

## Российский «черный кабинет»

Д.А. Ларин

*270 лет назад, в начале 1742 г., в России в составе Коллегии иностранных дел была создана служба, в задачи которой входила организация перехвата и перлюстрации секретной шифропереписки иностранных корреспондентов, ее дешифровки, перевода и доклада в высшие инстанции. По аналогии с аналогичными европейскими службами отечественная получила название «черный кабинет». Именно тогда началась регулярная работа по криптоанализу иностранных шифрованных сообщений, так что этот год можно с полным правом считать временем создания дешифровальной службы России.*

Прежде чем перейти к рассказу о первых шагах регулярного отечественного криптоанализа, немного истории. XVII, XVIII вв. и первая половина XIX в. вошли в историю криптографии как эра «черных кабинетов» – специальных государственных органов по перехвату и дешифрованию переписки. В штат «черных кабинетов» входили криптографы-дешифровальщики, агенты по перехвату почты, специалисты по вскрытию пакетов, писцы-копировальщики, переводчики, граверы, специализировавшиеся на подделке печатей, химики, их наличие было необходимо из-за активного использования стеганографических методов защиты информации, так называемых невидимых чернил, специалисты по имитации почерков и т.д. Таким образом, «черные кабинеты» состояли из высококвалифицированных специалистов в различных областях деятельности. Первый «светский» «черный кабинет» (без криптоаналитической составляющей) был организован по приказу императора Священной Римской империи Максимилиана I в первом десятилетии XVI в. Это была одна из первых в Европе служб перлюстрации почтовой корреспонденции<sup>1</sup>. Подобные службы, работавшие на папский престол, в составе которых были и дешифровальщики, появились в Ватикане еще ранее<sup>2</sup>.

Во все времена дешифровальщики тесно сотрудничали со специалистами по перехвату и перлюстрации (тайное и безуликовое ознакомление с содержанием переписки): без перехвата нет дешифрования. До изобретения во второй половине XIX в. электрических способов передачи информации (телеграф, телефон, радио) существовали два основных способа передачи сообщений – почта и специальные курьеры. Первый способ был дешевле и быстрее, но менее безопасным, так как «черные кабинеты» располагались, как правило, именно на почтамтах.

Для защиты информации, помимо шифрования, использовались физические методы. Конверты тщательно опечатывались сургучными и восковыми печатями, прошивались по контуру нитками, часто вместе с письмом в конверт вкладывался некий специальный знак (например, волос), при вскрытии целостность этого знака нарушалась (тот же волос выпадал из конверта), и адресат мог понять, что с письмом уже кто-то ознакомился. С курьерами было еще сложнее – их надо было подкупить, напоить, усыпить, а иногда даже убить, чтобы добыть секретную депешу.

О возможности перехвата тайных сообщений было известно еще в Древней Руси, в связи с чем уже тогда принимались меры по защите информации<sup>3</sup>. Практический перехват сообщений внешних

Ларин Дмитрий Александрович – к.т.н., доцент кафедры ИТС МИРЭА (ТУ). E-mail: vestnik@mgimo.ru

и внутренних противников российской власти осуществлялся во время правления великого князя Московского Ивана III (XV в.) и первого русского царя Ивана IV Грозного (XVI в.), а также на протяжении всего XVII в., при этом имеется информация о регулярных попытках чтения шифропереписки иностранных государств, которые нередко приводили к успеху<sup>4</sup>.

Огромная работа по перехвату внешней и внутренней переписки была организована во время правления Петра I. Вся иностранная почта доставлялась в Посольский приказ для вскрытия и досмотра. Кроме зашифрованных сообщений врагов интересовала Петра и информация, содержащаяся в шифропереписке руководителей и дипломатов союзных России и нейтральных государств. Такая переписка велась, Петр I не запрещал иностранным представителям использовать шифры, но требовал представление ему открытых текстов зашифрованных посланий (речь, естественно, идет о тех посланиях, которые удавалось перехватить).

Эти представители могли хранить свою тайну от кого угодно, но не от первого императора России. Однако не всегда иностранные представители выполняли это указание, но в этом случае Петр I не шел на осложнение дипломатических отношений. Так, например, в 1710 г. Петр I потребовал, чтобы посол Дании Юст Юль представил зашифрованный документ с расшифрованным текстом на обороте (речь в документе шла о полномочиях посла). Юль заявил, что такой документ выдает шифр, на что Петр I ответил, что особенной беды в том не будет, так как между царем и королем датским не должно существовать никаких тайн<sup>5</sup>.

Петр I был самым высокопоставленным в истории криптоаналитиком. Криптоанализ – наука о дешифровании шифров, он применяется к «чужим» шифрам для получения информации и к собственным – для оценки их стойкости и соответственно возможности использования для защиты своих секретов. Именно этим Петр I и занимался. Сохранились его резолюции относительно ряда российских шифров: «А которую вы перво прислали, и та не годна, понеже так, как простое письмо, честь можно»<sup>6</sup>, «Сия цифирь зело к разобранию легка»<sup>7</sup>. При этом важно отметить, что занимался оценкой стойкости российских шифров не кто-нибудь, а сам царь.

В Петровскую эпоху стали проявлять в России интерес и к шифрам иностранных государств. Конечно, о регулярном дешифровании иностранной переписки речь пока не шла, однако заинтересованность в получении информации таким методом уже была. Русским дипломатам, разведчикам и другим представителям за границей предписывалось добывать любую информацию, касавшуюся шифров, организации связи, открытых текстов (против атаки «открытый текст – зашифрованный текст» подавляющее большинство шифров того времени было неустойчиво). На этих лиц и их зарубежную агентуру также возлагалась задача организации перехвата иностранных сообщений за границами России<sup>8</sup>.

Определенные меры по перехвату сообщений и добыче шифров предпринимались и после смерти Петра I. Приведем ряд примеров, относящихся к концу 30-х гг. XVIII в. При добыче информации российская сторона иногда применяла самые жесткие меры. В 1738 г. главными политическими противниками России были Швеция (на севере) и Турция (на юге). Российский двор, опасаясь создания их союза, был обеспокоен слухами о переговорах между ними. Императрица Анна Иоанновна повелела принять все возможные меры для получения соответствующей информации. Командующим русскими войсками на юге был фельдмаршал Б.К. Миних. Под его началом служил полковник русской армии Х. фон Манштейн. Приведем выдержку из его воспоминаний: «Предосторожности русского министерства, принимаемые против шведских интриг, доходили до самых насильственных мер и даже до смертоубийства на большой дороге... Ходили слухи о заключении между Швецией и Портою договора. Русский посол в Стокгольме Бестужев уведомил, что в Константинополь послан майор Цинклер с тем, чтобы доставить оттуда ратификации договора. Тотчас после получения этого известия граф Миних послал офицеров с несколькими унтер-офицерами в Польшу»<sup>9</sup>.

По другим данным, информация о Цинклере была получена от агентуры российской разведки в Швеции. Была поставлена задача любой ценой перехватить Цинклера и забрать имеющиеся у него документы. Русским военным удалось захватить необходимые документы, при этом Цинклер был убит. Однако в бумагах Цинклера не было обнаружено почти ничего интересного и после изучения их отправили по почте в Гамбург, откуда переслали в Швецию. В Швеции убийство Цинклера вызвало бурю негодования. По этому поводу Манштейн пишет: «Российская императрица (Анна Иоанновна) отреклась от этого ужасного дела, торжественно объясняя, что она об этом ничего не знала... А для того, чтобы сами убийцы не проговорились, их всех арестовали и сослали в Сибирь, где они несколько лет провели в остроге. Императрица Елизавета, вступив на престол, приказала их выпустить и приписать к гарнизонным полкам далеко во внутренность России... Это верно, что императрица не знала о распоряжении, сделанном относительно Цинклера и что большую часть происшедшего от нее скрыли, даже по учинении убийства. Всем делом распоряжались герцог Курляндский, граф Остерман и фельдмаршал Миних»<sup>10</sup>.

А вот примеры добычи криптографической информации. В середине XVIII в. русский посланник в Швеции барон Корф получил доступ к секретной информации, в том числе к открытым текстам дипломатической зашифрованной переписки Швеции. Однако через некоторое время, почувствовав наличие канала утечки, шведы усилили защиту переписки своего МИДа. Правительству Швеции в 1747 г. пришлось изменить систему канцелярской переписки, потому что

## ■ 2012 – Год российской истории

Корф имел возможность узнавать обо всех тайных государственных делах. Шведское правительство официально жаловалось в Санкт-Петербург на вмешательство русского посла во внутренние дела Швеции и требовало его отзыва из страны. Из Санкт-Петербурга отвечали протестами на действия антирусской партии в Швеции<sup>11</sup>.

Теперь же приведем пример добычи шифров оперативным путем. В 1739 г. герцогом Мекленбург-Шверинским Карлом Леопольдом<sup>12</sup> в Россию был направлен с секретным поручением французский генерал-майор Дюк де Фаллари. Однако российские спецслужбы получили информацию о неблагоприятных намерениях посланца немецкого герцога: «Российское министерство<sup>13</sup> заранее предвещено было о неблагоприятных предложениях, Фалларию<sup>14</sup> вверенных, и давно знало сего постыдными поступками обезглавленного негоциатора, то и предписало по приезде его в Россию арестовать»<sup>15</sup>.

Фаллари прибыл в Ригу 15 мая 1739 г. и на третий день пребывания на российской территории был арестован и отправлен в Санкт-Петербург под конвоем майора Астраханского полка Федора Воейкова. Во время обыска среди прочего представителями российских спецслужб был найден шифр многоалфавитной замены (буквы латинского алфавита заменялись на двух- и трехзначные числа, в основном применялись числа из второй сотни, каждой букве соответствовали 3 шифрообозначения). Благодаря этой находке были прочитаны секретные инструкции, также конфискованные у Фаллари, в которых ему предписывалось «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 мекленбург-шверинских земель»;
- 3) готовить почву для супружества дочери Карла Леопольда с сыном курляндского герцога Бирона»<sup>16</sup>.

Это не соответствовало планам российского двора: на этот престол имелись другие кандидатуры. Императрица Анна Иоановна послала Карлу Леопольду грамоту с известием об аресте Фаллари. Мекленбургский герцог поспешил отмежеваться от француза и в ответном послании заявил, что ничего общего с Фаллари не имеет. Он описал «коварные замыслы сего аккредитованного им дипломата, назвал его злодеем и плутом, который старался у Папы<sup>17</sup> обратить его в католическую веру и даже попросил императрицу, чтобы Фаллари был предан по делам его наказанию»<sup>18</sup>. Фаллари был посажен в тюрьму, а впоследствии сослан в Сибирь.

Однако какой-либо системы в осуществлении перехвата и перлюстрации секретной переписки и специальной службы, выполняющей эти задачи, в России на тот момент не было. Лишь с

занятием российского престола императрицей Елизаветой Петровной вопросам криптографической деятельности стало уделяться регулярное и должное внимание. К чести русской дипломатии следует отнести то, что она не только сумела закрепить успехи, достигнутые при Петре I, но стала играть решающую роль в делах Западной Европы. Русское правительство могло проводить, несмотря на смену лиц на престоле, более решительную политику. Международным успехам России способствовало и наличие в ее правящих кругах выдающихся дипломатов. При этом в руководстве Российской империи осознали, что ознакомление с иностранной перепиской является крайне важным источником информации и добыча ее от случая к случаю является непродуктивной, пришло время поставить данные действия на регулярную основу.

Как уже отмечалось выше, первым барьером на пути к иностранным секретам были физические меры защиты. Как и в Европе, их преодоление стало первой задачей отечественного «черного кабинета». Организация службы перлюстрации в России во многом связана с именем выдающегося государственного деятеля и дипломата Алексея Петровича Бестужева-Рюмина (1693–1766 гг.). Рассмотрим его биографию подробнее. В 1708 г. он по приказу Петра I был отправлен 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. В 1717 г. он возвращается на русскую службу и направляется на дипломатическую работу в Данию и Гамбург. В 1740 г. он был вызван в Россию фаворитом Анны Иоанновны Бироном и назначен кабинет-министром. А.П. Бестужев принял деятельное участие в борьбе за назначение Бирона регентом после смерти Анны Иоанновны. Вместе с Бироном он был арестован в ночь на 9 ноября 1740 г., заключен в тюрьму и приговорен к четвертованию. Однако казнь его была заменена ссылкой.

В октябре 1741 г. Бестужев вновь был возвращен в Петербург и по вступлении на престол императрицы Елизаветы Петровны осыпан милостями и назначен вице-канцлером (вторым лицом в правительстве), сенатором и главным директором почт. 25 апреля вместе с отцом<sup>19</sup> и братом А.П. Бестужев-Рюмин получил графское достоинство. Занимая при дворе все более значительное положение, он начинает активно проводить свою политику, направленную на союз с Англией и Австрией против Франции и Пруссии. Французские дипломаты, аккредитованные в России, приложили немало стараний к тому, чтобы свергнуть Бестужева. Особую активность в этом проявлял французский посол маркиз Шетарди<sup>20</sup>.

С 1744 по 1758 г. А.П. Бестужев-Рюмин занимает должность канцлера (главы правительства). Из-за придворных интриг в феврале 1758 г. Елизавета Петровна лишила канцлера чинов и знаков отличий. Он был обвинен в неисполнении высо-

чайших повелений, во вмешательстве в командование армией и в тайной переписке с великой княгиней Екатериной (будущей императрицей). Алексея Петровича снова приговорили к смертной казни, но и на этот раз ее заменили ссылкой в деревню Горетово Можайского уезда. Ссылка канцлера продолжалась до воцарения императрицы Екатерины II. Он был вызван в Петербург, и Екатерина возвратила опальному государственному деятелю чины, ордена и присвоила звание генерал-фельдмаршала (одно из самых высших воинских званий в тогдашней России). 31 августа 1762 г. торжественно обнародованным указом он был оправдан «во взведенных на него обвинениях». Прежнее влияние он, однако, утратил. Императрица обращалась к нему иногда за советами по иностранным делам; он сохранил внешнее первенство среди вельмож, но все его попытки вмешиваться во властные дела встречали решительный отпор новых царедворцев. Скончался Алексей Петрович Бестужев-Рюмин в 1766 г.<sup>21</sup>

Отметим также, что в 1741–1757 гг. Бестужев участвовал во всех дипломатических делах, договорах и конвенциях, которые Россия заключила с европейскими державами. Бестужев-Рюмин, как один из крупнейших российских дипломатов и государственных деятелей, по отзывам современников, обладал умом светлым и гибким, принадлежал к числу образованнейших людей своего времени (ему приписывают изобретение так называемых «бестужевских капель»), отличался трудолюбием, был чрезвычайно деятелен, не запятнал себя никакими «осязательными доказательствами милостивого расположения иностранных дворов»<sup>22</sup>.

Итак, перлюстрация переписки иностранных дипломатов была организована в России А.П. Бестужевым-Рюминым в начале 1742 г., то есть как раз в тот период, когда он назначается главным директором почт. По его распоряжению почтовые службы должны были вскрывать и копировать все письма зарубежных послов (даже к дамам), уходящие и прибывающие из-за границы. Частные письма, пересекающие границу, также, по возможности, вскрывались все, но копировались наиболее интересные. В российских архивах сохранилось большое количество документов, отражающих деятельность «черного кабинета» в первые годы его существования. Например, сохранились русские копии писем, датированных 1742 г.:

– от «голландского в Швеции министра Пехлина к находящемуся в Санкт-Петербурге обер-маршалу голландскому Бриммеру»;

– от «голландского в Санкт-Петербурге резидента Шварца к Генеральным штатам, к графине Фагель в Гаагу, к пансионерному советнику фон дер Гейму и пр.»;

– от «австро-венгерского в Санкт-Петербурге резидента Гогенгольца к великому канцлеру графу Ульфреду и к графу Естергазию, а также секретаря его Бослера к маркизу Вотте»;

– от «английского в Санкт-Петербурге министра Вейча к милорду Картерсту в Ганновер и к герцогу Ньюкастлскому» и др.<sup>23</sup>.

Все эти документы были сшиты в толстые книги и переведены на русский язык. На некоторых, в том числе самых первых, перехваченных документах есть пометки «Ея Императорское Величество слушать изволила»<sup>24</sup>. Из данной цитаты следует, что уже в 1742–1743 гг. результаты работы «черного кабинета» докладывались императрице Елизавете Петровне. По установленному порядку канцлер или вице-канцлер несколько раз в месяц докладывали императрице о международном положении и прочих государственных делах. При докладах обязательно присутствовал секретарь (тогда им был Иван Пуговишников), который вел подробный протокол, переписываемый затем набело, и, подписанный канцлером или вице-канцлером подшивался в дело. Таким образом, было запротоколировано все, о чем государыня «изволила рассуждать»<sup>25</sup>. Среди «рассуждений» императрицы материалы перлюстрированной (а впоследствии дешифрованной) переписки занимали немалое место. При этом на совещаниях с канцлером императрица довольно часто обсуждала вопросы работы «черного кабинета».

Работа перлюстраторов была весьма нелегкой. Выше уже были приведены примеры способов физической защиты посланий, которые при этом надо было преодолеть. В этой связи следует отметить, что безуликовая перлюстрация шифрованных сообщений была непростой задачей. Фактически главой российского «черного кабинета» в начальный период его работы стал назначенный Бестужевым-Рюминым Санкт-Петербургский почт-директор Фридрих Аш. В его обязанности входило вскрытие и запечатывание посланий. Вот как описывает этот процесс и возникающие трудности в одном из писем Бестужеву-Рюмину сам первый российский профессиональный перлюстратор: «... 29-го числа прошлого месяца купно (вместе) с депешью от господина Мардефельда<sup>26</sup>, вчерась пополудни с великим респектом получил. И не применил по силе данного мне милостивейшего приказа оную депешу распечатывать, а в ней находилось три пакета, а именно первый в придворный почтовый амт (почтовая служба) от г-на барона Мардефельда самого, второй – к финансовому советнику Магирусу в Кенигсберг от секретаря Варендорфа, а третий – от господина Латдорфа<sup>27</sup> к его брату в Ангальтбернбург. Последние два письма без трудности распечатать было можно, чего ради и копии с них при прилагаются. Тако же де конверт (конверт) в придворный почтовый амт в Берлине легко бы было распечатать, однако ж два в оном письма, то есть к королю и в кабинет, такого состояния были, что хотя всякое удобовыполненное старание прилагалось, однако ж оных для следующих причин ответить невозможно было, а именно: конверты не только по углам, но и везде тем клею обвязанная, под конвертом крестом на письмах нитка таким образом утверждена была, что оный клей от пара кипятка, над чем письма я

## ■ 2012 – Год российской истории

несколько часов держал, никак распуститься и отстать не мог. Да и тот клей, который под печатями находился (кои я хотя искусно снял), однако же не распустился. Следовательно же, я к привеликому моему соболезнованию, никакой возможности не нашел оных писем распечатать без совершенного разодрания конвертов. И таки я оные пакеты запечатал и стафету в ея дорогу отправить принужден был...»<sup>28</sup>.

Как видим, несмотря на то что Аш к тому времени уже был первоклассным специалистом, он мог справиться отнюдь не со всеми способами физической защиты посланий, существовавших в то время, однако все же большинство писем удачно и безуликово перлюстрировалось. Помимо Аша, в штат «черного кабинета» входили особые секретари и переводчики, в обязанности которых входило копирование иностранной дипломатической переписки и ее перевод на русский язык для доклада главным образом Бестужеву-Рюмину или самой императрице.

Однако эффективная работа «черного кабинета» была бы вряд ли возможна без наличия в его штате человека очень редкой и оригинальной профессии. Как мы уже отмечали выше, одним из распространенных методов физической защиты было опечатывание конвертов. В XVIII в. печати на конвертах были обычно сургучными, на которых ставился оттиск личной или государственной печати отправителя. В то время на подобные печати наносилась тонкая затейливая резьба, обычно фамильный или государственный герб в сочетании с дополнительными рисунками и надписями для затруднения подделки. В ходе вскрытия конверта печати нередко повреждались и требовали восстановления. Эту задачу выполнял «печатнорезчик», который по оттиску печати делал ее копию для опечатывания вновь закрытого конверта к отправителю. Это была тонкая и кропотливая работа, требующая аккуратности и высокого мастерства. Тем не менее Аш имел образцы печатей всех послов и других сотрудников дипмиссий, которые работали тогда в России.

В 1742 – 1744 гг. резчиком печатей в российском «черном кабинете» работал некий Купи, француз по национальности. Аш тщательнейшим образом проверял его работу, осматривая сделанные образцы, при необходимости делал замечания и после их устранения докладывал Бестужеву-Рюмину о результатах для окончательного утверждения работы. Вот пример подобного письма Аша, датированного февралем 1744 г.: «Печатнорезчик Купи от своей болезни отчасти оправился и уже начало подделыванием некоторых штемпелей учинил, из которых и сегодня два отдал, но один назад взять принужден был, дабы усмотренные мною в нем прогрешение поправить, а другой, которой барона Нейгауза<sup>29</sup> есть, я за нарочитой нахожу и оной при чем полагаю ...»<sup>30</sup>.

Но Бестужев-Рюмин был строже, он писал: «Из Государственной коллегии иностранных дел Санкт-петербургскому почт-директору господину Ашу. На рапорт Ваш от 29 февраля здесь в 6-е

марта полученный в резолюцию объявляется... присланная от Вас печать барона Нейгауза при сем возвратно к Вам отправляю, дабы Вам, оную имев, столь меньшим трудом в рассматриваемом без формы исправляться могли. Рекомендую, впрочем, резчику Купи оные печати вырезывать с лучшим прилежанием, што ныняшняя нейгаузова не весьма хорошего мастерства»<sup>31</sup>.

Обратим внимание на заглавие этого документа. Как видим, деятельностью «черного кабинета» руководила Коллегия иностранных дел (предшественница МИД). В данном случае Россия пошла по пути стран Европы, имевших подобные службы. Эти службы подчинялись или непосредственно входили в штат внешнеполитических ведомств, а территориально располагались на главном почтамте в столице страны, так продолжалось до середины XIX в., а в России – несколько дольше. Впоследствии контроль за перепиской (перлюстрация), как правило, осуществлялся органами внутренних дел, а дешифровальные подразделения включались в состав военных ведомств, разведок и спецслужб. Некоторые из них непосредственно организовывались для этих целей: можно вспомнить в этой связи АНБ США, образованное 60 лет назад (4 ноября 1952 г.). Заметим также, что деятельность по созданию шифров в России с 1549 по 1917 г. велась также большей частью во внешнеполитическом ведомстве (Посольский приказ, Коллегия иностранных дел, Министерство иностранных дел).

Однако вернемся к подделке печатей. В феврале 1745 г. Бестужев-Рюмин доложил Елизавете Петровне о работе «черного кабинета». В частности, он упомянул о работе резчика Купи. В ответ императрица сказала (приведем цитату одного из «Протоколов докладов Ея Императорского Величества Елизавете»): «В Санкт-Петербурге. 12 февраля 1745 года пополудни при докладе происходило: ... 20. При сих 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 оною такие печати делать заставить не здесь в Санкт-Петербурге, 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 у того мастера обыскать и отобрать, чтобы ничего у него не осталось, и сверх того присягою его утвердить надобно, дабы никому о том не разглашал»<sup>32</sup>.

Как видим, Елизавета стремилась содержать службу перлюстрации в особом секрете и была озабочена «засильем» там иностранных специалистов. По некоторым сведениям, впоследствии печати изготавливались гравером Академии наук. При этом справедливости ради надо отметить, что перешедшие на русскую службу иностранцы в XVIII – XIX вв. внесли значительный вклад в развитие российской криптографии, о некоторых из них мы расскажем далее.

Итак, хоть и с трудом, физическую защиту иностранных корреспондентов в российском «черном кабинете» преодолевать научились. Однако, как показывал почти 200-летний опыт работы отечественной криптографической службы, самые интересные и важные сведения содержатся именно в зашифрованных частях писем. Хотя в самом начале работы российского «черного кабинета» зашифрованные тексты даже не копировались. В сохранившихся в российских архивах переводах иностранной переписки тех времен часто можно видеть такие пометки в тексте: «Далее... страниц цифрами писано было...»<sup>33</sup>. Затем переводчик делает пропуск и дает следующий далее текст письма. Однако российскому руководству, прежде всего в лице Бестужева-Рюмина, было понятно, что дальше так продолжаться не может. Пришло время сделать следующий шаг – начать дешифрование иностранной шифропереписки. И вскоре Бестужеву-Рюмину удалось найти для отечественного «черного кабинета» такого специалиста. Прежде чем подробно рассказать о нем, сделаем небольшое отступление.

В настоящее время благодаря работам К. Шеннона<sup>34</sup> и В.А. Котельникова<sup>35</sup> криптоанализ стал строгой математической наукой. В описываемые же времена это было искусство или, в крайнем случае, редкое ремесло – удел талантливых одиночек. Однако уже с древних времен криптография вообще и криптоанализ в частности вызывали большой интерес у математиков<sup>36</sup>. Здесь же заметим, что наиболее известными математиками-криптоаналитиками были француз Франсуа Виет и англичанин Джон Валлис. Сейчас неизвестно, знал ли об этом Бестужев-Рюмин, но интуитивно он правильно определил профессию первого российского дешифровальщика – им стал тогда уже известный математик Христиан Гольдбах (1690–1764 гг.). Рассмотрим его биографию подробнее.

Родился Х. Гольдбах в Кенигсберге. История его приезда в Россию напрямую связана с организацией Петром I в России Академии наук. Как известно, Петр Великий (1672–1725 гг.) вошел в историю России как великий реформатор. Главным итогом Петровских реформ стало преодоление серьезного отставания России от европейских держав в военной, экономической, политической областях. Огромное значение Петр придавал повышению образовательного уровня населения России. По его инициативе открывались учебные заведения, с одной стороны, сотни молодых людей отправлялись учиться за границу, с другой стороны, в Россию были приглашены для работы и преподавательской деятельности многие иностранные специалисты. Уже в первые годы своего царствования Петр ощутил огромную потребность России в большом числе образованных людей, способных осуществлять его планы, руководить вновь 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<sup>37</sup>.

Кстати следует отметить, что в 1712 г. Петр встретался с великим немецким математиком Лейбницем, чтобы уговорить его разработать проекты развития образования и государственного устройства в России. Интересовался Лейбниц и криптографией. Так, курфюрст Ганновера через этого великого математика попытался выведать методы, которые упомянутый выше английский дешифровальщик Валлис использовал при криптоанализе французских шифров, а также попросил обучить криптоанализу нескольких молодых людей из числа своих подданных. К сожалению для курфюрста, Валлис заявил, что в случае необходимости он рад будет оказывать ему услуги, но делиться своими знаниями без разрешения короля Англии не может. Лейбниц придавал в своих проектах развитию шифрования и криптоанализа большое значение. Если бы не смерть Лейбница, то первый немецкий математик-криптограф мог бы появиться в России еще раньше, чем Гольдбах<sup>38</sup>.

24 января 1724 г. последовал императорский указ об организации Академии наук, а при ней – университета и гимназии. Через немецкого философа и математика Вольфа, с которым Петр длительное время вел переписку относительно развития науки, в Россию был приглашен ряд ученых из Европы. Среди них были и математики, подбор которых оказался поразительно удачным. Приехали Герман, ученик Якова Бернулли, два сына знаменитого Иоганна Бернулли – Николай и Даниил и, наконец, Христиан Гольдбах. В 1727 г. по приглашению Гольдбаха в Россию прибыл один из самых замечательных математиков всех времен Леонард Эйлер. По приезде в Россию Х. Гольдбах в течение 15 лет (1726–1740 гг.) исполнял обязанности конференц-секретаря Академии наук. Как математик, Гольдбах известен классическими трудами по теории чисел и математическому анализу. В первых томах «Комментариев Петербургской Академии наук» – первом научном российском журнале – Гольдбах напечатал ряд статей об интегрировании дифференциального уравнения Риккати, о превращении расходящихся рядов в сходящиеся и др.

Как известно, с 1729 г. и до конца своих дней Гольдбах 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 число, большее или равное шести, может быть представлено в виде суммы трех простых чисел<sup>39</sup>.

А.П. Бестужев-Рюмин решил привлечь к дешифровальной работе в Коллегии иностранных дел математика, специалиста по теории чисел Х. Гольдбаха. Одним из аргументов при выборе его кандидатуры могло быть то, что при дворе Гольдбах исполнял обязанности одного из вос-

## ■ 2012 – Год российской истории

питателей Петра II, а к воспитанию коронованных особ всегда привлекались наиболее доверенные люди. Дешифровальная деятельность, разумеется, не могла быть поручена кому попало. И вот 18 марта 1742 г. императрица Елизавета Петровна подписала именной указ о назначении Гольдбаха на «особливую должность», а дело об этом в архивах российского внешнеполитического ведомства 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»<sup>40</sup>. С этого времени вся дальнейшая жизнь Гольдбаха была связана с дешифровальной службой. И именно эту дату следует считать началом отчета регулярной работы по дешифрованию иностранной переписки в России.

Однако успех пришел к первому российскому профессиональному дешифровальщику далеко не сразу. Последовало более года напряженной работы, прежде чем на полях копии одного из писем австрийского посла барона Нейгауза (о проблемах с подделкой печати которого было сказано выше) из тех, что датированы июлем 1743 г., появилась пометка: «Разобраны с цифр (возможно, шифротекст этого письма представлял собой набор цифр) искусством статского советника Гольдбаха; в цифрах имевшиеся места внесены, для знака линиями подчеркнуты и прочее малое число еще не разобранных цифров каждая тремя пунктами означены»<sup>41</sup>.

Из этого документа следует, что в представляемых вице-канцлеру Бестужеву-Рюмину переводах перлюстрированных писем те места, которые дешифрованы, подчеркнуты, чтобы было ясно, какую именно информацию зашифровали. Далее, как говорится, дело пошло. 30 июля 1743 г. Гольдбах представил Бестужеву-Рюмину пять дешифрованных писем, 2 августа – также пять, 10 августа – два, 20-го – снова пять, 27 и 30 августа – по два письма. Всего с июля по декабрь 1743 г. им было дешифровано 61 письмо «министров прусского и французского дворов»<sup>42</sup>. Как видим, Гольдбах работал и против своих соотечественников, отдавая без остатка свой талант служению России.

Результаты работы по криптоанализу иностранных шифров сразу привлекли внимание императрицы. Елизавета Петровна уделяла вопросам криптографической деятельности большое внимание. Как указывалось выше, с самого начала работы по перлюстрации корреспонденции иностранных дипломатов канцлер и вице-канцлер докладывали ее содержание Елизавете, как только появился новый источник информации – дешифрованные фрагменты иностранной переписки, – Елизавета сразу обратила на это внимание. Заслуги Гольдбаха были высочайше оценены, в том числе и материально. В начале января 1744 г. с Гольдбахом был перезаключен договор о службе в России, из протокола докладов Елизавете от 3 января 1744 г. следует: «...18. Слушать же и

всемилоостивейше 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 вознаграждение до 1000 рублей пожаловать, Ея Императорское Величество на сие всемилоостивейше соизволила»<sup>43</sup>.

Одним из важнейших результатов работы Х. Гольдбаха стало дешифрование переписки французского посланника в России маркиза Шетарди, хотя это не был первый (а точнее, четвертый) взломанный в России иностранный шифр, ознакомление российского руководства с этой перепиской имело далеко идущие дипломатические последствия. Одним из первых документов, где упоминается о дешифровании переписки Шетарди, была записка следующего содержания: «Переводы корреспонденции маркиза Шетарди 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 пиесы перевод с его письма гласит... И тако сие уже четвертая цифирь, которую помянутый статский советник разобрал, а именно сперва нейгаузову, потом далионову<sup>44</sup> с французскими министрами при иностранных дворах, да его же с статским секретарем Амелотом и сие, шетардиеву. По неже он уповае в кратком времени употребляемую и статским секретарем Амелотом и придворную цифирь маркиза Шетардия разобрать...». На полях же рядом с этим текстом написано: «Сии пиесы поданы Ея Императорскому Величеству самим государственным вице-канцлером в 3 апреля 1744 года»<sup>45</sup>.

Таковы были первые шаги отечественного криптоанализа. Научный подход и активное заинтересованное внимание руководителей государства к специальной службе позволили России добиться быстрых и важных успехов в дешифровании корреспонденции Франции, Англии, Германии.

### **Larin D.A. Russian «Black Chamber».**

**Summary:** 270 years ago at the beginning of 1742 the special body as a part of the Foreign Affairs Collegium was created in Russia. The main task of this body was the interception and perustration of foreign reporters' secret cipher messages. A work of deciphering, translating the messages and reporting the produced information to the governing body was organized. By the analogue with European services this domestic organization was called «The Black Chamber». Since then the regular work of cryptanalysis of the foreign reporters' secret cipher messages was begun. So this year may be considered as a starting point of creation of the Deciphering Service of Russia.

**Ключевые слова**

Криптоанализ, шифр, дешифрование, Российский «черный кабинет», Христиан Гольдбах.

**Keywords**

Cryptanalysis, cipher, decrypting, Russian «black chamber», Christian Goldbach.

**Примечания**

1. Черняк Е. Пять столетий тайной войны. М.: Международные отношения, 1991. С. 248.
2. Подр. см.: Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. М.: Гелиос, 2002, Kahn D. The codebreakers. N- Y: Macmillan Publ. Co., 1967.
3. Подр. см.: Ларин Д.А. Истоки отечественной криптографии // Математика для школьников. №4. М., 2009. С. 49-64. Ларин Д.А. Защита информации в Древней Руси // Вестник РГГУ №12/10, серия «Информатика. Защита информации. Математика». Научный журнал. М.: РГГУ, 2010. С. 13-35.
4. Подр. см.: Бабаш А.В., Шанкин Г.П. Указ. соч. Скрытников Р.Г. Иван Грозный. М.: Наука, 1980. Кудрявцев Н.А. Государево Око. Тайная дипломатия и разведка на службе России. М. / ОЛМА-ПРЕСС, 2002. Очерки истории российской внешней разведки в 6 томах (далее очерки) / под ред. Е.М. Примакова и С.Н. Лебедева. М.: Международные отношения, 1997. Т.1.
5. Юль Юст. Записки, М., 1899.
6. Соболева Т.А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002. С. 73.
7. Бабаш А.В., Шанкин Г.П. Указ. соч. С. 215.
8. Подробнее о криптографической деятельности в России во времена правления Петра I можно прочитать в статье Ларина Д.А. Криптографическая деятельность в России при Петре Великом // Защита информации. INSIDE. СПб. 2009. №5. С. 76-88; №6. С. 73-86.
9. фон Манштейн Х.Г. Записки о России генерала Манштейна. СПб.: Тип. В.С. Балашева, 1875 // <http://www.runivers.ru/bookreader/book53498/#page/1/mode/1up>.
10. Фон Манштейн Х.Г. Указ. соч.
11. Очерки.
12. Подр. см.: Соболева Т.А. Указ. соч. С. 107.
13. Там же.
14. Так в тексте документа. Архив. Указ. Документ.
15. Соболева Т.А. Указ. соч. С. 107.
16. Там же. С. 107-108.
17. Речь здесь идет о Папе Римском.
18. Соболева Т.А. Указ. соч. С. 108.
19. Интересно отметить, что упомянутый выше Майнштейном в связи с делом Цинклера русский посланник в Стокгольме и есть брат нашего героя М.П.Бестужев-Рюмин.
20. Соболева Т.А. Указ. соч. С. 109-110.
21. «Бестужевы-Рюмины (П.М., М.П., А.П.)» Сайт «Русский биографический словарь» <http://www.rulex.ru/01029006.htm>. 6.11.2011.
22. <http://ru.wikipedia.org>
23. Соболева Т.А. Указ. соч. С. 111.
24. Там же.
25. Там же.С. 112.
26. Министр (по-современному – посол, в те времена для руководства важными дипломатическими миссиями назначались специальные министры) прусского двора в Санкт-Петербурге.
27. Прусский дипломат, работавший в то время в Санкт- Петербурге.
28. Соболева Т.А. Указ. соч. С. 113.
29. В то время австрийский посол в России.
30. Соболева Т.А. Указ. соч. С. 114.
31. Там же. С. 114-115.
32. Там же. С. 115.
33. Там же.С. 116.
34. Шеннон К. Работы по теории информации и кибернетике. М.: Иностранная литература, 1963.
35. Подр. см.: Бабиевский В.В., Бутырский Л.С., Ларин Д.А., Шанкин Г.П. Криптографический фронт Великой Отечественной. Советская шифровальная служба. // Защита информации. INSIDE. №5. 2010. С. 87-96, №6. 2010. С. 74-86.
36. Подр. см.: Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Криптография и математика // Математика для школьников. №4. М., 2008. С. 49-59.
37. Подр. см.: Буганов В.И. Пётр Великий и его время. М.: Наука, 1989.
38. Подр. см.: Бабаш А.В., Шанкин Г.П. Указ. соч. С. 166-167.
39. Подр. см.: Соболева Т.А. Указ. соч. С. 117-118.
40. Там же. С. 118.
41. Там же. С. 119.
42. Там же.
43. Там же. С. 120.
44. Далион – французский министр, участвовавший в политических интригах в России в описываемый период времени.
45. Соболева Т.А. Указ. соч. С. 120.