которых для каждого шифра было несколько. Этот прием, когда разные части одной и той же депеши писались на разных языках, приводил к тому, что при зашифровании не только практически вдвое увеличивалось число используемых кодовых обозначений, но, что самое существенное, смешивались и в определенной степени выравнивались статистические характеристики шифртекста, столь важные для расшифрования при отсутствии ключа. При этом основные правила как для русской, так и для иноязычной части были одинаковыми, т. е. множество пустых, зашифрование больших кусков псевдотекста, которые при расшифровании уничтожались, и т. д

Как говорилось в правилах: «В случае нужды смешаемы быть имеют между русскими французские речи и сочинения, равно как и между французскими русские... Пустые числа употребляются в начале и в конце параграфов по строке, по полуторе, по две и более, а иногда по одному только, по два и по три числа. Иногда пиесы начинаются или оканчиваются самыми значущими. Но во всяком случае часто пишутся пустые в самой середине параграфа и вместо просодии (пробелов. — *Т. С.*), а иногда и вмешиваются и в середине фразисов и речений. Да сверх того ставятся между пустыми и самые значущие числа, кои не понадобятся и уничтожаются» [6].

Вообще правила к этому типу шифров составляются весьма полные и подробные. Изучение их дает представление о криптографических взглядах составителей шифров того времени. Так, в этих правилах обосновывалось отмеченное нами и для более ранних шифров обязательное наличие двух и более шифробозначений для гласных, наиболее употребительных имен собственных и слогов· «Сія новая цыфра зделана столь пространна въ томъ единственно намъренiи, чтобъ означить въ ней всъ гласныя,

такъ же часто употребляемыя имяна и ръчи многими числами, и прибрать къ ним возможныя окончанія: частое повтореніе первыхъ и стеченіе вторыхъ, когда они многими изображены слогами, открываютъ обыкновенно цыфру».

Важнейшим условием правильного шифрования считалось постоянное равномерное использование всех шифробозначений, включая пустышки и те, которые исключались при расшифровании. Такие величины следовало вставлять в середину фраз и даже слов.

Увеличение использования шифробозначений, в частности, могло достигаться и тем, что при повторении одних и тех же слов или имен собственных в тексте шифровать их с помощью других элементов шифра, нежели в первый раз. Например, зашифровав слово в первый раз, набрав его по буквам, в другой раз набирать его по слогам или использовать дважды слоги, но в разных сочетаниях с буквами и т. п. С другой стороны, в этих шифрах одному шифробозначению порой соответствовали разные слова (например, Китай, китаец, китаянка). Это делалось для того, «чтобы не было неиспользованных слов». При расшифровании из контекста, как правило, легко можно было выбрать необходимое слово.

Во всех правилах подчеркивалась необходимость строгого соблюдения правил пользования шифрами, давались частные рекомендации по их практическому использованию. Так, например, не разрешалось запоминать наизусть шифробозначения, в том числе гласных и слогов, хотя это было и легко, так как они использовались чаще других величин. Такое запоминание, по мнению составителей, мешало использовать другие шифробозначения этих же словарных величин, вставлять пустые, что облегчало поиск ключа к шифру. И вообще рекомендовалось не особо полагаться на память, так как это могло привести к ошибкам, изменяющим смысл шифровок.

Читая сейчас эти старые правила пользования государственными шифрами России, невольно обращаешь внимание на их целевую направленность на воспитание у лиц, имеющих дело с шифрами. чувства долга, глубокого и осознанного уважения к государственным интересам: «Пространство ея (цифири. — *Т. С.*) испужаетъ можетъ быть и своихъ, пока они с нею не спознаются: но пусть трудна она и въ самомъ деле; нетъ въ свете ни труда, ни прилежания, коими бъ не должно жертвовать сохранению цыфръ, когда сему превращению вверяются часто великия государственныя тайности».

Сохранившийся в архиве один из шифров, которым пользовалась императрица Екатерина Великая для переписки с канцлером, представляет собой именно такой тип шифра [7]. Но в екатерининскую эпоху появляются шифры еще более сложного устройства, с еще более подробными и сложными правилами. Характерным для них является то, что кроме двух словарей (русского и французского), они имеют еще и два так называемых прибавления, которые включают в себя дополнительный перечень отдельно русских и отдельно французских слов и словосочетаний, а также еще раз алфавит и перечень слогов, предлогов, а для французских прибавлений — дифтонгов и артиклей с кодовыми обозначениями другой, в отличие от основного словаря, значности. Так, например, в цифири 1781 г. для переписки Коллегии с находившимся во Франкфурте-на-Майне графом Румянцевым [8] словарные величины 1-го листа (русского словаря) имели кодовые обозначения от 1001 до 2000, 2-го листа (французского словаря) — с 3001 до 4000, французское дополнение состояло из 299 величин с шифробозначениями от 500 до 799, русское дополнение также имело трехзначные шифробозначения: с 222 до 321, с 666 до 765 и с 888 до 987. Чтобы «вмешивать» величины из русского прибавления в текст, шифруемый по основной части,

следовало употреблять в качестве переходных числа от 222 до 322 (сколько угодно и в любой последовательности), а также от 666 до 766 и от 888 до 988, т. е. всего триста чисел, которые следовало писать «с прибавкой нуля в конце».

По этому типу шифров следовало шифровать, меняя в строке значность шифробозначений (с 3- на 4-значные и наоборот) по особым правилам. Весь шифртекст писался слитно без разделения шифробозначений точками.

Когда корреспондент располагал несколькими шифрами со словарями на разных языках, ему рекомендовалось иногда использовать русскую часть от одного шифра, а французскую часть от другого. Так, например, в правилах к одному из цифирных ключей, принадлежавшему послу в Стокгольме Рикману, говорилось: «А чтоб в случае нужды можно было вмешивать между русских и французские слова, то для сего употреблять французскую генеральную цифирь, дав приметить разбирателю то постановлением чисел, значущих А,Б,С». По окончании французского текста следовало поставить шифробозначения, соответствовавшие слогам бю, ки. Русское приложение этот шифр Рикмана имел свое собственное [9].

Частная переписка Екатерины II и ее окружения также иногда шифровалась. В основном для этого использовались специальные коды, с помощью которых слова и фразы заменялись на другие слова и фразы, скрывающие истинное содержание письма (жаргонные коды).

Два таких кода 1788 г. для переписки великого князя Павла Петровича и великой княгини Марии Федоровны были опубликованы П. В. Стегнием в замечательной книге «Хроники времен Екатерины II» (М.: Олма-Пресс, 2001). Здесь, например, фраза «Поцелуй еще раз Александрин» означает «Вам придется покинуть Петербург»; «Что Вам пишут из Турина?» — «Письма от императрицы весьма любез-

ны»; «Пришлите мне черную ленту на трость» — «Ваши письма перлюстрируются» и т. д.

Дипломаты и тайнопись

28 января 1779 г. Екатерина II утвердила штат заграничных учреждений Коллегии иностранных дел — «Штат постам министерским вне государства». Звание посла по этому штату было присвоено лишь русскому представителю в Варшаве, большинство же русских представителей за границей именовались «министрами второго ранга». Такие министры находились при дворах главных европейских государств: в Вене, Париже, Лондоне, Берлине, Стокгольме, Мадриде, Константинополе, Лиссабоне, Неаполе, Дрездене, Гааге, Копенгагене, Регенсбурге. Некоторые дипломатические представители назывались просто министрами (в Венеции, Эйтине, Митаве) и резидентами (в Гданьске, Гамбурге). К министерским постам были добавлены также «генеральный консул или комиссар» в Италии и «генеральный консул» в Архипелаге (Англии). Всего министерских должностей по штатам 1779 г. было 21. При министрах в заграничных представительствах России состояли: один советник посольства, один или два титулярных советника, один переводчик, один или два студента.

И лишь по штатам, утвержденным 6 января 1800 г. императором Павлом I, министров второго ранга заменили послы и посланники. Послы назначены были в Вену и Стокгольм, посланники — в Берлин, Лондон, Копенгаген, Мюнхен, Лиссабон, Неаполь, Турин и Константинополь. В Париже, Мадриде, Гааге в тот год по политическим обстоятельствам не было вовсе русских представителей. В Регенсбурге министра заменил резидент, вместо министров и резидентов в Дрездене и Гамбурге были назначены поверенные в делах, а в Данциге и Венеции — генеральные консулы.

Вся переписка этих лиц шифровалась и держалась в строгом секрете. Большое внимание соблюдению тайны уделялось и в самой Коллегии в отношении лиц, работающих по шифровальной части. Рассуждая «о наилучшем содержании в секрете всех в секретной экспедиции дел», Коллегия еще в 1744 г. определила приказать всем служителям этой экспедиции (и архива) «ни с кем из посторонних людей об этих делах не говорить, не ходить на дворы к чужестранным министрам и никакого с ними обхождения и компании не иметь». Этот приказ подтвержден был вторично 28 марта 1758 г.: «Для сохранения вящего секрета при нынешних военных и всяких важных обстоятельствах» секретарям секретной экспедиции вменялось в обязанность строго смотреть за переводчиками, «чтобы дела, им порученные, по столам не лежали и чтобы товарищи их не читали этих дел». В заключение приказа подтверждалось запрещение кого-либо постороннего пускать в апартаменты, занятые секретной экспедицией.

При Екатерине II, 15 марта 1781 г., Коллегия в третий раз получила приказание не допускать знакомства «чинов департамента иностранных дел» с иностранными министрами и их свитой. При этом императрица указала, чтобы, кроме «министров департамента иностранных дел, каковыми ее величество почитает канцлера (или без сего звания управляющего оным департаментом), вице-канцлера и членов секретной экспедиции», никто из прочих чинов коллегии не ходил в дома чужестранных министров, не имел с ними разговоров о делах, никого из них в своем доме не принимал и ни под каким видом не вел с ними переписки или пересылки. То же самое запрещение возобновлено было указом 3 августа 1791 г.

Уже с петровских времен один и тот же шифр мог употребляться для переписки центра (царя, канцлера, Коллегии иностранных дел) не с одним, а с не-

сколькими министрами или другими политическими, дипломатическими, военными деятелями одновременно. Вначале такая связь по одному шифру осуществлялась с лицами, направляемыми в одно и то же место или находящимися в одном месте или стране. Примером такого шифра может служить цифирь 30-х годов для переписки с коронным гетманом Синявским и бискупом Куявским [10]. Это — простая замена букв латинского алфавита на двузначные цифры, по 2 шифробозначения на букву.

Самый ранний из обнаруженных нами шифров, по которым велась переписка одновременно с несколькими лицами (осуществлялась своего рода общая и циркулярная связь), относится к совсем раннему времени — периоду Посольского приказа. Эта цифирная азбука содержит не только алфавит-кириллицу, как другие шифры этого времени, но и небольшой словарик имен («персон»). В нее включены пять пустышек, а в качестве шифробозначений использованы слоги и буквы той же кириллицы. В архиве сохранилось два экземпляра этого шифра, причем на одном из них «суплемент» и пустышки отсутствуют. Именно на этом экземпляре сохранилась надпись: «Такова азбука с князем Меншиковым, с Гаврилом Ивановичем (графом Головкиным. — *Т. С.*), Федором Михайловичем (графом Апраксиным. — *Т. С.*), с князем Репниным. Писать сею азбукою к государю письма».

На другом экземпляре азбуки помещены такие примечания: «Сие слова без разделения и без точек и запятых писать. А вместо точек и запятых и разделения рече вписывать из ниже писанных буквы по одной.

Буде же когда случится писать имяна ниже писанных персон, то оныя писать такими знаки, как против каждой отмечено. Однако ж писать все всплош, нигде не оставливая, а между ими ставить помянутые буквы, которые ничего не значат» [11].

В своем роде это единственная азбука из шифров описанного нами первого типа, по которой предусматривалось писать шифртекст слитно, без разделения шифробозначений точками. При пользовании всеми другими азбуками обязательным было написание шифробозначений вместе с точками, которые как бы входили в состав шифробозначений. Например: 1. 12. 8. 51. и т. д.

Уже в 20-х гг. XVIII в. была организована, говоря современным языком, одна из первых сетей общей связи, которая сохранялась и развивалась и в более позднее время. В этой сети переписка велась между центром (в данном случае в лице императрицы Елизаветы Петровны) и российскими министрами, находившимися при европейских дворах. Корреспондентов в этой сети было всего шестеро: императрица́, посол в Гааге граф Головкин, посол в Вене граф Бестужев-Рюмин, резидент в Гданьске тайный советник Ланчинский, резидент в Берлине советник канцелярии Гросс, посол в Лондоне граф Чернышев. Переписка велась по описанной нами выше цифирной азбуке 1749 г.

Однако уже через год эта сеть связи была расширена. В письме к послу графу Чернышеву из Коллегии от 5 февраля 1750 г. говорилось о том, что ему высылаются для одновременного пользования сразу пять цифирей, четыре русских и одна немецкая, одна из них «под знаком О — русская цифирь генера́льная для корреспондования как с Коллегией, так и с прочими российскими министрами... а именно: с графом Бестужевым-Рюминым, с графом Головкиным, с Ланчинским, с Паниным, с Гроссом, с князем Голицыным».

Именно здесь мы встречаем впервые название «генеральная цифирь» в отношении шифра, используемого на общей линии связи. В отличие от индивидуальных шифров, на которых, как правило, писалось имя лица, в пользование кому шифр предназначался, «генеральные цифири» имели буквенное, значковое или цифровое обозначение.

Одновременно с описанной, графу Чернышеву высылалась другая, немецкая генеральная цифирь, с помощью которой ему следовало переписываться как с перечисленными выше лицами, так еще с графом Кейзерлингом, бароном Корфом и секретарем посольства в Польше Ржичевским.

Все шифры были присланы Чернышеву при письме, в котором говорилось о них так:

«№ — 1 цифирь русская, единственно для корреспондования с Коллегией;

№ — 2 цифирь русская для корреспондования с Коллегией;

№ — 3 цифирь русская, генеральная, для корреспондования как с Коллегией, так и с прочими российскими министрами...

Под сим же третьим номером приобщается копия с немецкой генеральной цифири, дабы оною по востребованию обстоятельств на немецком и французском языках как в Коллегию писать, так с реченными персонами (перечисленными нами выше. — *Т. С.)*, которым равномерные и точного содержания копии ныне ж для того намерения посылаются, корреспондовать можно было.

№ — 4 русская цифирь единственно для корреспондования с Коллегией».

Кроме прочего, это письмо показывает, сколько шифров использовал российский представитель за границей одновременно.

Нами установлено, что разработка генеральных цифирей с середины XVIII в. Коллегией иностранных дел велась постоянно. Выводились из действия они примерно через два года. Сеть корреспондентов росла год от года. Из генеральных цифирей XVIII в. нам известны:

— генеральная цифирь на русском языке 1762 г., по которой обменивались корреспонденцией с Коллегией и между собой: Бестужев-Рюмин (Париж), Кейзерлинг (Вена), Корф (Копенгаген), Панин (Стокгольм), Голицын (Лондон), Пушкин (Гданьск), А. Симолин (Митава), Д. Симолин (Регенсбург), Салтыков («заграничная армия»), Обрезков (Константинополь);

— генеральная цифирь того же 1762 г., объединявшая тех же корреспондентов, но переписку по ней можно было вести сразу на трех языках: русском, французском и немецком. Дополнительно этот шифр в 1764 г. был дан генерал-майору князю Репнину, направлявшемуся в качестве полномочного министра к прусскому двору, а также генерал-аншефу князю Волконскому;

— генеральная цифирная азбука 1764 г. на русском и французском языках была разослана русским представителям в Вене, Варшаве, Копенгагене, Лондоне, Стокгольме, Берлине, Гааге, Париже, Дрездене, Митаве, Регенсбурге, Гданьске, Мадриде, Гамбурге, Константинополе;

— генеральная цифирная азбука на французском языке была разослана в те же пункты в 1768 г.;

— генеральная цифирь 1768 г. на русском и французском языках была разослана также в те же 15 адресов;

— генеральная цифирь 1768 г., также на русском и французском языках. Разослана эта цифирь была тем же лицам и дополнительно главнокомандующему генерал-аншефу князю Голицыну;

— генеральная цифирь на французском и русском языках 1771 г. обозначена вместо употреблявшихся ранее знаков двенадцатью числами: шесть — для пользования русской частью шифра и шесть — для пользования французской его частью. Эта цифирь в январе 1771 г. была разослана в Митаву, Гданьск, Берлин, Дрезден, Париж, Мадрид, Гаагу, Лондон, Гамбург, Копенгаген, Стокгольм, Вену, Регенсбург, Варшаву, Командующему 1-й и 2-й армиями генерал-фельдмаршалу графу Румянцеву, генерал-аншефу князю Долгорукову. В 1779 г. этот же шифр был дан отправленному в Португалию чрезвычайно-

му посланнику и полномочному министру графу Нессельроде;

— генеральная цифирь 1773 г. на русском языке под знаком «165». Разослана, по сравнению с предыдущей, в первые 14 адресов.

— генеральная цифирь под знаком «40, 68 и 77» — самая большая из известных нам цифирей XVIII в. Она включала 2000 словарных величин и объединяла Коллегию с пятнадцатью корреспондентами за рубежом: Стакельбергом в Варшаве, министром Голицыным в Вене, министром Ассебургом в Регенсбурге, министром Барятинским в Париже, министром Зиновьевым в Мадриде, посланником Белосельским в Дрездене, посланником Голицыным в Гааге, министром Симолиным в Стокгольме, министром Долгоруковым в Берлине, министром Сакеном в Копенгагене, министром Мусиным-Пушкиным в Лондоне, резидентом Гроссом в Лондоне, посланником Стахиевым в Константинополе, резидентом Ребиндером в Гданьске, князем Репниным в Берлине [12] .

В 1771 г. была параллельно организована общая сеть связи, охватывающая совершенно иной регион. Так, с помощью генеральной цифири 1771 г. под знаком «1631» переписывались между собой и с Коллегией иностранных дел десять корреспондентов: полномочный министр Булгаков в Константинополе, граф Воронцов в Венеции, граф Разумовский в Неаполе, полномочный министр Мордвинов в Генуе, полномочный министр князь Юсупов в Турине, граф Мореннго во Флоренции, Псаро — поверенный в делах на Мальте, коллежский советник Хемницер в Смирне, генеральный консул в Молдавии, Валахии и Бессарабии Северин, коллежский асессор Юлиниц в Сицилии.

Рассылали шифры и ключи обязательно при циркулярных рескриптах за подписью канцлера и вице-канцлера. Вот текст одного и таких документов:

«Циркулярный рескрипт во Гданьск к резиденту Ребиндеру.

Для употребления по важным материям переписки Вашей сюда ко двору нашему, так и с пребывающими при чужестранных дворах нашими министрами и должность их исправляющими за нужно признали мы доставленные из нашей Коллегии иностранных дел в 1773 г. к тем министрам нашим при циркулярных рескриптах цифирные ключи русские и французские переменить ныне новыми, кои при сем к Вам и посылаем с нарочным курьером, а именно: четыре ключа, из коих два на русском и французском языках единственно для корреспонденции с упомянутыми министрами нашими и поверенными в делах, а с кем именно — в том будет Вам служить прилагаемая при сем всем им роспись...

По Ея Императорского Величества указу.

Подписан посему:

граф Никита Панин,
граф Иван Остерман» [13].

Государственное дело

В Коллегии иностранных дел велся тщательный учет всех цифирей. Перечень цифирей, списки лиц, кому они были разосланы, от кого получены обратно отдельные экземпляры, на каком языке цифири составлены и другие необходимые сведения заносились в особые реестры.

Если экземпляр генеральной цифири кем-то из корреспондентов утрачивался или возникало подозрение, что цифирь оказывалась известной неприятелю, то немедленно издавался императорский указ о выводе этого шифра из действия и замене его другим. Этот указ сразу же рассылался всем корреспондентам, входившим в данную сеть связи. Сохранился один из таких указов, датированный 1776 г. Текст

его содержит достаточно полное описание правил замены утраченной генеральной цифири:

«Указ Ея Императорского Величества самодержицы всероссийской из государственной Коллегии иностранных дел находящемуся в Гданьске поверенному в делах титулярному советнику Волчкову.

Получено здесь известие от полномочного министра при мадридском дворе камергера Зиновьева, что находящийся при нем канцелярский служитель, едучи к нему из Мадрида в Сент-Илдефонс, потерял дорогой вверенные ему, министру, цифирные ключи генеральной корреспонденции.

В рассуждение сего неприятного обстоятельства за необходимо нужно признано здесь для пользы дел и службы Ея Императорского Величества повелеть Вам чрез сие: 1-е: находящиеся у Вас генеральные цифирные ключи 1773-го г. как на руеском, так и французском языках вовсе и таким образом отменить, чтоб оные отнюдь уже Вами нигде и никак употребляемы не были. 2-е: писать сюда впредь от получения сего указа тако же и в переписке Вашей с другими при иностранных дворах находящимися министрами употреблять до получения нового вскоре уже за сим Вам доставляемого генерального ключа, старые генеральные ключи 1768-го года, ибо бывшие после оных ключи 1771-го г. подвержены некоторому сомнению.

Преподавая Вам до времени новых цифирей сие запасное наставление, признано здесь за нужно подтвердить Вам в то же время единожды навсегда, чтоб Вы сами впредь хранили у себя цифирные ключи и заочно не выпускали их из рук, в чем и обязываетесь Вы Вашею присягою верности Ея Императорскому Величеству.

Граф Никита Панин, граф Иван Остерман
В Санкт-Петербурге сентября 12 дня 1776 года.
Отправлен нарочной стафете того же числа» [14].

Обратим внимание читателя на то, что оба документа подписаны графом Паниным. Никита Иванович

Панин был крупнейшей политической фигурой той эпохи. С его именем тесно связаны блестящие успехи России в области внешней политики в первое 20-летие царствования Екатерины II. Лично не расположенная к Панину, императрица ценила в нем искусного политика, который, не будучи человеком сильной инициативы, всегда готов был откликнуться на ее запросы, внести ясность в ее намерения и выгодно отличался от многих современников своим широким образованием, гуманностью и неподкупной честностью.

Родился граф Никита Иванович Панин в Данциге 15 сентября 1718 г. Проведя молодость в военной службе, он начал дипломатическую деятельность в 1747 г., когда назначен был посланником в Копенгаген. В следующем году, 31 января, Панин был переведен посланником в Стокгольм и пробыл здесь 12 лет до 18 февраля 1760 г. С падением Бестужева-Рюмина он был отозван и назначен 29 июня 1760 г. воспитателем к Великому Князю Павлу Петровичу. При императоре Петре III он тайно примкнул к партии императрицы Екатерины и поэтому вступление ее на престол открыло ему широкий путь к возвышению. С 1762 г. он состоял неофициальным советником императрицы по делам внешнего и внутреннего управления, а после отъезда канцлера графа Воронцова в заграничный отпуск занял 17 октября 1763 г. место «старшего члена Коллегии иностранных дел» с обязанностью «производить все иностранной коллегии дела». В 1764 г. Панин предложил императрице свою политическую систему, которой он дал название «Северного аккорда» и сущность которой состояла в союзе России с Пруссией, Польшей, Англией, Швецией и другими северными государствами против Австрии, Франции и Испании. Перечисленные северные державы имели, однако, слишком много счетов между собой, чтобы согласиться на совместные действия. Фридрих II, которому нужен был только союз с Росси-

ей, всячески препятствовал осуществлению проекта. Старания Панина привлечь Швецию к «Северному аккорду», дав победу в этой стране русскому влиянию над французским, стоили громадных издержек, но не увенчались успехом. С конца 1764 г. Панин состоял «первоприсутствующим» в Коллегии иностранных дел. 22 сентября 1767 г. возведен был в графское достоинство и получил чин действительного тайного советника. По вступлении в брак Великого Князя Павла Петровича Панин оставил должность воспитателя цесаревича и вслед за тем 22 сентября 1773 г. получил почетное звание «министра первого класса». Положение Панина при дворе поколебалось в 1781 г. В мае этого года он взял отпуск и выехал из Петербурга, но в сентябре вернулся и вновь вступил в управление делами иностранной политики. Однако не восстановил своего влияния. Умер Н. И. Панин в 1783 г.

В период 1762—1783 гг. во многом именно по указаниям Н. И. Панина изготовлялись новые шифры и проводилась работа по дешифрованию иностранной переписки. Кроме того, под его руководством осуществлялись отдельные («активные») мероприятия по добыче иностранных шифров.

В архивах сохранилось множество документов, свидетельствующих о деятельности Панина в качестве руководителя шифровально-дешифровальной службы России. Так, например, на изученном нами экземпляре генеральной цифири 1768 г. имеются записи:

*«Его сиятельство граф Никита Иванович (*Панин. — *Т. С.) изволил приказать, что скорее сделаны были две цифири, одна русская, а другая французская, совсем от нынешних отменные, с порядочными по алфавитами шифрантами; и чтоб по два экземпляра каждой цифири и шифранта к нему потом прислано было. В Петергофе 13 июля 1768 года».*

«По сей записи все исполнено. И цифири с шифрантами... посланы к его сиятельству в Петергоф в 28-го сего июля».

Как видим, на составление генеральной цифири по приказанию Панина понадобилось всего четырнадцать дней.

Для ведения переписки, в том числе и шифрованной, все крупные политические и военные деятели России имели специальный штат канцелярских работников. Шифрование и расшифрование текстов сообщений производилось специальными секретарями-переводчиками, каждый из которых владел двумя-тремя иностранными языками. Примером того, как было организовано ведение секретной переписки, в том числе шифрованной, крупными государственными деятелями могут служить документы о переписке князя Голицына.

15 декабря 1768 г. императрица Екатерина II подписала указ Коллегии иностранных дел, в котором говорилось:

«Служба наша требует, чтоб назначенный от нас к командованию главной нашей армией против Порты Оттоманской генерал-аншеф князь Голицын беспрепятственную корреспонденцию производил с министрами нашими при других дворах находящимися. Потребное в том наставление дано ему от нас самих, а Коллегии иностранных дел чрес сие повелеваем... предписать... нашим министрам, дабы они о всем происходящем в их местах достоином и нужном к сведению его генерал-аншефа прямо от себя ему сообщали... Коллегия иностранных дел, исполняя сие наше повеление, собою при том усмотрит, что для безопасности такой корреспонденции цифирные ключи и потребные к тому канцелярские служители означенному генералу даны быть долженствуют, нужно с переводчиками польского и турецкого языков, потому что ему в них вседневная почти нужда предстоять будет.

Екатерина» [15].

Уже через неделю, 23 декабря 1768 г. князю Голицыну Коллегией иностранных дел были направлены необходимые цифирные азбуки, в том числе и генеральная, кроме того выделен такой штат помощников и переводчиков для секретной переписки: «Для корреспондования на латинском, французском, немецком и итальянском языках — надворный советник Фридрих Крейдеман, для турецкого языка — переводчик Василий Пастушков, для латинского и польского языков — переводчик Василий Слогвинский, для письма на иностранных языках — переводчик князь Михайло Вадбальский, да для письма российского — два канцеляриста: Александр Катытулов и Семен Александров» [16].

Всем этим лицам Коллегией было определено высокое годовое жалованье и выданы подъемные. А ведь сам Голицын также неплохо владел латынью, немецким и французским языками. Но ведение секретной шифрованной переписки было делом очень трудоемким и, естественно, специальный штат работников для этой цели был просто необходим. Они имели в своем распоряжении шифры того лица, к кому были приставлены, и вели всю его переписку в соответствии с особыми инструкциями, создававшимися в Коллегии иностранных дел. Для повышения надежности переписки необходимо было пользоваться постоянно разными шифрами, употребляя их попеременно, «чтоб в случае, ежели б две или три пиесы вдруг шифрованы быть надлежали, оные разными цифирьми писаны были». Особое внимание следовало уделять знакам, обозначающим ту или иную цифирь. С одной стороны, корреспонденту своему шифрующий должен был указать тот шифр, которым он пользовался, с другой стороны, эту информацию необходимо было как можно старательнее скрыть. Поэтому заглавия цифирей следовало шифровать в самом начале шифрсообщения, но «между пустыми и ничего не знаменующими числами», а

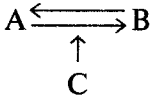
также еще много раз таким же способом в других строках.

Высшие государственные лица России в конце XVIII — начале XIX вв. придавали большое значение криптографической службе. Лично государственный канцлер, а им в тот период являлся граф Иван Остерман (сын Андрея Остермана), неукоснительно следил за строжайшим соблюдением правил пользования отечественными шифрами, требовал их своевременной замены. При малейшем подозрении о компрометации шифров давал указания об их досрочной замене или о внесении в них существенных изменений. Так, в январе 1800 г. Остерман приказал русскому послу в Берлине вывести из действия общий код 1799 г., поскольку возникло подозрение о его компрометации: код этот мог попасть в руки противника вместе с багажом одного русского генерала во время революции во Франции. Аналогичное подозрение о возможной компрометации вынудило вывести из действия код послов в Мадриде и Лиссабоне, хотя он использовался в течение не полных девяти месяцев. Русские послы предупреждались, что все конфиденциальные сообщения должны тщательно шифроваться с помощью одного из новых ключей. Это следовало делать и в том случае, если сообщения посылались с курьерами. Уже Панин в качестве дополнительной меры предосторожности писал многие свои сообщения невидимыми (симпатическими) чернилами, помещая их под маскировочный текст, т. е. текст отвлеченного содержания. Тем самым гарантировалась сохранность сообщений от тайной перлюстрации (по современной терминологии — неявной компрометации), поскольку проявление симпатических чернил сразу указало бы на то, что письмо побывало в чужих руках.

Русской разведке того времени принадлежит идея использования контролируемых каналов шифрованной связи не только для «пассивного» дешифрования пере-

даваемых по этим каналам сообщений, но и активного их использования в целях получения определенной информации, в первую очередь интересующей разведку и руководителей государства. Это замечательный факт в истории именно отечественной криптографии, который на протяжении всех последующих периодов времени не терял своей актуальности и является актуальным в настоящее время.

Схема этой идеи следующая:



Здесь С контролирует канал связи между А и В, которые об этом не знают и не догадываются. С теми или иными способами, но достаточно аккуратно, побуждает А послать В интересующую С информацию. Способы эти могут быть самыми разными и определяются полностью искусством С влиять нужным образом на А, чтобы тот послал В требуемую информацию. При кажущейся простоте этой схемы (или идеи) в практике разведок она встречается крайне редко и каждый раз при этом она выдается чуть ли не за новое гениальное открытие участвующих в этом специалистов. Представляется, что такая ситуация объясняется тем, что разведки всех стран, по-видимому, не очень заботятся о знании истории мировой и, в частности, русской криптографии, о накоплении и использовании исторического опыта.

Итак, 26 марта 1800 г. из Петербурга русскому послу в Берлине сообщалось: «В нашем распоряжении есть шифры, с помощью которых переписывается король [Пруссии] со своим поверенным в делах в России. В случае, если у Вас возникнут подозрения в вероломстве министра иностранных дел Пруссии графа Кристиана фон Хаунвитца, то

Ваша задача будет состоять в том, чтобы под каким-то предлогом заставить его написать сюда письмо по интересующему нас вопросу. И сразу же, как только будет дешифровано его письмо или письмо его короля, я проинформирую Вас о содержании» [17].

Приведем лишь один пример, когда идея активного использования контролируемого канала связи выдвигается в криптографической практике как бы впервые. Речь идет о ситуации, сложившейся в апреле—июне 1941 г. на Тихом океане в период подготовки нападения немцев на англичан. В это время американской стороной был частично дешифрован военно-морской код Японии, в результате чего американцы могли читать подавляющее большинство обычных сообщений. Из дешифрованной с помощью этого кода переписки следовало, что японцы готовят удар по американцам, но о месте удара было только известно, что его кодовое обозначение «AF». По ряду соображений была высказана гипотеза, что «AF» — это остров Мидуэй и цель японцев — начать крупные военные операции с высадки десанта и захвата этого острова. От правильности этого предположения «зависели как само существование американского флота, так и будущий ход всей войны на Тихом океане» [18]. В этой обстановке возникла идея передать по радио открытое сообщение из гарнизона Мидуэя, которое наверняка было бы перехвачено японцами и сообщено по радио (в шифрованном виде) командованию. Их зашифрованное донесение будет перехвачено и дешифровано американцами, и, если предположение верно, географический указатель, который используют в этом случае японцы, будет соответствовать Мидуэю с соответствующим кодовым обозначением «AF». Так и случилось на самом деле. Криптографы, подсказавшие эту идею, были награждены высокими орденами.

Известно, что стремление сохранить в тайне содержание своей деятельности заставляло применять шифры членов всех тайных организаций во все времена и во всех странах. Эти же традиции существовали и в России. В XVII — XVIII вв. в среде раскольников, офеней, разбойников был широко распространен тарабарский язык — своеобразный шифр для устного общения. В нем слова говорились «навыворот». Например, вопрос: «Давно с Дону?» звучал как «Онвад с Унод?» По современной классификации этот язык соответствует частному случаю применения шифра перестановки. В средние века применялись шифры в писаниях «еретиков» и т. д. Еще в начале XVIII в., по преданиям не без участия Петра I, проникли в Россию некоторые системы масонских организаций, к тому времени нашедших уже широкое рапространение в Европе.

Особую организационную и деятельную активность «вольные каменщики» начали проявлять в последней трети XVIII в. Вначале относившаяся к ним лояльно, Екатерина II постепенно изменила свои взгляды, что и повлекло те гонения на масонов, которым они подвергались со стороны правительства уже с конца XVIII в. «Благодушно-презрительная точка зрения императрицы на «свободных каменщиков» помогла беспрепятственному внедрению и развитию масонства в России в течение первых двадцати пяти лет ее царствования, до тех пор, пока она под «чудачествами» и «странными одеяниями» не стала прозревать вольномыслия, опасного для самодержавной своей власти: в действиях масонов она увидела резкое проявление новой, только что нарождавшейся общественной силы, и среди масонов — почти всех лиц, которые известны были несочувствием ее правительственной системе и ее личному материалистическому «умоначертанию», а

во главе их — своего сына и наследника, великого князя Павла Петровича» [19].

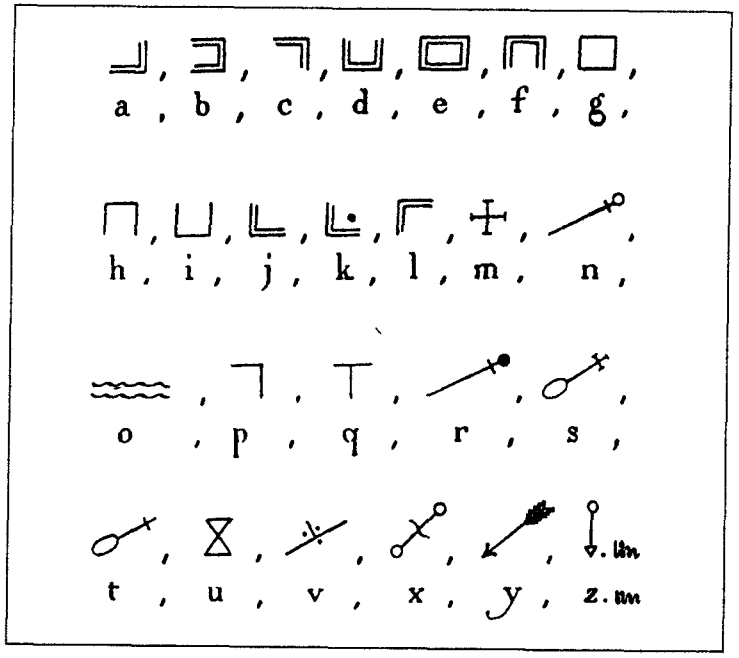
На отношение императрицы к масонству оказала влияние Французская революция. Взятие Бастилии и последующие события развеяли все «демократические» иллюзии русской императрицы. Она уже сравнивает членов Учредительного собания с Пугачевым и решает вопрос довольно просто: «До сих пор считали заслуживающим виселицы того, кто будет замышлять разрушение страны, а тут занимается этим целая нация или, лучше сказать, тысяча двести депутатов этой нации. Если бы повесили из них несколько человек, то я думаю, что остальные бы образумились» [20]. Такое отношение к французскому движению делало императрицу особенно внимательной к аналогичным движениям внутри ее монархии. К тому же к 80-м гг. XVIII в. в Германии началось усиленное преследование тайных обществ, имевших отношение к масонству. В борьбе с представителями тайных обществ немецкие правительства не применяли никаких выработанных юридических норм, преследуя их законными и незаконными способами. Екатерина внимательнейшим образом изучила деятельность российских масонов. Одним из главных источников информации служила их переписка.

Из книги Я. Л. Барскова «Переписка московских масонов XVIII века» [21] можно видеть, как много внимания уделяло правительство частной переписке всех заинтересовавших его лиц. Московский почтдиректор И. Б. Пестель (отец декабриста), занимавший этот пост с 1789 по 1806 г., снимал копии с писем масонов в двух экземплярах. Один из них предназначался для московского главнокомандующего князя Прозоровского, другой же отсылался в Петербург графу Безбородко, который сообщал наиболее интересные письма Екатерине II.

Любопытное, на наш взгляд, замечание делает редакция известного журнала «Русская старина» о содержании перлюстрированной при Екатерине II

переписки: «Перлюстрации внутренней и внешней корреспонденции времени Екатерины II «Русская старина» обязана обширным собранием весьма интересных материалов: это переписка лучших, образованнейших людей 1790—1795 гг.» [22].

По традиции, сложившейся в Европе, в своей переписке масоны использовали особые шифры. Внешне в своем большинстве они выглядели как шифры простой замены, где буквы алфавита заменялись особыми графемами — «гиероглифами» по терминологии того времени. Однако это были гораздо более сложные, так называемые семантические шифры.



Трудность дешифрования здесь обусловлена тем, что учение «вольных каменщиков» проводило в жизнь свои гуманитарно-философские идеи, воплощая их в целый ряд символов и обрядов. «Символ предоставляет мысли свободу, простор; догмат сковывает, подчиняет. Язык в ложах наших иносказательный», — учили масоны-риторы. И действительно, были установленные условные наименования для предметов, имевших отношение к обрядам, внутреннему распорядку, обиходу, всей жизни масонов. Глубина постижения сокровенного смысла символов, обрядов и т. п. зависела от степени масонского посвящения. Особенное место занимали здесь теоретические степени посвящения.

Например, в русских архивах сохранились многочисленные списки предметов занятий масонов в степени теоретических братьев, но многие из них написаны шифром, и расшифровка их весьма сложна, ибо с глубоко рассчитанной постепенностью открывали обряды посвящения целый ряд символов, возбуждая цепь идей. Одному символу можно было придать различные значения в зависимости от идей, заключенных в данной степени посвящения. Так, например, циркуль, открытый на шестьдесят градусов, как символ высшего разума, носился всеми членами ордена. «Помятуйте, — писалось в Вольно-Каменщическом уставе, — что совершенный Великий Мастер далеко распростертым циркулем размеряет и испытует вашу работу; для сего размеряйте действия свои циркулем разума» [23]. Таким образом, при взгляде на шифрзнак, обозначающий в шифре циркуль, масон вспоминал и Великого Строителя мира, и данные им в ложе обеты вести строго обдуманную жизнь. Однако этим значение такого шифрзнака не исчерпывалось. Он мог обозначать еще довольство ниспосланной Провидением долей, напоминал каждому брату о предназначенном ему круге действий, призывал к братскому единению. Наконец, под циркулем представляли солнце, св. Иоанна Крестителя, Януса, огонь, Меркурий, дух, волю, сердце, красоту. Решающее значение для дешифрования масонских текстов имеет знание обрядов и символов. Один из крупнейших русских масонов конца XVIII — начала

XIX в. граф М. В. Виельгорский поучал братьев: «Каменщик должен всячески вникать в таинственные обряды наших лож, где каждый предмет, каждое слово имеет пространственный круг значений и сие поле расширяется, подобно как, всходя на высоту, по мере того как возвышаешься, то видимый нами горизонт распространяется».

Переписка русских масонов перлюстрировалась уже с июля 1790 г. 22 апреля 1792 г. был арестован и затем посажен в Шлиссельбургскую крепость Н. И. Новиков — известный издатель, один из руководителей масонского движения в России. Позднее другой масон сенатор И. В. Лопухин, автор «Нравоучительного катехизиса истинных франкмасонов», писал об этих событиях: «Неудовольствия оныя правительства, подозрения, скрытные присмотры полиции, толки и шум публики, то уменьшаясь, то прибавляясь, продолжались лет семь. Много имели мы неприятелей, а защитников с голосом никого, ни при дворе, нигде. Мы столько были невинны, что и не старались оправдываться, а только при случаях простодушно говорили правду о цели и упражнениях нашего общества, но нам не верили.

Хотя и собрания наши наконец пресеклись, однако подозрение на нас нисколько не уменьшилось. Открывали на почте наши письма, и всех моих писем копии, особливо к одному тогда приятелю, бывшему в чужих краях, отсылались к Государыне. Я сим ни мало не беспокоился и знавши писал всегда так, как бы я говорил наедине в полной откровенности.

Однажды вздумалось мне воспользоваться сим обстоятельством, чтобы в письме к моему приятелю... описать все существо и действие нашего общества... Я написал все сие точно для того, чтоб она прочитала» [24].

Перлюстрация существовала и в последующие царствования. Так, император Павел I, в юные годы сам посвященный в одну из высших степеней масонства, находясь под влиянием своих воспитателей масонов графа Н. И. Панина и князя А. Б. Куракина, позднее охладел к движению «вольных каменщиков». Перлюстрация частной переписки в павловскую эпоху проводилась активно, и сам император даже не считал нужным скрывать этого. В Москве было перехвачено письмо некоего чиновника Приклонского к И. М. Муравьеву совершенно невинного свойства. Однако этим письмом граф Ф. В. Ростопчин воспользовался для того, чтобы погубить своего врага графа Н. И. Панина. Он изменил в нем имена, чем придал письму порочащий Панина смысл, и в таком виде показал его Павлу [25].

Глава восьмая

НОВЫЙ ВЕК

Криптографическая служба России в первой половине XIX века

Начало XIX в. ознаменовалось бурными политическими и военными событиями. Как сто лет назад до этого многое в Европе и все в России определялось личностью и деятельностью Петра Великого, так теперь все в Европе и многое в России оказалось в вихре событий, определявшихся появлением и деятельностью другого гиганта — Наполеона Бонапарта Возникали и распадались военные и политические союзы, победы сменялись поражениями Война создавала героев и кумиров, диктату войны подчинилась логика политики

Фундамент Российского государства, заложенный в XVIII столетии, оказался достаточно прочным для того, чтобы теперь, в годину небывалых испытаний, выдержать все и одержать победу. Немало способствовали этому и успехи русских криптографов

В начале века была проведена реорганизация высшего государственного управления России, которое в течение всего XVIII века сохраняло коллегиальные начала. Высочайшим манифестом императора Александра I от 8 сентября 1802 г. вместо коллегий учреждались министерства. Одновременно с созданием Министерства иностранных дел именным указом

правительствующему Сенату министром иностранных дел и государственным канцлером был назначен граф Александр Романович Воронцов, который с 1761 по 1768 г. состоял полномочным министром в Англии, а в 1773 г. был назначен президентом Коммерц-коллегии. Этот ответственный пост граф занимал до 1794 г., когда вышел в отставку Теперь император вновь призвал его на государственную службу, как одного из просвещеннейших сановников екатерининской эпохи.

Тем же манифестом министрам вновь учрежденных министерств было предписано немедленно заняться образованием своих канцелярий и подбором для них штатов. А. Р. Воронцов также создает временную канцелярию. Канцелярии МИД впервые было дано определенное устройство с разделением на четыре экспедиции. Первая экспедиция ведала азиатскими делами, вторая — перепиской с Цареградской миссией и всеми внутренними делами, третья — «перепиской на французском языке с министрами в чужих краях и внутри государства», а также выдачей заграничных паспортов, четвертая — нотами и записками от иностранных министров, получаемыми или доставляемыми. Каждая экспедиция была вверена управляющему (коллежскому советнику). Были образованы и три секретные экспедиции: первая — цифирная (шифровальная), вторая — цифирная (дешифровальная) и третья экспедиция — газетная (служба перлюстрации). В состав первой цифирной экспедиции входила литография, о работе которой мы расскажем особо. Обязанности управляющего канцелярией МИД определялись так: он «надзирает вообще, ко всем экспедициям; за порядком архива и регистрацией; ему поручается хранение цифирных ключей и весь внутренний порядок канцелярии, а также сношение с главным директором почт, переписка с нашими министрами вне государства» [1] Следовательно, вся

криптографическая деятельность, а также руководство службой перлюстрации были сосредоточены в канцелярии МИД. Руководил этой работой под непосредственным наблюдением министра управляющий канцелярией.

Возможно, читатель обратил внимание на то обстоятельство, что, рассказывая о криптографической службе XVIII столетия, мы постоянно стремились подчеркнуть важность участия в руководстве ее деятельностью высших государственных лиц. Стиль этого руководства, собственно личность высшего государственного чиновника во многом определяли отношение государства к этой службе и, как следствие, ее успехи или неудачи.

В 1806 г. министром иностранных дел назначается барон А. Я. Будберг. Это назначение бывшего генерала от инфантерии было обусловлено, кроме его успешной деятельности в Стокгольме в 1797—1801 годах и близости его к императору Александру I, также тем, что он всецело разделял мысли царя о необходимости продолжения вооруженной борьбы с Наполеоном. Мирный договор с Францией, подписанный русским поверенным П. Я. Убри в Париже 8 июля 1806 г., не был утвержден императором Александром I, причем новый министр иностранных дел барон Будберг разъяснил Государственному совету, что Убри не понял данного ему поручения и превысил свои полномочия. Решено было продолжать войну, и русская армия 22 октября 1806 г. перешла границу, выступив на защиту Пруссии. В бытность Будберга министром экспедиции Канцелярии получили названия отделений, во главе которых, как и раньше, находились управляющие. Ими были: М. Ф. Юдин, П. Я. Убри, А. А. Жерве, С. М. Броневский. Канцелярия министра очень быстро сосредоточила в себе всю политическую переписку с дипломатическим корпусом и с русскими представителями за границей.

Поражение под Фридландом 2 июня 1807 г. показало нецелесообразность дальнейшей борьбы с Наполеоном и привело к заключению перемирия 9 июня. Враждебное отношение к Франции сменилось отношениями тесного союза. 13 июня 1807 г. состоялось свидание императора Александра I с Наполеоном на плоту, посреди реки Неман, против Тильзита. 25 июня (7 июля) 1807 г. вместе с мирным договором подписан был в Тильзите трактат наступательного и оборонительного союза с Францией. Вполне естественно, что уже 30 августа 1807 г. барон Будберг высочайшим указом был уволен с поста министра иностранных дел, а 12 февраля следующего, 1808 г., он окончательно вышел в отставку.

В начале XIX в. канцелярия МИД не имела строго определенного устройства и дела ее распределялись среди личного состава по усмотрению министра. До 1808 г. начальником I экспедиции, куда входила цифирная часть, являлся А. А. Жерве. Затем он назначается управляющим канцелярией, а начальником этой экспедиции, преобразованной в отделение, становится Х. И. Миллер. Дешифровальную часть в этот период возглавляет Христиан Бек. Сохранились некоторые документы, позволяющие судить о характере деятельности секретной экспедиции канцелярии МИД периода начала XIX в. и войны с Наполеоном.

Письмо от 8 марта 1812 г. Х. И. Миллеру:

«Г. Канцлеру угодно, чтобы Вы, милостивый государь мой, Христиан Иванович, немедленно занялись составлением двух совершенно полных лексиконов как для шифрования, равно и для дешифрования на российском и французском языках, и чтобы Вы снеслись по сему предмету с Александром Федоровичем Крейдеманом, стараясь соединенными силами привести работу сию к скорейшему и успешнейшему окончанию.

А. Жерве» [2].

Х. И. Миллер и А. Ф. Крейдеман являлись не только составителями лексиконов, т. е. словарей к шифрам, но и самих шифров. Эту работу выполняли и некоторые другие сотрудники. После составления цифири специалистом-криптографом в XVIII в. она набело переписывалась от руки специальным секретарем в нужном количестве экземпляров. Теперь цифири изготовлялись уже типографским способом. В отношении каждой цифири заведующим секретной экспедицией при этом составлялась докладная записка такого содержания:

«В Государственную коллегию иностранных дел.

От нижеподписавшегося покорнейшее доношение.

Составив по приказанию сей Коллегии новую генеральную цифирь на российском и французском языках, ею одобренную, и отобрав цены за изготовление передвижных машин, равно и за напечатание наборных и разборных таблиц и за бумагу, имею честь представить о том подробную записку, прося покорнейше помянутую Коллегию благоволить на сей расход определить сумму.

Коллежский советник Христиан Миллер.

Октябрь дня 3 1804 года.

За машины:

за 15 пар машин с двойными передвижными дощечками по 125 р. за пару — 1875 рублей.

Типографщику:

за набор разборных таблиц для российской цифири с напечатанием по 20 р. за таблицу — 40 р.

за набор двух разборных таблиц для французской цифири с напечатанием по 20 р. за таблицу — 40 р.

за набор одного листа и напечатание чисел и букв, принадлежащих к разборным таблицам обеих сих цифирей, — 10 р.

за набор 112 $^1/_2$ страниц российской наборной азбуки и напечатание по 30 р. за страницу, а за все 112 $^1/_2$ страниц — 3375 р.

за набор 122 $^1/_2$ страниц французской наборной азбуки и напечатание по 30 р. за страницу, а за все 122 $^1/_2$ стра-ницы — 3675 р.

Бумаги:

Александрийской 83 л. по 2 р. 50 к. каждая — 207,50

Итого 9222 р. 50 к.

Коллежск. сов. Хр. Миллер» [3].

В начале XIX в. в МИД был организован так называемый цифирный комитет, в состав которого вошли наиболее опытные и квалифицированные криптографы. В задачи комитета входил анализ и введение новых систем шифров, контроль за их правильным использованием и хранением, вывод из действия устаревших или скомпрометированных шифров, составление заключений, отчетов и докладных для руководителей МИД и императора по вопросам деятельности шифровальной и дешифровальной службы. Этот комитет подчинялся министру, а возглавлял его «главный член цифирного комитета».

Как и в XVIII столетии, информация, полученная путем криптоанализа, то есть дешифрования переписки, продолжала служить важнейшим источником сведений для Министерства иностранных дел и военного ведомства России. Русские дешифровальщики сыграли значительную роль в первом поражении до тех пор непобедимой наполеоновской армии. Д. Кан пишет: «Этот военный гений вполне определенно не придавал большого значения криптографии, хотя и в этих вопросах он не был полностью ограниченным человеком, как его характеризовали некоторые историки». Во время своих военных походов император Франции пользовался двумя системами шифров: «большим шифром» — для связи с командующими крупными военными формированиями и «малым шифром» — для переписки с небольшими армейскими подразделениями. «Большой

шифр» представлял собой код на 200 величин и был подобен «великому шифру» Россиньоля. Интересно, что французы, несмотря на имевшийся печальный для них опыт состязания с русскими криптографами в XVIII в., так его и не усвоили. Они по-прежнему считали свои шифры абсолютно надежными и не допускали и мысли о том, что русские способны их «расколоть», впрочем, как и вообще выиграть войну. Как показала история, они глубоко заблуждались. Позднее Александр I в своих воспоминаниях о войне лично цитировал переписку генералов Наполеона, в свое время дешифрованную российской криптографической службой.

Американский историк Флетчер Пратт приводит такую выдержку из разговора, состоявшегося после войны 1812 г. между Александром I и командующим одним из корпусов армии Наполеона маршалом Макдональдом: «Конечно, — сказал император России Александр, пытаясь успокоить маршала относительно поражений Франции, — нам очень сильно помогло то, что мы всегда знали намерения вашего императора из его же собственных депеш. Во время последних операций в стране были большие недовольства, и нам удалось захватить много депеш». «Я считаю очень странным, что Вы смогли их прочесть, — заметил несколько печально Макдональд, — кто-нибудь, наверное, выдал Вам ключ?» Русский был удивлен. «Отнюдь нет! Я даю Вам честное слово, что ничего подобного не имело места. Мы просто дешифровали их» [4].

В первой половине XIX в. длительное время руководство криптографической службой России осуществлял Карл Васильевич Нессельроде (1780—1862). Дипломатическую службу граф Нессельроде начал в 1801 г. в Берлине сотрудником русской миссии. В 1810 г. он становится статс-секретарем министерства, в непосредственном заведовании которого находилась канцелярия, а в 1826 г. — министром иностранных дел и вице-канцлером. С 1845 г. граф К. В. Нессельроде государственный канцлер. На этом посту он находился до выхода в отставку 18 февраля 1856 г.

Расширение сети шифрованной связи

Как и в XVIII в., шифрованная переписка в XIX в. велась по политическим, военным, экономическим и другим важнейшим государственным вопросам. Прежде всего, это были русские дипломатические представители за границей. Как указывалось выше, по штатам екатерининского царствования русских «министерских постов» за границей было 21; в последний год царствования императора Александра I их было 24. Это были: чрезвычайные и полномочные послы, которые пребывали в двух городах — Лондоне и Париже; чрезвычайные и полномочные посланники в Вене (до 1822 г. здесь был посол), Берлине, Стокгольме, Копенгагене, Дрездене, Мюнхене, Карлсруэ, Франкфурте-на-Майне (с 1815 г.), Риме (с 1803 г.), Неаполе, Турине, Мадриде, Филадельфии (с 1809 г.), Константинополе; министры-резиденты в Гамбурге и Кракове (с 1815 г.); поверенные в делах в Гааге, Штутгарте, Флоренции, Берне (с 1814 г.), Лиссабоне, Тегеране.

Присвоение лицу, аккредитованному при дворе той или иной державы, званий посла или посланника в то время, так же, как и в XVIII в., не было тесно связано с международным положением державы. В царствование Александра I при дворах великих держав послы иногда сменялись посланниками, и наоборот, в зависимости от служебного положения вновь назначавшегося представителя. Так, в Вене с 1801 по 1808 г. пребывали послы, а в 1810—1822 гг. — посланники; в Париже с 1807 по 1812 г. — послы, с 1814 по 1821 г. — посланник, а с 1821-го — посол.

Взаимные юридические отношения уполномоченных различных степеней: 1) послов, к которым были приравнены легаты и нунции, 2) посланников и 3) поверенных в делах — установили выработанным на Венском конгрессе 19 марта 1815 г. регламентом о ранге дипломатических агентов. Особый четвертый разряд дипломатических представителей, а именно министров-резидентов, установлен был на Аахенском конгрессе 21 ноября 1818 г.

Число консульств к концу царствования Александра I увеличилось значительно по сравнению с последними годами XVIII столетия. В 1825 г. было 24 генеральных консульства: в Англии, Бразилии, Молдавии и Валахии, Венеции, Генуе (Сардинском королевстве), Данциге, Египте, Копенгагене, Ливорно, Морее, Нидерландах, Норвегии, Португалии, Персии, Пруссии, Рагузе и Долмации, Сардинии, Сицилии, Смирте, Требизонте, Триесте, Филадельфии, Швеции, Штеттине, кроме того, были генеральный комиссар в королевстве Неаполитанском и комиссар по торговым делам в Мемеле. Консульств числилось 21, вице-консульств — 11, консульских агентов — 3.

Обширная шифрпереписка велась Министерством иностранных дел и по внутриполитическим вопросам. В частности, в тот период она была сопряжена с политикой, проводимой в Средней Азии (Малая, Внутренняя и Средняя Орда, экспедиция капитана Муравьева для решения туркменского вопроса и др.) и на Кавказе. Этими вопросами занимался азиатский департамент МИД. Кстати, в его же ведении была и знаменитая пекинская духовная миссия. Впервые учрежденная императором Петром I и окончательно признанная китайским правительством в 5-й статье Кяхтинского договора 21 октября 1727 г. миссия, во главе которой находился архимандрит, посылалась в составе десяти лиц. Светские члены (в числе четырех или пяти) обязаны были изучать китайский, маньчжурский, а также монгольский и тибетский

языки. Миссию, сменявшуюся периодически и остававшуюся в Пекине не менее десяти лет, сопровождал пристав, назначавшийся обыкновенно из чиновников министерства. Этим приставам поручалось входить в доверительные переговоры с китайцами по делам пограничным и торговым. Естественно, что шифрованная переписка с центром велась при этом активно.

Наиболее существенной переменой в устройстве центрального управления МИД России в период царствования императора Николая I является образование в 1832 г. двух департаментов: департамента внутренних сношений и департамента хозяйственных и счетных дел. Департамент внешних сношений в этот период также приобрел более устойчивую организационную форму. Кроме директора в этот департамент входили: 1) лица, состоящие при вице-канцлере для политической переписки: действительный статский советник барон Р. Ф. Остен-Сакен и статский советник барон Ф. И. Бруннов, 2) чины министерской канцелярии с ее правителем во главе, 3) чины, заведовавшие секретными экспедициями (цифирными и газетной) и литографией, о чем мы ниже скажем особо. Все перечисленные лица, включая управляющих секретными экспедициями, работали непосредственно под руководством вице-канцлера К. В. Нессельроде.

В 1832 г. должность правителя канцелярии исполнял Емельян Афанасьевич Кудрявский, который 19 января 1835 г. был назначен ее директором. В этот же день были учреждены должности старших советников министерства. Высочайший указ вице-канцлеру гласил: «Состоящим в ведомстве министерства иностранных дел тайным советникам графам Лавалю и Беку, и действительным статским советникам барону Роману Сакену, барону Бруннову, барону Шиллингу и Аделунгу всемилостивийше повелеваем быть старшими советниками того министерства». Секрет-

ными экспедициями в то время заведовали Х. А. Бек (дешифрование), П. Л. Шиллинг (шифры и литография), Н. С. Лаваль (перлюстрация). Ф. П. Аделунг руководил учебным заведением иностранных языков, двое же (барон Р. Остен-Сакен и барон Ф. Бруннов), состоя при вице-канцлере, заведовали в ближайшем с ним сотрудничестве важнейшей политической перепиской, причем Остен-Сакен писал по делам Запада, а Бруннов — преимущественно по делам Востока.

В 1846 г. присвоенное ранее наименование трех секретных экспедиций — «Департамент внешних сношений» — было заменено новым — «особая канцелярия министерства». Управляющие экспедициями были непосредственно подчинены канцлеру (гр. К. В. Нессельроде) наравне с директорами департаментов МИД. В особой канцелярии была сосредоточена политическая переписка.

Шифровалась, как и прежде, переписка с российскими представителями за границей, а также переписка внутриполитическая по линии азиатского комитета МИД и с восточными окраинами России.

Что касается развития заграничных учреждений министерства, то в царствование императора Николая I вновь учреждены были миссии в Рио-де-Жанейро (1828 г.), в Афинах (1830 г.), в Брюсселе (1853 г.), при дворах вновь образовавшихся государств: Бразильской империи (1822 г.), королевств Греческого (1830 г.) и Бельгийского (1831 г.). После присоединения вольного города Кракова к Австрии в 1846 г. уничтожена была должность министра-резидента и генерального консула в этом городе. В Испании с 1831 по 1856 г. не было русского представителя, так как правительство не признавало королевы Изабеллы. Во Франции, вследствие недружелюбного отношения императора Николая I к королю Людовику-Филиппу после отъезда посла графа Палена П. П., в течение 1841—1853 гг. в Париже находился исполнявший должность поверенного в делах Н. Д. Киселев.

Были учреждены также генеральные консульства в Сербии (1839 г.), на острове Корфу (1842 г.), в Бейруте (Сирия и Палестина, 1843 г.) и в Андрианополе (1847 г.). Всего в последний год царствования Николая I было 18 генеральных консульств, штатных консульств — 20 и вице-консульств — 5. Число нештатных консульских учреждений увеличилось значительно: в 1854 г. было 86 нештатных консулов, вице-консулов и консульских агентов.

По линии азиатского комитета, как и раньше, велась шифрованная переписка по вопросам управления подвластными России «киргизскими ордами», а также сношений с Бухарой, Хивой, Китаем, Персией. Впоследствии важнейшее значение приобрели события, происходившие на восточных окраинах России, связанные с деятельностью образованного «Амурского комитета».

Барон П. Л. Шиллинг фон Канштадт и его тайна

Постоянное увеличение числа корреспондентов, сетей и линий шифрованной связи, рост объема шифрпереписки повлекли за собой настоятельную необходимость в поисках способа быстрого размножения шифрдокументов. Наконец такой способ был найден и связано это событие с именем выдающегося ученого и изобретателя Павла Львовича Шиллинга фон Канштадта.

Своей разнообразной и плодотворной деятельностью барон Шиллинг прочно вошел в историю отечественной науки и культуры. Родился П. Л. Шиллинг фон Канштадт в апреле 1786 г. в Ревеле в семье командира Низовского мушкетерского полка. По окончании в 1802 г. Первого кадетского корпуса в Петербурге он в чине подпоручика начал служить в Генеральном штабе русской армии. В 1803 г. семейные обстоятельства заставляют Шиллинга оставить

военную службу и перевестись в Коллегию иностранных дел, где он работал переводчиком русской миссии в Мюнхене. В результате обострения отношений России с наполеоновской Францией русское посольство в 1812 г. было спешно отозвано из Мюнхена в Россию. В период Отечественной войны 1812—1814 гг. проявляется одна из замечательных черт личности Шиллинга — высокий патриотизм, безграничная любовь и преданность России. После двукратного ходатайства он получает назначение штабс-ротмистром 3-го Сумского драгунского полка в действующую армию. За храбрость, проявленную в боях, Шиллинг в 1814 г. награжден первым боевым орденом, а затем одной из самых почетных наград — саблей с надписью «За храбрость». В том же году, будучи с армией в Германии, он заинтересовался изобретенным еще в 1798 г. А. Зенефельдером способом литографирования*.

После окончания Отечественной войны уже ничто не побуждало П. Л. Шиллинга оставаться в армии и он подал прошение о возвращении с военной службы в Коллегию иностранных дел. Барклайде-Толли эту просьбу поддержал, и в октябре 1814 г. Павел Львович вернулся к своим занятиям и научным замыслам. В МИДе он сразу же обратил внимание тогдашнего статс-секретаря министерства графа К. В. Нессельроде, в ведении которого состояла, как мы знаем, канцелярия министерства, на только что входивший тогда в употребление в Европе литографский способ печати. Шиллинг был тотчас же командирован на родину изобретения, в Баварию (где добывалась порода камней, наиболее пригодная для литографирования), и, ознакомившись там с этим способом, в 1817 г. устроил министерскую литографию. 12 июня 1818 г. барон Шиллинг был назначен управляющим литографией. Одновременно Шиллинг явился инициатором использования этого метода печати для размножения топографических карт и других военных документов. С этого же времени П. Л. Шиллинг становится заведующим цифирной частью, которая в 1832 г. преобразуется в экспедицию.

* Литография — способ плоской печати, при котором печатной формой служит поверхность камня (известняка). Изображение на литографический камень наносят жирной литографической тушью или литографическим карандашом.

Однако в кругах научной и культурной общественности Шиллинг завоевал всеобщее признание литографированием документов иного рода, а именно китайских рукописей. «Ревностный пропагандист китайской литературы», по выражению синолога академика Клапрота, Шиллинг добился такого уровня воспроизведения китайских рукописей, который был равен «по тщательности и изяществу самым совершенным образцам китайской печати». Клапрот отмечал, что русское издание китайского текста «оставляет далеко позади все, что было издано до сих пор в Европе». Шиллинг был страстным любителем и знатоком восточной культуры. Во время своей поездки по Южной Сибири он собрал ценнейшие коллекции китайских, маньчжурских, монгольских, тибетских, японских и индийских рукописей. Богатейшие собрания этих манускриптов были переданы ученым в Азиатский музей Академии наук в Петербурге. Он собрал также интересные коллекции по этнографии Средней Азии.

Этот безусловно выдающийся человек известен как петербургский знакомый А. С. Пушкина, К. Н. Батюшкова, А. Мицкевича, А. И. Тургенева [5]. Исследователи жизни и творчества А. С. Пушкина при изучении лиц пушкинского круга обращают особое внимание на П. Л. Шиллинга, приводят свидетельства многочисленных встреч великого поэта с Шиллингом и даже некоторые даты. Так, например, 19 ноября 1818 г. А. С. Пушкин и П. Л. Шиллинг в компании с

Н. И. Гнедичем, В. А. Жуковским, М. С. Луниным, А. И. Тургеневым и другими лицами выезжали в Царское Село для проводов уезжавшего в Италию Батюшкова. 25 мая 1827 г. возвратившийся из ссылки в Петербург Пушкин вместе с Шиллингом, П. А. Вяземским и А. А. Олениным принимал участие в прогулке в Кронштадт, а 6 июня Пушкин и Шиллинг были у Карамзиных. В ноябре—декабре 1829 г. Шиллинг готовился к экспедиции в Восточную Сибирь и Китай в сопровождении И. Я. Бичурина, и Пушкин, по словам Н. В. Путяты, собирался ехать с ними, но получил отказ Бенкендорфа. К этому времени относится карандашный портрет Шиллинга, выполненный Пушкиным в альбоме Ек. Н. Ушаковой. О встречах Пушкина и Шиллинга в 1830-х годах писал позднее М. П. Погодин [6].

П. Л. Шиллинг запечатлелся в отзывах современников не только как «умный, ученый», «необычайно толстый человек», «весельчак, отличный говорун», игравший в шахматы две партии одновременно, не глядя на шахматные доски, и побеждавший обоих противников в один и тот же момент. Прежде всего это был выдающийся и известный ученый. Как востоковед П. Л. Шиллинг в 1827 г. становится членом-корреспондентом Академии наук (по отделению языка и словесности). Другой областью научного знания, в которую П. Л. Шиллинг внес значительный вклад, является электротехника. В 1812 г. он впервые демонстрировал на реке Неве в Петербурге взрыв изобретенной им электрической мины, затем повторно опыты взрывания были проведены в 1815, 1822 и 1827 гг. После русско-турецкой войны 1828—1829 гг. электрическая мина Шиллинга была подвергнута войсковым испытаниям, а с 1833 г. осваивалась в специальном саперном подразделении.

Научные открытия Эрстеда, исследовавшего действие электрического тока, проходящего по проводнику на расположенную вблизи магнитную стрелку,

Швейггера, обнаружившего, что если магнитную стрелку поместить внутри рамки, состоящей из нескольких витков проводника, обтекаемого током, то действие тока на магнитную стрелку значительно усиливается, а также Стерджена, сконструировавшего электромагнит, и другие изобретения создали научные предпосылки для успешного решения проблемы передачи сообщений с помощью электрических сигналов.

Во многих странах в то время занимались вопросами электрического телеграфирования, однако П. Л. Шиллинг первым создал практически пригодный электромагнитный телеграфный аппарат. Публичная демонстрация этого аппарата состоялась 21 октября 1832 г. в квартире на Царицыном лугу в Петербурге (Марсово поле, д. 7). На этом доме сохранилась установленная Русским техническим обществом в 1886 г. в связи со 100-летием со дня рождения выдающегося ученого мемориальная доска со следующей надписью: «Здесь жил и умер русский изобретатель электромагнитного телеграфа Павел Львович Шиллинг».

В основу действия первого телеграфного аппарата Шиллинга положено явление отклонения магнитной стрелки в результате действия электрического тока. Аппарат состоял из клавиатурного передатчика и шестистрелочного приемника. Передатчик и приемник соединялись линией из восьми проводов. В приемнике семь проводов включались в мультипликаторы, состоящие из рамок с обмотками, при прохождении тока по которым отклонялись соответствующие стрелки. Восьмой провод был общим [7]. Шиллинг разработал такой телеграфный код, который позволял при передаче единичных сигналов осуществлять прием наибольшего числа букв сообщения при наименьшем числе требуемых для этого линейных проводов и «рабочих знаков», т. е. числа срабатывающих сигнальных дисков, обозначающих дан-

ную букву. В разработанном П. Л. Шиллингом телеграфном коде для шестистрелочного электромагнитного аппарата любая буква алфавита обозначалась одним, двумя или максимально тремя рабочими знаками одного цвета (белого или черного). Требуемое для передачи одной буквы или цифры одновременное нажатие на клавиатуре аппарата максимально четырех (включая общую) одноцветных клавиш было вполне приемлемо. Определение принятой буквы или цифры при одновременном появлении на сигнальных дисках приемника не более трех рабочих знаков также не представляло затруднений.

Таким образом, П. Л. Шиллинг нашел решение, позволившее осуществить наиболее быстрое телеграфирование при наименьшем числе необходимых для этого проводов и наиболее простом определении переданной буквы или цифры (комбинация из одного, двух или максимально трех одновременно появляющихся рабочих знаков).

Для демонстрации работы созданного аппарата П. Л. Шиллинг снял на время у владельцев дома, в котором жил, весь этаж. Клавиатурный передатчик аппарата был установлен на одном конце этажа, где в небольшом зале собрались приглашенные, а приемник — в другом конце этажа, в рабочем кабинете П. Л. Шиллинга. Линейные провода имели длину, несколько превышающую 100 м. Телеграмма, состоявшая из десятка слов, на глазах у собравшихся была быстро и без искажений принята. Это произвело на присутствующих огромное впечатление.

Интерес к изобретению в самых разных кругах русского общества был настолько велик, что демонстрация работы электромагнитного телеграфного аппарата не прекращалась почти до самых рождественских праздников. Выдающийся русский военный инженер того времени К. А. Шильдер, ознакомившись с изобретением П. Л. Шиллинга, после демонстрации аппарата писал своему другу об электромагнитном телеграфе: «В скором времени сообщу тебе еще одно интересное дело. Оно касается проекта телеграфа на неопределенное расстояние, основанного на гальванизме, с помощью которого возможно будет во всякое время телеграфировать с быстротой мысли. Я надеюсь, что он будет когда-нибудь испытан до Москвы, если только опыты в малом виде сделают очевидным то, что в техническом отношении не подлежит малейшему сомнению...» [8].

П. Л. Шиллинг, начиная с 1811 г. и до конца своей жизни, занимался еще одним важнейшим вопросом — созданием линии, практически пригодной для передачи электрических сигналов по изолированному проводу (кабелю). При монтаже телеграфного аппарата медные провода изолировались шелком или просмоленной пенькой. Так, обмотка мультипликаторов была выполнена медным проводом, покрытым одним слоем шелковой пряжи, а соединения между мультипликаторами — медным проводом, покрытым одним слоем пеньки, густо пропитанной озокеритом.

Для прокладки телеграфной линии между станциями в земле П. Л. Шиллинг применял такие же провода, как для изобретенных им же еще в 1812 г. электрических мин. Так как передающая и принимающая станции соединялись восьмипроводной линией, то все восемь проводов заключались в общую пеньковую изоляцию, а затем просмаливались. Провода же, предназначавшиеся для прокладки в воде, изолировались несколькими слоями шелка или пеньки, причем провода, изолированные шелком, в таких случаях покрывались лаком.

В 1836 г. под руководством П. Л. Шиллинга была проложена экспериментальная подземная кабельная телеграфная линия между крайними помещениями здания Адмиралтейства в Петербурге, которая действовала более года. В этом же году Шиллинг предложил линейные провода между телеграфными станциями подвешивать на деревянных опорах.

В следующем году П. Л. Шиллинг начал работу над проектом первой подводной телеграфной линии связи между Петергофом и Кронштадтом, однако она не была завершена в связи со смертью Павла Львовича. 25(6) июля 1837 г. изобретатель электромагнитного телеграфа был со всеми почестями похоронен на Смоленском кладбище в Петербурге.

Итак, научные заслуги Павла Львовича Шиллинга достаточно хорошо известны, его имя с одинаковым уважением произносится как учеными-гуманитариями, так и естествоиспытателями. И все же до сих пор полный спектр научных интересов Шиллинга не представлен его биографами, одна область его деятельности осталась неведомой как для его современников, так и для потомков. Окружению П. Л. Шиллинга было известно, что он состоит на службе в Министерстве иностранных дел в качестве ответственного чиновника. Упоминание об этом его биографическом факте в различных изданиях естественным образом воспринимается современным читателем как деятельность Павла Львовича на дипломатическом поприще, тем более что он предпринимал заграничные поездки, участвовал в научных заграничных экспедициях. На самом же деле П. Л. Шиллинг фон Канштадт состоял в должности заведующего одной из секретных экспедиций Канцелярии МИД, о чем мы уже упоминали, а именно цифирной экспедиции, кроме того, он заведовал литографией министерства. На этих должностях он состоял до конца жизни. П. Л. Шиллинг был одним из крупнейших криптографов XIX века, чья деятельность должна явиться предметом особого научного интереса для историков — специалистов в этой области.

Состоявший с 1817 г. в должности заведующего литографией МИД, бывший членом цифирного комитета с момента его образования в 1823 г., барон Павел Львович Шиллинг работал в цифирном отде-

лении, где составлялись шифры. Заведовал отделением тайный советник Трефурт. В 1828 г. Шиллинг вступает в должность начальника этого секретного отделения.

В историю криптографии П. Л. Шиллинг вошел прежде всего как изобретатель шифров так называемого биграммного типа. Такой шифр он изобрел, работая в цифирном отделении МИД, еще до своего назначения его начальником, и документальные сведения об этом событии имеются в деле I экспедиции за 1823 г. Сохранилось распоряжение Нессельроде цифирному комитету от 22 марта рассмотреть шифр, предложенный П. Л. Шиллингом, а также рапорт членов цифирного комитета Нессельроде по этому поводу от 14 июня.

Словарь биграммного шифра составляют двузначные буквенные сочетания (язык французский), кодовыми обозначениями являются двух-, трех- или четырехзначные числа, «взятые по два раза каждое для переменной передачи буквенных биграмм то одним, то другим числом». Внешне биграммный шифр представлял собой наборно-разборную таблицу, наклеенную на коленкор, при которой имелось обязательное наставление для пользования шифром. Буквенные сочетания словаря такого шифра могли быть русскими или французскими, могли быть и двойные русско-французские словари. Переписка с помощью биграммного шифра, изобретенного П. Л. Шиллингом, велась на французском языке и шифровались при этом биграммы (двойные сочетания букв и знаков препинания) французского алфавита. Тип шифра — простая замена, в основном на 992 знака (992=32×31) с «пустышками». Важно отметить, что шифровались не идущие подряд биграммы открытого текста, а буквы (и знаки), расположенные на длине Т периода транспаранта, на котором расписывалось передаваемое сообщение. Биграммы, таким образом, составлялись «по вертикали» из двух строк

транспаранта: первая буква — из первой строки, вторая — из второй. Если в конце сообщения не хватало знаков второй строки для образования биграммы, то недостающая часть второй строки заполнялась произвольным образом и шифровались уже отдельные знаки.

Вероятностные характеристики шифрованных знаков этой простой замены, конечно, не подчиняются равномерному закону. Вероятность появления каждого шифрзнака определяется произведением вероятностей появления соответствующих ему знаков открытого текста биграммы. Цепные зависимости здесь типа цепей Маркова для знаков языка, расположенных друг от друга на расстоянии 20—25 знаков, как известно, практически отсутствуют. Однако эти вероятности и не такие «редкие», как, скажем, если бы шифровались «горизонтальные» биграммы, составленные из рядом стоящих знаков открытого текста. Эта уменьшенная редкость или, как говорят, «диаграммность» шифрованного текста, усложняет дешифрование сообщений, закрытых таким шифром, хотя, естественно, с современных позиций этот шифр нельзя считать криптографически стойким.

Предельный срок действия каждого из таких шифров был определен Цифирным комитетом в шесть лет, если за этот срок шифр не будет скомпрометирован. Позднее (1858 г.) этот предельный срок был уменьшен до трех лет. Как будет видно из дальнейшего, это правило часто нарушалось, что не могло не сказаться на тайне переписки.

Нам известны некоторые биграммные ключи барона П. Л. Шиллинга. О них есть сведения в «Описи цифирям», составленной Трефуртом, где наряду с данными о других цифирях, составленных со времени образования цифирного комитета, указывается, что «13 августа 1823 г. от члена оного Комитета Г [осподина] Ст [атского] Сов [етника] Бар [она] Шиллинга фон Канш [тадта] получены его сочинения биграммный

ключ № 1 и № 2, № 3 на франц [узском] языке, а также пакет с бумагами, относящимися к составлению этих цифирей» [9].

В феврале 1824 г. экземпляр № 1 биграммного шифра Шиллинга был направлен цесаревичу Константину Павловичу; в январе 1826 г. тот же первый, а также второй экземпляры даны князю Меншикову при отправлении его в Персию; в 1828 г. граф К. В. Нессельроде получил третий экземпляр этого шифра при отправлении в Америку.

В 1826 г. Шиллинг составил цифирь для адмирала Синявина. В 1827 г. этот экземпляр шифра был передан К. В. Нессельроде, в том же году еще три экземпляра этого шифра направлены в миссию в Вашингтон.

В том же году П. Л. Шиллинг составил «генеральную цифирь» под № 16, партикулярные цифири № 4, 5, 6, 8, 9 и 10, а также «военный шифр» на русском языке № 28.

В литографии, которую Шиллинг организовал и которой заведовал все годы службы в министерстве, проводились работы по размножению и копированию государственных документов. Со времен деятельности Шиллинга в практику МИД вошел обычай каждый день предоставлять на просмотр министру литографированные копии с перлюстрированных документов и писем, большинство из которых, естественно в дешифрованном виде, также направлялось для ознакомления государю. Материалы перлюстрации и дешифрования переписки были обычной темой обсуждения на заседаниях Цифирного комитета.

П. Л. Шиллинг весьма заботливо относился к сотрудникам литографии, учитывая важность их работы. Перед нами одна из докладных его вице-канцлеру Нессельроде, текст которой гласит: «Литографские ученики Ефимов, Пальцев и Григорьев при хорошем поведении усердным исправлением своей должности, а первый из них сверх того и оказанным

искусством в печатании противу своих товарищей, заслуживают внимания начальства, почему долгом поставляю себе испрашивать у Вашего сиятельства в награждение им, первому звание унтер-офицера и 75 рублей, а двум последним по 50 рублей, равно и переплетчику Пазову, занимавшемуся наклейкою цифирных таблиц, 100 рублей» [10].

Перед изучающим историю того или иного вида государственной деятельности неизбежно возникает вопрос выявления отношения самого государства к этому виду деятельности на том или ином этапе. Важнейшим аспектом этой проблемы является осознание государством (олицетворяющими его субъектами) необходимости правильной оценки данного вида деятельности для «нормального», с учетом известных критериев, функционирования государственной системы. Правильная политика в этой сфере, продуманное и своевременное стимулирование могут предотвратить последствия, которые приведут к сбою в работе всей системы. Естественным образом нас в первую очередь интересует отношение первых лиц Российского государства к криптографической службе в различные исторические эпохи.

Значение криптографической службы в обеспечении успешного функционирования государства прекрасно осознавалось, и это мы старались показать читателю, на протяжении всего XVIII столетия. В Петровскую эпоху, когда эта служба только создавалась, приобретала общие очертания, опыт участия в ее формировании высших государственных лиц, включая самого императора, свидетельствовал об осознании государством заинтересованности в ее успешном функционировании. Ярко проявилась эта заинтересованность в елизаветинскую и екатерининскую эпохи, когда проходило становление такой отрасли криптографической деятельности, как дешифровальная служба.

Успехи европейской криптографии требовали от российских специалистов постоянного совершенствования методов работы, упорных теоретических поисков. Государство осознавало необходимость такой деятельности и всемерно ее поощряло. Как и в какой форме осуществлялось поощрение, можно узнать, например, из письма графа К. В. Нессельроде П. Л. Шиллингу от 23 марта 1830 г.:

«Барону Шиллингу фон Канштадту
от графа Нессельроде.

Секретно

М[илостивый] Г[осударь] мой!

Государь император в награду особенных на пользу службы трудов Вашего Превосходительства при составлении и изготовлении новых цифирей, всемилостивейше пожаловать Вам соизволил 1000 червонных голландских, высочайше повелел выдать Вам сию сумму без всякого вычета из государственного казначейства.

Принимавшим под руководством Вашим участие в сем деле коллежскому советнику Нестеровичу и VII класса Иванову пожаловано каждому на том же основании по 2000 рублей ассигнациями; надворный советник Геслер удостоен знаков ордена Св. Анны 2-й степени, императорскою короною украшенных; титулярные советники Гасс и Быков получили следующие чины, а титулярному советнику Рахонину пожалован бриллиантовый перстень в 1000 рублей.

Я поставляю себе за особенное удовольствие уведомить Вас, М[илостивый] Г[осударь] мой, о таковом монаршем внимании к отмеченным заслугам Вашим и к усердной службе находящихся при Вас чиновников, покорнейше прошу Ваше Превосходительство объявить им о пожалованных им наградах» [11].

С большим уважением и вниманием относилось правительство и к научной деятельности Шиллинга, стремясь направить ее в русло, максимально полез-

ное для России. Показательным в этом отношении является еще один документ, а именно письмо того же Нессельроде Шиллингу от 5 мая 1835 г. В этот период Павел Львович серьезно заболел и собрался ехать для лечения на европейские курорты. Выезд за границу на длительный срок для такого важного чиновника, каким являлся барон Шиллинг, требовал разрешения государя. В связи с этим Нессельроде пишет:

«Милостивый Государь, барон Павел Львович!

Вследствие всеподданнейшего доклада, коим я испрашивал высочайшего разрешения о позволении Вашему Превосходительству ехать за границу для поправления минеральными водами расстроенного здоровья Вашего, Государю Императору угодно было изъявить на то всемилостивейшее соизволение и вместе с тем с разрешения Его Величества, дабы соделать пребывание Ваше в чужих краях полезным для службы, поручается Вам заняться нижеизложенными предметами, поколику то обстоятельства Вам позволяют:

1) Ознакомиться с новыми открытиями, сделанными в последних годах в Германии, Франции и Англии в науке электромагнетизма и способами составления искусственных магнитов, от коих можно ожидать весьма важные приложения в механике.

2) Изыскать выгоды и невыгоды телеграфических систем Пруссии, Франции и Англии.

3) Узнать в полноте вновь изобретенный способ доктора Рейхенбаха обугливать до 80-ти куб. сажень дров вокруг в особенно устроенных для сего печах, и наконец,

4) присутствовать в Бонне в собрании естествоиспытателей, имеющее быть там в сентябре месяце.

Признавая пользу вышеизложенных сведений и в уверении, что Вы, милостивый государь, употребите все старание к приобретению оных для распространения в нашем отечестве, Государь Император всемилостивейше повелеть соизволил сохранить Вам, яко чиновнику, и за границей имеющему заниматься делами службы, положенное Вам жалованье...

Нессельроде» [12].

Мы приводим полностью текст этого весьма содержательного документа, ибо он, с одной стороны, подтверждает заботу правительства о здоровье и благополучии ответственного сотрудника МИД — ученого, криптографа, инженера П. Л. Шиллинга фон Канштадта, а с другой стороны, показывает, насколько активно российское правительство и в первой половине XIX в. стремилось использовать достижения мировой научно-технической мысли на благо процветания нашего Отечества. Особо нам бы хотелось обратить внимание читателя на ту положительную роль, которую в этом процессе играли министр иностранных дел граф К. В. Нессельроде и криптограф барон П. Л. Шиллинг.

Глава девятая

РОССИЙСКИЕ ШИФРЫ И КОДЫ ВО ВТОРОЙ ПОЛОВИНЕ XIX — НАЧАЛЕ XX в.

Во второй половине XIX века криптографическая служба России претерпела существенную реорганизацию, в результате которой она перестала быть привилегией МИД, а была создана еще в двух ведомствах: военном и Министерстве внутренних дел. Этот факт свидетельствует о росте значения криптографии в деятельности государственных органов, о существенном расширении сфер ее использования.

Развитие внешних и внутренних сетей связи, рост объема шифрованной переписки повлекли за собой увеличение числа вводимых в действие шифров и кодов. Постепенно выкристаллизовывается классификация шифров по своему назначению и целям.

Шифры разделяются прежде всего по языковому принципу. В зависимости от языка шифруемой информации появляются русские, французские, немецкие, английские и прочие шифры. По отраслевому назначению они делятся на шифры МИД, шифры военного ведомства, включая и императорские шифры, шифры жандармерии и образованного в 1880 г. в структуре Министерства внутренних дел Департамента полиции, а также шифры, которые использовались гражданскими ведомствами для закрытия своей секретной информации (например, Министерства финансов). Особняком стоят агентурные шифры, предназначенные для связи с разведчиками и агентами. Шифры МИД, Военного министерства и Министерства внутренних дел разделялись на секретные и несекретные. Помимо них вводились еще так называемые шифры специального назначения. В одной из инструкций к шифрам МИД говорилось, что несекретными ключами следовало пользоваться во всех тех случаях, когда содержание сообщения само по себе не могло считаться секретным, но когда, тем не менее, передача его в незашифрованном виде почему-либо не представлялась удобной, например, когда желательно было избегать преждевременной огласки передаваемых сообщений в печати и т. п. Интересное добавление содержалось в примечаниях к этой инструкции: «Следует полагать, что несекретные ключи известны иностранным правительствам, тем не менее они представляют безусловную тайну для публики и должны храниться если не с секретными ключами, то, во всяком случае, с секретными делами установлений, которые ими снабжены». Ключи специального назначения использовались для сношения с «различными правительственными установлениями, а также с частными учреж- дениями и лицами».

Рассмотрим подробнее деятельность криптографической службы в каждом из упомянутых министерств и разработанные там во второй половине XIX — начале XX в. шифры.

Совершенствование криптографической службы и шифров МИД

15 апреля 1856 г. граф К. В. Нессельроде оставил управление МИД, сохранив за собой должность государственного канцлера. За шестидесятилетнюю верную службу престолу и государству он был осыпан милостями.

Новым министром иностранных дел назначается лицейский товарищ А. С. Пушкина князь Александр Михайлович Горчаков. До этого назначения он в 1833—1838 гг. был советником посольства в Вене, в 1841—1855 гг. — посланником в Штутгарте, и в то же время с 1850 г. — посланником при германском союзе, а во время Восточной войны с 1852 по 1854 г. вел в качестве русского представителя дипломатические переговоры в Вене. Наиболее видное положение Горчаков занимал в первые годы царствования Александра II, до 1863 г., являясь поборником всех реформ императора. «В Вашей опытности, в пламенной любви Вашей и преданности Престолу и Отечеству, — сказано было в высочайшем рескрипте Александра II на имя князя А. М. Горчакова 19 апреля 1864 г., — я нашел достойного исполнителя всех моих намерений и желаний». 17 апреля 1862 г. Горчаков был возведен в звание вице-канцлера, 13 июня 1862 г. — в день пятидесятилетия поступления на службу — в звание канцлера иностранных дел. 18 марта 1871 г. в день ратификации Лондонского договора о нейтрализации Черного моря он был «всемилостивейше пожалован с нисходящим потомством титулом светлости».

В первые годы управления князя Горчакова Министерством иностранных дел были сделаны некоторые изменения в устройстве канцелярии. Высочайше был утвержден новый штат канцелярии, затем в 1862 г. особая канцелярия (секретная экспедиция) была соединена с канцелярией. В это же время установлены были испытания способностей лиц, «поступающих на службу по министерству».

Следует отметить особо, что, принадлежа к наиболее широко образованному кругу лиц высшего света, князь Горчаков был весьма озабочен развитием отечественной исторической науки. В этой связи он нашел возможность открыть доступ ученым в Государственный и Московский главные архивы министерства, представляющие собой богатейшее собрание исторических документов и материалов. 19 января 1863 г. были высочайше утверждены правила для допуска ученых к занятиям в государственном архиве. Научная разработка всех его сокровищ была значительно облегчена разбором всех его дел, произведенным в 1864—1870 гг. директором архива К. И. Злобиным при содействии историка академика П. П. Пекарского. Благодаря их самоотверженному труду, разработанным ими классификациям и характеристикам документальных источников, нашедшим достойное продолжение в трудах всех последующих поколений работников этого архива, сегодня мы можем работать с грамотно разобранными и систематизированными бесценными историческими материалами.

В результате деятельности по обработке архива МИД еще в 1861—1862 гг. было осуществлено издание «Писем русских государей» в четырех томах, с 1880 г. начал издаваться «Сборник московского главного архива министерства». В 1874 г., почти через сто лет после указа императрицы Екатерины II 1779 г. об издании договоров России с иностранными державами, было начато обширное издание «Собрание трактатов и конвенций, заключенных Россией с иностранными державами». Рассмотрим вопрос о том, насколько обширна была сеть корреспондентов МИД, пользующихся шифрованной связью в рассматриваемый период.

В царствование императора Александра II установился обычай назначения послов при дворах великих держав. В Париж, Лондон, Константинополь, Вену стали прибывать только послы. В 1871 г. учреждено было посольство в Германии, а в 1876 г. — в Объединенной Италии.

В 60–70-х годах были учреждены постоянные представительства при дворах держав Дальнего Востока, Китая и Японии, а также в странах Балканского полуострова — Валахии, Молдавии, Румынии, Сербии, Черногории и в вассальной Болгарии. В этот же пе-

риод назначен был дипломатический агент в Египет и учреждено несколько генеральных консульств: в Восточной Румелии, Эрзеруме и Салониках, а в начале 80-х годов — в Яссах.

В 1875 г. русских посольств за границей было пять: в Берлине, Вене, Константинополе, Лондоне и Париже; миссий — двадцать одна: в Афинах, Берне, Брюсселе, Вашингтоне, Веймаре, Гааге, Гамбурге, Дармштадте, Дрездене, Иеддо, Карлсруэ, Копенгагене, Лиссабоне, Мадриде, Мюнхене, Пекине, Риме, Рио-де-Жанейро, Стокгольме, Тегеране и Штутгарте. Существовало также двадцать шесть генеральных консульств, сорок три консульства и семь вице-консульств.

Еще с 18 мая 1880 г., вследствие болезни светлейшего князя Горчакова, Министерством иностранных дел начинает управлять статс-секретарь Николай Карлович Гирс. До этого он последовательно занимал должности генерального консула в Египте (1856—1858), в Молдавии и Валахии (1858—1863) и в Стокгольме (1872—1875). 2 декабря он был назначен товарищем министра иностранных дел и сенатором и одновременно управляющим азиатским департаментом министерства. 28 марта 1882 г. Гирс назначается министром иностранных дел.

Руководящие начала внешней политики царствования императора Александра III были выражены в циркулярном шифрованном сообщении русским представителям при дворах иностранных держав 4 марта 1881 г., в котором говорилось: «Вступая на прародительский престол, Государь Император наследует предания, освященные временем, деяниями предшественников, трудами, кровью поколений, создавших Русское государство... Россия... ныне достигла своего естественного развития; ей нечего желать, нечего домогаться от кого бы то ни было; ей остается лишь упрочивать свое положение, охранять себя от внешней опасности и развивать внутренние силы, нравственные и вещественные, накопляя запасы средств и умножая свое благосостояние...»

В рескрипте на имя Н. К. Гирса от 18 мая 1883 г. было заявлено, что «мирное развитие сил России должно составить исключительный предмет государственных интересов...»

По указу императора Александра III принятый издавна в политической переписке французский язык был заменен с 1887 г. русским, за исключением тех случаев, когда дипломатические представители сообщали о словесных или письменных переговорах с иностранными министрами, происходивших на французском языке. Между центральным управлением министерства и посольствами и миссиями были установлены с 1888 г. регулярные срочные курьерские сообщения.

В годы царствования Александра III были учреждены новые миссии в Корее, в Мексике, учреждено политическое агентство в Бухаре, генеральное консульство в Сетходе. На 1881 г. за границей находилось 127 посольских и консульских установлений, в последний же год царствования Александра III их было уже 144.

После смерти статс-секретаря Гирса, последовавшей в 1895 г., МИД управлял статс-секретарь Алексей Борисович Лобанов-Ростовский, однако в августе 1896 г. он внезапно скончался.

В 1897—1900 гг. МИД возглавлял Михаил Николаевич Муравьев, а после его смерти — с декабря 1900 г. — Владимир Николаевич Ламздорф.

В 1902 г. у России за границей было восемь императорских посольств, двадцать пять миссий, три политических и дипломатических агента, двадцать девять генеральных консульств, шестьдесят девять консульств и тридцать девять вице-консульств. Всего же различных штатных установлений министерства за границей было сто семьдесят три, кроме того, имелось более трех сотен нештатных кон-

сулов, вице-консулов и консульских агентов. Это широкое развитие сети русских дипломатических и консульских учреждений в иностранных государствах наглядно свидетельствует о том, насколько значительно увеличилась и расширилась сеть шифрованной связи, которая от первоначально более узкой географии применения распространилась до отдаленных стран Азии, Африки, Американского континента.

Рассмотрим некоторые наиболее типичные шифры России, впервые появившиеся и использовавшиеся на линиях связи МИД во второй половине XIX — начале XX в.

Биграммные шифры. Система изобретенного П. Л. Шиллингом биграммного шифра уже была нами описана выше. Коллеги Павла Львовича после его смерти продолжили разработку шифров биграммного типа. Эти шифры использовались активно в течение всего XIX столетия и даже в начале XX. Нами выявлены некоторые из этих шифров.

Французский биграммный телеграфный ключ № 302 создан в 1855 г., введен в действие в 1856 г., выведен из действия в 1867 г. Употреблялся «уполномоченным при Парижском конгрессе» бароном Брунновым для сношений с МИД. Издано было пять экземпляров этого ключа.

Французский биграммный ключ № 303 аналогичен предыдущему. Введен в действие в 1857 г. для сношений МИД с миссией в Дармштадте.

Французский биграммный ключ № 313 аналогичен ключу № 302, введен в действие в 1857 г. Предназначался для консульств на Балканском полуострове (Мостар, Рагуза, Сараево, Белград, Виддин, Янина), миссий в Константинополе и Вене, а также употреблялся для ведения секретной переписки с Азиатским департаментом МИД, Канцелярией и Походной канцелярией. Этот шифр был выведен из действия в 1872 г. «ввиду более чем шестилетнего

использования». Как видим, в нарушение требований цифирного комитета ключ находился в действии 13 лет.

Французские биграммные ключи № 314 и 315 аналогичны предыдущим, введены в действие в 1858 г. Ключ № 314 «вследствие 3-годичного пользования» был заменен биграммным ключом № 328, ключ же № 315 остался в употреблении на длительный срок. Использовались эти шифры для сношений МИД с посольствами и миссиями в Афинах, Берлине, Берне, Бухаресте, Брюсселе, Карлсруэ, Константинополе, Копенгагене, Дармштадте, Дрездене, Франкфурте, Гамбурге, Ганновере, Гааге, Лиссабоне, Лондоне, Мадриде, Мюнхене, Неаполе, Париже, Риме, Стокгольме, Штутгарте, Турине, Варшаве, Вене, Вашингтоне, Веймаре.

Французский биграммный ключ № 316 введен в действие в 1857 г. исключительно для сношений МИД с миссией в Дармштадте. Уничтожен этот шифр в 1867 г.

Французский биграммный ключ № 323 введен в действие в 1860 г. для консульств на Балканах и в Турции (Адрианополь, Битолия, Варна, Белград, Виддина, Вена, Константинополь, Мостар, Рагуза, Сараево, Скутара, Филлиполь, Янина), а также для переписки с МИД генерального консульства в Лондоне. Использовался этот шифр до начала XX в., когда было признано цифирным комитетом, что и впредь его можно употреблять, но «для специальной надобности».

Французский биграммный ключ № 324 также введен в действие в 1860 г., действовал до начала XX в. на линиях связи МИД с Берлином, Константинополем, Лондоном, Парижем, Веной, Бухарестом. Использовался для переписки с генерал-губернатором Одессы.

Французский биграммный ключ № 328 был создан как генеральный. Он имел словарь меньшего объема, чем вышеперечисленные, — 992 двубуквенных

сочетания. Введен в действие в 1861 г. для сношения между собой и с МИД миссий в Афинах, Берлине, Берне, Бухаресте, Брюсселе и других европейских государствах. Выведен в резерв в 1891 г.

Французский биграммный ключ № 329 аналогичен предыдущему. Ключи № 328 и 329 были введены на смену биграммным ключам № 314 и 315.

В 1872 г. вводится некоторое усовершенствование в структуру биграммных шифров. Составитель шифров сотрудник шифровального отдела МИД Нелидов предложил существенно уменьшить число букв латинского алфавита и знаков препинания в открытом тексте (как это использовано в биклавных шифрах, о чем мы расскажем ниже) с тем, чтобы можно было использовать в качестве шифробозначений латинские биграммы и буквы. Поэтому французский ключ № 359/360, изобретенный в 1872 г. Нелидовым, получил название *биграммно-буквенного*. Содержит биграммные сочетания букв латинского алфавита (кроме k, w, y), знаки препинания (. , -) — 676 величин, а также 26 букв латинского алфавита — всего, таким образом, 702 величины. Шифробозначения — двузначные сочетания из 26 букв латинского алфавита и 26 отдельных букв латинского алфавита, служащих для передачи отдельных букв текста. Предназначался для телеграфа, введен в действие в 1873 г. Эти ключи были отосланы в Берлин «для испытания пригодности» и в 1876 г. возвращены обратно в МИД с заключением: «Ключи 359/360 вполне пригодны для французской переписки МИД... и ввиду этого подлежат сохранению». Принцип системы этих шифров биграммный с той лишь разницей, что: 1) две буквы текста передаются не тремя числами, как в биграммах, а двумя буквами; 2) при шифровании двубуквенные сочетания не составляются из букв двух рядов переписанного для этой цели по известному транспаранту текста, но из крайних букв каждой строки переписанного по транспаранту текста, двигаясь с двух концов к середине.

Последнее усовершенствование несло и некоторую криптографическую нагрузку. Поскольку к тому времени стало ясно, что противнику известен принцип шифрования по данной системе, то целесообразно было ввести некоторые изменения в этот принцип, что, конечно, усложняло работу дешифровальщиков. Нужно было еще догадаться, в чем состоят эти изменения.

Вторая группа биграммных шифров — это так называемые *русские биграммные шифры*, по которым шифровались сообщения, написанные на русском языке. Предназначались эти шифры как для внутренней, так и для внешней переписки. Поскольку в русском языке число биграмм превосходило число трехзначных чисел (их вместе со знаками препинания было 1296), то составители шифров пополняли недостающее число шифробозначений — трехзначных чисел — однозначными, двузначными и четырехзначными.

Русский биграммный ключ № 304 — так называемый «генерал-губернаторский шифр», предназначался «для секретного сообщения из Петербурга с теми из генерал-губернаторов, в местопребывании коих находятся телеграфные станции». Это были следующие пункты: Петербург, Москва, Киев, Одесса, Рига, Гельсингфорс, Варшава, Вильно. Имелись экземпляры этого ключа у военного министра, министра внутренних дел и шефа жандармов. Введен шифр в действие в 1857 г. В 1863 г. его экземпляр был отослан генерал-губернатору в Тифлис. Именно этот ключ был первой попыткой составления русского биграммного шифра.

Впоследствии, когда было введено правило о соединении цифр для передачи по телеграфу сначала в трехзначные, а затем в пятизначные группы, пользование этой системой было признано невозможным и она была заменена сначала сочетаниями из цифр и букв для передачи русских двубуквенных сочетаний (как, например, в биграммном ключе

№ 334 — см. ниже), а затем уже биграммными ключами, в которых число букв было сокращено до 28 (ключи № 347, 375, 380, 381 и др.). Эти ключи использовались и в начале XX в. Ключ № 304 был выведен из действия (в своем первоначальном виде) в 1892 г. как вследствие указанных причин, так и вследствие того, что в процессе использования было утрачено большое число его экземпляров.

Русский «двузначный» ключ № 331 также составлен по системе биграммных шифров П. Л. Шиллинга в 1861 г. Этот шифр отличался тем, что не имел двойных чисел в качестве кодовых обозначений. 1296 двубуквенным сочетаниям были приданы 1296 чисел: 7 однозначных, 75 двузначных, 591 трехзначное и 633 четырехзначных. Использовался этот ключ для шифрпереписки между Министерством народного просвещения с попечителями учебных округов, выведен из употребления в 1883 г.

Русский биграммный ключ № 334 был составлен по системе П. Л. Шиллинга Г. Ф. Эстом. Печатал этот шифр, как и другие шифры того времени, Ф. Годениус. Ключ включал 1482 двубуквенных сочетания. Кодовыми обозначениями служили 1500 трехзначных чисел, из которых 1000 — числа от 000 до 999, 500 — сочетания из двузначных чисел с одной из 10 латинских букв, взятых каждая по два раза «для переменной передачи валер» (словарных величин. — *Т. С.*). Шифр этот предназначался для переписки по почте между консульствами «в Турции»: в Адрианополе, Бейруте, Биталии, Бухаресте, Варне, Виддине, Белграде, Иерусалиме, Коржу, Мостаре, Призряне, Рагузе и др. Выведен из употребления в 1872 г. Это был первый русский биграммный ключ, в котором двубуквенные сочетания (словарные величины) передаются при наборе лишь трехзначными сочетаниями. Но ввиду превышающего количества возможных буквенных сочетаний тогдашнего русского алфавита (1396) над количеством трехзначных чисел Г. Ф. Эст,

которому была поручена работа над шифром, дополнил недостающие числа сочетаниями из двух цифр и одной из десяти букв (французского) алфавита. Об этом сохранилась докладная записка барона Дризена в цифирный комитет от 11 января 1862 г. [1] При составлении следующих биграммных шифров для русских текстов обошлись без таких сочетаний цифр и букв, т. к. сократили число двубуквенных «валер» до 1000, исключив некоторые буквы русского алфавита. Так составлены, например, ключи № 347, 356, 375 и др

Русский биграммный ключ № 347 введен в действие в 1865 г. Использовался для переписки МИД с консульствами на Балканском полуострове: в Бухаресте, Константинополе, Галаце, Яссах, Измаиле, Тульче, Белграде. В 1871 г. заменен биграммным шифром № 356, как использовавшийся более четырех лет. Однако в 1903 г. этот шифр вновь был введен в действие «в консульствах Австро-Венгрии», а именно в Будапеште, Сараево, Триесте, Вене и др.

Русский биграммный ключ № 356 введен в действие в 1869 г. «в консульствах на Востоке», где использовался до 1888 г.

Нам известно, что ключ № 356 являлся одним из тех шифров, экземпляры которых были украдены из Российской миссии в Пекине 19 августа 1888 г. Вследствие этого шифр был выведен из употребления, но лишь на некоторое время. Несмотря на очевидность компрометации, в начале 90-х годов ключ № 356 вновь ввели в действие, но уже в другом регионе. В 1894 г. он был направлен в Амстердам, Гаагу, в 1896 г. — в Берн, Женеву, в 1893 г. — в Гаммерфест и Стокгольм. В 1898 г. произошла еще одна компрометация этого шифра: один экземпляр его был утрачен начальником Адриатической эскадры. Вероятно, именно это событие, наконец, заставило руководителей шифрслужбы окончательно изъять ключ № 356 из употребления, как ука-

зывалось в соответствующем заключении «вследствие почти $^1/_4$-векового всемирного использования». Нам известно, что за весь период применения его использовали в 124 пунктах.

Русский ключ № 361, подобный предыдущему, был составлен Нелидовым в 1876 г. Этот ключ содержит биграммные сочетания из 28 букв упрощенного русского алфавита, знаков препинания и 31 отдельной русской буквы и знака. Всего, таким образом, его словарь содержал 992 величины, которым соответствовали трехзначные кодовые обозначения. Вначале ключ этот был разослан в консульства на Востоке: в Александрию, Афины, Бухарест, Пекин и др., затем распространен на Австро-Венгрию, Персию, Балканский полуостров, а, кроме того, направлен в Тифлис, Одессу. Во время турецкой войны этот шифр отослали в действующую армию (генерал Игнатьев, барон Фредерикс, великий князь Михаил Николаевич), военному губернатору в Болгарии, адмиралу Лесовскому, контр-адмиралу Крамеру. С 1882 г. он использовался в различных консульствах в Европе, а также на международном конгрессе. Несмотря на то, что экземпляр этого шифра был также украден в Пекине в 1888 г., его окончательно вывели из действия лишь в 1903 г. Но и после этого тогдашний начальник шифровального отдела МИД и член цифирного комитета барон Таубе писал: «ключ № 361 может применяться как временный в специальных случаях, кроме Дальнего Востока».

Совершенно очевидно, что российским криптографам того времени представлялось возможным использовать шифры на линиях связи в каком-то регионе даже в тех случаях, если они были скомпрометированы в другом регионе. Вероятно, решающим обстоятельством здесь являлась дальность расстояния. Такое же эйфорическое настроение вселяло в криптографические умы и понятие времени: выведенный из действия в какое-то время шифр,

возможно даже скомпрометировнный, мог вновь вводиться в действие через значительный промежуток времени. Очевидно, предполагалось, что за давностью времени он оказывался абсолютно забыт противником.

Автором французских двубуквенных ключей № 362 и 363 также являлся Нелидов. Изобретенные в 1876 г., они подобны биграммным ключам № 359, 360 и 361. Об этих ключах барон К. Таубе также писал, что их можно использовать и в начале XX в.

Биклавные шифры. После смерти П. Л. Шиллинга в июле 1837 г. управляющим первой секретной экспедицией Канцелярии МИД назначается Артур Миллер [2]. Однако уже через три года его сменяет на этом посту действительный статский советник барон Н. Ф. Дризен. В архиве сохранился составленный в самом начале уже XX в. тогдашним начальником I экспедиции К. Таубе обзор российских шифров XIX в. [3]. В этом содержательном документе указывается, что барон Дризен является автором шифров так называемой биклавной системы. Эти шифры использовались очень широко в течение XIX столетия в учреждениях МИД параллельно с биграммными шифрами Шиллинга.

Биклавный шифр представляет собой шифр многозначной замены, состоящий из 26 различных простых замен с достаточно сложным выбором замены на каждый знак открытого текста, определяемым двумя ключами. При этом отдельным знакам открытого текста (буквам и знакам препинания) соответствуют два знака шифрованного текста. Таким образом длина шифрованного текста не соответствует длине открытого текста.

Основу шифра составляют: портфель с 24 передвижными полосками — главная часть двойного ключа, две таблицы (шифровальная и дешифровальная) — вторая часть двойного ключа и календарь набора и разбора.

Каждая полоска представляет собой случайный набор с повторениями 20 букв латинского (французского) алфавита из 26 букв. Таким образом каждая полоска может содержать 20 или менее латинских букв. Для удобства они записываются группами по четыре буквы в каждой с пропусками. Каждая полоска имеет свой номер, обозначенный цифрой или буквой.

Например, полоска «W» имеет вид:

q d u f k z i v d k i l s w k m p z l g

Шифрующая таблица представляет собой квадрат 26×26, строки которого обозначены 23-мя буквами латинского алфавита (без букв k,w,y) и тремя знаками пунктуации (— , .) и столбцы которого обозначены всеми 26 буквами латинского алфавита. Каждая колонка этой таблицы заполняется случайным образом бесповторно 26-ю знаками, составляющимися из 17 букв латинского алфавита и девяти цифр: 1, 2, 3, 4, 5, 6, 7, 8, 9.

Процесс шифрования осуществляется следующим образом. Открытый текст, предназначенный для шифрования, записывается на так называемый транспарант, где каждая строчка содержит 24 клетки. Текст пишется по четыре знака с пропусками в одну клетку. Таким образом, в каждой строке транспаранта записывается по 20 знаков, форма записи соответствует форме шифрованной полоски. Если текст закончился не в конце строки, то добавляется слово «конец» и какие-либо еще произвольные знаки. Каждый транспарант содержит 8 горизонтальных строк. Таким образом длинное сообщение может быть записано на нескольких транспарантах. При записи шифруемого текста на транспарант рекомендовалось вначале проделать все возможные сокращения текста, не меняющие смысла сообщения. Далее производилась замена трех букв и некоторых знаков

препинания на знаки, входящие в промежуточный текст, а именно: буква k заменялась на qq, буква w заменялась на vv, буква y заменялась на ii, знак «;» заменялся на «.,» и т. д.

После записи сообщения на транспарант производится шифрование.

Из 24 полосок в строго определенном порядке выбираются восемь полосок согласно суточному ключу. Маркантом этого ключа является дата зашифрования, которая ставится в начале сообщения. Первая полоска подставляется к первой строке сообщения, например, получаем следующий текст и набор знаков на полоске:

	zes- miss ions -se- serv	
W		
	qduf k ziv akil swkm pzeq	

Знаки текста с буквами полоски образуют вертикальные биграммы, которые определяют входы шифровальной таблицы (координаты шифрованного текста). Например, первая вертикальная пара zq определяет знак шифртекста j, находящийся в z-й строке и q-м столбце шифровальной таблицы, т. е. знак z зашифровывается в знак j. Так шифруются первые 20 знаков. Следующие 20 знаков шифруются с помощью следующей полоски, определяемой суточным ключом, и т. п. Если шифруемый текст превышает 20×8=160 знаков, то процедура шифрования повторяется, начиная с первой полоски (в нашем примере W).

Расшифрование сообщения производится в обратном порядке, и очевидно, что открытое сообщение восстанавливается однозначно при наличии, конечно, у корреспондента соответствующих ключей.

Из описанной процедуры шифрования ясно, что криптографическая стойкость данного шифра держится на неизвестном противнику заполнении полосок, определяющих выбор последовательности 26 замен, и суточном ключе.

Хотя это число и достаточно велико, тем не менее криптографическая стойкость данной системы шифра ни в коей мере не может держаться на этом суточном ключе, поскольку она допускает последовательное опробование полосок шифра одну за другой. Сначала при дешифровании (при известной шифровальной таблице и известных полосках) опробуются одна за другой полоски (24 варианта). Критерием правильности опробования первой полоски является появление открытого (читаемого) текста. Далее опробуется вторая полоска из числа оставшихся и т. д. Всего получается T = (24 + 23 + ... + 17) = 164 элементарных опробования (э. о.). За одно э. о. принимается опробование одного варианта полоски. Если текст шифровался не с начала, а где-то с середины, то число вариантов опробования увеличится не существенно: T=(164 + 10 = 174 (э. о.).

Содержание полосок, как говорилось выше, — это основной ключ. Он действует значительно дольше, чем суточный ключ, но, тем не менее, его тоже достаточно часто меняли (полоски менялись обычно два раза в год).

Многие корреспонденты имели различные наборы этих ключей, чем обеспечивалась конфиденциальность переписки и создавалась определенная гарантия от компрометации шифра.

Перешифровальные таблицы, определявшие 26 простых замен, были второй частью ключа. Данный шифр для своего времени можно считать достаточно стойким при сохранении в тайне основного ключа (содержимого полосок) и суточного ключа.

Главная слабость этого шифра состоит в сравнительно коротком периоде T этого шифра (T=160 букв) и отсутствии разового ключа. Надо полагать, что в те времена за сутки шифровалось не более одного сообщения (в условиях мира) от конкретного корреспондента. По этой причине не было необходимости во введении еще дополнительных разовых ключей. Сами

сообщения также не были достаточно длинными, поэтому глубинных перекрытий шифра здесь не ожидалось. Не случайно поэтому шифры этого весьма оригинального типа использовались наряду с биграммными шифрами на протяжении почти сорока лет. Вот некоторые из выявленных нами таких шифров.

Русско-французский биклавный ключ № 305 был изобретен в 1853 г. бароном Дризеном и им же отпечатан. Календари введены в 1858 г. Предназначался исключительно для переписки миссий в Константинополе с МИД. В 1860 г. Дризеном было предложено включить в этот шифр таблицы для зашифрования русского текста, а не только французского, как это было первоначально. Это предложение принято цифирным комитетом на заседании 24 марта 1860 г., протокол которого подписали тогдашние члены этого комитета: тайный советник Толстой, тайный советник Гильфердинг, тайный советник Вестман и действительный статский советник барон Дризен. Теперь шифр состоял из двух наборных и разборных таблиц «для французского и русского набора». В 1869 г. этим шифром пользовался князь Горчаков при своей поездке на конгресс в Париж. Однако в том же году шифр был выведен из употребления.

Французский биклавный шифр № 306 изобретен бароном Дризеном и введен в действие в 1856 г. Предназначался для сношений с МИД миссии в Турине (Флоренции). В 1865 г. заменен биклавным ключом № 342, т. к. использовался уже более шести лет. В 1869 г. «ввиду устарелой системы» был уничтожен.

В 1856 г. были введены в действие аналогичные предыдущему и также составленные бароном Дризеном ключи: *№ 307* — для миссии в Афинах, *№ 308* — для миссии в Стокгольме, *№ 309* — для миссии в Риме, *№ 310* — для миссии в Неаполе и *№ 311* — для миссии в Мадриде.

В том же году был введен в действие *французский биклавный ключ № 313* для циркулярной связи мис-

сий в Афинах, Берлине, Брюсселе, Константинополе, Копенгагене, Дрездене, Франкфурте, Гамбурге, Ганновере, Лиссабоне, Лондоне, Мадриде, Мюнхене, Неаполе, Париже, Риме, Стокгольме, Турине, Вене и дипломатической канцелярии в Варшаве. Сожжен в 1867 г. «вследствие устарелости системы».

В 1859 г. были введены в действие составленные бароном Дризеном *русско-французские биклавные ключи: № 317* — для переписки МИД с Лондоном, *№ 318* — с Парижем, *№ 319* — с Веной, *№ 320* — с Парижем.

В том же 1859 г. был составлен *французский биклавный ключ № 322* для переписки князя Горчакова с императором. Однако этот ключ не был своевременно введен в употребление и впоследствии, в 1877 г., получил другой номер (364), и им пользовались во время русско-турецкой войны для переписки между главной квартирой Южной армии и МИД.

Русский биклавный шифр № 322 составлен был по системе барона Дризена и введен в действие в 1862 г. для переписки МИД с Веной и Константинополем. В 1876 г. экземпляры этого шифра отосланы в Тегеран и Токио, а также великому князю — Главнокомандующему действующей армией в русско-турецкой войне, и генералу Игнатьеву.

Французский биклавный шифр № 339 составлен бароном Дризеном и введен в действие в 1864 г. для двадцати восьми миссий в Европе и Америке. Использовался в сети общей связи. Кроме корреспондентов МИД, экземплярами этого шифра располагали Походная канцелярия и Императорская главная квартира. Выведен из действия в конце 90-х годов «вследствие устарелости системы».

Французские биклавные шифры № 340—345 составлены были для телеграфа в 1865 г. также бароном Дризеном. Предназначались шифры для сношений в сети общей связи, в которую входили МИД России, а также посольства в Берлине, Вене, Константинополе, Лондоне, Париже, Флоренции. Однако вскоре

эти ключи были заменены на более старые ключи той же системы № 305 и № 306.

Французский биклавный шифр № 348 составлен по системе барона Дризена, введен в действие в 1870 г. для миссий в Европе, а с 1871 по 1882 г. использовался также на азиатских линиях связи. Кроме того, экземпляры этого ключа были у министра иностранных дел князя Горчакова, в Имперторской главной квартире, Походной канцелярии, азиатском департаменте МИД, в действующей армии у генерала Игнатьева и барона Фредерикса. На европейских линиях связи этот ключ был выведен из действия лишь в 1891 г.

Французские биклавные шифры № 350—355 действовали параллельно с предыдущим ключом на европейских линиях связи. Введены эти ключи в действие в 1869 г., а выведены из действия лишь в 1891 г.

Французский биклавный ключ № 357 составлен по системе барона Дризена для телеграфа. Введен в действие в 1871 г. для переписки МИД с миссией в Вашингтоне. Сожжен в Вашингтоне в 1884 г.

Французский биклавный шифр № 364 составлен был по системе барона Дризена и введен в действие в 1877 г. для сношений с начальником канцелярии при действующей Южной армии. В 1878 г. отправлен в посольство в Константинополе и в действующую армию барону Фредериксу. Не употреблялся с 1888 г.

Как видим, биклавные шифры применялись длительное время весьма успешно и считались российскими криптографами достаточно надежными. Выведены из употребления они были не в силу криптографических изъянов, а по иным причинам. Так, в своем обзоре шифров XIX в. Таубе писал в 1901 году: «Система биклавная не применима в настоящее время ввиду смешанной передачи буквами и цифрами, не допускаемой телеграфными конвенциями». Нам известно, что некоторое незначительное число шифров биклавного типа применялось для зашиф-

рования секретной почтовой корреспонденции и в начале XX в.

Шифровальные коды. Как мы уже рассмотрели выше, коды и кодовые таблицы в России получили широкое распространение уже с конца XVIII в. и использовались в качестве основного вида шифров весьма длительное время. Продолжали они активно использоваться и в XIX в. Коды были разных типов, они постепенно видоизменялись и совершенствовались как в эксплуатационном, так и в криптографическом отношении.

Объем кодов варьировался от 300 до 10 000 словарных величин. В первые 50—70 лет в России в основном использовались коды объемом 300, 600, 900 и 1200 величин. К концу XIX — началу XX в. появились коды объемом 10 000 словарных величин и более. К 1917 г. наибольшее распространение имели коды именно такого объема.

Лингвистической науке известно, что активная лексика любого языка, в том числе и русского, то есть та часть всего словарного запаса языка, без которой невозможно свободное общение на этом языке, составляет лишь небольшую часть этого словарного запаса. Это обстоятельство было уже в ранний период принято во внимание российскими криптографами. Ими были выделены для помещения в словари кодов примерно 7—8 тысяч активно использующихся слов и словосочетаний русского языка. Тысячу с небольшим в коде обычно составляют слова, отражающие специфику переписки, которую предстоит шифровать с помощью этого кода. Например, словари военных кодов отличаются в этой своей части от словарей кодов дипломатических или кодов, используемых в торговом ведомстве. Например, военные коды отражают специфику военной переписки, и в их словари помещены наименования воинских подразделений, перечислены воинские звания, должности, виды оружия, команды и т. п. И наконец, около тысячи словарных величин в коде приходится на календарь, обозначение чисел, времени, другие специальные величины и, конечно, имена собственные и географические наименования, активно используемые в переписке на данной линии связи или в данном ведомстве. Включение в словарь кода большего числа величин, безусловно, делает его избыточным по существу и громоздким в пользовании. Такая избыточность словаря может быть оправдана лишь в некоторых кодах. Примером этому может служить рассматриваемый нами ниже словарь кода Николая II, который содержит большое количество эмоционально-экспрессивной лексики, необходимой для выдерживания определенного стиля деловой переписки императора. Однако это исключение.

Практически с самого начала употребления кодов в них были кодовые величины, в которых одному кодовому обозначению соответствовало несколько словарных величин, с одной стороны, и, с другой стороны, одной и той же словарной величине, наиболее часто употребляемой, соответствовало несколько кодовых обозначений. Это было важнейшее условие повышения криптографической стойкости кода, соблюдаемое в России, как и во всех других передовых странах мира. Этой же цели служило и наличие буквенно-слоговой таблицы, которая, кромо того, неограниченно расширяла словарные возможности кода. Вариантами кодовых обозначений достигали относительного выравнивания частот встречаемости в криптограммах шифробозначений, затрудняли дешифрование.

Второе важное условие для кода — необходимость наличия пустышек — нулей, т. е. кодовых обозначений, не соответствующих никаким словарным величинам. Такие пустышки должны были беспорядочно разбрасываться по тексту криптограммы. Эта мера повышения стойкости шифра обладала большой эффективностью и успешно применялась в практи-

ке криптографии в России уже с первой четверти XVIII столетия, перекочевав на некоторый период времени и в коды. Тем не менее указанные ухищрения не в состоянии были до конца сделать шифртексты сообщений равновероятными. Рано или поздно при накоплении шифрматериала постепенно выявляются часто встречающиеся кодовые обозначения, соответствующие наиболее часто употребляемым словарным величинам. Этот момент и является отправной точкой при дешифровании сообщений и успешно использовался дешифровальщиками как в России, так и в других государствах.

История зарождения кодов относится к началу XVI века и связана с именем криптографа Папы Ри́мского — Маттео Ардженти, который изобрел буквенный код на 1200 величин, где буквы, слоги, слова и даже фразы заменялись группами букв. Переход от буквенных кодовых обозначений к числовым относится к 1586 г. и приписывается Триентеру Концимо.

Следующий крупный шаг в развитии шифров, близких к кодам (их можно назвать «полукодами»), был сделан через 50 лет, когда начальником «счетной части» — дешифровального отделения — Франции при кардинале Ришелье уже упоминавшимся нами Антуаном Россиньолем был создан для дипломатической переписки шифр, который не был дешифрован на протяжении двух столетий и получил название «Великого шифра». Это был буквенно-слогово-словарный шифр, объемом около 600 величин, которым придавалось несколько значений пропорционально повторяемости их в открытом тексте.

Этот «Великий шифр» Россиньоля начинает уступать место алфавитным и неалфавитным кодам, в современном понимании, лишь со второй половины XIX в. И это происходит одновременно как в странах Европы, так и в России и, частично, в Азии. Эти коды в основном применялись в дипломатической

переписке, пробовали их использовать и в военном ведомстве. В Турции в 1877 г. во время войны с Россией применяли уже четырехзначный цифровой код, составленный специально для Турции в Германии. Но опыт русско-турецкой войны, как, кстати сказать, и франко-прусской, показал практическую непригодность существовавших в то время военно-полевых шифров, оказавшихся громоздкими и непрактичными, дающими большое число механических ошибок, и в то же время недостаточно стойких и гибких.

Большинство кодов России конца XIX — начала XX в. были *алфавитными*, т. е. буквы, слоги, слова, словосочетания словаря кода располагались в порядке алфавита, а соответствующие им кодовые обозначения представляли собой естественные числовые последовательности. Это обстоятельство в огромной степени облегчило дешифрование, поскольку место каждого кодового обозначения определялось местом слова в словаре соответствующего языка эквивалентного объема. Все эти соображения, естественно, давали возможность опытным криптографам противника восстанавливать код и дешифровать сообщение. Применялись и неалфавитные коды, коды пропорциональные и непропорциональные. В зависимости от вида кодовых обозначений различались *цифровые, буквенные и буквенно-цифровые коды.* Последние два вида кодов преобразовывались в цифровые, когда сообщения передавались по телеграфу.

С конца XIX в. в Европе появились теоретические труды, в которых описывались методы дешифрования алфавитных и неалфавитных кодов. С этого времени повсеместно начинают использоваться *коды с перешифровкой.* Перешифровки были различными, от весьма наивных, по сути своей чисто маскировочных, до очень сложных. Последние применялись на наиболее важных каналах связи. Подробнее об этих кодах России будет сказано далее.

Коды и кодовые таблицы интенсивно использовали: МИД, военное ведомство, МВД, Министерство финансов и некоторые другие гражданские ведомства. Коды и кодовые таблицы объемом до 1000 — 1200 словарных величин было принято называть *«словарными ключами»* и, в зависимости от словаря конкретного кода, называть французскими, русскими, немецкими.

Вот словарные ключи XIX в., которые нам удалось обнаружить в АВПРИ. Заметим, что создателями шифров этого типа были все тот же барон Дризен и другой сотрудник цифирного отделения МИД — М. Сухотин.

Русский словарный ключ № 299 на 600 словарных величин был введен в действие в апреле 1854 г., изъят из употребления в 1901 г. Изобрел этот шифр и издал барон Дризен. Предназначался он для связи командующих частями Дунайской армии во время Крымской кампании. В 1891 г. этим шифром были снабжены Бухара, Кашгар, Кульджа, Сеул, Пекин, Токио, Иркутск, Омск, Ташкент, Хабаровск, Урга, Чугучак, Владивосток.

Русский словарный ключ № 300 на 600 словарных величин также составил барон Дризен. Введен код в действие в 1855 г., изъят из употребления сразу по окончании Крымской войны в январе 1857 г. Предназначался он для главнокомандующего Южной армией и военных и морских сил в Крыму князя Горчакова. В 1860 г. этот ключ был послан в Вашингтон. Не употреблялся с 1871 г.

Русский словарный ключ № 317 на 1000 словарных величин предназначен для секретной переписки по телеграфу. Введен в действие в 1859 г. Этим кодом был снабжен генерал Игнатьев, посланный в Китай, для его переписки с МИД и с миссией в Вашингтоне с 25 февраля 1859 г. по 11 февраля 1861 г., а также для сношений миссий в Пекине с Вашингтоном и азиатским департаментом МИД. Использовался до 1871 г.

Французский словарный ключ № 321 на 1000 словарных величин. Введен в действие в 1859 г. для переписки: 1) графа Адлерберга с МИД во время путешествия императора в 1859 г.; 2) князя Александра Баттенбергского в Софии с императором и с МИД — с 1881 г. Выведен из действия в 1884 г.

Русский словарный ключ № 326 на 1000 словарных величин. Введен в действие в 1861 г. для переписки МИД с миссиями в Пекине, Урге, Хакодате. Не употреблялся с 1880 г.

Французский словарный ключ № 326 на 1000 словарных величин был введен в действие для сношений статского секретаря для царства Польского г. Тимовского с наместником в Варшаве. Не употреблялся с 1863 г.

Русский словарный ключ № 330 на 1000 словарных величин. Введен в действие в 1861 г. для переписки Морского министерства с начальником эскадры в Средиземном море. Не употреблялся с 1888 г.

Русский словарный ключ № 333 на 300 словарных величин был введен в действие в 1862 г. «для сношений Варшавского военного генерал-губернатора с шестью военными начальниками в Царстве Польском». В 1863 г. ключ этот был совершенно переделан и заново отпечатан в Варшаве под тем же номером и назван «Шифр Царства Польского. Новый шифр». В свою очередь сам ключ № 333 был переделан из старого словарного ключа № 151.

Русский словарный ключ № 336 имел объем 920 словарных величин. Внешне он представлял собой бумажные таблицы, наклеенные на коленкор. Изготовлялся ключ по требованию Морского министерства «для сношений Министерства морского в случае открытых военных действий». Введен в эксплуатацию в 1863 г. В 1871 г. послан в Вашингтон, Токио, Пекин, Нагасаки; в 1886 г. — в Афины, Фучжоу, Ханькоу, Сеул, Нью-Йорк. Этот ключ был также у военных губернаторов во Владивостоке и Хаба-

ровске. В 1888 г. первый экземпляр ключа был украден в Пекине, в 1891 г. — в Вашингтоне. В связи с компрометацией код в том же году был выведен из употребления.

Русский словарный ключ № 337, так же, как и предыдущий, был введен в действие в 1863 г. Первоначально служил для переписки наместника на Кавказе с миссиями в Константинополе и Тегеране, затем распространен на консульство в Персии. Выведен из действия в 1895 г.

Русский словарный ключ № 338 был издан в 1864 г. объемом 900 словарных величин для переписки азиатского департамента МИД с генерал-губернаторами в Оренбурге, Восточной и Западной Сибири, в Туркестане. Не употреблялся с конца XIX века.

Русский словарный ключ № 346 на 600 словарных величин был введен в действие в 1865 г. для переписки Министерства финансов с государственными таможнями, Министерством путей сообщения, Государственным контролем. Выведен из действия в 1867 г. вследствие утраты одного экземпляра.

Русский словарный ключ № 349 введен в действие в 1868 г. на линиях связи Министерства финансов для телеграфной шифрпереписки. Изъят из употребления в 1879 г. вследствие утраты двух экземпляров. В 1901 г. вновь введен в действие для сношений Министерства финансов с таможнями. Кроме того, этот шифр был введен в действие в 1900 г. в Министерстве государственных имуществ, в 1902 г. — в Порт-Артуре, Харбине, Мукдене; в 1904 г. он был направлен в Маньчжурскую армию и действующую армию.

Русский словарный ключ № 368 введен в действие в 1879 г. для сношений Министерства финансов с таможнями. Объем этого шифра — 650 словарных величин. Ключ этот также принадлежит к общему типу малых кодов (словарных ключей).

Как же непосредственно в рассматриваемый период в секретной экспедиции МИД проходила работа

по организации составления шифров? На этот вопрос частичный ответ содержится в отчете о деятельности этой экспедиции, написанном тогдашним ее начальником Ф. Годениусом.

Автор пишет о том, что в 1862 г. было признано необходимым снабдить наши российские консульства в Турции биграммным шифром, «но применительно к русскому языку». Хотя это применение к особенностям русского алфавита представляло значительные трудности, экспедиция все их преодолела, и затем составленный ею русский биграммный шифр № 334 (в количестве двенадцати экземпляров) был разослан в консульства. В то же время в эти же консульства были отправлены новые передвижные полоски (lames mobilis) для русского биклавного шифра за № 332 в количестве девяноста экземпляров.

Вслед за этим экспедиции был поручен огромный труд, а именно «изготовление изобретенного д [ействительным] с [татским] с [оветником] Г. Гамбургером шифра». После «неусыпных семимесячных трудов» означенный шифр был изготовлен и по приказанию начальства разослан в 1863 г. в главные миссии.

Нам известно, что в это же время Г. Гамбургером был составлен шифр, получивший название *chiffre polilexique*, на 900 словарных величин, в котором кодовыми обозначениями были трехзначные числа, повторяющиеся 26 раз каждое в зависимости от букв специальных полосок, выбираемых в особых календарях. Этот шифр был введен в действие в апреле 1862 г. и использовался до 1897 г. в переписке МИД с посольствами в Европе.

В то же время экспедиция изготовила изобретенный действительным статским советником Румом так называемый *экономический шифр*. Хотя было издано тридцать экземпляров, этот шифр не был признан удобным к употреблению. Ни один экземпляр его не сохранился.

В 1864 г. I цифирная экспедиция снабдила все миссии новым биклавным шифром для общей связи за № 339 взамен находившегося уже продолжительное время в употреблении шифра за № 312. Всего было изготовлено двенадцать экземпляров шифра № 339. Азиатский департамент получил для использования четыре экземпляра русского словарного шифра за № 338 для корреспонденции с генерал-губернаторами в Оренбурге, Западной части Восточной Сибири.

В 1865 г. были заготовлены и разосланы по принадлежности «новые партикулярные биклавные шифры с календарями» за № 340, 341, 342, 343, 344 и 345, изготовлен и разослан новый русский биграммный шифр за № 347. Кроме того, по требованию Министерства финансов туда были высланы тридцать экземпляров вновь изготовленного русского словарного шифра № 340.

Итак, можно понять, что цифирная экспедиция работала активно и весьма напряженно. Однако успех дела зависит от организации деятельности службы в целом, в том числе от правильного ведения секретного делопроизводства, соблюдения правил пользования шифрами, условий их хранения. В этих вопросах положение дел оставляло желать лучшего. Как следует из приведенных нами сведений, не соблюдались, как правило, сроки пользования шифрами. Были и другие серьезные недостатки. Так, например, в 1866 г. цифирная экспедиция МИД занималась «проверкой всех находящихся в некоторых странах шифров, а равно контролем всех книг, которые ведутся о состоянии заготовленных и разосланных экспедицией шифров». При этом оказалось, что, с одной стороны, некоторые миссии имеют у себя шифры в огромном количестве, из которых многие, конечно, вовсе не употребляются. С другой стороны, проверка обнаружила, что некоторые уже закрытые миссии не возвратили находившихся в них

шифров. Вследствие этого были даны необходимые распоряжения и приняты соответствующие меры к исправлению существующего положения.

Перешифровальные ключи. Коды с перешифровкой. Во второй половине XIX в. в России уже хорошо понимали слабости применения кодов в чистом виде, без усложнений, особенно слабости алфавитных кодов. Как известно, к этому времени начальником армейского криптографического отделения Франции Базери был дешифрован «Великий шифр» Россиньоля. Основываясь на его методе, с помощью диаграмм распределения слов по буквам для словарей на разные объемы слов, дешифровальщики ведущих стран мира, в том числе и России, раскрывали алфавитные коды иностранных государств и осуществляли успешный анализ и частичное дешифрование неалфавитных кодов.

В связи с этим возникла необходимость ввести усложнения, чтобы увеличить стойкость кодов.

В инструкциях к шифрам МИД и Военного министерства России неоднократно рекомендовалось применять различные способы увеличения стойкости. К этим способам относили: и своевременную смену ключей и кодов, и применение одновременно нескольких кодов в тех местах, где была такая возможность, и применение различного рода приемов типа использования разных вариантов кодовых обозначений, и, наконец, применение различных способов и систем перешифровок.

Параллельное применение нескольких кодов требовало больших затрат на составление и издание большого их количества и поэтому широкого распространения не получило. В России, как во многих других странах, применялись различные виды перешифровок кодов: с помощью колонной замены, гаммирования и перестановок. Здесь пойдет речь о наиболее типичных видах перешифровок.

Все перешифровальные ключи (системы) имели свой сквозной порядковый номер и каждому присва-

ивалось наименование по буквам греческого алфавита: Альфа, Бета, Гамма, Дельта, Лямбда и т. д. Каждое сочетание кода перешифровкой с перешифровальным ключом также получало свое наименование. Например, сочетание «Русского консульского ключа № 447» (кода) с перешифровкой перешифровальным ключом № 448 «Лямбда» называлось «Ангара».

Для одних кодов перешифрование было обязательным, для других — в случаях передачи особо секретного сообщения. Составители шифров понимали, что коды легко компрометируются (теряется их стойкость), если содержание зашифрованного с их помощью сообщения становится дословно известным противнику. Поэтому в случаях, если из МИД в какое-либо посольство, консульство или обратно передавался какой-то текст, известный или становившийся известным, то этот текст необходимо было передавать, в обязательном порядке используя сочетание специальных кодов и перешифровок. Так, например, в 1916 г. для этой цели использовались «Французский общий малый дипломатический ключ № 431» и «Английский малый дипломатический ключ № 407» с обязательным перешифрованием.

Неотъемлемой частью шифров становятся лозунги (в современной терминологии — ключи), меняющиеся в те или иные моменты времени в соответствии с правилами. Лозунг представлял собой более или менее короткий цифровой или буквенный ряд. Ключи были нескольких видов. Одни из них носили название «общих», ими снабжались загранучреждения определенного региона. Все остальные ключи назывались «специальными». Одни из них предназначались для связи лишь узкого круга корреспондентов или даже для одного посольства с центром (индивидуальные ключи).

При зашифровании стандартные словосочетания, включая целые фразы, заменялись условными словами — «постоянными», что делалось для сокращения

длины сообщения, и «переменными» — для дополнительного обеспечения секретности.

Рассмотрим некоторые типичные варианты таких шифров.

«Передвижной условно-словарный ключ № 437» [4]. Первое упоминание о нем в документах относится к 1910 г. В «Руководстве» к этому шифру сказано, что он был «предназначен для шифрования приведенных в секретных сообщениях выражений общего характера и ссылок, независимо от набора любым секретным ключом (или сочетанием ключей) открытого текста шифруемого сообщения».

Шифр этот состоял из четырех частей.

Первая часть — это непосредственно код (словарный ключ), цифровой, трехзначный, объемом 1000 словарных величин.

Вторая часть — перешифровальная, представлявшая собой набор «перешифровальных групп». На каждые сутки имелась своя перешифровальная группа, содержащая трехзначное число (дополнительный к коду ключ). Под первичным шифрованным текстом, полученным при зашифровании по коду, подписывалась эта трехзначная перешифровальная группа, и из верхних цифр вычитались нижние по модулю 10. Таким образом, перешифровальная группа есть не что иное, как короткая периодическая гамма с периодом три.

Третью часть шифра составляет таблица из 1000 передвижных условных выражений (слов), в которой каждое выражение соответствовало трехзначному числу. Таким образом, полученный после перешифрования набор трехзначных чисел заменялся на набор условных выражений. Каждое условное выражение представляет собой некое латинское слово (или имя собственное, встречающееся в литературе). Условные латинские выражения располагались в таблице в алфавитном порядке, трехзначные числа — в возрастающем арифметическом порядке, т. е. тре-

тью часть шифра можно назвать обратным алфавитным кодированием. Слово «передвижной» означает, что эта часть должна со временем меняться, и, таким образом, она служила секретным ключом шифра.

Четвертую часть шифра составляют 25 таблиц цифровых замен, называемые шифром «Секунда». В каждой таблице присутствует 20 замен, т. е. всего имеется 20×25 = 500 простых замен. Они предназначены для зашифрования чисел в сообщении (дат, ссылок на номер предыдущего или данного сообщения и т. д.). Таким образом, эти числа шифруются не по коду, а с помощью замен «Секунда». Для этого указанные числа открытого сообщения представляются в виде 5-значных групп с приписыванием слева недостающего до полной пятерки числа нулей. Далее в начале шифрсообщения указывается условный номер выбираемой таблицы замены, например, соответствующий первой таблице, и далее производится шифрование каждой цифры набора 5-значных групп по своей порядковой замене. Первая цифра первой заменой (столбцом), вторая — второй и т. д. Если число цифр превосходит 20, то следующие цифры после 20 шифруются по второй таблице и т. д.

Таким образом, ключ № 437 представляет собой шифр, который можно назвать «код + гамма + обратный код + набор простых замен для шифрования чисел».

Шифр «код + гамма» хорошо известен специалистам. В 50—60-х годах XX столетия в криптографической литературе было опубликовано немало работ, посвященных анализу этой системы и возможностям ее дешифрования. Методы дешифрования были основаны на использовании цифровой структуры гаммы перешифрования, на ее короткой периодичности и на возможности проводить арифметические операции (сложение, вычитание) с цифровыми знаками шифртекста.

Применение в шифре № 437 обратной операции кодирования практически сводит на нет возможно-

сти применения указанных методов дешифрования, по крайней мере, до тех пор, пока не удастся накопить достаточно большой объем шифрматериала, чтобы с достаточно большой надежностью можно было бы снять обратный (алфавитный) код.

Что касается применения четвертой части шифра — особого зашифрования дат и ссылок, — то ее целесообразность можно в какой-то мере объяснить желанием уйти от кодирования стандартов в сообщении, которые, как известно, служат необходимым подспорьем для дешифрования кодов, особенно в наиболее трудный момент начала этой работы. Это объяснение можно подтвердить и тем обстоятельством, что в «Руководстве» рекомендуется все стандартные выражения, входящие в сообщение, не шифровать кодом, а «заменять их на постоянные условные выражения» (в отличие от «передвижных», участвующих в третьей части шифрования) и ставить их в начале шифрсообщения, отделяя от текста шифрсообщения двумя структурными пятизначными группами — группой дня.

При передаче сообщения по радиотелеграфу, где требовалось, чтобы весь текст был представлен в виде набора пятизначных цифровых групп, рекомендовалось не применять третьей части шифра — обратного кодирования цифровых групп передвижными условными выражениями. По-видимому, предполагалось, и не без основания, что и без этого усложнения шифр получался достаточно стойким.

Перешифровальный ключ № 448 «Лямбда» [5] предназначался для перешифрования первичного цифрового шифртекста, полученного при шифровании сообщения с помощью какого-либо цифрового кода. Представляет собой шифр колонной замены с периодом T = 10 000 суммарных шифров, при этом все подстановки шифра (размера 10×10) набираются случайно и равновероятно. Все они отпечатаны и сброшюрованы в две книги по 667 страниц каждая. На

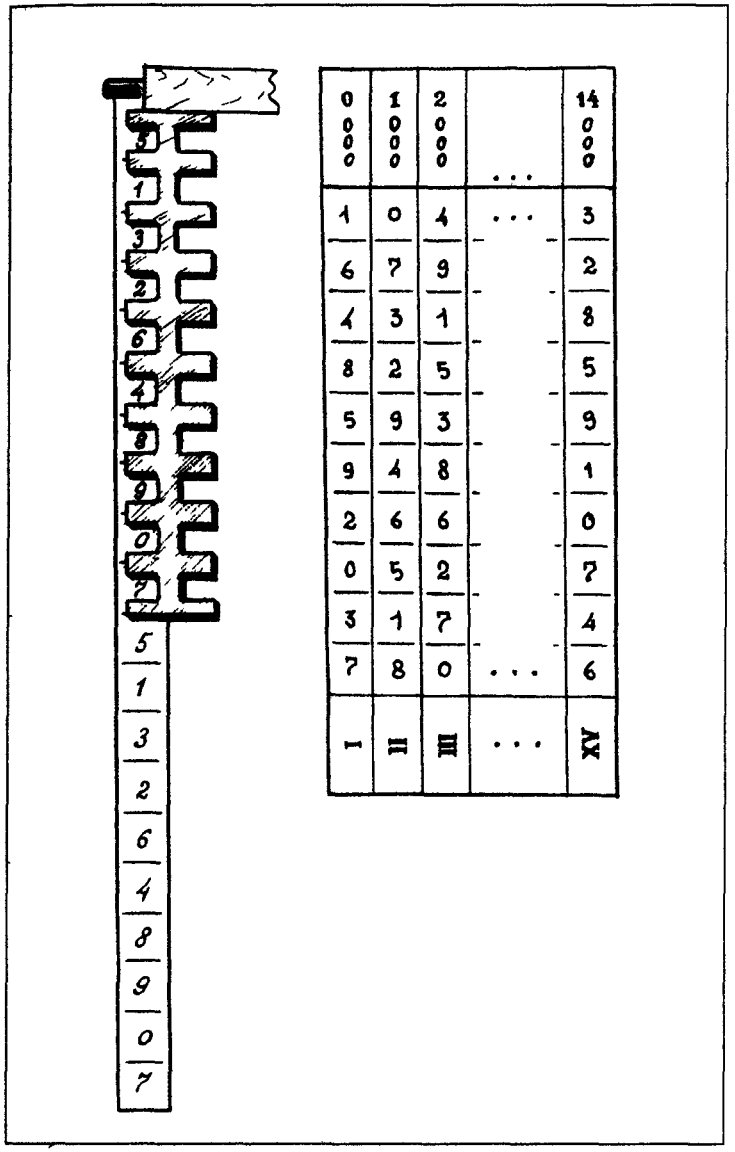
всех страницах имеется по 15 вертикальных столбцов, каждый столбец представляет собой лишний ряд подстановки. Все они пронумерованы цифрами от 1 до 10 000 (сквозная нумерация). Кроме того, пронумерованы все столбцы на каждой странице от 1 до 30 (внутренняя нумерация).

Верхний ряд подстановки меняется и служит одним из ключей. В качестве этого ряда берется один из столбцов книги. Его порядковый номер указывался Цифирным отделением на определенный период и, как правило, менялся два раза в месяц.

Шифровальщик, приступая к работе, выбирал начальный столбец, который назывался «исходным столбцом» Его номер он помещал в криптограмму, предварительно зашифровав посредством «особых указательных групп», о которых мы подробнее скажем ниже Далее он шифровал первичный шифртекст, последовательно применяя к каждому знаку текста свою замену. После зашифрования заменой с номером 10 000, шифровальщик переходил к столбцу с номером 1 (по циклу).

Для большего удобства пользования такой сложной системой шифра использовался прибор «Скала». Этот деревянный прибор содержал вертикальную целлулоидную ламу с десятью пустыми клетками, размер которых совпадал с длиной шифровальных столбцов в книге. Шифровальщик вписывал в клетки ламы цифры, соответствующие указанному ключу (номеру столбца), и прикладывал прибор последовательно к шифровальным столбцам. Каждый раз получалась подстановка для шифрования.

Номер начального столбца шифровали особо. Для этого шифровальщик три раза подряд выписывал номер исходного столбца (3×4 = 12 цифр) и добавлял дважды записанный номер последнего используемого столбца (с той целью, чтобы помочь расшифровать текст при каких-либо сбоях или ошибках). В результате получался «указательный ряд» из двад-



Прибор «Скала» со вставленной ламой и первый лист перешифровального ключа «Лямбда»

цати цифр. Например: 2563 2563 2563 4812 4812. Далее брался столбец, указанный в качестве ключа цифирным отделением (столбец, выписанный на ламе), и столбец, стоящий рядом с ним (10+10=20 цифрам). Эта последовательность, называемая «календарным рядом», подписывалась под указательным рядом и производилось вычитание по модулю 10. Полученный ряд вставлялся в криптограмму в условном месте.

Как видим, данная система перешифрования была значительно сложнее лозунгового гаммирования короткой периодической гаммой и, очевидно, криптографически более стойкой.

Шифром «Лямбда» были снабжены «центральные и все штатные заграничные установления МИД, а равно чиновники МИД при наместнике Е [го] И [мператорского] В [еличества] на Кавказе и начальнике Закаспийской области и чиновники по дипломатической части при Приамурском, Туркестанском и Иркутском генерал-губернаторах». На время войны этим шифром снабжалась также дипломатическая канцелярия при штабе Верховного Главнокомандующего.

Военные шифры и шифрсвязь

Итак, изучая историю деятельности криптографической службы МИД, мы установили, что именно здесь на протяжении всего XVIII и примерно половины XIX столетия кроме дипломатических и иных шифров составлялись шифры и для Военного ведомства. Во второй половине XIX века цифирная экспедиция МИД также в определенной степени обеспечивала это ведомство шифрами, однако уже с конца 40-х годов в Главном штабе Военного министерства организуется и начинает работать собственная ци-

фирная экспедиция. Создававшиеся здесь шифры утверждались военным министром. Экземплярами военных шифров снабжались старшие начальники войск и военных управлений, поименованные в особом списке. В этот список входили император и члены императорской фамилии, занимающие важные военные посты, военный министр, начальники главных управлений военного министерства, командующие войсками в округах, начальники штабов округов, командиры корпусов, комендантты крепостей, наказные атаманы и др.

Естественно, что шифрованная переписка по линии военного министерства велась не только в военный период, но и в мирное время. Зашифровывались сообщения, касающиеся мобилизационной и военной подготовки, а также готовности армий и крепостей к военным действиям и некоторые другие сведения.

В военное время из цифирной экспедиции МИД в Военное министерство поступали экземпляры тех шифров, которые действовали в сетях общей связи, куда в силу политических, военных или иных причин могли входить дипломатические представители России за границей, командующие действующими армиями, военно-морскими силами и иные лица.

Во второй половине XIX в. большинство шифров военного министерства представляли собой коды малого (до 1000 словарных величин) объема. Кодовыми обозначениями здесь являлись трех- и четырехзначные числа. Военные шифры этого типа обычно использовались в течение длительного времени, перерабатывался лишь относительно быстро устаревавший словарь, что объясняется, например, переменой географии военных действий и т. п. Коды с перешифровкой, созданные в 60-х годах, использовались еще в начале XX в. «Словарные ключи» были наиболее распространенным типом шифров, исполь-

зуемых в конце XIX в. в Военном ведомстве. Их так и называли «военными ключами».

Имея универсальные принципы построения, шифры Военного министерства конца XIX — начала XX в. отличались друг от друга некоторыми особенностями. Рассмотрим их.

Военный шифр (конца 40-х годов XIX в.) [6] представляет собой код на 600 словарных величин. В словарь включены буквы, слоги, слова, числа. В качестве кодовых обозначений использованы трехзначные числа от 100 до 699. Для удобства работы составлялись наборная и разборная таблицы (шифрант и дешифрант). Для усложнения кода предлагалось использовать пустышки, которыми являлись числа от 700 до 999. В «Наставлении к шифру» рекомендовалось ставить их, по крайней мере, по две-три в каждой строке.

При ошибочном написании какой-либо кодовой группы «дабы не скоблить или переписывать своего шифрования» предлагалось ставить вслед за ошибочными числами «кодовые группы-уточнители», входящие также в состав словарных величин.

Рекомендовалось, кроме того, не шифровать наиболее употребительные стандартные фразы, место пребывания, число и месяц года. Обороты типа «милостивый государь», «с истинным почтением имею честь быть» и подобные не употреблять совершенно.

Шестой ключ Военного министерства 1906 г. [7] представляет собой трехзначный многовариантный цифровой код с маскировкой и скрытым началом сообщения. Объем — 1000 словарных величин. Последними являются слова, слоги, буквы русского алфавита. Всем буквам и наиболее часто встречающимся словам приданы по два и более кодовых обозначения, остальные словарные величины имеют по одному кодовому обозначению. В правила, кроме того, введено одно обязательное требование: если в тексте телеграммы встречаются одни и те же слова,

то их следует набирать разными способами, избегая повторений кодовых обозначений. Отдельно даны перешифровальные цифровые таблицы.

В правила также введено требование обязательно прятать начало сообщения. С этой целью цифровой шифрованный текст разбивается справа налево (с конца криптограммы) на группы по пять цифр каждая. В первой с конца группе оставляется четыре цифры. Пятизначные группы на письме отделяются одна от другой с помощью тире. Если в последней группе, соответствующей началу открытого сообщения, оказывается меньше пяти цифр, то шифровальщик добавляет необходимое число произвольных цифр. Количество произвольно добавленных цифр указывается числом, которое ставится в самом конце цифрового набора, превращая группу, ранее четырехзначную, в пятизначную. Если в начале телеграммы произвольных цифр ставить не требуется, то в конце последней группы ставится ноль.

В шифре была предусмотрена маскировка: в каждой пятизначной группе криптограммы необходимо было переместить вторую и четвертую цифры одну на место другой, оставив без изменений первую, третью и пятую цифры. В результате этой маскировки перемещались цифры, принадлежащие одной и той же или разным трехзначным кодовым группам. Тем самым нарушались порядковые (алфавитные) связи, если код был алфавитным или содержал какие-то части «с плохо размешанными», неслучайными кодовыми обозначениями.

Указанные усложнения нельзя трактовать как перешифровку кода, но как маскировочные меры они, естественно, могли существенно усложнить действия противника по дешифрованию этих систем.

Конечно, когда дешифровальщику становились известными все эти усложнения, он легко от них избавлялся, совершая обратные процедуры переста-

новки знаков и определяя начало сообщения по последней цифре криптограммы.

Исходящий номер проставлялся в конце телеграммы, причем он набирался буквами. Если телеграмма являлась ответом на ранее полученную, то номер последней проставлялся цифрами в начале данной.

Ввиду того, что иногда зашифровывался не весь текст телеграммы, а отдельные его части, то в криптограмме цифровой текст мог перемежаться с текстом открытым. При этом каждая шифрованная его часть оформлялась в группы из пятизначных цифр всякий раз как самостоятельная телеграмма. Указанные правила пользования шифром были подписаны начальником отдела Генерального штаба генерал-майором Марковым и начальником цифирного отделения полковником Лео.

Ключ Военного министерства № 7 1905 г. [8] был алфавитным трехзначным цифровым кодом на 900 словарных величин, размещенных на 18 таблицах 5×10. При этом первая цифра этого кода менялась по ключу в соответствии с показателем (маркантом) так называемой малой таблицы.

При наборе сообщений этим шифром считалось необходимым менять показатели и соответствующие им табличные цифры через произвольное число набираемых букв, слогов и слов. Однако признавалось желательным, чтобы эта перемена производилась не реже чем через 13 набранных кодовых обозначений.

Если в тексте телеграммы повторялись одни и те же слова, то они обязательно набирались каждый раз различным способом, избегая повторений одних и тех же кодовых обозначений. Все остальные правила шифрования этим шифром — стандартные.

По окончании набора весь цифровой текст разбивался слева направо на пятизначные группы. При этом первая группа была четырехзначной, а в конце

прибавлялось при необходимости нужное число произвольных цифр, чтобы последняя группа шифртекста была обязательно пятизначной. Число это ставилось в начале первой группы, превращая ее в пятизначную.

Перед отправкой шифртелеграммы обязательно проверялась правильность ее зашифрования путем расшифрования.

Особенностью построения словарных величин в этом шифре было то, что разные части речи могли помещаться за одним и тем же кодовым обозначением, например: возбу,д,жд; возвра,т,щ.

Вот список лиц, пользовавшихся в своей переписке «Седьмым ключом Военного министерства» и имевших поэтому его экземпляры: император, его императорское высочество генерал-фельдцехмейстер, его императорское высочество главнокомандующий войсками гвардии и Петербургского военного округа, военный министр, командующий Императорской главной квартирой, начальник Генерального штаба, начальник Главного штаба, начальник канцелярии Военного министерства, товарищ генерал-фельдцехмейстера, товарищ генерал-инспектора по инженерной части, главный интендант, начальник Главного управления казачьих войск, главный военно-медицинский инспектор, командующие войсками в округах, начальник Варшавского укрепрайона, начальники штабов округов, командиры корпусов, командиры крепостей, начальники кавалерийских и пехотных дивизий и стрелковых бригад, войсковые наказные атаманы казачьих войск, морской министр, начальник Главного морского штаба, начальники эскадр, военно-морские агенты.

Буквенный ключ Военного министерства, литер «В» 1910 г. [9] представляет собой таблицу 30×30, в каждой строке которой в произвольном порядке расписаны все буквы алфавита. В верхней строке и крайнем левом столбце записан алфавит. Таким образом

каждая координата таблицы (каждый знак) определяется двумя знаками алфавита.

Шифрование осуществляется следующим образом: выбирается показательная группа (показатель) — слово или набор слов с числом знаков не менее десяти (например, «маршевая рота»). Этот показатель пишется перед шифруемым сообщением. Далее расписывается текст сообщения, а над каждым знаком этого сообщения — знак показательной группы; показательная группа повторяется столько раз, какова длина сообщения:

показательная группа	**МАРШЕВАЯРОТАМАРШЕВАЯ РОТА...**
текст сообщения	**ПЕРЕПИСКАИЛИСНЯТИЕ КОПИЙС...**

Шифрзнак находится на пересечении столбца с номером М и строки с номером П.

Таким образом, данный шифр — табличный шифр замены, состояший из тридцати простых замен, причем информация о том, какой замене принадлежит тот или иной шифрзнак, известна. Очевидно, что стойкость такого шифра минимальна.

В качестве показательной группы можно было использовать и нешифруемую часть сообщения, если таковая имелась в тексте.

Шифр войск гвардии и Петербургского военного округа 1911 г. [10] (см. илл. на вкладке) представляет собой код на 100 словарных величин — букв, цифр, слогов и словосочетаний. Кодовые обозначения — двузначные числа.

Оформлен код в виде таблицы, на которой расположено десять таких кодов с одной и той же словарной основой.

Пользоваться этим ключом следовало таким образом. Перед шифрованием корреспондент выбирал номер кода (ключа), ставил его в начале сообщения и шифровал по этому коду 10—13 словарных величин. Далее он переходил к другому ключу и шифровал следующие 10—13 словарных величин. В этом в общем-то достаточно простом коде обращает на себя внимание найденная удобная форма шифра, позволяющая сравнительно просто и быстро осуществлять процесс шифрования.

Шифры императора Николая II. Первый из них, шифр 1911 г., представляет собой небольшую вытянутую в ширину книжечку, размером 14,5×21 см в очень красивом изумрудно-зеленом муаровом переплете. На обложке золотом вытеснен герб России — двуглавый орел и надпись золотыми буквами: «Ключ Военного министерства. Лит. М» [11]. Хранился этот шифр в специальном кожаном футляре-кошельке.

Ключ состоит из десяти кодовых таблиц набора и стольких же таблиц разбора за № 0—9. В таблицы набора помещены все буквы алфавита (кроме Ъ и О) и цифры от 0 до 9. Кроме того, в таблицы включены наиболее употребительные слоги. Кодовые обозначения — двузначные числа от 00 до 99, приданные словарным величинам в каждой из десяти таблиц в произвольном порядке (т. е. код неалфавитный). Таким образом, код состоит из десяти самостоятельных кодовых таблиц объемом в 99 величин каждая.

При шифровании пользовались одновременно всеми 10 таблицами Для определения номера используемой таблицы служил особый показатель (шифровальный ключ), состоявший из пяти цифр, который устанавливался особым распоряжением начальника Главного штаба на определенный срок. Номера таблиц вынесены на клапаны.

При наборе под всеми подлежащими зашифрованию буквами, цифрами или имеющимися в таблицах слогами шифруемого текста последовательно писались цифры показателя. Цифра показателя над буквой, слогом или цифрой текста обозначала номер таблицы набора, из которой следовало брать соответствующие кодовые обозначения. Поскольку показа-

тель имел длину 5, то отсюда следует, что через каждые 5 знаков для шифрования использовалась одна и та же таблица.

Найденные в таблицах кодовые обозначения подписывались под этими буквами, цифрами или слогами в таком порядке, чтобы цифра, обозначающая единицы в каждом двузначном кодовом обозначении, приходилась под цифрой десятков (например, кодовые обозначения 31 или 05 писались: $\frac{3}{1}$ или $\frac{0}{5}$).

При окончании набора все эти обозначения (столбцы) разбивались на группы по пять столбцов и писались в следующем порядке, разделяясь группа от группы чертой: сначала по порядку, считая слева направо, все группы из верхних цифр (обозначающих десятки), а затем в таком же порядке и отделяясь такой же чертой группы из нижних цифр (единицы).

Если в последней группе оказывалось менее пяти столбцов, но более двух (например, $\frac{320}{597}$), то последнее обозначение повторялось для пополнения группы до пяти столбцов ($\frac{32000}{59777}$). Если же таких обозначений оставалось одно или два (например, $\frac{3}{0}$ или $\frac{47}{23}$), то их следовало писать в одну строку и группу дополнить до пяти цифр повторением последней (например, $\frac{3}{4}$ писать 34444, во втором случае $\frac{47}{23}$ — 42733).

Пример набора:

текст: сомкнуть на 378 верст...
показатель: 35721

3	5	7	2	1	3	5	7	2	1	
со	м	к	н	у	т	ь	на	3	7	
4	3	0	0	6	5	2	9	6	6	
6	9	7	6	1	5	6	7	9	2	...

Зашифрованная телеграмма имеет вид:

43006—69761—52966—56792...

Сохранился экземпляр этого ключа, принадлежавший самому императору. Кроме Николая II, экземпляры шифра имелись у трех великих князей, военного министра, начальника Генерального штаба, начальника Главного штаба, начальников канцелярии и законодательного отдела Военного министерства, у начальников главных военных управлений, командующих войсками в округах, начальников окружных штабов, корпусов, крепостей, дивизий, бригад, у председателя Совета министров, министра внутренних дел, министра иностранных дел и некоторых других лиц. Всего в списке лиц, обладавших экземплярами этого шифра, значится 76 человек.

Описанный выше показатель сообщался особым письмом, в том числе и к императору, начальником Главного штаба.

Второй шифр Николая II, который нам хотелось бы отметить, это *«Особый шифр № 1-й Государя Императора»* [12], являющийся кодом с перешифровкой. Перешифровка предствляла собой двузначную гамму, периодически меняющуюся после каждых девятнадцати знаков по линейному закону. Эту перешифровку также можно классифицировать как маскировку, поскольку она легко снималась, как только дешифровальщик получал информацию о процессе ее получения (из даты посылки телеграммы). Как и предыдущий, этот код состоял из самостоятельных кодовых таблиц (их было уже 13), содержащих по 99 словарных величин (букв, слогов, цифр) каждая.

Пользоваться этим шифром следовало таким образом. Подлежащие набору слова текста разбивались слева направо на группы по 19 букв каждая, в последней группе букв могло быть меньше. В начале каждой группы ставилась черта. Для набора произвольно выбиралась одна из 13 наборных таблиц и ее номер ставился в начале первой 19-буквенной группы над чертой. При наборе каждой буквы первой 19-буквенной группы к каждому числу, имевшему соответствующее кодовое обозначение, прибавлялось

одно и то же число, называемое «ключом телеграммы». Этот ключ определялся из числа и месяца, которые показывались в начале текста телеграммы. Чтобы определить ключ данной телеграммы, следовало сложить число показанного дня с числом, которому соответствовал показанный месяц.

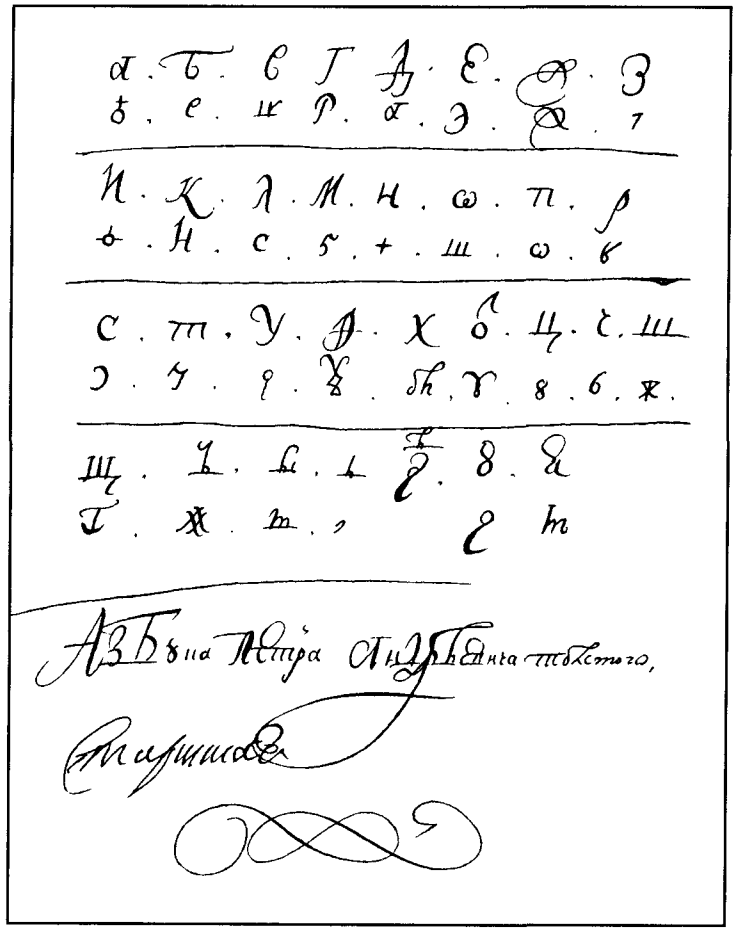
Так, например, если телеграмма начиналась словами: «Харбин, тринадцатого июня...», — то число дня будет «13», а месяца «6» и, следовательно, ключ телеграммы: 13 + 6, т. е. 19. Если при сложении получалось однозначное число (например, 3 января), то к нему следовало приписать 0.

Дойдя до следующей, второй 19-буквенной группы, шифрующий менял наборную таблицу, не соблюдая при этом никакой последовательности. Номер новой таблицы ставился над чертой. По этой таблице набирались 19 букв второй группы. Перед каждой следующей 19-буквенной группой также менялась таблица. При этом к числам, соответствовавшим по таблице набираемым буквам, прибавлялся ключ телеграммы, уменьшенный для второй группы на единицу, для третьей — на два, для четвертой — на три и т. д. Такой уменьшенный ключ телеграммы назывался «ключом группы». Когда ключ группы рядом таких последовательных вычитаний доходил до следующей за шифрованной с ключом группы, равной 1, 19-буквенная группа шифровалась с ключом, увеличенным на 1, т. е. 1, равным 2, затем — 3 и т. д. до числа, соответствовавшего первоначальному ключу телеграммы. От него ключ группы опять последовательно уменьшался до единицы и т. д.

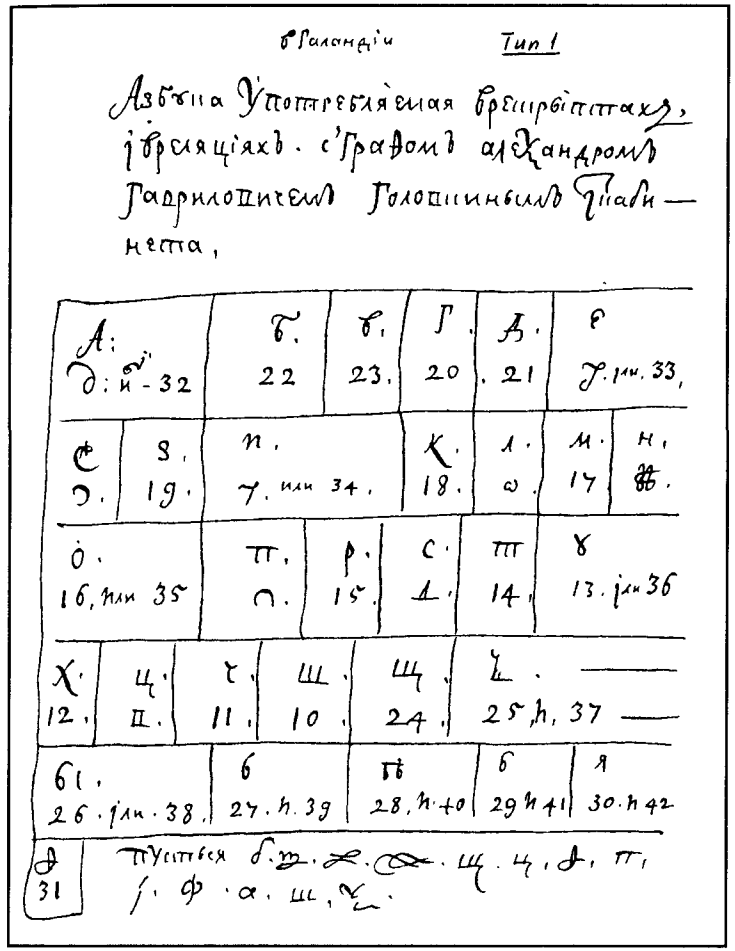
Для отправки по телеграфу перешифрованный таким образом текст шифртелеграммы разбивался на пятизначные цифровые группы. Так как в каждой 19-буквенной группе двузначных чисел впереди ставилось двузначное число, обозначающее номер таблицы, то каждая из этих групп состояла из 40 цифр.

Русские буквы.	Пермские письмена.	Русские буквы.	Пермские письмена.
А		О	
Б		П	
Г		Р	
Д		С	
Е		Т	
Ж		У, В	
ДЖ		Ц	
З		Ч	
ДЗ		Ш	
І		Ы	
К		Ю	
Л		Ю	
М		Ö	
Н		Я	

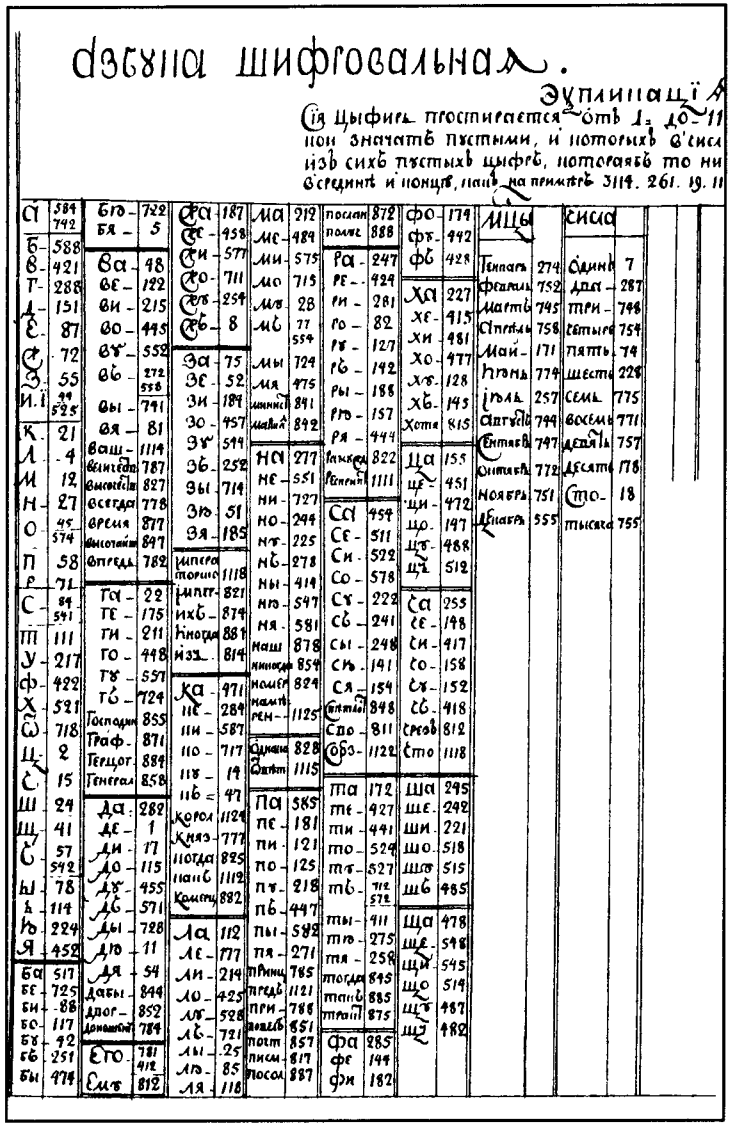
Пермская азбука



Азбука П. А. Толстого, написанная рукой Петра I. 1700 г.

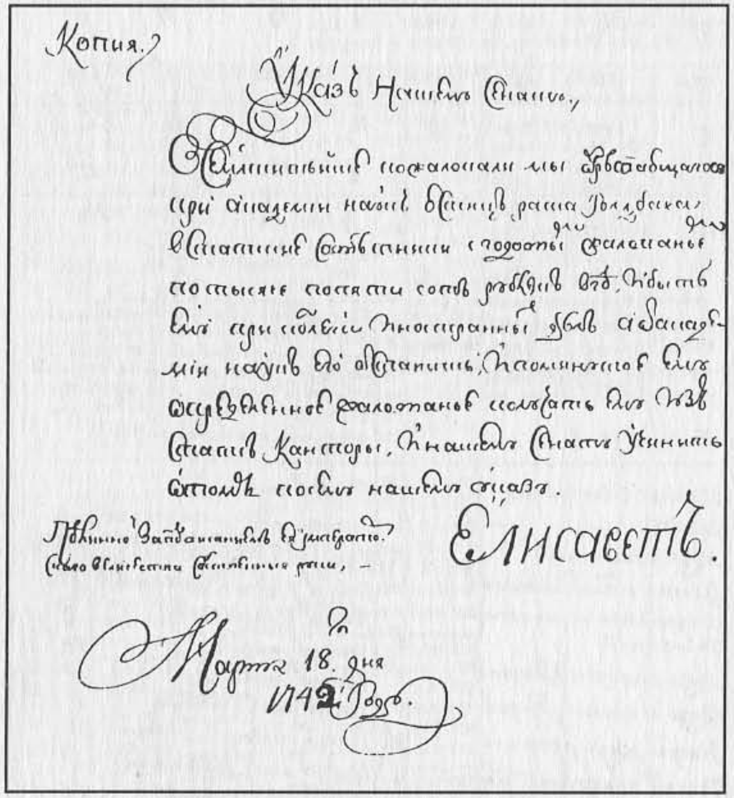


Азбука А. Г. Головкина. 20-е годы XVIII в.



Шифр 30-х годов XVIII в.
с правилами пользования

Шифр И. И. Неплюева.
30-е годы XVIII в.


Копия.

Указъ Нашему Сенату

Елисаветъ

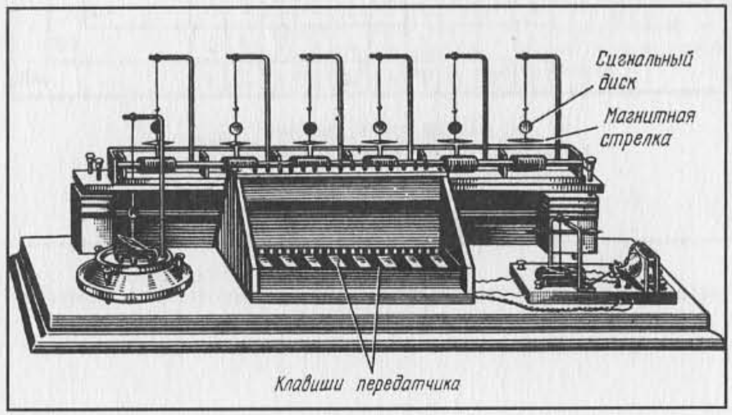
Марта 18. дня 1742 году.

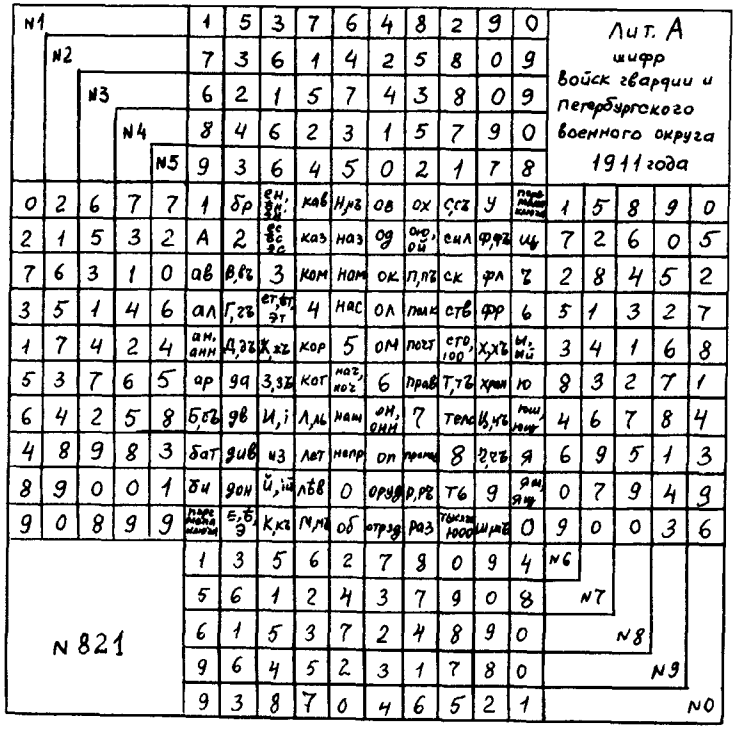
Указ императрицы Елизаветы Петровны о назначении Х. Гольдбаха на «особливую» должность в Коллегию иностранных дел. 18 марта 1742 г.


А. П. Бестужев-Рюмин. 40-е годы XVIII в.


П. Л. Шиллинг фон Канштадт

Телеграфный аппарат П. Л. Шиллинга

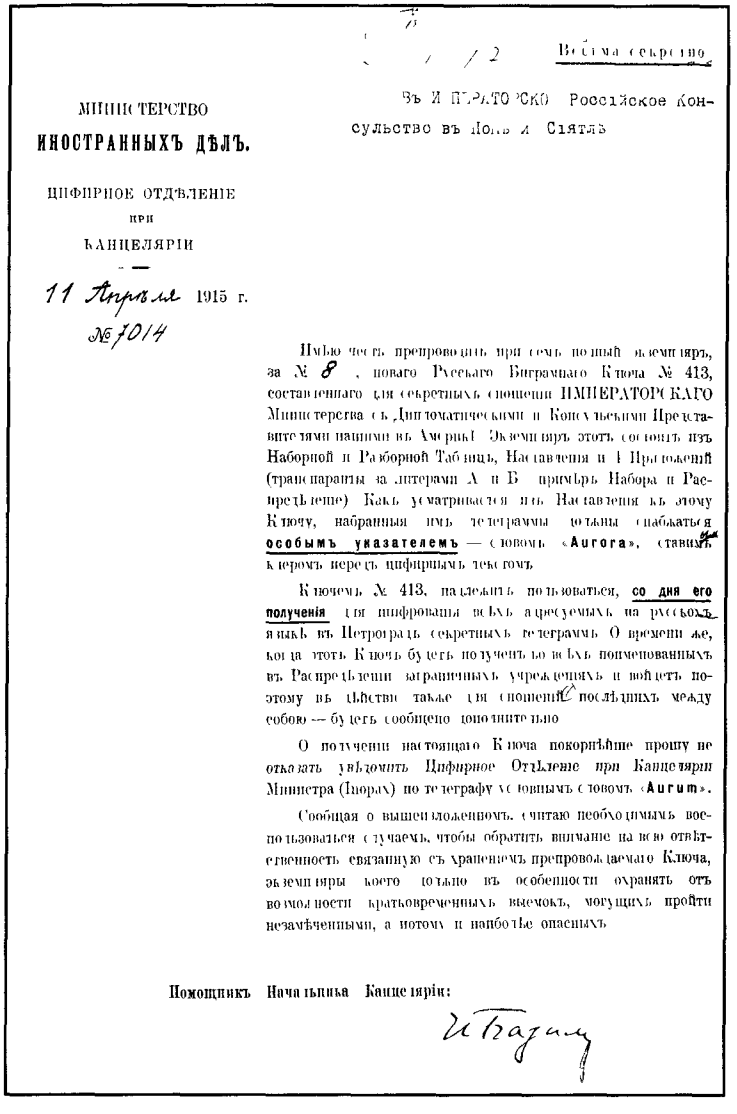




Лит. А
шифр
войск гвардии и
Петербургского
военного округа
1911 года

N821

Шифр войск гвардии
и Петербургского военного округа. 1911 г.



Всѣмъ секретно.

Въ И ПЕРАТОРСКО Российское Консульство въ Лондонѣ и Сіятлѣ

МИНИСТЕРСТВО
ИНОСТРАННЫХЪ ДѢЛЪ.

ЦИФИРНОЕ ОТДѢЛЕНІЕ
при
КАНЦЕЛЯРІИ

11 Апрѣля 1915 г.
№7014

Имѣю честь препроводить при семъ полный экземпляръ, за № 8, новаго Русскаго Биграмнаго Ключа № 413, составленнаго для секретныхъ сношеній ИМПЕРАТОРСКАГО Министерства съ Дипломатическими и Консульскими Представителями нашими въ Америкѣ. Экземпляръ этотъ состоитъ изъ Наборной и Разборной Таблицъ, Наставленія и 4 Приложеній (транспаранты за литерами А и Б примѣръ Набора и Распредѣленіе). Какъ усматривается изъ Наставленія къ этому Ключу, набранныя имъ телеграммы должны снабжаться **особымъ указателемъ** — словомъ «**Aurora**», ставимымъ передъ ключомъ передъ цифирнымъ текстомъ.

Ключемъ № 413, надлежитъ пользоваться, **со дня его полученія** для шифрованія всѣхъ адресуемыхъ на русскомъ языкѣ въ Петроградъ секретныхъ телеграммъ. О времени же, когда этотъ Ключъ будетъ полученъ во всѣхъ поименованныхъ въ Распредѣленіи заграничныхъ учрежденіяхъ и войдетъ поэтому въ дѣйствіе такъ для сношеній послѣднихъ между собою — будетъ сообщено дополнительно.

О полученіи настоящаго Ключа покорнѣйше прошу не отказать увѣдомить Цифирное Отдѣленіе при Канцеляріи Министра (Іюрах) по телеграфу условнымъ словомъ «**Aurum**».

Сообщая о вышеизложенномъ, считаю необходимымъ воспользоваться случаемъ, чтобы обратить вниманіе на всю отвѣтственность связанную съ храненіемъ препровождаемаго Ключа, экземпляры коего только въ особенности охранять отъ возможности кратковременныхъ выемокъ, могущихъ пройти незамѣченными, а потому и наиболѣе опасныхъ.

Помощникъ Начальника Канцеляріи:

И Базили

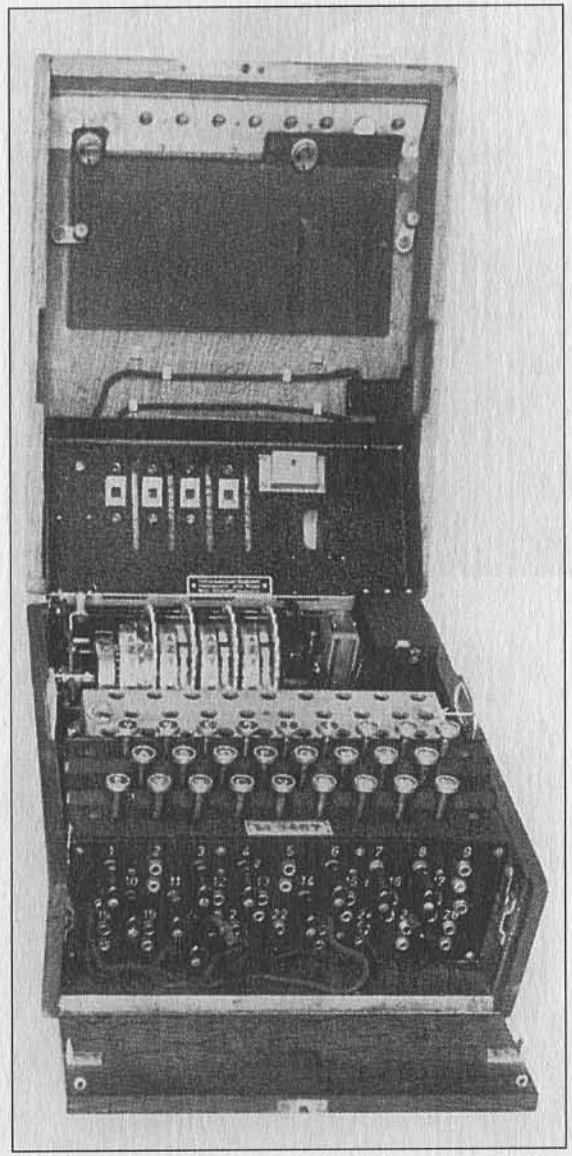
Сопроводительное письмо к шифру, подписанное
начальником канцелярии Министерства иностранных дел И. Базили

Г. И. Бокий,
студент Горного кадетского корпуса
им. императрицы Екатерины II.
Санкт-Петербург, 1899 г.

Г. И. Бокий и А. М. Горький в зверопитомнике СОАОКа. 1929 г.

В. Н. Яковлева,
председатель
Петроградской ЧК.
Ноябрь 1918 г.

Ф. И. Эйхманс,
заместитель начальника
спецотдела



Шифрмашина «Энигна»

Г. О. Ярдли

Эмблема американского Центра истории криптологии

У. Фридман в рабочем кабинете

Б. А. Аронский

С. С. Толстой

Юбилейный знак криптографической службы России

Сотрудники Биосада с председателем СОАОК

При разбивке их на пятизначные группы получалось восемь таких групп, что очень облегчало проверку текста криптограммы.

Сохранился и еще один шифр, которым пользовался Николай II [13]. Это — разнозначный код объмом 10 000 словарных величин. Состоит он из двух книг, первая из которых включает «Наборные таблицы», а вторая — «Разборные таблицы». Внешне каждая книга оформлена как довольно объемный том размером 16,5×22 см в вишневом муаровом переплете с золотым тиснением.

В словаре кода имеется несколько типов словарных величин, каждому из которых приданы кодовые обозначения разной значности. Так, на задней крышке переплета наклеен специальный листок, на котором отпечатаны падежные и глагольные окончания. Эта категория словарных величин имеет однозначные кодовые обозначения.

Таблицы чисел, дни месяцев, имена членов императорской фамилии, важнейшие города мира имеют кодовые обозначения от 000 до 999. Основная масса словарных величин, представляющая собой буквы, слоги, слова, словосочетания, имеет четырехзначные кодовые обозначения от 0000 до 9999. Последняя по порядку тысяча таких кодовых обозначений (от 9000 до 9999) обозначает губернские и уездные города России.

Все словарные величины расположены на листах кода в два столбца по пятьдесят величин на странице. Цифры, обозначающие тысячи и сотни, помещены в верхних углах страниц (00—99).

Важно отметить, что использование в кодовых величинах одного кода кодовых обозначений неодинаковой длины, как это имело место в данном случае, существенно затрудняло дешифрование.

Каков же лексический состав словаря царского кода? В основном, кроме общеязыковой лексики, сюда помещены слова, свойственные военной и политической переписке. Например: агитация, аэро-

стат, аккредитованный, артиллерия, арьергард, батальон, дипломатический агент, мина Уайтхеда, мина заграждения, мина донная и т. п., а также: гусар, гусарский, драгун, драгунский, егерь, егерский, кирасир, кирасирский, муниципальная колонна, пионер, пионерский, дирижабль, цеппелин, летчик и др. Словосочетания: «уклоняясь от боя», «приостановить бой», «возобновить бой» и др.

Большая часть такой лексики, естественно, устарела, (например, ландьерг, ландьерный, лангштурм, лангштурмный, гиеволете, гиеволетерный и т. д.), но словарь кода в целом представляет собой интересный и ценный источник для исторической лексикологии. Интересен он и с точки зрения стилистики, так как, являясь средством для составления деловых сообщений, неожиданно содержит множество слов с эмоционально-экспрессивной окраской: бескорыстный, безотрадный, благородный, болезненный, благополучный, бюрократический, ни под каким видом, молва, нелепый, неправдоподобный, честолюбивый, эпитет и т. п.

Николаю II докладывались все вопросы, касающиеся использования императорских шифров. Вот докладная военного министра, представленная Николаю II 15 июля 1906 года:

«В[есьма] секретно.

Всеподданейше представляю при сем Вашему Императорскому Величеству экземпляр № 1 изменений порядка набора и разбора телеграмм по шестому ключу Военного министерства, вводимых в действие с 25-го сего июля, причем начальству военных округов указано, что при сношениях с центральными управлениями министерств эти изменения должны быть применяемы немедленно по получении их на местах...» [14].

Здесь же рукой военного министра написана резолюция царя: «Высочайше повелеваю экземпляр № 1 изменений порядка набора и разбора телеграмм

по шестому ключу Военного министерства передать в Военно-Походную Его Императорского Величества канцелярию».

Насколько подробно информировался Николай II по вопросам об использовании шифров, можно заключить и из докладной царю, составленной военным министром 9 августа 1906 г., в которой, в частности, докладывается: «Седьмой ключ Военного министерства военного времени входит повсеместно в действие с 10-го сентября сего года... но до 10-го сентября следует в начале телеграммы ставить пятизначную группу «31475»...» [15].

Экземпляры шифров, принадлежавшие царю, находились всегда в месте его пребывания и содержались в канцелярии Министерства императорского двора, в Императорской главной квартире, а в военное время в Военно-Походной Его Императорского Величества канцелярии».

В военном ведомстве строго соблюдались правила пользования шифрами и их хранения. Правилами предписывалось при утере хотя бы одного экземпляра шифра немедленно выводить его из употребления и заменять новым. Такая же замена должна была производиться при подозрении, что тайна шифра противником открыта.

Снятие копий с шифров категорически запрещалось, а потому в военное время полевые штабы армий, отдельных корпусов и отдельно действовавших отрядов снабжались запасными экземплярами шифров для выдачи их в необходимых случаях тем лицам, которых не было в списке, упомянутом нами выше, но которым, по мнению командующих армиями или других главных войсковых начальников, следовало иметь тот или иной шифр.

Экземпляры ключей военного времени, выданные командующим войсками в округах, командирам корпусов, комендантам крепостей и наказным атаманам, хотя и находились в непосредственном распоряже-

нии этих лиц, должны были храниться в помещении соответствующих штабов в «запертых секретных хранилищах»: шкафах, сундуках, ящиках и обязательно в особо секретных пакетах, запечатанных личной печатью тех лиц, на чье имя они были выданы. Так же строго хранили экземпляры шифров (ключей) и начальники главных управлений Военного министерства и начальники штабов округов. Замену ветхих экземпляров шифров, передачу шифров от увольняемых лиц и т. п. производил Главный штаб. Там же определялся срок действия шифров.

С целью сохранения шифров в секрете инструкциями предписывалось ни в коем случае не оставлять в делах документы, зашифрованные шифром. Лица, использующие шифр, обязаны были помещать в дела копии отправленных шифрсообщений, но изложенные «обыкновенным письмом». Черновики уничтожались. Лицо, получившее шифрсообщение, также было обязано уничтожить подлинник, поместив в дело входящих документов соответствующую копию, изложенную «простым письмом». Проверка шифров военного времени, находящихся в округе, в армии и т. д., производилась не реже одного раза в год.

Шифры МВД и других ведомств. Агентурные шифры

Шифры Департамента полиции, жандармерии, гражданских ведомств существенно уступали шифрам МИД и Военного министерства по своим криптографическим качествам. Так, например, *«секретный телеграфный ключ шефа жандармов»* 1907 г. [16] представлял собой набор из тридцати простых замен, где буквам открытого текста соответствовали две цифры текста шифрованного, номер ключа — простой замены — проставлялся в открытом виде в начале сообщения. В правилах к этому шифру сообщалось, что

«секрет этого ключа не доступен тем, что в нем цифры составлены в произвольном порядке и, кроме того, он имеет 29 изменений».

При этом адресат депеши, подпись и все числа не зашифровывались и вставлялись в сообщение в открытом виде, отделяясь от шифробозначений с двух сторон (или с одной стороны — в конце или начале сообщения) знаками «тире».

Другой жандармский шифр — это алфавитный цифровой код на 110 величин, одно- и двузначный, со сдвигом, т. е. первые словарные величины (агитатор, администрация фабрики, арестовать и т. д.) имеют соответственно кодовые обозначения: 87, 88, 89 и далее по циклу.

Естественно, весьма характерным является лексическое наполнение словарей подобных шифров: беспорядок, бить, буйство, вести себя дерзко, вина администрации фабрики, вина рабочих, возбуждение дела о стачке, драка, забастовка, зачинщик, казаки, сжечь, социалистический и т. п.

Среди множества шифров России агентурные шифры всегда занимали особое положение. В соответствии с названием они предназначались для связи разведчиков и агентов с центром.

К сожалению, к настоящему времени сохранилось очень мало сведений об этих шифрах. По инструкции они должны были уничтожаться, как только надобность в них пропадала, и эти правила неукоснительно соблюдались. Тем не менее, нам удалось найти некоторые материалы, позволяющие здесь остановиться подробнее на этом вопросе.

Одним из основных требований, предъявляемых к агентурным шифрам, является обеспечение максимально возможной безопасности их пользователю. Поэтому вся документация к шифру (ключи, правила пользования) должна была обладать свойством «скрываемости» или же, в идеале, свойством «безуликовости». Кроме того, сам процесс шифрования

должен был быть максимально простым и быстрым, даже если его приходилось осуществлять в самых неблагоприятных условиях. Эти требования зачастую входили в противоречие с требованиями высокой криптографической стойкости, и в этих условиях криптографы обычно выбирали некую золотую середину. Рассмотрим некоторые виды таких шифров, применявшихся в России в интересующую нас эпоху.

Шифры Цезаря. Шифр Юлия Цезаря, изучаемый в школах разведчиков всех стран, с исторической точки зрения, как мы уже писали, является одним из важнейших этапов в развитии криптографии. Большинство систем шифров замены более позднего происхождения являлись вариантами шифра, изобретенного за несколько десятков лет до нашей эры. Простейшими агентурными шифрами в рассматриваемый период были также шифры простой замены, в которых используемые простые замены были достаточно структурными и потому легко запоминались. Таким образом, это были самые старые безликовые шифры «на память», аналогичные системе «шифр Цезаря» с небольшими изменениями, как-то: сдвиг шифралфавита на 2, 3, 4 и больше знаков, замена каждой буквы алфавита следующей по алфавиту буквой, использование лозунга. Обычно ключ определялся датой зашифрования сообщения. Очевидно, что эти шифры легко поддавались дешифро- ванию уже в то время.

Более сложным шифром был шифр многозначной замены, получивший название «прыгающий шифр». Он появился в конце XIX века и криптографически представлял собой несколько простых замен, которыми агент должен был пользоваться при шифровании сообщения, переходя от одной замены к другой через каждые пять—семь или девять знаков текста. Этот шифр был в действии непродолжительное время, так как для агентов он был слишком сложен и

они предпочитали «шифр Цезаря» с часто меняющимися ключами.

Книжные шифры. В качестве агентурных шифров использовались и книжные шифры. Выбиралась определенная книга, в качестве шифробозначений использовались номера страниц, строк, мест в строках, где находились шифруемые буквы. Этот тип шифра также можно отнести к безуликовым шифрам, естественно, при аккуратном пользовании книгой. Книжные шифры обладали несравненно большей криптографической стойкостью по сравнению с шифрами простой замены. Тем не менее в «черных кабинетах», где дешифровали такие шифры, было подмечено, что шифрзнаки, соответствующие большим номерам строк или мест в строке, обозначали, как правило, редко встречающиеся знаки открытого текста. Это была зацепка для раскрытия сообщения и поиска соответствующей книги. Дело в том, что, оказывается, как правило, каждый корреспондент предпочитает находить в книге буквы, стоящие недалеко от начала строки или начала страницы. В противном случае подсчет занимает много времени, и при этом увеличивается вероятность появления ошибки. Редко встречающиеся буквы по необходимости могут оказаться где-то далеко от начала страницы или строки.

Тем не менее, поскольку книга обеспечивала дешифрование всего сообщения, всегда пытались отыскать используемую книгу. Не случайно при аресте и обыске лиц, подозреваемых в шпионаже, в первую очередь обращали внимание на их библиотеки. Заметим, что книжные шифры широко применялись в России в деятельности нелегальных партий и групп, о чем подробнее мы расскажем ниже.

Шифры перестановок. Номерные ряды. В конце XIX — начале XX в. получили большое распростране-

ние в качестве агентурных шифров различные виды шифров перестановок — от старейших шифров — «Трафарета Кардано», изобретенного математиком Жеромом Кардано в середине XVI столетия, до новых шифров — простых вертикальных перестановок, шахматных и произвольных лабиринтов, прямоугольных и прямолинейных решеток и двойных перестановок.

В шифры перестановок вносились различные усложнения, такие как: спиральная выписка, выписка по диагоналям, выписка по лозунгу и распределителю, использование фигурных вертикальных перестановок (со столбцами различной длины).

Следует отметить, что впервые шифр, близкий к шифру двойной перестановки, был изобретен в России народовольцем Михайловым в эпоху царствования Александра II.

В качестве агентурных в России часто использовались шифры вертикальной перестановки с усложнениями. Текст сообщения записывался в таблицу с колонками. Далее текст выписывался по колонкам. Порядок выбора колонок определялся ключом, который пользователи знали на память. Этот ключ должен был меняться достаточно часто (например, не реже, чем один раз в два месяца).

Необходимо отметить, что этот ключ — на память (шкала вертикальной перестановки) определялся номерным рядом некоторого легко запоминаемого лозунга. Например, брался лозунг «Боже, царя храни». Под этим лозунгом составлялся номерной ряд, определявший порядок выписки колонок. Нами было найдено описание ключа военного агента 1911 г. [17], в котором дается пример составления шифрсообщения:

Б	О	Ж	Е	Ц	А	Р	Я	Х	Р	А	Н	И
3	8	5	4	12	1	9	13	11	10	2	7	6
S	O	O	B	T	S	C	H	I	T	E	A	D
R	E	S	B	E	R	N	S	T	R	A	S	S
E	P	I	A	T	I	V	A	N	O	W	L	E
W	I	K	O	W	O	U						

Здесь вторая строка — номерной ряд. Буквы алфавита упорядочиваются слева направо, и, таким образом, каждая буква лозунга получает свой порядковый номер. Далее шифртекст выписывается пятизначными группами (недостающие до пяти в конце сообщения знаки выбираются произвольно):

SRIOE AUSRE WBBAO OSIKD SEASL OEPIC...

Расшифрование по известному лозунгу производится очевидным способом.

Итак, документально подтверждено, что номерные ряды были известны и успешно применялись в России уже в начале XX в. Автор их не известен, но следует полагать, что это — отечественное изобретение.

О криптографической стойкости таких шифров написано немало специальных статей. Углубление в данную проблематику не составляет предмет нашего изучения. Поэтому мы здесь отметим только, что вообще все шифры перестановок легко отличаются от других типов шифров. Такое отличие обнаруживается, например, с помощью простого статистического анализа встречаемости букв текста сообщения. Диаграммы частот знаков шифрсообщений должны соответствовать диаграммам вероятностей встречаемости этих знаков в соответствующем языке.

В XIX — первой половине XX в. в мировой практике в ходу были шифры вертикальной, двойной вертикальной перестановки, шифры решеток. Наиболее часто в качестве агентурных использовались шифры вертикальной и двойной вертикальной перестановок.

Анализ этих шифров показывает, что, если взять наиболее характерные биграммы языка (например, известно, что для русского языка характерными биграммами являются СТ и МС) и составить все расстояния, расположенные между знаками этих биграмм в шифртексте, то некоторые среди них долж-

ны будут выделяться. И сами эти расстояния (или некоторые их делители) должны равняться глубине колонной таблицы, используемой для шифра перестановки. После определения этой длины собирают по ней возможные в тексте другие биграммы. После чего из биграмм составляют четверки знаков и т. д.

По-видимому, русские криптографы знали об этих слабостях шифров вертикальной перестановки и по этой причине вводили некоторые усложнения. В частности, они использовали колонки прямоугольной таблицы различной длины [18]. Хотя это далеко не всегда спасало от раскрытия сообщений, процесс их дешифрования все же стоил значительно больших усилий и изобретательности.

В 1919 г., когда Советское государство своих шифров еще не имело и пользовалось старыми дореволюционными шифрами, использовались и шифры вертикальной перестановки. Так, например, таким шифром пользовался Бела Кун при зашифровании сообщений, посылаемых в Москву В. И. Ленину во время венгерской революции. В своей книге Г. Ярдли указывает, что эти сообщения были перехвачены американцами.

Глава десятая

О ЧЕМ УМОЛЧАЛА ИСТОРИЯ

Перлюстрация дипломатической переписки в XIX — начале XX в.

С началом нового века мало что изменилось в деятельности «черных кабинетов». В «либеральных проектах» царствования Александра I перлюстрация забыта не была. Уже в 1805 г. в «секретном направлении» комитету высшей полиции говорилось: «Через сношения с дирекцией почт комитет должен получать немедленные и верные сведения о подозрительных переписках», а в параграфе 3 положения «Комитета общей безопасности» от 13 января 1807 г. читаем: «Для получения таковых сведений (о проживающих в столице и вновь приезжающих подозрительных людях, о разглашаемых слухах, сочинениях и известиях, вредные последствия иметь могущих, и о скопищах и собраниях подозрительных) комитет дает нужные предписания обер-полицмейстеру и, буде нужно, употребит к тому по своему усмотрению и другие лица. Министр внутр. дел сообщать будет оному известия через губернатора из губерний получаемые и открываемые по дирекции почт о подозрительных переписках» [1].

К концу царствования Александра I, как известно, правительственный шпионаж распространился чрезвычайно широко, и, конечно, перлюстрация за-

нимала видное место среди способов, с помощью которых правительство узнавало о том, что говорят и делают в обществе. В этом отношении определенный интерес представляет переписка министра внутренних дел при Александре I О. П. Козодавлева с тогдашним московским почт-директором Д. П. Руничем, часть из которой опубликовал в свое время А. В. Предтеченский [2].

Николай I, Александр II охотно читали выписки из перлюстрированных писем и в архиве секретной экспедиции при царской канцелярии находились таковые с их собственноручными пометками, как и другие документы с царскими подписями, касающиеся этой секретной деятельности. Перлюстрация дипломатической, военной, частной и иной корреспонденции продолжалась и в дальнейшем. Материалы, раскрывающие эту сторону деятельности государства, сохранились в архивах, часть из них опубликована. На наш взгляд, большую ценность в этом отношении представляют мемуары государственных деятелей той эпохи. И здесь нам бы хотелось остановиться на таком ценнейшем историческом источнике, каким является «Дневник» В. Н. Ламздорфа [3].

Владимир Николаевич Ламздорф родился в 1844 г. в родовитой дворянской семье. Род Ламздорфов (Ламбздорффов) уходит своими корнями в XIII в. к германскому рыцарю Отто фон Ламездорпе. В XIV—XIX вв. представители этой фамилии проживали в Эстляндии, Лифляндии и Курляндии. В России дед В. Н. Ламздорфа Матвей Иванович, к которому сам Ламздорф относился с чувством глубочайшего почитания, начал свою служебную карьеру еще при Екатерине II, участвовал в чине генерала в русско-турецких войнах, а затем стал первым губернатором вновь присоединенной Курляндии. Позднее дед стал воспитателем будущего императора Николая I. В. Н. Ламздорф очень ревниво относился к своей

карьере, к положению при дворе, безраздельно причисляя себя к придворной российской аристократии.

Образование В. Н. Ламздорф получил в аристократическом Пажеском корпусе, свою карьеру начал в качестве придворного камер-пажа и через три десятка лет с гордостью вспоминал, как 24 ноября 1861 г. царь Александр II спросил его на лестнице дворца, не из Ламздорфов ли он, опознав по фамильному сходству. В 1866 г. Ламздорф поступает в Министерство иностранных дел. Его дипломатическая служба была начата на весьма скромных должностях, но с 1878 г., после пребывания у царя в Ливадии вместе с будущим министром иностранных дел Гирсом, карьера Ламздорфа резко убыстряется, на него сыплются награды. В 1879 г. он уже камергер и управляющий литографией министерства с правом на хорошую казенную квартиру в здании министерства. С апреля 1881 г. — второй советник министра, с сентября 1882 г. — директор канцелярии министерства, с апреля 1886 г. — первый советник министра. По совместительству он является членом Цифирного комитета.

Вся жизнь и карьера Ламздорфа были тесно связаны с центральным аппаратом министерства. «Граф Ламздорф,— вспоминал впоследствии С. Ю. Витте, — вечно работал, и вследствие этого, как только он поступил в Министерство иностранных дел, он всегда был одним из ближайших сотрудников министров... Граф Ламздорф был ходячим архивом Министерства иностранных дел по всем секретным делам этого министерства» [4].

В январе 1895 г., после смерти министра иностранных дел Н. К. Гирса, Ламздорф, располагавший всеми секретными внешнеполитическими архивами, оказывается на некоторое время человеком, наиболее посвященным в тайны дипломатии царской России. «Странным является мое положение в данный момент, — записывает он в дневник, — мои

секретные архивы содержат все тонкости политики последнего царствования. Ни молодой государь (Николай II. — *Т. С.)*, ни почтеннейший Шишкин, назначенный временно управляющим министерством иностранных дел, не имеют ни малейшего представления о документах, доверенных в последние годы исключительно и совершенно бесконтрольно мне. Я работал в глубокой тени возле моего бедного старого начальника (Н. К. Гирса. — *Т. С.*), меня никто не знает, и вот теперь, когда исчезли как он сам, так и государь, которому он столь замечательно помогал править, я оказываюсь в положении единственного обладателя государственных тайн, являющихся основой наших отношений с другими державами» [5].

В 1900 г. В. Н. Ламздорф назначается министром иностранных дел России. На этом посту он находится до 1906 г.

В течение многих лет В. Н. Ламздорф вел дневник, который хранится в настоящее время в Центральном государственном архиве Октябрьской революции в Москве и представляет собой бесценный документ эпохи. Сам Ламздорф, очевидно, представлял ценность своих записей для потомков. Так, он писал на страницах дневника: «Мое положение дает мне возможность записывать факты, вскрывать подспудные стороны исторической игры в карты; это может оказаться полезным в будущем. Сколько исследований пришлось бы тогда делать в секретных и недоступных архивах, чтобы выяснить даже частицу того, что мне легко сделать сегодня путем фотографирования, если можно так выразиться, своего рабочего дня» [6].

В свой дневник Ламздорф, кроме регулярных скрупулезных записей о текущих событиях, в первую очередь связанных с высшей государственной политикой и дипломатией, помещал копии важнейших документов, в том числе копии перлюстраций.

Наряду с авторским текстом и отдельными газетными вырезками значительное место в дневнике отводится Ламздорфом цитированию различных документов на русском, французском, немецком и английском языках. Некоторые документы заносятся им в дневник без всякой субъективной оценки и притом с исчерпывающей полнотой.

В числе прочих подобных документов Ламздорф зафиксировал в дневнике в виде копий английского текста [7] происходивший в 1895 г. обмен письмами между русским царем Николаем II и его двоюродным братом германским кайзером Вильгельмом II, а также копии перлюстраций переписки германского посольства в России. В качестве примера можно привести перлюстрированную телеграмму кайзеру Вильгельму II, посланную из Петербурга 18 (30) сентября 1895 г. его флигель-адъютантом Хельмутом Мольтке после свидания с Николаем II. Ламздорф вносит в дневник копию полного текста расшифрованной телеграммы Мольтке и внизу приписывает: «Государь вернул эту перлюстрацию без всякой пометы; как видно, доклад Мольтке о состоявшейся аудиенции у Его Величества является точным» [8]. Пометы Николая II порой поражали Ламздорфа своей некомпетентностью. Так, на перлюстрации одной из телеграмм, пришедших из Берлина в адрес германского посла в России Радолина и содержащей несколько рекомендаций, государь сделал помету: «Детски глупые советы!» Ламздорф пишет по этому поводу: «Я не особенно понимаю, почему глупые? Сознаюсь, что я, наоборот, восхищен той тщательной заботливостью и высоким благоразумием, с которыми Берлин направляет первые шаги своего нового посла в области, которая ему еще не достаточно знакома. Совсем неплохо было бы и нам последовать такому примеру» [9]. Однако были на перлюстрациях пометы Николая II и другого типа. Ламздорф пишет: «В пакете с возвращенными бума-

гами имеется телеграмма от Капниста [10], на которой нашим августейшим повелителем сделаны озорные пометы в духе тех, которые иногда делал покойный государь Александр III в адрес Михаила Горчакова» [11].

Российская служба перлюстрации к концу XIX в. накопила уже колоссальный опыт. Традиционно большое внимание уделялось перлюстрации дипломатической корреспонденции, а также так называемых «шпионных» писем для генеральных штабов — военного и морского. Эта корреспонденция получалась в Петербурге и отправлялась за границу в особых пост-пакетах, была зашифрована и опечатана. Все эти предосторожности, однако, не спасали ее от перлюстрации. В этом пост-пакете она и попадала в «черный кабинет», притом обязательно. Туда же она попадала и в случае, если доставлялась на почту всего за несколько минут до заделки пост-пакета перед отправкой его на вокзал. В «черных кабинетах» имелась полная коллекция безукоризненно сделанных металлических печатей как всех иностранных посольств, консульств, миссий и агентов в Петербурге и Министерстве иностранных дел за границей, так и всех послов, консулов, атташе министров и канцлеров. С помощью этих печатей вскрывать и заделывать дипломатическую корреспонденцию не представляло никаких трудностей.

За предшествовавший период существования «черных кабинетов» в России, т. е. со времен царствования Елизаветы Петровны, русским перлюстраторам были известны и практиковались три способа производства поддельных печатей. В старину печать отливалась из свинца по форме, снятой гипсом с негатива печати, сделанного из воска. Этот способ, кроме того, что был сложен из-за четырехкратного переснимания оттиска (негатива — воском, позитива — гипсом, вновь негатива — свинцом и, наконец, снова позитива уже на самом письме — сургучом),

давал недостаточно резкие отпечатки. В середине XIX в. один из чиновников МИД изобрел способ производства поддельных печатей из серебряного порошка с амальгамой. Этот способ был очень прост и скор, а печати получались резкие. Однако они имели существенный недостаток — были весьма недолговечны, ломались от малейшего неосторожного прикосновения. Наконец, уже в начале XX в. другим секретным чиновником МИД России был изобретен остроумнейший способ производства идеальных печатей из твердого металла. Резкость получаемого оттиска была безукоризненна, сама печать — долговечна, а время, необходимое для ее изготовления, исчислялось минутами. Талантливый чиновник, изобретший этот способ производства печатей, а кроме того, аппарат для вскрытия писем паром, по докладу министра Столыпина царю был награжден орденом Владимира 4-й степени «за полезные и применимые на деле открытия».

Вследствие того, что, с одной стороны, дипломатическая корреспонденция многими посольствами сдавалась на почтамт незадолго до ее заделки в пост-пакеты и отправки на вокзал, а, с другой стороны, за получением приходящей почты курьеры являлись на почтамт тотчас по прибытии ее с вокзала, с этой корреспонденцией приходилось очень спешить, так как во время ее фотографирования за ней приходили почтовые чиновники, которых внизу курьеры бранили за то, что они долго возятся с разбором посольских пост-пакетов. Фотографии снимались при освещении лентой магния, выделявшего при горении массу дыма, а так как окна должны были быть закрыты ставнями, чтобы не обращать внимания на себя даже служащих почтамта, то атмосфера в конце каждой такой операции в фотографической комнате становилась невыносимой.

В период русско-японской войны одному из ведущих русских криптографов В. И. Кривошу-Нема-

ничу, работавшему тогда в Генеральном штабе, пришлось поехать в служебную командировку во Францию в связи с проводимой совместно с французами дешифровальной работой. Там он в числе прочего ознакомился с работой «черного кабинета» в Париже.

Оказалось, что парижский «черный кабинет» был устроен аналогично петербургскому. Эта «секретная часть» находилась в частном доме. Официальная вывеска на нем гласила, что здесь располагается какой-то землемерный институт. Один из служащих «секретной части» действительно знал толк в лесоводстве и деле землеустройства, и если какой-то частный человек туда забредал, то ему давалась вполне квалифицированная нужная справка. В передней комнате, куда мог прийти с улицы кто угодно, на стенах висели карты, планы каких-то лесов, земельных участков, имений и пр., а на столах лежали свежие газеты, вырезки из них, письменные принадлежности. Из этой комнаты была дверь в следующую, в которой также не было ничего секретного, но был шкаф, служивший дверью в третью комнату. Таким образом, чтобы пройти в действительно секретную часть, необходимо было идти через шкаф, зная, как его открыть (наступить одновременно на две дощечки на полу и нажав одно из украшений шкафа). Дверь автоматически сама запиралась за прошедшим через нее. В третьей комнате, имевшей сообщение пневматической почтой с главным телеграфом, проводилась регистрация поступивших телеграмм, их разбор по странам и передача по принадлежности в кабинеты дешифровальщикам, занимавшимся с ними везде по двое. У дешифровальщиков были подлежащие их ведению коды, которыми они пользовались, и книга, куда заносились все результаты их работы.

Эта книга передавалась в следующую комнату, там все сведения сортировались «по вопросам», содержащимся в сообщении. Из одной телеграммы делались

две-три разные выписки, если она содержала два-три разных вопроса. Один экземпляр таких выписок хранился тут же, а другой посылался министру (иностранных дел, военному, морскому) или президенту республики, словом, тому, кому полагалось знать данное сообщение. В следующей комнате была перлюстрационная часть, имевшая сообщение пневматической почтой с главным почтамтом. Все прибывающие в Париж дипломатические пост-пакеты прежде всего прямо с почты отправлялись в эту перлюстрационную часть, где их вскрывали, читали, в случае надобности фотографировали или списывали, а затем либо переводили, либо направляли для дешифровки в кабинеты дешифровальщиков. После прочтения и фотографирования письма вновь заклеивались и отправлялись по той же трубе пневматическим способом на почтамт.

Кроме раскладки материалов «по вопросам», в «секретной части» делались еще сводки «по вопросам». Таким образом, в каждый данный момент можно было иметь полностью весь ход развития данного вопроса вполне разработанным и всесторонне освещенным с разных точек зрения, если о нем писали представители разных правительств.

Для президента ежедневно выпускался «листок» со всеми полученными за сутки сведениями — нечто вроде дипломатической газеты. Все коды французы покупали у де Вернина, который иногда приезжал в Париж. Имелись у них и все русские коды, что отнюдь не скрыли от Кривоша-Неманича. Однако он с удовольствием заметил, что один очень простой способ пользования кодом, изобретенный им самим и сообщенный министру, в Париже известен не был.

Так добывались материалы для дешифровальной службы Франции. Но прибегали и к другим способам. Например, когда уезжал или приезжал курьер с пост-пакетом, то вместе с ним до границы

(или от границы до Парижа) ехал агент. Этот агент за соответствующее вознаграждение получал от курьера пост-пакет на 30—40 минут, пока на границе таможенные чины проверяли багаж пассажиров. В распоряжении агента на пограничной станции была комнатка, где он вскрывал пост-пакеты, фотографировал их содержание и, заделав, возвращал курьеру.

«„Черные кабинеты", разумеется, существовали везде, даже в самых демократических республиках Америки и Старого Света, и в каждой стране практикуется свой способ вскрытия писем, подделки печатей и отмечания того, что данное письмо уже подвергалось перлюстрации. Но справедливость требует сказать, что нигде в мире „черный кабинет" не работал так чисто, как в России, и в особенности в Петрограде» — так писал в своих воспоминаниях один из опытнейших русских перлюстраторов той поры С. Майский [12]. Он же свидетельствует, что очень грубо работали перлюстраторы Германии и Австрии. В секретном деле знаменитая немецкая аккуратность не подтверждалась.

Письма, перлюстрированные в российских «черных кабинетах», как бы они хитро заделаны ни были, не сохраняли на себе ни малейшего следа вскрытия даже для самого пытливого глаза. Даже опытный глаз перлюстратора не всегда мог уловить, что письмо уже однажды вскрывалось. Никакие ухищрения, к которым прибегали те, кто стремился сохранить дипломатическую корреспонденцию от перлюстрации (царапины печати, заделка в сургуч волоса, нитки, бумажки и т. п.), не гарантировали ее от вскрытия и абсолютно не узнаваемой подделки. Весь вопрос сводился только к тому, что на перлюстрацию такого письма требовалось несколько больше времени.

Однако порой иностранные дипломаты узнавали о перлюстрации своей переписки совершенно не-

ожиданным образом. Так, Ламздорф в своем дневнике приводит случай, когда министр иностранных дел Лобанов-Ростовский в разговоре с одним из иностранных дипломатов оказался чересчур откровенным и повел с ним речь о чем-то, чего не мог знать русский министр из официальных источников. Это обстоятельство стало известно германскому послу, чьи интересы оказались в данном случае задетыми. Германский посол тотчас же сделал необходимые выводы, и в Берлин была отправлена телеграмма, заканчивающаяся такими словами: «Использую этот шифр из осторожности, так как предыдущий употреблялся слишком часто и у меня появились основания для недоверия. Меня предупредили, прошу о новом шифре». Ламздорф, приводя этот документ, добавляет: «Сабанин, старший чиновник нашей экспедиции по перлюстрациям, прилагает к данному документу письмо на имя князя Лобанова; в нем он привлекает внимание министра к вредоносности тех «предупреждений», наличие которых выясняется из телеграммы. Князь пишет Вакселю (вице-директору канцелярии МИД России. — *Т. С.*), рекомендуя самую высокую осмотрительность при обращении со столь секретными документами; однако совершенно очевидно, что проболтаться в данном случае могли Лобанов или Шишкин при их разговорах с дипломатами или же с министром финансов и его агентами» [13].

Как же старались сохранить тайну своей переписки русские дипломаты, зная о практике вскрытия дипломатической почты? Были различные приемы. Вот один из них. Про графа Н. П. Игнатьева в «черном кабинете» бытовало предание, что он, будучи послом в Турции, отправлял свои донесения в простых (не заказных) письмах, заделанных в грошовые конверты, которые пролежали некоторое время вместе с селедкой и мылом. Адрес на конверте он заставлял писать своего лакея, притом не на имя министра

иностранных дел, а на имя его дворника или истопника, по частному адресу. Эти меры действительно спасали корреспонденцию графа от перлюстрации.

Дешифровальная служба МИД и Военного ведомства

Истина и пути ее достижения...

Всякий ученый, чем глубже постигает предмет своего исследования, тем яснее осознает относительность своих знаний, субъективность своих представлений о сущности и причинах явлений. То, что казалось истиной, целью вчера, сегодня, с получением новой информации, становится лишь этапом. Не являются исключением и исторические исследования. То или иное направление исторической науки высвечивает лишь какую-то грань, не охватывая в целом всей картины исторического процесса. Но плод каждого истинно научного труда способен обогатить эту картину, расцветить ее свежими красками, поставить вопросы, ответы на которые скрывают великую тайну человеческой истории. Изучение роли и места криптографической службы в истории нашего государства — одно из направлений таких исследований, которое, к сожалению, долгое время оставалось вне поля зрения российских ученых.

Изобретенный в конце XIX — начале XX в. А. С. Поповым и Маркони радиотелеграф, широкое распространение радиопередатчиков послужили толчком для более интенсивного развития шифровальной и дешифровальной деятельности. Возможность быстрой передачи шифрованных сообщений на большие расстояния, а также возможность перехвата сообщений в пунктах передачи, приема и по пути следования депеш обусловливали рост криптографических отделов и отделений с привлечением на эту службу большого количества телеграфистов, радиотехников, лингвистов, математиков.

Усиливается разведывательная, агентурно-оперативная деятельность, направленная на получение информации о шифрах и ключах к ним, а также на получение материалов, способствующих дешифрованию переписки.

Не случайно годы, предшествующие началу Первой мировой войны, называют годами украденных кодов. Но начиная с конца 70-х годов XIX в. имело место неоднократное хищение агентурой шифров и кодов предполагаемых противников.

Россия, к сожалению, в этой деятельности бывала и пострадавшей стороной. Особенно крупная кража шифров произошла, как это следует из изученных нами архивных материалов МИД, в русском посольстве в Пекине в 1888 г. [14].

Накануне русско-японской войны 1904—1905 гг. в Порт-Артуре были выкрадены планы укреплений крепости и шифры, использовавшиеся русским военным командованием [15]. Кража была совершена под руководством небезызвестного Сиднея Рейли, бывшего в Корее с разведывательными поручениями и именовавшего себя в это время представителем фирмы, торгующей лесом. После кражи Рейли спешно отправился в Японию, где продал добытые документы за большие деньги японцам. Япония в это время была союзницей Англии, и британская разведка ничего не имела против этого частного бизнеса своего ценного агента. Это обстоятельство, несомненно, сыграло свою роль в быстром падении Порт-Артура и в последующем поражении России в этой войне.

По оценкам современных историков, русская военная разведка в начале XX в. была сравнительно слабой. В основном она пользовалась сведениями, получаемыми от военных агентов (атташе). Некоторые разведывательные данные поступали от дипломатов, морских атташе, чиновников Министерства финансов. Разведывательная служба России работа-

ла бессистемно, общей программы не было. Такая ситуация существовала по всем разведывательным линиям, в том числе и в отношении разведки против Японии.

В 1911 г. видный специалист в области агентурной разведки В. Клембовский писал: «Мы не знали японцев, считали их армию слабой и плохо подготовленной, думали легко и быстро справиться с нею и... потерпели полную неудачу» [16].

Эти недостатки не замедлили сказаться в самом начале войны с Японией. Например, к 1 апреля 1904 г. (дню высадки японской армии на материк) Россия не имела никакой информации о возможном времени и месте высадки.

Вместе с тем русская разведка имела и некоторые успехи. Так, за несколько недель до нападения японского флота на Порт-артурскую эскадру в руках русских разведчиков оказался экземпляр книги японского кода, при помощи которого японское посольство в Гааге вело переговоры со своим правительством. К сожалению, такие случаи были весьма редки.

Историческая практика свидетельствует, что дешифрование кодов, особенно неалфавитных, требует больших усилий и занимает длительное время, даже если известно некоторое количество кодовых обозначений. Например, в начале 20-х годов XX в. «черному кабинету» США, для того чтобы доказать недостаточную криптографическую стойкость кода военно-морских сил США, пришлось провести такой объем необходимой работы, что одни лишь статистические данные, полученные на основе анализа шифрованных материалов, составили 1300 страниц и 650 тысяч отдельных статей. Только после этого пришел ожидаемый успех.

Иностранные державы, как и Россия, обычно использовали в переписке десятки различных кодов, хотя основными из них были всего два или три.

Остальные являлись лишь вторичными кодами, основанными на двух первоначальных. Считалось удобнее перерасполагать старый код в ином порядке, нежели создавать новый.

В конце XIX в. шифровальная служба в МИД была организована следующим образом.

При канцелярии министра был так называемый шифровальный департамент с двумя отделениями. В одном отделении шифровались свои русские сообщения министерства послам и консулам за границу и разбирались получаемые от них из-за границы сообщения. Во главе этого отделения долгие годы стоял барон Таубе. В другом разбирались копии с шифртелеграмм, перлюстрированных в «черном кабинете» главного телеграфа в Петербурге, а также присылаемые на этот телеграф из больших городов Российской империи (Москвы, Варшавы, Киева, Одессы и др.), являвшихся местом пребывания иностранных консулов. Штат этого второго отделения шифровального департамента состоял из 10—12 человек во главе с Долматовым. Один из крупнейших русских криптографов того времени В. И. Кривош-Неманич, вспоминая позднее о работе этого отделения, писал, что среди его сотрудников действительными знатоками дела были всего 2—3 человека, весь же остальной штат чиновников имел лишь весьма отдаленные сведения об искусстве шифра и дешифрования. Именно здесь работал Эрнест Феттерлейн.

Специального учебного заведения, где бы преподавалось искусство криптографии, в России не было, и поэтому чиновниками в шифровальный департамент, как, впрочем, и во все другие департаменты министерства, назначались не лица, обладающие суммой определенных знаний и известными способностями, а окончившие лицей или юридический факультет. Крупным недостатком являлось и то обстоятельство, что работники дешифровального отделения в основном владели лишь французским, не-

мецким и некоторые английским языками. Между тем министерство постоянно испытывало потребность в специалистах, владеющих и другими, более редкими языками. Поэтому департамент постоянно обращался за квалифицированной языковедческой помощью к ученым, преподавателям, иным лицам, владеющим тем или иным языком. Так, для помощи в дешифровании иностранной дипломатической переписки привлекались профессор Попов, преподававший в Петербургском университете китайскую словесность, его однофамилец, также Попов, окончивший факультет восточных языков и хорошо знавший японский язык. Этот последний даже за счет министерства был направлен в командировку в Японию с целью совершенствовать свои знания в языке. Для переводов с венгерского или, как тогда говорили, мадьярского языка обращались за помощью к Кривошу-Неманичу, работавшему в Генеральном штабе и знавшему 14 языков. Цензоры Комитета иностранной цензуры Смирнов и Жуковский переводили соответственно с турецкого и персидского языков. Все эти лица для дешифрования получали в министерстве коды, которые разрешалось брать домой. Эти коды департамент приобретал в Брюсселе у некоего де Вернина, основным занятием которого было выкрадывание шифров и кодов из посольств с помощью работавших там и подкупленных им лакеев, швейцаров, денщиков и т. д. Де Вернин делал с украденных документов довольно приличные фотографии и продавал их русским. Таким образом, в шифровальном департаменте была собрана полная коллекция кодов и департамент даже делился ими с морским и сухопутным генеральными штабами, переписывая или фотографируя свои. Бывали случаи, когда дешифровальщики департамента самостоятельно составляли коды. Так, однажды, когда долго не удавалось купить один германский код, двум сотрудникам было дано поручение его восстановить по

ежедневно получаемым министерством многочисленным копиям с телеграмм, зашифрованных этим кодом. Над этим заданием работали больше года два человека. Когда работа приближалась к концу и код был уже в значительной степени раскрыт, немцы вывели этот код из действия или сменили ключ, и, таким образом, вся работа пропала даром.

Во время русско-японской войны шел очень оживленный обмен шифрованными сообщениями между Японией, с одной стороны, и Англией и Германией — с другой. Код, который при этом использовался, был составлен на английском языке и имел пять различных ключей. Кривошу-Неманичу удалось раскрыть три ключа, с помощью которых разбиралось большинство перехватываемых телеграмм. В Париже, а, как известно, Франция была союзницей России в этой войне, также работали над раскрытием этого кода. Там были также раскрыты два ключа к нему: один из тех, что уже знал Кривош-Неманич, а другой особый. Дешифрованные японские телеграммы французы пересылали в Россию. Таким образом, неизвестным для дешифровальщиков России и Франции оставался один ключ. В этой ситуации Министерство иностранных дел командировало Кривоша-Неманича в Париж для совместной работы с французами. Французы приняли российского криптографа, снабженного соответствующими бумагами, как своего человека и ввели его в святая святых своей секретной службы — в «Surete generale», где он и проработал около десяти дней, пока не был открыт пятый способ применения японского кода. Кривош-Неманич был первым русским криптографом, подробно познакомившимся с работой дешифровальной службы Франции того времени. Эти сведения были, безусловно, с успехом русскими использованы, а многие полезные вещи внедрены в практику.

Из архивных документов видно, что дешифровальщики-аналитики МИД России работали успеш-

но и накануне, и в первый год Первой мировой войны. В 1913—1914 гг. они раскрыли 2 939 телеграмм из переписки государств из коалиции противника, в том числе: австрийских — 569, германских — 171, болгарских — 246, турецких — 181.

Дешифровальщики всегда работали в тесном контакте с разведкой, одна из важнейших задач которой была выкрасть код, сфотографировать его, естественно, положив затем на место, дабы не скомпрометировать Ставилась и более трудная, но и более эффективная задача — внедрить агента в среду противника, имеющую доступ к шифрам и кодам Эта сторона работы разведки описана в литературе достаточно подробно.

Большим подспорьем для раскрытия шифров и кодов являлись полученные агентурным путем открытые тексты, которые можно было привязать к соответствующим шифрованным сообщениям. Для кодов, например, это сразу давало достаточное число раскрытых кодовых групп, после чего значительно облегчалась работа по дешифрованию других сообщений. Зачастую коды просто-напросто покупались и продавались. Европейским центром такой деятельности разведок того времени была Вена — сердце балканских государств, где сталкивались интересы многих стран. В Вене производились всевозможные сделки по покупке и продаже копий секретных документов, писем, карт, кодов, планов, чертежей и т. п. Там Германия агентурным путем приобрела английский военно-морской шифр, Австро-Венгрия получила итальянский шифр.

Известна история вербовки русской разведкой начальника отдела австрийской разведки и контрразведки полковника Альфреда Редля. Еще в 1902 г. он за большую сумму продал России копию единственного военного словарного кода Австрии, равно как и австрийские планы ведения войны на Восточном фронте. Несмотря на то, что Редль был разоблачен

еще за два года до начала войны, австрийская армия потерпела поражение в Галиции в самом начале войны с Россией [17].

В конце XIX — начале XX века Россия активно использовала возможности подкупа иностранцев, имевших доступ к шифрам, кодам, шифрованной переписке. Особо важная корреспонденция иностранных дипломатов не отправлялась по почте, а обычно упаковывалась в специальные портфели с секретными замками и отправлялась к месту назначения с особыми курьерами. В результате она не попадала в «черный кабинет» и не могла быть перлюстрирована обычным образом. Однако из этого положения разведчики выходили с легкостью, обычно пуская в ход презренный металл. Как свидетельствует Майский, не было случая, чтобы золото не открывало замок портфеля и не давало возможность всего за несколько минут взглянуть глазом объектива фотоаппарата на содержание тщательно запечатанных вложений портфеля. В этих делах все сводилось только к тому, во сколько червонцев обойдется вся эта манипуляция.

Здесь кстати будет заметить, что все или почти все эти курьеры, фельдъегери, служители и прочие были подкуплены. За весьма небольшую мзду, выплачиваемую им помесячно или поштучно, они приносили в указанное место не только все содержимое корзины у письменного стола своих господ, но и копировальные книги из канцелярий, черновики их писаний, подлинники получаемых писем и официальных донесений и даже целые коды и шифровальные ключи. Для достижения этого им приходилось брать у спящего хозяина ключи от письменного стола или от несгораемого шкафа, снимать с них отпечаток из воска и заказывать дубликаты ключей или пускать ночью в канцелярию посольства таких лиц, которые могли бы выбрать то, что было нужно. «Поражаться надо было доверию некоторых послов к своим лаке-

ям, которые продавали их за гроши. Однажды произошел такой случай: вместо одного посла великой державы был назначен другой, который должен был с собой привезти весь новый штат служащих, так как прежний посол старым своим слугам не доверял, но в письме к новому послу он очень ходатайствовал за одного, по его выражению, «незаменимого» человека, своего выездного лакея, т. е. именно за то лицо, которое за незначительное месячное вознаграждение доставало из посольства все, что было угодно», — писал Майский.

Майский же указывает, что Россией коды, кроме Брюсселя, приобретались в Париже и Вене, где известные лица производили открытую торговлю иностранными кодами за определенную цену (совершенно тождественную в обоих упомянутых городах). При этом коды, представляющие меньший интерес, например греческий, болгарский или испанский, которые и достать было легче, ценились дешевле — тысячи в полторы-две, а такие коды, как германский, японский или Северо-Американских Штатов, стоили по несколько десятков тысяч; цены же шифрдокументов остальных стран колебались между 5 и 15 тысячами. Этим торговцам кодами можно было давать заказы достать тот или иной новый код, и они выполняли все заказы в весьма непродолжительные сроки [18].

Глава одиннадцатая

КРИПТОГРАФИЯ И ПОЛИЦИЯ

«Господину Соколову...»

В дополнение к действовавшим «черным кабинетам», занимавшимся перлюстрацией дипломатической корреспонденции, в связи с ростом революционного движения в России в 80-х годах XIX в. в стране было учреждено семь перлюстрационных пунктов для перехвата переписки российских граждан: в Петербурге, Москве, Киеве, Харькове, Одессе, Тифлисе, Варшаве. Позже такие пункты открылись в Вильно, Риге, Томске, Нижнем Новгороде, Казани. Однако последние действовали короткое время. В Тифлисе перлюстрационный пункт действовал с перерывом (1905—1909 гг.), т. к. был разгромлен во время революционных событий 1905 г.

Эти перлюстрационные пункты создавались на почтамтах при отделах цензуры иностранных газет и журналов. Официально они назывались «секретными отделениями». Общее руководство всей перлюстрационной работой в России возлагалось на старшего цензора Петербургского почтамта, который был наделен правами помощника начальника Главного управления почт и телеграфов и в то же время находился в подчинении министра внутренних дел, от которого получал распоряжения и санкции на про-

ведение перлюстрации. Более 30 лет, до ухода в отставку в 1914 г., эту должность исполнял действительный тайный советник Фомин, затем до октября 1917 г. — тайный советник Мордарьев. Перлюстрированные материалы из секретных отделений направлялись в Департамент полиции для расшифрования, в случае необходимости, а также дальнейшего использования. Старший цензор переписывался с Департаментом полиции под псевдонимом. Направляемые ему письма шли на имя «его превосходительства С. В. Соколова», что означало, что переписка предназначается для отдела цензуры [1].

Перлюстрирование писем было действием незаконным, оно шло вразрез с Уложением о наказаниях, предусматривающим кару за нарушение почтового Устава. Поэтому работа по перлюстрации держалась в строгом секрете. Никаких циркуляров по ведению этой работы издано не было. Существовало негласное распоряжение об уничтожении всей переписки и всех материалов перлюстрационных пунктов в случае народных волнений. Этим объясняется то, что множество документов погибло в 1905 г. и почти все материалы были уничтожены во время Февральской революции 1917 г.

Особенно тщательно подбирались служащие «черных кабинетов». Как правило, это были всесторонне проверенные люди, «безоговорочно преданные престолу», давшие подписку о неразглашении тайны. Среди сотрудников перлюстрационного пункта в Петербурге были люди, кроме цензуры служившие в других учреждениях: МИД, банке, университете и др., т. е. сохранялась традиция, заведенная еще в середине XVIII в. Непосредственно перлюстрацией по всей России занимались всего 40—50 человек, которым помогали работники почт, отбиравшие письма. В места, где перлюстрационные пункты отсутствовали, в случае необходимости командировались чиновники из центрального пункта в Петербурге. Но чаще

губернские жандармские управления привлекали к этой работе узкий круг местных почтовых чиновников и проводили перлюстрацию сами.

Работа в «черных кабинетах» была организована следующим образом. Письма для вскрытия отбирались по двум спискам. Первый список Особого отдела Департамента полиции содержал фамилии лиц, письма которых подлежали просмотру, и адреса, посланные по которым письма подлежали перлюстрации. Также должны были перлюстрироваться письма, освещающие деятельность съездов, партконференций противоправительственных организаций, содержащие материалы об их подготовке, проведении, деятельности основного партийного состава и членов различных организаций. Второй список составлялся Министерством внутренних дел и предписывал перлюстрацию писем общественных и политических деятелей, редакторов газет и журналов, профессоров, членов Государственного совета и Государственной думы, членов царской фамилии. Не подлежали перлюстрации письма только самого министра внутренних дел и царя. В материалах чрезвычайной следственной комиссии Временного правительства, разбиравшей в 1917 г. вопрос о перлюстрации, имеются данные о том, что в 1910 г. командир Отдельного корпуса жандармов П. Курлов обратился к старшему цензору с просьбой, чтобы адресованные ему письма не носили явных следов вскрытия. Такая же просьба высказывалась поборником перлюстрации директором Департамента полиции С. П. Белецким [2].

Степан Петрович Белецкий вместе со Столыпиным служил в Гродно, затем был вице-губернатором в Самаре. В 1909 г. Столыпин лично встречал вызванного им в столицу С. П. Белецкого. Премьер знал, что делает. Вот характеристика, данная Белецкому одним из его сослуживцев: «В этом чиновнике скрывалась потрясающая, именно полицейская, память на мелочи. Умный. Бескультурный. Вышел из низов.

Лбом пробил дорогу. Короткие пальцы. Желтые ногти. Чувствителен к взглядам: посмотришь на руку — прячет ее в карман, глянешь на ногу — убирает ее под стул. Нос пипочкой, глаза влажные, словно вот-вот пустит слезу. На пальце колечко — узенькое. Чадолюбив, с хохлацким акцентом: „телехрамма", „хазеты", „ханспирация" ...» Столыпину был нужен свой человек в МВД. Так С. П. Белецкий появился в знаменитом здании Департамента полиции на набережной реки Фонтанки; был назначен вице-директором этого департамента.

По сведениям за 1904 г., в списке Особого отдела Департамента полиции значилась одна тысяча адресов, за которыми велось наблюдение.

Самый большой поток писем шел через Петербургский почтамт. Ежедневно здесь вскрывалось от двух до трех тысяч писем. Конверты вскрывались особыми косточками или длинными иглами, отпаривались, отмачивались в ванночках. Письма с «интересными» сведениями откладывались для снятия копий. Просмотренные письма запечатывались, на обратной стороне в одном из уголков ставилась точка (мушка) — условный знак, свидетельствовавший о том, что письмо уже просмотрено и чтобы оно не было подвергнуто перлюстрации вторично. В «черном кабинете» письма задерживали недолго — всего час или два. Лишь в тех случаях, если их текст был написан симпатическими чернилами или зашифрован, их в подлиннике отправляли в Департамент полиции, где и подвергали соответствующей обработке. Копии и выписки из писем делали в двух экземплярах. Один экземпляр по списку Департамента полиции отправляли директору этого департамента, а второй (и оба экземпляра по списку Министерства внутренних дел) шел министру внутренних дел. На местах, в других городах, перлюстрировалась только та корреспонденция, которая шла из этого города или в город, но не транзитная. Копии также

делались в двух экземплярах, один из них направлялся в Петербург на имя Соколова.

С местными властями перлюстрационные пункты контактов не имели. Однако, когда в письмах попадались указания на то, что готовится какое-либо политическое событие, забастовка, экспроприация и т. д., выписка посылалась местному градоначальнику. В Московском отделении цензуры в таком случае выписку заклеивали в конверт, делали надпись «Анненкову» и опускали конверт в коммерческий ящик для градоначальства на почтамте. Фамилия «Анненков» была также псевдонимом.

По данным Департамента полиции, ежегодно по всей стране подвергалось перлюстрации приблизительно 380 тысяч писем, из которых делалось от 8 до 10 тысяч выписок. По более точным подсчетам, за 1907—1914 гг. наибольшее количество выписок падает на 1907 г. (11 522), а затем идет спад до 7935 в 1910 г. В 1911 г. поток вновь возрастает до 8658, а в 1912 г. до 10 тысяч. Одновременно возрастает количество шифрованных писем и писем, написанных химическими (т. е. симпатическими) чернилами.

Из некоторых источников известно, как относился к перлюстрации внутренней переписки Николай II. Когда какое-либо письмо представляло собой исключительный интерес, то кроме отправления выписки из него по назначению — министру внутренних дел, начальнику Генерального штаба или в Департамент полиции, — дубликат ее представлялся царю, а иногда, смотря по содержанию письма, выписка представлялась только ему одному. С этой целью такие выписки, чисто напечатанные на пишущей машинке и в особом большом конверте с напечатанным на нем адресом царя относились одним из секретных чиновников, пользовавшихся исключительным доверием царя, лицу, служившему и жившему во дворце и имевшему без особого доклада доступ к царю. Через это же лицо царь передавал приказания следить

за перепиской кого-нибудь из его приближенных или даже членов царской фамилии, подозреваемых им в каких-либо неблаговидных поступках. Так, благодаря перлюстрации, по сличению почерков удалось узнать фамилию лица, сообщавшего за границу разные нежелательные, с точки зрения придворной этики, сведения, или имя автора анонимно изданной в Лондоне на английском языке книги с изложением тайн царского двора, каковым оказался пользовавшийся особым расположением Николая II барон.

Когда великий князь Михаил Александрович, увлеченный красотой дочери предводителя дворянства одной из южнорусских губерний, серьезно подумывал о браке с ней, то царем было приказано снимать фотографии с переписки любовной четы и дешифровать детски наивный шифр, которым они думали скрыть свои планы на будущее. Благодаря перлюстрации их намерение уехать в Англию, чтобы там обвенчаться, было расстроено.

Отношение царя к перлюстрации было весьма своеобразным. Он ею, по-видимому, очень интересовался, так как, когда дней восемь — десять не получал конверта с выписками, то спрашивал, почему ему ничего не присылают. Когда же получал хорошо ему знакомый по внешнему виду конверт, то, по свидетельству Майского, оставлял дело, которым занимался, сам вскрывал конверт и принимался тотчас же за чтение выписок. Несмотря на это, обычно он не принимал никаких мер, согласно данным, черпаемым из выписок. Так, например, он не удалил от себя барона — автора английской книги о тайнах дворца, и ничем не дал понять лицу, сообщавшему за границу нежелательные сведения, что он осведомлен о его неблагонадежности. То же замечалось и тогда, когда деятельность какого-нибудь министра критиковалась всеми и в письмах прямо приводились не только его промахи, но и злоупотребления, превышение власти, лихоимство или просто преступ-

ления. Царь все это читал, иногда приказывал «привести более точные и подробные данные», а любимец-министр продолжал себе благодушествовать на своем посту и набивать карманы, пока совсем не оскандалился. Заметим, что ст. 1104 действовавшего Уложения о наказаниях предусматривала отстранение почтового служащего от должности за распечатывание письма «хотя из одного только любопытства», а «если содержание письма будет сообщено другому», то предусматривалось заключение в тюрьму на срок от четырех до восьми месяцев. Согласно ст. 1102, если почтовый чиновник «из-за каких-либо видов согласится с кем-либо передавать ему письма, адресованные на имя другого лица без позволения последнего», то он приговаривался к тюремному заключению или ссылке на поселение [3].

Насколько Николай II интересовался деятельностью «черного кабинета» видно из того, что он однажды собственноручно отобрал три золотых и серебряных с гербами и бриллиантами портсигара в качестве царских подарков и передал их секретному чиновнику для раздачи сослуживцам в виде поощрения за полезную деятельность. В этом отношении император Николай II резко отличался от своего отца императора Александра III, который, когда ему доложили вскоре после его воцарения о «секретной экспедиции» и объяснили ее назначение, ответил: «Мне этого не нужно» и в течение всего своего царствования отказывался читать выписки из писем, добытые перлюстрацией, хотя несколько министров делали попытки заинтересовать его этим [4].

Криптографическая служба Департамента полиции

Дешифровальная служба в Департаменте полиции работала все активнее. И связано это было прежде всего с ростом революционного движения в стране.

А рассматривать историю революционного движения всегда следует параллельно с изучением истории сопутствующего ей политического сыска. Впервые эта мысль была высказана М. А. Осоргиным — членом комиссии Временного правительства по спасению архивов московской охранки [5]. С ним нельзя не согласиться. В этой связи особый интерес представляют исторические источники, раскрывающие деятельность главного органа политического сыска царской России в конце XIX—начале XX в. — Департамента полиции (ДП).

Создан ДП был в 1880 г. как орган, не только руководящий розыскными действиями императорской исполнительной политической полиции, но, главным образом, как учреждение, призванное стоять на страже охраны существовавшего государственного строя, с которым и боролись с нарастающей силой все революционные партии и группы. На первых порах, когда только еще происходило становление ДП, его возглавлял В. Ф. Медников. Уровень подготовки сотрудников в тот период был весьма низкий. Достаточно сказать, что во главе политического отдела стояли люди, бывшие до того в филерских отрядах. Однако обострявшаяся политическая ситуация в стране привела к необходимости совершенствовать работу ДП. Уже в 90-е годы XIX в., когда его директором был назначен Степан Петрович Белецкий, начинает активно изменяться кадровый состав сотрудников этого органа, углубляется и совершенствуется его работа. В 1900-х годах уже девять из десяти служащих ДП были людьми с высшим образованием и в большинстве случаев с практическим служебным стажем. Белецкий чрезвычайно заботился о всестороннем развитии своих сотрудников, расширении их кругозора, углублении знаний. Так, все, что было нового в подпольной прессе и на русском и заграничном книжном рынке из области социальных вопросов, все выписывалось ДП, переводилось, чита-

лось, посылалось в форме ежемесячников розыскным офицерам. Всякие сведения, даже личного свойства, касавшиеся того или иного видного деятеля политической оппозиции, принимались Белецким во внимание при обсуждении планов борьбы с различными революционными партиями и группами.

О наиболее интересных для наблюдения лицах в охранных отделениях ДП велся особый дневник — «Сводка данных наружного наблюдения», иногда с приложением списка лиц, «выясненных наружным наблюдением». В дневнике имелись графы: «кличка», «установка», «местожительство», «от кого взят», «с кем виделся», «куда заходил», «кто его посетил и когда». Наружное наблюдение, как известно, велось «филерами», которых следует отличать от «секретных сотрудников». Филер — это простой «шпик», гороховое пальто (несколько выше по типу был филер разъездной и заграничный). Все сведения, полученные с помощью наружного наблюдения, тщательно записывались, попавшие в поле зрения ДП лица выяснялись («устанавливались») и в заключение составлялась чрезвычайно любопытная справка, которая прилагалась к каждому дневнику. Имея такую справку — «картограмму», заведующему секретной агентурой достаточно было ввести в круг интересовавших его лиц одного «сотрудника», чтобы превратить наблюдение наружное в наблюдение внутреннее. Картограмма как бы одухотворялась внутренним светом, и интересующее полицию лицо начинало фигурировать на бланках и карточках отдела внутренней агентуры. Все сказанное этим лицом завтра же делалось известным, поступки — записанными, письма — прочитанными, жизнь — изученной. Осоргин пишет: «Вы окутывали себя вуалем конспирации, вы шептали свою тайну на ухо ближайшему другу, вы переписывались своим шифром по условному безопаснейшему адресу, и днем позже ваш шепот переписывался на машинке, ваш шифр

подшивался к делу, а почтовое ведомство посылало в агентурный отдел письма на условный адрес. Ибо даже тяжелый и долгий революционный опыт не выкуривал из нас излишней доверчивости... Есть весьма видные и искренние революционные деятели, круг ближайших соратников и друзей которых состоял на 50—75% из провокаторов. Это может быть подтверждено документами, совершенно неопровержимыми» [6].

Наибольший урон революционному движению наносили агенты ДП, занимавшие в революционных партиях ответственные посты. В среде социал-демократии работали такие крупные агенты, как член ЦК РСДРП(б), глава большевистской фракции IV Государственной думы Р. В. Малиновский (агентурная кличка «Икс»), член Московского областного бюро ЦК РСДРП(б) А. С. Романов (агентурная кличка «Пелагея»), член Московского комитета РСДРП(б) А. И. Лобов (агентурная кличка «Мек») и многие другие. В других партиях также, естественно, работали агенты ДП. Уровень агентурной работы ДП в начале XX в. был весьма высок. Задачи, которые ставились перед агентами, были чрезвычайно сложными, доступными для решения людям с широчайшей эрудицией. Руководство ДП в борьбе с политическим противником выступало на равных, ведя свою «игру» на высочайшем уровне. Задачи такого типа, как внедрение в какую-то среду, отслеживание событий, отчет о них и о деятельности отдельных лиц, считались наиболее простыми. Основные задачи были гораздо интереснее и тоньше. Частично о них рассказал в своих показаниях допрошенный в качестве одного из основных свидетелей по делу Р. Малиновского в 1918 г. сам С. П. Белецкий. Из этих показаний следует, что перед агентурой ДП ставилась задача влиять на политику, проводимую той или иной партией, на принимаемые решения. Одним из примеров такого влияния является раскол между

большевиками и меньшевиками в 1914 г., которого упорно добивался Белецкий. Сам он так описывает это:

«Делая Малиновского не сотрудником Охранного отделения, а Департамента полиции, не только органа руководительного розыскными действиями имперской исполнительной политической полиции, но главным образом учреждения, призванного стоять на страже охранения существовавшего в то время государственного строя, с которым боролась социал-демократия, я лагерь своих политических противников изучал всесторонне... Изучая с одинаковым вниманием как большевистское, так и меньшевистское течение того времени, я большевиков в ту пору, взятых в отдельности, или, лучше сказать, в своей обособленности, не так опасался, чтобы предполагать в лице их одних наличность достаточных в то время сил и средств для нанесения серьезного удара правительственному строю. Для меня более серьезную опасность в ту пору представляли меньшевики, которые обдуманно, не порывисто, сознательно и постепенно шли к намеченной ими цели, нанося незаметные, но мне ощутительные удары; в это время намечалось со стороны меньшевистской партии стремление, путем уступок, идти на реальное полное слияние с большевиками, и я понимал, насколько такая соединенная и сплоченная сила была опасна существовавшему строю с точки зрения будущего; поэтому этого соединения я не должен был допустить и, взвешивая тот лагерь, в который я должен был проникнуть для осуществления своих планов, я пошел в сторону наименьшего сопротивления, считаясь со многими, выгодно для меня складывавшимися условиями, в том числе и с личностью партийного вождя г. Ленина, который при своем большом уме, партийной убежденности, фанатической ненависти к самодержавному режиму все-таки был догматик, больше знал австрийскую, чем русскую действительную жизнь и не имел в

*самом себе качеств борца-руководителя. Давая ему Малиновского, который мог и умел, в силу особенностей своей натуры и своих качеств, своим видимым энтузиазмом и энергией не только внушить к себе доверие, но, я бы сказал, загипнотизировать Ленина, я рассчитывал сделать Ленина горячим сторонником идеи раскола с меньшевиками, то есть того, что мне в ту пору реально необходимо было достигнуть. Мне преследование и достижение в конце концов намеченной цели стоило больших напряжений и сил. Прежде всего, мне надо было потратить много усилий, чтобы самого Малиновского, по своей натуре склонного к позировке и самоуверенности, сдерживать, заставить серьезно проникнуться моими намерениями, так как, оставляя в стороне Ленина, вполне в Малиновского уверовавшего, я должен был считаться с окружающими Ленина лицами, с его женою, г. Крупской, с г. Родомысльским (*Г. Зиновьевым. — *Т. С.), имевшим, с моей точки зрения, тяготение к меньшевикам, и с Трояновским и его подозрительно ко всему относившейся женою г. Розмирович... Затем мне надо было изучить социал-демократическую думскую фракцию в целом в числе новых лиц, до сего в нее не входивших, повести там через Малиновского борьбу, и, наконец, мне все-таки необходимо было и не дать возможности идее большевизма разрастаться, что было для меня затруднительно при наличии Малиновского как одного из видных вожаков ее в России, и только то, что он одновременно был моим сотрудником, облегчало меня. Достиг ли я своей цели, — это видно из того, что за мой период управления Департаментом полиции Ленин и его сторонники в Государственной думе не только не пошли на слияние с меньшевиками — членами Государственной думы, несмотря на сильный напор последних, но даже образовали вошедшую в разговорный обиход «шестерку», а Ленин вместе с командированным мною за границу Малиновским, доведенным даже до председателя фракции, осенью 1913 г., совершая турне по*

Европе, судя по имеющимся в Департаменте донесениям заграничной агентуры, окружавшей их сотрудниками и филерским наблюдением, оба были горячими проповедниками полной изоляции большевиков от меньшевиков» [7].

Шифры, которые использовали в своей переписке члены революционных организаций, представляли для полиции особый интерес. Поэтому в число задач, которые ставились перед агентами, входила и добыча шифров и ключей к шифрам. Вот выдержка из докладной директору ДП, представленной начальником отделения «по охранению общественной безопасности и порядка» в Петербурге 12 ноября 1903 г.:

«Вся конспиративная переписка партии эсеров шифруется при помощи известного календаря Гатцука, издаваемого в Киеве. Упомянутый комитет пользуется адресом: Москва, Лубянка, Варсонофьевский пер., д. Рябушинских, Дмитрию Ксенофонтовичу Тихомирову.

Ключом к переписке с Москвой и Харьковом служит имя «Николай», с Екатеринославом — «Огюст Кант», а заграничная переписка шифруется по 8-й книге за август сего г. журнала «Мир Божий». 2-му отделению при дешифровании заграничной переписки следует к проставленной на письме дате прибавить число 13, т. е. разницу между старым и новым стилем, и полученное число укажет ту страницу в указанной книге, с которой начата шифровка» [8].

Некоторые сведения о шифрах революционеров, добытых агентурным путем, дают журналы входящих документов ДП за 1906—1908 гг. и 1909—1915 гг. [9]. Так, например, в 1906 г. ДП была агентурным путем получена и затем дешифрована шифрованная переписка известных меньшевиков Степана Цосаря, Петра Кирноса, Леонида Комендантова, М. Мандельштама; из Донского охранного отделения сюда же при-

слали ключ к шифрпереписке комитетов РСДРП(б) с ЦК, а также ключ к шифру большевика М. Покровского.

В 1907 г. ДП получена и дешифрована переписка большевика Николая Буренина, получен ключ к шифру ЦК РСДРП(б) для переписки с Киевской организацией, ключи к шифрам социал-демократов Южного района.

В 1908 г. по агентурному доносу был захвачен шифрованный архив Московской военной организации РСДРП(б). Но в журналах имеется запись: «Разобрать невозможно». Однако нам известно, что всего за три года до этого при разгроме полицией редакции газеты «Новая жизнь» в числе прочих документов была захвачена записная книжка с шифрованными записями, которые были дешифрованы весьма легко и быстро.

В том же 1908 г. одесская охранка прислала в ДП ключ к шифру ЦК РСДРП(б), были также получены шифры «Рабочая азбука», «Бородино», ключи к шифрам местных организаций РСДРП(б), например Полтавской, и др. Подробнее о шифрах подполья мы расскажем в следующей главе.

В 1909 г. через агентуру ДП получен ключ к шифру политических арестованных, содержавшихся в кутаисской тюрьме, получена и дешифрована переписка известного большевика — химика Александра Чесского из Самары, из Харькова получен ключ к шифру «Грунке», «коим пользуются организации РСДРП» [10]. Из Екатеринославского охранного отделения сообщили ключ к шифру РСДРП(б) (книжка «Смерть» № 70), из Иркутска поступил ключ к шифрам арестантов иркутского тюремного замка. Начальник одесского охранного отделения со сводкой агентурных сведений по городу Керчи сообщает ключ к шифру социал-демократического подполья (сборник «Знание» № 17). Московскому охранному отделению удалось получить ключ к

шифру ЦК РСДРП(б) для переписки с Петербургским комитетом. Начальник самарского губернского жандармского управления сообщил ключ к шифру, использовавшемуся в переписке саратовской и уральской социал-демократических организаций. В этом же году ДП получил ключи к шифрам для переписки крымской организации с ЦК РСДРП(б), ключи к шифрам пермской организации РСДРП(б), ключи к шифрпереписке Московского комитета с ЦК РСДРП(б).

В 1911 г. ДП получил и дешифровал переписку Якова Свердлова и его жены К. Т. Новгородцевой, секретаря ЦК РСДРП(б) Нины Агаджановой, агента ЦК по центральному промышленному району В. Яковлевой и В. Куйбышева, Г. Пятакова. Были также получены ключи к шифрам социал-демократии Латышского края, шифр для переписки В. Ленина с В. Бажановым, Е. Розмирович, копии шифров Н. Крупской, Г. Петровского и др.

В Департаменте полиции, куда поступали материалы из «черных кабинетов» и иногда от министра внутренних дел, шла дальнейшая «разработка» перлюстрации: регистрация, расшифровка, проявление химических текстов, копирование, размножение копий. На основании полученных сведений велась переписка с губернскими жандармскими управлениями, выяснялись личности писавших, адреса, «принимались меры». Каждое перехваченное письмо получало свой номер. Простые и «химические» письма регистрировались раздельно: первые просто получали номер, к химическим прибавлялась буква «Х». Фамилии, упоминаемые в письмах, заносились в картотечный алфавит. Именные карточки составлялись на автора письма, получателя, на все имена и фамилии, упоминаемые в письме. Так подробно расписывались только письма революционеров. Письма государственных и общественных деятелей редко проходили такую обработку. Они, как правило, не регистри-

ровались, подшивались в отдельные дела в порядке хронологии. К тому же от министра внутренних дел порой перлюстрация в ДП вообще не поступала по каким-то причинам.

В ДП вся перлюстрация сосредоточивалась в 5-м отделении Особого отдела ДП, где шла разработка материалов по партиям. Копии писем, касавшихся деятельности партий эсеров, анархистов, террористических организаций, шли во 2-е отделение Особого отдела, которое занималось этими партиями; материалы по социал-демократическим организациям шли в 3-е отделение, национальных организаций — в 4-е. Здесь же шла дальнейшая разработка этой переписки, но уже розыскного характера, на основании сведений, получаемых из писем. Это была кропотливая и сложная работа, требующая глубокого знания революционного подполья. Изучая впоследствии этот механизм, член комиссии временного правительства по разработке материалов охранных отделений М. А. Осоргин писал, что при работе с перлюстрационным материалом устанавливались «не только адрес, но и каждое лицо, упомянутое в письме, иногда только уменьшительным именем, одной буквой или описательным выражением» [11].

Копии писем посылались в соответствующие охранные отделения и губернские жандармские управления для выявления лиц, принятия мер, установления наблюдения. Эти, уже вторичные, копии вместе с материалами по разработке и переписке с соответствующими губернскими жандармскими управлениями группировались в делах по наблюдению за партиями, организациями, отдельными лицами. По социал-демократическому движению эти документы концентрировались в делах по наблюдению за РСДРП(б) [12].

Прочтением тайнописной и шифрованной переписки революционных партий и групп занимались специальные сотрудники Особого отдела ДП, в част-

ности, его 2-го и 5-го отделений. Среди них, в первую очередь, следует отметить безусловно выдающегося криптографа Ивана Александровича Зыбина. И. А. Зыбин поступил на службу в ДП в середине 90-х годов XIX в. и уже в 1901—1902 гг. стал ведущим дешифровальщиком этого ведомства, хотя официально он именовался «старшим помощником делопроизводителя». К концу своей службы в ДП (1916 г.) Зыбин официально стал именоваться «делопроизводителем». Работая в области дешифрования переписки революционного подполья, Зыбин естественно накопил огромный теоретический и практический опыт. Кроме того, являясь от природы личностью высокоодаренной, обладая прекрасной памятью, Зыбин был широко образован, что позволяло ему получать сведения о шифрах не чисто научно-аналитическим способом, но и с помощью косвенных сведений. Именно Зыбин ввел в практику чинов полиции, производивших арест или обыск революционеров, обычай тщательно искать среди имеющихся у них книг именно те, что могли бы представлять интерес для Зыбина-дешифровальщика.

Вот отрывок из его письма от 7 февраля 1910 г. начальнику саратовского губернского жандармского управления: «...отобранные по обыску у мещанина Николая Сергеевича Кузнецова записи зашифрованы 4, 15, 25, 29 и 35-й страницами какой-то неизвестной книги и разбору не поддаются по недостаточности материала. Прошу Ваше Высокоблагородие уведомить в самое непродолжительное время, не было ли обнаружено по обыску у названного Кузнецова, кроме означенных записей, какого-либо издания или легальной книги с пометками на отдельных страницах или загрязненной более других какой-либо страницей от частого, сравнительно с другими, употребления и, кроме того, не встретилось ли одно и то же издание у прочих лиц, принадлежащих к одной с Кузнецовым организации, т. к. подобное явление в

большинстве случаев указывает, что таковое издание служит ключом для шифрованных сношений» [13].

В 1903 г. в ДП разработкой поступающих химических, как их тогда называли, и шифрованных документов занимались четыре человека. Один из них — Владимиров — занимался разбором и переводом химических писем, прокламаций и т. п., написанных на еврейском языке. В. Н. Зверев, ротмистр Мец и И. А. Зыбин вели входящий и исходящий журналы документов, доставляемых цензурой, пополняли алфавит лиц и адресов, упоминавшихся в переписке, проявляли и воспроизводили документы, подлежащие отправке по назначению, вели переписку с цензурой. «...В первую очередь разбирались химические письма «Бунда», «Искры» и др. организаций, содержащие в себе адреса и явки, а затем уже документы, отбираемые при обысках и арестах» [14]. Ежегодно И. А. Зыбину выдавали 150 рублей «из секретных сумм» в возмещение расходов по постоянным поездкам в цензуру, так как письменных сношений с цензурой ДП избегал [15]. Прекрасно работал ученик и помощник Зыбина В. Н. Жабчинский, который в свое время окончил Петербургский университет. В одной из докладных Зыбин сообщает, что Жабчинский может разбирать шифры на любом языке [16].

В отделении Зыбина для проявления писем революционеров, написанных «химией», подбирали специальные вещества. Вот некоторые рецепты, приведенные в одной из докладных:

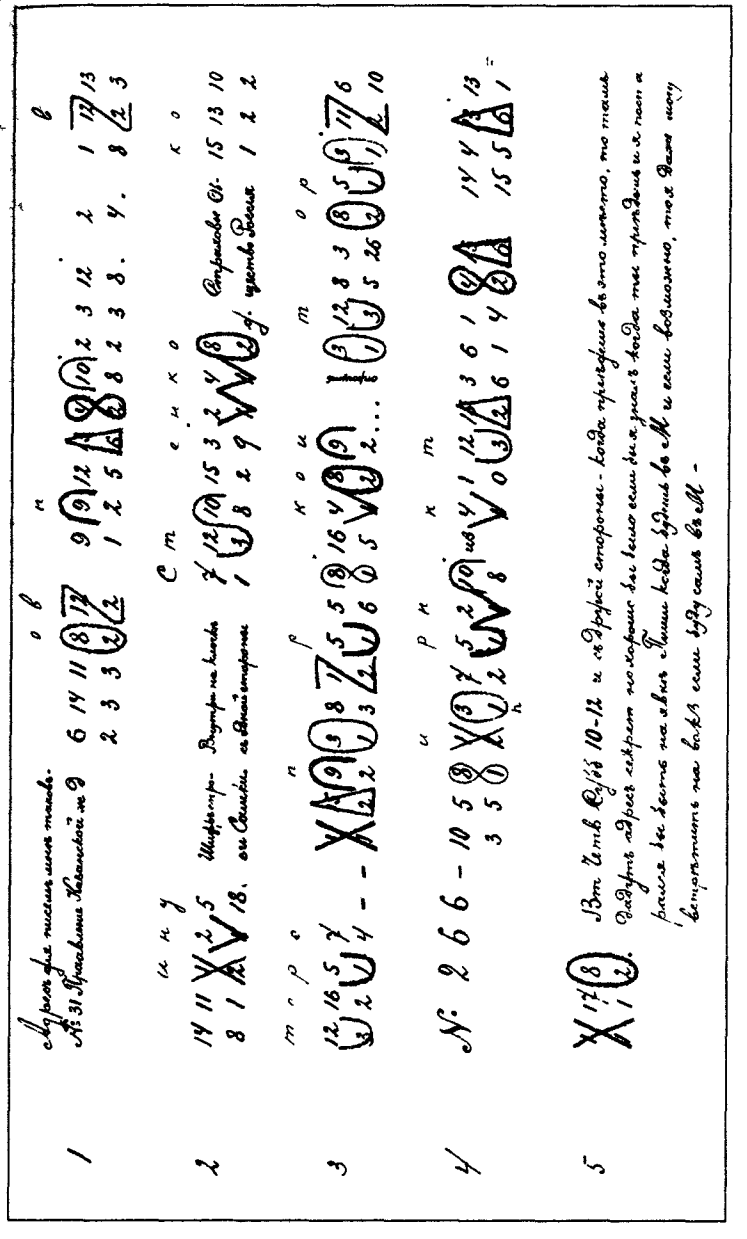
«1. Растворить азотнокислое серебро при подкуривании аммиаком и при освещении вольтовой дуги.

2. Раствором эскулина (флюоресцирующих мест не заметно при освещении вольтовой дуги).

3. 5% раствором ализариновых чернил (контроль — бумага с надписями чистой водой).

4. Раствором желтой кровяной соли (0,5%).

5. Раствором сернистого аммония (1%).



Страница рабочей тетради И А Зыбина

6. Раствором аммиака (1%).

7. Раствором красной кровяной соли с бромистым калием (1%).

Ввиду проб (1, 2, 3) пробы йодом, нагреванием и полуторахлористым железом как менее чувствительные и бесполезные применены не были» [17].

В ДП строго охраняли секреты, связанные с криптографией, фамилии сотрудников отделения И. А. Зыбина не разглашались. Так, например, в 1908 г. из уфимского окружного суда тогдашнему начальнику Особого отдела ДП Е. К. Климовичу были направлены шифрованная записка и ключ к шифру. В сопроводительном письме, подписанном судебным следователем, излагалась просьба расшифровать письмо, сообщить, какая подпольная организация пользуется таким шифром, и дать возможность допросить в качестве эксперта сотрудника ДП, который будет проводить эту работу. Через неделю в Уфу был направлен ответ. В нем сообщалось содержание записки, которую удалось расшифровать, давалась краткая характеристика шифра (достаточно распространенного). Однако ДП был категорически против допроса специалиста-криптографа.

Аналогичный случай был в 1915 г. На этот раз допросить криптографа пожелал судебный следователь из Витебского уезда. По приказу директора ДП Брюн-де-Сент Ипполита было направлено письмо самому прокурору Петроградской судебной палаты с просьбой одернуть провинциального следователя. В письме указывалось, что «...разоблачение произведшего дешифровку лица является для Департамента полиции по особым соображениям весьма неудобным» [18].

Отделение Зыбина проводило и экспертизу почерков. Так, например, в сентябре 1910 г. «старший помощник делопроизводителя, коллежский советник Зыбин и чиновник для письма ДП коллежский регистратор Жабчинский рассматривали фотоснимки

воззвания под заголовком «РСДРП», начинавшееся словами: «Товарищи! Тяжелое и безотрадное время...» и подписанное: «Орловская группа РСДРП», а также протокол допроса ротмистром Шульцем крестьянина Ивана Федоровича Курбатова». Был проведен подробный анализ почерка воззвания и почерка Курбатова и дано очень осторожное заключение «о схожести букв». Подобных свидетельств нами найдено в архивах несколько.

В своей работе Зыбин и его помощники отнюдь не были «слепыми» исполнителями руководящих указаний начальства. Они постоянно стремились совершенствовать дешифровальную службу ДП, неоднократно писали докладные записки о состоянии ее работы, выходили с предложениями.

Уже в своей докладной записке от 22 мая 1903 г. директору ДП Белецкому И. А. Зыбин писал, что разрабатывать шифрованные документы с каждым годом становится все труднее и труднее по ряду причин. Во-первых, как он мог наблюдать, за последние два года, то есть с 1901 по 1903 г., их количество стало «огромным», во-вторых, сравнительно легкие приемы шифрования текста, где ключом служит какое-нибудь слово или стихотворение, постепенно оставляются и «более опытные революционные деятели (группа «Искра» и др.) пользуются для переписки в настоящее время или двойными ключами, или страницами малоизвестных книг и брошюр, избирая для каждого отдельного корреспондента отдельную книгу и избегая повторения страниц, что крайне усложняет работу» [19]. Чтобы сделать свои поиски ключей более успешными, криптографы ДП стремились получить несколько писем из одного пункта.

Условия работы дешифровальщиков также не способствовали успеху. Из-за тесноты помещений и крайней скученности в них служащих химические тексты приходилось проявлять непосредственно в кабинете заведующего Особым отделом ДП, а наи-

более кропотливую работу с ними вообще проводить на дому. Дома же сотрудники разбирали и все шифрованные письма.

Еще в 1901 г. Зыбин направил докладную начальнику Особого отдела ДП Л. А. Ратаеву, в которой указывал на то, что резко начал возрастать поток шифрованных писем, получаемых при обысках и арестах. Вместе с тем, все эти письма, как правило, для дешифрования направлялись в ДП, так как в среде чинов жандармского корпуса своих специалистов по шифрам не было. Основы дешифрования преподавались только в Академии Генерального штаба. Что касается жандармских офицеров, для которых такие знания были также необходимы, то они их не получали В связи с этим Зыбин предлагал свои услуги для занятий с офицерами штаба Отдельного корпуса жандармов с целью ознакомить их с техникой разбора наиболее употребительных в революционном подполье шифров. Он считал, что для получения ими необходимых знаний достаточно посвящать этому два часа в неделю. Вместе с ними могли бы заниматься офицеры наиболее важных жандармских управлений и охранки. «И в скором времени можно̀ было бы достигнуть того, чтобы в каждом из наиболее важных жандармских управлений, а также в охранных отделениях имелись офицеры, «знакомые» с приемами дешифрования», — писал Зыбин [20].

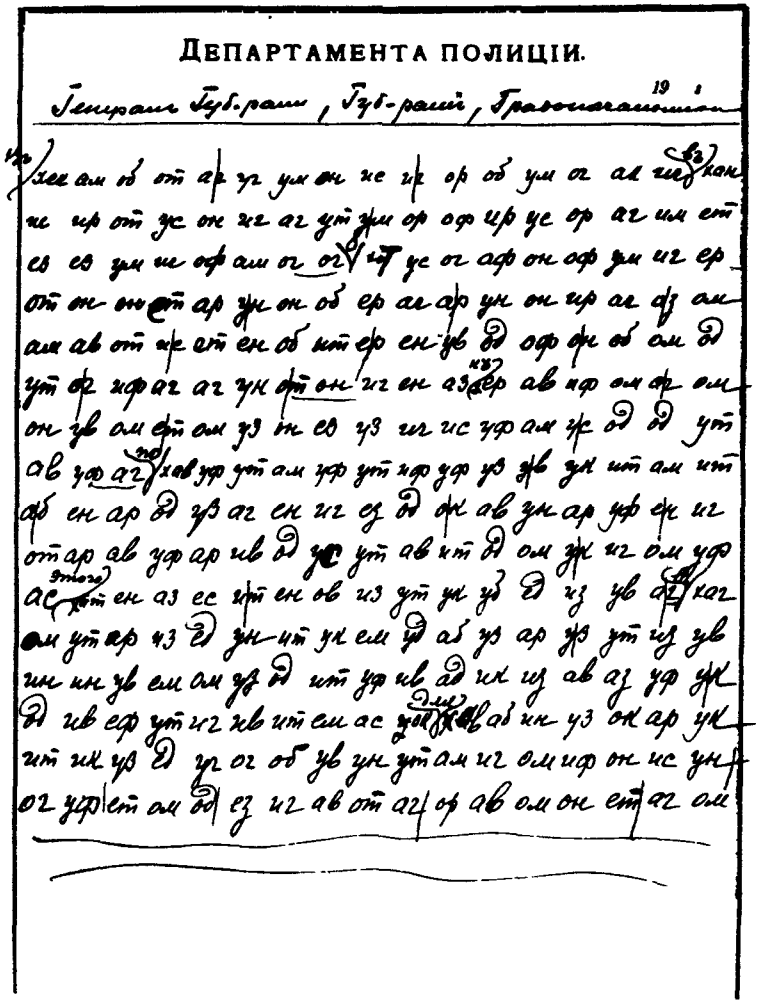
Такие занятия Ивану Александровичу разрешено было проводить. Одновременно с этим он стал преподавать основы дешифрования и для офицеров Главного военного штаба

Необходимость иметь у себя специалистов по дешифрованию испытывали и другие ведомства В июле 1915 г. проходил съезд управляющих кабинетами научно-судебной экспертизы при прокурорах судебных палат. На съезде внимание присутствующих было обращено на то, что этим кабинетам нередко

приходится иметь дело с расшифровкой документов. Не имея специальной литературы и соответствующих руководств, сотрудникам кабинетов самим приходилось изыскивать способы и приемы расшифрования. Съезд принял решение о временном командировании чинов кабинетов в Департамент полиции, МИД и Военное министерство для ознакомления с практиковавшимися приемами расшифрования, имея в виду, что в этих ведомствах накоплен по данному вопросу уже большой опыт. Однако само Министерство юстиции не торопилось выполнять решение съезда. Лишь через год, в июле 1916-го, было направлено письмо начальнику Особого отдела ДП Е. К. Климовичу с просьбой допустить сотрудника московского кабинета Русецкого на стажировку в ДП и ознакомить его с наиболее распространенными видами шифров и приемами их разбора. Такое разрешение было дано [21].

Именно И. А. Зыбину присылались на экспертизу и новые системы шифров, которые предполагалось использовать на внутренних линиях связи. Вот одно из сохранившихся сделанных им заключений, оно датировано 20 июля 1910 г.:

«Предлагаемая система шифрования с помощью двух вращающихся концентрических кругов является мало удобной, во-первых, потому, что по ней подлежащий зашифрованию текст предварительно пишется длинными 40-буквенными группами в две строки каждая, последнее возможно лишь в тех случаях, когда весь текст депеши шифруется сплошь, без всяких пропусков; во-вторых, обязательное отделение каждого слова от следующего за ним знаком препинания, причем последний всякий раз обозначается парою цифр, излишне удорожает шифр и др.; в-третьих, сама система концентрических кругов излишне громоздка и не достигает цели в смысле сохранения секрета депеши, так как при любом наложении кругов и при всяких комби-


ДЕПАРТАМЕНТА ПОЛИЦІИ.

Фрагмент шифртелеграммы ДП

нациях для обозначения каждой буквы и каждого знака препинания имеется лишь два числа — четное и нечетное. Например, буква А всегда будет обозначаться числом 37 или 28; буква Б — 39 или 20 и т. п., вследствие чего круги эти являются совершенно излишними; значения букв гораздо удобнее можно расположить в виде таблицы, как в Департаментском полицейском ключе, в котором, между прочим, для каждой буквы имеется от двух до четырех значений» [22].

Несмотря на многочисленные сигналы «снизу», исходившие отнюдь не только от рядовых сотрудников, но и от руководителей среднего уровня, криптографическая служба ДП тем не менее не подвергалась конструктивным изменениям в течение многих лет. А ведь время было совсем не простое, надвигалась политическая буря, и это хорошо понимали и Зыбин, и его коллеги. Чем обернулось непринятие необходимых мер по совершенствованию этой службы в скором времени, уже в годы Первой мировой войны, мы расскажем в дальнейшем.

Глава двенадцатая

ШИФРЫ ПОДПОЛЬЯ

Конспирация — прежде всего

В революционном подполье опыт использования шифров передавался из поколения в поколение. Уже члены организации «Народная воля» применяли так называемый «тюремный шифр» — вариант «шифра Полибия», — обошедший все тюрьмы и крепости, все остроги и централы. Творцом его считается декабрист Михаил Александрович Бестужев, находившийся в 1826 г в Алексеевском равелине Петропавловской крепости. В этом шифре буквы алфавита выписываются в квадрат 6×6 и заменяются биграммой, состоящей из номера строки и номера столбца соответствующей буквы. При перестукивании арестанты передавали буквы ударами, обозначавшими координаты буквы в таблице. Народовольцы стали пользоваться и книжным шифром, о котором речь пойдет ниже. Вообще конспирация и конспиративная переписка (тайнописью — «химией», шифром) были у революционеров в ранний период на достаточно высоком уровне. В какой-то мере ослабление внимания к конспиративным требованиям дало возможность полиции получить и дешифровать переписку народовольцев, в результате чего известная группа членов этой организации была арестована и

казнена после убийства царя Александра II 1 марта 1881 г.

С увеличением числа революционных организаций и количеством их членов в 90-е годы XIX в. произошло значительное снижение уровня конспирации. Длительное время не придавалось особого значения обучению членов революционных организаций конспиративным правилам и приемам. О них не писали, не говорили, не дебатировали. Предполагалось как бы, что конспиративные приемы даются от рождения или приобретаются с практикой. Следствием этого явились массовые систематические провалы. Это дало повод одному из лидеров «Бунда» Л. Розенталю (подпольный псевдоним «Бундовец») в своей книге «Шифрованное письмо», изданной в 1904 г. в Женеве, писать: «Если... мы обратимся к социал-демократическим организациям, то... рассматривая вопрос исключительно с точки зрения конспиративной ловкости и выдержки наших революционеров (имеются в виду российские революционеры всех партий и групп того времени вообще. — *Т. С.*), мы видим, что они не только стоят несравненно ниже деятелей Народной Воли, но почти не делают успехов из году в год» [1]

Еще в конце XIX в., несмотря на уже богатый опыт подпольной борьбы с самодержавием, российским революционерам суровые требования конспирации, осторожности, а главное, выдержки все еще казались невыполнимыми, стеснительными, тормозящими живое дело. Сплошь и рядом осторожность объявлялась трусостью, отсутствием настоящей революционности и товарищеских чувств.

Поистине замечательной была в русском революционере вера в шифры Более 99% писем, которыми обменивались революционеры, были шифрованными. Их отправляли почтой, доверяли им самые важные тайны. «Бундовец» пишет: «На чем основана наша вера в неразрешимость шифра? Что, если

мы ошибаемся? Если тайна, доверенная шифру, уже не тайна? Если мы все время пребываем в состоянии мистификации?..

Основываясь на случаях раскрытия писем бюро Департамента полиции и нашем личном опыте, мы не только ставим вышеприведенный вопрос о самообмане, но даем на него вполне определенный утвердительный ответ: да, мы, российские революционеры, в отношении шифров пребываем в состоянии вредного самообмана... И нам, и некоторым товарищам нашим приходилось иногда поневоле предпринимать попытки раскрывать письма без ключа. Это случалось тогда, когда корреспондент перепутывал ключ или, если в отсутствии товарища, обыкновенно ведшего переписку, получалось письмо из такого города, для которого тот позабыл сообщить ключ. И что же? Не было ни одного случая, когда бы шифр оставался неразобранным» [2].

Большое значение придавалось вопросам конспирации в рядах социал-демократии. Сохранение в тайне обширной партийной переписки, которая была не только одним из важных способов связи в нелегальных организациях, но служила и каналом идейного и организационного руководства, требовало соблюдения строжайшей дисциплины. В. И. Ленин лично предъявлял в этом отношении жесткие требования. От одного он требовал писать письма шифром или «химией», другого предупреждал: «Не пишите, пожалуйста, никаких инициалов в письмах — господь их знает, вполне ли здесь надежна почта», третьего предостерегал: «...не пишите прямо в письмах ничего... никто не должен знать, где и кем издано... Все черняки сжечь!». Он указывал: «Ни издания листовок, ни транспорта, ни спевки насчет прокламаций, ни посылки их проектов и пр. и пр. нельзя поставить без правильной конспиративной переписки. В этом гвоздь!»

В январе 1901 г. вышел первый номер «Искры», которой предстояло сыграть решающую роль в

образовании РСДРП. Е. Д. Стасова позднее вспоминала, с какой сложной, трудоемкой и кропотливой работой было связано ведение конспиративной переписки: «Прежде всего надо было подготовить текст письма и отметить для последующей шифровки наиболее конспиративные сведения. После этого на отдельном листке нужные места зашифровывались и тщательно проверялись, чтобы не было ошибок, которые чрезвычайно затрудняли дешифровку письма... Требовалось еще на каком-либо иностранном языке написать так называемое внешнее письмо, чтобы не вызвать малейших подозрений... И, наконец, за внешним письмом следовала последняя процедура — между строк явного письма различными химическими составами (химией) вписывалось конспиративное зашифрованное письмо». У «Искры» в России было, помимо комитетов и групп, около ста корреспондентов. В месяц секретарю редакции Н. К. Крупской приходилось так обрабатывать до 300 писем.

Еще в работе «Насущный вопрос», написанной в ссылке в 90-х годах, Ленин писал: «Против нас, против маленьких групп социалистов, ютящихся по широкому русскому «подполью», стоит гигантский механизм могущественного современного государства, напрягающего все силы, чтобы задавить социализм и демократию. Мы убеждены, что мы сломим в конце концов это полицейское государство, потому что за демократию и социализм стоят все здоровые и развивающиеся слои всего народа, но чтобы вести систематическую борьбу против правительства, мы должны довести революционную организацию, дисциплину и конспиративную технику до высшей степени совершенства» [3].

Как известно, «Искра» наряду с газетой и научно-политическим журналом «Заря» выпускала различные книги, брошюры и прокламации. За

три года было выпущено 56 таких изданий, в которых обобщался накопленный революционный опыт, содержались политические и экономические идеи. К числу этих изданий относится и брошюра Бахарева «О шифрах», изданная, как и книга «Бундовца», в Женеве, но несколько раньше, в 1902 г. В ней рассматривались некоторые шифры, применяемые революционерами, приводился их элементарный анализ и давались рекомендации по их использованию «чтобы,— как писал автор,— предостеречь от постоянно допускаемых ошибок». Помимо вопросов о шифрах в брошюре излагались способы «химической переписки» и «перестукивания в тюрьме».

Шифры российских революционеров

В период XIX — начала XX в. в российском революционном подполье применялись многочисленные и разнообразные шифры. Здесь мы приводим лишь те из них, которые имели наибольшее распространение. Названия шифров сохранены те, которые употреблялись в то время.

Единозначный парный шифр. Это шифр простой замены, который составлялся из случайной фразы, состоящей из 17 букв тогдашнего алфавита, например: «ЖЕЛЕЗНЫЙ ШПИЦЪ ДОМА». Оставшиеся 17 букв алфавита подписывались под этой фразой в алфавитном порядке:

Ж Е Л Е З Н Ы Й Ш П И Ц Ъ Д О М А

Б В Г Й К Р С Т У Ф Х Ч Щ Ь Э Ю Я

Каждая верхняя буква с лежащей под ней нижней составляли пару, в которой одна буква при шифровании взаимно замещалась другой.

Очевидно, что это весьма ненадежный шифр, что было известно, но удобный для запоминания. Поэтому применялся он лишь для очень кратких записей.

Непарный единозначный шифр. Если в единозначном шифре половина букв была связана с другой половиной, что, конечно, облегчало его раскрытие, то в данном шифре, бывшем столь же легким для запоминания, была сделана попытка ужесточить такую зависимость между буквенными знаками.

Составлялись две 17-буквенные фразы, например: 1) железный шпицъ дома и 2) цырюльникъ худощав. Дополнив каждую 17-буквенную фразу недостающими буквами, записывали их рядом с соответствующей фразой: в первом случае справа от нее, во втором — слева. Один ряд при этом писался под другим:

ЖЕЛЕЗНЫЙШПИЦЪДОМА БВГЙКРСТУФХЧЩЬЭЮЯ

Я ЭШИФТС ПМЙЗЖЬЕГБЪ ЦЫРЮЛЬНИКЪХУ ДОЩАВ

Каждый горизонтальный ряд включает в себя полную азбуку. Каждая буква нижнего ряда заменяет при шифровании верхнюю, и наоборот.

Непарный единозначный шифр также не имел широкого применения вследствие своей простоты для раскрытия.

Простой квадратный шифр. Запоминается лозунг, состоящий из десяти букв, например: ЭТА КОРОБКА. Затем составляется квадрат 10×10, лозунг записывается в первый столбец квадрата, далее, как это делается по шифру Виженера, по горизонталям таблицы записываются буквы в порядке алфавита. Лозунг придумывается таким образом, чтобы в таблице появились все буквы алфавита (это почти всегда достигается). Теперь каждая буква алфавита шифруется с помощью двузначных чисел — номеров строки столбца. Например, у нас слово «агент» может быть зашифровано так: 31, 17, 85, 94, 49.

1	2	3	4	5	6	7	8	9	0
1	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
3	А	Б	В	Г	Д	Е	Ж	З	И	Ъ
4	К	Л	М	Н	О	П	Р	С	Т	У
5	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
6	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
7	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
8	Б	В	Г	Д	Е	Ж	З	И	Ъ	Й
9	К	Л	М	Н	О	П	Р	С	Т	У
0	А	Ъ	В	Г	Д	Е	Ж	З	И	Й

Иногда берут квадрат большей величины за счет выбора более длинного лозунга. В этом случае каждая буква может заменяться четырехзначным числом, которое иногда писали в виде дроби.

Этот шифр имеет некоторые преимущества по сравнению с предыдущими. Он в некоторой степени нарушает статистические буквенные закономерности открытого текста. При умелом выборе ключа более часто встречающиеся буквы имели больше цифровых вариантов и т. д. Отметим, что, несмотря на очевидную ненадежность этого шифра, он очень активно использовался в революционном подполье.

Сложный квадратный шифр. Предыдущий шифр имел наряду с другими тот недостаток, что расположение букв в таблице примитивно: они просто идут в алфавитном порядке. Авторы сложного квадратного шифра стремились уничтожить именно этот недостаток. Достигалась эта цель при помощи введения распределителя (номерного ряда).

Возьмем слово из 10 букв: «КВАДРАТНЫЙ». Пронумеруем буквы в соответствии с их порядком в алфавите:

К	В	А	Д	Р	А	Т	Н	Ы	Й
6	3	1	4	8	2	9	7	0	5

Получим число, содержащее десять различных цифр (номерной ряд), оно-то и будет распределителем. С помощью этого номерного ряда переобозначались номера столбцов в простом квадратном шифре.

Нельзя отрицать, что сложный квадратный шифр представлял для своей разгадки в тот период значительные трудности. Но не было случая, чтобы даже сами революционеры не могли расшифровать зашифрованное этим шифром письмо. Что же говорить о специалистах из Департамента полиции. Отметим, что для образования этого шифра использовался номерной ряд. Поскольку об этом шифре «Бундовец» писал в 1904 г., то отсюда также следует, что понятие номерного ряда использовалось российскими революционерами по крайней мере уже в самом начале XX в.

Прерывистый квадратный шифр (с фиктивными цифрами). Система этого шифра та же, что и у двух предыдущих, с той лишь разницей, что, стремясь сбить с толку противника и сделать текст недоступным для расчленения на отдельные биграммы, его авторы ввели новый элемент — фиктивные цифры или пустышки.

Пусть дан ключ из восьми букв: «МОЯ ЩЕТКА» и условлено считать фиктивными цифрами, например, 4 и 7. Составляется квадрат 10×10, в котором 4-й и 7-й горизонтальные ряды, а также 4-й и 7-й столбцы оставляются пустыми. В остальных клетках развернут ключ по методу простого квадратного шифра. Сверху и слева ставится обычная нумерация. Таким образом в цифровых биграммах, соответствующих буквам, цифры 4 и 7 отсутствуют. Шифрование заключается в том, что при наборе, выбирая из таблицы нужные биграммы, пишущий время от времени вставляет между ними произвольные пустышки (четное или нечетное число фиктивных цифр). Тот же прием применим и к сложному квадратному шифру.

Несомненно, что прерывистый квадратный шифр не очень сложен. Тот плюс, который он дает своими «фиктивными» цифрами, был самообманом и легко выявлялся. Между тем количество действительных знаков в нем сильно уменьшено.

Множественный квадратный шифр. Вместо того, чтобы пользоваться одним ключом и одной таблицей квадратной системы, составляют их несколько, например две, три, четыре, и затем при шифровании берут знаки сначала из первой таблицы, потом из второй и т. д.; наконец возвращаются опять к первой и, таким образом, периодически обходят все ключи. Положим, например, что ключами служат слова: «ЭТА КОРОБКА», «НАЧАЛЬНИК», «АЛЕКСАНДР». По простой квадратной системе составляют три таблицы. Прежде, чем пользоваться этой системой, надо условиться о «переходе» с одного ключа на другой. Обычно это было какое-то короткое условное слово или двукратное или трехкратное повторение одной буквы, выраженное, конечно, в разных знаках.

Таблицы составлялись или по простой квадратной системе, или по сложной, или часть по одной, а часть по другой. Соответственно употреблялись три формы множественного квадратного шифра:

1. Множественный простой квадратный шифр;
2. Множественный сложный квадратный шифр;
3. Множественный смешанный квадратный шифр.

Если текст был не очень большой, ключи выбраны удачно, если тщательно прослежены частоты повторяемости каждой буквы, если переходы от ключа к ключу делались достаточно часто (например, после 10—20 букв), а сигналы продуманы рационально или просто обходились без них, то для рассматриваемого периода данный шифр принадлежал все же к весьма трудным для разгадки системам. Громоздкость и трудоемкость, однако, ограничивали его использование.

Периодический раздельный шифр («гамбеттовский»). Сущность гамбеттовского шифра заключается в том,

что буквы открытого текста, преобразованные в числовой ряд в соответствии с алфавитным порядком, видоизменяются числовым же ключом (короткой гаммой), накладываемым последовательно, периодически.

Предположим, необходимо зашифровать фразу: «Письмо не получила». Подставим вместо букв числовые значения их места в русском алфавите; получим ряд: 17, 9, 19, 30, 14, 1, 15, 6, 17, 16, 13, 21, 25, 9, 13, 1. Пусть ключом будет слово «ЕВРОПА», которое в числовом выражении имеет вид: 6, 3, 18, 16, 17, 1. Наложим ключ (гамму) периодически на цифровой текст (фразу) столько раз, сколько он на ней уместится, и произведем сложение вертикальных пар чисел. В результате получаем шифртекст:

Ключ:	6	3	18	16	17	1	6	3	18	16	17	1	6	3	18	16
Текст:	17	9	19	30	14	1	15	6	17	16	13	21	25	9	13	1
Шифр-текст.	23	12	37	46	31	2	21	9	35	32	30	22	31	12	31	17

Такой периодический раздельный шифр был весьма употребителен. «Раздельным» его называли потому, что из-за чередования двузначных и однозначных чисел их обычно писали раздельно. Впрочем, писали и слитно, вставляя перед однозначными числами ноль.

В этом шифре одно и то же число может передавать различные буквы, так как получается от сложения разных пар чисел.

Шифр этот становится более трудным для раскрытия, если укладывается в тексте ничтожное число раз. Это могло быть либо при очень коротком тексте, либо при длинном ключе. Обыкновенно длина ключа колебалась от 10 до 25 букв, а при таких размерах даже короткое письмо легко могло быть дешифровано.

Несколько более надежным был сокращенный гамбеттовский шифр.

В этом шифре сложение знаков шифра и текста берется по модулю объема алфавита, т. е. по модулю 30. Иногда использовался другой модуль, например 40.

Легко заметить, что и этот шифр не является стойким. Разумеется, раскрытие его усложняется, если взять очень длинный ключ и очень малый текст. Но большие ключи неудобны, а длина текста зависела от обстоятельств.

Замаскированный гамбеттовский шифр («наполеоновский»). Эта система предполагает большую квадратную таблицу из 28×28 знаков. В первом горизонтальном и левом вертикальном рядах писался непрерывный последовательный ряд чисел от 19 до 28 (по числу букв тюремной азбуки). Затем заполнялись все клетки горизонтальных строк цифрами в возрастающем порядке, начиная от крайнего левого числа: всякий раз, дойдя до 28, следовало начинать опять с единицы (т. е. по модулю 28). Наконец, выше первого ряда чисел и левее первого столбца выписывалась тюремная азбука.

Ключом служила условная фраза или слово. Допустим, ключом является «СИЛЬНЫЙ ПОЖАР», и требуется зашифровать фразу: «Нам нужен наборщик, нет ли подходящего». Чтобы записать первую букву Н, отыскивается тот горизонтальный ряд, который начинается с этой буквы (по тюремной азбуке — 13-й), а затем тот вертикальный столбец, который начинается с первой буквы ключа — С (то есть — 17-й). Отыскиваем клетку, в которой они пересекаются, — в ней имеется число, которое и пишем в шифртексте вместо буквы Н. Так же находим другие замены.

Нетрудно заметить, что составление трудоемкой таблицы этого шифра не делает «наполеоновский» шифр надежнее «сокращенного гамбеттовского». Методы раскрытия этих ключей просты и аналогичны. Об этом шифре «Бундовец» писал: «Наполеон как-то сказал, что от великого до смешного один

шаг. Курьезно, что носящий его великое имя шифр оказывается смешным фарсом, водевилем с переодеванием. А между тем он кое-где у нас употребляется» [4]. Так, нам известно, что в 1902 г. в киевской Лукьяновской тюрьме этот шифр был рекомендован как безусловно надежный, совершенно не доступный раскрытию.

Разностный «гамбеттовский» шифр с двойным периодом. Описанные уже нами системы шифров революционеров основывались на сложении букв текста и ключа. Однако были ключи, где производилось и вычитание. Вот один из разностных периодических шифров, использовавшихся на практике. Возьмем ключ: «ШКУРНЫЙ ВОПРОС» и фразу: «Нам нужны наборщики».

Первая буква ключа Ш (соответствует 24-й по тюремной азбуке) больше первой буквы текста Н (13) на 11. Это выражается так: 1—11. В этом двучлене единица обозначает первую букву текста, а 11 — то, что она меньше первой буквы ключа на 11 единиц.

Вторая буква ключа К (10) больше второй буквы текста А (1) на 9, что записывается так: 2—9.

Третья запишется 3—7, четвертая 4—3.

Пятая буква ключа Н (13) меньше соответствующей буквы текста (19), поэтому последняя изображается так: 5+6.

Таким образом записывается весь текст. Однако этим дело не кончается. Начинает использоваться второй период, который представлял обыкновенно короткое число, например 795. Его называли «вторичным периодом» или «числовым ключом». Его три цифры последовательно прибавляются по модулю к каждому члену наших двучленов, но оставляя знак («+» или «—») числам первичного текста:

Первичный текст	1—11;	2—9;	3—7;	4—3;	5+6; ...
Числовой ключ	7, 9,	5, 7;	9, 5;	7, 9;	5, 7; ...
Окончательный текст:	8—20;	7—16;	12—12;	11—12;	10+13; ...

Легко заметить, что этот шифр очень трудоемок в применении, что отнюдь не компенсируется его надежностью.

Слитный периодический шифр с однородным ключом. Эта система представляет весьма существенное видоизменение предыдущего шифра. Изменение состоит в том, что первоначальный текст и ключ при превращении в числа пишутся не раздельно (то есть не отделяя друг от друга числа, соответствующие отдельным буквам), а слитно; сложение производится между двумя сплошными рядами цифр, начиная слева. В случае, если от сложения цифр ключа и текста получается число, большее 9, то единицу десятков переносят вправо. Например, знакомая уже фраза «Нам нужен наборщик» при ключе «ШКУРНЫЙ ВОПРОС» по тюремной азбуке изобразится так:

Слитный текст:	13112131976131312141625910
Слитный текст:	24101916132693141516141724
Шифртекст	37213057019725453657766644

И эта система не обладала надежностью, была неудобна в применении. Составители шифра заметили, что в нем имеется тот недостаток, что первичный текст и ключ благодаря способу своего составления обладают заранее известным неравномерным распределением цифр (преобладание знаков 1, 2 и т. д.). Поэтому была сделана попытка избавиться от недостатка по крайней мере в числовом ключе, который в новом шифре называется разнородным.

Слитный периодический шифр с разнородным ключом. Это тот же сложный периодический шифр, но в котором сложение и вычитание осуществляется уже по модулю 10.

Вторичный слитный шифр (комбинация с квадратным). Шифр состоит в том, что числовой ключ накладывается на предварительно зашифрованный по

другой системе текст. Иными словами, это комбинация периодического шифра с каким-нибудь иным, например квадратным, прерывистым и т. д., выражающимся числом, а не буквами.

Естественно, этот шифр более надежен, чем предыдущие, однако он чересчур громоздок. Составлять первичный шифртекст, приготовить числовой период (чем длиннее, тем хлопотливее), надписывать его, складывать, помня, где остановились на ключе при остановках и перерывах, — все это делало систему малопригодной к употреблению.

Книжный шифр. До сих пор мы имели дело с системами, где либо искусственно составлялся определенный ограниченный известным образом пронумерованный ряд букв, либо записанный цифрами текст подвергался искусственному изменению с помощью периодической гаммы.

Книжный шифр имеет дело со случайным набором цифр и в этом его большое преимущество. При неизвестной книге, используемой для шифрования, частой смене страниц и внимательном шифровании этот шифр был весьма надежным. Чтобы сохранить тайну шифра, революционеры обычно придерживались таких правил:

1. Заранее условливались о странице, с которой следовало начать шифрование, чтобы не обозначать ее открыто;

2. Пользовались не одной, а многими страницами;

3. Сигналы для перехода со страницы на страницу были, как правило, внутренние, то есть незаметные внешне (чаще всего это были условные буквы);

4. Из специальных ухищрений прибегали к такому: на каждой странице начинали счет не с первой строки, а с заранее условленной, например седьмой.

Чтобы облегчить шифрование по книге, обычно использовали бумажную ленточку. Ее прикладывали вертикально к левому краю страницы и наноси-

ли на нее нумерацию строчек. Поэтому, чтобы всякий раз не отсчитывать строчку, прикладывали к странице ленту и на ней находили готовую нумерацию.

Большие преимущества этой системы бросаются в глаза. Количество знаков, которыми она располагает, оставляет далеко позади все искусственные системы. Если на одной странице 2000 букв, то обыкновенная книга в 20 листов даст до 600 тысяч букв. Этот шифр является многозначным, кроме того, буквы в книге находятся в естественной пропорции, то есть именно в той, которая наиболее выгодна для шифрования. Самая частая буква О в книге из 20 листов встретится до 67 тысяч раз, а самая редкая Ф — всего 60 раз. В применении книжный шифр был также прост и удобен.

Единственным, но очень важным недостатком книжного шифра была необходимость постоянно иметь при себе ключ, и это нередко давало полиции возможность его получить.

Именно поэтому большое распространение приобрел стихотворный шифр, который был тем же книжным, но его было легко держать в голове.

Чтобы пользоваться этой системой, корреспондентам достаточно условиться относительно выбора стихотворения. Затем стихотворение выписывалось в той форме, как оно обыкновенно печатается, строки нумеровались и, выбрав нужную букву, обозначали её дробью, где, как в книжном шифре, числителем служит номер строки, знаменателем — место буквы в ней.

Этот шифр безусловно надежен лишь в случае, если стихотворение крайне редкое, даже совершенно неизвестное. Но такое требование, конечно, сильно уменьшает подвижность шифра, легкость по передаче от одного корреспондента к другому. Трудно также при обширной переписке запоминать несколько таких стихотворений.

Текст, зашифрованный книжным шифром

Конспиративная переписка в революционном подполье

На страницах подпольных изданий конца XIX — начала XX в. регулярно помещались статьи, целью которых было способствовать тому, чтобы каждый революционер обязательно овладел искусством нелегальной связи с применением шифров, умел правильно составлять тексты писем, зашифровывать и расшифровывать их, применять тайнопись, ибо незнание приемов конспирации, неумение пользоваться шифрами, ошибки, допускаемые в шифрованной переписке, могли привести к провалу.

Мы уже говорили о книге Розенталя («Бундовца»), которая сыграла большую роль в деле «криптографического образования» революционеров, принадлежавших к самым различным партиям и фракциям. Другие организации, заботясь о конспиративности своей деятельности, также публиковали и распространяли среди своих членов подобные работы.

Так, в номере «Искры» от 20 декабря 1901 г. содержались такие рекомендации:

«...Шифр — это оружие обоюдоострое, ибо жандармы легко сумеют раскрыть всякий шифр, если не применять при шифровании особых предосторожностей. Безусловно необходимо:

1) не отделять слово от слова; 2) не повторять часто одинаковых знаков, особенно для наиболее употребительных букв; 3) писать шифр так, чтобы нельзя было узнать системы шифра; 4) не употреблять слишком известных стихотворений и книг. Без соблюдения этих правил шифр прямо-таки недопустим».

Кто является автором этих строк, нам неизвестно, но очевидно, что принадлежат они кому-то из руководителей российской социал-демократии того вре-

мени. В. И. Ленин придавал большое значение правильному использованию шифров при ведении конспиративной переписки. Некоторые сохранившиеся замечания его по этому поводу показывают, насколько слабыми шифрами пользовались социал-демократы периода «Искры». 3(16) декабря 1902 г. он писал Д. И. Ульянову (Фите):

«Ваше письмо от 15/XI получено. Написано оно неизвестным нам ключом, впрочем, мы расшифровали все, за исключением адресов. (Не шифруйте иначе, как целыми фразами, иначе очень легко раскрыть ключ). Адреса повторите...» [5].

Н. К. Крупская также постоянно обращает внимание искровцев на недопустимость использования ненадежных шифров. Например, получив плохо зашифрованное письмо от В. П. Краснухи, она в ответном письме, написанном позднее 9 (22) октября 1902 г., пишет:

«Перво-наперво позвольте Вас выругать, что называется, на все корки, за небрежную шифровку. Не зная, что Вы условились о ключе с Евгением, я недоумевала, каким ключом Вы пишете, и, наконец, расшифровала Ваше письмо без ключа в какие-нибудь $^1/_2$ часа. Это прямо скандал. Не повторяйте одних и тех же знаков для одной и той же буквы, иначе вся шифровка никуда не годится». [6].

Умение и опыт приходили с практикой. Естественно, иной раз учились на ошибках, порой трагичных. В том же 1902 г. Г. М. Кржижановский писал: «За нами отчаянно следят... Чтобы что-нибудь сделать под нашей фирмой, надо быть прямо гением конспирации».

Известно, что революционные события 1905—1907 гг. стали проверкой возможностей, надежности организации многих партий. В период нарастания ре-

волюционной волны В. И. Ленин находился в Петербурге и сотрудничал в газете «Новая жизнь». В этом органе им было опубликовано несколько статей, отражавших содержание политического момента. 18 октября 1905 г. газета была закрыта, в ее редакции произведен обыск. Во время этого обыска полиции удалось захватить записную книжку, содержавшую адреса явок, пароли, ключи к шифрам, которыми пользовались члены большевистской партии в 63 городах России, то есть почти все большевистское подполье. По всей вероятности, эта записная книжка принадлежала Н. К. Крупской, ибо только она располагала такими собранными воедино обширными сведениями. Записи в книжке были зашифрованы, но полиции удалось их расшифровать и получить тем самым важнейшую информацию. В записной книжке указывались ключи к шифрам — книги, брошюры и т. п. Следовательно, в переписке использовались в основном книжный и стихотворный шифры. Например:

«Вильно

Писать: Венгерский переулок, 9. 9.

Анне Каценеленсонбоген; ключ:

вторая глава «Евгения Онегина», сумма глав.

Варшава

Новый Свет, 37. Наўчная библиотека, внутри «для Адольфа»; ключ: «Московские ведомости» того дня, каким помечено письмо.

Владимир

явка: Статистическое бюро Губернской земской управы.

1. Федор Аркадьевич Благонравов: «Я слышал, что отец Ваш продает имение в средних губерниях».

2. спросить Николая Ивановича Воронова, сказать: 99, ответ — 72.

Писать: Губернская земская управа, Статистическое бюро, господину заведующему; ключ: «Песнь о вещем Олеге».

Гомель

Писать: Липовая ул., Годе Сауловне Быховской, «Звезда» Вересаева, сумма после перер. след., «Нищета философии», изд. «Молот», 7 стр., «Брожу ли я вдоль улиц шумных...».

Москва

угол Арбата и Спасо-Песковского пер., дом Чулкова, присяжный поверенный Лидов (от Марата): «Я по делу графа Капниста», до 11 часов утра; писать: Московский комитет: дом Шемшурина, Варваре Александровне, ключ: Богданов, 1 часть, 2 издание произведений, стр. 7; Бюро: Москворецкая ул., д. Бахрушина, в лечебнице доктора Блоха его же и спросить от 10 до 2 «Я по поводу ампутации волос». Ответ: «Я согласен».

Явки: (комитет) Долгоруков, 42, зубной врач Никитина-Макаревская или мужа: «Я от упрямца». Открыто писать с единицей.

Комитет писать:

Старая Басманная, Гороховский пер., 15—7. Вера Михайловна Левицкая.

Большая Никитская, у Никитских ворот, магазин «Грамотей», любой продавщице от Старовера.

Тверская, 71, зубной врач Дукович, под арку, направо: «Дайте ножик, дайте вилку».

Тверская глазная лечебница, фельдшер Антонина Ивановна Савинова: «Москва»... [7].

Сведения, почерпнутые полицией из этой записной книжки, позволили провести массовые аресты членов организации по всей стране. В частности, был арестован секретарь Московского комитета РСДРП(б) Шанцер («Марат»), что накануне революционных событий в Москве было большим ударом для большевиков.

Как мы уже говорили, добыча шифров и ключей к шифрам революционеров составляла одну из главных задач действовавших в революционной среде агентов полиции. Получив сведения о шифрах, агенты немедленно передавали их в полицию или писа-

ли о них в своих донесениях. Перед нами одно из донесений уже упоминавшегося нами агента по кличке «Пелагея» ротмистру ДП Ганько от 21 апреля 1915 г. [8]. Агент доносит:

«...На днях в Москву из Петрограда приехала по поручению ЦК РСДРП(б) некая «Татьяна Сергеевна»... «Татьяна Сергеевна» имеет широкие полномочия по воссозданию на местах социал-демократических большевистских организаций и подготовке почвы к предстоящему летом текущего года созыву партийного съезда или конференции, и с этой целью ей поручено объехать область центрального промышленного района и юг, где она должна по выполнении первой задачи заручиться адресами для транспортировки партийной литературы...

«Татьяна Сергеевна» почти ежедневно сносится с П[етербургским] К[омитетом], которому сообщает о достигнутых ею результатах и полученных связях, причем пользуется цифровым шифром:

Мы 1
Азбуку 2
Весь 3
День 4
Писали 5
Бумаги 6
Книжку 7
Извели 8
Мы 9
Фыркающих 10
Отвергали 11
Эх 12
Ящерицу 13
Предпочли 14
Плъшь 15

Указанные цифры обозначают только слова ключа, например, 12 — эх, нужная же для зашифрования буква обозначается порядковой цифрой, занимаемой буквой в слове ключа, так, например, зашифрованная буква «а» будет обозначена: 2—1, или 5—4, или 6—4, или 10—5, или 11—7.

Однако кроме этих цифр при шифровке между ними вставляются еще произвольные цифры с таким расчетом, чтобы каждая буква была обозначена четырьмя цифрами; так, та же буква «а» в окончательно зашифрованном виде будет обозначена: 7251, или 3544, или 2634, или 1025, или 1147.

При этом нужно иметь в виду, что между цифрами ключа вставляется только однозначная цифра, поэтому, если зашифрованная буква состоит из двух однозначных цифр, то произвольные цифры вставляются одна перед цифрой ключа, причем нельзя ставить только 1, а другая — между цифрами ключа; если же зашифрованная буква состоит из двузначной и однозначной цифр, как, например, «а» — 11—7, то вставляется только одна однозначная цифра между ними. Таким образом, зашифрованное слово «Москва» будет обозначаться так:

392211171534327613873109 5

Для расшифровки, так как все указанные цифры пишутся подряд, нужно весь зашифрованный текст разбить на группы по четыре цифры, из коих выкинуть произвольно вставленные цифры, имея в виду, что если первая цифра будет «1», то произвольно вставленная — только одна цифра между цифрами ключа, то есть по счету третья, в противном случае — вставлено две цифры — первая и третья...»

Итак, мы видим, что шифрами пользовались все члены революционных организаций. Однако составляли их, как правило, лица, имевшие математическое образование. Розенталь («Бундовец») в своей книге «Шифрованное письмо» предлагает к использованию им самим изобретенный «рациональный шифр», который, по его мнению, удовлетворял всем основным требованиям, предъявляемым к шифрам революционеров-подпольщиков. Однако этот шифр представлял собой шифр пропорциональной замены и относительно его особой стойкости автор заблуж-

дался так же, как и авторы других, рассмотренных им в книге шифров, которых он подверг критике.

В среде социал-демократов также были изобретатели шифров. Нам бы хотелось здесь подробнее остановиться на двух из них — Г. И. Бокии и В. Н. Яковлевой, во-первых, потому, что мы в своей книге в дальнейшем еще вернемся к этим именам, а во-вторых, потому, что жизнь и деятельность этих лиц представляют, на наш взгляд, значительный интерес для изучающих отечественную историю. И Глеб Бокий, и Варвара Яковлева принадлежали к ядру социал-демократической большевистской партии и играли видную руководящую роль в революционном движении, а также в ранний послереволюционный период. Оба этих незаурядных человека погибли в период сталинских репрессий конца 30-х гг., а их имена предали забвению. В свое время, в течение многих лет по крупицам с трудом собрав материал о жизни и деятельности Глеба Бокия, я написала книгу, выступив как автор под моей прежней фамилией Алексеева. В литературной обработке текста принимала участие под псевдонимом «Николай Матвеев» Н. М. Беркова [9]. О В. Н. Яковлевой я опубликовала небольшую статью в одном из специальных изданий. Популярную книгу для детей о революционной деятельности большевиков В. Н. Яковлевой и ее мужа — известного ученого-астронома и математика, профессора Московского университета П. К. Штернберга — в свое время написал писатель Л. Э. Разгон [10].

Глеб Иванович Бокий родился в 1879 г. в старинной дворянской семье. Его предок Федор Бокий (Bokiej)-Печихвостский, мелкопоместный шляхтич, чей герб в польско-литовской геральдике представлял собой «секиру, обращенную острием вправо, а поверх нее крест», был назначен во второй половине XVI в. владимирским подкоморием в Литве и упоминается в переписке Ивана Грозного с Андреем Курбским. Подкоморий в средневековой Польше и

Литве — третейский судья, в компетенцию которого входили вопросы о границах владений (межевой суд). Подкоморий назначался королем на постоянный срок. Ф. Бокий-Печихвостский был назначен от Владимиро-Волынского воеводства. Прадедом Глеба Бокия был известный русский математик академик Михаил Васильевич Остроградский — ученый, много сделавший для развития отечественной науки, который задолго до отмены крепостного права имел немалое мужество заявить, что людей надо ценить не по их положению, а по их знаниям и способностям. Отец Глеба Ивановича, действительный статский советник (этот гражданский чин соответствовал генеральскому званию) Иван Дмитриевич Бокий, был автором учебника «Основания химии», по которому училось не одно поколение гимназистов, принимал участие в воспитании великих князей.

В 1896 г. после окончания реального училища Глеб Бокий поступает в Горный кадетский корпус имени императрицы Екатерины II в Петербурге — крупнейшее в то время высшее техническое учебное заведение России. Высокоодаренному юноше, обладавшему кроме личных достоинств многочисленными сословными привилегиями, была уготована блестящая научная карьера. Кстати, его старший брат Борис Бокий, чей барельефный портрет и ныне можно увидеть на одном из зданий Горного института в Москве на улице Вавилова, стал крупным ученым-горняком, профессором Петербургского горного института. Однако судьба Глеба Бокия сложилась иначе. Уже в ранней юности, движимый демократическими идеями, он выбирает для себя путь революционера и в 1897 г. вступает в петербургский «Союз борьбы за освобождение рабочего класса», с 1900 г. он член РСДРП. Большевик Глеб Бокий 12 раз подвергался арестам, провел полтора года в одиночной крепостной камере, два с половиной года — в сибирской ссылке, от побоев в тюрьме он получил травматиче-

ский туберкулез. На протяжении 20 лет (с 1897 по 1917 г.) он являлся одним из руководителей петербургского большевистского подполья.

1914—1915 гг. были для подпольщиков особенно трудными. Сменяя одна другую, накатывались волны жесточайших репрессий. Особенно большой урон понесли петербургская и московская организации большевиков. С целью избавить свою работу от участившихся провалов, зная о наличии в партийных центрах провокаторов, петроградские большевики организовали так называемую «группу 1915-го г. при ЦК», куда вошли самые надежные, много раз проверенные лица, и в том числе В. Молотов, А. Аросев, Г. Бокий. Ужесточалась партийная дисциплина, самые серьезные требования предъявлялись к соблюдению конспирации.

Старая большевичка, член партии с 1915 г. В. Ф. Алексеева, вспоминая о работе в подполье того времени, писала: «Конспирация в большевистском подполье, которое подвергалось особенно беспощадным расправам со стороны царских властей, действительно была суровой и сложной и потому не всегда легко давалась людям, особенно новичкам, не искушенным в борьбе...

При аресте Глеба Ивановича забирали и его по виду самые обычные ученические тетради, исписанные математическими формулами, а на самом деле — записями о подпольных делах, зашифрованными математическим шифром. Шифр этот являлся изобретением Глеба Ивановича, и ключ к нему был известен только ему одному. Лучшие шифровальщики, какими только располагала царская охранка, ломали головы над этими «формулами», подозревая в них шифр. Однако раскусить этот орешек они так и не смогли. «Сознайтесь, — говорил Глебу Ивановичу следователь, — это шифр?» А Глеб Иванович невозмутимо отвечал: «Если шифр, то расшифруйте». С досадой следователь возвращал ему эти загадочные тетради» [11].

В конце 1916 — начале 1917 г. Г. И. Бокий был членом Русского бюро ЦК РСДРП, с апреля 1917 — секретарем Петербургского комитета, в октябре 1917 г. он член Петербургского военно-революционного комитета, один из руководителей вооруженного восстания.

Была автором собственных систем шифров и глава большевистской организации центрального промышленного района, секретарь московского областного ЦК РСДРП(б) В. Н. Яковлева.

Дочь московского купца второй гильдии, Варвара Николаевна Яковлева окончила математический факультет Высших женских курсов в Москве. Активная участница революции 1905—1907 гг. В. Н. Яковлева являлась крупным партийным организатором, кандидатом в члены ЦК, автором Устава партии, принятого VI съездом РСДРП(б).

Так же как и Г. И. Бокий, В. Н. Яковлева создавала шифры, которыми пользовались и другие революционеры. К сожалению, ни тетради Бокия, ни шифры Яковлевой не сохранились. В архивах ДП есть лишь некоторые их письма, зашифрованные другими, уже известными нам шифрами. Некоторые из таких шифрованных писем Яковлевой были получены полицией при следующих обстоятельствах.

В конце декабря 1913 г. она во второй раз бежала из сибирской ссылки. Не без труда добравшись до Москвы (по дороге она сломала ногу), Варвара Николаевна вместе со своим мужем П. К. Штернбергом выехала в Петербург. Из Москвы и Петербурга она написала несколько писем оставшимся в ссылке в Нарыме своим близким товарищам: В. Куйбышеву, В. М. Косыреву, И. Н. Смирнову. Письма перехватила полиция. Одно из них и содержит записи, которые могут проиллюстрировать, как Яковлева пользовалась книжным шифром [12].

Начало письма написано открытым текстом и по содержанию носит частный характер. Но вот его зак-

лючительная часть: «Ну-с, а в заключение вот Вам задача. Вы, я помню, занимались в последнее время геометрией. Так вот посидите для практики над этой задачей. Она мало интересная, зато для упражнения — сущий клад. Все необходимые данные написаны на вложенной бумажке. Напишите мне, решите ли ее...» А вот что написано на вложенном листе бумаги:

«X—5, Y—6
X—5, Y—8
X—5, Y—4
X—3, Y—14
X—6, Y—3
X—6, Y—8
X—6, Y—7
X—4, Y—1
X—7, Y—4 и т. д.»

Таким образом, дается множество «координат кривых» и предлагается: «Вычертить кривые по данным координатам точек. Определить все точки их пересечения, провести через них кривую и найти ее уравнение».

Несложный математический анализ этого письма показывает, что никаких кривых и никаких иных функций по этим данным не построить. А вот то, что это книжный шифр, вряд ли можно подвергнуть сомнению. Первые координаты здесь — «иксы» — означали номер строки книги, а вторые — «игреки» — номер выбранной буквы в строке. Нумерация кривых, которая также присутствовала в письме, соответствовала номеру выбранной страницы книги.

Шифр применен Яковлевой со знанием дела: с малым числом использованных знаков на каждой странице и без наличия использованной книги-ключа текст этого письма не поддается дешифрованию. Как и опасалась Варвара Николаевна, письмо попало в руки полиции. Но, судя по тому, что в архивном деле отсутствуют какие-либо комментарии к нему, дешифровальщики ДП его не дешифровали.

Глава тринадцатая

ПЕРЕД БУРЕЙ

Криптография в годы Первой мировой войны

Экономический потенциал, уровень военных, технических и научных возможностей каждой из сторон, степень и уровень оснащенности линий связи, готовность к получению информации о противнике, как лакмусовая бумажка, выявила война. Установилось мнение о слабости криптографической службы России периода Первой мировой войны, о том, что в первые месяцы войны радиосообщения вообще не шифровались, а посылались в открытом виде, что послужило одной из причин неудач, сопутствующих действиям русской армии в тот период. В действительности дело обстояло несколько иначе.

В Военном ведомстве к началу войны дела складывались весьма плачевно.

После военных неудач России в Маньчжурии пост военного министра занял Александр Федорович Редигер, при котором Россия стала быстро набирать военную мощь. Имя Редигера почтенно и уважаемо. Профессор Академии российского Генштаба, всем внешним обликом воплощение интеллигента (залысина, тонкий облик, пенсне), Редигер принял военную машину России в период поражений на полях Маньчжурии. Автор многих научно-военных трудов,

которые долгое время считались почти классическими, высокообразованный человек, он имел смелость указывать Николаю II на необходимость демократических реформ в армии. Обрусевший швед, Редигер был суховатым педантом-аккуратистом. Некрасивый и лишенный светского блеска, он не развлекал царя своими докладами, а лишь пытался вовлечь его в ту сложную работу, которую проводил сам... Вот он опять стоит на пороге, а из-за эполет Редигера выглядывают адъютанты, и скоро кабинет императора оказывается завален схемами железных дорог Германии, графиками мобилизации Австрии, картограммами достоинств пушек Крезо и Шнайдера, Круппа и Путилова... В руках исполнительных генштабистов шуршали свитки новых схем, и Николай II прилагал неимоверные усилия, чтобы, скрывая зевок, показать министру, как ему все это было безумно интересно.

После поражения в войне с японцами Россия быстро набирала военную мощь. Поэтому премьер-министр Столыпин, понимая, что ассигнования на дело обороны — вопрос важнейший, активно подружился с Государственной думой, где проводились острые дебаты по вопросам таких ассигнований. А к портфелю военного министра судорожными рывками, словно пантера, завидевшая лань, уже давно подкрадывался ситцехлопчатобумажный фабрикант, глава партии октябристов Александр Иванович Гучков, с которым Столыпин вошел в глубоко конфиденциальные отношения... Гучкова военные дела привлекали смолоду. Он сражался в Трансваале за буров против англичан и был жестоко ранен пулей «дум-дум», участвовал в Македонском восстании за свободу Греции, под Мукденом был взят в плен японцами. Гучков смело дрался на кровавых дуэлях. Робким купчишкой его никак не назовешь.

27 мая 1908 г. Гучков пошел на конфликт с великими князьями, плотно захватившими все высоты военного правления. Главный удар он обрушил на

Николая Николаевича, который возглавлял Совет Государственной Обороны. Гучков прицелился точно: если ты занимаешь ответственный пост, так будь любезен быть ответственным за свои деяния. Но в том-то и дело, что их высочества Романовы суду общества не подлежали. А Гучков говорил:

— Постановка неответственных лиц во главе ответственных отраслей военного дела является делом совершенно ненормальным... Государственный Совет Обороны во главе с великим князем Николаем Николаевичем является серьезным тормозом в деле улучшения нашей армии и нашего флота...

Конечно же, речь Гучкова — это слова Столыпина, но премьер, нанося удар по камарилье, кажется, не рассчитал силы взрыва. Рикошетом осколки полетели в него же, Столыпина, — назревал кризис власти. Со дня на день все ждали, что премьер подаст в отставку. Вместо этого Петр Аркадьевич выкинул фортель: от октябристов переметнулся к националистам и устоял.

В то же время военный до мозга костей, профессионал, Редигер доказывал царю, что армия не должна исполнять карательные функции:

— Допустимо ли держать в гвардии офицеров, которые тушили папиросы о тела женщин, лишали узников воды, насильно поя их водкой, практиковались, осмелюсь доложить, прыганьем по грудной клетке человека до тех пор, пока не раздавался хруст ребер?

Но, как писал очевидец, «нет той картины человеческих страданий, которая могла бы тронуть это высушенное вырождением сердце, нет предела полномочиям, которые царь не был бы готов дать кому угодно для непощадного избиения своих подданных».

Абсолютно не желающий утомлять себя вниканием в военные проблемы государства, к тому же не желая прощать Редигеру то, что он публично не опроверг высказывания Гучкова в Думе, царь решил отыграться на военном министре, отправив его в

отставку. Для его замены Николай II не выбрал никого лучше, чем тогдашнего киевского генерал-губернатора Сухомлинова.

Владимир Александрович Сухомлинов за непреодолимое желание петушиться перед дамами до весьма преклонных лет был прозван Шантеклером.

Начальник киевского охранного отделения Николай Николаевич Кулябко был извещен еще осенью 1907 г. одним из своих агентов наружного наблюдения, что в доме киевского генерал-губернатора Сухомлинова была попойка, на которой присутствовал кроме прочих австрийский консул Альтшуллер, подозреваемый в шпионаже в пользу Австро-Венгрии, и остался ночевать. Причем секретные документы об этих подозрениях находятся в том же доме, где он сейчас ночует...

Альтшуллер бывал часто не только в доме генерал-губернатора, но и в его служебном кабинете, куда имел доступ на правах друга, и адъютанты генерал-губернатора уже не раз ловили его за руку в те моменты, когда он начинал рыться в секретных бумагах. В это время радио еще только входило в быт нашей армии, оно было новинкой и называлось «беспроволочным телеграфом». На первых киевских опытах армейского радирования присутствовал и Альтшуллер, внимательно приглядываясь. Офицеры киевских штабов иногда звонили на дом главнокомандующему военным округом Сухомлинову и... вешали трубку:

— Опять к телефону подошел консул Альтшуллер, а назвался такими словами: «Генерал-губернатор у аппарата». Но его выдает акцент, каким Сухомлинов, слава богу, пока еще не владеет!

В декабре 1908 г. Сухомлинов был вызван в столицу и назначен начальником Генштаба, приняв дела от генерала Ф. Ф. Палицына, который сдал Сухомлинову несколько шкафов военных планов на будущее. Тут была разработка операций на все случаи жизни — будь то перестрелка на Кушке или натиск германских полчищ на Вильно. С какой-то непонятной подлостью Сухомлинов стал вырывать из досье листы и схемы, нарочно перепутывал страницы, кромсал планы ножницами, обливал таблицы чернилами. Испортив все, что только можно, Сухомлинов потом сам же жаловался генералу А. А. Поливанову, бывшему помощником Редигера:

— Алексей Андреевич, не пойму, за что так ценили Федю Палицына? Ведь он мне такой компот оставил, что я, человек опытный, и то не мог разобраться.

Этому-то человеку и вверил царь Военное ведомство весной 1909 г., отправив Редигера в отставку, именно под его руководством русские армии вступили в Первую мировую войну. Безусловно, он был абсолютно вреден на занимаемом посту, но зато приятен во всех отношениях и удобен императору. Его доклады царю не имели ничего общего с докладами Редигера. Рассказав царю свежий анекдот, Сухомлинов выгружал на стол эскиз юбилейного значка, куски цветного сукна для пошива военных мундиров. Император отодвигал в сторону модели остроконечных пуль, оставшиеся от Редигера, с удовольствием прикладывал к своему мундиру новую тряпочку...

Когда в начале августа 1914 г. вместе со спешно эвакуированным из Берлина русским посольством в Петербург вернулся военный атташе полковник Базаров, он с изумлением обнаружил, что все его доклады, посылавшиеся в Петербург министру Сухомлинову в период 1911—1914 гг. и содержавшие важнейшие разведывательные данные о военном потенциале немцев, военным министром вообще не читались.

Министром иностранных дел в довоенный период и период войны являлся Сергей Дмитриевич Сазонов, который получил портфель министра иностранных дел в кабинете Столыпина. Сазонов был его родственником и ставленником, выходцем из культурной семьи москвичей-славянофилов. Лицеист по

образованию, он был полиглот и музыкант, знаток истории и политики.

В Министерстве иностранных дел России, как и прежде, в период войны организацией всей шифровальной службы ведал цифирный комитет. В 1915 г. в него входили: А. Нератов, В. Арцимович, Н. Базили, К. Таубе, Э. Феттерлейн, Ю. Колемин, М. Чекмарев, Н. Шиллинг, И. фон дер Флит. Все это были весьма просвещенные люди, опытные специалисты-криптографы. Они ведали всеми вопросами криптографии. Так, барон Константин Фердинандович Таубе пришел на службу в МИД в 1877 г. после окончания Императорского Александровского лицея, из которого был выпущен с чином 9-го класса. Начав работу с должности чиновника «при канцелярии», пройдя все ступени иерархической лестницы, он оказался на ее верху: в 1913 г. был произведен в тайные советники. За криптографическую деятельность награжден российскими и иностранными орденами: Святого Владимира 3-й и 4-й степени, Станислава 1-й степени, прусским Короны 3-й степени, аннамским Дракона, бельгийским Леопольда, черногорским Князя Даниила трех степеней, испанским Изабеллы Католической, французским Почетного Легиона, персидскими Льва 1-й степени и Солнца 2-й степени, греческим Спасителя, датским Данеброга, папским Пия, бухарским Золотой Звезды 1-й степени, итальянским Короны. Был также награжден медалями, почетными знаками, деньгами. Большими заслугами в криптографической деятельности обладали все члены цифирного комитета, которые располагали сведениями о всех использующихся на линиях связи шифрах, о действовавших системах ключей, времени и способах изготовления шифрдокументов, о местах использования тех или иных шифров, количестве изготовленных экземпляров шифров, времени их использования, причинах изъятия и т. п. Такие сведения сводились в регулярные отчеты, и,

таким образом, имелась на каждый период времени достаточно полная картина состояния шифровального дела в системе МИД.

Война показала, что Россия не смогла предвидеть опасность затяжки со своевременным вводом новых специальных шифров и кодов на военный период по линии МИД. Уже к концу 1914 г. стало ясно, что действующие коды не обеспечивают в достаточной мере тайну шифрованной корреспонденции и вместе с тем не позволяют ускорить самый процесс шифрования. Министерством было предложено срочно изготовить для снабжения своих учреждений: 1) особые словари в 10 тысяч знаков, наборные и разборные: дипломатический русский, дипломатический французский, два восточных и консульский; 2) словарные наборные и разборные таблицы с особыми вертикальными шифрами; 3) особые ключи для перешифрования. Однако через два года, осенью 1917-го, в докладе, представленном руководством шифровального отдела Временному правительству, констатировалось, что выполнение этой намеченной в начале 1915 г. программы провалилось и что пришлось в качестве временных мер вводить более слабые шифры — «трехзначные словари».

Как известно, по планам русского командования, спасая положение французов на Марне, две русские армии, а именно — 1-я армия под командованием П. К. Ренненкампфа и 2-я армия под командованием А. В. Самсонова, должны были спешно, раньше сроков завершения мобилизации, войти в Восточную Пруссию, обходя Мазурские болота с севера и юга, и оттянуть на себя жар битвы.

Армии оказались разделенными непроходимыми Мазурскими озерами, поэтому связь между ними осуществлялась в основном по радио.

Военное ведомство имело специальные шифры для военного времени. Задолго до войны, еще при Редигере, был создан специальный шифр для войсковых

соединений. Это был довольно сложный лозунговый шифр двойной вертикальной перестановки по двум номерным рядам-распределителям, с частой сменой ключей. К сожалению, этот шифр после объявления войны не был сразу разослан армейским шифровальщикам, как это предусматривалось ранее. Эта ошибка, сделанная сознательно или бессознательно, сыграла определенную роль в поражении армии Самсонова на Мазурских островах у Танненберга. При взаимодействии 1-й и 2-й армий оказалось, что в армии Раненкампфа новый шифр уже получен, а старый уничтожен, в армии же Самсонова еще действовал старый шифр. Чтобы иметь связь, пришлось переговариваться по радио в открытую, чем не могло не воспользоваться немецкое военное командование.

К этому надо добавить, что разведка и связь в армиях были поставлены из рук вон плохо. При наступлении забывали о своих тылах. Обозы погибали в хвосте армии Самсонова, не успевая подтягиваться за нею, а связи между частями практически не было. Армия не имела запасов телеграфной проволоки, командование и разведка вынуждены были вести переговоры по телефонам из квартир местных жителей, что, конечно, не оставалось тайной для немцев. Пруссия же уже в то время была опутана телефонными проводами. С любой захудалой фермы немцы могли докладывать прямо в штабы Кенигсберга о продвижении русской армии. Русская военная разведка обнаруживала потаенные телефонные аппараты в погребах с картошкой и даже в пчелиных ульях. В то же время в критические моменты приказы командующего Северо-Западным фронтом генерала Жилинского о своевременном отходе армий к определенным рубежам, передаваемые по телеграфу, просто не доходили до Самсонова.

Среди причин, повлекших за собой гибель героически сражавшейся армии А. В. Самсонова, историки указывают и на тот бесспорный факт, что 1-я армия Раненкампфа просто не пошла на соединение со 2-й армией, и эту «непостижимую неподвижность» 1-й армии сразу же отметили командовавшие немецкими войсками Людендорф и Гинденбург. Раненкампф второй раз фактически предал Самсонова, оставив его армию без поддержки. Как известно, в первый раз он это сделал во время русско-японской войны в боях под Мукденом. Позже, в Мукдене, Самсонов пришел к отходу поезда, когда Раненкампф садился в вагон, и при всех публично исхлестал его нагайкой. Что же было причиной предательского бездействия Раненкампфа в Мазурских болотах в августе 1914 г.: и на этот раз охватившая его трусость или затаенное чувство мести Самсонову?

Неразбериха со связью наблюдалась и в других русских армиях. Шведский криптограф Гульден (Gulden) в своей статье (Revus Militarie Fransaise, august 1931) пишет, что в германском имперском архиве можно прочитать, что русские радиостанции очень часто передавали свои сообщения открытым текстом, военные радиостанции не получали во время мобилизации комплекты необходимых для связи шифров. При таком беспорядке в начале войны неоднократно случалось, что радиостанции, прибывающие на фронт, принадлежавшие в мирное время разным радиоподразделениям, не могли обмениваться шифрованными сообщениями по той простой причине, что отдельные радиороты снабжали свои радиостанции собственными шифрами. Поскольку после мобилизации на один и тот же участок фронта могли попасть радиостанции разных рот, то в первые же дни войны выяснилось, что радиостанции, приданные одному и тому же армейскому корпусу или кавалерийской дивизии, говорят на разных шифрязыках. А поскольку одна радиостанция не понимала другую, то при отсутствии надежной про-

волочно-телеграфной связи приходилось повторять шифрсообщения открытым текстом.

Наличие слабых военных шифров, недостаточно продуманных инструкций к ним, большое количество нарушений шифрдисциплины, — все это в совокупности вело к тому, что русские шифры успешно раскрывались австрийскими и немецкими специалистами. На германском Восточном фронте непосредственный факт организации дешифрования русских шифрсообщений произошел как бы случайно (хотя рано или поздно это все равно бы произошло). Некий немецкий языковед Добнер (Deubner), несмотря на свои преклонные лета, вступил добровольцем в ряды ландштурма для работы переводчиком русского языка. Его направили в район укреплений Кенигсберга. Вначале он переводил открытые тексты русских радиограмм. Мало-помалу в его руках скопился большой материал. Вскоре профессор заметил, что некоторые радиограммы и шифрограммы являются повторением одна другой. Известно, и мы об этом писали, что для слабых шифров и кодов того времени такой материал являлся неоценимым подспорьем для начала эффективного раскрытия шифра или кода. И хотя русские понемногу сумели согласовать шифры своих радиостанций, противник уже имел в своих руках раскрытые шифры и коды.

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. [1].

Можно отметить снижение числа дешифрованных телеграмм по ряду государств: это объясняется,

в первую очередь, резким сокращением передачи таких телеграмм по радио. Так, за время с июля 1915 г. по март 1916 г. 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. В отчете за 1915—1916 гг., подготовленном старшим чиновником при канцелярии МИД Долматовым и направленном товарищу министра иностранных дел, указывается на встречающиеся трудности при дешифровании за счет появления в переписке большого числа новых слов (в итальянских и английских кодах), за счет частой смены кодов. Так, Англия до войны ежегодно выпускала два новых кода, а в отчетном же военном году она выпустила их пять, что крайне затруднило их дешифрование. Следует, кстати, отметить, что в указанном отчете, как и требовали традиции того времени, высказывается ходатайство о награждении наиболее отличившихся в дешифровании криптографов. А именно высказывается просьба наградить деньгами гг. Наньерского (итальянские шифры) — 1000 рублей, Циглера (английские и греческие шифры) — 2300 рублей, фон Берга (австрийские и германские шифры) — 1100 рублей, Рамминга (японские шифры) — 1150 рублей, Феттерлейна (персидские и французские шифры) — 2400 рублей и Струве (английские шифры) — 900 рублей. Как видим, это немалые суммы и они были даны.

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 пору-

чения, 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.

Более широко и масштабно развернуть дешифровальную работу во многом не удавалось из-за слабости подразделений радиоперехвата и большой нехватки специалистов-криптографов. Исторические материалы показывают, что многие неудачи русской криптографии этого периода 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».

Изученные нами журналы входящих документов Особого отдела ДП того времени, о которых мы уже говорили, позволяют установить, что и сюда с фронта присылали шифрованные документы для дешифрования. Материалы начали поступать уже в 1914 г. 25 августа 1914 г. из Архангельска от военного губернатора поступило в ДП сообщение, что на рейде у села Ковда Александровского уезда был задержан немецкий пароход «Удгарт», имевший радиотелеграфную станцию, причем в каюте радиста была обнаружена шифртелеграмма. Эта телеграмма и направлялась для дешифрования в ДП. Лишь через полгода (!), в январе 1915 г. Архангельск дождался ответа: «Эксперт пришел к заключению, что означенная телеграмма составлена на условном языке

(зашифрована) и без ключа не может быть прочтена-переведена. Переводил коллежский асессор Ярилов». Можно представить себе реакцию в Архангельске на такое послание.

Между тем Зыбин оставался верен себе. 13 марта и 14 апреля 1915 г. генерал-квартирмейстером при Верховном главнокомандующем были доставлены в ДП «шифрованные документы с театра войны». В первый раз были привезены пять кратких радиограмм, из которых четыре оказались искаженными при передаче, а пятая заключала исправленный текст двух предыдущих. При разработке оказалось, что они зашифрованы при помощи особого кода. ДП обратился с письмом к генерал-квартирмейстеру, но ответа не последовало. 14 апреля ДП получил копию телеграммы австрийского военного министра из Вены, объемом всего в десять знаков, зашифрованную словарным ключом, разобрать которую, естественно, также оказалось невозможно. В своей докладной по этому поводу Зыбин с горечью пишет, что не имеет никакой возможности получить какие-нибудь дополнительные сведения о присланных документах, присылка их в ДП занимает три — пять дней, в этом случае, если они и будут дешифрованы, то сведения уже устареют и будут представлять лишь исторический интерес. И вновь Иван Александрович сам предлагает свои услуги, для того чтобы поработать некоторое время непосредственно в Главном штабе, своими знаниями «послужить Родине в годину испытаний». К сожалению, мы не располагаем сведениями, была ли удовлетворена просьба статского советника.

Однако в дешифровальной работе по этому направлению были и некоторые успехи. Еще в январе 1915 г. из Генеральной квартиры Генерального штаба поступили фотографические снимки германского шифра с переводом и правилами пользования. Вско-

ре поступили один германский и пять австрийских ключей к шифрам. В апреле были присланы восемь копий шифрованных телеграмм австрийских и германских военных агентов в Вену, Берлин и Брашов. В журнале имеется пометка о том, что тексты телеграмм разобраны. В августе 1915 г. были также прочитаны австрийские шифрсообщения. В это же время дешифровали телеграмму Берковича к Маннергейму, присланную из штаба командующего 6-й армией. В апреле 1916 г. были получены и дешифрованы три немецких шифрованных сообщения, присланных начальником контрразведки штаба 3-й армии, и два шифрсообщения — из штаба Юго-Западного фронта. Имеется запись от 31 марта, что получено четыре книги германских дипломатических шифров, а через некоторое время получили две книги турецких шифров, отобранных у Ахмета Джемиль Бея, и вскоре шифр, который использовался «немецкими шпионами в Дании и Швеции». С помощью добытых шифров или иным способом весной и летом 1916 г. было прочитано свыше 30 шифрованных немецких сообщений. В августе 1916 г. чинам 5-го отделения Особого отдела ДП, которым руководил Зыбин, в награду за дешифровальную работу было выдано 540 рублей.

В то же время и в 1915-м, и в 1916 гг. в ДП поступали в большом количестве немецкие и австрийские шифрованные радиограммы. Но ни одна из них дешифрована не была.

В Военном министерстве с началом войны были организованы дешифровальные отделения при всех штабах армий и флотов.

До войны Россия располагала очень малым числом радиостанций пеленгации и перехвата. Опыт первых же военных действий убедил командование в необходимости создания таких станций, оснащения их соответствующим радиооборудованием, техникой и специалистами — радистами и дешифровальщиками.

Наиболее интенсивно и успешно эта работа развернулась у моряков на Балтике. Так, на побережье Балтийского моря уже в августе 1914 г. было выделено: в южном районе — три радиоприемника (Гапсаль, Кильконд, Даггерорт), в северном районе — три в Гельсингфорсе и один в Ганге, в западном районе — также три радиоприемника (Абор, Престэ, Утэ).

Пеленгаторные станции (компасного типа — 32 луча) были установлены в Ганге, на о. Рэншер, о. Эзель и в Гапсале.

В первый период систематизации и обработки материалов перехвата непосредственно на станциях организовано не было. Все шифровки передавались на районные центральные станции, где, как правило, материал залеживался из-за неимения или нехватки криптографов или просто не обрабатывался.

Ценность отдельных расшифрованных телеграмм вскоре показала, что необходимо создать специальный информационный центр и станции особого назначения — дешифровальный центр. Морским Генеральным штабом были утверждены штаты таких станций. В штаты каждой станции входило семьдесят три человека, из них: начальник станции — капитан I ранга, дежурные офицеры и дешифровальщики — 10—12 человек во главе с начальником дешифровальной группы, действительным статским советником.

К августу 1915 г. в Штитгамне была закончена постройка станции особого назначения, работники которой с этого момента приступили к тщательной обработке немецких шифрованных телеграмм.

Немцы в войну применяли морской трехбуквенный код с перешифровками. Русские дешифровальщики достаточно быстро открывали новые ключи и читали немецкие сообщения и приказы.

Благодаря работе небольшой группы экспертов (начальник станции капитан I ранга Петров, лейте-

нанты Барлевен и Измалков, мичманы Марков и Тимофеевский, надворный советник Павлович, статские советники Орлов и Проффен) военное командование почти всегда было осведомлено о деятельности немецких кораблей. Минные поля и банки, о которых немцы сообщали всем своим кораблям после их постановки, также становились известны русским.

Во время войны к традиционным источникам добывания шифров и кодов (кража, покупка, дешифрование) добавились затонувшие или захваченные корабли противника, захваченные узлы связи, сбитые самолеты и дирижабли.

Хорошо известна история захвата немецкого морского кода с крейсера «Магдебург», события которой относятся к концу августа 1914 г. В Балтийском море был потоплен германский крейсер «Магдебург». Несколько часов спустя русским удалось подобрать тело утонувшего немецкого младшего офицера с этого корабля. Окостеневшими руками мертвец прижимал к груди шифр и кодовые книги ВМС Германии. Оказалось, что это был военно-морской код для связи центра с кораблями, он же использовался для шифрования телеграфной переписки между Берлином и германскими военно-морскими атташе за границей. В первую очередь, русское командование приняло все меры к тому, чтобы немцы не узнали о компрометации шифров. В частности, с этой целью водолазам, обследовавшим «Магдебург», был объявлен выговор за нерадивую работу, которая якобы не дала ничего ценного. Эта информация была сообщена капитану «Магдебурга» и части команды, взятой в плен. В результате скомпрометированный код немцами не был заменен.

6 сентября к главе английского Адмиралтейства первому лорду Уинстону Черчиллю с визитом прибыл русский военно-морской атташе. Он получил из Петрограда сообщение с изложением случившегося

и уведомлявшее о том, что русское адмиралтейство с помощью данного шифра и кодовых книг (код с перешифровкой простой заменой) может дешифровать, по меньшей мере, отдельные участки военно-морских телеграмм. Кроме того, находки с «Магдебурга» были ценнейшим материалом для криптографической работы над дешифрованием других кодов с перешифровкой. Русские считали, что Адмиралтейству Англии следовало бы иметь эти книги. Как указывает Д. Кан, это была поразительная и неожиданная удача, пожалуй, самая счастливая во всей истории криптографии [2].

Получив сообщение из России, британское Адмиралтейство, как пишет об этом У. Черчилль в книге «Мировой кризис» [3], немедленно послало за шифрами в Архангельск военный корабль. В октябре шифры были доставлены в Лондон. Код являлся главным, но не единственным средством шифрования. Тем не менее уже в начале ноября 1914 г. удалось снять усложнения (перешифровку) кода и добиться регулярного чтения радиограмм, посылаемых германским правительством и военным командованием [4].

Английская разведка эффективно использовала подарок русских. Она не только дешифровала ценные телеграммы, но и посылала телеграммы от имени германского командования. Одна из таких телеграмм привела к крупной победе англичан на море: была уничтожена немецкая эскадра под командованием генерала Шпее осенью 1914 г. недалеко от Южной Америки. В составе эскадры находились крейсеры «Шарнхорст» и «Гнейзелай», вооруженные новейшими дальнобойными орудиями. Ложным приказом, переданным Шпее по захваченным шифрам, его эскадру заставили идти из чилийского порта Вальпараисо к Фолклендским островам, где их ожидали английские мощные военные корабли, которые расстреляли немецкую эскадру в упор.

Благодаря дешифрованию немецких телеграмм англичане выиграли не одно морское сражение, спасали свои транспорты, добивались серьезных успехов на дипломатическом поприще в борьбе за нейтральные страны (например, за Аргентину).

Нельзя не сказать о том, что наряду с успехами Россия терпела и многие неудачи. Общая слабость и отсталость государства от передовых стран не могли не сказаться и на криптографической службе. Мы уже говорили о неудачах, связанных с никуда не годной шифрованной радиосвязью царских армий, и о том, что из-за слабости российских шифров и различных нарушений шифрпереписку русских армий читали и австрийцы, и немцы, и англичане. В частности, немцами и австрийцами был раскрыт русский военный код, что позволило им свободно читать передававшиеся по радио донесения и приказы царских штабов. Это была одна из причин тяжелых потерь, понесенных русской армией.

Кроме того, в российской специальной службе даже не была поставлена на должную высоту информация о скомпрометированных шифрах, из-за чего они продолжали употребляться и после компрометации. 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, оказывается совершенно необходимым изъять все эти ключи из употребления...» [5].

Несмотря на большие затруднения в обеспечении войск всеми видами снабжения, в том числе и средствами связи, уже примерно в середине сентября 1914 г. командованию удалось обеспечить русские войска шифровальными средствами. 14 сентября

Ставка отдала распоряжение о том, что все военные приказы подлежат зашифрованию.

Принятая тогда шифрсистема представляла собой многоалфавитный шифр цифровой замены, в котором преимущество многоалфавитности почти сводилось на нет тем, что допускалось зашифрование нескольких букв подряд по одному алфавиту. Шифр этот представлял собой таблицу, состоявшую из девяти строк. В верхней строке был вписан русский алфавит, в следующих восьми — двузначные цифровые группы, расположенные и составленные в случайном порядке. Слева строки имели случайную нумерацию. При зашифровании строки использовались поочередно: 1, 2 и т. д. С помощью каждой строки шифровалось несколько букв открытого текста, их число определялось шифровальщиком. Для того чтобы адресат мог прочитать сообщение, в начале криптограммы пять раз проставлялась цифра, соответствовавшая количеству знаков, зашифрованных одной строкой. Когда в процессе шифрования шифровальщик хотел сменить это число, он вставлял в текст криптограммы пятизначную группу, элементами которой была одна и та же цифра, соответствующая новому числу знаков, шифруемых одной и той же строкой.

Этот шифр без труда был раскрыт уже 19 сентября 1914 г. начальником русского отделения дешифровальной службы Австро-Венгрии капитаном Германом Покорным с помощью анализа частот встречаемости букв, отслеживания структуры наиболее часто встречающихся в открытом тексте слов. Значительно упрощало задачу чередование в русских сообщениях участков открытого и шифрованного текста. Правда, вскоре было запрещено одновременное использование открытых и шифрованных текстов, но это было сделано слишком поздно, противник уже читал переписку, что оказало большое влияние на ход боевых действий.

Примерно в это же время для русского шифра был изменен ключ, сам же шифр остался неизменным. Новый ключ был определен Покорным в кратчайший срок из-за того, что одна из русских радиостанций передала зашифрованную по старому ключу криптограмму, переданную раньше и зашифрованную новым ключом.

В ноябре — декабре 1914 г. при передаче русских шифрсообщений уже ежедневно меняли порядок использования шифралфавитов, но по-прежнему сами эти алфавиты оставляли без изменений. И в результате дешифровальщики неприятеля постоянно читали шифрпереписку.

В этот же период русские сумели захватить ключи к немецкому шифру, что навело наконец русское командование на мысль о том, что многочисленные успехи противника в значительной степени являются следствием его информированности о содержании русской шифрованной переписки. В действие ввели новый шифр, причем на этот раз были изменены все его элементы. На некоторое время шифрпереписка русских армий оказалась для противника вне контроля, что лишило его очень важных сведений и во многом предопределило исход сражений в районе Бжезины в пользу русских армий. Кан этот эпизод комментирует как случайную догадку русских о необходимости смены шифра, которая помешала немцам «одержать полную победу, хотя им и удалось выбить из колеи хваленую военную машину русских. Никогда больше она не угрожала немецкой земле» [6].

Здесь Кан, как и во многих других местах своей книги, пытается провести мысль о том, что русские со своим интеллектом не способны конкурировать с западными специалистами. Он говорит, например, о том, что русские в 1915 г. использовали элементарный «шифр Цезаря», большое число таблиц которого, применявшихся в разных армиях, ежедневная смена ключей «поставили перед полуграмотными

мужиками непосильные для них задачи» [7]. Следует сказать, что применявшийся русской стороной шифр был достаточно далек от систем шифров, называвшихся «шифрами Цезаря», как это видно из описанных нами выше систем военных шифров России. Кроме того, в системе российской шифровальной службы работали, как читатель это мог уже увидеть, достаточно грамотные люди, хотя специалистов, как правило, не хватало. Конечно, эти системы русских шифров при том неизбежном обилии нарушений, которые во многом являлись следствием общей дестабилизации государственной деятельности в России в тот период вообще, естественно поддавались дешифрованию. Подчеркнем, однако, что в не меньшей степени и шифры западных специалистов того времени поддавались дешифрованию и вскрывали их с успехом русские криптографы — те самые «полуграмотные мужики», о которых с таким презрением пишет Д. Кан.

А. А. Маниковский, выпустивший в 1920 г. в Москве первую часть своего капитального труда «Боевое снабжение русской армии в войну 1914—1918 гг.», подчеркнул, что нельзя рассматривать вопросы технические — вооружение армии и флота — в отрыве от строя, существовавшего в России. Он открывал свою книгу словами: «Россия проиграла эту войну из-за недостатка боевого снабжения». Именно такое мнение сложилось в широких слоях общества на основании голосов, шедших из наших военных округов, из самой армии. Безусловно, это напрямую касалось и вопросов постановки криптографической защиты.

На грани крушения

Изучение документов и материалов, содержащих сведения по истории криптографической службы России, позволяет получить дополнительные знания

о политическом и экономическом кризисе, в который империя вступила уже в конце XIX столетия. Кризис этот постепенно углублялся и в период Первой мировой войны уже охватил все структуры государственного организма, что, естественно, не могло не отразиться на состоянии и настроениях всех частей общества. Убедительным доказательством этому служит то бесспорное обстоятельство, что в России росли и множились политические партии и группы, оппозиционные существовавшему режиму, включавшие представителей всех слоев населения — от аристократических партий либералов и кадетов и т. п. до партий, объединявших социальные низы.

Из письма Великого князя Александра Михайловича к Николаю II (от 4 февраля 1917 г.):

«Мы переживаем самый опасный момент в истории России: вопрос стоит, быть ли России великим государством, свободным и способным самостоятельно развиваться и расти, или подчиниться германскому безбожному кулаку, — все это чувствуют: кто разумом, кто сердцем, кто душою и вот причина, почему все за исключением трусов и врагов своей родины отдают свои жизни и достояние для достижения этой цели. И вот в это святое время, когда мы все, так сказать, держим испытания на звание человека в его высшем понимании, как христианина, какие-то силы внутри России ведут Тебя и, следовательно, Россию к неминуемой гибели...

Теперь... ни один министр не может отвечать за следующий день, все разрознены; министрами назначаются люди со стороны, которые никаким доверием не пользуются и, вероятно, сами удивляются, что попадают в министры... их назначение для общего дела приносит только вред, их поступки граничат с преступлением...

Твои советники продолжают вести Россию и Тебя к верной гибели...

Недовольство растет с большой быстротой, и чем дальше, тем шире становится пропасть между Тобой и Твоим народом...

Как это ни странно, но правительство есть сегодня тот орган, который подготавливает революцию, народ ее не хочет, но правительство употребляет все возможные меры, чтобы сделать как можно больше недовольных, и вполне в этом успевает. Мы присутствуем при небывалом зрелище революции сверху, а не снизу» [8].

М. В. Родзянко (1859—1924) — один из лидеров партии октябристов, крупнейший помещик России, с ноября 1912 г. бессменный председатель IV Государственной думы — в своих воспоминаниях «Крушение империи» писал о том, что вся внутренняя политика, которой неуклонно держалось императорское правительство с начала войны, неуклонно и методично вела к полной государственно-хозяйственной разрухе. Но и после свержения самодержавия, в период деятельности Временного правительства, этот кризис продолжал углубляться, разрушая, кроме прочего, все государственные институты.

Этот кризисный процесс не мог не отразиться и на деятельности криптографической службы. Довольно припомнить министерскую чехарду в тех ведомствах, куда она входила. Так, лишь с осени 1915 г. по осень 1916 г. сменилось пять министров внутренних дел: князя Щербатова сменил А. Н. Хвостов, его сменил Макаров, Макарова — Хвостов-старший и последнего — Протопопов. На долю каждого из этих министров пришлось около двух с половиной месяцев управления. За это же время было три военных министра: Поливанов, Шуваев и Беляев. Аналогичная картина наблюдалась и в МИД. Можно ли говорить при таком положении вещей о сколько-нибудь серьезной и последовательной работе этих министерств в целом?

Вполне естественно, что и в среде криптографов как в капле воды отразилась сложившаяся ситуация. Демократические идеи и настроения проникали всюду, в том числе в святая святых государственной власти — Департамент полиции. Некоторые его сотрудники сочувственно относились к революционерам, при возможности старались им помочь избежать ареста, скрыть улики во время обысков и т. п. Перед нами текст одной из докладных заведующему ДП от января 1916 г., которая, на наш взгляд, весьма любопытна. Некто пишет:

«Ваше превосходительство!

Вы удивляетесь, что секреты Департамента полиции являются достоянием публики, а дело очень просто: находящиеся на службе в ДП писцы и чиновники постыдным образом продают эти тайны. Удачно удален Зыбин, теперь не мешало бы заглянуть в действия Крылова, последователя некогда уволенного Циппа. Крылов (старший) во всех отделах ДП имеет своего человека, если же дело касается до другого учреждения, то составляет подложные документы и является как уполномоченный ДП, путается с жидами, не имеющими прав на жительство в столице, сообщая им секретные циркуляры...» [9].

В нашу задачу не входит выяснять что-либо подробнее об упомянутых в этой докладной записке лицах. Их фамилии, кроме фамилии Зыбина, нам неизвестны, но это и не суть важно. Также не особенно важно сейчас для нас и то, что традиция «Народной воли», имевшей своих агентов среди сотрудников царской охранки, вероятно, была продолжена ее преемниками и, как результат, в революционные организации в той или иной мере попадала информация о ближайших планах органов полиции и жандармерии. Принадлежал ли к числу таких информаторов И. А. Зыбин или он просто сочувствовал движению, мы также не знаем. Следует отметить другое: революционный процесс шел активно, он уже захватил все структуры общества, и общество раскололось. Кстати, когда архивы охранки начали изучаться в 1917 г. специальной комиссией Временного правительства, то в списках лиц неблагонадежных оказалась и фамилия другого известного нам криптографа — В. И. Кривоша-Неманича.

И вот удивительное дело! Видя эту надвигающуюся лавину чудовищного хаоса, видя безразличие к судьбе государства высших сановников и осознавая трагедию разрушающегося государства, на его защиту встали рядовые государственные служащие. Работники криптографической службы России в том числе.

5 октября 1917 г. управляющий шифровальной частью МИД, член Цифирного комитета Юрий Александрович Колемин подал подготовленную им совместно с его помощником М. Н. Чекмаревым докладную записку на имя министра иностранных дел Сазонова [10].

Эта записка, по словам Колемина, писалась в момент, когда специальная служба России «оказалась на грани крушения». Поэтому Колемин считал совершенно необходимым безотлагательную ее полную реорганизацию. Он писал: «Отделение (шифровальное. — *Т. С.*) теперь функционирует. Но я не вижу возможности, чтобы оно оказалось впоследствии жизнеспособным без проведения в жизнь указанных мною принципов, которые, по моему глубокому убеждению, могут быть изменены в частностях, но не по существу». Иначе дело идет «к неминуемому банкротству, последствия которого могут быть для нас неисчислимыми». Записка Колемина представляет чрезвычайный интерес и по своему глубокому политическому и философскому содержанию, выходящему далеко за рамки обычного служебного документа, может быть поставлена в один ряд с работами выдающихся государственных и общественных деятелей России того времени. Эта записка показывает, что в переломный

для государства революционный период о его судьбе, о сохранении базовых структур реально заботились отнюдь не верховные власти. Колемин четко формулирует мысль о том, что криптографическая служба всегда являлась одной из важнейших структур государства. Ее работникам вверяются важнейшие государственные тайны и секреты. Это обстоятельство обусловливает необходимость постоянной государственной заботы о стабильности и надежности работы этой службы. Впервые Колемин ставит вопрос о создании для этого необходимых гарантий, как материальных, так и моральных.

Необходимость перестройки деятельности криптографической службы в общем понимали и руководители министерства. Но вопрос пытались решить лишь формально, хотя и был подготовлен проект, созданный наспех, в котором была сделана попытка скопировать подобную немецкую специальную службу. В этих условиях и появился документ Колемина.

В своей записке Ю. А. Колемин указывает, что работники криптографической службы всегда считаются как бы людьми «второго сорта», «рядовыми чиновниками», что особенно бросается в глаза на фоне привилегированных дипломатов. Но между тем этим людям «второго сорта» «шифры и вместе с ними все государственные тайны даются прямо в руки... Но это еще не все. Получив шифры и государственные тайны в свои руки, эти люди навсегда замыкаются в... экономические рамки ничтожного оклада. Прозябание на местах и беспросветная будущность — вот к чему сводится горизонт этих людей». Колемин пишет:

«На каком именно основании тут предполагалось бы, что они должны чувствовать особую с интересами своего дела солидарность, остается неизвестным, за исключением только того случая, если удалось бы набрать

полный штат таких идеалистов, добросовестность коих можно было бы безнаказанно эксплуатировать, что, очевидно, не входит в расчеты законодателя. Я не отрицаю, что во время войны можно и на самом деле рекрутировать такой благонадежный кадр даже на основании только что изданного положения. Стоит только обратиться, как это и делается, к раненым офицерам, числящимся на действительной службе, чтобы иметь людей, исполняющих свой воинский долг хотя бы и в тылу. Но ведь такое состояние — не вечно. Когда-нибудь да кончится война и настанет час демобилизации. И в этот час наши шифровальщики перестанут быть прикомандированными к нам офицерами и очутятся всецело в условиях „делопроизводителей" VIII и VII разряда шифровального отделения».

Достигается ли необходимая цель копированием иностранных образцов, слепым, автоматическим перенесением их на русскую почву? Ответ Колемина:

«Я считаю своею обязанностью высказать глубокое мое убеждение, что эта цель не достигается вовсе. Я осмеливаюсь утверждать, что здесь имеется одна только неизбежность провала всего нашего дела о шифрах и возможность нанесения нашим интересам непоправимого вреда.

На самом деле, при осуществлении задания, заключающегося в перенесении на русскую почву иностранных образцов, хотя бы и хороших, нельзя упускать из виду необходимости согласовать их с нашей социальной восприимчивостью, которая слагается из целой сети факторов, от грубых материальных условий до нашего сокровенного психического облика включительно. Иначе материальная копия может вылиться в карикатуру».

Ю. А. Колемин дает глубокий сравнительный психологический портрет специалиста-немца и специалиста-русского. Вот образец его рассуждений:

«Германская душа, исторически выработанная из векового кругозора феодализма и тысячами нитей связанная с последним и питающаяся из него, — эта душа везде заявляет о себе в присущем немецкой жизни кастовом начале, устоявшем и по сей день против напора демократической мысли. Слишком резкие внешние формы этого начала, конечно, успели стушеваться в Германии, но, по существу, в немецкой социальной психологии это начало пребывает. Немец всегда входит в какой-нибудь весьма резко ограниченный социальный круг, имеющий свои собственные понятия о чести. Немецкая душа не мирится с демократическими идеями об общечеловеческом достоинстве, а мыслит человеческое достоинство лишь в рамках особого социального круга... И одновременно немецкая душа устроена так, что не будет искать почестей, ни иного удовлетворения, кроме тех, которые предназначаются ей внутри предопределенного круга, — прежде всего, конечно, того, в котором родился немецкий человек, а затем и того, в котором он живет по сложившимся обстоятельствам. Для немца существует известный кастовый горизонт и он не чувствует побуждений возвыситься над ним и не проявляет никаких несовместимых со своим социальным положением вожделений».

Ясно, что на таком фоне можно найти для какого угодно дела необходимую уже природно организованную социальную силу. «Поэтому,— рассуждает Колемин, — если в каком-нибудь германском ведомстве, например в ведомстве иностранных дел, потребуется устроить для шифровальной работы какой-нибудь особый штат канцелярских чиновников, людей «второго служебного ранга», в сравнении с дипломатами, у коих они состояли бы в подчинении, исполняя для них только черную работу без каких-либо видов на участие в их служебных и социальных преимуществах, но все-таки абсолютно преданных своему делу, ставящих высоко свою корпоративную

честь и оправдывающих оказываемое им доверие, — сейчас же немецкая жизнь дает возможность рекрутировать в соответствующих социальных слоях целый кадр «субалтернбеамтен» в каком угодно числе. Таким образом, в условиях германской жизни этот институт имеет свое оправдание».

Колемин представляет себе этот образец скопированным и перенесенным в русскую среду. Какой получится результат? А вот какой:

«Прежде всего глубоко демократическая русская социальная масса не имеет таких специальных общественных слоев, которые могли бы по внутреннему признаку своего мировоззрения служить преимущественным центром набора искомого кадра чиновников. Для русского чувства нет никаких каст и никакого социального достоинства, кроме достоинства общечеловеческого, и распределение людей по разрядам у нас будет поэтому всегда случайным, основанным на признаках внешних. И никакие человеческие силы не заставят русского человека ограничить себя в смысле низведения своей внутренней нравственной удовлетворенности до узких пределов того круга, в который он насильственно и материально замыкается. Русские идеалы всегда безмерны, и в своем роде это проявляется и в сфере нашего материального и социального существования.

И вот наши русские специалисты-криптографы будут попадать в безвыходные условия второразрядной службы со всеми внутренними предпосылками неудовлетворенности. Они будут принадлежать к хорошо известному классу „вечно обиженных"...»

Мы думаем, что читатель оценит приведенную цитату по достоинству, не забывая, что автор этих строк отнюдь не философ или писатель, а всего лишь чиновник. И пишет он не научный труд или роман, а деловой документ, то есть, казалось бы, сухую бумажку. Вероятно, все дело в том, что этот

чиновник обладал по-настоящему тем самым «государственным мышлением», которое так часто отсутствует в необходимых случаях, широчайшей эрудицией и в конечном счете истинным чувством человеческого достоинства, которое не позволяет смириться с тем, что бессмысленно и бездумно уничтожается дело, которому ты посвятил жизнь, дело, создававшееся трудами целых поколений.

«Но если бы и устояла честность,— продолжает Колемин, — *то рвение к делу вряд ли устоит. А создавать организацию, в которую заложено игнорирование стимулов производительности труда — дело безнадежное. Из такого учреждения, при наступлении нормальных условий, лучшие силы уйдут, а с остальными оно будет влачить свое жалкое существование до краха... и притом до такого краха, который при совершившемся уже приспособлении всего Министерства к новому порядку ведения нашей секретной переписки может обойтись очень дорого».*

Колемин дает конкретные предложения для организации корпорации работников криптографической службы, деятельность которых была бы обусловлена соответствующими гарантиями как экономического, так и морального свойства, и, что не менее важно, корпорации, свободной от протекционизма и других пороков.

Так, для работников специальной службы МИД Колемин предлагает следующее. Прежде всего, эти работники постоянно должны себя чувствовать «особо доверенными чинами». Почетное их положение должно быть обеспечено в такой исключительной мере, чтобы они не чувствовали обиды в этом отношении при сопоставлении себя с дипломатами, которые проходят мимо них по служебной лестнице к высшим почестям и окладам. И это достижимо только при создании таких корпоративных условий, которые явно и недвусмысленно подчеркивают в отно-

шении служебных прав то исключительное доверие, которым пользуются эти чины. Тогда и эта служба в глазах всех будет считаться показателем исключительного достоинства того лица, которое ее отправляет. Для насаждения и укрепления этого корпоративного начала требуется установление внутри корпорации, с одной стороны, строгого принципа старшинства, исчисляемого со дня поступления, а с другой — невозможность попасть в нее иначе, как на младшую должность и притом только с согласия самой корпорации, известным образом и при известных гарантиях выраженного. Внутри корпорации должны были бы существовать, во-первых, особый товарищеский дисциплинарный суд и, во-вторых, отдельный от общеминистерского товарищеский суд чести. Заграничные назначения следовало бы нормировать так, чтобы в них широким образом проявлялось бы самоопределение корпорации и чтобы одновременно исключен был всякий произвол и обеспечено было назначение подходящего кандидата и с точки зрения служебной. Порядок периодического возвращения из-за границы в центр или поддержание связи заграничных чинов со своей центральной корпорацией должны быть так или иначе обеспечены. Необходимо было бы затем выработать особую формулу присяги, приводить к ней членов этой корпорации и т. д.

Наконец, материальные перспективы этих чинов должны были бы нормироваться таким образом, чтобы отсутствие иерархических служебных повышений находило равноценную компенсацию в постепенном росте окладов по принципу выслуги лет, причем можно было бы вносить сюда и некоторую поправку в смысле влияния трудолюбия и исполнительности на срок выслуги. Срок выслуги должен был бы быть установлен такой, который оставлял бы место более осязательной надежде на скорое материальное улучшение, т. е. не слишком продолжительный, на-

пример каждые три года. Лучше, казалось бы, в этом отношении уменьшить прибавку при более скорой выслуге, чем увеличить ее при выслуге большой. Колемин пишет: «Не следовало бы, кажется, установить предела для прибавок, а нормировать их таким образом, чтобы каждый из этих чинов при поступлении в молодом возрасте мог бы надеяться к концу своей службы иметь оклад, соответствующий, например, жалованью советника миссии при посольстве...» Колемин считает, что не следует открывать доступ в корпус лицам слишком молодым, ввиду необходимости базироваться при принятии какого-нибудь кандидата на вылившийся уже в определенные очертания его нравственный облик и на известное уже прошлое человека. Возраст мог бы быть установлен, например, в 22—25 лет. Необходимо было бы также установить предельный возраст службы в корпусе, например 60 лет. При таком порядке вещей наиболее длительный возможный срок службы внутри корпуса определился бы в 35—36 лет, что в бюджетном отношении дает 11 прибавок за трехлетние выслуги. Если бы каждая прибавка была определена в 750 рублей, то получилось бы, что, начав службу с годовым окладом 1800 рублей, криптограф выходил бы на пенсию, получая 9800 годовых.

Мы так подробно приводим здесь содержание докладной записки Колемина потому, что, как можно видеть, она не потеряла своей актуальности и ныне. Заключает свою докладную Юрий Александрович так: «Я счел своей обязанностью соорганизовать при деятельной поддержке моего помощника М. Н. Чекмарева и при содействии всего личного состава новое Отделение согласно требованиям Министерства, и я вложил в это дело всю свою душу. Но я считаю необходимым почтительнейше ходатайствовать о том, чтобы при возможном банкротстве всего этого дела в будущем, на случай непризнания основательными выраженных мною взглядов, я не был бы

тогда признаваем как организатор ответственным за его неминуемое, на мой взгляд, крушение».

Деятельность Ю. А. Колемина имела активную поддержку среди служащих шифровального отдела и созданного для обработки внутренней шифрпереписки шифротделения МИД. 8 октября 1917 г. состоялось очередное общее собрание служащих шифровального отделения, порядок дня которого, записанный в протокол, гласит: «1) выборы двух делегатов в междуведомственное совещание для обсуждения проекта Ю. А. Колемина об организации шифровальной службы, 2) выборы пяти лиц в комиссию по организации шифровальной службы, 3) обмен мнениями и текущие дела».

Собрание постановило выразить благодарность от имени всех служащих шифровального отделения Юрию Александровичу Колемину и Михаилу Николаевичу Чекмареву за их труды по улучшению деятельности отделения и условий службы. 19 октября 1917 г. каждый из чиновников шифровального отделения МИД подписал текст присяги, которую составил Ю. А. Колемин для криптографов. Вот ее текст:

«Я, нижеподписавшийся (следует звание, имя и отчество. — *Т. С.), вступая в исправление моих обязанностей, обещаю, что буду всегда свято и ненарушимо соблюдать перед посторонними лицами молчание о всех материалах, при помощи которых я буду исполнять возложенное на меня ведение секретной переписки Министерства иностранных дел. Обещаю, что буду свято и ненарушимо сохранять в тайне от посторонних лиц все сведения, которые будут проходить через мои руки и перед глазами моими при ведении этой секретной переписки. Обещаю, что буду всегда осторожно, обдуманно и предусмотрительно обходиться с вверенными мне тайными материалами, обещаю, что буду всегда осторожно, обдуманно и предусмотрительно относиться к тем условиям, при которых я могу с со-*

служивцами по отделению говорить об имеющихся у нас профессиональных сведениях, дабы всеми силами моими содействовать ненарушимости и непроницаемости этих тайн, составляющих собственность не мою, а доверяющего их мне Министерства, ведающего при помощи их, через меня, интересами моего Отечества. Обещания сии подкрепляю благородным и честным моим словом.

Петроград 19 октября 1917 г.»

Для каждого типографским способом был отпечатан отдельный экземпляр присяги. Служа своему Отечеству, своей подписью, а также честным и благородным словом скрепили присягу 23 человека.

До Октябрьской революции оставалось менее недели.

Глава четырнадцатая

РАЗЛОМ

Пролетарская революция 1917 г. круто изменила судьбу России. Ломке, разрушению подверглись вековые государственные устои, традиции, отношения. Крушились судьбы людей. Над гигантскими просторами России реял окровавленный ангел.

Разрушению или коренной перестройке подверглись все без исключения государственные службы и институты. Не составила исключения и криптографическая служба России.

Вероятно, предполагалось, что в новом государственном механизме ей предстояло занять соответствующее и весьма важное место. Однако в первые годы Советской власти государство располагало лишь тем арсеналом материальных средств и профессиональных кадров, которые остались от прежней царской специальной службы и не были на стороне и в распоряжении белого движения. Не имея возможности в условиях начавшейся Гражданской войны уделить необходимое внимание созданию новой специальной службы, Советское государство было вынуждено пользоваться старыми царскими кодами и шифрами, располагать весьма скудными кадрами специалистов. Большинство криптографов старой службы враждебно отнеслись к победе Октябрьской революции. Те же специалисты, которые перешли на сторону Советской власти, в большинстве своем ока-

зались разбросанными по различным полевым штабам Красной Армии, возглавляя в них шифровальные группы.

В руках Советской власти оказались почти все архивные и действующие шифрдокументы бывших цифирных отделов царской России. Однако эти документы были хорошо известны специалистам-криптографам, оказавшимся во вражеском лагере, и поэтому, хотя и стали активно применяться, не могли служить действенным средством защиты оперативной информации.

К сожалению, многие ценнейшие материалы Временного правительства России, архивов командующих вооруженными силами белых армий, включающие и документы тайной переписки и шифров, были вывезены из России. То же самое следует сказать об архиве, включающем документы царской охранки с 1895 г. по 1917 г. Они были переданы бывшим русским послом в Париже известному американскому разведчику и промышленнику Герберту Гуверу. В настоящее время все эти документы и архивы находятся в Гуверовском институте войны, революции и мира при Стэнфордском университете в Калифорнии. Кстати сказать, ведущим экспертом этого института по «русскому вопросу» вплоть до самой своей смерти был А. Ф. Керенский.

Крайне плохо обстояло дело с дешифрованием иностранной и военной переписки. В Красной Армии не было организованной дешифровальной службы, так как созданные при штабах шифргруппы имели главной задачей создание шифров и защиту ими секретной переписки.

Белая армия в основном унаследовала шифровальные, радиотехнические и иные средства, а также опыт, традиции и кадры специалистов криптографической службы царской России. Попытаемся более подробно осветить положение, в котором находилась криптография России в период Гражданской войны. О криптографической службе белогвардейцев дают представление архивы правительства А. В. Колчака, находящиеся в Государственном архиве Российской Федерации (ГАРФ) в Москве.

Радиосвязь и радиоразведка у белогвардейцев

Как известно, в ноябре 1918 г. в Сибири, на Урале и на Дальнем Востоке установилась власть правительства адмирала А. В. Колчака, которому активно содействовали командующие войсками Антанты в Сибири — французский генерал М. Жаннен, американский генерал У. Гревс, американский адмирал О. Найт, английские генералы А. Нокс и Д. Уорд.

Основной базой Колчака, получившего всю полноту власти, стала Сибирь. Урал, Оренбургская губерния и Уральская область являлись фронтовой и прифронтовой зонами, Дальний Восток, номинально находившийся под властью Колчака, был занят американскими и японскими войсками.

К весне 1919 г. Колчак создал значительные вооруженные силы, включавшие Западную, Сибирскую, Оренбургскую и Уральскую армии, численностью до 400 тысяч человек, в том числе около 30 тысяч офицеров, на фронте — 130—140 тысяч штыков и сабель. 30 апреля 1919 г. власть Верховного правителя признало «временное правительство Северной области».

10 июня Колчак назначил Н. Н. Юденича главкомом белогвардейских войск на северо-западе России, 12 июня о своем подчинении Колчаку заявил А. И. Деникин. Правительство США передало Колчаку кредиты, предназначавшиеся ранее Временному правительству, предоставило (наряду с Великобританией и Францией) значительное количество оружия,

обмундирования и т. п. Колчак располагал золотым запасом России, захваченным в Казани белочехами в ходе мятежа чехословацкого корпуса в 1918 г.

Известно, что Колчаком были созданы правительство (председатель П. В. Вологодский), совет верховного правителя («звездная палата»), правительствующий сенат, департамент милиции и государственной охраны, различные политические органы, призванные осуществлять идеологическую и осведомительскую работу. Основные задачи этих органов сводились к «содействию, осведомлению и подъему духа» среди белогвардейских войск, а также среди населения, организации пропаганды и агитации, направленных на подрыв Красной Армии и советского тыла. Общее руководство этими органами осуществлял «Осведверх» (центральный осведомительный отдел, образованный при главном штабе главковерха весной 1919 г.). Во второй половине 1919 г. «осведорганы» существовали во всех войсковых соединениях, а также в тыловых округах. Наряду с ними идеологическую работу вели: отдел печати при канцелярии «омского правительства», состоявший из российского телеграфного агентства, пресс-бюро, бюро иностранной информации и др. В их распоряжении были достаточно мощные радиостанции, радиотелеграф, которые использовались для передачи и приема информации.

Частично информация, интересовавшая руководителей белого движения, добывалась агентурным путем. В задачу агентов Колчака входило получение не только собственно военной информации, но и сведений, касающихся различных сторон жизни Советской республики. Однако добываемые агентурным путем данные не могли идти ни в какое сравнение с информацией, получаемой белыми из перехвата и обработки советских радиосообщений. В определенной степени об этом свидетельствует, например,

шифртелеграмма Колчака русскому посланнику в Греции от 5 апреля 1919 г.:

«Прошу передать Наратову: давно не имеем от Вас сведений о положении дел на юге России. Последние сведения относятся к середине февраля. Единственным источником информации нам служат перехватываемые большевистские радио. Не откажите осветить нам современную военно-политическую обстановку на Дону и в Екатеринодаре» [1].

Радиоразведка и радиоперехват использовались белогвардейцами очень активно и не без успеха. Радиоразведка оформилась в России организационно и получила развитие еще в годы Первой мировой войны и велась по трем линиям: 1) Главного (разведывательного) управления Генерального штаба, которое осуществляло радиоперехват телеграмм радиостанций командования германских и австро-венгерских армий; 2) штаба Верховного главнокомандующего, ведущего перехват сообщений военно-полевых радиостанций на фронтах; 3) морского Генерального штаба, который ведал перехватом шифринформации от военно-морских радиостанций противника на Балтийском и Черном морях. Главному управлению Генерального штаба принадлежали Царскосельская, Московская, Николаевская, Тверская, а также Киевская, Рижская, Одесская, Житомирская и другие радиостанции, на которых велся систематический перехват неприятельских телеграмм. Многие из этих радиостанций, их материальные средства и кадры полностью или частично оказались в руках белой гвардии.

Кроме радиостанций военного ведомства, постановлением министра внутренних дел по телеграфной части от 2 февраля 1908 г. в империи было предусмотрено два вида радиотелеграфных станций: а) станции специального назначения, используемые, как это следует из названия, специальными ведом-

ствами, и б) станции общего пользования, то есть такие, которые являлись открытыми для приема телеграмм от публики. Функции организации радиотелеграфных станций, приема и передачи всех радиотелеграфных сообщений были сосредоточены в Главном управлении почт и телеграфов Министерства внутренних дел. Радиотелеграфные станции были рассредоточены по территории страны. Многие из них в 1918—1919 гг. также были в распоряжении белых армий.

По данным, представленным Колчаку Министерством морского флота в феврале 1919 г., в ведении продолжавшего существовать Главного управления почт и телеграфов находилось девять действовавших стационарных радиостанций, радиус действия которых определялся соответствующей их мощностью, колебавшейся от 1,5 до 35 киловатт [2].

В Омске, Чите, Хабаровске, Екатеринбурге были установлены радиостанции мощностью до 35 киловатт, которые использовались как для передачи информации, так и для перехвата открытых и шифрованных сообщений. Связь с Деникиным поддерживалась по линии связи Омск — Таганрог. Радиотелеграф на юге России был установлен также в Гурьеве, Новороссийске, Николаеве, Севастополе.

Из числа радиостанций Военного ведомства наиболее мощной была Читинская радиостанция, принимавшая депеши из Владивостока. Военная радиостанция во Владивостоке (на острове Русском) еще в октябре 1918 г. была передана американцам для установки и использования их собственной аппаратуры на период военных действий. Они обязаны были обеспечить связь с европейской территорией России и после окончания войны передать станцию Российскому правительству. Американским морским командованием во Владивостоке была введена в действие «отправительная» радиостанция, состоявшая из «двух отдельных отправителей» мощностью в 25 и

65 киловатт, а также приемная радиостанция. Как было предусмотрено русско-американской договоренностью, американцы должны были довести общую мощность этой радиостанции до 300 киловатт. Однако каких-либо мер для ускорения ввода этой станции на полную мощность они не предпринимали.

Значительной мощностью обладала радиостанция Колчака, расположенная в Омске, — месте непосредственного пребывания Верховного правителя. Она была в свое время построена французами. У колчаковцев имелась возможность с помощью этой радиостанции сноситься с Архангельском, где располагалась штаб-квартира временного правительства Северной области, главой которого с мая 1919 г. стал генерал Е. К. Миллер, а также с Севастополем — для связи с армиями, действовавшими на юге России. Активно поддерживалась связь с Парижем, Стокгольмом, Христианией (в 1624—1925 гг. название г. Осло), Гельсингфорсом, Афинами, Лóндоном, Токио.

Созданное Юденичем 11 августа в Таллине «северо-западное правительство» для передачи информации также использовало мощные радиостанции (до 35 киловатт), установленные союзниками в Ямбурге и Таллине. Они активно работали до декабря 1919 г.

Организация надежной шифрсвязи с учетом ее огромного значения, преодоление возникающих сложностей с передачей и приемом сообщений на большие расстояния были предметом постоянного внимания и забот белой гвардии. Об этом наглядно свидетельствуют приводимые ниже данные.

Так, управляющий Морским министерством 2 февраля 1919 г. докладывал Колчаку:

«Имею честь препроводить копию радио из Архангельска от генерал-губернатора генерала Миллера, принятую случайно на французской радиостанции нашими морскими телеграфистами в крайне искаженном виде вследствие того, что во время

работы постоянно прерывали другие радиостанции. Эта радио передана Архангельском на радиостанцию в Дудинке (устье Енисея), откуда еще не прислана в Омск. Сегодня Дудинка запрошена мною» [3].

Дудинка принимала радиограммы из Архангельска через Диксон.

Колчаку в ряде случаев было проще сообщаться через Министерство иностранных дел, чем напрямую в регионы. Это же относится и к другим руководителям белого движения. Не имея возможности привести здесь большой фактический материал, мы ограничимся лишь одной шифртелеграммой посла в Париже В. А. Маклакова Колчаку от 10 мая 1919 г.:

«Генерал Миллер просит передать Вологодскому... Радио... отправлена 3-го мая, была повторена 6-го мая Омскому и получена квитанция. Радио... отправлена 7-го мая. Омск дал квитанцию 8-го мая. Телеграмма очень важная. Маклаков» [4].

Весной 1919 г. у колчаковцев возникает ситуация, когда «срочная потребность противобольшевистского фронта в мощной радиостанции не может быть удовлетворена получением таковой из-за границы» [5]. Не было денег. Тогда-то и возбуждается вопрос о передаче Владивостокской радиостанции, временно находившейся в ведении американцев, Российскому правительству Колчака. При этом полагалось крайне желательным получить в первую очередь 25-киловаттную радиостанцию с тем, чтобы срочно перевести ее в Томск для организации непосредственной связи со штабами Деникина и Юденича. Об этом писал военный министр управляющему Министерством иностранных дел И. И. Сукину в июне 1919 г. [6].

Министерство морского флота также обращается к Сукину с просьбой о необходимости передачи

мощной морской радиостанции во Владивостоке русскому морскому ведомству. В справке, составленной министром морского флота, говорится: «Учитывая... невыгодность положения русского правительства в смысле как монополизации международных сношений в руках иностранного правительства, так и возможности территориальных захватов в будущем, настоятельно необходимо ликвидировать это положение и вернуть радиостанцию Русскому правительству» [7]. Ранее, как мы писали, было предусмотрено возвращение этой радиостанции России после конца войны, однако положение изменилось, а формальный повод к этому был: мир уже был заключен, соответствующий документ скрепили подписи командующего Сибирской флотилией и Главнокомандующего флота США.

Возвращая себе радиостанцию во Владивостоке, Колчак стремился решить и некоторые другие задачи. Интересен в этом отношении доклад Колчаку его военного министра от 3 июня 1919 г. Министр считал, что если радиостанцию колчаковцы себе вернут, то, во-первых, будут иметь надежную радиосвязь базы снабжения армии и флота (во Владивостоке. — *Т. С.*) с правительством, «что особенно в настоящее время при частых перехватах действия проволочного телеграфа является чрезвычайно важным», во-вторых, иметь быструю и надежную связь с правительствами союзных государств, в-третьих, иметь радиосвязь «вне зависимости от тех или иных политических группировок» [8]. При этом министр подчеркивал необходимость точного оговаривания тех пунктов по побережью Тихого океана, через которые передача радиограмм соответствующим правительствам может быть произведена в кратчайший срок.

Колчак считал необходимым вернуть себе радиостанцию со всем оборудованием, установленным на ней американцами, и принять все возможные меры против возможности ее захвата не только Красной

Армией, но и каким-либо иностранным государством.

К весне 1919 г. вопрос о налаживании связи приобретает для армий Колчака первостепенное значение. В Лондон направляется делегация во главе с генералом Головиным для переговоров о немедленной постройке в России дополнительной радиостанции. И вот 27 мая 1919 г. посол в Париже Маклаков передает по телеграфу:

«Генерал Головин, находящийся в Лондоне, сообщает, что англичане согласны установить большую радиостанцию в Екатеринодаре для прямых сношений с Омском, Парижем, Лондоном и приступить к работам немедленно при условии наличного платежа около 10 000 фунтов. Установка в кредит возможна, но приступ к работе затянется. Прошу срочного отпуска денег или согласия на установку в кредит» [9].

А денег не было. Солидарность капиталистов имеет, как известно, свои, только ей присущие особенности. Капиталисты не были бы капиталистами, если одновременно не пытались бы использовать слабость бывшего партнера в корыстных целях. Бывшие союзники России по мировой войне считали деньги. Первый шаг на этом пути уже был сделан в конце 1917 г., когда Англия и Франция заключили 10 декабря секретное соглашение о разделе европейской части нашей страны на «зоны действия». Несколько позже была достигнута договоренность, что Сибирь и Дальний Восток являются «зонами действия» США и Японии. Генерал Д. Л. Хорват, один из руководителей белого движения на Востоке страны, хорошо знавший закулисную сторону «помощи» бывших союзников, позже признавал: «Все наши бывшие союзники преследовали в борьбе с большевиками собственные эгоистические цели. Но

никто не помогал России. Сильная Россия никому, кроме русских, не нужна».

Исход войны не позволил Колчаку ввести в действие радиостанции особой мощности.

Нельзя не отметить широкое применение в белых армиях шифрованных передач по радио и для управления войсками при помощи стационарных и полевых радиостанций. Такими радиостанциями были снабжены армии, корпуса, дивизии, конные отряды, военные корабли. В специальных подразделениях радиосвязи и радиоразведки перехватываемые открытые и шифрованные сообщения анализировались, на их основе составлялись ежедневные сводки и схемы радиосвязи советских военных частей. В частности, активную радиосвязь и радиоразведку вели Западная и Уральская армии Колчака. Большое число радиостанций действовало в регионах Уфы, Уральска, тесная связь поддерживалась с Астраханью, Гурьевом, Красноводском и Баку. Против организованного в августе 1919 г. Туркестанского фронта под командованием М. В. Фрунзе велась радиоразведка в Гурьеве, Форте Александровском. Активно работала радиосвязь между Колчаком и Деникиным на линии Тифлис — Баку.

Организация шифровального дела у Колчака

Шифровальное дело было поставлено в белой армии достаточно солидно: сохранялись традиции, техническая база царской шифровальной службы, частично кадры шифровальщиков, криптографов и переводчиков. Цифирное отделение, как оно продолжало именоваться, находилось в министерстве иностранных дел колчаковского правительства и подчинялось непосредственно начальнику первого департамента этого министерства. Широко использовались старые шифры и коды, оставшиеся с прежних вре-

мен. Вместе с тем создавались и новые шифры. Так, 2 февраля 1919 г. управляющий цифирным отделением писал, обращаясь к начальству: «...ввиду скомпрометированности старых ключей Министерства иностранных дел, цифирное отделение приступило к составлению новых секретных ключей для телеграфных сношений заграничных представителей с центральными установлениями министерства и между собой» [10].

В том же месяце цифирным отделением Министерства иностранных дел были изготовлены два «перешифровальных ключа» (№ 560 и 570), введение которых в действие, по мнению изготовителей, «вполне обеспечивало бы сохранение тайны секретной корреспонденции министерства». Издавались изготовленные ключи типографией военной газеты «Русская армия», где соблюдались соответствующие условия для сохранения тайны издания. Перед изготовлением шифров или ключей типография определяла сметную их стоимость. Эти данные сообщались типографией в цифирное отделение, и его управляющий составлял прошение об отпуске денег. Денег же было очень и очень мало.

В архиве Колчака сохранились лишь единичные образцы использовавшихся шифров. В основном это были буквенно-слоговые разнозначные таблицы замены. Срок действия таких шифров определялся в полгода. Это были типичные шифры, широко применявшиеся в белых армиях. Как известно, криптографическая стойкость их невелика. Такие шифры раскрываются на материале в несколько десятков знаков. Кроме таких шифров в белой армии использовались и коды объемом в несколько тысяч словарных величин. Коды были в основном алфавитные, редко использовались неалфавитные небольшого объема, в которых имелось некоторое число пустышек. Такие коды, даже при соблюдении всех правил пользования, не являются шифрами высокой стойкости и могут раскрываться на материале достаточного объема. Поскольку шифровались телеграммы сравнительно большой длины и массив этих телеграмм, зашифрованных одним и тем же кодом, был достаточно велик, при организации регулярного перехвата таких шифртелеграмм дешифрование их было сравнительно простой задачей. Она облегчалась еще тем, что шифровалась не вся телеграмма целиком, а только отдельные ее куски. Хотя мы знаем, что еще в период Первой мировой войны это было категорически запрещено.

Определить виды использовавшихся шифров в значительной степени помогают ошибки в ведении секретного делопроизводства. Как показывают изученные документы, в начальный период при первых победах на фронтах ошибки в работе с шифрдокументами почти не допускались. Однако по мере ухудшения военной обстановки допускалось все больше небрежности. И вот теперь в делах вместе с открытыми текстами сообщений мы находим подшитые криптограммы, что категорически запрещалось всеми инструкциями. Открытые тексты обычно уже подготовлены для зашифрования, то есть разделены на словарные величины вертикальными линиями. Эти данные позволяют восстановить словари использовавшихся шифров, например для линий связи с иностранными представительствами в 1919 г.

Как мы указывали выше, разработка и издание таких шифров велись постоянно. Например, 17 июля 1919 г. цифирным отделением МИД была завершена работа над изданием нового «секретного ключа» (кода), объемом 8000 словарных величин, а через неделю еще одного — новой буквенно-слоговой таблицы.

В качестве агентурных шифров белая гвардия использовала и шифры перестановки, а именно лозунговые шифры вертикальной перестановки.

Сохранившиеся сведения о шифрах, применявшихся в белых армиях, хотя в сущности и невелики, между тем достаточны для того, чтобы в настоящее время можно было бы оценить уровень проводившейся здесь криптографической работы, определить ее эффективность.

В своей внешней и внутренней переписке, в радиограммах все важные сведения зашифровывались в обязательном порядке. Такую зашифрованную информацию можно разделить на три вида:

1. Политическая, дипломатическая и деловая переписка с заграничными посольствами и представительствами;
2. Разведывательные данные;
3. Сведения о военной обстановке, положении на фронтах, распоряжения, приказы, стратегические и тактические планы командования, планы военных операций.

Краткие сообщения, содержащие важные сведения, шифровались целиком, в длинных же сообщениях шифровались лишь выборочные, наиболее важные места.

Передаче сообщения, как обычно, предшествовала некоторая подготовительная работа с текстом: подчеркивались куски текста, которые следовало зашифровать, далее текст телеграммы либо переводился на французский язык, либо просто писался латинскими буквами (своего рода предварительное шифрование), необходимая часть его зашифровывалась и записывалась пятизначными цифровыми группами.

Так, телеграмма, направленная генералом Миллером 16 октября 1919 г. лондонскому представителю Саблину, готовилась для передачи следующим образом.

Этап первый. Составляется открытый текст телеграммы и в нем подчеркиваются слова, подлежащие зашифрованию:

«Зимние рейсы между Норвегией и г. Мурманском будут установлены с наступлением зимы не менее раза в неделю, согласовывая со срочными норвежскими пароходами, но пока замерзания нет, это не установлено точно. В настоящее время три парохода находятся на пути в Берген и четвертый выходит из Бергена и Мальмо, все для вывоза продовольствия. Генерал Миллер» [11].

Этап второй. Текст, подлежащий зашифрованию, пишется латинскими буквами:

«Zimnie reisy mejdu Norwegiei gorodom Murmanskom budut ustanovleny s nastupleniem zimy ne menee raza v nedeliu soglasovyvaia so srocnymi norvejskimi parohodami...»

Текст телеграммы, подлежащий зашифрованию, написанный чернилами от руки или отпечатанный на пишущей машинке, разбивался карандашом на словарные величины, затем шифровался.

Шифртекст:

«18566 24307 54945 38536 20043 45496 63241 81137 82174 15070 64444 17004 57526 85551 88317...» [12].

Сохранившиеся тексты, разбитые на словарные величины, позволяют установить, что здесь использовалась буквенно-слоговая таблица. Как видно из приведенного примера, слова разбивались на произвольные слоги. При относительно коротких шифртекстах, аккуратной смене ключей и тщательном соблюдении правил пользования буквенно-слоговые таблицы являются достаточно стойким шифром.

Дальние расстояния, на которые передавались сообщения, сравнительно малая мощность и слабое техническое исполнение радиостанций, невы-

сокая квалификация шифровальщиков, — все это не могло не сказаться на качестве получаемых адресатами телеграмм, что приводило к необходимости их повторять. Типичными для 1919—1920 гг. являются телеграммы о том, что какие-то слова или целые телеграммы не поддаются расшифрованию, например: из телеграммы от 22 июня 1919 г. генералу Миллеру из Парижа от Маклакова: «*В Вашей телеграмме не поддаются расшифрованию два слова*»; из телеграммы Миллеру посла в Христиании Пилара: «*Ваша телеграмма... доставлена лишь 27 августа, поддается разбору лишь с очень большим трудом*» [13].

Анализ материалов архива Колчака, касающихся шифрованной переписки, показывает, что наличие большого числа нарушений шифрдисциплины при шифровании и передаче радиограмм, использование старых шифров, — все это, в принципе, позволяло дешифровать переписку белых или существенную ее часть как на внешних, так и на внутренних линиях связи. Во всяком случае, для таких опытных криптографов, как И. А. Зыбин, Н. А. Ямченко (о нем мы скажем ниже), перешедших на сторону Советской власти, это не составило бы большого труда. Но в тот период советская сторона не располагала силами и средствами для успешного проведения такой работы. Во всяком случае, данных об успешном перехвате и дешифровании переписки белых армий не имеется. Советская сторона испытывала острый дефицит в радиоперехватывающих средствах и их оснастке, хотя войсковые соединения и перехватывали радиопереговоры, ведущиеся по линиям связи фронтовых и дивизионных соединений белых армий.

Белогвардейский радиоперехват

Белые активно и достаточно успешно перехватывали советские шифрованные и открытые радиограммы в период 1918—1920 гг. Хранящиеся в фон-

дах ГАРФ материалы радиоперехвата показывают, что им удавалось полностью или частично перехватывать, обрабатывать, дешифровать правительственную, дипломатическую и военную переписку Советской республики.

С советской стороны в основном применялись шифры простой и пропорциональной замены. Генерал-майор Дентервиль, командовавший экспедиционными войсками в Персии и Баку (1918 г.), в своих воспоминаниях писал, что благодаря использованию Красной Армией на Каспийском море старого царского кода, копия которого имелась в его штабе, английским войскам удалось занять Баку и другие районы Кавказа. В период борьбы с Врангелем советской стороной применялся шифр «Республика», представлявший собой «шифр Виженера» с чередованием букв алфавита внутри квадрата в соответствии с ключом-лозунгом. Применялись не менее широко шифры «Москва» и «Секунда». Шифр «Москва» также представлял собой «шифр Виженера», где в качестве лозунга использовался тот же открытый текст, но сдвинутый на один шаг вправо, иначе расшифрование было бы невозможно. При этом первая буква лозунга была заранее оговоренной и менялась в соответствии с расписанием. Шифр «Секунда» был обычным шифром замены на 9, 2, 13 колонок.

В 1919—1920 гг. были разработаны и применялись более стойкие шифры: «Пулемет», «Агитатор», «Советский» и др.

Складывавшаяся в период Гражданской войны неблагоприятная ситуация с обеспечением тайны шифрпереписки Советской республики достаточно убедительно раскрывается в ряде архивных документов, в частности в шифртелеграмме, посланной уполномоченным РВСР на Украине, командующим войсками Украины и Крыма, членом Политбюро ЦК КП(б)У М. В. Фрунзе в центр 19 декабря 1920 г.:

«Москва, Предсовнаркома Ленину, Предреввоенсовета Троцкому, Главкому, Наркомвнудел Чичерину, ЦК РКП.

Из представленного мне сегодня бывшим начальником врангелевской радиостанции Ямченко доклада устанавливается, что решительно все наши шифры вследствие их несложности расшифровываются нашими врагами. Вся наша радиосвязь является великолепнейшим средством ориентирования противника. Благодаря тесной связи с шифровальным отделением морфлота Врангеля, Ямченко имел возможность лично читать целый ряд наших шифровок самого секретного военно-оперативного и дипломатического характера; в частности, секретнейшая переписка Наркоминдела с его представительством в Ташкенте и Европе слово в слово известна англичанам, специально организовавшим для подслушивания наших радио целую сеть станций особого назначения. То же относится к расшифрованию свыше ста наших шифров. К шифрам, не поддававшимся прочтению немедленно, присылались ключи из Лондона, где во главе шифровального дела поставлен англичанами русскоподданный Феттерлейн, ведавший прежде этим делом в России. Общий вывод такой, что все наши враги, в частности Англия, были постоянно в курсе всей нашей военно-оперативной и дипломатической работы. Копию доклада Ямченко препровождаю с нарочным. Изложенное докладываю для принятия соответствующих мер.

19 декабря Командвойск Укр Фрунзе» [14].

На этой телеграмме имеется резолюция Ленина: «Сохранить секретно и напомнить мне вместе с докладом Ямченко»

Эта телеграмма дает возможность оценить тот урон, который несла советская сторона за счет слабости криптографической защиты своих передач.

Белые прежде всего проявляли существенный интерес к информации политического характера. Такая информация ими скрупулезно собиралась, об-

рабатывалась и использовалась для принятия соответствующих решений. По ней регулярно составлялись аналитические отчеты и обзоры. Особое внимание уделялось обработке телеграмм, подписанных руководителями партии или членами правительства. Материалы радиошифрперехвата, содержащиеся в архивах белых армий, представляют собой ценнейший и до сих пор не исследовавшийся исторический источник. Здесь имеются перехваченные тексты сообщений самого разного содержания, порой не зафиксированные другими источниками. Кроме введения в научный оборот новых документов, материалы радиошифрперехвата позволяют восстановить, уточнить, дополнить и т. п. тексты известных документов.

Пристальное внимание белыми уделялось изучению личностей советских руководителей. С этой целью специально собирались подробные данные о них, составлялись политические характеристики, подробно обрисовывался их человеческий облик.

Из доклада о политическом положении в России в конце января 1919 г.:

«Правой рукой Ленина является председатель Центрального исполнительного комитета Советов Свердлов, главная черта характера которого — непоколебимая воля... Для уничтожения большевизма более полезным является поддержка партии Троцкого, которая благодаря своей политике, не признающей компромиссов, скорее приведет большевистскую Россию к краху» [15].

Заметим, кстати, что аналогичные характеристики Троцкого давались агентами ДП еще в 1908 г. Вообще опыт и знания о конкретных лицах, в свое время накопленные ДП, активно использовался белыми.

Вместе с тем в архивах белого движения содержатся материалы, позволяющие составить представление о личностях его лидеров, об их взаимоотношениях. Вот, например, как относился адмирал Колчак уже в 1919 г. к недавнему главе Временного правительства:

«Шифртелеграмма в Париж. Маклакову. 27. XI. 1919. На Керенского никаких официальных поручений не возлагалось и возлагать не предполагается, в пользовании им шифром ему надлежит категорически отказывать» [16].

Идеологические вопросы также находились в центре внимания руководителей белого движения. Для иллюстрации этого положения можно привести такие примеры.

Из «Доклада о наблюдениях, имевших место на советской территории», Архангельск, 7 мая 1919 г.:

«...Школы. Большевики очень высоко ставят свою систему образования. Они ввели систему Монтессиори и Гори в начальных школах и учредили пролетарские университеты. Здесь кроме обычных предметов учащимся преподают политические доктрины большевистской партии. Повсюду учреждено большое количество этих школ, а в наиболее глухих местах обучают по граммофонным пластинкам, содержащим речи, изложенные простым языком. Совершенно очевидно, что они весьма энергично распространяют свои политические убеждения на публику, как, например, поезда для пропаганды с печатными станками, чтобы ежедневно давать свежие газеты» [17].

Из «Доклада начальнику осведомительного отдела Управления 2-го генерал-квартирмейстера штаба Верховного главнокомандующего» 17 июня 1919 г.:

*«...Большевики возлагают большие надежды на агитацию в тылу и проводят ее с колоссальной затратой денег и энергии. Они посылают преданных себе лиц в Сибирь, снабжая их громадными деньгами. В Сибири эти агитаторы высматривают элементы, недовольные существующим порядком, и составляют из них пятерки с тем, чтобы каждый из членов организуется дальше (*так в подлиннике. — *Т. С.). Сорганизованным бандам подсказывают, смотря по моральным качествам набранных, и соответствующие лозунги...*

Целью большевиков на Востоке ставится довести к грандиозному мятежу и разрушить исправную коммуникацию в тылу русской армии» [18].

Белые тщательно следили за дипломатической деятельностью Советской России. Так, перехватывалась и дешифровалась переписка, связанная с переговорами о Брестском мире, которой активно обменивались Советское правительство и делегация.

Тщательно отбиралась и анализировалась информация о деятельности ВЧК. В частности, были перехвачены материалы, содержащие все подробности раскрытия ВЧК заговора Локкарта.

Благодаря радиоперехвату руководители белого движения в значительной степени могли контролировать конкретные действия и планируемые операции Красной Армии на Восточном и Туркестанском фронтах, следить за связью фронтов с центром. Так, например, сохранились тексты перехваченных и раскрытых шифртелеграмм, относящихся к середине лета 1918 г., отразивших напряженную обстановку в Туркестане:

«Ташкент. Из Москвы. 24. VII. 1918 г. Совдеп. Колесову.

Из Москвы через Царицын направляются Вам подкрепления под управлением Туркестанского комиссара.

Нарком Бонч-Бруевич

Военнарком Аралов»

«Москва. Из Ташкента. 25. VII. 1918 г. Троцкому. Копия Бонч-Бруевичу.

Вторично именем революции молим о подкреплении нас боевыми припасами, а главное — патронами, необходимыми срочно для Оренбургского фронта и целого ряда фронтов Республики, особенно Семиреченского, где восстали чехословаки, ферганцы, и Закаспийского — для подавления восстания белой гвардии.

Предсовнаркома Туркестанской республики Колесов» [19].

Благодаря радиоперехвату белые были информированы и о положении в Ташкенте в течение лета — осени 1918 г., что несомненно сыграло роль при подготовке и проведении ташкентского восстания под руководством К. Осипова в январе 1919 г. В архиве сохранились перехваченные тексты телеграфных переговоров с Москвой комиссаров-большевиков М. С. Качуринера, Н. В. Шумилова.

Так же тщательно следили за деятельностью Советов Сибири, находившихся в тылу войск Колчака.

15 августа 1918 г. колчаковской радиостанцией было перехвачено сообщение из Читы, направленное «Всем». В этом сообщении подробно говорилось о положении в Сибири в тех местах, где была свергнута Советская власть. Подписали сообщение председатель Центрального исполнительного комитета Советов Сибири Н. Н. Яковлев (брат В. Н. Яковлевой. — *Т. С.*), представители Забайкальского исполкома П. Бутенин и Н. Матвеев.

Регулярное чтение шифртелеграмм, связанных с деятельностью Центросибири, позволяло белым быть постоянно в курсе тех усилий, которые предпринимали ее руководители в марте — августе 1918 г. для координации деятельности Советов Западно-Сибирской, Восточно-Сибирской областей и Дальневосточного края. Благодаря этому они располагали информацией о важнейших планах и мероприятиях, осуществляемых Центросибирью в тот период, как органом, возглавлявшим в регионе борьбу за Советскую власть. Нет сомнений в том, что данные радиошифрперехвата в определенной степени способствовали успехам белых войск во время их наступления при взятии Читы в августе 1918 г.

Глава пятнадцатая

СОЗДАЕТСЯ ЗАНОВО

Проект Г. И. Бокия

Организация и деятельность криптографической службы России в первые годы Советской власти представляет значительный интерес для специалистов разных направлений как с точки зрения изучения становления специальной службы Советского государства на начальном этапе, так и с точки зрения обобщения исторического опыта в различных его аспектах. Именно к этому времени относится зарождение научных методов криптографического анализа, развитие радиотелеграфной шифрованной связи и радиошифрперехвата. В этот период началось критическое осмысление состояния безопасности отечественных линий связи и определение форм будущей шифровальной службы страны.

В 1921 г., когда Гражданская война была уже на исходе, особенно остро перед руководителями страны встали проблемы экономические и внутриполитические. Неотложная необходимость коренной реорганизации криптографической службы, обслуживающей интересы армии, остро проявилась и в других ведомствах, где таковая продолжала существовать в соответствии с традициями, сложившимися в царской России. Здесь прежде всего следует указать Наркомат иностранных дел. Его руководители в течение 1919—1920 гг. постоянно информировали Совнарком

о неблагополучном положении в криптографической службе этого ведомства.

20 августа 1920 г. нарком иностранных дел Г. В. Чичерин писал в записке на имя В. И. Ленина: «...Иностранные правительства имеют более сложные шифры, чем употребляемые нами. Если ключ мы постоянно меняем, то сама система известна многим царским чиновникам и военным, в настоящее время находящимся в стане белогвардейцев за границей. Расшифрование наших шифровок я считаю поэтому вполне допустимым...» [1].

Чичерин был абсолютно прав. Нами, в частности, уже упоминался Феттерлейн — один из криптографов МИД России, ставший теперь одним из ведущих криптографов Англии.

Однако мнение Чичерина о том, что причина утечки шифрованной информации кроется в слабости используемых шифров, в том, что многие работники криптографической службы царской России оказались на Западе, разделяли не все. Часть советских руководителей искали причину в предательстве, действии в шифрорганах вражеских агентов (утечки данных по оперативным каналам). Вот письмо Л. Б. Красина В. И. Ленину от 10 сентября 1920 г.:

«Владимир Ильич!

Еще в мае в бытность в Копенгагене по некоторым признакам я начал подозревать, что с шифрованной перепиской через Наркоминдел не все обстоит благополучно. В Англии эти подозрения укрепились, и в последующий мой приезд в Москву я обращал внимание тов. Чичерина на необходимость коренной чистки в соответственном отделе... Наконец, сегодня мы почти официально извещены, что тайные наши депеши отнюдь не представляют тайны для Велпра. Дело не в провале шифра или ключа, а в том, что в Наркоминделе неблагополучие, так сказать, абсолютное, и лечить его надо радикально... По-моему, поправить дело

можно только созданием при Наркоминделе шифровального отделения независимо от самого Комиссариата и персонально подобранного из людей либо по партии, либо лично известных в течение десятка — полутора лет... Кроме того, надо завести особый ключ с Оргбюро или Политбюро и особо важные депеши посылать этими ключами, совершенно эпатируя К[омиссариа]т в деле их расшифрования. Не думайте, что все это излишняя мнительность, нет, дело обстоит очень серьезно...» [2].

Ленин внимательно относился к таким сообщениям. Он несколько раз лично давал рекомендации по совершенствованию системы пользования шифрами, повышению шифрдисциплины, излагал свое мнение о принципах построения шифровальной службы. Например, в записке Г. В. Чичерину от 25 ноября 1920 г. он писал:

«Тов. Чичерин! Вопросу о более строгом контроле за шифрами (и внешнем и внутреннем) нельзя давать заснуть.

Обязательно черкните мне, когда все меры будут приняты. Необходима еще одна: с каждым важным послом (Красин, Литвинов, Шейнман, Йоффе и т. п.) установить особо строгий шифр только для личной расшифровки, т. е. здесь будет шифровать особо надежный товарищ, коммунист (может быть, лучше при ЦК), а там должен шифровать или расшифровывать лично посол (или «агент») сам, не имея права давать секретарям или шифровальщикам.

Это обязательно (для особо важных сообщений, 1—2 раза в месяц по 2—3 строки, не больше).

Ваш Ленин» [3].

Как мы уже отмечали, в декабре 1920 г. начальник захваченной радиостанции Врангеля И. М. Ямченко подтвердил еще раз, что советская сторона применяет шифры недостаточной стойкости. А еще в сентябре 1920 г. Политбюро рассмотрело «предложение т. Ленина принять меры к усложнению шифров и к более строгой охране шифрованных сообщений». Политбюро постановило поручить Л. Д. Троцкому, наркому по военным и морским делам, «организовать комиссию из представителей Наркомвоен, Наркоминдел, ЦК РКП и Наркомпочтеля» [4].

О последнем ведомстве следует сказать особо.

В функции Всероссийской чрезвычайной комиссии по борьбе с контрреволюцией, саботажем и преступлениями по должности входило проведение контроля за иностранной перепиской. Органы ВЧК организовали, по примеру соответствующих служб царской России, службу перлюстрации шифрованной корреспонденции аккредитованных в Москве представителей некоторых иностранных государств. Известно, что уже в начале 20-х гг. в Москве находились дипломатические и торговые посольства и миссии Германии, Англии, Турции, Италии, Финляндии, Польши, Ирана, Афганистана и прибалтийских государств. Кроме телеграмм, поступавших с телеграфа, часть шифрованной иностранной переписки и переписки белой гвардии по заданиям ВЧК и военных органов перехватывалась на Серпуховской приемной радиостанции Реввоенсовета и Шаболовской радиостанции Наркомпочтеля. Эти сообщения вместе с перехватом открытых сообщений иностранной прессы направлялись в так называемый отдел обработки материалов Особого отдела ВЧК. В отделе обработки материалов предпринимались попытки расшифровать перехватываемые радио, получаемые при обысках и арестах членов контрреволюционных организаций шифрованные документы. В отдельных случаях это удавалось сделать. Вот, например, одна из дешифрованных в сентябре 1920 г. телеграмм контрразведки генерала Врангеля:

«30. Военная. Таганрог. Начальнику контрразведки полковнику Бучинскому.

Доношу: по имеющимся у меня сведениям, на юге России скрываются известные большевистские деятели японцы Гедионака и Накамура. К розыску их меры приняты. 20 сентября, полковник Анжело».

Однако большинство поступавших в отдел шифрдокументов оставалось не расшифрованными. Что касается дипломатической шифрованной переписки, то она совсем не читалась.

Будучи заинтересованной в использовании данных шифрпереписки, ВЧК направляла материалы для дешифрования в военные органы. Вот один из документов:

«В Полевой штаб Реввоенсовета Республики. 14. IV. 1920.

Согласно резолюции начальника отдела обработки материалов Особого отдела ВЧК при сем препровождается три копии перехвата неприятельских радиограмм от 3 и 4 апреля с просьбой расшифровать в срочном порядке и возвратить в отдел обработки материалов 00 ВЧК».

Через двадцать дней, 4 мая 1920 г., в Полевой штаб РВСР был послан вторичный запрос по этому же делу. И лишь в июне был получен типичный для подобной ситуации того времени ответ:

«Ввиду невозможности установить ключ к этим телеграммам последние возвращаются в нерасшифрованном виде...»

Итак, мы видим, что к концу Гражданской войны Советская Россия фактически не располагала действенной и надежной криптографической службой. В начале 1921 г. вопрос о создании единого органа, который вобрал бы в себя все возможные

криптографические силы республики и был бы способен организовать криптографическую деятельность на уровне ведущих иностранных государств, встал особенно остро. Причин этого можно указать несколько.

Первая группа причин кроется в итогах Гражданской войны. Мы уже говорили о том, что криптографическая служба Советской Республики периода Гражданской войны по существу заимствовала средства, методы и частично кадры царской специальной службы, и этот факт сыграл крайне негативную роль ввиду того, что для бывших царских криптографов, оказавшихся в рядах белой гвардии или в специальных службах иностранных государств, находившихся в состоянии войны с Россией, шифры, использовавшиеся советской стороной, составляли секрет полишинеля. Следует, однако, обратить внимание и еще на одно важное обстоятельство.

Как известно, еще в годы Первой мировой войны Ленин пришел к выводу о возможности победы революции в одной стране. Но это рассматривалось им как возможность, притом маловероятная. Сразу же после октября 1917 г., под влиянием общего революционного подъема в Европе, в политико-теоретической мысли большевиков возобладало представление о том, что чуть ли не вся планета стоит в преддверии всемирной пролетарской революции. Ее развитие представлялось как распространение системы Советов по всему миру. Проходивший в июльские дни 1920 г. II конгресс Коминтерна принимает знаменитый Манифест. «Коммунистический Интернационал, — говорилось в нем, — есть партия революционного восстания международного пролетариата... Советская Германия, объединенная с Советской Россией, оказалась бы сразу сильнее всех капиталистических государств, взятых вместе. Дело Советской России Коммунистический Интернационал объявил своим делом. Международный пролетариат не вложит меч в ножны до тех

пор, пока Советская Россия не включится звеном в федерацию Советских республик всего мира».

Весна и лето 1920 г. в известном смысле вообще были временем переломным. К сожалению, все еще не опубликованы многие материалы, которые могли бы пролить свет на важные стороны формирования политики партии в тот период. Но обратимся к такому источнику, как стенографический отчет IX конференции РКП(б), проходившей в сентябре 1920 г.

Условия вполне выявившейся тогда неспособности держав Антанты сокрушить Советскую власть с помощью интервенции, с одной стороны, и быстрый рост революционного движения на Западе — с другой, побудили ЦК партии перейти, как говорили делегаты конференции, от «политики обороны» к «политике наступления против мирового капитала». И в качестве первого шага на этом пути была названа «советизация Польши». Об этом говорили на конференции многие делегаты: Н. И. Бухарин, Ф. Э. Дзержинский, Г. Е. Зиновьев, К. Б. Радек, В. В. Оболенский (Осинский), И. В. Сталин и другие. Но, пожалуй, наиболее четко выразил общую точку зрения Л. Б. Каменев, который играл в дальнейших событиях одну из первых ролей [5].

«В продолжение двух с половиной лет, — подчеркивал он на конференции, — Советская Россия была осажденной крепостью, на которую ее враги нападали приступом... Наше наступление на Польшу было первой вылазкой осажденного гарнизона... Мы сказали, что мы достаточно сильны для того, чтобы устроить вылазку на соединение с армиями европейских пролетариев».

Мало кто из вождей Советской России сомневался в успехе наступления на Варшаву. Ф. Э. Дзержинский, например, даже в принципе не допускал срыва в Польше. «Я и в ЦК, — говорил он на сентябрьской конференции, — стоял на той точке зрения, что польский рабочий класс ожидает Красную Революционную Армию для того, чтобы избавиться от гнета помещиков и антантовского, который душит его в продолжении всего периода так называемой независимости Польши». В. И. Ленин также активно поддерживал идею наступления на Варшаву.

Разгром Красной Армии, ведомой М. Н. Тухачевским, под Варшавой явился поражением не столько военным, сколько политическим. Он заставил по-новому оценить расстановку сил на международной арене и признать, что мировая революция — дело отнюдь не ближайшего будущего, и Советской России предстоит какое-то время существовать в окружении враждебных империалистических государств. Следовательно, необходимо было укрепить обороноспособность страны, в том числе совершенствовать специальную службу.

Другая группа причин связана с экономической и политической обстановкой в стране, которая также оставалась исключительно сложной.

16 ноября 1920 г. последний корабль под Андреевским флагом покинул Керченскую бухту, увозя на чужбину остатки врангелевских войск. Гражданская война на европейской территории страны закончилась. И хотя в ряде районов, преимущественно на Дальнем Востоке, еще до осени 1922 г. продолжали тлеть отдельные ее очаги, начался период мирного строительства.

Тяжелую картину представляло собой хозяйство страны. Разрушенные заводы и фабрики, ржавые остовы взорванных мостов и затопленные шахты, сожженные деревни, вытоптанные поля...

Сумма ущерба, нанесенного России двумя войнами — Первой мировой и Гражданской — превышала 39 млрд золотых рублей. Потери населения достигли 20 млн человек. Объем промышленной

продукции по сравнению с довоенным уровнем сократился в семь раз, на 40% уменьшилось сельскохозяйственное производство.

Хозяйственная разруха обострила политический кризис в стране. В его основе лежало недовольство крестьян политикой «военного коммунизма», в особенности запрещением частной торговли и продразверсткой.

С осени 1920 г. по стране покатилась волна крестьянских мятежей — ширился и разрастался тот самый «русский бунт вообще против всякой власти», о котором подробно и убедительно говорит в своей книге «Россия. Век XX. 1901—1939» политолог и историк В. В. Кожинов [6]. В конце февраля 1921 г. мятежами и восстаниями были охвачены уже значительные районы Украины, Поволжья, Западной Сибири. Антисоветским силам здесь удалось поставить под ружье около 150 тысяч человек. А в начале марта 1921 г. восстал Кронштадт...

Именно в этот период, в самом начале 1921 г. и начинает проводиться реальная организационная работа по созданию единой криптографической службы страны.

В. И. Ленин, изучив досконально вопрос, зная мнение МИД и других заинтересованных ведомств, поручает изыскать пути наведения порядка в шифровальном деле руководству ВЧК, хотя шифровальные службы, повторяем, по традиции сохранялись и в МИД, и в Военном наркомате. Возможно, на выбор базового ведомства повлияла сложность обстановки, а также то обстоятельство, что главной функцией ВЧК уже в тот период было обеспечение государственной безопасности в целом. Как мог заметить читатель, именно на обеспечение государственной безопасности направлена и деятельность криптографической службы.

В десятых числах января 1921 г. коллегия ВЧК принимает решение созвать совещание представи-

телей заинтересованных ведомств для подготовки соответствующих предложений по воссозданию криптографической службы. В обсуждении вопроса принимали участие представители ЦК РКП(б), ВЧК и наркоматов. В результате этой работы к марту были подготовлены предложения об учреждении межведомственной шифровальной комиссии при Совнаркоме Республики, состоящей из представителей Наркомвоена, ВЧК, Наркоминдела и Наркомвнешторга под председательством представителя ВЧК — начальника Специального отдела. Однако представленный ВЧК проект деятельности этой комиссии принят не был, так как оказалось очевидным, что в создавшихся условиях, при наличии у всех наркоматов множества труднейших неотложных собственных задач, всю работу по созданию и организации деятельности специальной службы должно взять на себя одно ведомство, а именно ВЧК. Было принято постановление, предложенное Лениным: «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». 12 апреля на заседании Малого Совнаркома с проектом о создании Специального отдела при ВЧК выступил будущий начальник этого отдела, человек, которому предстояло стать главным организатором криптографической службы страны и ее первым руководителем, — Глеб Иванович Бокий.

Вот текст этого проекта [7]:

«Имея в виду: 1) Отсутствие в Республике центра, объединяющего и направляющего деятельность шифровальных органов различных ведомств, и связанные с этим бессистемность и случайность в по-

становке шифровального дела, 2) Возможность, благодаря этому при существующем положении широкого осведомления врагов Рабоче-Крестьянского государства о тайнах Республики, Совет Народных Комиссаров постановил:

I

Образовать при Всероссийской Чрезвычайной Комиссии «Специальный отдел», штаты в коем утверждаются Председателем ВЧК. Начальник Специального отдела назначается Совнаркомом.

В круг ведения Специального отдела при ВЧК включить:

I. Постановку шифровального дела в РСФСР:

А. Научная разработка вопросов шифровального дела:

а) анализ всех существующих и существовавших русских и иностранных шифров;

б) создание новых систем шифров;

в) составление описаний шифров и инструкций по шифровальному делу и пользованию шифрами;

г) собирание архивов и литературы по шифровальному делу для сконцентрирования такового при Спецотделе;

д) составление и издание руководств по вопросам шифрования.

Б. Обследование и выработка систем шифров:

1. Обследование всех действующих в настоящее время шифров и порядка пользования ими шифрорганами;

2. Окончательная обработка инструкций по шифровальному делу и пользованию шифрами и выработка правил работы шифрорганов;

3. Распределение вновь выработанных систем шифров между всеми ведомствами.

В. Организация учебной части:

1. Выработка программы школы шифровальщиков;

2. Создание школы шифровальщиков;

3. Укомплектование школы преподавателями и учениками.

Г. Учет личного состава шифровальных органов. Наблюдение за закономерной постановкой шифровального дела. Инструктировка и инспекция шифровальных органов:

1. Учет и проверка всех сотрудников всех шифрорганов;

2. Распределение всяких сотрудников всех шифрорганов между последними в зависимости от индивидуальных качеств каждого работника и фактической потребности в работниках в том или ином шифрорганe, а также зависимо от государственной важности каждого учреждения;

3. Чистка неблагонадежного и неспособного элемента из всех шифрорганов;

4. Наблюдение за закономерной постановкой шифровального дела во всех шифрорганах;

5. Инструктировка и инспекция всех шифрорганов и проведение в жизнь Инструкции и правил по шифровальному делу.

II

Постановка расшифровального дела в РСФСР:

1. Изыскание способов повсеместного улавливания всех радио, телеграмм и писем неприятельских, иностранных и контрреволюционных;

2. Открытие ключей неприятельских, иностранных и контрреволюционных шифров;

3. Расшифровка всех радио, телеграмм и писем неприятельских, иностранных и контрреволюционных.

Все распоряжения и циркуляры Специального отдела при ВЧК по всем вопросам шифровального и расшифровального дела являются обязательными к исполнению всеми ведомствами РСФСР».

Оценивая этот документ сегодня, а к его содержанию мы еще вернемся, можно утверждать, что в функциях Спецотдела уже с самого начала были предусмотрены по существу все направления деятельности в области криптографии, которые в совокупности обеспечивают безопасность передачи информации.

5 мая 1921 г. постановлением Малого Совнаркома при ВЧК был создан Специальный отдел, начальником его и одновременно членом коллегии ВЧК назначен Г. И. Бокий.

Пионеры советской криптографии

Итак, Спецотдел был создан в мае 1921 г. при ВЧК. В течение 20—30-х гг. в связи с реорганизациями структуры органов этот отдел имел следующие наименования:

с 5 мая 1921 г. по 6 февраля 1922 г. — 8-й Спецотдел при ВЧК;

с 6 февраля 1922 г. по 2 ноября 1923 г. — Спецотдел при ГПУ;

со 2 ноября 1923 г. по 10 июля 1934 г. — Спецотдел при ОГПУ;

с 10 июля 1934 г. по 25 декабря 1936 г. — Спецотдел ГУГБ НКВД СССР;

с 25 декабря 1936 г. по 9 июня 1938 г. — 9 отдел ГУГБ НКВД СССР.

Однако несмотря на реорганизации, в отличие от других подразделений (например: СПО — секретно-политического отдела, ИНО — иностранного отдела и т. д.) Спецотдел был *при* ВЧК, ОГПУ и т. д., то есть пользовался автономией. В изучаемый период это выражалось в том, что он сообщал информацию и адресовался непосредственно в Политбюро, ЦК, правительство самостоятельно, а не через руководство ведомства, при

котором отдел находился. Известно, что сотрудники других подразделений относились к Спецотделу скептически, так как «там никого не арестовывали и не допрашивали».

В начале 20-х гг. отдел включал шесть, а позднее семь отделений. Однако собственно криптографические задачи, в строгом понимании, решали только три из них: 2-е 3-е и 4-е. Так, сотрудники 2-го отделения Спецотдела занимались теоретической разработкой вопросов криптографии, выработкой шифров и кодов для ВЧК (ГПУ — ОГПУ — НКВД) и всех других учреждений страны (включая МИД, Военное ведомство и др.). Отделение в первые годы работы состояло из семи человек, его начальником являлся Ф. Г. Тихомиров.

Перед 3-м отделением стояла задача «ведения шифрработы и руководство этой работой в ВЧК» (ГПУ — ОГПУ — НКВД). Состояло оно вначале всего из трех человек, руководил отделением старый большевик, бывший латышский стрелок Ф. И. Эйхманс, одновременно являвшийся заместителем начальника Спецотдела. Эйхманс организовывал шифрсвязь с заграничными представительствами СССР, направлял, координировал их работу.

Сотрудники 4-го отделения, а их было восемь человек, занимались «открытием иностранных и антисоветских шифров и кодов и дешифровкой документов». Начальниками этого отделения были: с мая по декабрь 1921 г. — Ященко, с января по август 1922 г. — Горячев, с августа 1922 по сентябрь 1923 г. — Эльтман, с сентября 1923 по январь 1938 г. — Гусев. А. Г. Гусев все это время выполнял обязанности помощника начальника Спецотдела.

Перед остальными отделениями Спецотдела стояли такие задачи:

1-е отделение — «наблюдение за всеми государственными учреждениями, партийными и общественными организациями по сохранению государственной тайны»;

2-е отделение — «перехват шифровок иностранных государств; радиоконтроль и выявление нелегальных и шпионских радиоустановок; подготовка радиоразведчиков»;

6-е отделение — «изготовление конспиративных документов»;

7-е отделение — «химическое исследование документов и веществ, разработка рецептов. Экспертиза почерков, фотографирование документов».

Как видим, Специальный отдел включал перечень задач, аналогичный соответствующему подразделению Департамента полиции.

Кадровому составу Спецотдела, на наш взгляд, следует уделить особое внимание. И здесь следует вновь обратиться к личности его первого руководителя Глеба Ивановича Бокия. Ранее мы уже упоминали это имя в связи с шифрами подполья. Д. Кан в своей книге дал этому человеку такую характеристику:

«Начиная примерно с 1927 г. (у Кана ошибка в дате. — *Т. С.)* вплоть до указанного выше времени (1937 г. — *Т. С.),* его (Спецотдела. — *Т. С.)* начальником был старый большевик и друг Ленина Глеб И. Бокий, который в то же самое время был членом Верховного суда СССР. Он родился в 1879 г. и принимал участие в революционном движении. Он неоднократно подвергался арестам и был приговорен к трем годам ссылки в Сибирь. Во время революции был секретарем ячейки большевиков в Петербурге. В начале 20-х годов Бокий возглавлял ЧК в Туркестане, где он навел такой страх на местных жителей, что после его отъезда еще долго ходили о нем различные легенды. Например, рассказывали, что он питался мясом собак (что было особенно отвратительным для мусульманского населения), что он пил кровь людей и т. д. Однако не лишены основания утверждения о том, что как глава Спецотдела Бокий во время своих отпусков, которые он проводил на даче около Батуми, устраивал дикие оргии, на которые приглашались тщательно отобранные люди. Дверь его кабинета всегда была закрыта, и через специально вмонтированный в нее глазок он изучал своих посетителей. Высокий и сутулый, со злым выражением лица и холодными голубыми глазами, он производил впечатление, что само уже ваше присутствие было ему ненавистным. Он приводил в трепет девушку, бывшую на ночном дежурстве, когда выходил из своего кабинета и заводил с ней разговор. Бокий никогда не носил шляпу, но всегда, независимо от сезона, надевал плащ. Бокий, вероятно, был скорее администратором, чем криптографом. Он был казнен во время большой чистки, проведенной Сталиным. Позже установлено, что он в нарушение социалистической законности тайно хранил золотые и серебряные монеты» [8].

Что можно сказать об этом пассаже? Жаль, что во многом хорошая и полезная книга американского автора, включающая множество достоверных фактов и взвешенных оценок, содержит такие откровенно надуманные места. Это, безусловно, снижает ее уровень и научную ценность.

К глубокому сожалению, роль и место русской дворянской интеллигенции в РСДРП вообще и в деятельности ее большевистского крыла в частности является темой малоизученной в исторической науке. Объяснимое «невнимание» к этой теме в советский период сменилось в последние десять лет активным распространением заведомо ложной «исторической информации», некой «молвы» о том, что в результате «октябрьского переворота» к власти пришли «малограмотные мужики», «кухарки» стали управлять государством. Относительно того, что к власти в тот период пришли люди, в чьей образованности, грамотности и эрудиции вряд ли можно

сомневаться, неоспоримо свидетельствует то обстоятельство, что именно они сумели в кратчайший срок из хаоса и разрухи возродить великую страну, восстановить все необходимые элементы государственности. Участие многих представителей тогдашнего правящего сословия в революционном движении в рядах РСДРП(б) является историческим фактом. Отказавшись от привилегий, богатства, зачастую блестящей научной, служебной, а то и придворной карьеры, они посвятили свою жизнь борьбе за демократические преобразования, стремясь создать на Земле общество всеобщего гражданского равенства и справедливости. Среди них были: дочь известного архитектора Д. В. Стасова, племянница знаменитого критика В. В. Стасова Е. Д. Стасова, сын крупного помещика В. Р. Менжинский, сестры Зинаида и Софья Невзоровы, Г. М. Кржижановский, Г. В. Чичерин, Н. А. Семашко и многие другие.

Именно *созидательный аспект* деятельности большевиков в тот период очень быстро оценили многие и перешли на их сторону. Этому обстоятельству особое внимание уделяет в своем исследовании В. В. Кожинов, цитируя, в частности, В. В. Шульгина, который писал еще в 1929 г.: «Одних офицеров Генерального штаба чуть ли не половина осталась у большевиков. А сколько там было рядового офицерства, никто не знает, но много» [9].

К представителям российского дворянства в РСДРП(б) принадлежал и Г. И. Бокий.

Г. И. Бокий, поступив в 1896 г. в Петербургский горный институт — в ту пору крупнейшее высшее техническое учебное заведение России, учился в нем дольше необходимого срока в связи с многочисленными арестами и ссылками, И несмотря на то, что диплом он так и не успел получить, образование имел прекрасное. Его учителями были такие корифеи отечественной науки, как Е. С. Федоров, И. В. Мушкетов, В. И. Миллер, А. И. Лутугин,

В. И. Бауман и многие другие (кстати, о восстановлении Бокия в числе студентов Горного института после очередного вынужденного отсутствия всегда ходатайствовали некоторые из этих профессоров). Неоднократно Г. И. Бокий участвовал в научных экспедициях, в том числе в экспедиции генерала Жилинского в 1901 г. в бассейн реки Чу в районе Петропавловска Акмолинского. Параллельно с учебой в институте и революционной деятельностью в течение 16 лет Бокию пришлось работать и гидротехником, и горным инженером. Уровень преподавания специальных предметов в Горном институте, а также математический и физический курсы, которые там читались, несомненно позволили Бокию приобрести обширные научные знания. Как серьезный революционер он, кроме того, специально изучал многочисленные европейские труды по философии, политэкономии, политике и т. д., работал над своим образованием настолько упорно, что позволял себе спать не более четырех часов в сутки, о чем сохранились воспоминания очевидцев.

Являясь в течение двух десятков лет одним из руководителей революционного подполья Петербурга, Бокий несомненно приобрел колоссальный опыт организаторской работы, сплотил вокруг себя группу людей надежных и грамотных. Были среди них студенты и выпускники столичных вузов. Интересно, что некоторые из них, например В. Дингельштедт, А. Васильев работали с ним в Туркестане в 1919—1920 гг., где Бокий возглавлял Особый отдел Восточного, а затем Туркестанского фронтов. Относительно же «людоедства» Глеба Ивановича... В. Будников, ординарец Бокия, в голодное время, чтобы как-то поддержать больного туберкулезом командира, движимый лучшими чувствами, как-то сварил ему кошку на обед...

Некоторых из своих старых товарищей Бокий привел с собой на работу в Специальный отдел. Что

касается самого Глеба Ивановича, то, на наш взгляд, в тот период было трудно подобрать более удачную кандидатуру на пост организатора и руководителя криптографической службы страны.

В свое время работая над книгой о Г. И. Бокии, мне пришлось изучить множество документов и материалов, сохранивших облик этого человека. К числу людей, близко знавших Г. И. Бокия в течение десятков лет, принадлежал Максим Горький. В своем очерке «Соловки» он так писал о нем: «Человек из породы революционеров-большевиков старого, несокрушимого закала. Я знаю почти всю его жизнь, всю работу и мне хотелось бы сказать ему о моем уважении к людям его типа, о симпатии лично к нему. Он, вероятно, отнесся бы к такому «излиянию чувств» недоуменно, оценил бы это как излишнюю и, пожалуй, смешную сентиментальность» [10].

По своей натуре Г. И. Бокий был боец. Он постоянно трудился, полностью отдавая себя работе. В отношениях с коллегами — руководителями и подчиненными — был всегда принципиален. По свидетельству хорошо знавших его людей (Е. Д. Стасовой, прекрасной, к сожалению ныне почти забытой писательницы М. В. Ямщиковой, имевшей литературный псевдоним Ал. Алтаев), он решительно выступал против культивировавшихся уже с конца 20-х — начала 30-х годов, внедрявшихся и опекавшихся фактов личной преданности, подобострастности, угодничества к каждому руководителю. Боролся против чинопочитания, уже въедавшегося во все поры служебного аппарата. Он говорил, что авторитет руководства — это в первую очередь авторитет ума, честности, трудолюбия, скромности. Сам Бокий был скромен и нетребователен к личным удобствам чрезвычайно.

Хотелось бы указать на такое свойство Бокия в качестве руководителя криптографической службы,

как чувство противника. Известно, что во время военных действий это — главное качество, характеризующее талантливого полководца. Знать, чувствовать противника, прогнозировать его замыслы, предвосхищать направление главного удара и, наоборот, наносить ему неожиданный удар — все это бесценные качества военного руководителя. Естественно, эти качества неоценимы для руководителя любого вида разведки или контрразведки, который имеет дело с противником постоянно в мирное или военное время. Как свидетельствуют результаты работы, Бокий обладал этими качествами, по крайней мере в 20-е годы. Чувство противника — не проявление свыше, оно основано на глубоком знании противника, знании его научного и технического потенциала, интеллектуальных способностей и возможностей, уровня мышления, психологии, включая национальную, приемов и методов его работы. Чтобы иметь эти знания, надо прежде всего детально разработать механизм их получения. Этот вопрос, по-видимому, как об этом свидетельствуют факты, также хорошо продумывался. Спецотдел был связан с внешней разведкой и контрразведкой, которые поставляли ему информацию наряду с шифрами.

У этого человека были слабости и недостатки, но на сделку с совестью он не шел никогда. Во многом по этой причине у него были плохие и с годами все ухудшавшиеся отношения со Сталиным. Эти люди знали друг друга в течение многих лет подпольной работы. Вместе были членами Русского бюро ЦК РСДРП(б) в 1917 г., членами ЦК партии, членами Военно-революционного комитета в революционную осень. Иными словами, Бокий, как и Сталин, в предреволюционный и революционный период входил в ядро, руководящую верхушку большевистской партии. Думаю, что позднее, если бы Бокий покривил душой и где-то хотя

бы в малой доле принял участие в создании культа личности Сталина, то, исходя из его партийного авторитета, вполне мог бы войти в состав высшего политического руководства страны. Но уже с середины 20-х годов он занял антисталинскую позицию и в результате оказался одной из первых жертв репрессий 1937 г. в органах государственной безопасности.

В советской науке в 20-е годы в области труда совершаются крупные открытия, разрабатываются приоритетные направления (зачатки теории гуманизации труда, производственной демократии, качества трудовой жизни и др.), к которым за рубежом пришли гораздо позже. Эти идеи, в разработке которых принимали участие в том числе и представители старой научной и технической интеллигенции, были оплодотворены идеей перестройки и обновления. Полноценное развитие личности, создание условий для совершенствования мастерства, проявление самостоятельности, отказ от авторитарных форм управления и организации труда — характерные черты организации труда того времени, которые, к сожалению, не успели широко развиться. Как следует из приведенного текста проекта о создании Спецотдела, Г. И. Бокий, несомненно, выступал носителем, проводником всех этих идей. Как главнейшая ставилась для Специального отдела задача научной разработки вопросов шифровального дела. Обращают на себя внимание и другие четкие, профессионально продуманные формулировки, в том числе такие: «...выработка программы школы шифровальщиков и методов преподавания в таковой...» или «распределение... сотрудников всех шифрорганов между последними в зависимости от индивидуальных качеств каждого работника...» и т. д.

Для реализации задуманного проекта Г. И. Бокий пригласил на работу в отдел старых специалистов-

криптографов. Представляется очевидным, что в разработке самого проекта создания Спецотдела приняли участие и В. Н. Кривош-Неманич, и И. А. Зыбин, и И. М. Ямченко. Вклад каждого из них в становление советской криптографической службы огромен. Их опыт работы уникален.

В. Н. Кривош-Неманич, кроме блестящего знания множества иностранных языков, выдающихся дешифровальных способностей, обладал колоссальным опытом работы и уникальными знаниями. До революции В. Н. Кривоша-Неманича неоднократно направляли в заграничные командировки со специальными заданиями, в числе которых были и задания по сбору сведений о работе криптографических служб других государств. Приезжая из таких командировок, Кривош-Неманич составлял справки для руководства, делал специальные доклады, вносил свои предложения по совершенствованию работы специальной службы России Однако далеко не все его наблюдения использовались, не все его советы и рекомендации принимались. И теперь Г. И. Бокий самым тщательным образом изучал и анализировал все сведения, которые ему сообщал Кривош-Неманич, внимательно прислушивался к его советам, стремясь максимально полно использовать все полезное.

Так, несомненно полезным Бокий посчитал то обстоятельство, что, например, французская криптографическая служба добывала информацию для дешифрования различными путями и в разных видах. Материал, поступавший в секретную часть, состоял: из копий всех телеграмм, отправляемых или получаемых посольствами и вообще написанных шифром, из пост-пакетов с дипломатической корреспонденцией, из подлинных писем послов, приносимых в оригинале или снятых на пленку, из кодов, чертежей, планов, черновиков, рваных бумаг и т. д., которые добывались через подкуплен-

ных служащих посольств. Таким образом, в секретную часть Франции поступало решительно все и зачастую одна и та же бумага 4—5 раз: и в виде порванного черновика, и в виде зашифрованной телеграммы, и в виде корреспонденции из дипломатического пост-пакета. Этот способ многоканального получения материалов Бокий немедленно взял на вооружение.

Бокий знал, что средства, отпускаемые на криптографическую службу в других странах, огромны. Зато и результаты были ощутимы. Так, во Франции служащие секретной части получали оклады раза в 3—4 выше, чем служащие других ведомств. На непредвиденные расходы у них имелись неограниченные кредиты.

Другим важнейшим и необходимым условием успешной работы Спецотдела было наличие в его штате лиц, хорошо владеющих самыми разными языками, в том числе и малораспространенными. Именно отсутствие в штатах шифровально-дешифровальных служб дореволюционной России таких людей Кривош-Неманич считал одним из главных недостатков.

Все работники криптографической службы, включая технических работников (секретарей, посыльных и т. п.), должны быть заинтересованы в своей работе, для них должно быть невыгодно ее потерять. Так, во Франции женщины, служившие в секретной части в начале XX в. (переписчицы, склейщицы, дежурные в конспиративных квартирах, уборщицы и пр.), все были женами, сестрами, дочерями или содержанками служащих. Оберегать секрет порученного им дела было в интересах самих служащих, так как он их кормил, и кормил хорошо.

Французская служба была устроена по образцу английской и американской.

Вскоре после создания отдела его сотрудниками становятся такие бывшие сотрудники криптографи-

ческой службы царской России, как Г. Ф. Булат, Е. С. Горшков, Э. Э. Картали, Е. Э. Мориц и некоторые другие. К дешифровальной работе в качестве экспертов-аналитиков, как их тогда называли, в то же время или немного позже (1923 г.) были привлечены: Б. А. Аронский, Ф. А. Блох-Хацкелевич, В. И. Геркан, П. А. Гольдштейн, К. Н. Иосса, Р. В. Кривош-Неманич (сын В. Н. Кривоша-Неманича), Г. К. Крамфус, Б. Ю. Янсон, Г. П. Майоров, П. А. Мянник, В. К. Мицкевич, С. С. Толстой, И. Г. Калтград, Б. П. Бирюков и другие.

В создании основ новой криптографической службы приняли участие люди, до сего времени и не работавшие в этой области. Как мы говорили уже, это были люди, которых лично пригласил Бокий для работы в отдел, исходя из их деловых качеств. В числе их были: А. Г. Гусев, А. М. Плужников, Ф. И. Эйхманс, В. Х. Харкевич и некоторые другие.

В беседе с автором этих строк известный ныне писатель, а в 30-е годы сотрудник Спецотдела, зять Г. И. Бокия Л. Э. Разгон, хорошо знавший состав служащих отдела, вспоминал: «В спецотделе работало множество самого разного народа, так как криптографический талант — талант от бога. Были старые дамы с аристократическим прошлым и множество самых интересных и непонятных людей. Был немец с бородой почти до ступней. Был человек, который упоминается почти во всех книгах о Первой мировой войне — шпион-двойник, был Зыбин, председатель месткома, известный как дешифровальщик, прочитавший когда-то переписку Ленина...»

Кстати сказать, такое положение с кадрами было и в некоторых других отделах, где работали как члены партии, выходцы из рабочей среды, так и люди совсем иного рода. Так, например, в иностранном отделе (ИНО), где обязательно требовалось превос-

ходное знание иностранных языков, положение было аналогичным.

Подтверждение такого кадрового состава ВЧК—ОГПУ можно найти и в воспоминаниях Г. Агабекова — бывшего заместителя начальника ИНО, опубликованных в Париже в начале 30-х годов. Рассказывая о чистке, проведенной в ОГПУ в 1928 г., он писал: «В первую очередь началась чистка партячеек ГПУ. Комиссия — из вождей ЦКК — Сольца, Караваева и Филлера. Чистка началась в августе 1928 г. Проверяли личные дела, охотно донося, затем было партийное собрание, где все рассказывали биографии. Оказалось, например, что в Иностранном отделе нет сотрудников с пролетарским происхождением (ни одного). Много дворян, детей царских чиновников и др. Лиза Горская, предавшая Блюмкина, оказалась дочерью польского помещика... Но все оставили как есть, аппарат не тронули, так как все это были испытанные чекисты» [11].

Личный состав отделений Спецотдела проходил по гласному и негласному штату. К негласному штату относились криптографы и переводчики, для которых были установлены должности «эксперт» и «переводчик», работники же отделений, непосредственно не связанные с криптографической работой (секретари, курьеры, машинистки и др.), представляли гласный состав. К 1933 г. в Спецотделе по штатам числилось 100 человек, кроме того, по секретным штатам — еще 89.

Глава шестнадцатая

ТАЙНАЯ ВОЙНА

Спецотдел в 20—30-е годы

В связи с организацией Спецотдела 25 августа 1921 г. был издан приказ ВЧК, предписывающий всем органам ВЧК в центре и на местах всякого рода ключи к шифрам, шифрованную переписку и документы, обнаруживаемые при обысках и арестах, а равно добываемые через осведомителей, агентуру или случайно, направлять в Спецотдел при ВЧК.

Аналогичный приказ последовал при образовании Государственного политического управления (ГПУ) в 1923 г.

Работа Спецотдела началась с детального изучения наследства, полученного из архивов специальной службы дореволюционной России. Это были шифры, их детальное описание, документы по дешифрованию, материалы шифрперехвата. Среди этих документов, в частности, были материалы по дешифрованию шифров Турции, Персии, Японии, других государств, а также копии и подлинники шифров США, Германии, Японии, Китая, Болгарии, учебные пособия и др. Сотрудники отдела тщательно изучали эти материалы, осознавая важность проводимой работы. Большую роль в этот и последующий периоды сыграли знания и опыт И. А. Зыбина, В. Н. Кривоша-Неманича и других старых криптографов. При их активном участии при Спецотделе были организованы 6-месячные кур-

сы, на которых изучались основы криптографии, решались учебные задачи по дешифрованию. На курсы набирали людей способных и грамотных. Первый выпуск курсов состоял из 14 человек, пятеро из которых пришли на работу в дешифровальное отделение отдела, остальные — в другие отделения.

Необходимым условием успешной работы Спецотдела было наличие материалов шифрперехвата. В способах их получения сохранялись традиции дореволюционных служб. Кроме снятия копий с шифровок иностранных государств, проходящих через Центральный телеграф или доставляемых дипломатической почтой, чем занимался отдел Политконтроля, был усилен перехват шифртелеграмм, передаваемых по радиоканалам. С этой целью были задействованы военные радиостанции, предоставленные в распоряжение Спецотдела радиовещательные станции, в том числе радиостанция Коминтерна. Несовершенство радиоприемной аппаратуры, ее нехватка, а также сильная изношенность имеющейся не могли обеспечить высокой достоверности текстов перехватываемых шифртелеграмм. Таким образом, к трудностям первых лет работы Спецотдела, связанным с относительно невысокой общей подготовленностью и малочисленностью личного состава, прибавлялись трудности, связанные с недостатком и низким качеством материалов для дешифрования. Перед руководством Спецотдела встали задачи организации и налаживания работы всех звеньев специальной службы в стране, включая добычу шифрматериалов и техническое оснащение радиостанций. В этой связи Спецотделом проводилась работа по разработке и изготовлению специальной техники. В тесном контакте работал Спецотдел с Иностранным отделом ВЧК, а затем ОГПУ, контактируя и имея связь с агентурой, ориентированной на добычу шифров и кодов.

Сохранился отчет о работе Спецотдела за 1921 г. В нем, в частности, указано, что с самого начала ста-

ла успешно проводиться разработка и изготовление новых кодов и шифров. Только за этот год было введено в действие на различных линиях связи 96 новых кодов. Эта работа сотрудников Спецотдела активно поддерживалась правительством. Характерной для того времени является телеграмма секретаря ЦИК СССР А. С. Енукидзе Г. И. Бокию, хотя и относится она уже ко 2 сентября 1924 г. и связана с окончанием работы над телеграфным кодом:

«Поздравляю тов. Г. И. Бокия с окончанием составления «Русского кода» — этого громадного и сложного труда.

«Бытие определяет сознание». Бытие и необходимость современных сношений, быстрая связь и экономия во времени толкнули людей к созданию этого нового языка «кода», языка, не похожего ни на один человеческий язык.

Как маленький кусочек радия при разложении испускает колоссальное количество энергии, так и слова «кода» — короткие, непонятные и неудобопроизносимые для нашего языка, при расшифровке развертывают перед нами ряд фраз и мыслей, посылаемых или получаемых нами издалека.

Как стенография стала необходимой для точной записи и размножения человеческой речи, так и язык «код» становится и должен стать необходимым в сношениях между людьми, находящимися на разных точках земного шара.

Я уверен, что «код» получит широкое применение во всех наших учреждениях Союза ССР.

Раз темп работы Октябрьской революции нас привел к тому, что мы вынуждены были красивый и гибкий русский язык произносить с сокращением слогов, то по проводам и воздушным волнам мы смело будем сноситься концентрированным языком «код», тем более, что он будет доходить до адресатов в красивом, развернутом и понятном виде.

Я со своей стороны призываю все учреждения ввести у себя при сношениях по телеграфу и радио язык «код».

А. Енукидзе» [1].

Становление советской разведки и контрразведки потребовало от Спецотдела разработки агентурных шифров. Очевидно, что все советские разведчики, имена которых теперь уже хорошо известны (Р. Зорге, К. Филби и др.), могли успешно справляться со своими задачами во многом благодаря надежности и другим оперативным качествам шифрдокументов, изготовленных Спецотделом. Надо, однако, сказать, что в 20-е и 30-е годы, а частично и в более поздний период, агентурные советские шифры были уликовыми, их владельцы были вынуждены хранить у себя или ключи, или гамму, или инструкцию по шифрам, что создавало определенную опасность. Так, К. Филби в своей книге «Моя тайная война» говорит, что он вынужден был хранить инструкцию пользования кодом, написанную на крошечном клочке материала, напоминающего рисовую бумагу, в кармане для часов. И однажды при обыске только благодаря своей находчивости и самообладанию он сумел незаметно сунуть ее в рот и проглотить [2].

В конце 1919 г. знаменитому английскому криптографу Г. Ярдли удалось дешифровать советский агентурный шифр вертикальной перестановки по шифрсообщениям большого объема, изъятым у владельца немецкого аэроплана, приземлившегося в Латвии по пути в СССР. Колонки этого шифра были неодинаковой длины, что создавало большие трудности для дешифрования. Из расшифрованного сообщения следовало, что автор письма — резидент, руководящий советской разведывательной сетью обширного района на Западе. В числе дешифрованных сообщений имелась «Инструкция агентам, вербующим шпионов в дипломатических миссиях». В своей книге «Американский черный кабинет» Ярдли приводит ее полностью и отмечает, что Япония и Советский Союз являлись единственными странами, пытающимися добиться успеха в использовании конструкции кодовых слов неодинаковой длины. Он также говорит, что это — мощное оружие, при помощи которого можно запутать любую шифровку. Применяла такие шифры Россия и в 30-е годы.

С первых месяцев своего существования Спецотдел начал успешно проводить работу по дешифрованию иностранной переписки. Коллегия ВЧК принимала все меры к тому, чтобы организовать ее наилучшим образом и обеспечить полную секретность. Был установлен порядок, согласно которому обо всех раскрытых шифрах и добытых сведениях Спецотдел докладывал ЦК партии, Совнаркому, председателю ВЧК и руководителям других заинтересованных ведомств.

Коллегия ВЧК придавала большое значение оперативному использованию дешифруемой секретной переписки. Все срочные и особо важные дешифрованные сообщения докладывались немедленно.

Уже в то время дешифрованные материалы активно использовала советская разведка, Комиссариат иностранных дел, некоторые другие организации.

Для того чтобы читатель мог получить представление о проводившемся в начальный период существования Спецотдела дешифровании иностранной переписки, коротко остановимся на некоторых успешно проведенных работах.

Первый положительный результат был достигнут в разработке немецкого дипломатического кода, которым пользовался полномочный представитель германского правительства в Москве. Это был цифровой пятизначный код с перешифровкой гаммой многократного использования. Начиная с июня 1921 г., расшифровывалась вся переписка линии связи Москва — Берлин.

С 1922 г. Германия вводит на дипломатических линиях связи буквенный код с перешифровкой гам-

мой многоразового использования. Коды и большая часть перешифровальных средств раскрывались аналитическим путем в Спецотделе. Раскрытие таких шифров позволило контролировать переписку многих линий дипломатической связи Германии и ее консульств в Ленинграде, Киеве, Одессе, Харькове, Тбилиси, Новосибирске, Владивостоке вплоть до 1933 г., когда количество читаемой переписки резко сократилось из-за того, что немцы стали применять гамму одноразового использования.

В августе 1921 г. было осуществлено дешифрование первых турецких дипломатических телеграмм. Уже в начале 20-х годов криптографы Спецотдела добились возможности читать переписку внутренних линий связи Турции и отдельных линий связи военных атташе. Турки применяли главным образом четырехзначные коды с перешифровкой короткой гаммой, меняющейся через двое суток, а также коды без перешифровки. Дешифрованная переписка содержала сведения, представляющие большой интерес для советской стороны, и активно использовалась. Многие дешифрованные телеграммы направлялись, например, в Закавказскую ЧК, и это давало возможность принимать меры по пресечению шпионских действий иностранных, а в данном случае турецкой, разведок. В 1921 г. стала разрабатываться английская шифрпереписка.

Большую помощь Спецотделу в период 20—30-х годов оказал Иностранный отдел ОГПУ, разведчики которого добыли больше десяти английских кодов. По этим шифрам читалась часть дипломатической переписки, однако не вся, так как возникали сложности с раскрытием перешифровки.

Среди читавшейся переписки имелось много материалов, представлявших большой интерес для Советского правительства, органов советской разведки и контрразведки. В числе таких документов были, например, телеграммы о советско-английских отно-

шениях, о продаже англичанами оружия странам, граничащим с СССР, о деятельности английской разведки в Средней Азии и др.

Хотя работа по раскрытию польских шифров начала проводиться вскоре после организации Спецотдела, первые практические результаты были получены лишь в 1924 г., когда были раскрыты два кода II разведывательного отдела генерального штаба польской армии для связи с военными атташе в Москве, Париже, Лондоне, Ревеле, Вашингтоне и Токио.

Для органов ОГПУ особую ценность имели дешифрованные телеграммы, освещавшие шпионскую деятельность кадровых разведчиков, находившихся под официальным прикрытием иностранных дипломатических, военных и консульских представительств в СССР. Так, начатое в 1924 г. чтение дешифрованной переписки польских военных атташе позволило получать секретные сообщения польской разведки, пытавшейся широко проводить шпионскую работу на территории СССР. Советская разведка была очень заинтересована в получении подобной информации.

Естественно, что в начальный период своей работы Специальному отделу пришлось встретиться с большими трудностями. Опытных криптографов было мало, и каждому из них приходилось возглавлять работу по нескольким направлениям. Молодые сотрудники еще не обладали необходимыми криптографическими и языковыми знаниями. Перехват шифрпереписки по многим линиям связи велся нерегулярно, возможности выделенных технических средств были весьма ограниченны. Все работы, связанные с анализом шифрматериалов, проводились только вручную. Были и другие трудности. Однако по мере укрепления Спецотдела, роста мастерства его сотрудников объем криптографических исследований по раскрытию шифров начал неуклонно возрастать. К 1925 г. проводилась разработка шифров уже 15 государств. В 1927 г. началось чтение япон-

ской переписки, а в 1930 г. — переписки некоторых линий связи США.

Кроме разработки шифров иностранных государств, одной из актуальных задач дешифровального отделения Спецотдела в описываемый нами период была разработка так называемой внутренней шифрованной переписки, то есть нелегальной переписки белогвардейских и других контрреволюционных организаций, враждебных советскому строю политических группировок. Архивные документы показывают, что специалисты 4-го отделения Спецотдела смогли раскрыть сотни различных шифров, ключей и условностей, ими были прочитаны тысячи всевозможных писем, донесений и других конспиративных документов, в том числе исполненных тайнописью.

Одной из контрреволюционных организаций, шифрпереписка которой была впервые дешифрована в 1921 г., являлся руководимый Б. Савинковым «Народный союз защиты Родины и свободы». Анализом ряда шифрованных документов было установлено, что члены этой организации использовали шифры пропорциональной замены. Вскоре они были раскрыты.

Шифры организации Б. Савинкова строились в квадрате 10×10 или были шифрами по слову на длину алфавита, строки ключа чередовались. Фактически получались ключи к шифру или в прямоугольнике 10×30, или выявлялась 10-значная перешифровальная гамма. Было раскрыто 26 ключей к шифру и дешифровано более 30 документов, содержащих пароли, конспиративные явки.

В 1922—1924 гг. главным образом проходили материалы меньшевистских организаций. За эти годы было дешифровано 38 документов и раскрыто 17 ключей к шифру. По этим материалам было установлено 65 адресов с паролями и явками.

На протяжении 1922, 1927—1928, 1930—1931 годов проходили материалы монархических организаций.

Было раскрыто 39 различных документов, установлено 7 ключей и небольшой шифр-код на 1000 величин.

В начале 20-х годов Спецотделом было исследовано много шифрматериалов царского департамента полиции и жандармерии. Было прочитано 90 документов, по ним составлено 10 основных ключей. По дешифрованным материалам было установлено много секретных агентов полиции и жандармерии, работавших теперь на фабриках и заводах разных городов.

Перехватывалась и доставлялась в Спецотдел переписка уголовного розыска КВЖД. Было дешифровано 355 телеграмм, раскрыто 33 ключа к шифру и один код на 900 величин.

В эти же годы Спецотделом разрабатывались и материалы шифрпереписки различных зарубежных партий. В 1936 г. были раскрыты 3 шифра национал-социалистической партии Германии, использовавшиеся для внешних сношений. Ключом являлась перестановка простого шифра замены по свастике. Потом свастика разрезалась, складывалась в квадрат и из прямоугольника выписывалась.

Криптографическая служба в Красной Армии

В конце 20-х годов было положено начало дешифровальной работе в Красной Армии. 28 марта 1928 г. на совещании у начальника II отдела Управления делами Наркомвоенмора и РВС СССР было принято постановление об организации «военно-морской части по дешифровке в Центре, в Москве». Но дело продвигалось крайне медленно. Собравшееся 10 января 1929 г. новое совещание, посвященное тому же вопросу, на котором кроме руководителей ОГПУ и Спецотдела, представителей штаба РККА и Военно-морского флота были также работники морских штабов Балтийского и Черного морей, вновь подтвердило необходимость организации соответствующей дешифро-

вальной службы. Однако прошел еще год, а «военно-морская часть по дешифровке» еще не была создана.

В конце февраля 1930 г. Г. И. Бокий подготовил проект письма К. Е. Ворошилову, в котором писал:

«Специальный отдел при ОГПУ считает такой темп, взятый штабом РККА в разрешении вопроса об организации военно-морской части по дешифровке, слишком медленным. Желательно ускорить разрешение этого вопроса, т. е. в отношении дешифровальной службы РККА отстала от армий своих возможных противников, у которых это дело давно налажено».

И лишь в августе 1930 г. было создано первое дешифровальное подразделение при штабе РККА. Находилось оно в оперативном подчинении Спецотделу при ОГПУ и фактически входило в его состав. По штату оно проходило 13-м сектором 7-го отдела Штаба РККА. Приказом РВС от 5 августа 1930 г. вводилось Положение о 7-м отделе. В одном из пунктов этого Положения было записано, что на отдел возлагались вопросы организации дешифровальной работы, руководство и контроль над ней. «Начальник 7-го отдела в специальном отношении подчиняется начальнику Специального отдела при ОГПУ». Начальником военно-морского дешифровального сектора было решено назначить помощника начальника Спецотдела при ОГПУ Павла Хрисанфовича Харкевича. Вновь созданное подразделение было необходимо укреплять и расширять в кадровом отношении. Костяк его составили сотрудники Спецотдела, теперь уже бывшие. Но набирались и новые кадры.

Из письма начальника штаба РККА Б. М. Шапошникова начальнику Военной академии им. М. В. Фрунзе от декабря 1930 года: «При 8-м отделе вверенного мне Штаба (в этот период 7-й отдел был переименован в 8-й. — *Т. С.*) по приказанию народного комиссара по военно-морским делам и Председателя РВС СССР т. Ворошилова организован дешифровальный орган по дешифрованию шифрсообщений иностранных армий и флотов, а также изучения постановки шифрдела в иностранных армиях.

Учитывая сложность комплектования указанного органа соответствующими лицами, прошу выдвинуть 5 кандидатов из слушателей Западного и Восточного факультетов при вверенной Вам Академии, оканчивающих последнюю а 1931 г. Кандидаты должны быть членами ВКП(б) и владеть одним из нижеследующих иностранных языков: английский, французский, японский, польский и румынский».

Развитие дешифровальной службы в армии шло быстрыми темпами. Менее чем через год 13-й дешифровальный сектор реорганизуется в 5-й отдел 4-го управления штаба РККА, но по-прежнему остается в оперативном подчинении Спецотделу при ОГПУ. Все работники отдела имели хорошую языковую подготовку и зарекомендовали себя людьми, обладающими аналитическими способностями. Ведущими специалистами в дешифровании военных шифров того времени стали Б. В. Звонарев, К. Г. Тракман, П. М. Шунгский и др.

В январе 1931 г. открываются объединенные дешифровально-разведывательные трехмесячные курсы «спецназначения» для подготовки криптографов дипломатического и военного направлений. Начальником курсов назначается П. Х. Харкевич, а преподавателями Зыбин, Ямченко, Аронский, Кильдишев. В 1934 г. начальником этих курсов был назначен опытный криптограф, работавший в Спецотделе с 1921 г., С. Г. Андреев.

В связи с увеличением объема и повышением значения дешифровальной работы в 1932—1933 гг. создаются дешифровальные группы при полномочных представительствах ОГПУ в Киеве, Тбилиси, Хабаровске, Ташкенте и Ленинграде, а затем в Чите и Вла-

дивостоке. Позднее эти группы были преобразованы в дешифровальные отделения. Так, в 1932 г. создается дешифровальное отделение в Особой Краснознаменной Дальневосточной Армии (ОКДВА), а в 1935—1936 гг. — в Забайкальском, Среднеазиатском и Киевском военных округах. Эти отделения, так же как и в центре, находились в оперативном подчинении ОГПУ.

7 июня 1934 г. начальник 4-го управления (разведывательного) штаба РККА Я. К. Берзин, куда входила в то время армейская дешифровальная служба, представил наркому по военно-морским делам, председателю Реввоенсовета маршалу К. Е. Ворошилову доклад о дешифровально-разведывательной службе.

В докладе отмечалось, что дешифровально-разведывательной работой в стране совместно занимаются Спецотдел при ОГПУ и соответствующий отдел 4-го управления штаба РККА. Берзин в своем докладе раскрывает принципиальную сложность организации дешифровально-разведывательной работы и подготовки специалистов необходимой квалификации. Он пишет: «Дешифровально-разведывательная служба — одна из сложнейших специальностей. Подготовка кадров для нее — более трудное дело, чем в какой-либо другой области науки и техники». Берзин в этом докладе показал исключительно глубокое понимание важности и сложности криптографической работы. Он сформулировал основные качества, которыми должен обладать специалист-криптограф. Я. К. Берзин исходил из специфики работы, определяемой теми шифрсредствами, которые применялись в его время, но тем не менее все перечисленные им в докладе качества являются необходимыми для работника этой службы и сейчас, хотя, естественно, не охватывают всего.

Криптографы, как считает Берзин, должны:

— быть абсолютно преданными своему государству, так как они посвящаются в особо секретные государственные дела;

— иметь высшее образование;

— владеть в совершенстве не менее чем одним иностранным языком;

— владеть способностью к ведению самостоятельной работы научно-исследовательского характера;

— обладать широкой научной эрудицией;

— обладать беспримерным терпением;

— обладать быстрой сообразительностью и хорошей ориентировкой;

— обладать незаурядной угадливостью;

— обладать комбинационной способностью.

Он также считал, что просто удовлетворять указанным требованиям не достаточно. Чтобы стать хорошим специалистом, необходимо постоянно овладевать знаниями в области криптографии. «Такие работники, — писал Берзин, — вырабатываются в течение многих лет и только благодаря использованию накопленного ранее опыта в специальном деле...»

Общая численность дешифровального отдела 4-го управления штаба РККА была 46 человек. Однако для полного выполнения поставленных перед отделом задач такого количества специалистов было недостаточно. Берзин писал: «Шифрдокументы поступают от 52 стран, однако разрабатываются совместно со Специальным отделом при ОГПУ лишь только документы 22 стран... За 1933 г. при напряженной работе подчас за счет преждевременного износа умственных и физических сил работников ДРС разработано только 42% имеющихся для разработки материалов. 58% иностранных шифрованных документов, могущих дать ценную добавочную информацию, остались неразделанными из-за недостатка кадров».

В докладе была высказана просьба об усилении службы кадрами, в том числе предлагалось увеличить численность кадрового состава на 10 человек и перевести 16 человек вольнонаемных в административный состав.

Несмотря на скромность просьб, изложенных в докладе Берзина, они не были в 1934 г. удовлетворены, и отдел продолжал работать в прежнем численном составе.

Международная обстановка продолжала с каждым годом усложняться и это ставило перед Вооруженными Силами Советского Союза вопрос об усилении дешифровально-разведывательной работы.

22 ноября 1934 г. было объявлено Постановление ЦИК и СНК СССР об утверждении Положения о Народном комиссариате обороны СССР, согласно которому в его состав было включено Разведывательное управление, ранее входившее в состав штаба РККА. 15 декабря 1935 г. был изменен и утвержден новый штат Разведуправления РККА, в который дешифровальная служба вошла под наименованием 7-го отдела. Численность отдела составляла 53 человека и 5 человек постоянного состава было выделено на Центральные курсы ДРС.

Начальником 7-го отдела был назначен полковник П. Х. Харкевич, его заместителем майор Б. В. Звонарев — замечательный криптограф, в совершенстве владевший четырьмя иностранными языками — тремя европейскими и японским. В 1935 г. за выполнение специального задания командования он был награжден именными золотыми часами наркома обороны, а в 1936 г. — орденом Красного Знамени. Дело в том, что специалисты дешифровально-разведывательного отдела совместно со специалистами Спецотдела раскрыли в октябре 1935 г. японский дипломатический код «ТИ», о чем было доложено начальнику Разведывательного управления РККА С. Г. Урицкому. Последний написал рапорт заместителю наркома Гамарнику. Однако Гамарник, учитывая важность события, распорядился доложить о нем лично наркому Ворошилову. Вот докладная С. Г. Урицкого К. Е. Ворошилову:

«15 октября с. г. японское правительство отклонило свой основной код и ввело вместо него новый. Создалась угроза не иметь информации о военных мероприятиях Японии по линии дешифровки японских шифртелеграмм в нужный момент. Помощник начальника... отдела РУ РККА т. Звонарев Б. В. совместно с работниками его подразделения тт. Шунгским, Калининым, Мыльниковым и работниками Спецотдела ГУГБ НКВД тт. Ермолаевым и Ермаковой в минимально короткий срок, в 6 дней, раскрыли указанный код и обеспечили бесперебойную расшифровку японских шифртелеграмм. Эти результаты достигнуты благодаря систематической подготовке т. Звонаревым своего подразделения к выполнению стоящих перед ним задач. Непосредственно при раскрытии кода особо важную роль сыграли тт. Звонарев и Шунгский.

Ходатайствую о награждении ценными подарками... т. Звонарева Б. В. и специалистов тт. Шунгского, Калинина и Мыльникова...»

На этом рапорте нарком обороны наложил резолюцию: «Наградить т. Звонарева золотыми часами, а остальных тт. серебряными (хорошими) часами. К. В. 27.XI.35 г.»

Итак, середину 30-х годов можно считать периодом завершения организационного становления криптографической службы СССР. К этому времени эта служба уже располагала в основном оформившимся объединенным криптографическим аппаратом в центре и дешифровальными подразделениями на периферии — в некоторых оперативно важных территориальных органах ЧК, военных округах и флотилиях.

Глава семнадцатая

ПРОТИВОБОРСТВО

Советская разведка и иностранные шифры

Сведения о разведывательной деятельности являются абсолютно секретными и составляют особо охраняемую тайну в любом государстве. Естественно, абсолютной тайной в условиях существовавшего в стране режима была окружена деятельность советской разведки по добыче иностранных шифров в 20—30-е годы. Для многих такая информация представляется тайной и до сих пор. Однако на Западе сведения об этой деятельности ОГПУ—НКВД появились, и притом в открытой печати, в самом начале 30-х годов. Связано это было с тем, что в 1929 г. эмигрировал или, как говорят, «бежал на Запад» один из руководителей Иностранного отдела ОГПУ — Г. С. Агабеков.

Георгий Сергеевич Агабеков (настоящая фамилия Арутюнов) родился в 1895 г. в Ашхабаде, ушел со второго курса Ташкентского института восточных языков на войну и с началом революции покинул армию в чине штабс-капитана. В 1918 г. он вступил в коммунистическую партию. В это время Агабеков командует частями Красной гвардии в Туркестане, затем в Сибири занимает пост командира дивизии, сражаясь против армии адмирала Колчака. В 1920 г. Агабеков переводится на службу «по линии ВЧК». Он поступает в Иностранный отдел под начало

М. А. Трилиссера. Зная персидский язык, Агабеков стал заниматься проблемами Средней Азии и Афганистана. В 1922 г. он был на важной и ответственной работе в Бухаре в качестве «начальника агентуры». В Бухаре Агабеков наладил дело таким образом, что в его руки попал весь разведывательный аппарат бухарского штаба. В 1923 г. он был назначен начальником отделения контрразведывательного отдела ГПУ (КРО).

Сам Агабеков так мотивировал свое бегство из СССР в одной из эмигрантских газет Парижа:

«До настоящего времени работал честно и преданно для Советской России.

В последние два года я стал замечать, что революционный энтузиазм в СССР стал переходить среди коммунистических низов в подхалимство и бюрократизм, вырождаясь в заботу о сохранении своих мест и боязнь лишиться куска хлеба. Среди коммунистических верхов вопрос о революции свелся к борьбе за портфели.

В то время как эта привилегированная группа варится в собственном соку и, бросая революционные фразы о свободе и пр., на самом деле душит всякое проявление свободы — в это время рабочий класс приносит колоссальные материальные и моральные жертвы для осуществления преступно-фантастической пятилетки и физически истребляется, а крестьянство загоняется в колхозы и разоряется дотла, ибо, фактически разрушая индивидуальное хозяйство, сталинское правительство не дает взамен ничего. Результаты этого — перманентный голод в такой аграрной стране, как Россия. В области внешней политики — лживые революционные призывы к рабочим Запада. Одновременно с провозглашением лозунга «освобождение угнетенного Востока» сталинское правительство ведет империалистическую политику в Китае, Персии, Афганистане и на всем Ближем Востоке, что

я докажу фактами в своей готовящейся к печати книге.

В области торговли я считаю преступным при наличии фактического голода в России вывоз из СССР продуктов и трату вырученных денег на заполнение карманов совчиновников и поддержку компартий других стран.

С режимом, создающим невыносимую жизнь громадному стопятидесятимиллионному народу СССР и властвующим силой штыков, несознательности армии и неорганизованности классов рабочих и крестьян, — я обещаю отныне бороться.

Я имею сотни честных друзей-коммунистов, сотрудников ГПУ, которые так же мыслят, как и я, но, боясь мести за рубежом СССР, не рискуют совершить то, что делаю я.

Я — первый из них, и пусть я послужу примером всем остальным честным моим товарищам, мысль которых еще окончательно не заедена официальной демагогией нынешнего ЦК.

Я зову вас на борьбу за подлинную, реальную, настоящую свободу» [1].

Читая эти строки, кто-то, возможно, проникнется уважением к их автору. Может даже показаться, что поступок Агабекова был продиктован самыми светлыми устремлениями. И все же постараемся осмыслить это событие более глубоко.

Известно, что, начиная с Агабекова, некоторые другие советские разведчики также покидали свою родину, оказывались «невозвращенцами»: Игнатий Рейсс, Александр Бармин и даже резидент советской разведки в Западной Европе генерал Вальтер Кривицкий... Все они формулировали побудительные мотивы своего поступка примерно одинаково, так же, как и Агабеков, утверждая, что в СССР произошел «контрреволюционный переворот» и «Каины рабочего класса... уничтожают дело революции» [2].

Ниже мы еще вернемся к происходившим в 30-х годах в СССР событиям, здесь же рассмотрим поступки этих людей с профессиональной для них точки зрения. Конечно, политические взгляды и убеждения — дело сугубо личное, также частным делом являются и вопросы места жительства и т. п. Но ведь все эти люди были сотрудниками спецслужбы и потому являлись носителями важнейшей секретнейшей информации, представляющей государственную тайну. Оказавшись на Западе, ни один из них не счел возможным сохранить молчание о своей деятельности в советских органах госбезопасности. Каждый, как правило, выступал в прессе, весьма откровенно, походя, раскрывая разведывательные структуры, способы и методы работы разведки и многое другое. Они, очевидно, считали вполне моральным этой торговлей государственными секретами зарабатывать себе на жизнь. Борьба за правду и предательство — вещи несовместимые. Например, из Кривицкого Джейн Аргер — профессиональный офицер разведки из сотрудников МИ-6 (английская разведывательная служба) вытянула при допросе важнейшие сведения о том, что советская разведка послала в Испанию во время гражданской войны молодого английского журналиста. Этим был поставлен под удар советский разведчик Ким Филби. Он писал, что за время его службы (с 1934 по 1963 г.) «не было ни одной глубокой операции против советской разведки, которая принесла бы какие-то результаты. СИС («Сикрет интеллидженс сервис». — *Т. С.*) жила лишь неожиданными подачками, которые судьба буквально бросала иногда ей в руки, если не считать одного-двух исключений... Эти подачки приходили в виде редких перебежчиков из СССР. Они «выбирали свободу» подобно Кравченко, который, последовав примеру Кривицкого, быстро разочаровался и покончил жизнь самоубийством» [3].

В 1930 г. в эмигрантской газете «Последние новости», выходившей в Париже, были опубликованы воспоминания Агабекова [4]. В начале 30-х годов здесь же вышла его книга. В своих публикациях автор приводит сведения по интересующей нас теме.

Агабеков рассказал, что в середине 20-х годов чекистов весьма интересовали отношение Афганистана к басмачеству и роль афганского консула в Ташкенте в этом вопросе. Для целей осведомления был вы-бран переводчик Хубанио, таджик по национальности, так как афганский консул также был таджиком. Подосланный к консулу, Хубанио быстро с ним сдружился. Используя племенную вражду между афганцами и таджиками, он уговорил консула продать нам шифры и секретную переписку консульства. Консул запросил за это 10 тысяч рублей золотом. Так как денег не было, чекисты разработали следующую операцию. Выбрав день, когда в консульстве остались только консул и секретарь (охрану можно было не считать, так как она была нашей), Агабеков пригласил консула на ужин, а секретаря вызвала к себе его подруга. В конце пиршества консулу подсыпали в стакан снотворного и, когда он заснул, у него с часовой цепочки сняли ключи от несгораемого шкафа. Быстро проникнув в консульство, чекисты сфотографировали шифры и секретную переписку.

С 1924 г. Агабеков занимал должность начальника Восточного сектора ИНО ОГПУ в Москве, был резидентом ОГПУ на Ближнем Востоке (Турция, Греция, Сирия, Палестина, Египет). Из его воспоминаний, касающихся этого времени, мы узнаем, что большой интерес для чекистов представляла деятельность английского генерального консульства в Мешхеде. Состояло оно из генерального консула и военного атташе, являвшегося одновременно представителем индийского генерального штаба. Оба они переписывались с британским посланником в Тегеране и с индийским генеральным штабом. Штаб информировал военного атташе о положении на Востоке посредством месячных и шестимесячных сводок. Агабеков пишет: «Всю переписку мы аккуратно получали и пересылали в Москву (1923—1927 гг.), в ОГПУ». Делалось это так. У предыдущего резидента ОГПУ в Персии Апресова состоял агентом некто Мирзоев, глубокий старик, азербайджанец, родившийся в Персии. Еще в 1923 г. Мирзоев завербовал на персидской почте чиновника, ведающего иностранной корреспонденцией. Между Персией и Индией дипкурьеры были очень редки, и пакеты, запечатанные сургучными печатями, обычно доверялись персидской почте.

Завербованный советской разведкой чиновник задерживал на сутки корреспонденцию, получаемую на имя английского консула, и вечером, в день получения, передавал ее через Мирзоева чекистам. Пакеты немедленно вскрывались, документы копировались и в ту же ночь возвращались обратно. На следующее утро почту благополучно доставляли английскому консулу.

Апресов, а вслед за ним Агабеков вскрывали почту, а затем опечатывали ее, судя по описанию, абсолютно тем же способом, каким это делалось в царских «черных кабинетах» России в начале XX в. Печать изготовлялась тем же способом, о котором в свое время рассказывал Осоргин. Апресов документы переписывал, используя для быстроты почти весь наличный персонал советского консульства. Это было опасно и грозило провалом. В 1925 г. в Мешхед прибыл в качестве резидента Браун, старый партиец, друг Трилиссера, работавший до этого в Лондоне и Китае. Он несколько улучшил дело, начав фотографировать документы, за неимением электричества пользуясь магнием. Агабеков, прибывший ему на смену в 1926 г., работал так же. Вскоре старик Мирзоев

умер, продолжил работу его сын, получая 1 доллар за пакет.

Какую информацию получали чекисты, располагая шифрами и секретной перепиской в Мешхеде? В поступавших из Тегерана пакетах на имя английского военного атташе большей частью находились месячные сводки о положении в Персии, рассылавшиеся во все британские консульства из Тегерана военным атташе майором Фрэзером. Из Индии поступали сводки о положении в Западном Афганистане и в Южной Персии по донесениям Белуджистанского осведомительного бюро и английского военного атташе в Кабуле. Наконец, поступали отпечатанные в виде брошюр шестимесячные сводки о положении на всем Дальнем и Среднем Востоке. Необходимые документы отправляли в Москву.

В том же 1926 г. Агабеков был направлен в Тегеран. Вскоре одним из его агентов был завербован шифровальщик при Совете министров Персии. Это было очень кстати, потому что как раз в это время начались торговые переговоры в Москве между Караханом и персидским послом Али-Гулиханом. Благодаря услугам этого шифровальщика русские имели возможность получать все инструкции, посылавшиеся персидским правительством своему представителю в Москве. Советская сторона, таким образом, знала, по каким пунктам Персия готова уступить в крайнем случае, а из ответных телеграмм Али-Гулихана узнавали его подлинное мнение о различных пунктах проекта.

Эти сведения сослужили хорошую службу советскому послу в Тегеране, который в беседах с министром двора Теймурташем знал все его карты. Насколько хорошо было поставлено перехватывание шифртелеграмм персидского правительства можно судить по следующему случаю. Однажды полпред СССР в Персии Я. Х. Давтян, вернувшись от министра Теймурташа, вызвал Агабекова и сообщил, что

ему удалось убедить Теймурташа пойти на некоторые уступки. Теймурташ обещал послать Али-Гулихану в Москву соответствующие инструкции. Не будучи уверен, сдержит ли Теймурташ обещание, Давтян просил достать телеграмму, которую отдаст Теймурташ. Полчаса спустя копия такой телеграммы была доставлена Давтяну.

В 1925—1926 гг. советским военным атташе в Персии был Бобрищев — бывший офицер царской армии. Ему удалось завербовать себе на службу всех шифровальщиков главного штаба Персии, благодаря чему он знал не только дислокацию персидской армии, но был в курсе всех изменений в персидской армии и ее движения. Кроме того, в Персии перехватывалась вся переписка партии дшиналов. Нам известно, что при дешифровании этой переписки в Спецотделе были большие трудности, ввиду особой специфики языка. Тем не менее Спецотделом в 1924—1926 гг. было раскрыто 22 документа этой армянской молодежной организации и установлено 5 ключей к шифру.

Агабеков свидетельствует, что чекисты перехватывали корреспонденцию всех иностранных миссий в Тегеране: «Мы... изучали пути следования секретной корреспонденции иностранных миссий в Тегеране и наиболее важных персидских министров, главным образом Министерства иностранных дел и Военного министерства. Изучение путей и подготовка продолжалась четыре месяца. В сентябре 1927 г. вопрос был разрешен. Первой почтой, которую перехватил агент № 10, была турецкая. Она заключала в себе донесения турецкого военного атташе с подробными сведениями о событиях в Курдистане» [5].

Постепенно стали перехватывать переписку остальных миссий: английских консулов в Персии посланнику в Тегеране (консулы в Исфагани, Ширазе, Кермане и других местах), бельгийского посланни-

ка в Тегеране в Брюссель, а также французского, голландского, чехословацкого, японского, польского и немецкого консулов. Осторожнее всех были немцы. Они вкладывали запечатанные пакеты в металлическую трубку со специальным знаком, затем упаковывали трубку и запечатывали. Однако это их мало спасало. Вся их переписка наряду со всей другой аккуратно поступала в Москву.

В 1989 г. журнал «Собеседник», а затем газета «Правда» впервые поместили статьи о жизни и трагедии другого советского довоенного разведчика — Дмитрия Александровича Быстролетова [6]. Одиннадцать лет его считали одним из лучших советских заграничных агентов, а шестнадцать последующих лет он провел за колючей проволокой сталинских лагерей, где хотя и не погиб, но был физически страшно изуродован и превратился в инвалида. Быстролетов также говорил о том, какое внимание придавали советские разведчики в Европе добыче шифров.

Шел 1928 год. В советское полпредство в Париже пришел посетитель с желтым портфелем и едва ли не с порога предложил купить у него за 200 тысяч франков коды и шифры Италии. Причем в будущем гость пообещал за те же деньги сообщать о всех очередных изменениях шифров и кодов. Сотрудник советского представительства сфотографировал документы, убедившись в их подлинности. Но затем совершил грубейшую ошибку. Решив сэкономить деньги, он вернул подлинники документов посетителю со словами: «Это фальшивка. Убирайтесь вон, иначе я позову полицию». Однако когда с документами ознакомились в Москве, немедленно было решено возобновить контакты с хозяином желтого портфеля. Д. А. Быстролетову было поручено найти этого человека и возобновить получение от него материалов. Задача казалась невыполнимой, однако уже через два месяца советский разведчик добился успеха. Быстролетов установил, что человек,

приносивший документы в советское полпредство, был всего лишь передаточным звеном в торговле шифрами, организованной министром иностранных дел Италии графом Чиано, женатым, кстати, на дочери дуче. Спустя некоторое время хозяин портфеля — отставной офицер швейцарской армии по фамилии Росси — продал Быстролетову шифры.

Быстролетов же работал и с источником, получившим псевдоним «Арно». Это был человек, который однажды в начале 30-х годов явился к нашему военному атташе в Лондоне и представился рабочим типографии Форин офиса. Он предложил покупать у него копии экземпляров с тех ежедневных депеш, которые из разных стран слетаются во внешнеполитическое ведомство и размножаются после дешифровки в его типографии. Кроме того, незнакомец пообещал, если все пойдет хорошо, передать шифры и коды. Сначала «Арно» исправно поставлял обещанные материалы, но затем стал работать хуже. Тогда Быстролетову было приказано установить личность этого человека и за-ставить его работать активнее. С огромным трудом, с помощью множества ухищрений советская резидентура сумела установить, что типографский рабочий «Арно» — вовсе не дилетант, а профессиональный разведчик, высокопоставленный чиновник Форин офиса, специалист по разработке шифров и дешифрованию. К сотрудничеству с советской разведкой его толкнули долги. Быстролетов установил тесный контакт с «Арно» и регулярно получал от него документы и информацию. Однако в 1932 г., когда «Арно» заинтересовался сам сэр Р. Вэнситтарт — начальник британской разведки и контрразведки, Москва приказала всем работающим по этой линии, кроме Быстролетова, немедленно выехать на континент. «Ганс» (кличка Быстролетова) добился разрешения остаться еще, чтобы напоследок выбить из «Арно» шифры на будущий год. «Это был решающий момент, — вспоминал Дмитрий Александрович. — Моя

жена передала мне паспорт на имя А. Галласа и пистолет, чтобы при необходимости застрелился».

Впоследствии сэр Вэнситтарт, которому стоило большого труда замять скандал, связанный с разоблачением агента в недрах Форин офиса, сказал: «Какое счастье, что такие позорные истории в Англии случаются раз в сто лет». Он ошибался.

Большой интерес представляет, конечно, и вопрос о работе, какую проводили разведки различных государств по добыче советских шифров и кодов. В Национальном государственном архиве США в Вашингтоне хранятся документы третьего рейха, которые проливают свет на деятельность немецкой разведки того периода. Так, в 1932 г. в Буэнос-Айресе был украден советский код для коммерческой корреспонденции; были пересняты: общевойсковой командирский код № 5 «ОКК-5» 1938 г., переводная таблица дежурного радиста «ПТ 38-А» линий связи РККА 1938 г., постовой код СН и С Северного флота 1940 г., ключевая таблица № 14 (на 1-й странице указана маскировка показательных групп) 1940 г. и другие шифры. В 1938 г. были пересняты правила пользования кодом «Четвертый», в 1939 г. захвачен оперативно-тактический код «Третий» (наборно-разборная книга). Много там и шифрдокументов периода войны, особенно периода 1943—1944 гг. Хранятся там фотокопии: Инструкции органам НКВД по ведению шифрработы от 7 октября 1942 г., Инструкции по организации связи в авиасоединениях и авиачастях (книга около 50 страниц) 1943 г., кодовая таблица «ВС-22» 1948 г. и др. [7].

Обстоятельства добычи немцами этих документов нам пока не известны.

Проверка боем

В предвоенный период советской криптографической службой нередко практиковалось формирование особых оперативных групп для выполнения специальных задач. О работе некоторых таких групп нам бы хотелось рассказать.

Специальные группы комплектовались из числа опытных военных криптографов и разведчиков, которые направлялись в те районы, где велись военные действия. А таких мест в 30-е годы было немало. Такие группы командировались в Испанию, Монголию, Китай и другие горячие точки планеты.

Когда 18 июля 1936 г. радиостанция испанского города Сеута передала в эфир фразу «Над всей Испанией безоблачное небо», мало кто знал, что это условный сигнал испанским фашистам для начала мятежа против республиканцев. Вскоре сотрудники Спецотдела Ф. М. Огарышев, Г. К. Муха и З. В. Березин стали готовиться к командировке. После месячной подготовки они вместе с группой радиоперехвата на пароходе «Чичерин» отправились в Испанию. В порт Картахена группа прибыла на одиннадцатые сутки и сразу же направилась в Валенсию, где начала работу в помещении генерального штаба испанской республиканской армии. В первую очередь был организован перехват шифрпереписки испанских мятежников и итальянского корпуса, прибывшего на выручку генерала Франко. Основным шифром испанских мятежников являлся шифр пропорциональной замены с некоторыми усложнениями, но использовались и другие шифры.

Вначале криптографам было трудно: незнание языка и особенностей переписки привело к тому, что первые результаты работы дешифровальщиков были весьма скромными. Но постепенно с помощью словарей и испанских переводчиков овладели языком, изучили переписку и дело пошло. Группа стала давать все больше и больше информации республиканскому военному командованию и нашим военным советникам. В расшифрованных телеграммах широко освещалась деятельность мятежников, указыва-

лись источники и базы снабжения, приводились другие сведения.

Криптографам оперативной группы помогали и их товарищи в Москве. Выдающийся советский криптограф дешифровальщик Б. А. Аронский, работавший в Спецотделе с начала 20-х годов и внесший большой вклад в победу над фашистской Германией, вспоминал такой случай периода войны в Испании. В Москве была расшифрована телеграмма, в которой сообщалось, что из Марселя в Барселону или в другой порт, занятый «красными», выйдет судно с определенными внешними признаками. Командование испанских мятежников дало приказ крейсеру и авиации выйти навстречу кораблю и потопить его, под каким бы флагом он ни шел. Об этом немедленно было сообщено в Марсель еще до отплытия корабля. Оказалось, что на борту этого судна находилось много советских танкистов, летчиков и бойцов интернациональных бригад, следовавших в республиканскую Испанию. Благодаря советским криптографам их жизни были спасены.

Кроме войсковой переписки оперативная группа в Испании регулярно читала переписку агентурной сети мятежников по так называемому коду «Сиг». Эта агентурная сеть вела тщательное наблюдение за прибытием кораблей в порты республиканской Испании, прослеживая весь их путь в Средиземном море.

Оперативная группа закончила выполнение задания в начале 1939 г., ее работники были награждены орденами и ценными подарками.

В начале 1938 г. оперативная группа советских криптографов была направлена в Китай для оказания помощи китайской стороне в войне с Японией. В течение 19 месяцев опергруппой было раскрыто 10 японских войсковых шифров, которые широко применялись в японской армии в Китае и в военно-воз-

душных силах Японии. Ежемесячно группа расшифровывала около 200 телеграмм.

11 мая 1929 г. Япония напала на Монгольскую Народную Республику у реки Халхин-Гол. В соответствии с договором о взаимопомощи к месту событий прибыли части советских войск и вместе с ними специальная оперативная группа, разместившаяся в населенном пункте Тамгац-Булак. Еще будучи в Улан-Баторе, советские криптографы-дешифровальщики успешно начали снятие перешифровки к коду 1357, принадлежавшему Квантунской армии, однако сам код тогда еще не был раскрыт. В первых же боях этот код был захвачен нашими войсками, а так как действовал он до ноября 1939 г., то вся проходившая по нему японская шифрпереписка расшифровывалась нашими криптографами.

В дешифрованной войсковой переписке имелись ценные сведения о расположении частей противника, ходе боев, потерях, расходовании боеприпасов и другие данные. Во время военных действий оперативная группа криптографов ежедневно выпускала сводку расшифрованных телеграмм для командующего 1-й армейской группой войск Г. К. Жукова.

Работа иного характера

Изучая деятельность Спецотдела в период 20—30-х годов, нельзя ограничиться рассмотрением лишь криптографической ее направленности. Этот отдел проводил и иную работу, что определялось, на наш взгляд, двумя главными причинами. Во-первых, несмотря на то, что формально он был при ВЧК—ГПУ—ОГПУ—НКВД, его некая закрепленность за этими органами, увы, в определенной степени предписывала его сотрудникам выполнение и некоторых задач отнюдь не криптографического свой-

ства. Во-вторых, расширение функций Спецотдела определялось, по-видимому, в значительной мере тем, что Г. И. Бокий был, с одной стороны, членом коллегии ВЧК—НКВД, а два года (1925—1926) и заместителем Ф. Э. Дзержинского, а, с другой стороны, этот человек был видным государственным деятелем. Его традиционно ведущее положение в партии выделяло Бокия из числа других руководителей органов. Бокий был членом ВЦИК РСФСР всех созывов и членом ЦИК СССР, делегатом всех съездов партии, начиная с VI, куда он был делегирован как секретарь Петербургского комитета партии, член ЦК. Видимо, для таких деятелей партии, какими были Бокий и, естественно, Дзержинский, работа в органах была лишь одной из граней их деятельности по строительству государства нового типа. Бокий был и членом Верховного суда СССР, и видным деятелем Коминтерна.

Таким образом, масштаб работы, задачи, которые решали эти лица, были значительно крупнее, нежели деятельность одного ведомства, даже такого, как чекистские органы.

Аппарат же этих органов в целом, в том числе и сотрудники Спецотдела использовались в связи с этим нередко для решения общегосударственных проблем. В Спецотделе такая «специфика» его работы проявлялась практически с самого момента создания.

В начале мая 1921 г. Ленин лично поручил Бокию провести расследование, связанное с хищениями ценностей из Государственного хранилища ценностей в Москве (Гохрана). Этот факт известен и даже описан Юлианом Семеновым в его романе «Бриллианты для диктатуры пролетариата». Не вдаваясь в подробности, мы здесь остановимся лишь на некоторых обстоятельствах этого дела, десять томов которого и сейчас хранятся в Российском государственном военном архиве в Москве.

В 1920 г. московская ЧК уже проводила расследование хищений в Гохране, некоторые меры были приняты, но, как оказалось, результатов не дали.

Уже при первом ознакомительном обследовании Гохрана, проведенном 5—6 мая 1921 г., Бокий имел возможность убедиться, что разборка, сортировка, хранение ценностей (золотых, серебряных вещей, драгоценных камней и т. п.) осуществлялись здесь без должного учета, что дало возможность совершать крупные хищения как работникам Гохрана, так и призванным их контролировать работникам Рабоче-крестьянской инспекции (Рабкрина или РКИ).

Через несколько дней Бокий представил полный план расследования. Ленин одобрил его и предложил не только ревизовать Гохран, но и создать комиссию, которая бы подготовила предложения по исправлению его работы и работы Рабкрина. Возглавить комиссию было предложено Бокию.

Под видом инспекторов Рабкрина на работу в Гохран были приняты три сотрудника Спецотдела. С этого момента к Бокию регулярно стала поступать информация о состоянии дел в Гохране. Вскоре выяснилось, что основными расхитителями ценностей являются оценщики Гохрана Пожамчи, Александров и Шелехес. Как ювелиры, это были крупнейшие специалисты.

До революции Пожамчи представлял несколько заграничных фирм по продаже драгоценных камней в России. Вел дела с размахом, был хозяином крупных ювелирного и часового магазинов в Москве. Александров также прежде владел торговой фирмой по продаже драгоценных камней и жемчуга в Москве, в Антверпене имел фабрику по гранению алмазов. Был ювелирный магазин и у Шелехеса.

В сейфах этих трех лиц во время устроенной внезапной проверки обнаружили бриллиантов более чем на 4 тысячи карат. Притом таких бриллиантов, которые имели особую ценность на мировом рынке.

Крали ценности в Гохране и работники Рабоче-крестьянской инспекции.

Во время расследования хищений в Гохране между Бокием и Лениным произошел такой инцидент. Оказалось, что один из оценщиков Гохрана, а именно Я. С. Шелехес, имел двух братьев — старых революционеров. Семью Шелехесов знали Бухарин, Томский, Крупская и другие. Поэтому сразу же после ареста Якова Шелехеса от этих лиц последовали просьбы о его освобождении.

Ленин, под давлением родственников и знакомых Шелехеса, настаивал на его освобождении или смягчении меры наказания. Из письма Бокия Ленину от 9 августа 1921 г.:

«Вами поручено мне ведение следствия по делу Гохрана, о ходе какового следствия я Вас еженедельно ставлю в известность. Среди арестованных по сему делу имеется оценщик Гохрана гр-н Шелехес Яков Савельевич (родной брат т. Исаева-Шелехеса), за которого хлопочут разные «высокопоставленные лица», вплоть до Вас, Владимир Ильич... Эти бесконечные хлопоты ежедневно со всех сторон отрывают от дела и не могут не отражаться на ходе следствия.

Уделяя достаточно внимания настоящему делу, я убедительно прошу Вас, Владимир Ильич, разрешить мне не обращать никакого внимания на всякие ходатайства и давления по делу о Гохране, от кого бы они ни исходили, или прошу распорядиться о передаче всего дела кому-либо другому...» [8].

Ответ Ленина, полный глубочайшего возмущения строптивостью Бокия, пришел в тот же день.

И все же Бокий довел расследование до конца. Вина преступников, в том числе и Шелехеса, была доказана. Они были расстреляны.

В тот же период работники Спецотдела расследовали ряд других дел, в том числе хищения в Коминтерне. Нам бы хотелось обратить здесь внимание читателя на то, что главным в этой деятельности Бокия и его коллег было не просто ведение собственного расследования как такового, а поиски путей совершенствования работы государственных органов и учреждений.

Было у Спецотдела еще одно большое дело, которым занимались его сотрудники много лет и которое также было чрезвычайно далеко от криптографии.

Еще в 1919—1920 гг. ЦК партии поручил Бокию стать одним из организаторов системы исправительно-трудовых учреждений страны. Бокий привлек к этой работе и других сотрудников отдела. Однако, перед тем как коротко остановиться на ней здесь, позволим себе сделать некоторые предварительные замечания.

Мы не сделаем открытия, сказав, что вопрос об учреждениях подобного типа, создававшихся в России в первые годы Советской власти, сложен и заслуживает тщательного изучения, что, собственно, сейчас и делается, и не только силами ученых-историков, но и силами отдельных заинтересованных лиц и организаций, в том числе и общественных. Но все, что связано с системой сталинских лагерей, болью отзывается в сердце народном, это вечная и незаживающая рана. Именно поэтому этой теме посвящают свои произведения лучшие деятели нашей культуры, искусства, литературы. Однако исследователей подобной темы подстерегает, на наш взгляд, большая опасность — опасность оказаться во власти некой молвы, исходить в своих выводах из ложных или неточных посылок. Что мы имеем в виду? На наш взгляд, любое историческое исследование имеет реальную научную ценность лишь в том случае, если помогает, хотя бы в небольшой степени, приблизиться к пониманию истинной исторической картины, выявить подлинные причины исторических событий.

Последние годы книжные прилавки завалены изданиями на историческую тему. Но только часть из них представляет собой скрупулезные и добросовестные исследования. Большинство же написанных бойким языком творений весьма легковесны. То же самое можно сказать и о подавляющем большинстве мемуаров.

На ТВ на поток поставлены выступления лиц, до сего времени не имевших ничего общего с исторической наукой, теперь же с легкостью необыкновенной объясняющих зрителям события далекого и недавнего прошлого. Поражает категоричность суждений и оценок этих новоиспеченных «историков». В погоне за популярностью и сенсацией или по каким-то другим причинам, на основании выхваченных из общей картины фактов, а порой и просто слухов читатели и зрители приучаются категорично судить о людях и событиях. Как тут не вспомнить слова В. Каверина: «Умные, способные, образованные люди заняты тем, чтобы убирать малейшие преграды на торном пути читательского (зрительского, слушательского. — *Т. С.*) сознания».

Чешскому просветителю XVII в. Яну Амосу Каменскому мы обязаны появлением аббревиатуры SCHOLA — Sapienter Coqitare Honeste Operare Loqui Arqute — «Мудро мыслить, благородно действовать, умело говорить». Эти же «уроки истории» порой учат говорить безграмотно, а действовать — не думая о последствиях.

«Позвольте, а как быть с фактами, которые приводят очевидцы того или иного события?» — спросит меня пытливый читатель. Факты, как известно, вещь упрямая. Но вот очевидцы...

Один факт, даже яркий, на наш взгляд, еще не может быть основанием для окончательного вывода. Любой факт может быть истолкован субъективно, что обычно и происходит.

Для наглядности представим себе описание того или иного события, например какого-то боя периода Великой Отечественной войны, данное разными его участниками — солдатами, офицерами, генералами, видевшими все своими глазами. Их описания будут в значительной степени отличаться одно от другого, а возможно, окажутся даже взаимоисключающими. И причины тому могут быть разные. Во-первых, любые впечатления сугубо индивидуальны, во-вторых, все эти лица в бою стояли как бы на разном уровне, позволяющем понять и оценить ход происходящего. Чем такой уровень выше, тем шире поле обзора, больше информации, глубже понимание происходящего. Чем ниже уровень, тем субъективнее впечатление. Выжно и время описания. Если рассказ ведется по горячим следам, то сведения более правдивы и достоверны. Если уже прошло какое-то время, то последующие жизненные события накладываются на предыдущие и многое предстает в ином свете. На первое впечатление может оказать влияние и чье-то иное мнение, да и просто может подвести память.

Чтобы восстановить реальную картину прошлого, надо иметь не один факт, а целое море фактов, которые важно бережно сопоставлять и делать *предварительные* выводы. Факты необходимо прверять и перепроверять, искать им различные толкования и объяснения.

Ключ к пониманию исторических событий или персонажей получить чрезвычайно трудно. История от других наук отличается тем, что выводы в ней всегда носят относительный характер. Особенно важным нам представляется то, что изучающий историю должен попытаться проникнуть сквозь толщу времени, насколько это возможно, в сознание и мировосприятие людей *иного* времени, пусть даже не столь отдаленного. Ведь люди прошлого всегда другие, можно даже сказать, что они представляют другую цивили-

зацию. Наша логика — не их логика, их поступки детерминированы другой эпохой, они видели и знали то, чего не видим и не знаем мы. И рассуждаем мы об их поступках, исходя из нашего сегодняшнего восприятия действительности, лишенные, по существу, возможности рассуждать иначе. Именно поэтому надо, вероятно, быть особенно осторожными в выводах и избегать категоричности в суждениях.

Кто из наших читателей видел фильм Марианны Голдовской «Власть соловецкая», читал соответствующую литературу, тот наверняка вспомнит упоминавшиеся в этой связи фамилии Бокия, Эйхманса, некоторых других сотрудников Спецотдела. Кровавая история ЧК... Что можно, казалось бы, к этому добавить? Однако вопрос сложнее, чем кажется на первый взгляд. На основании многолетних исследований разных исторических источников мы приходим к выводу, что история советских исправительно-трудовых учреждений довоенного времени пережила по крайней мере два различных этапа. Первый из них относится к 20-м, второй — к 30-м годам. Это соотносится с эволюцией, которую претерпела советская политическая и государственная система того же времени.

Исправительно-трудовые учреждения существуют во всех странах. Однако они различны. Разница заключается в принципах организации таких учреждений, в методах их работы. Пришедшие к власти большевики начали в этом отношении, как говорится, «за здравие». Вспомним хотя бы знаменитую Болшевскую коммуну ГПУ, организованную в 1924 г. Сейчас о ней мало что известно, в отличие от коммуны, описанной А. С. Макаренко. Причина кроется в том, что вложившие душу в ее создание, в дело воспитания из уголовных элементов — кадров для воровского мира — полноценных граждан своей страны люди: М. С. Погребинский, С. П. Богословский и другие были расстреляны, а их дело, по существу, вычеркнуто из ис-

тории. Кто помнит теперь, что были коммунарами этой коммуны корифей нашего футбола Хомич и многие, многие другие. Житель подмосковного города Королева Яков Гиршевич Резиновский, с которым я познакомилась когда-то, еще с довоенных пор собирал материалы по истории этой коммуны. В результате его самоотверженной, подвижнической работы была создана уникальная огромная коллекция документальных материалов о людях той эпохи, их делах и судьбах. Разве не важен опыт их работы сейчас, когда на новом «революционном витке» ее истории нашу многострадальную страну вновь захлестнула волна преступности, в том числе и детской?

Спецотдел принимал участие в создании Болшевской коммуны, в работе с болшевцами. Однако главным для Спецотдела всегда был СЛОН — Соловецкий лагерь особого назначения. Бокий много лет возглавлял комиссию по инспектированию лагерей, в том числе СЛОНа. С 1922 по 1928 г., правда, с перерывами, заместитель начальника Спецотдела Ф. И. Эйхманс был начальником Соловецкого лагеря.

Кстати сказать, «открытие» Соловков в качестве лагеря принадлежит отнюдь не чекистам. В пору существования Северного правительства генерала Миллера здесь были расстреляны сотни «красных».

Эйхманс создал здесь организацию СОАОК — Соловецкое отделение Архангельского общества краеведения, в задачи которого входило изучение собственно научных проблем, связанных с биологией, гидрохимией, фауной островов, ведением фенологических наблюдений, а также работой историко-археологической секции, предполагавшей создание музея истории островов и Соловецкого монастыря. Читатель может посчитать, что мы что-то преувеличиваем, пытаемся приукрасить картину. Но нет, первые создатели системы лагерей делали упор на воспитательный,

созидательный аспект. В июне 1923 г. по случаю годовщины СОАОК Соловки посетили Шмидт, Руднев, Бенкен и другие известные ученые. Выступивший здесь на торжественном заседании профессор Бенкен предложил создать единый научный центр по связи общества с академической наукой, высказал пожелание организовать экскурсионную работу и присылать студентов на Соловки на практику с целью изучать и популяризировать их опыт.

В 1924 г. на Соловках стал издаваться журнал «Соловецкие острова» Во вступительной статье к первому номеру тот же Эйхманс писал: «...Исправительно-трудовая политика Соловецких лагерей, воспитательно-просветительная работа как метод этой политики, вопросы местной экономики и промышленности, изучение края, опыты ведения культурного сельского хозяйства на севере, пути, приведшие в Соловки невольных их обитателей, — вот содержание, определяющее... цель и задачи журнала...»

Сейчас можно говорить с презрением о наивности людей, отдававших все силы, здоровье, жизнь построению общества справедливости, но вряд ли это будет верной оценкой их деятельности. Когда-то в юности Дзержинский написал в письме сестре Альдоне: «Я хотел бы объять своей любовью все человечество, согреть его и очистить от грязи...» Вероятно, эти чувства были побудительными мотивами для многих его единомышленников, работников Спецотдела в том числе.

В 1930—1931 гг. Эйхманс возглавлял научную экспедицию на остров Вайгач, которая имела целью определить запасы свинца на острове и составить его геологическую карту. Экспедиция состояла из заключенных Соловецкого лагеря из числа «каэров» (контрреволюционеров — политических заключенных), среди которых были специалисты геологи, химики и т. д., а также других заключенных, составив-

ших три рабочие бригады. Два года провели участники экспедиции на острове. Их жизнь в это время не отличалась ничем от жизни участников любой другой научной экспедиции. Охраны не было. На пароходах «Георгий Седов» и «Глеб Бокий» завозили им строительный лес для поселка, продукты и необходимое оборудование. Бегала по острову овчарка по кличке Вайгач, подаренная Эйхмансу перед экспедицией... Армандом Хаммером Иногда прилетали самолеты. Остров был изучен досконально, карта составлена. После экспедиции все ее участники были отпущены на свободу Такая научная работа с заключенными была не случайна. Очевидно, что эти идеи принадлежали Бокию и его ближайшему окружению.

Другие сотрудники тоже в разное время работали с заключенными лагерей. Например, два года ведал лагерем на Колыме П. Х. Харкевич — помощник Бокия, будущий начальник армейской дешифровальной службы...

Картина могла бы сложиться весьма идиллическая, но мы далеки от такого понимания вещей. В недрах внешне, казалось бы, благополучной системы уже давно, в те же 20-е годы, зародился и теперь принимал все большие размеры монстр политической диктатуры, монстр террора. Искажалась сама суть государства и, как следствие, его жизнь во всех проявлениях. Эти искажения прежде всего сказались на структурах власти, на их функционировании. Повлияло это и на деятельность Спецотдела. Руководство отдела оказывалось все больше вовлекаемым в поток кошмарной круговерти. Руководители государства требовали решения общих задач, отодвигая решение криптографических, главных для отдела задач на второй план.

В стране все шире разворачивалась борьба с политическим инакомыслием любыми средствами и способами. Коллективизация, раскулачивание вызва-

ли голод в стране и, как следствие, недовольство политикой партии не только в деревне, но и со стороны голодающих рабочих и армии, состоявшей в своем большинстве из тех же крестьян. Прокатилась волна восстаний. Недовольных карали, и карали жестоко. В лагеря стали ссылать уже не только уголовников или каэров, если так можно сказать, прежнего образца, как это было в начале 20-х, а совершенно новую категорию «политических» — партийных оппозиционеров или им сочувствующих. Часто жертвами репрессий становились люди, не имевшие ничего общего ни с политикой, ни с оппозиционными группами.

Например, в ночь на 28 апреля 1933 г. в Луганске местными властями были произведены аресты среди рабочих, бывших когда-то членами социалистических партий, и интеллигенции. Всего арестовали до 400 человек с целью предупреждения готовящейся общей забастовки местных предприятий, в том числе металлургического завода им. Ворошилова. Среди арестованных оказались и партийцы, входившие в состав делегации, которая за несколько дней до этого была в Харькове у Г. Петровского с жалобой на сокращение пайка и на перерывы в продовольственном обеспечении, с просьбой об увеличении зарплаты в соответствии с ростом цен [9].

Кровавая фантасмагория, в которую оказалась ввергнута страна, тяжким бременем ложилась на души и совесть старых партийцев — теперешних государственных и партийных руководителей. Многие начинали осознавать ужас трагедии, пытались сопротивляться. Гибли в борьбе естественной и насильственной смертью. Можно предположить, что мысль о всеобщей причастности к созданию системы террора отравляла сознание и жизнь многих. Но не всех. Фанатики, стоя подчас в позе праведников, губили и предавали других. Потом, естественно, гибли сами в мясорубке порожденной

ими системы. В среде высших партийных и государственных деятелей атмосфера также становилась все более невыносимой. Чекисты пытались сопротивляться складывающейся системе. Уже в марте — апреле 1933 г. по требованию Политбюро ЦК, которое во все времена определяло задачи, стиль и методы работы всех звеньев государственной системы, в том числе и органов государственной безопасности, Коллегия ОГПУ была вынуждена исключить из союзных, краевых и областных коллегий ОГПУ 23 члена коллегий, а из краевых и областных управлений 58 руководящих работников органов. Их обвинили в примиренческом отношении к внутрипартийным оппозиционным элементам. Во исполнение решения Политбюро коллегия ОГПУ предоставила своим областным и краевым коллегиям право вынесения окончательных постановлений о применении «высшей меры социальной защиты» — расстрела по делам о вредительстве и саботаже в государственном хозяйстве без представления таких постановлений на утверждение коллегии ОГПУ.

Летом 1933 г. прокурор СССР, он же первый заместитель Менжинского Акулов и второй заместитель Менжинского — начальник Управления союзной милиции Прокофьев были кооптированы в состав Политбюро. Известно, что в 1936 г. был отстранен от должности и арестован Г. Ягода, ставший наркомом НКВД после смерти Менжинского, а до этого бывший уже с 1921 г. заместителем главы чекистских органов. Кроме обвинения в шпионаже, Ягоде были предъявлены обвинения в том, что органы опоздали с репрессиями на три-четыре года. Заступивший на пост наркома НКВД Н. И. Ежов, давно занимавший крупнейшие партийные посты (члена Политбюро, председателя ЦКК), был идеальным исполнителем для воплощения в жизнь активной репрессивной

и карательной политики. Переполнялись, и притом в значительной степени членами РКП(б), лагеря, которые не имели уже ничего общего с исправительно-трудовыми колониями начала 20-х годов. Только в июле — декабре 1936 г. в лагеря Западно-Сибирского края были отправлены 4767 человек [10]. Был открыт новый лагерь на севере Красноярского края в районе Дудинки. Это был концлагерь «особой изоляции» на 1000 человек, предназначенный для бывших партийцев, приговоренных к длительному заключению. Во второй половине 1937 г. в Енисейске была закончена постройка нового политизолятора «особого назначения» на 1500 заключенных. С назначением Ежова сеть политизоляторов росла с каждым месяцем: лишь с ноября 1936 г. по июль 1937 г. их было открыто восемь, а до того существовало всего три. Ежов начал проводить политику репрессий и против сотрудников НКВД. Им предъявлялись различные обвинения, в том числе в сочувствии партийным оппозиционерам, спасении людей от арестов.

В феврале — марте 1937 г. была проведена очередная чистка НКВД. Ежовым и его ставленниками были раскрыты «чрезвычайные злоупотребления» в аппарате НКВД, как в Центре, так и на местах со стороны «завуалированных троцкистов и других партоппозиционеров». Было установлено, что чекистами практиковалось «уничтожение в делах своих единомышленников опасных для них свидетельских показаний и замена их благоприятными показаниями несуществующих свидетелей», при обысках не приобщались к делам найденные компрометирующие материалы, «при помощи подлога» высылаемым изменялись места и районы ссылки, а осужденным к принудительным работам в концлагерях приписывался «параграф 0», предоставлявший право на платную должность и свободный выход в выходные дни, и т. д. и т. п. [11].

Документы, содержащие сведения о сопротивлении чекистов репрессиям 30-х годов, есть. Их изучение поможет прояснить многое в нашей истории. Ведь даже в самый страшный период 1937—1938 гг. такие примеры были. Так, в сентябре 1937 г. на партийные круги Воронежа поражающее впечатление произвело исчезновение референта по следственному производству областного отдела НКВД Гуднева. За день до своего исчезновения он освободил без доклада начальнику управления НКВД четырех человек, арестованных за «подрывную агитацию против ЦК и выпуск нелегальной литературы». Расследованием было установлено, что перед своим исчезновением Гуднев уничтожил находившиеся у него в производстве дела на лиц, арестованных по таким статьям Уголовного кодекса, которые грозили высшей мерой наказания. Одновременно с Гудневым скрылись освобожденные им лица [12].

Начальник Спецотдела НКВД, комиссар госбезопасности III ранга Г. И. Бокий был арестован 7 июля 1937 г. Постановление на арест подписал Н. И. Ежов Следствие по этому делу Ежов поручил вести своему заместителю, одновременно являвшемуся начальником Главного управления рабоче-крестьянской милиции (ГУРКМ) Льву Николаевичу Бельскому, 1889 года рождения, члену РКП(б) с 1917 г. Непосредственно допросы проводил старший лейтенант госбезопасности Али (Кутебаров Э. А.) — помощник начальника ОБХСС ГУРКМ. Пытали страшно. Почти одновременно с Бокием был арестован Эйхманс, которого Али лично знал с 1920 г.

В сохранившемся следственно-уголовном деле говорится о том, что Г. И. Бокий обвинялся в принадлежности к контрреволюционной масонской организации «Единое трудовое братство» и шпионской деятельности в пользу одного из иностранных государств.

Попробуем разобраться, что это были за обвинения и откуда они взялись, хотя это, на первый

взгляд, напрямую не связано с нашей темой. Дело в том, что в последние годы в некоторых публикациях стало упоминаться имя Глеба Бокия (до того забытое и малоизвестное) именно в связи с масонством. Авторов подобных сочинений можно понять: масоны — тема модная, а масоны в ВЧК — тема, интересная вдвойне. И вот мы наблюдаем, как без полного и глубокого изучения данного вопроса бойко используются материалы уголовного дела Бокия (ведь доступ для исследователей в специальный архив сейчас несложен). А вопрос-то совсем не простой, как не проста и личность Глеба Ивановича Бокия, изучению жизни и деятельности которого я посвятила многие годы. История криптографической службы России стала предметом моих научных исследований позже, а вначале был Бокий...

Началось все с приглашения на научный философский семинар В. Я. Козлова, доктора физико-математических наук, члена-корреспондента АН СССР, одного из руководителей 8-го Главного управления КГБ СССР, где я в то время работала.

На одно из заседаний семинара был вынесен доклад В. Н. Никифорова о Глебе Ивановиче Бокии. Именно здесь я впервые услышала эту фамилию и что-то узнала о первом руководителе криптографической службы Советской России. Вадим Николаевич Никифоров, старший научный сотрудник одного из отделов, в свое время принимал участие в подготовке исторического сборника, вышедшего в Управлении к 50-летию специальной службы, и заинтересовался Бокием. В. Н. Никифоров приводил известные ему материалы о Глебе Ивановиче и, главное, поставил вопрос о необходимости изучения жизни и деятельности этого человека, его вклада в создание нашей службы. Я решила работать над поиском документов и материалов о Бокии. Никифоров сразу же предостерег меня, что это будет нелегко: со времени ареста и расстрела Глеба Бокия его

имя не принято было упоминать в стенах нашего учреждения, и хотя он был реабилитирован еще в 1957 г., но до сих пор руководство не приветствует интерес к его личности. Возник вопрос: где искать хоть какую-нибудь информацию? Никифоров уже пробовал что-то найти, но не особенно успешно. Решили, что я начну поиски, опираясь на основные вехи биографии Бокия, указанные в первом издании Большой советской энциклопедии.

Уже через несколько дней, снабженная необходимым письмом о теме моего научного исследования, я отправилась в Центральный партийный архив. Однако на мой запрос документов о Бокии — секретаре Петербургского комитета РСДРП(б) в 1917 г., члене Русского бюро ЦК партии, одном из ближайших соратников Ленина в подготовке и проведении вооруженного восстания, мне была выдана тоненькая папочка с двумя листками бумаги, на которых рукой Бокия была заполнена краткая партийная анкета. И все. Собственно фонда Бокия не было. Начинать поиски пришлось практически с нуля. Имя человека, входившего в самое ядро ленинской когорты большевиков, имевшего партбилет за номером 7, известнейшего и авторитетнейшего петербургского подпольщика, практически отсутствовало в книгах и других печатных изданиях, где, по логике вещей, непременно должно было быть. С огромным трудом удавалось находить какие-то отрывочные сведения в архивах, разыскивать еще живых людей, его знавших. Именно тогда я впервые реально осознала, как мощно и мастерски была переиначена история нашей страны, из нее бесследно исчезли или потеряли всякое значение основные действующие лица, реальные события либо замалчивались, либо представлялись в искаженном свете. Именно изучая жизнь и деятельность Бокия, я поняла, как лживы наши учебники и другие источники по истории партии. Позднее я узнала о конкретных приказах

сталинского руководства, появлявшихся на свет в период репрессий 30-х годов за подписью уполномоченного СНК СССР по охране военных тайн в печати и начальника Главлита РСФСР Садчикова, которые обязывали все наркоматы и соответствующие учреждения проводить «тщательную проверку по изъятию из библиотек... всех книг, брошюр, портретов врагов народа, а также уничтожать скульптуру, диапозитивы на стекле и пленке, клише, негативы и матрицы с изображением врагов народа, перечисленных в приказах Главлита...» [13].

Архивы сохранили эти распространявшиеся Главлитом списки «врагов народа», сотни и тысячи наименований книг, брошюр и иных печатных источников, содержащих хотя бы краткие сведения об этих теперешних «врагах»... Имена и тем паче дела этих людей старательно стирались из истории. Незначительная часть таких тотально уничтожавшихся печатных источников сохранилась в фондах спецхранения некоторых библиотек. Естественно, доступ к ним был жестко ограничен.

Другой подобной акции по сокрытию правды история, наверное, не знает. Уничтожение книг в «самой свободной и счастливой стране мира» в 30-е годы озарено кровавыми отблесками костров из книг, разожженных фашистами и полыхавших в то же самое время в Европе. Разница лишь в том, что если веселые «наци» под звуки маршей тащили на костер книги, написанные чуждыми им писателями и философами, экономистами и историками, отнюдь не принадлежавшими к кругу национал-социалистов, то в Советском Союзе «республик свободных» «огню» предавались печатные источники, авторами которых были *свои* же братья по партии. Здесь была создана *система* уничтожения исторических документов и свидетельств.

В моем собственном окружении, в той самой службе КГБ, которая была детищем Бокия и кото-

рую он возглавлял 17 лет, о нем почти никто ничего не знал. Собственно, несколько человек мне говорили, что слышали это имя от прежде работавших сотрудников, но ничего толком не знали. Естественно, атмосфера в нашем ведомстве была такова, что ни у кого и в мыслях не было попытаться узнать правду. Чекисты старшего поколения, кого я еще успела застать, прекрасно владели всеми правилами игры, свято чтили традиции своего ведомства, сохранившиеся еще со сталинских времен.

В поисках материалов о Бокии я работала в партийных, исторических, специальных архивах Москвы, Ленинграда, Ташкента. Тогда же познакомилась с уголовным делом Бокия. Собирала материалы по крупицам, важна была каждая мелочь. Мне хотелось восстановить как можно полнее облик Бокия.

Я разыскала родственников Г. И. Бокия. Алла Глебовна Бокий, младшая дочь Глеба Ивановича, хотя и родилась в год его гибели и не могла помнить отца, рассказала мне кое-что со слов своей матери Елены Ивановны Доброхотовой, второй жены Бокия. Тогда же я познакомилась с зятем Бокия — бывшим мужем его второй дочери Оксаны – писателем Львом Эммануиловичем Разгоном, который в 30-е годы работал в Спецотделе ОГПУ, где был комсомольским вожаком и даже участвовал в комиссиях по чистке. Известно, что в те годы было проведено несколько чисток партийных рядов. Члены комиссий проверяли преданность и благонадежность членов партии и давали заключение оставлять их в партии или исключать со всеми вытекающими последствиями.

Разгон знал и помнил многих сотрудников, рассказывал об их работе, об атмосфере, царившей в отделе. Рассказывал о лагере, в котором сидел, о гибели своей первой жены Оксаны Бокий, страдавшей диабетом и оказавшейся в заключении без медицинской помощи, об их маленькой дочери Наташе.

Совершенно особенными были мои встречи с

племянником Глеба Ивановича, сыном его старшего брата Бориса, Георгием Борисовичем Бокием – крупным ученым, членом-корреспондентом Академии наук, сотрудником ФИАН. После смерти отца в 1927 г. Георгий Борисович, в то время семнадцатилетний юноша, очень сблизился с Глебом Ивановичем, подолгу жил у него. Конечно, он многое знал и многое помнил. Но кроме его рассказов из наших встреч я вынесла еще одно: смогла представить себе облик Глеба Бокия. Дело в том, что Глеб, Борис и Георгий Борисович были очень похожи. Разговаривая с Георгием Борисовичем, я постоянно чувствовало это сходство: культура речи, деликатность в общении с людьми, широта интересов моего собеседника приоткрыли передо мной атмосферу семьи Бокиев, мир, в котором вырос и который впитал в себя когда-то Глеб Иванович Бокий.

Меня могут упрекнуть в чрезмерном пристрастии к моему герою. Это верно лишь отчасти. Ведь по мере сбора материала сквозь толщу времени для меня все явственнее проступали черты Глеба Ивановича Бокия – красивого и сильного человека, романтика и бесстрашного борца за свободу и демократию.

Шло время. Я работала над сбором материалов уже около пяти лет и все чаще стала задумываться над тем, что пора писать книгу. Однако было одно «но»: следовало получить специальное разрешение.

По существующим правилам, выход в открытый мир со своими публикациями или выступлениями сотрудников нашего ведомства, включая ученых, мягко говоря, не приветствовался. В отдельных случаях, когда тема таких публикаций была далека от наших внутренних вопросов, работы разрешалось печатать, но только после тщательной экспертизы их содержания специально создаваемыми комиссиями. Теперь же вопрос встал о публикации книги об одном из руководителей ВЧК—НКВД. За разрешением я отправилась к «главному ученому» нашей службы Владимиру Яковлевичу Козлову.

Выслушав мою эмоциональную речь, он, помолчав, сказал: «А вы знаете, какой это был страшный человек? Про него говорили разное, про какие-то оргии на даче...» — И он вновь пересказал мне покрытую паутиной молву. «Но, Владимир Яковлевич, после ареста Бокия про него специально распускали ложные слухи, не упоминали его имя в книгах, старались уничтожить все воспоминания о нем. Бокия вообще выбросили из истории страны, предварительно облив грязью. И с дачей все было совсем не так, как в распущенных слухах. Ведь столько лет прошло, пора все расставить по местам». Убеждала я начальника долго и наконец он сдался: «Хорошо, но только о жизни Бокия до его службы у нас». Я заверила Козлова, что так и будет. Когда я, счастливая, что получила разрешение, пошла к двери огромного кабинета, он проговорил мне вслед: «А вы знаете, говорили, что Бокий любил женщин!» — «Правда? Действительно, аморальный субъект! Но, знаете, Владимир Яковлевич, думаю, это было не единственное его достоинство!»

Прекрасный криптограф, опытнейший руководитель, замечательный человек, Владимир Яковлевич всегда оставался человеком системы и моей шутки не понял. Или сделал вид, что не понял.

А что касается женщин... В юности, на ежегодных балах, которые давались в Горном институте, на вечерах, проводившихся украинским студенческим землячеством, главой которого многие годы был Глеб Бокий, наверное, не одна из петербургских курсисток заглядывалась на него. Особенно когда Глеб брал гитару в руки и запевал сильным баритоном то задушевные украинские, то веселые студенческие песни.

Любил Глеб свою первую жену Софию Доллер, мать его двух дочерей. Поэтому, вероятно, совсем не простым было для них расставание в 1919 г. после

десяти лет совместной жизни. О душевном состоянии Софии Александровны красноречиво говорит ее письмо Горькому, написанное сразу после разрыва с Глебом:

«...Месяц пролежала я больная в постели. Давят, душат эти проклятые стены. И так хочется вырваться из тисков этого города на простор и раздолье степей. И вот, когда становится невмоготу, когда нет сил жить настоящим, я беру Ваши книги, Ваши первые тома, где так много солнца, воздуха, где степь и море пели Вам песни свои, вся целиком ухожу в них — все, все забываю — горе, невзгоды и становлюсь другой, освеженной, отдохнувшей. И такое чувство глубокой благодарности является к Вам. Так хочется Вас видеть и сказать Вам большое спасибо от всей глубины души...»

Много лет после развода Глеб Бокий жил один, воспитывал свою старшую дочь Лену. Младшая дочь Оксана осталась с матерью, которая вскоре вышла замуж за ближайшего друга Глеба, его однокашника по Горному институту, крупного советского государственного деятеля Ивана Михайловича Москвина.

Любил Глеб Иванович и свою вторую жену Елену Доброхотову, также работавшую в Спецотделе. Их маленькой дочке Алле было всего несколько месяцев, когда Бокия арестовали.

Из своих товарищей по партии Бокий любил и ценил трех женщин, глубоко перед ними преклонялся: Надежду Константиновну Крупскую, Елену Дмитриевну Стасову и Нину Августовну Подвойскую. Много было вместе сделано и пережито.

Яркой чертой личности Глеба Бокия была его способность увлекаться чем-то новым, пытаться познать или найти что-то неизведанное. Так, еще в юности он увлекся идеей найти сокрытый где-то трон Чингисхана. И всерьез этим занимался во время поезд-

ки на реку Чу в составе экспедиции генерала Джунковского и работы десятником на строительстве «кругобайкальской», как тогда говорили, магистрали. У него был огромный интерес к идеям Блаватской и Рериха, искавших загадочную страну Шамбалу. Когда Елена Ивановна Рерих приезжала в середине 20-х годов в Москву с посланием «от махатм из страны Шамбалы», Бокий встречался и говорил с ней. Отсюда интерес Бокия к масонам. Он считал, что масоны бывают разные: современные, с деятельностью которых надо бороться, и масоны древние. Еще в начале 20-х годов Бокий, заинтересовавшись легендой о стране Шамбале, рассказал о ней друзьям. Он говорил об обитателях этой страны как о древних масонах — поборниках свободы и в какой-то степени носителях идей коммунизма. Глеба Бокия связывала многолетняя, со студенческих лет, дружба с писательницей М. В. Ямщиковой (псевдоним Ал. Алтаев). В начале века Маргарита Владимировна, будучи женой студента Гапеева, принимала участие в бурной жизни студентов-горняков, позднее помогала Бокию и Максиму Горькому в организации работы журнала «Молодая Россия», а в год революции была привлечена Бокием к работе в газете «Солдатская Правда». После революции у Алтаевой часто собирались бывшие студенты-горняки Иван Москвин, В. Кострикин, Борис Стомоняков и другие. Почти всегда бывал и Глеб Бокий. Бывшие однокашники, многие из которых теперь стали крупными государственными деятелями, известными специалистами, за чаем в уютной обстановке скромной алтаевской квартирки вспоминали старые годы, шутили, пели старинные студенческие песни. Иногда разговоры велись и на современные темы. Так продолжалось до ареста Бокия.

Как-то в разговоре с Алтаевой он сказал, что название «Шамбала» указывает на присутствие в местности, где оно встретилось, когда-то «народной

мудрости», близкой к коммунизму, и там, где ручей, речонка или гора называются «Шамбала», была эта мудрость когда-то... Возможно, читатель воспримет с недоумением эти рассуждения Бокия. Но это было действительно так. Этим же его привлекли семинары Барченко, идея продвижения коммунизма на Восток, опираясь на «ростки коммунизма» в Шамбале. Никаким масоном он не был. Просто время было другое и люди были другие, нам — рационалистам — едва ли дано их понять.

В начале 1956 г. к Алтаевой обратилась Елена Дмитриевна Стасова с просьбой подписать письмо к прокурору о реабилитации Глеба Бокия.

В ответном письме Стасовой Алтаева пишет 2 апреля 1956 г. (не могу не привести его почти целиком):

«...Благодарю Вас за совет относительно Глеба, но спешу вывести Вас из заблуждения, не по моей вине случившегося. Вы советуете мне указать номер моего партийного билета под подписью к прокурору, но ведь у меня нет никакого партийного билета, так как я никогда не была членом партии и никогда за такового себя никому не выдавала. Я работала в Военной организации в 17—18 годах как беспартийная и даже скрыла, что я писательница, считая, что меня будет легче руководителям учить непривычной газетной работе...

Но что мне писать в отзыве? Что я знаю Глеба со студенческой скамьи, после отсидки в тюрьме, знаю в момент Октября, что он меня привлек к работе в «Солдатской Правде»? Что я с ним общалась до его исчезновения с горизонта Москвы и что я убеждена в его беззаветной преданности партии?..

*Леночка (*старшая дочь Бокия, в тот момент только что вернувшаяся из ссылки, где она провела восемнадцать лет. — *Т. С.) в ужасном положении. Ей некогда делать ни «умности», ни глупости: ради куска хлеба она взяла место машинистки в тресте на 400 р., из которых платит за угол 200 р., 200 остаются ей,*

и она до глубокой ночи щелкает на машинке, чтобы приработать, возвращаясь в 200-рублевый угол, чтобы переночевать...

Ей необходимо окончание дела с отцом — ведь это мешает ей получить документы о прежней службе, а я изнемогаю от своих и чужих дел, заваленная работой над выходящими книгами, которые в руках верхоглядов в издательствах приводят меня в ужас. И главное... то, что не знаешь, кому верить, — это самое ужасное. Хочется только с достоинством окончить этот отрезок жизни.

И вот моя подпись под «отзывом» и все «титулы» под ним сводятся к чему? Член Союза советских писателей, «старейшая»; стаж 66 лет; работала в «Солдатской Правде» до июльских событий 17 года; и дальше невозможно же перечислять и то, что делала как советский писатель. Будет ли это компенсировать отсутствие партийного билета?

Эти соображения заставляют меня просить заранее Литфонд после моей смерти и кремации похоронить меня на литературных мостках Волкова кладбища, где не спрашивают номер партийного билета и довольствуются принадлежностью к корпорации.

Простите, что я пишу, ударяя педаль на минор. Это невольно. Скажу откровенно — не могу привыкнуть к бюрократизму во всех инстанциях жизни, потому что помню хорошо весну революции и ту простоту отношений в Смольном и в Питере, которым давал тон Владимир Ильич и которая не привилась в Москве.

Целую Вас крепко несмотря на беспартийность
Сердечно Ваша Алтаева» [14].

Бокий и ему подобные большевики, вероятно, смогли понять и постигнуть происходящее раньше и глубже других. В этом кроется начало их трагедии. Вспомним март 1918 г. Жаркие партийные баталии по поводу Брестского мира. Впервые высказанный

Лениным тезис о спасении революции любой ценой. Именно Бокий и его окружение начали активное сопротивление этой «любой цене». Им приклеили ярлык «левых коммунистов», по существу, догматиков идеи. Они пытались сопротивляться, и за это их стали все дальше отодвигать на задний политический план. Кем стали уже в середине 20-х годов когда-то наиболее крупные партийные организаторы Яковлева, Бубнов, Бокий и другие их единомышленники? На первый план выдвинулись совершенно другие лица, которые и стали диктовать правила. С их помощью принцип достигать, как казалось, необходимого «любой ценой» набирал силу. В светлое общество будущего должны, обязаны радостно и с песней идти все. И неважно, что кому-то хочется не петь, а рыдать. И неважно, что любая революция режет по живому, что революционные потрясения раскололи страну, лишили родины миллионы людей, разбили семьи, породили кровь и злобу. Должны идти. А кто не хочет, того заставим. Или уничтожим. И ведь верили, искренне верили, что это справедливо.

Трагедия Бокия и ему подобных большевиков была, на наш взгляд, в том, что они понимали ту свою роль и ту свою ответственность за разжигание когда-то пусть и справедливого революционного гнева в массах, из которых и вырос страшный монстр террора. Справиться с ним оказалось невозможно.

Но Бокий всегда пытался сопротивляться нарушению закона. Архивы сохранили документы с именами множества спасенных им людей. Теперь кажется невероятным, что он, один из столпов партии, уже к концу 20-х годов не ходил ни на одно партийное собрание. Сталина презирал и не скрывал презрения. Его пытались убрать с поста начальника Спецотдела уже в начале 30-х годов, но он устоял — вероятно, сыграл роль партийный авторитет. Сталину откровенно говорил: «Не ты меня назначал, не тебе меня и снимать».

После ареста Бокия страшно пытали. Расстреляли только в октябре. Жертвами сталинских репрессий стали более 40 советских криптографов, в том числе Ф. И. Эйхманс, А. Г. Гусев и другие...

На пороге войны

События 30-х годов, фактическое вхождение криптографической службы страны в систему органов безопасности, сталинский террор нанесли ей существенный урон, однако служба продолжала работать, в определенной степени выполняя свои задачи. Можно утверждать, что в предвоенные годы не было ни одного важного события в международной жизни, которое не нашло бы своего отражения в дешифруемой переписке. Дипломатическая, военная, полицейская, разведывательная переписка позволяла получать важнейшую информацию.

Для того чтобы читатель мог составить себе представление о характере и значении дешифруемой в тот период переписки иностранных государств, возьмем такой важный вопрос международной жизни конца 30-х — начала 40-х годов, как агрессивный внешнеполитический курс Германии и Японии.

Если говорить о Германии, то центральное место в переписке этого периода занимала информация дипломатических органов, раскрывавшая ее планы в отношении европейских стран и ее политику продвижения на Восток. В дешифруемой переписке излагалась также позиция правительств ряда других государств по международным проблемам в связи с аналогичным курсом Германии. В этой шифрпереписке содержалась и убедительная информация о подготовке Германии к развязыванию войны против СССР, о создании блока агрессивных государств, направленного прежде всего против Советского Союза, о концентрации войск в граничащих с СССР районах, об усилении разведывательной деятельности, и другие материалы.

Так, в дешифрованной советскими криптографами переписке содержались сведения о преднамеренном обострении Германией отношений с нашей страной, передавались сведения о наращивании немецких войск в Болгарии, Румынии, Польше, Восточной Пруссии и Финляндии, то есть вдоль границ Советского Союза, о мероприятиях по противовоздушной обороне, эвакуации населения из пограничной зоны, о частичной и общей мобилизации в странах — сателлитах Германии, о предупредительных мерах, принимавшихся посольствами некоторых иностранных государств в Москве исходя из предполагавшегося нападения Германии на СССР, и многое другое.

Сведения о предстоящем нападении поступали вплоть до 21 июня 1941 г. из многих заслуживающих внимания источников, в том числе прочитанных документов государственных деятелей, дипломатов, военных атташе, разведывательных органов иностранных государств и в ряде случаев от правительственных и военных кругов самой Германии.

Сотрудничество между дипломатической и военной дешифровальной службами, сложившееся в начале 30-х годов и выразившееся в прикомандировании к Спецотделу сначала военного дешифровального отдела, а в 1939 г. — и созданного лишь за год до этого дешифровального отделения разведотдела Наркомата Военно-Морского Флота, имело своей целью объединение усилий этих служб для работы над раскрытием шифров иностранных государств, поскольку ни та, ни другая служба в отдельности в то время не располагала достаточными возможностями для самостоятельной работы.

Военные криптографы работали вместе с сотрудниками спецотдела над дипломатическими и военными шифрами. Особого разграничения между специалистами, формально принадлежавшими к разным ведомствам, не существовало. Нередко криптографы

Спецотдела использовались для работы над военными иностранными шифрами и даже являлись руководителями разработок. Бывало и обратное: порой свыше половины состава военных криптографов переключалось для работы над дипломатическими шифрами.

Следует отметить, что длительная совместная работа криптографов двух служб, а этот период продолжался около десяти лет, имела во многом положительное значение. Вместе с тем существовавшие условия работы военной дешифровальной службы в системе НКВД с течением времени становились помехой для ее дальнейшего развития.

В предвоенное время, то есть к концу 30-х годов, работа советских криптографов определялась значительной активизацией шифрованной переписки иностранных государств и увеличением ее перехвата. При этом работа усложнилась тем, что значительно повысилась стойкость наиболее важных иностранных шифров, некоторые государства стали применять на военных и дипломатических линиях связи шифровальные машины. К этому времени, например, основным шифром для связи верховного командования немецкой армии со штабами армейских группировок, корпусов и дивизий была шифрмашина «Энигма». В других армиях — японской, английской, итальянской — стали активнее применяться коды с перешифровкой. Японские посольства, аккредитованные в странах Азии, Америки и особенно Европы, наиболее важную переписку вели на так называемой «шифрмашине Б».

Кроме того, работа над иностранными шифрами в предвоенный период требовала большого количества квалифицированных работников, которыми советская криптографическая служба в то время еще не располагала ни в центре, ни на местах.

В силу этих, а также некоторых других причин, о которых мы скажем ниже, отечественная криптогра-

фическая служба в тот период была не в состоянии обеспечить в больших масштабах раскрытие иностранных шифрсистем. Главным образом это относилось к военным шифрам, в то время как, исходя из складывавшейся в конце 30-х годов международной обстановки, Советские Вооруженные Силы должны были получать точную и подробную информацию об иностранных армиях.

Уже начиная с середины 30-х годов стало резко увеличиваться количество передач шифрованных материалов по каналам радиосвязи. Специальная служба требовала организации перехвата максимально большого количества шифртелеграмм вероятного противника. Однако служба радиоразведки в то время была и малочисленной, и плохо вооруженной технически. Материал перехватывался с большими пропусками и с множеством искажений, что затрудняло его дешифрование.

В феврале 1939 г. начальник 4-го управления доложил начальнику Генерального штаба командарму I ранга Б. М. Шапошникову о том, что «радиостанции ОСНАЗ стали не в состоянии обеспечивать перехват всей шифрованной военно-стратегической и правительственной радиокорреспонденции капиталистических стран. С бурным ростом средств мировой правительственной радиосвязи и колоссальным ростом количества действующих радиостанций к стратегической радиоразведке СССР предъявляются чрезвычайно возросшие требования как в количественном, так и в качественном отношениях». Был проведен учет роста перехваченных телеграмм по годам и изложена просьба об увеличении штатов отдельных радиостанций.

Таким образом, к концу 30-х годов перед военной шифровально-разведывательной службой возникла еще одна непреодолимая в то время проблема — обеспечение достаточно полного и качественного шифрперехвата.

Эти и другие причины выявили необходимость немедленного создания самостоятельной военной дешифровальной службы, находящейся в полном ведении Наркомата обороны. В июле 1939 г. по этому вопросу было принято постановление Комитета обороны при Совнаркоме СССР. В соответствии с приказом наркома обороны от 16 июля того же года при 5-м управлении РККА был организован 11-й отдел — военно-дешифровальная служба. А через год, в августе 1940 г., этот отдел был преобразован в 10-й отдел разведывательного управления Генштаба Красной Армии. На этот отдел и его органы в военных округах было возложено дешифрование военной и разведывательной переписки иностранных государств. Дешифровальной службе были переданы из НКВД все действовавшие в войсковой переписке шифры, другие шифрдокументы, включая перехваченную шифрпереписку.

После выделения военной криптографической службы Спецотдел (в 1939 г. он был преобразован в 7-й отдел Главного управления государственной безопасности НКВД) в области дешифрования сосредоточил свое внимание на раскрытии шифров и чтении переписки дипломатических органов, атташатов, разведывательных органов (кроме войсковой разведки) и полиции капиталистических государств. Уже опыт работы советской криптографической службы в период 30-х годов показал, что именно дешифрование переписки позволяет добывать сведения о противнике, которые зачастую невозможно получить другими средствами разведки. Поэтому перед войной особое внимание было обращено на подготовку специалистов-криптографов и на привлечение на службу специалистов высокой квалификации. Но спохватились слишком поздно. Время было упущено. Лишь в мае 1941 г. из Московского университета и других учебных заведений на работу в криптографическую службу НКВД и НКО при-

шла значительная группа кандидатов физико-математических и технических наук и работников с высшим математическим и техническим образованием. Пополнение службы этими кадрами со временем позволило значительно расширить фронт проводимых работ и поднять уровень криптографических исследований.

Что же касается 30-х годов, то следует признать, что в этот период в советской криптографической службе наблюдалось постепенное отставание уровня научных исследований в теории криптографии, замерли поиски и разработка принципиально новых идей и методов дешифрования новых шифрсистем. Если указанное обстоятельство отрицательно повлияло на методы дешифрования применявшихся в то время ручных шифров и кодов с различными усложнениями, то оно сказалось просто катастрофически на разработке теории и практики дешифрования уже появляющихся в это время электромеханических шифраторов, и в первую очередь «Энигмы». Трудно сейчас сказать, как бы сложились первые годы Великой Отечественной войны, если бы советские криптографы обладали в то время методами дешифрования этой машины, как в состоянии были это делать англичане, а ранее — французы и поляки.

Уместно напомнить здесь, что «Энигма» — это название электрической дисковой шифровальной машины со счетчиковым движением дисков, которая использовалась верховным главнокомандованием вермахта, центральным аппаратом полиции, СД и СС Германии для шифрования секретных приказов, докладов и другой корреспонденции, передававшейся по радио и, следовательно, доступной для радиоперехвата. Гитлеровское командование было уверено, что передаваемые ими сообщения не поддаются дешифровке, но эти надежды оказались необоснованными.

Уже Первая мировая война дала сильный импульс развитию криптографии почти во всех передовых капиталистических странах и, в первую очередь, развитию методов криптоанализа, методов машинного синтеза.

Япония, например, приглашала к себе читать лекции по криптографии крупных специалистов из других стран, посылала на учебу в криптошколы своих студентов. В этом плане она «не брезговала» связями даже с такими, казалось бы, не очень развитыми странами, как Польша. Известно, что японцами приглашался читать лекции по криптографии капитан польской армии Ян Ковалевский — малоизвестный в то время специалист по кодам. В будущем Я. Ковалевский стал крупнейшим специалистом-криптографом, сыгравшим огромную роль в дешифровании немецкой шифровальной машины «Энигма». Накануне Второй мировой войны он был приглашен к себе британской разведкой. Кстати, в Польше у него была небольшая группа студентов, состоявшая из шести армейских и трех морских офицеров. Студентами Ковалевского были Ризабар Ито и Квишио Накасуки. Ито впоследствии стал блестящим дешифровальщиком иностранных кодов. В частности, он собственноручно раскрыл кодовую систему Плейфера (Playfair), применявшуюся на британских линиях связи, а также армейский полевой шифр. Ито был также переводчиком книги Ярдли «Американский черный кабинет», ставшей в Японии бестселлером. Позднее он возглавлял отделение связи в военно-морском генеральном штабе и сыграл важнейшую роль в создании «Красного кода» и особенно шифратора «Purple», которые использовались при шифровании наиболее секретной дипломатической переписки. Напомним, что служба радиоперехвата Японии была организована в 1929 г. в военно-морском флоте. В ее специальное отделение входили четыре офицера и три операто-

ра. Одним из офицеров был Накасуки — также ученик Ковалевского.

Польские специалисты писали, что «Энигма» была раскрыта в Польше в январе 1933 г., а работа над шифром продолжалась до сентября 1939 г. За несколько недель до начала войны Польша поделилась своими достижениями с союзниками — Англией и Францией. 22—25 июля 1939 г. польский генеральный штаб передал французам и англичанам по одному экземпляру машины «Энигма», описание методов дешифрования и средства автоматизации процесса дешифрования — так называемые «криптографические бомбы», являвшиеся по сути дела ранними вариантами компьютеров. Осенью 1939 г. в Гре-Арменвийе под Парижем был создан польско-французский центр под названием «Бруно» по раскрытию шифров «Энигмы». К центру был прикомандирован представитель британской службы шифров майор Макмиллан, который поддерживал постоянную связь с английским дешифровальным центром в Блечли (под Лондоном). Только за период с октября 1939 г. до поражения Франции в апреле 1940 г. в центре было дешифровано около 15 тысяч немецких оперативных приказов, секретных донесений, директив. Французское руководство заранее было предупреждено о многих намерениях противника, о группировке его войск, их дислокации и передвижении.

В книге английского автора Ф. Уинтерботэма «Операция Ультра» рассказывается, как западные союзники использовали этот успех в борьбе против гитлеровской Германии и развили его дальше с помощью созданной уже ими дешифровальной машины, получившей название «Ультра». Для развития и совершенствования организации дешифрования и был создан дешифровальный центр в Блечли при правительственной школе кодов и шифров, развернуты пункты для чтения сообщений «Энигмы» в различных частях земного шара,

сформированы специальные подразделения связи, продуманы меры по сохранению в тайне системы «Ультра» и ее работы. С конца апреля 1940 г. радиограммы, идущие из ставки Гитлера, высших штабов вермахта командующим и обратно в ставку, регулярно перехватывались и расшифровывались союзниками и докладывались английскому и американскому руководству — Черчиллю, Рузвельту, командующим войсками на театрах военных действий и другим лицам по строго ограниченному списку. Когда в 1942 г. в Англии была создана электронная вычислительная машина «Колосс», на раскрытие любой немецкой шифртелеграммы уходили буквально минуты.

Таким образом, на протяжении всей войны как командующие вермахта, так и японское командование, которому немцы передали «Энигму» для работы, были практически лишены возможности использовать такой мощный фактор, как внезапность. Точные сведения о противнике, которыми располагало англо-американское руководство благодаря системе «Ультра», облегчали ему планирование и ведение операций, давали огромное преимущество. Ничего подобного в Советском Союзе не было, хотя советские криптографы и сделали многое для победы над Германией. Достижения в годы войны таких криптографов, как С. С. Толстой, Аронский, Звонарев и других, по раскрытию шифров и кодов противника можно назвать выдающимися. Заметим, однако, что задолго до войны, в 1930 г., японцы купили ранний, несложный вариант «Энигмы» и приспособили ее для своих целей, в первую очередь для дипломатических каналов. Лишь в 1940 г. американцы разгадали этот шифр и поделились им с англичанами. Такую возможность подхода к электромеханическим шифраторам того времени русские криптографы и разведчики, вовлеченные руководством страны в крова-

вую политическую бойню внутри государства, также упустили.

Огромную роль сыграла информация, полученная с помощью «Ультра» во время боевых действий во Франции и эвакуации английских войск из Дюнкерка, в ходе «битвы за Англию», в сражениях в Северной Африке и Италии, при подготовке и осуществлении операции «Оверлорд», в сражениях в Нормандии и Западной Европе, в ходе войны на море. Верховный главнокомандующий вооруженными силами западных союзников на европейском театре военных действий американский генерал Эйзенхауэр назвал систему «Ультра» «решающим фактором победы союзников». Маршал военно-воздушных сил Великобритании Слессор говорил об «Ультра» как о «невероятно ценном источнике разведывательных данных», который оказывал «почти сказочное влияние на стратегию, а иногда даже и на тактику союзников».

К сожалению, англичане лишь в одном случае передали информацию, полученную с помощью системы «Ультра», Советскому Союзу, правда, без ссылки на первоисточник. У. Черчилль накануне нападения немцев на Советский Союз сообщил Сталину о сосредоточении крупных немецких сил в Восточной Германии.

Рассмотрим, что обеспечило успех англичан в дешифровании «Энигмы», а следовательно, те необходимые направления, те компоненты работы, которые были упущены советской криптографической службой в 20-е и 30-е годы.

1. Правильный прогноз развития шифрсредств. Внимание этому виду анализа.

Справедливо было подмечено, что шифр блочной гаммы одноразового использования, несмотря на его абсолютную криптографическую стойкость, не является перспективным. Он требует слишком большого времени для зашифрования и очень громоздок, чтобы применять его в сколько-нибудь широком масш-

табе. Поэтому пришли к правильному выводу о том, что наиболее вероятно обращение криптографов Германии к машинным шифрам, которые уже в 20-е годы получили реальное очертание и которые обладают такими важнейшими качествами, как быстродействие, легкость в обращении при шифровании и расшифровании.

В проведенном прогнозе с очевидностью представилось, что огромная германская военная машина, ориентированная на «блицкриг», должна иметь надежную и быстродействующую организацию радиосвязи, так как прокладка наземных линий едва ли будет возможна, а одноразовые шифры будут слишком громоздкими и совершенно неприемлемыми при большом объеме радиопередач. Нам неизвестно о ведении таких прогнозных анализов Спецотделом. Возможно, они и были, но документальные свидетельства этого пока не обнаружены.

2. Продуманные оперативные мероприятия.

Англичане своевременно давали своим агентам задание вести целенаправленный поиск такой шифровальной машинной системы. Сначала удалось найти польского механика, работавшего на заводе в Восточной Германии, где изготовляли искомые шифрмашины. Найдены были описания и чертежи всех изобретенных за последнее время шифрмашин, среди которых оказался патент первого варианта «Энигмы». Наконец, поездка в Польшу самого руководителя «40-й комнаты» криптографов Элестера Деннистона привела к удаче.

Подобные задачи перед советской разведкой, по-видимому, в тот период не ставились. Во всяком случае, возможность купить документы, связанные с машинным шифрованием или даже сами машины, как мы уже говорили, была. Вспомним, что этим воспользовались японцы. Вне поля зрения советской разведки оказалась и работа центра в Блечли.

3. Привлечение к работе научных специалистов, практиков-аналитиков и талантливых организаторов.

В Блечли были привлечены к работе несколько самых выдающихся математиков Англии: Александер, Беббут, Милнер Барри, Гордон Уэлгмет. Все они обладали помимо математических способностей даром глубокого анализа, расчета многочисленных возможностей вариантов, рассматриваемых, например, в шахматных партиях. Не случайно многие из перечисленных математиков были крупными шахматистами, а Александер — чемпионом Англии по шахматам. Вместе с ними трудились молодые специалисты-криптографы — Дилли Нокс, Дж. Х. Тилтмен, Оливер Стреги — незаурядные люди, создавшие электронную быстродействующую систему для дешифрования «Энигмы». Был там и Купер — также блестящий математик с превосходными музыкальными способностями, сильнейший игрок в бридж. Эти лица в кратчайшие сроки (почти за полгода) разработали или усовершенствовали методы дешифрования, построили электронную специализированную вычислительную машину «бронзовая богиня». К началу 1942 г. было создано уже новое поколение усложненных «богинь», которые обслуживались несколькими тысячами людей.

Вся эта работа привела к тому, что уже в феврале 1940 г. началась массовая передача зашифрованных радиограмм по линиям радиосвязи и их массовое дешифрование.

В Советском Союзе математики высокого класса были привлечены в криптографическую службу лишь в конце 40-х годов, когда уроки войны заставили правительство в корне пересмотреть свое отношение к ней. В 1949 г. было создано Главное управление специальной связи (ГУСС) при ЦК КПСС. Это означало, что криптографическая служба выводилась из чекистских органов и подчинялась непосредственно политическому руководству страны, то есть поднималась на совершенно иной уровень. Для ее укрепления и расширения были задействованы значительные финансовые и материальные ресурсы. Примерно в это же время в Математическом институте АН СССР (МИАН им. Стеклова), во главе которого тогда стоял классик советской математики И. М. Виноградов, его заместитель Марджанишвили создает и затем возглавляет Отдел прикладных исследований (ОПР). Организованный в то же время Отдел прикладной математики МИАН, выросший затем в крупный институт, возглавил М. В. Келдыш. Предполагалось, что отдел Келдыша будет работать, как принято говорить, «на космос», а ОПР — на криптографию. Для этой последней работы были привлечены и некоторые ученые из ленинградского отделения МИАН: А. А. Марков, Ю. К. Линник, Д. К. Фадеев и другие. Однако не все было просто. Некоторые академические ученые под разными деликатными предлогами отказались от этой работы «на КГБ», среди них называют имена крупного алгебраиста А. И. Мальцева, известного ученого академика И. Р. Шафаревича... Кадры математиков-криптографов стали готовиться на базе Московского государственного университета им. М. В. Ломоносова. Последовало запоздалое прозрение.

Лишь в этот момент было признано, что в 30-е годы внимание к криптографической службе было недостаточным, существовало непонимание и недооценка ее роли, места и задач в общегосударственном масштабе, что привело к явному отставанию от Запада вообще и от главного на тот период противника — Германии, Японии, в частности.

4. Своевременная организация работ по добыче ключей к «Энигме».

К началу апреля 1940 г. количество радиограмм «Ультра» резко возросло. Однако в это время «бронзовая богиня» еще была несовершенна и действова-

ла с перебоями. Англичанам помогла работа по добыче ключей. У берегов Норвегии был сбит немецкий самолет, на котором нашли машину «Энигма» с полным комплектом рабочих ключей. Позднее такое же ценное имущество было захвачено у немецкого танкового подразделения связи, проскочившего слишком далеко во время битвы за Францию. В мае 1941 г. моряки захватили немецкую подводную лодку с машиной «Энигма» и картой рабочих ключей в полной сохранности. Это не только обеспечило англичанам прямой доступ к секретным радиосообщениям противника, но и оказало бесценную услугу ученым из Блечли: они смогли завершить работу над «бронзовой богиней».

Известно, что в 1942—1943 гг. «Энигма» оказалась захваченной и одним из советских войсковых подразделений. Однако никаких последствий этот замечательный факт не имел: до конца войны машина пролежала на складе среди другого забытого и никому не нужного имущества. Как заметил когда-то Н. Н. Головин: «Научная организация требует не только выдающихся представителей науки — она требует также достаточно высокого уровня социальной среды. Без этого мысли выдающихся ученых уподобляются колесам, не сцепленным с остальным сложным механизмом. Они могут вертеться, но вся работа для данного механизма происходит впустую» [15].

Заключение

Взгляд на прошлое с позиций настоящего всегда подкреплен новыми накопленными знаниями, и в частности знанием последствий исторических событий. В этом смысле, конечно, такой взгляд более объективен и точен. С высоты времени всегда проще судить о событиях прошлого, говорить об ошибках, рассуждать о возможных иных путях развития. Обстоятельства легче анализировать, справляться с ними сложнее. По-видимому, и сегодняшняя наша деятельность тоже будет переоцениваться будущими поколениями, и в этих оценках найдут свое место и скепсис, и отрицание. И все же хотелось бы верить, что будет и понимание.

В заключение этой работы, посвященной истории Российского государства с точки зрения становления и развития одного из видов государственной деятельности — криптографической службы России, хотелось бы сделать некоторые выводы и обобщения.

Начало развития криптографии как необходимого и достаточно надежного средства сохранения государственных секретов в России, по существу, относится к эпохе Петра Великого. Этот период и весь XVIII в. характеризуется широким использованием шифрпереписки, организацией первых шифровальных служб, появлением первых наметок анализа, созданием шифров с последующим их усложнением. Разработка шифров, их доставка на места эксплуатации были четко организованы и подчинялись действию определенной системы. Постоянно разрабатывались шифры для индивидуальной, циркулярной связи и для все

расширяющихся систем общей связи, включавших большое число корреспондентов. Создававшиеся шифры постоянно усложнялись, что увеличивало их криптографическую стойкость. Из правил пользования шифрами видно, что составители шифров обладали навыками дешифрования, правильно понимали значение лингвистических, статистических характеристик шифрованных и открытых текстов для использования их при дешифровании. Русские шифры обладали своеобразием: активно использовались пустышки, многоязычные шифры, специальные усложнения, что затрудняло их дешифрование.

40-е годы XVIII столетия, а точнее 1742 г., можно с полным правом считать временем создания дешифровальной службы России. К этому периоду сложилась определенная система дешифровальной деятельности: была организована служба перехватывания и перлюстрации секретной шифрпереписки иностранных корреспондентов, организовано ее дешифрование, перевод, доклад сообщений в высшие инстанции. Была осознана необходимость организации криптографической службы как единой слаженной системы, важность придания ей научной базы. К дешифровальной аналитической работе был привлечен известный математик И. Х. Годьдбах, дело которого продолжил У. Т. Эпинус и другие крупнейшие ученые. Научный подход и активное внимание руководителей государства к специальной службе позволили России добиться быстрых и важных успехов в дешифровании переписки корреспондентов Франции, Англии, Германии — стран, где соответствующие службы были созданы значительно раньше и опыт работы был несравненно большим. Дешифрование иностранной переписки сыграло большую роль в выработке и осуществлении внешней и внутренней политики России.

В XIX в. в России, как и в других передовых государствах Европы, в вопросах применения шифров начинает постепенно входить и развиваться принцип

иерархии. Для каждого уровня корреспондентов, как правило, применялись свои системы шифров или свои правила пользования ими: от простых в эксплуатации, но менее стойких к сложным и более стойким.

Сравнивая шифры России с шифрами других развитых государств того времени, следует сделать вывод, что по крайней мере по криптографической стойкости, а также по ряду других критериев, включая (в определенной мере) и критерии, характеризующие эксплуатационные качества, отечественные шифры не уступали шифрам таких передовых стран, как Англия, Франция, Италия. Действовавшие в России разновидности кодов и многоалфавитных шифров были примерно теми же, что и в указанных странах. Российские криптографы успешно дешифровали переписку этих стран в течение всего рассматриваемого периода, естественно, творчески усваивая достижения зарубежной криптографии.

Увеличение объемов шифрпереписки потребовало упрощения процессов обработки информации и ускорения процессов шифрования и расшифрования. По этой причине в России в это время, как и в других странах, появляются различные шифровальные приспособления, облегчающие шифрование и расшифрование. Указанные в биклавных ключах приспособления типа таблиц, передвижных полосок-лам, календарей для набора и разбора, рамок служили этой цели. Практически эти приспособления весьма близки шифровальным устройствам, использовавшимся в середине и конце XIX века во Франции и получившим название «Линейки Сен-Сира», которые были разработаны специальной криптографической комиссией при военной академии Сен-Сир.

По-видимому, можно сделать вывод о том, что если Россия в чем-то и отставала от стран Западной Европы, то это все-таки относится к вопросам углубленной механизации и автоматизации процессов шифрования и дешифрования. К этому можно доба-

вить вопросы организации широкой подготовки кадров криптографов и разработки теории криптографического анализа шифров и опубликования результатов этой разработки в фундаментальных трудах, оказавших большое влияние на последующее развитие криптографической мысли.

Так, известно, что еще в начале XIX в. знаменитый Томас Джефферсон изобрел дисковый шифратор, состоявший из набора деревянных дисков, по окружности которых размещались буквы алфавита в определенном порядке. Диски устанавливались так, чтобы на некоторой горизонтальной линии находился открытый текст, тогда шифрованный текст получался на другой горизонтальной линии, определяемой ключом. Как и следовало ожидать, это изобретение не нашло применения в тот период. Но сам этот факт, несомненно, в последующем дал толчок созданию электромеханических дисковых шифраторов.

Другое изобретение, сделанное в 1860 г. лондонским профессором Чарльзом Уинстоном, представляет собой двухдисковый шифратор — весьма удобное для шифрования устройство, но, правда, содержащее малое число простых замен.

В чем еще можно усмотреть отставание России от стран Европы, так это, во-первых, в написании и публикации книг, посвященных теории криптографии и, в частности, анализу существовавших в то время шифров и методов дешифрования, и, во-вторых, в широте постановки вопросов изучения криптографии. В Европе в это время выходит книга Фридриха Казисского «Искусство тайнописи и дешифрования» (Германия, 1863 г.) и монография Огюста Керкгоффса «Военная криптография» (Франция, 1883 г.). Обе эти книги содержали глубокий анализ шифров, раскрывали многие методы дешифрования, включая и методы с использованием математики, формулировали основные требования к стойким шифрам, не потерявшие своей актуальности и в настоящее время.

В истории России XIX — начала XX в. нельзя назвать ни одного имени крупного математика или группы молодых специалистов, впоследствии выросших в крупных ученых, которые бы профессионально занимались теорией криптографии, анализом шифров и разработкой методов дешифрования. П. Л. Шиллинг в этом плане был скорее исключением, чем правилом, но и он был инженером-электротехником и не имел каких-либо крупных теоретических трудов в области математики. В то время в странах Западной Европы многие математики занимались вопросами криптографии, что в конечном счете не могло не сказаться в дальнейшем на ее быстром развитии в этой прикладной области исследования. Достаточно вспомнить профессора математики в Кембридже Чарльза Беббиджа, который успешно применял математические методы в криптоанализе. Он уже в то время конструировал и применял аналитические машины для вычислений, и его идеи о логической структуре вычислительной машины были в некоторой степени использованы в современных ЭВМ.

Известно также, что во всех главных государствах мира криптографию как предмет стали изучать в военных академиях с 1881 г. В России, к сожалению, такая практика запоздала приблизительно на два десятка лет. Что касается применения в России и странах Западной Европы кодов, то можно сказать, что они сравнимы по стойкости и по эксплуатационным качествам. Коды использовались без перешифровки. Известно, что перешифровка была введена, в том числе и в России, с целью увеличения криптографической стойкости только в XX в. после выхода в 1901 г. книги французского офицера Базери «Раскрытые секретные шифры», где автор доказал возможность дешифрования применяемых в мировой практике кодов в чистом виде без усложнений.

Криптография в России практически весь рассматриваемый период была уделом сравнительно

небольшой группы лиц, хотя и высокообразованных, квалифицированных и талантливых.

Опыт русско-турецкой и других войн показал, что используемые коды мало пригодны для целей шифрования в военных условиях. Эти шифры оказались громоздкими, ненадежными из-за большого числа ошибок, допускавшихся в процессе шифрования и расшифрования. Из этого опыта следовало делать правильные выводы и вести интенсивную работу по созданию новых стойких шифров, надежных в эксплуатации, поддающихся механизации и автоматизации.

К сожалению, в этих вопросах Россия стала постепенно отставать от Европы, что в конечном итоге сказалось уже в первой половине XX столетия — в Первой мировой и Великой Отечественной войнах. Общее отставание России в промышленном отношении от стран Запада не могло не сказаться на отставании в развитии средств и методов связи (телеграфной связи, радиосвязи), а следовательно, и на развитии шифрсвязи, что также проявилось в Первую мировую войну и в значительной мере повлияло на исход крупных сражений. В активе России не было крупных побед на суше или на море во время этой войны, которые были бы достигнуты за счет каких-либо успехов в использовании информации, полученной криптографическими методами, или за счет радиоигр или имитации сообщений от имени командования противника, посланных с помощью раскрытых шифров, как это было, например, у англичан против немцев (Ютландское сражение, телеграмма Циммермана, уничтожение немецких крейсеров адмирала Шпее в декабре 1914 г. у Фолклендских островов, вызов и уничтожение немецких циппелинов во Франции в октябре 1917 г.) или у немцев против тех же англичан (история спасения немецких крейсеров «Гебен» и «Бреслау»).

Криптография широко применялась в революционном подполье, однако большая часть перехватываемой переписки дешифровалась Департаментом полиции с помощью аналитических и агентурных методов. Шифры, использовавшиеся в подполье, создавались лицами, имевшими математическое образование и определенные знания в вопросах криптографии, поэтому методы для их дешифрования должны были быть достаточно высоки.

В период Гражданской войны значительная часть арсенала сил и средств, кадрового состава криптографической службы царской России была унаследована белой гвардией. Несмотря на то, что советская сторона частично располагала старыми кадрами специалистов-криптографов, имела в своем распоряжении системы шифров и кодов, применявшихся белой гвардией, из-за слабого оснащения станций радиоперехвата, отсутствия квалифицированных кадров в необходимом количестве, линии шифрованной связи белых практически не контролировались. Сохранившиеся в архивах материалы радиоперехвата представляют собой ценный исторический источник для более полного и детального воссоздания истории России указанного периода.

В начале 20-х годов в Советской России началось критическое осмысление состояния безопасности отечественных линий связи и определение организационных форм будущей шифровальной службы страны. В начальный период этой деятельности руководители страны уделяли этой службе должное внимание. В результате был создан Специальный отдел при ВЧК как единый центр криптографической службы страны. Структура отдела, кадровый состав, задачи и методы его работы во многом продолжали традиции специальной службы России. В этом было как положительное, так и отрицательное начало. Успехи советской специальной службы в создании новых систем ручных шифров, создании системы радиоперехвата, подготовки кадров специалистов-криптографов свидетельствуют о большой, целенаправленной и продуманной ра-

боте, которая велась в стране в области становления и развития криптографической службы. С другой стороны, подход к криптографии как к виду деятельности узкого круга специалистов, оторванность от достижений мировой криптографической мысли, отсутствие криптографов-математиков, обладающих широкими и фундаментальными аналитическими познаниями, привели к значительному отставанию от стран Запада.

К сожалению, полнокровная система криптографической службы, в которой каждая часть, включая отслеживание противника и работу на перспективу, действовала бы активно, создана не была. Во-первых, на наш взгляд, это было обусловлено именно традициями специальной службы России конца XIX — начала XX в., где отсутствовала мощная аналитическая база, а работа велась так же, как и в Спецотделе пусть и талантливыми, но специалистами-практиками. Во-вторых, тем, что криптографическая служба была создана в лоне ВЧК и в результате этого с первых же шагов оказалась повязанной оперативными, политическими и другими задачами, весьма далекими от развития научной и практической базы криптографии. Таким образом, криптография в России в рассматриваемый период времени проявляла себя, вероятно, скорее как деятельность, а не как наука.

Криптография — это одно из наиболее важных и эффективных средств защиты государственных секретов от противника и получения важнейшей секретной информации о его действиях. Несмотря на отмеченные нами серьезные недостатки, в рассматриваемый временной период криптографическая служба России в целом надежно закрывала секретную информацию, передаваемую по отечественным каналам связи, и, с другой стороны, давала значительные объемы достоверной информации о противнике, оказывающей большое влияние на экономическую, военную, социальную стратегию государ-

ства и на принятие внешних и внутренних политических решений. Со временем роль криптографической службы в деятельности государства возрастает, шифрсвязь становится важнейшим и незаменимым звеном управления хозяйством страны, вооруженными силами, необходимым средством ведения дипломатической и другой внешнеполитической работы.

Отечественная криптографическая служба всегда являлась составной частью государственной машины, точнее — разведки и контрразведки, начиная с XVIII в. и до новейшего времени. На структуру, методы, размах деятельности криптографической службы постоянно влияли два фактора: внешнеполитический, который порождался потребностями России, ее менявшимся положением в системе других государств, и внутриполитический, определявший уровень экономики, науки, культуры по сравнению с другими государствами.

По мере развития методов и средств шифрования и дешифрования, увеличения криптографической стойкости шифров задача обеспечения безопасности государства криптографическими методами становится все более комплексной, решение ее может быть эффективным с привлечением и других методов — контрразведывательных, организационных, инженерно-технических и т. д.

В последнее время все чаще возникает вопрос о том, что в связи с резким изменением политической ситуации в мире, в связи с окончанием «холодной войны», увеличением взаимного доверия между странами криптографическая деятельность может потерять свою актуальность и необходимость. На наш взгляд, ответ на этот вопрос подсказан всем ходом развития мирового сообщества и он может быть только отрицательным. Ни одно из передовых государств современного мира не свертывает работы по криптографии. Криптография не теряет свою актуальность, речь мо-

жет идти лишь об изменении приоритетных направлений деятельности специальной службы.

История хранит много примеров, когда забвение или недооценка криптографических работ со стороны высшего руководства государства (как, впрочем, и работ в области разведки и контрразведки в целом) приводили соответствующие страны к отрицательным результатам, и понадобились многие годы, чтобы ликвидировать их последствия. К таким примерам можно отнести Англию периода XVII—XVIII вв., когда она была «владычицей морей» и свой политический расчет строила на принципе грубой военной силы, существенно сокращая расходы на задачи специальной службы. В конце XVII в. при короле Якове II секретная служба Англии вообще пришла в упадок, «было утрачено даже искусство раскрытия неприятельских шифров». Наполеон I в походе на Россию также не очень беспокоился о стойкости своих шифров, о последствиях этого мы писали. В 1929 г. президент США Г. Гувер и государственный секретарь Стимсон ликвидировали свой «черный кабинет». Стимсон при этом заявил: «Джентльмены не читают переписку друг друга». И хотя вскоре после этого служба была воссоздана, США понесли определенный урон. Наконец, 20—30-е годы нашего века в России были далеко не лучшими годами отечественной криптографии.

К концу 30-х годов в нашей стране криптография еще не стала наукой, но аналитические методы анализа и синтеза шифров постоянно использовались, развивались со временем, и к ним все чаще и шире привлекались методы различных наук — математики, физики, химии. В 20—30-е годы XX в. в мировой практике становится все более очевидным, что наука и техника — это те рубежи, где решается вопрос о том, кто удержит победу в «тайной войне умов», что победа будет на той стороне (и не только в криптографии), которая лучше организует научные исследования, эффективнее использует их достижения в практической деятельности, у кого будет выше научно-технический уровень соответствующих работ.

История, в особенности XX в., четко показала, что ни в коей мере нельзя оставлять без внимания крупные теоретические исследования, направленные на перспективу, исследования, которые теперь принято классифицировать как фундаментальные. Отставание здесь особенно чревато отрицательными последствиями. Именно крупные исследования время от времени дают такие непредсказуемые выходы, которые рождают принципиально новые направления криптографии и оказывают революционизирующее воздействие на всю последующую криптографическую деятельность. Такие открытия и повороты в криптографии по своей значимости и конечной пользе не раз перекрывали все затраты на фундаментальные исследования, делая их «практически» рентабельными в длительном интервале времени. Но парадокс и трагедия наша в том, что подобные революционные сдвиги за счет фундаментальных исследований происходят сравнительно редко и потому при текущем рассмотрении материальных, финансовых и людских затрат эти обстоятельства не всегда принимались и принимаются в расчет. Впрочем, это беда не только криптографии, но и всей отечественной науки в целом.

Примечания

Глава первая

1. Сперанский М. И. Тайнопись в юго-славянских и русских памятниках письма. Энциклопедия славянской филологии. Вып. 3, 4. Л., 1929.
2. Подробнее см.: Симонов Р. А. Математическая мысль Древней Руси. М., 1977.
3. Панченко А. М. Русская стихотворная культура XVII века. Л., 1973. С. 111.
4. Гогешвили А. А. Акростих в «Слове о полку Игореве» и других памятниках русской письменности XI—XIII веков. М., 1991. С. 9.
5. Руководство к изучению богослужения православной церкви протоиерея Константина Никольского. СПб., 1901. С. 18.
6. Гогешвили А. А. С. 51—53.

Глава вторая

1. Попов А. Н. Дипломатическая тайнопись времен царя Алексея Михайловича. СПб., 1853.
2. Пекарский П. Наука и литература в России при Петре Великом. Т. 1. СПб., 1862. С. 287—288.

Глава третья

1. Голиков И. И. Деяния Петра Великого, мудрого преобразователя России, собранные из достоверных источников и расположенные по годам. Ч. XI. М., 1789. С. 356—357. (Изд. 2. Т. XIX. М., 1842. С. 534—535). Эта азбука была также опубликована в: Письма и бумаги Петра Великого. Т. VII. Вып. 2. М.—Л., 1946. С. 734—735.
2. Тромонин К. Я. Достопамятности Москвы. Тетрадь 1. М., 1843. С. 128.
3. Материалы для истории Гангутской операции. Вып. I. Ч. I. Пг., 1914. С. XXV—XXIX.
4. Сборник Русского исторического общества (далее: Сб. РИО). Т. XI. СПб., 1873. С. 253 и приложения к С. 31 и 34.

5. Архив внешней политики Российской империи (далее: АВПРИ). Ф. Цифирные азбуки. Оп. 19/1. Д. 177.
6. Сб. РИО. Т. XI. С. 30 31.
7. АВПР. Ф. Цифирные азбуки. Оп. 1. Д. 12.
8. «Письма и бумаги». Т. IV. Ч. II. СПб. 1900. С. 573—574.
9. АВПРИ. Ф. Цифирные азбуки. Оп. I. Д. 11.
10. Там же. Д. 17.
11. Там же. Д. 18
12. Там же. Д. 21.
13. См. письмо Головина от 4/VII 1702 г.: «Письма и бумаги». Т. II. С. 375; Письмо Петра I от 16/III 1709 г. к Гольцу из Воронежа было написано по-немецки, шифровал его Абрам Веселовский: «Письма и бумаги». Т. IX. Вып. I и 2. С. 125 и 772.
14. «Письма и бумаги». Т. IV. С. 821.
15. АВПРИ. Ф. Цифирные азбуки. Оп. 19/I. Д. 11.
16. Там же. Д. 8.
17. Там же. Д. 41. Л. 21.
18. Там же. Л. 37.
19. Подъяпольская Е. П. Шифрованная переписка России в первой четверти XVIII века. Проблемы источниковедения. Т. 8. М , 1959.
20. Никифоров Л. А. Русско-английские отношения при Петре I. М., 1950. С. 64—65. К числу корреспондентов Куракина, которых перечисляет Л. А. Никифоров, следует добавить И. И. Неплюева, бывшего в 1725 г. резидентом в Константинополе.
21. «Письма и бумаги». Т. IV. С. 591, 627 и др.; Т. IX. Вып. 1 и 2. С. 408 и 1286; 137 и 793; 381, 393, 126. Т. X. С. 173, 198.
22. Там же. Т. IV. С. 677, 711.
23. Там же. Письмо Петра I от 12/III 1796 г.
24. Там же. Т. V. С. 279. Шифр этот не сохранился.
25. Центральный государственный архив древних рукописей. Кабинет Петра I. Кн. 60. Л. 29; «Письма и бумаги». Т. IX. Вып. 1. С. 52.
26. «Письма и бумаги». Т. IX. Вып. 1. С. 36.
27. Там же. С. 137, 151.
28. Там же. С. 217.
29. Там же. Т. IX. Вып. 2. С. 967.
30. Там же. Т. VII. Вып. 2. С. 820.
31. См. Сб. РИО. Т. XI. СПб., 1873. С. 239—240, 252—256, 259—262, 325.

Глава четвертая

1. Костомаров И. И. Царевич Алексей Петрович. М., 1989. С. 33—34.

2. АВПРИ. Ф. Цифирные азбуки. Оп. 19/1. Д. 89. Л. 17.
3. Там же. Д. 119.
4. Там же. Д. 120.
5. Там же. Д. 46.
6. Там же. Д. 47.
7. Там же. Д. 45.
8. Там же. Д. 58.
9. Там же. Д. 65.
10. Там же. Д. 85.
11. Там же. Д. 99.
12. Там же. Д. 53.
13. Там же. Д. 54.
14. Там же. Д. 55.
15. Там же. Д. 56.
16. Там же. Д. 61.
17. Там же. Д. 65.
18. Там же. Ф. Секретнейшие дела. Оп. 6/1. Д. 8. Л. 4—5.
19. Там же. Л. 7.

Глава пятая

1. АВПРИ. Ф. Секретнейшие дела. Оп. 6/1. Д. 5. Л. 8—9.
2. Меклебургский герцог Карл Леопольд был женат на дочери царя Ивана V Алексеевича, их дочь принцесса меклебургская Анна (1718—1747) правительница России в 1740—1741 гг. под именем Анны Леопольдовны, мать объявленного наследником престола Ивана VI Антоновича. Свергнуты в 1741 г.
3. АВПРИ. Ф. Секретнейшие дела. Оп. 6/1. Д. 17. Л. 41.
4. См., например, Брикнер А. Вскрытие чужих писем и депеш при Екатерине II. С. 74; Перегудова З. И. Важный источник по истории революционного движения. Исторический опыт Великого Октября. М., 1986. С. 374.
5. Брикнер А. Русская старина. 1873. № 1.Указ. соч. С. 75.
6. АВПРИ. Ф. Секретнейшие дела. Оп. 6/1. Д. 4—7.
7. См. Очерки русской культуры XVIII века. Ч. II. М., 1987. С. 82.
8. АВПРИ. Ф. Секретнейшие дела. Оп. 6/1. Д. 1. Л. 28—29.
9. Там же. Л. 20.
10 Там же. Л. 22.
11. АВПРИ. Ф. Внутренние коллежские дела. Оп. 2/6. Д. 8/4. Л. 16 об. — 17.
12. Там же. Д. 813. Л. 5 об. — 6.
13. АВПРИ. Ф. Секретнейшие дела. Оп. 6/1. Д. 16. Л. 257—257 об.
14. Там же. Д. 1. Л. 14.
15. Там же. Л. 154.
16. Там же. Л. 173 об.

17. Там же. Оп. 6/1. Д. 16. Л. 116.
18. Там же. Л. 116 об.
19. Там же. Л. 178—178 об.
20. Там же. Л. 11 об., 12 об. — 13, 16, 19 об. — 20.
21. Там же. Л. 116 об.
22. Там же. Л. 118 об.
23. Там же. Л. 119—119 об.
24. Там же. Л. 254—255.
25. АВПРИ. Ф. Внутренние коллежские дела. Оп. 2/6. Д. 813. Л. 58—58 об.
26. Там же. Л. 69 об. — 70.
27. АВПРИ. Ф. Секретнейшие дела. Оп. 6/1. Д. 814. Л. 392.
28. Там же. Л. 398.
29. Карнович Е. П. Замечательные и загадочные личности XVIII—XIX столетий. Л., 1990. С. 93—94.
30. Черняк Б. Пять столетий тайной войны. С. 265—266.

Глава шестая

1. Ломоносов М. В. Полн. собр. соч. Т. 8. М.—Л., 1958. С. 521.
2. Эпинус Ф. У. Т. Теория электричества и магнетизма. М., 1951. С. 10.
3. Россия и США. Становление отношений. 1765—1815 гг. М., 1980. С. 744.
4. Болховитинов Н. Н. В архивах и библиотеках США. Находки, встречи, впечатления. Американский ежегодник. 1971 г. М., 1972. С. 330—331.
5. Речь идет о завоевании США независимости.
6. Россия и США. Становление отношений. 1765—1815 гг. С. 117—118.
7. АВПРИ. Ф. Внутренние коллежские дела. Оп. 2/8, 1765 г. Д. 9. Л. 18 об.
8. Там же. Л. 21 22 об.
9. АВПРИ. Ф. Внутренние коллежские дела. Д. 11. Оп. 2. Л. 58—65; Д 49. Л. 226 об., 264, 322 об.
10. Подробнее см.: Долгова С. Р. Ерофей Каржавин автор первого перевода «Путешествий Гулливера» на русский язык. Русская литература. 1978. № 1. С. 99—103; Долгова С. Р. Творческий путь Ф. В. Каржавина. М., 1984.
11. Россия и США. Становление отношений. 1765—1815 гг. С. 145, 148.

Глава седьмая

1. АВПРИ. Ф. Цифирные азбуки. Оп. 19/1. Д. 21.
2. Там же. Оп. 19/2. Д. 62.

3. Там же. Д. 25.
4. Там же. Д. 131.
5. Там же. Д. 62. Шифр посланника и полномочного министра в Копенгагене барона Криднера.
6. Там же. Д. 88.
7. Там же. Д. 64.
8. Там же. Д. 126.
9. Там же. Д. 127.
10. Там же. Д. 170.
11. Там же. Д. 152.
12. Там же. Оп. 19/2. Д. 46, 51, 54, 55, 75, 76, 79, 80, 82, 85, 86.
13. АВПРИ. Ф. Внутриколлежские дела. Оп. 2/6. Ч. 1. Д. 384. Л. 1—1 об.
14. Там же. Д. 385. Л. 1—2.
15. Там же. Д. 246. Л. 1.
16. Там же. Л. 2—2 об.
17. Там же. Оп. 6/1. Д. 137. Л. 13.
18. Kahn D. The Codebreakers. N. Y., 1967. P. 649.
19. Масонство (репринтное воспроизведение издания 1915 г.). Т. II. М., 1991. С. 136—137.
20. Там же. С. 120.
21. Барсков Я. Л. Переписка московских масонов XVIII века. Петроград, 1915.
22. Цит. по: Н. К. Шильдер. Император Павел I. СПб., 1901. С. 480.
23. Масонство (репринтное воспроизведение издания 1915 г.). Т. II. С. 82.
24. Записки сенатора И. В. Лопухина (репринтное воспроизведение издания 1859 г.). М., 1990. С. 28—29.
25. Русская старина. 1873. № 1. С. 84.

Глава восьмая

1. Министерство иностранных дел России. Пб., 1902. С. 18.
2. АВПРИ. Ф. Шифровальный отдел. Оп. 480/3. Д. 5486. Л. 113.
3. Там же. Д. 5489. Л. 1—2.
4. Флетчер Пратт. Секретно и срочно. М.—Л., 1939. С. 51—52.
5. Черейский Л. А. Пушкин и его окружение. Л., 1989.
6. Цявловский М. А. Летопись жизни и творчества А. С. Пушкина. М., 1951. Т. 1. С. 165; Русский архив. 1899. № 6. С. 351; Цявловская Т. Г. Рисунки Пушкина. М., 1980. С. 311—314; Погодин М. П. В память о князе В. Ф. Одоевском. М., 1869. С. 57; «Русская литература» № 1. 1964. С. 131.

7. Марценицен С. И., Новиков В. В. 150 лет отечественному телеграфу. М., 1982. С. 5—9.
8. Яроцкий А. В. Павел Львович Шиллинг. М., 1953.
9. АВПРИ. Ф. Шифровальный отдел. Оп. 480/3. Д. 5497. Л. 91.
10. Там же. Д. 5479. Л. 6.
11. Там же. Л. 5—5 об.
12. Там же. Д. 5489. Л. 10—11.

Глава девятая

1. АВПРИ. Ф. Шифровальный отдел. Оп. 480/3. Д. 5484. Л. 45 об. 46.
2. Там же. Л. 104—105.
3. Там же. Л. 145 и далее.
4. Государственный архив Российской Федерации (далее: ГАРФ). Ф. 102. Оп. 248. Д. 15.
5. Там же. Д. 48.
6. Там же. Д. 44. Л. 6 18.
7. Там же. Л. 41—59.
8. Там же. Д. 14.
9. Там же. Д. 43.
10. Там же. Д. 55.
11. Там же. Д. 53.
12. Там же. Д. 45. Л. 17.
13. Там же. Л. 27.
14. АВПРИ. Ф. Шифровальный отдел. Оп. 480/3. Д. 78.
15. Там же. Д. 60.
16. ГАРФ. Ф. 248. Д. 52.
17. Там же. Д. 74.
18. Там же. Д. 31.

Глава десятая

1. Шильдер Н. К. Император Александр I. Т. II. СПб., 1897. С. 362, 363, 365.
2. См.: Красный Архив. 1927. № 6(25). С. 201—209.
3. Ламздорф В. Н. Дневник. 1894—1896. М., 1990.
4. Витте С. Ю. Воспоминания. Т. 2. М., 1960. С. 112—113.
5. Ламздорф В. Н. Дневник. С. 133—134.
6. Там же. С. 7.
7. Ламздорф, хорошо знавший французский и немецкий языки, учитывал, что письма другим монархам, носившие более или менее личный характер, Николай II предпочитал писать не на традиционном тогда для дипломатии французском языке, а по-английски, поскольку лучше знал этот язык.
8. Ламздорф В. Н. Дневник. С. 244—245.

9. Там же. С. 212—213.
10. Капнист Петр Алексеевич (1840-1904), граф, российский посол в Австро-Венгрии (1895—1904).
11. Ламздорф В. Н. Дневник. С. 336.
12. Майский С. Черный кабинет. Из воспоминаний бывшего цензора. Былое. 1918. № 3. С. 193.
13. Ламздорф В. Н. Дневник. С. 213.
14. АВПРИ. Ф. Шифровальный отдел. Оп. 3 Л. 70, 71, 84 и др
15. Черняк Е. Секретная дипломатия Великобритании. М., 1975. С. 131.
16. Клембовский В. Тайные разведки (Военное шпионство). СПб., 1911. С. 9—10.
17. Роуан Р. Разведка и контрразведка. М., 1937. С. 30.
18. Майский С. Черный кабинет. Из воспоминаний бывшего цензора. Былое. С. 190—192.

Глава одиннадцатая

1. Подробнее см: Перегудова З. И. Важный источник по истории революционного движения. Исторический опыт Великого Октября. К 90-летию академика И. И. Минца. М., 1986.
2. Майский С. Черный кабинет. Из воспоминаний бывшего цензора. Былое. С. 31.
3. Уложение о наказаниях. СПб., 1912. С. 701.
4. Майский С. Черный кабинет. Из воспоминаний бывшего цензора. Былое. С. 195—197.
5. Осоргин М. А. Охранное отделение и его секреты. М., 1917. С. 1.
6. Там же. С. 9—10.
7. ГАРФ. Ф. 1005. Оп. 8. Д. 1. Л. 1—10.
8. Там же. Ф. 102. Оп. 1. Д. 87. Л. 36 об.
9. Там же. Ф. 102. Оп. 248. Д. 71.
10. Там же. Д. 71. Л. 139 об.
11. Там же. С. 14.
12. Перегудова З. И. Важный источник по истории революционного движения. Исторический опыт Великого Октября. К 90-летию академика И. И. Минца. С. 148.
13. ГАРФ. Ф. 102. Оп. 248. Д. 89. Л. 9.
14. Там же. Д. 96. Л. 79.
15. Там же. Д. 89. Л. 2.
16. Там же. Д. 46. Т. 2. Л. 225—226.
17. Там же. Д. 85. Л. 23.
18. Там же. Д. 86. Л. 37.
19. Там же. Д. 96. Л. 80.
20. Там же. Л. 56—56 об.

21. Там же. Д. 85. Л. 2, 22
22. Там же. Д. 89. Л. 9—9 об.

Глава двенадцатая

1. Бундовец Шифрованное письмо. Женева, 1904 г. С. 6.
2. Там же. С. 15.
3. Ленин В. И. Полн. собр. соч. Т. 4. С. 194.
4. Бундовец. Шифрованное письмо. Женева, 1904 г. С. 59.
5. В. И. Ленин. Полн. собр. соч. Т. 46. С. 239.
6. Переписка В. И. Ленина и редакции «Искры» с социал-демократическими организациями России. 1900—1903 гг. Т. 2. М., 1969. С. 358.
7. ГАРФ. Ф. 102. Оп. 248. Д. 61.
8. Там же. Ф. 102. 1915 г. Д. 343. Л. 148—148 об.
9. Алексеева Т., Матвеев Н. В огне революционных боев. М., 1987.
10. Разгон Лев. Сила тяжести. М., 1986.
11. Алексеева В. Ф. Петроградское подполье. В огне революционных боев. М., 1975. С. 82.
12. ГАРФ. Ф. 102. 1914 г. Д. 122 Л. 242—243.

Глава тринадцатая

1. АВПРИ. Ф. Цифирный отдел. Оп. 2. Д. 66. Л. 14—16.
2. Kahn D. The Codebreakers. N. Y., 1967. P. 420.
3. У. Черчилль. Мировой кризис. М.—Л., 1932.
4. См. также Е. Б. Черняк. Пять столетий тайной войны. М., 1966. С. 518—519. Есть и другие версии получения немецкого кода, но, по мнению специалистов, эта самая достоверная. Версии не противоречат друг другу, поскольку документ мог быть получен одновременно разными путями.
5. АВПРИ. Ф. Цифирный отдел. Оп. 3. Д. 66 Л. 8.
6. Kahn D. The Codebreakers. N. Y., 1967. P. 186—187.
7. Там же. С. 187.
8. Щит и меч. 1990. № 13(16). 13 июля.
9. ГАРФ. Ф. 102. Оп. 248. Д. 77. Л. 12.
10. АВПРИ. Ф. Дела личного состава и хозяйственные дела. Оп. 480/3. Д. 5491.

Глава четырнадцатая

1. ГАРФ. Ф. 200. Оп. 1 Д. 261-А. Л. 91.
2. Там же. Д. 287. Л. 69.
3. Там же. Ф. 200. Оп. 1. Д. 276. Л. 2.
4. Там же. Л. 81.
5. Там же. Д. 194. Л. 20.

6. Там же. Д. 195. Л. 19.
7. Там же. Д. 192. Л. 8.
8. Там же. Л. 9.
9. Там же. Л. 70.
10. Там же. Д. 81. Л. 1.
11. Там же. Ф. 17. Оп. 1. Д. 50. Л. 191.
12. Там же. Л. 8, 23, 29—34.
13. Там же. Ф. 200. Оп. 1. Д. 343. Л. 89, 141.
14. Российский центр хранения и изучения документов новейшей истории (РЦХИДНИ). Ф. 2. Оп. 1. Д. 16581.
15. ГАРФ. Ф. 200. Оп. 1. Д. 287. Л. 62—63.
16. Там же. Д. 225. Л. 67.
17. Там же. Д. 343. Л. 8—9.
18. Там же. Д. 292. Л. 2.
19. Там же. Д. 44. Л. 9—10.

Глава пятнадцатая

1. РЦХИДНИ. Ф. 2. Оп. 2. Д. 390.
2. Там же. Д. 414. Л. 1.
3. Там же. Д. 423.
4. Там же. Ф. 17. Оп. 3. Д. 106; В. И. Ленин. Полн. собр. соч. Т. 41. С. 661.
5. После ноты Керзона и дальнейшего обмена нотами в конце июля 1920 года Л. Б. Каменев был направлен в Лондон в качестве председателя специальной правительственной делегации и в дни решающей фазы советско-польской войны находился в непосредственном контакте с Д. Ллойд-Джорджем и членами его кабинета.
6. Кожинов Вадим. Россия. Век XX-й. (1901—1939). М., 1999. С. 175, 176 и др.
7. ГАРФ. Ф. 130. Оп. 5. Д. 87. Л. 191—191 об.
8. Kahn D. Op. cit. P. 640.
9. Кожинов Вадим. Россия. Век XX-й. (1901—1939). С. 178—179 и далее.
10. Горький М. Собр. соч. М., 1958. Т. 17. С. 342.
11. ГАРФ. Ф. 5881. Оп. 1. Д. 503 Л. 60-61.

Глава шестнадцатая

1. ГАРФ. Ф. 78. Оп. 3316. Д. 17. Л. 1.
2. Филби К. Моя тайная война. М., 1968. С. 14—15.

Глава семнадцатая

1. ГАРФ. Ф. 5856. Оп. 1. Д. 461. Л. 9.
2. Цит. по: Кожинов Вадим. Россия. Век XX. (1901—1939). С. 312.

3. Филби К. Моя тайная война. С. 102, 107.
4. Последние новости. 1930. № 3474 от 26 сент. и другие номера. Мы использовали публикации Агабекова, хранящиеся в ГАРФ. Ф. 5856 Оп. 1. Д. 503.
5. Там же. Л. 53, 59—60.
6. Собеседник. 1989. № 48; Правда. 1990. 25 февр., 4 и 10 марта.
7. Национальный государственный архив США, RG 457, box. 1100, Soviet instructions for using code and sicher systems, part I.
8. Алексеева Т., Матвеев Н. В огне революционных боев. М., 1987. С. 251—252.
9. ГАРФ. Ф. 6075. Оп. 1. Л. 133.
10. Там же. Л. 234.
11. Там же. Л. 246—246 об.
12. Там же. Л. 267 об.
13. Российский государственный военный архив (РГВА). Ф. 9. Оп. 40. Д. 53.
14. РЦХИДНИ. Ф. 356. Оп. 1. Д. 180. Л. 55—56.
15. Цит. по кн.: Яковлев Н. Н. 1 августа 1914 года. М., 1987 г. С. 302.

Оглавление