
ШПИОНСКИЙ АРСЕНАЛ
КРИПТОЛОГИЯ И СЕКРЕТНАЯ СВЯЗЬ
СДЕЛАНО В СССР
ВАДИМ ГРЕБЕННИКОВ

Вадим Гребенников

Криптология и секретная связь. Сделано в СССР

«Алисторус»

2017

УДК 003.26
ББК 32.81

Гребенников В. В.

Криптология и секретная связь. Сделано в СССР /
В. В. Гребенников — «Алисторус», 2017

ISBN 978-5-906979-79-7

Криптология – наука, занимающаяся методами шифрования и дешифрования. Одна из старейших наук, которая зародилась несколько тысяч лет назад и продолжает активно развиваться сейчас.В книге подробно рассказано об истории зарождения и эволюции криптологии и специальной («закрытой») связи в Советском Союзе и современной России. Герои и предатели в этих сферах. История разработки и создания шифраторов и другого специального оборудования для защиты от «прослушки» различных видов связи. Как советская разведка охотилась за шифрами и кодами врага и каких успехов достигла.

УДК 003.26
ББК 32.81

ISBN 978-5-906979-79-7

Содержание

Вадим Гребенников
Криптология и секретная связь. Сделано в СССР

* * *

Кто владеет информацией, тот владеет миром.
Натан Ротшильд

Предисловие

Философ Фридрих Вильгельм Шеллинг писал: «То, что мы называем природой, – лишь поэма, скрытая в чудесной тайнописи». Такую же мысль высказывает и современная поэтесса Юнна Петровна Мориц:

Тайнопись – почерк всего мироздания,
почерк поэзии, кисти, клавира!
Тайнопись – это в тумане предания
огненный шрифт современного мира.

Бесспорно, самые первые символы и знаки, написанные или выдолбленные в камне или вырезанные на дереве, имели магический характер. Самые древние свидетельства того относятся к 17–16-му тысячелетию до н. э. На этих памятниках письменности изображены фигуры, ставшие «праотцами» известных сегодня магических символов: крестов, рун, колес, свастик. Впоследствии эти сакральные знаки накапливались, передавались в откровениях, устно и до 3–1-го тысячелетия до н. э. уже были системами, начали образовываться первые магические алфавиты.

Эти алфавиты осмысливались в те времена именно как набор священных символов с присвоенными им фонетическими значениями, что позволяло использовать эти знаки для письменности. Так возникли родственные финикийский, греческий, латинский, этрусский и рунический алфавиты, но достаточно значительная часть древних символов осталась за пределами этих алфавитов и продолжала использоваться исключительно с магической и художественной целью.

До нашего времени как магический дошел рунический алфавит. Руны (то есть знаки древнескандинавского алфавита) были разбиты на три группы по восемь штук в каждой. Основная система шифрования являла собой шифр (*араб.* sifr – ноль, ничто, пустота) замены – каждой руне отвечали два знака шифротекста (косые черточки разной длины). Число черточек сверху помечало номер группы, а снизу – номер руны в группе. Встречались и осложнения этой системы, например, руны в группах перемешивались.

Готское слово «runa» означает «тайна» и происходит из древнего немецкого корня со значением «прятать». В современных языках это слово также присутствует: немецкое «raunen» значит «нашептывать», латышское «runat» – «говорить», финское «runo» – «стихотворение, заклинание». Еще одним магическим алфавитом, который некоторые авторы относят к «руническим надписям», является огамический (ogam, ogum, ogham), распространенный в Ирландии, Шотландии, Уэльсе и Корнуолле в III–X веках н. э. В древнеирландских текстах было упоминание о том, что «ogam» служил для передачи тайных посланий, а также для гадания.

Вообще магическим алфавитом можно назвать любой алфавит, потому что каждая буква каждого алфавита имеет собственно символическое значение. Особенно это касается еврейского иврита и индийского санскрита, которые рядом с греческим и латинским алфавитами до сего времени используются оккультистами. Однако, невзирая на наличие сакральных значений у символов двух последних, они все-таки стали впоследствии в первую очередь признаками учености и культуры тех, кто их употреблял.

Символизм, который был заложен в каждую букву, выполнял две функции: во-первых, он скрывал тайны от непосвященных, а во-вторых, напротив, открывал их тем, кто был этого достоин, кто понимал скрытый смысл этих символов. Посвященные жрецы считали святотатством обсуждение священных истин высшего света или божественных откровений вечной

Природы на том же языке, который использовался простым народом. Именно из-за этого всеми сакральными традициями мира разрабатывались свои тайные алфавиты.

Иврит является одним из самых распространенных алфавитов в Западной магической традиции, а его буквы считаются вместилищем божественной силы. Например, буква еврейского алфавита «алеф» означает власть, человека, мага; буква «бет» – науку, рот, двери храма; «гимель» – действие, протянутую для рукопожатия руку и тому подобное. В алхимии буквы были также многозначительны: «A» выражало начало всех вещей; «Y» – отношение между четырьмя основными элементами; «L» – разложение; «M» – андрогинную природу воды в ее первобытном состоянии и тому подобное.

Греческий алфавит, подобно ивриту для евреев, служил грекам одним из средств познания мира. У греков буквы «A», «E», «H», «I», «O», «Y» и «Ω» отвечали семи планетам (небесам). Буквы «B», «Γ», «Δ», «Z», «K», «Λ», «M», «N», «П», «P», «Σ» и «T» приписывались 12 знакам Зодиака. Буквы «Θ», «Ξ», «Φ» и «X» являли собой четыре мировых элемента (стихии), а «Ψ» – «мировой дух». Алфавит использовался также для гадания и в разных мистериях. Так, например, пятая буква греческого алфавита «E» (эпсилон) служила символом «Духовного Солнца» в большом храме греческих мистерий в Дельфах, где в течение семнадцати веков проводились элевсинские посвящения.

В латинском алфавите гласные буквы «A», «E», «I», «O», «U» и согласные «J», «V» отвечали семи планетам. Согласные буквы «B», «C», «D», «F», «G», «L», «M», «N», «P», «S» и «T» руководили 12 астрологическими знаками. Буквы «K», «Q», «X», «Z» отвечали четырем стихиям, а «H» являла собой «мировой дух». Латинский алфавит использовался во многих оккультных знаковых фигурах.

Ученый Блез Паскаль писал: «Языки суть шифры, в которых не буквы заменены буквами, а слова словами, так что неизвестный язык является шифром, который легко разгадывается». Так, языки американских индейцев неоднократно использовались в качестве системы шифрования. Во время Первой мировой войны индейцы племени чокто (чахта) были первыми, кто помогал армии США шифровать военные сообщения, а в начале Второй мировой войны для ВМФ США это делали индейцы племени навахо. В 1960 году ирландские вооруженные силы в Конго, направленные туда по решению ООН, осуществляли переговоры на гаэльском языке.

С развитием фонетического письма письменность резко упростилась. В давнем семитском алфавите во 2-м тысячелетии до н. э. было всего около тридцати знаков. Ими обозначались согласные звуки, а также некоторые гласные и слоги. Упрощение письма стимулировало развитие криптологии и шифровального дела.

Правителям больших государств необходимо было осуществлять «скрытое» руководство наместниками в многочисленных провинциях и получать от них информацию о состоянии дел на местах. Короли, королевы и полководцы должны были руководить своими странами и командовать своими армиями, опираясь на надежную и эффективно действующую связь. В результате организация и обеспечение шифрованной связи для них было жизненно необходимым делом.

В то же время все они осознавали последствия того, что, если их сообщения попадут не в те руки, враждебному государству станут известны важные тайны. Именно опасение того, что враги перехватят сообщение, послужило причиной активного развития кодов и шифров – способов сокрытия содержания сообщения таким образом, чтобы прочитать его смог только тот, кому оно адресовано.

Стремление обеспечить секретность означало, что в государствах функционировали подразделения, которые отвечали за обеспечение секретности связи путем разработки и использования самих надежных кодов и шифров. А в это же время дешифровщики врага пытались раскрыть эти шифры и выведать все тайны.

Дешифровщики представляли собой алхимиков от лингвистики, отряд колдунов, которые пытались с помощью магии получить осмысленные слова из бессмысленного набора символов. История кодов и шифров – это многовековая история поединка между «творцами» и «взломщиками» шифров, интеллектуальная гонка шифровального «оружия», которое повлияло на ход истории.

Шифр всегда является объектом атаки криптоаналитиков. Как только дешифровщики создают новое средство, обнаруживающее уязвимость шифра, последующее его использование становится бессмысленным. Шифр или выходит из применения, или на его основе разрабатывается новый, более стойкий. В свою очередь, этот новый шифр используется до тех пор, пока дешифровщики не найдут его слабое место, и т. д.

Борьба, которая не прекращается между «творцами» и «взломщиками» шифров, способствовала появлению целого ряда замечательных научных открытий. Криптографы постоянно прилагали усилия для создания все более стойких шифров относительно защиты систем и средств связи, в то время как криптоаналитики беспрестанно изобретали все более мощные методы их атаки.

В своих усилиях разрушения и сохранения секретности обе стороны привлекали самые разнообразные научные дисциплины и методы: от математики к лингвистике, от теории информации к квантовой теории. В результате шифровальщики и дешифровщики обогатили эти предметы, а их профессиональная деятельность ускорила научно-технический прогресс, причем наиболее заметно это оказалось в развитии современных компьютеров.

Шифрование – единственный способ защитить нашу частную жизнь и гарантировать успешное функционирование электронного рынка. Искусство тайнописи, которая переводится на греческий язык как криптография (*др.-греч.* κρυπτός – тайный и γράφω – пишу), даст вам замки и ключи информационного века. Чтобы в последующем вся изложенная ниже информация была понятной, рассмотрим основные понятия и термины этой науки.

Информация, которая может быть прочитана и понятна без каких-либо специальных мероприятий, называется открытым текстом. Метод перекручивания и сокрытия открытого текста таким образом, чтобы спрятать его суть, называется шифрованием. Шифрование открытого текста приводит к его превращению в непонятную абракадабру, именуемую шифротекстом. Шифровка позволяет спрятать информацию от тех, для кого она не предназначается, невзирая на то, что они могут видеть сам шифротекст. Противоположный процесс превращения шифротекста в его исходный вид называется расшифровыванием.

Криптография – это мероприятия по сокрытию и защите информации, а криптоанализ (*греч.* ἀνάλυσις – разложение) – это мероприятия по анализу и раскрытию зашифрованной информации. Вместе криптография и криптоанализ создают науку криптологию (*греч.* λόγος – слово, понятие).

Криптология – это наука об использовании математики для шифрования и расшифровывания информации. Криптология позволяет хранить важную информацию при передаче ее обычными незащищенными каналами связи (в частности, через интернет) в таком виде, что она не может быть прочитанной или понятой никем, кроме определенного получателя. Криптоанализ являет собой смесь аналитики, математических и статистических расчетов, а также решительности и удачи. Криптоаналитиков также называют «взломщиками».

Криптографическая стойкость измеряется тем, сколько понадобится времени и ресурсов, чтобы из шифротекста восстановить исходной открытый текст. Результатом стойкой криптографии является шифротекст, который чрезвычайно сложно «сломать» без владения определенными инструментами дешифрования.

Криптографический алгоритм, или шифр – это математическая формула, которая описывает процессы шифрования и расшифрования. Секретный элемент шифра, который должен быть недоступный посторонним, называется ключом шифра.

Чтобы зашифровать открытый текст или разговор, криптоалгоритм работает в сочетании с ключом – словом, числом или фразой. Одно и то же сообщение, зашифрованное одним алгоритмом, но разными ключами, будет превращать его в разный шифротекст. Защищенность шифротекста полностью зависит от двух вещей: стойкости криптоалгоритма и секретности ключа.

Ну, а теперь перейдем к интересной и захватывающей истории русской криптологии и секретной связи…

Часть 1. Российская история

1.1. Древнерусская тайнопись

Наиболее ранней из известных по древнерусским памятникам письменности системой тайнописи была система «иных письмен». В этом виде тайнописи буквы кириллицы заменялись буквами других алфавитов: глаголицы, греческой, латинской или пермской азбуки.

Использование греческой тайнописи связывают с определенной модой, которая пришла в конце XVI века. Появление же этого способа тайнописи было обусловлено, с одной стороны, южнославянским влиянием, несшим кое-какие навыки и греческого письма, более близкого югу славянства, чем Руси, а с другого – оживлением отношений Московской Руси с греками, которые начались с конца XIV века.

Использование латинской азбуки как тайнописи относится к более позднему времени и обусловлено усилившимся западноевропейским влиянием. В распространении этого вида тайнописи, которая встречается в рукописях XVI и XVII веков, вероятно, известную роль играла школа с ее латинским языком преподавания.

Несколько обособленное место среди других алфавитов по отношению к тайнописи занимает пермская азбука. Эта азбука, которая была создана пермским епископом Стефаном на основе современного кириллического и греческого алфавитов, не приобрела практического применения и уже в XV веке, как малоизвестная, стала тайнописью. Но и в этом качестве она не была широко распространена.

Второй после системы «иных письмен» системой тайнописи, известной из русских рукописей, была система «измененных знаков», зафиксированная уже в XIV веке. 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.

Тахиграфия – это изменение написания букв, когда писалась или часть буквы, или наоборот, ее написание дополнялось новыми элементами. Сообщения нередко записывали справа налево или вверх ногами. Часто тахиграфия соединялась с использованием иностранных алфавитов.

Первая разновидность такой тайнописи была открыта ученым М. Сперанским в Смоленском Псалтыре 1395 года. По его свидетельству, этот Псалтырь Онежского Крестного монастыря сохранялся в свое время в Архангельском местном отделении Церковно-археологического комитета. Его писарь, монах Лука, который замечательно владел искусством письма, любил, по-видимому, и тайнопись. В этой рукописи он применил три вида тайнописи: один – измененных начертаний, второй – цифирь счетная, третий – система вязи.

Использовали писари древних рукописей и систему условных алфавитов. Как правило, в их основе лежали уже известные: греческий, глаголический, кириллический, в которых привносились какие-то изменения или дополнения. Однако случались в рукописях и оригинальные условные алфавиты, построенные или по какому-то определенному принципу, или абсолютно произвольных начертаний.

Образцом алфавита, придуманного специально для тайнописи, притом по особенному принципу, может служить ключ к тайнописи, изображенный на отдельном листе второй половины XVII ст. (Собрания Большой Патриаршей библиотеки № 93).

Здесь тайнопись заключается в замене обычных букв треугольниками и четырехугольниками, заимствованными из решеток, составленных из двух параллельных линий, пересеченных двумя такими же линиями под прямым углом. В полученных клеточках 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, ввиду места буквы в нем. Поскольку при таком размещении букв в клетках вся азбука не могла поместиться, то в этой тайнописи не оказывается знаков для таких букв кириллицы, как «ш», «ь» и тому подобных.

Следующий вид тайнописи, которая использовалась писарями в российских рукописях, – это «система замен». Выделяют два вида такой тайнописи: «простую литорею» (от *лат. litera* – буква) и «мудрую литорею», а также, как вариант этой последней, тайнопись «в квадратах». «Простая литорея» заключалась в том, что каждая из десяти по порядку азбуки согласных, поставленных в одном ряду, заменялась соответствующей ей буквой во втором таком же ряду, который состоял из последних десяти согласных, которые шли в обратном (справа налево) порядке.

Первый документ, который дошел до нас и содержал данный тип криптосистемы, датировался 1229 годом. Однако по-настоящему широкое распространение она получила в конце XVII века. Ключ к «простой литорее» такой:

Б	В	Г	Д	Ж	И	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

Слово «УКРАИНА», записанное «литореей», выглядит так: «УТМАИПА».

Более сложной разновидностью «литореи» была так называемая «мудрая литорея», где все буквы кириллической азбуки, включая гласные, заменялись на другие буквы и символы. К этому же виду тайнописи, которую использовали в XVI–XVII веках, относилась тайнопись «в квадратах», где таблицы замены букв выписывались в виде квадратов. Нередко писари прибегали к написанию фраз в обратном порядке, составляя своеобразные криптограммы, или не дописывали букву – подобный шифр назывался «полусловицей».

Цифровая система тайнописи, которую тогда называли «счетной» или «цифирной», была основана на употреблении букв как цифр и на разных практических действиях с ними и была очень распространенной. Следует сказать, что в древнерусских рукописях встречались разные ее виды: простая и сложная цифровая система, описательная система, система особенного применения арабских цифр, система значков, то есть с использованием разных значков для обозначения цифр-букв. Цифровая тайнопись существовала на Руси уже в самом начале XIV века.

Простая цифровая тайнопись заключалась в том, что для каждой цифры-буквы, которая отвечала желательной в обычном письме букве, давалось несколько преимущественно одинаковых слагаемых. Так, чтобы получить нужную букву, нужно было провести сложение, а полученная сумма, изображенная соответствующей цифрой-буквой, и была искомой буквой. Реже сумма состояла из разных цифр-букв, причем каждая группа цифр-слагаемых отделялась каким-либо знаком или пропуском от соседних. Буквы, что не имели цифрового значения, оставались неизменными.

Арабские цифры начали использоваться в качестве тайнописи лишь с того времени, как они начали входить в употребление в российской письменности, то есть со второй половины XVI века на российском юго-западе и с начала XVII века на северо-востоке.

К другим системам тайнописи, известным по древнерусским рукописям, принадлежал «мононкондил», разные приемы образного и фигурного письма, а также «акростих» (стихотворение, в котором начальные буквы строк образуют слово или фразу). «Акростих» – типичный для европейской средневековой письменной культуры прием организации поэтического тек-

ста – входил в арсенал художественно изобразительных средств древнерусских авторов уже с конца XI века.

Долгое время государственная тайнопись в трудах отечественных ученых именовалась «дипломатической тайнописью». В первый раз такой термин был введен ученым Поповым, который в 1853 году опубликовал труд «Дипломатическая тайнопись времен царя Алексея Михайловича с дополнением к ней». Следом за ним и другие исследователи российской тайнописи начали называть переписку при российском дворе «дипломатической тайнописью», а шифры, которыми она велась, «дипломатическими».

Следует, однако, отметить, что тайная дипломатическая переписка составляла лишь часть (правда, большую) шифрованной переписки при дворе, которая вместе с дипломатическими касалась и военных вопросов, а также внутренних государственных дел. Но именно в сфере дипломатии, со свойственными ей специфическими чертами и особенностями, в России почти на протяжении двух столетий проходило основное становление криптологии как государственно значимого дела. Политическая борьба, политическая игра – другими словами, ведение «большой политики» было немыслимо без охраны государственной тайны.

Активная внешнеполитическая деятельность царя Ивана IV Васильевича (Грозного) и связанные с ней войны повлияли на становление и развитие тайнописного дела. Годом рождения российской криптологической службы можно считать 1549 год, когда была образована «Посольская изба», позже названная «Посольским приказом», при котором работала «цифирная» палата тайных дел. С момента ее образования в России начали активно использовать криптологические методы в дипломатической и военной переписке.

Название «цифирной» палата получила, возможно, по старой алфавитной системе записи чисел. Выделение цифр, да и собственных имен в тексте раньше делалось с помощью «титла» – специального знака, который проставлялся над строкой. Шифры приходилось выделять в сообщении так же, как и цифры, то есть «титловать» их. Поэтому полностью понятно название шифра «цифрой», то есть текстом, который требует специального прочтения. Впрочем, возможно, что слово «цифирная» в названии палаты была буквальным заимствованием французского слова «chiffre», которое означало как шифр, так и цифру.

С конца XVI века российские послы за рубежом начали получать шифры в виде таблиц замены, которые нужно было «вытвердить гораздо памятно». В приказе царя Федора Иоанновича, который в 1589 году получил посол Николай Воркач, ему поручалось «писать письма мудрой азбукой, чтоб оприч Царского величества никто не разумел». В той азбуке каждая буква заменялась своим особенным знаком.

«Подьячие Посольского приказа», которые поддерживали связь с царскими представителями за границей, нередко пользовались шифрованной перепиской, которую называли «затейным письмом». Ключ к расшифровке этих посланий не записывался, его заучивали наизусть. Существовали разные варианты тайного письма, но по правилам конспирации никто из подданных не должен был знать все варианты тайнописи.

С началом правления династии Романовых (1613) укрепляются основы феодального строя. В 1619 году из польского плена вернулся отец царя Михаила Романова Федор, постриженный Борисом Годуновым в монахи под именем Филарета. Он лично занимался делами «Посольского приказа» и даже разрабатывал дипломатические шифры. Шифры, которые применялись в то время, были шифрами простой замены и перестановки.

Сами перестановки были достаточно простыми. Например, открытый текст разбивался на слоги, после чего в них осуществлялась перестановка букв. Так, слово «УЖГОРОД» превращалось в слово «ЖУОГДОР».

В 1633 году патриарх Филарет написал «для своих государевых и посольских тайных дел» особенную азбуку и «состав затейным письмом». Сохранился приказ российскому представителю в Швеции Д. Францбекову, из которого видно, что при составлении сообщений царю

посол должен был использовать тайнопись. Приказ заканчивался таким образом: «Да что он, Дмитрий [Францбеков], будучи в Свее [Швеции], по сему тайному наказу о тех или иных о наших тайных делах и наших тайных вестей проведает и ему обо всем писать ко государю царю и великому князю Михаилу Федоровичу всея Руси к Москве по сему государева тайному наказу ~~затейным~~ закрытым письмом».

До наших времен дошел черновик этого приказа, в котором слово «затейным» зачеркнуто и заменено «закрытым». Следовательно, можно прийти к выводу, что в России тайнопись превратилась в одно из средств сохранения государственных тайн.

Так, в инструкции российскому агенту в Швеции Дмитрию Андрееву говорилось: «Лета 7143 (1653) декабря 15 день… А про те тайные дела и про затейное письмо подьячий Иван Исаков и иной никто отнюдь не ведал, и черные о сих тайных делах тем же затейным письмом держать у себя бережно, чтоб о тех тайных делах и про то затейное письмо оприч его, Дмитрия, подьячий Иван Исаков и иной никто однолично не проведал».

Приведем также выдержку из присяги переводчика-шифровальщика конца XVII века: «…ему всякие государственные дела переводить в правду, и с неприятелями государскими тайно никакими письмами не ссылаться и мимо себя ни через кого не посылать, и в Московском государстве с иноземцами о государственных делах, которые ему будут даны для перевода, ни с кем не разговаривать».

При усилении центральной власти в годы правления царя Алексея Михайловича (1629–1676) применение шифров распространяется. В 1654 году царь образовал «Приказ большого государя тайных дел», которым руководил лично, а бояре к тайным делам не допускались. Как писал Г. Котошихин, «А устроен тот Приказ при нынешнем царе, для того чтоб его царская мысль и дела исполнилися все по его хотению, а бояре бы и думные люди о том ни о чем не ведали».

Главное должностное лицо приказа – «Тайный дьяк» – имел титул «дьяка в государевом имени», что означало право подписывать указы от имени царя. Главной задачей приказа был негласный контроль за высшими должностными лицами. «Подьячие приказа» присматривали за воеводами во время войны и посылались с посольствами за границу: «и то подьячие над послами и над воеводами подсматривают и царю, приехав, сказывают: и которые послы, или воеводы, ведая в делах неисправление свое и страшась царского гневу, и они тех подьячих дарят и почитают выше их меры, чтоб они, будучи при царе, их послов выславляли, а худым не поносили».

Сам царь, очень образованный для своего времени, лично также использовал шифры и в своей приватной переписке. Послы и резиденты всегда обеспечивались шифрами. Например, в 1673 году резидентом в Речь Посполитую (Польшу) был назначен полковник В. М. Тяпкин. По пути в Вильно его догнал царский гонец и вручил ему «знаки тайнописи и повеление царское пользоваться ими для донесений».

В государственной криптологии получают развитие и некоторые другие способы тайнописи, известные по древнерусским рукописям, например, таким как «мудрая литорея». Этим способом, в частности, был зашифрован текст, отлитый на большом колоколе Саввино-Сторожевского монастыря под Звенигородом. Шифрование текста, по предположению ученых, осуществил 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 века, 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…».

1.2. «Цифирные азбуки» Петра I

Первым русским царем, который четко осознал важность шифрования депеш и развития шифровального дела для обеспечения безопасности государства, был Петр I Великий (1672–1725). Эпоха его правления характеризуется усилением российского государства, всех его управленческих структур, а также структур исполнительной власти. Петр I осуществил ряд важнейших реорганизаций: организацию мануфактуры, строительство горных и оружейных заводов, развитие торговли, включая межгосударственную, создание Сената – высшего органа власти по делам законодательства и государственного управления, создание коллегий.

Активная внешнеполитическая деятельность Петра I требовала создания постоянной криптологической службы, способной обеспечить эффективную защиту своих сообщений и раскрытие дипломатической переписки других государств. Сначала функции криптослужбы выполнял «Посольский приказ», позже параллельно с ним начала функционировать «Посольская канцелярия» при Петре I.

Указом от 18 февраля 1700 года во главе «Посольского приказа» и принадлежащих ему приказов был официально поставлен выдающийся деятель и дипломат раннего периода петровского времени Федор Алексеевич Головин (1650–1706). Он заменил думского дьяка Е. И. Украинцева, который в 1699 году был отправлен послом в Константинополь на русском корабле, который впервые появился в водах Босфора.

При своем назначении Ф. А. Головин получил звание «начального президента государственной посольской канцелярии». Как генерал-адмирал Ф. А. 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 рубежом, оказывал большое влияние на внешнюю политику России в период Северной войны. Под непосредственным наблюдением Ф. А. Головина работало «цифирное» отделение.

Уже в самом начале XVIII века Петром I была создана «Походная посольская канцелярия», что сосредоточила в своем ведении важнейшую политическую переписку. Создание ее было вызвано частыми поездками Петра I. «Походная канцелярия» была преимущественно личной канцелярией императора, откуда выходили 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 к ее названию добавлялось слово «посольская».

Первое упоминание в документах о «Походной канцелярии» относится к 1702 году. В это время царь отправился «в поход» на Архангельск. В поездке его сопровождал начальник «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 в дальнейшем находиться под контролем бояр, наиболее важные дела решались Петром I уже в Архангельске.

В 1706 году «Посольский приказ» возглавил Гавриил Иванович Головкин (1660–1734), который был родственником Петра I по материнской линии. После смерти Ф. А. Головина, 23 сентября 1706 года, помощником Г. И. Головкина был назначен Петр Павлович Шафиров (1669–1739), который с 1703 года работал «тайным секретарем» при «Походной канцелярии».

До 1710 года «Походная канцелярия» окончательно обосновалась в Петербурге и из временного учреждения стала постоянной, причем с 1709 года ее стали называть просто «Посольской канцелярией». Именно там была сосредоточена вся работа по зашифровыванию и расшифровыванию переписки Петра I и его приближенных с разными корреспондентами, а также по созданию шифров и рекомендаций по их использованию.

В период с 1710-го по 1718 годы эта канцелярия стала главным органом внешних отношений России. Компетенция ее расширилась в ущерб «Посольскому приказу», который остался в Москве. Выросла численность личного состава канцелярии. В 1709 году Г. И. Головкин был назначен государственным канцлером, а П. П. Шафиров – вице-канцлером. Именно эти первые лица государства руководили деятельностью русской криптослужбы.

Канцлер и вице-канцлер давали указания по созданию новых шифров, замене обветшалых, обеспечению шифрами корреспондентов – дипломатов, военачальников, других государственных деятелей. Непосредственно им докладывались отчеты о создании новых шифров и добыче иностранных шифров.

Касательно русских «цифирных азбук» и ключей 1700–1720-х годов, они были шифрами замены, где элементы открытого текста, которые в дальнейшем будем называть шифровеличинами, заменяются условными обозначениями – шифробозначениями. Шифруемые тексты писались на русском, французском, немецком и даже греческом языках. В разных шифрах шифровеличинами выступали отдельные буквы, слова и стандартные выражения.

Как шифробозначения использовались элементы, как правило, алфавитов, специально составлявшиеся с этой целью, которые могли быть буквами кириллицы, латиницы, других азбук (например, глаголицы), цифры, особые значки. Часть таких значков, имевших иногда причудливые контуры, были нейтральны по значению, другие же были символами, до нашего времени почти абсолютно забытыми и известными лишь узкому кругу лиц, а в ту далекую эпоху несшими определенную смысловую нагрузку. К этим последним относились и астрологические символы планет, которые одновременно были и символами металлов.

В шифрах петровской эпохи использовались только индоарабские цифры, что было, вероятно, следствием того, что именно Петром I в начале XVIII столетия была выведена из применения архаичная буквенная кириллическая нумерация, которая применялась до этого. Реформировал Петр и кириллическое письмо, введя новый вид шрифтов, определивших современный вид русской письменности. Однако старые графемы (минимальные единицы письменной речи) продолжали использоваться в качестве тайнописи.

Употреблялись как шифробозначения и буквенные сочетания. Таким образом, в то время в России использовались однобуквенные, двухбуквенные, цифровые, буквенно-составные шифрозамены. Первые государственные шифры были шифрами простой или взаимнооднозначной замены, в которых каждой шифровеличине соответствовало только одно шифробозначение, и каждому шифробозначению – одна шифровеличина.

В русские шифры этого периода, как правило, вводятся «пустышки» – шифробозначения, которым не соответствует ни один знак открытого текста. Хотя обычно как пустышки использовалось всего 5–8 шифровеличин, понятно, что введение их в шифротекст, получавшийся в результате замены элементов открытого текста шифробозначениями, отражало стремление создателей шифров осмыслить дешифрование шифропереписки.

Эти пустышки разбивали структурные лингвистические связи открытого текста и, в известной степени, изменяли статистические закономерности, то есть именно те особенности текста, которые использовали, в первую очередь, при дешифровки шифра простой замены. Кроме того, они изменяли длину открытого сообщения, которое осложняло привязку текста к шифрособщению. Поэтому, по-видимому, не случайно, по данным Д. Кана, первый такой русский шифр был дешифрован англичанами лишь в 1725 году.

Кроме того, в некоторых шифрах шифробозначения-пустышки могли использоваться для шифрования точек и запятых, содержавшихся в открытом тексте. Как правило, это особо оговаривалось в кратких правилах пользования шифром, которые вставлялись в этих случаях в шифры.

Внешне шифр петровской эпохи представлял собой лист бумаги, на котором от руки была написана таблица замены: под горизонтально расположенными в алфавитной после-

довательности буквами кириллической или другой азбуки, соответствующей языку открытого сообщения, были подписаны элементы соответствующего шифроалфавита. Ниже могли размещаться пустышки, краткие правила пользования, а также небольшой словарь, который назывался «суплементом» и содержал некоторое количество слов (имен собственных, географических наименований) или каких-то стойких словосочетаний, которые могли активно использоваться в текстах, предназначенных для шифрования с помощью данного шифра.

Самым ранним шифром описанного типа была «цифирная азбука» 1700 года для переписки Коллегии иностранных дел (далее – КИД) с русским послом в Константинополе Петром Толстым. Она была шифром простой замены, в котором кириллической азбуке соответствовал специально составленный алфавит. Здесь же были 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». Второй особенно интересен: «Такову азбуку азволнил [изволил] во 1700 г. написать своею рукою Великий государь по друго диво еси же». Из этого выходит, что автором данного шифра был сам Петр Великий.

В Государственном архиве Татарстана находится собственноручное письмо Петра I Толстому, в котором он пишет, что посылает ему шифр для корреспонденций. Этот шифр имел такие правила пользования: «Сии слова без разделения и без точек и запятых писать, а вместо точек и запятых и разделения речей вписывать из нижеподписанных букв…»:

А	Б	В	Г	Д	Е	Ж	И	Й	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	Э	Ю	Я	
ь	ъ	ю	я	ф	а	бе	ва	гу	ди	

Слово «УЖГОРОД» превращалось в шифротекст «амнюинхицахизе».

Был здесь и небольшой словарь с именами некоторых государственных деятелей и названиями нескольких воинских подразделений и географическими названиями. Это обстоятельство также нашло отражение в правилах пользования, где говорилось: «Буде же когда случится писать нижеписанных персон имяна и прочее, то оныя писать такими знаки, какия против каждой отмечено, однакож все сплош, нигде не оставливая, а между ними ставить помянутыя буквы, которыя ничего не значат».

Интересным был и блокнот с шифрами, которыми переписывался Петр I. Это была тетрадь, листы которой были скреплены веревкой. Размер тетради: 20 Ч 16 см. На каждой ее странице было записано по одному шифру, а всего их было шесть:

1) шифр Петра I, который был ему прислан из КИД во Францию в 1720 году для переписки «от двора ко двору»;

2) шифр «для писем к графу Г. и барону П.»;

3) к князю Г. Ф. Долгорукому;

4) к князю А. И. Репнину (1715);

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 российским алфавитом отличался от предыдущих тем, что как шифробозначения в нем были использованы не буквы какого-нибудь алфавита, а числа. Рассмотрим еще несколько шифров раннего типа.

«Азбука, данная из государственной коллегии иностранных дел 3 ноября 1721 г. камер-юнкеру Михаилу Бестужеву, отправленному в Швецию», предназначалась для шифрования писем Бестужева к Петру I и в КИД. Алфавит в этом шифре был русским с простой буквоцифро-значковой заменой без усложнений. Эта и много других «азбук» хранились в конвертах, на которых были надписи о том, для каких целей предназначался данный шифр.

Шифры для переписки с царем или КИД в обязательном порядке вручались всем, кто следовал 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 герцогу Мекленбургскому. Дана Салтыкову 1 декабря 1721 г.».

Сохранились и шифры канцлера Г. И. Головкина. Так, шифры, которыми пользовался канцлер в 1721, 1724 и 1726 годы для переписки с разными государственными деятелями, были подшиты в одну тетрадь. У корреспондентов Г. И. Головкина были первые экземпляры этих шифров, у канцлера – вторые. Эта тетрадь содержала 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 т. п.

Все эти шифры построены одинаково, хотя и имеют некоторые особенности. Так, в «Азбуке Алексея Гавриловича Головкина» русский алфавит, где каждой согласной букве соответствовало по одному шифробозначению, а гласной – по два, одно из которых – буква латиницы, а другое – двузначное число или два двузначных числа.

Интересно, что, в отличие от многих других шифров, этот шифр написан не по горизонтальным строкам, а по вертикали в два столбца. В нем было 13 пустышек (букв кириллицы), обозначенных как «пустые между слов дабы расстановок не знать». Кроме того, были особые, также буквенные обозначения для запятых и точек. Таких обозначений было пять.

Как условные обозначения использовалась целая система цифр, идеограмм, особых значков, специально составленных алфавитов. Так, в шифровках Петр I изображал имя украинского гетмана Ивана Мазепы в виде топора и виселицы после того, как тот перешел к шведскому королю Карлу XII в октябре 1708 года, а руководителя восстания в 1707–1709 годах К. Булавина – в виде виселицы.

Петр I уделял особое внимание надежной рассылке шифров и ключей к ним. Он писал одному из своих послов: «При этом посылаем к вам ключ, и ежели сей посланный здорово с ним поедет, и о том к нам отпиши, дабы мы впредь нужные письма могли тем ключом писать и посылать». Выражения «здорово» (т. е. дошло) и «невредно» (т. е. получено) означали, что шифр или письмо дошли благополучно. По указанию Петра I курьер должен был «как можно меньше знать, что он перевозит, и быть довольным оплатой своего труда». Самому же курьеру приказывалось: «…отнюдь ничьей грамотки не распечатывать и не смотреть».

Следовательно, документы свидетельствуют, что в петровскую эпоху центром, где создавались шифры, где они вручались или откуда они рассылались корреспондентам, был сначала «Посольский приказ», потом – «Посольская походная канцелярия», а с 1720 года – Первая экспедиция КИД.

Вся деятельность по изготовлению шифров осуществлялась под непосредственным руководством самого императора, канцлера и вице-канцлера. Как в будущем в КИД, так и в «Посольском приказе» существовал специальный штат, которому поручалось зашифровывать и дешифровывать переписку. Текст, который подлежал шифрованию, переписывали должным образом дьяки «Посольского приказа», а затем переводчики и секретари КИД. Они же осуществляли и дешифровку писем.

В деловых бумагах нередко употреблялось слово «перевод», когда речь шла о расшифрованных письмах, и вспоминались «переводчики» – лица, которые занимались не только соб-

ственно переводом корреспонденции, но и ее расшифровыванием. В Посольском приказе, например, переводчиком польских писем был Голембовский. Он «переводил», т. е. дешифровывал письма, написанные тайнописью, которые приходили из Польши. П. П. Шафиров, посылая Головкину письма польских министров, писал: «А цифирь такая, чаю, есть у Голембовского».

Ключ к шифру вручали непосредственно тому лицу, с кем надлежало переписываться. Иногда части ключа могли пересылаться нарочными. Для этого их упаковывали в конверт, который опечатывался несколькими сургучными печатями. На конверте иногда писалось имя нарочного. Так, в 1709 году Я. В. Полонскому было поручено следить за движением войска бобруйского старосты и не допустить его соединения с корпусом шведского генерала Крассау. Я. В. Полонский был обязан применять шифр. «При этом посылаем к вам ключ, – писал Петр, – и ежели сей посланный здорово с им поедет, и о том к нам отпиши, дабы мы впредь нужные письма могли тем ключом писать и посылать».

Сообщения корреспондентов, полученные КИД, читались секретарями 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 КИД не было, посылать эти реляции к ним домой, а во время заседаний КИД о них докладывать, записывать налагаемые на них резолюции и составлять в ответ рескрипты.

Эти рескрипты прочитывались на следующем заседании, причем, согласно приказу от 5 апреля 1716 года, и черновые их списки, и переписанные начисто подписывались всеми членами КИД и скреплялись секретарем. Потом текст рескрипта зашифровывался и направлялся в соответствующий адрес с курьером. Вся работа КИД была строго регламентирована. Вход в апартаменты КИД позволялся только лицам, которые там служили. Инструкция от 11 апреля 1720 года, в которой было установлено устройство КИД, заканчивалась предписанием, как хранить государственные печати и «цифирные азбуки».

Для сохранения письма в тайне применялись соответствующие охранные мероприятия. Так, письмо Петра I барону Георгу Бенедикту Огильви от 17 февраля 1706 года сопровождалось такой 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».

Присылались в КИД такие азбуки в конвертах, которые опечатывались красными сургучными печатями, однако не государственными, а личными отправителей. Пересылали шифры довольно часто, ведь срок их действия был ограничен, и документы, у которых закончился срок действия, направлялись в КИД.

Постоянно шифрованная переписка осуществлялась с дипломатическими представителями России за рубежом, в частности: 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 российским двором имели: А. А. Матвеев – посол в Англии, Голландии, Австрии; Б. И. Куракин – посол в Риме, Лондоне, Нидерландах, Ганновере, Париже, и много других дипломатов, чьи шифры сохранились.

Часто зашифровывались письма и коронованных корреспондентов – польского короля Августа II, прусского короля Фридриха, хотя чаще эту переписку вели министры и вельможи союзных государств: 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 Михаила Раковицы, молдавского посланника Георгия Кастриота. Кратковременные дипломатические

миссии также сопровождались вручением секретной «азбуки» лицу, которое следовало из России за границу.

Высший командный состав армии и флота также имел шифры для переписки с царем. Известны шифрованные письма Петра I к адмиралу Ф. М. Апраксину, фельдмаршалу Г. Б. Огильви, фельдмаршалу Б. П. Шереметьеву, фельдмаршалу-лейтенанту Гольцу и их шифрованные ответы. При этом Петр I уделял большое значение качеству тайнописи. Так, царь с недовольством сообщал фельдмаршалу Г. Б. Огильви: «Цыфирь вашу я принял, но оная зело к разобранию легка».

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 шифры, в которых как шифровеличины использовались буквы, слоги, слова, словосочетания соответственно русские, немецкие, французские. Петр I особенно часто использовал французские шифры.

В одном из писем Г. Б. Огильви жаловался А. Г. Головкину, что не сумел прочитать 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 французской 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… Извольте ко мне через цифирь мою писать, чтоб я мог разуметь…».

Петр объяснил, почему он перешел в переписке тайнописью с немецкого языка на французский: «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».

Вручались шифры для секретной переписки и лицам, которые получали специальные военные задачи от царя. Наиболее близким лицом к Петру I, как известно, был А. Д. Меншиков, которому после Полтавской победы царь присвоил чин генерал-фельдмаршала. Шифрованная переписка между Петром и Меншиковым касалась чрезвычайно важных вопросов. Так, Петр I в январе 1708 года послал Меншикову шифрованное «Рассуждение», которое рассматривалось на военном совете в городе Вильно 3 февраля, и просил его высказаться по данному вопросу. В другом случае Петр требовал, чтобы Меншиков со своей стороны прислал «Рассуждение» цифирью.

Меншиков, в свою очередь, переписывался секретной 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. Комендант Полтавы А. С. Келин получил 19 июня 1709 года, т. е. за неделю до Полтавской битвы, зашифрованное 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».

Таким образом, военная шифрованная корреспонденция сопровождалась еще и условной сигнализацией. Сами письма пересылались в полых бомбах, поскольку осада шведами Полтавы не давала возможность переписываться иным образом. Через 2 дня, 21 июня, А. С. Келин сумел сообщить А. Д. Меншикову в шифрованном письме о наблюдавшейся из Полтавы в шведском лагере тревоге и перегруппировке вражеских войск в связи с переходом русской армии на правый берег Ворсклы.

Переписка, касавшаяся важных внутриполитических вопросов, также шифровалась. Так, специальный шифр был разработан для переписки о восстании на Дону в 1707–1708 годах. Ключ к этому шифру имели: Петр I, следивший за ходом восстания, А. Д. Меншиков – командующий кавалерией, адмирал Ф. М. Апраксин, занимающийся строительством гаваней и флота на юге России, где развивалось восстание, подполковник Преображенского полка В. В. Дол-

горукий, назначенный начальником всех вооруженных сил, выставленных против повстанцев, и азовский губернатор И. А. Толстой, которому была подчинена территория, где находился оплот от турецкой опасности – Азовская крепость.

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

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

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

Вместе с тем Петр прекрасно понимал, что Россия в значительной степени отстала от ведущих европейских государств в сфере криптологии, поэтому ликвидировать это отставание можно было, лишь внедрив европейские шифросистемы и пригласив ведущих криптологов Европы для работы в России. Сначала выбор Петра остановился на одном из лучших специалистов в этой сфере того времени – Готфриде Вильгельме Лейбнице, однако из-за его смерти криптослужба России еще на протяжении длительного времени не могла достичь европейского уровня.

1.3. «Черный кабинет» цариц

Во время пребывания на русском престоле Екатерины I вице-канцлером России и, следовательно, руководителем ее криптослужбы стал Андрей Иванович Остерман (1686–1747). В 1708 году он был принят переводчиком Посольского приказа и служил в Походной канцелярии царя. В июле 1710 года он был послан к прусскому и датскому королям, а по возвращении был назначен секретарем Посольской канцелярии.

В образованной в 1720 году КИД он занял место тайного советника канцелярии. Усидчивость, трудолюбие, дипломатическое искусство и знание в совершенстве четырех европейских языков сделали его незаменимым для императрицы. 24 ноября 1725 года она наградила А. И. Остермана званиям вице-канцлера с чином действительного тайного советника, а в начале следующего года он был назначен членом Верховного тайного совета. В ноябре 1726 года Остерман стал главным начальником над почтой (почт-директором), а 1 января 1727 года получил орден Андрея Первозванного.

В созданном 10 ноября 1731 года Кабинете министров барон А. И. Остерман приобрел первостепенное влияние на дела. После смерти канцлера Головкина А. И. Остерман получил звание первого кабинетного министра и, несмотря на конфликтные отношения между ним и Бироном, сохранил крепкое положение при дворе. Императрица Анна Иоанновна в затруднительных случаях советовалась с ним, потому современники называли его «оракулом» царицы, «душой» кабинета.

При А. И. Остермане криптологи КИД продолжали работу в соответствии с уже постоянными традициями. Научная мысль не стояла на месте, постоянно велись поиски новых шифров. 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 русским или латинским, 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, бы, бо, бу, бы, бя, ва, ве, вы, во, ву, вы, вя и т. п.

Суплемент был достаточно большим и включал не только необходимые имена царственных персон, государственных деятелей («персоны») и географические названия, как это было ранее, но и другую активную лексику. В этот раздел, например, могли входить слова: домогательство, склонность и т. п.

Раздел «счеты», или, как его еще называли, «исчисления», как правило, во всех кодах был одинаков. Он включал 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 прибавлены числа 50 000 и 100 000.

Месяцы также перечислялись в особом разделе, и почти во всех шифрах это объяснялось так: «Месяцы для того особливыми литерами изображены, чтоб оные употреблять, когда в контексте нужда востребует, а инако в обыкновенном месте датума писать не надлежит».

За редким исключением шифробозначения – это арабские цифры. Цифры как шифробозначения для разных частей словаря всегда имели отличия. Например, если для алфавита они могли быть одно-, двух-, трехзначные, то для «суплемента» – только трех- или четырехзначные, а для других частей (месяцы, счеты) только четырехзначные. Кроме того, могли быть и другие отличия. Так, если для алфавита и «суплемента» шифробозначениями могли быть разные числа, то для других разделов – лишь числа, которые заканчивались нулями: 700, 750, 720, 4000 и т. п. Вообще для каждой последующей части словаря характерна была все растущая значимость шифробозначений.

Эти шифры имели большое количество пустышек, которые вводились с целью усложнения шифра. Могли вводиться ошибочные дополнительные цифры, которые также не имели смысла, но не входили в число пустышек. В правилах пользования шифрами, хотя они были еще очень короткими, явно проступала тенденция к использованию при шифровании даже небольших текстов основной части или даже большинства словарных величин. Как шифробозначения использовались почти исключительно цифры в отличие от шифров первой четверти века, когда в этой роли чаще выступали разные идеограммы. В новом типе шифров они применялись крайне редко и лишь для обозначения «персон».

Однако вместе с этими шифрами продолжали активно использоваться и шифры старых образцов, в которых был лишь алфавит с шифробозначениями, – цифрами, буквами или причудливыми старинными идеограммами, такими, например, как в ранней «Цифирной азбуке» для переписки с Григорием Волковым и князем Куракиным.

Разработчики шифров в этот период уже знали, что частота использования гласных букв в языке более высокая, чем согласных. Поэтому в 1730–1740-е годы в новых шифрах гласным обязательно соответствовало по нескольку шифробозначений, а согласным – одно-два. Наблюдались попытки записи шифротекста без разделения шифробозначений точками (что раньше было абсолютно исключено) или с разделением их фальшивыми точками. Способ дешифровки в правилах оговаривался заранее. Пример такого шифрования приведен в «Цифирной азбуке» для переписки с государственным вице-канцлером графом Воронцовым.

Это был шифр простой замены, где буквам кириллицы соответствовали двузначные цифровые шифробозначения, причем гласным было прибавлено по шесть шифробозначений, а согласным – по два. В правилах сказано: «Сею цифирью писать двояким образом, без точек, и с фальшивыми точками, которые как бы расставлены ни были, токмо для разбору всегда по два номера брать надлежит».

Шифробозначения в этот период выбирались всегда по определенным порядковым алфавитным схемам, что обычно не способствовало надежности шифров. Например, этот шифр выглядел так:

А	Б	В	Г	Д	Е	Ж	З	И	К
11	12	13	14	15	16	17	18	19	20
40	57	58	59	60	41	74	75	42	80
62					63			64	
85					86			87	
99					98			97	
56					55			54	

Л	М	Н	О	П	Р	С	Т	У	…
21	22	23	24	25	26	27	28	29	…
81	82	83	43					44	…
			65					66	…
			88					89	…
			96					95	…
			53					52	…

Слово «УЖГОРОД» можно зашифровать так: 441.7592. 426. 5.315; 8.974.1.488.266.560 и т. п.

С начала 1730-х годов в России наблюдался переход от алфавитных кодов к неалфавитным. В алфавитных кодах открытый текст и шифробозначения (собственно код) нумеровались 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, разработчики шифров отметили, что такой параллелизм существенно облегчал восстановление открытого текста и самого кода, поскольку правильное угадывание некоторого числа шифробозначений позволяло упорядочить в алфавите шифробозначения других словарных величин.

Понятно, что избежать такой слабости кода можно было путем перемешивания шифробозначений. В этих случаях для облегчения процессов зашифровывания и расшифровывания необходимо было составить «шифрант» и «дешифрант» – части кода, предназначенные соответственно для зашифровывания и расшифровывания. В шифрантах в алфавитном порядке располагались элементы открытого текста (шифровеличины), т. е. буквы, слоги, слова, словосочетания, а в дешифрантах в порядке возрастания – шифробозначения, если они были цифровыми. Если же они были буквенными, то в дешифрантах шифробозначения также располагались в алфавитном порядке. Однако в шифрах этого второго типа буквенные шифробозначения были крайне редки, они встречались лишь иногда в отдельных частях шифров, например в суплементе.

В этот период у разработчиков шифров появилось явное стремление соотнести каждой букве алфавита в шифре как можно больше шифробозначений. Однако все эти шифробозначения имели один очень большой изъян: они писались подряд, что давало возможность легко их раскрыть. Так, например, «цифирная азбука» для переписки с бароном Кейзерлингом, отправленным в Польшу в декабре 1733 года, имела такой вид:

A	11	12	13	14	15
B	16	17	18	19	20
…	…	…	…	…	…
Z	131	132	133	134	135

А в еще одном шифре камергера графа Левенвольда каждой букве латинского алфавита соответствовало даже по десять шифробозначений:

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
…	…	…	…	…	…	…	…	…	…	…

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

Однотипные по сути, эти шифры второго типа 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 был листами, сшитыми

нитями в тетрадь, а дешифрант писался на отдельном развернутом листе. В обоих случаях в шифранте шифровеличины могли помещаться по-разному: или в порядке алфавита с выделением точек и запятых отдельно в конце, или по разделам (словарь, составная таблица, алфавит, числа – «счеты», календарь – «месяцы», пустышки). В это же время начали помещать в шифрант, а часто и в дешифрант, правила пользования шифром. Эти правила объясняли те усложнения и хитрости, которыми отличался данный шифр.

Рассмотрим некоторые наиболее характерные образцы таких шифров того времени.

В 1735 году резидент Алексей Андреевич Вешняков (1700–1745) прислал в КИД «цифры, которыми он корреспондует с генералитетом и министрами российскими, обретающимися при чужестранных дворах».

«Цифирь» была оформлена в виде прошитого нитями тетради. На первой странице – заглавие: «Цифирь секретная, посланная к ея императорского величества усадьбам министрам в Лондон и Дрезден». Вся страница разбита на три вертикальных графы. Первая графа – «Алфавит для сложения». В эту графу помещены буквы российского алфавита, которым отвечают двусмысленные цифровые шифробозначения (произвольные). Сюда же помещены в алфавитном порядке наиболее употребимые предлоги, местоимения, частицы: въ, изъ, как и т. д.

Вторая графа – «Разные знаменования» – содержала словарь шифра. Наряду с тем, что каждому шифробозначению соответствовало, как правило, по одной словарной величине (например, 100 – «Ея Императорское Величество», 199 – «двор Ея Императорского Величества»), некоторым шифробозначениям соответствовали целые группы словарных величин, необходимые из которых выбирались в соответствии с контекстом письма (например: 198 – английский король, двор, Англия).

Третья графа – «Для разбору» – дешифрант. На втором листе здесь приведены «Изъяснения для употребления сей цифири», в которых были раскрыты хитрости этого шифра.

Так, в шифробозначениях отсутствуют цифры 3 и 7, т. е. может быть 46, а не 47, 36 и т. д. Сами по себе любые двусмысленные или трехзначные цифры, которые содержат 3 и 7, служили для обозначения запятых и точек. При этом рекомендовалось: «Мешать оныя между всеми как в десятичных, так и в сотенных, яко прибавкой оных число умножится. Следственно знаменательное скроется так, что никакая комбинация открыть не может. Например: А – 29 можно представит: 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 значат. Следственно, яко оне бы не были, – но едино 29 будет видеть».

Писать рекомендовалось все цифры как без вставок, так и со вставками подряд «без роставок буква от буквы и речь от речи». Особенно рекомендовал автор шифра вводить «смешения с 3 и 7» при шифровании по буквам, где шифробозначения – двузначные («вот большей части десятеричных надлежит мешать с пустыми»), потому что «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 писаная смешением пустых прилежно».

И дальше приводился пример шифрования, из которого можно было сделать 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».

Сохранился также шифр, который А. А. Вешняков вручил в январе 1737 года для переписки аббату Косу, который был русским агентом. На шифре была надпись: «Цифры с аббатом

Косом, данная ему в Каменце от резидента Вешнякова при проезде его от Турской крепости в Россию». Этот шифр был построен по принципу шифров 1720-х годов: русский алфавит, каждой букве соответствовали одно-, двух- и трехзначные цифры. Правда, было много пустышек – 85. Такой же шифр был вручен Вешняковым аббату Косу и с латинским алфавитом.

Политическими агентами России были не только государственные иностранные деятели, но и другие лица. Например, в Турции русскими агентами в этот период были иерусалимские патриархи Досифей II (1641–1707), а позже Хрисанф (1655–1731). Через Досифея шла переписка России с молдавским правителем. Патриарх Хрисанф предложил канцлеру России Г. И. Головкину секретную «азбуку» для переписки, принятую российским двором с некоторыми поправками, по поводу чего Хрисанф писал Г. И. Головкину: «Приняли мы цифирь, которая прислана в дополнку нашей, и зело изрядна».

Кроме того, Хрисанф предложил ввести в секретную переписку еще некоторые условности: «А чтоб нам чащей писать к Великому Государю и к Вашему Высочеству и безопасно, сделали мы сию цифирь. Посылаем и обид печати. И как придет к вам какое письмо, в котором есть та печать, ведомо буди, что есть наше писание. 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».

Введение множества пустышек в старые типы шифров свидетельствовало об отчетливом понимании составителями «цифирных азбук» того влияния, которое имело на раскрываемость зашифрованного текста частота употребления одних и тех же величин, особенно букв. По мере усложнения шифров количество пустышек в них все увеличивалось, порой их объем в словаре мог превышать объем его значимых величин.

Так, например, немецкий шифр от января 1744 года, полученный от генерала барона Любераса для переписки с ним русских министров при иностранных дворах, имел 165 пустышек, а в шифре от января 1745 года для переписки КИД с действительным тайным советником и чрезвычайным посланником в Берлине графом Петром Григорьевичем Чернышевым (1712–1773) пустышек вообще было великое множество. В обычной таблице пустышек было 90 – от 1003 до 1093. Кроме того, в примечании было написано: «Все нумера свыше 3015 служат тако же пустыми, како пустыми употребляются и те нумеры, которые по порядку до 3015 не доставают». Значимых величин в данном шифре было около 400, таким образом, пустышки значительно превысили это количество.

В том же 1745 году П. Г. Чернышеву был послан еще один шифр, в котором было 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 разработчики шифров стремились в этот период поместить в них как можно больше пустышек, может служить шифр, посланный в 1747 году действительному тайному советнику в Берлине барону Герману Карлу фон Кейзерлингу (1697–1764). В этом небольшом по объему шифре для шифробозначений были выбраны числа из разных, кроме первой, сотен, а также первой, шестой, седьмой, восьмой тысяч. А в качестве пустышек были 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. Конверт, в котором доставили этот шифр в Берлин, был опечатан множеством сургучных печатей и на нем была надпись о том, что доставлен он был лейб-гвардии поручиком Измайловым.

В середине XVIII века во время царствования Елизаветы Петровны была создана секретная служба перлюстрации. Результаты работы этой службы несколько раз в месяц докладывались царице, однако это потребовало создания сильной криптоаналитической службы для «взлома» иностранных шифров. Новый этап в развитии российской криптослужбы (другими

словами – ЧК) был связан с именем графа Алексея Петровича Бестужева-Рюмина (1693–1768), назначенного в 1742 году главным директором почт. Он впервые в отечественной практике привлек к криптоаналитической деятельности профессиональных ученых-математиков, причем лучших из них, которые были тогда «светилами» европейской математической науки.

Первым, кого А. П. Бестужев-Рюмин привлек к такой работе, стал известный немецкий математик и специалист по теории чисел Христиан Гольдбах (1690–1764). Именной указ императрицы Елизаветы о его назначении на «особую должность» был датирован 18 марта 1742 года, а дело об этом названо «Об определении в Коллегию иностранных дел бывшего при Академии наук профессора юстицрата Христиана Гольдбаха статским советником с жалованьем 1500 рублей, о выдаче недоданного ему в Академии наук жалованья и о выдаче ему вперед жалованья».

Больше года Х. Гольдбах потратил на приобретение практических навыков в новому деле, но первый успех в дешифровке цифровых текстов неизвестного содержания пришел к нему лишь в июле 1743 года. С июля по декабрь 1743 года им было дешифровано 61 письмо «министров прусского и французского дворов». Весной 1744 года он уже мог «ломать» шифры повышенной сложности. На Х. Гольдбаха посыпались всевозможные милости императрицы, но отметим главное – «власти предержащие» реально ощутили, что математика для государства и для них лично – это не нечто престижно-декоративное, а «щит и меч», охранявшие их непосредственные интересы.

Сохранились русские копии дешифрованных писем 1742 года: 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.

Наибольшего успеха Х. Гольдбах добился в первых числах июня 1744 года, когда им была прочитана шифрованная депеша французского посла Иоахима-Жака Тротти маркиза де ла Шетарди в Париж. Этот случай стал хрестоматийным в истории криптологии. Зная, что его письма на почте раскрывались, маркиз де ла Шетарди был уверен, что прочитать его шифр было невозможно, и поэтому легкомысленно писал об императрице, что она полностью предавалась своим утехам, была несерьезна, глупа и распутна.

А. П. Бестужев-Рюмин, ставший канцлером, ловко использовал именно этот текст в борьбе против французской придворной партии (ранее у него уже были дешифрованные тексты практически всех писем этого посла). Он разыграл перед Елизаветой сцену дешифровки депеши, «вынужденно» произнося «поносные» слова. В результате 17 июня маркиз де ла Шетарди был изгнан из страны, а работа Х. Гольдбаха в сфере дешифровки не осталась без внимания и высоко была оценена императрицей.

В 1744 году она издала указ о выдаче ему в дальнейшем годовой платы в две тысячи рублей из Статс-Конторы. В 1760 году Х. Гольдбах получил звание тайного советника с ежегодной платой в 4500 рублей. Это было одно из наивысших званий в российском государстве, и награждались им дворяне за особые заслуги перед Отчизной. Отметим, кстати, что великому математику, механику и физику Леонарду Эйлеру (1707–1783), несмотря на его выдающиеся научные достижения и постоянное покровительство со стороны русского двора, указанное звание так и не было пожаловано.

Именно с момента появления Х. Гольдбаха в штате КИД директору Санкт-Петербургского почтамта барону Федору Юрьевичу Ашу (1690–1771) начали поступать распоряжения А. П. Бестужева-Рюмина тщательным образом копировать письма полностью, ни в коем слу-

чае не пропуская в них шифротекст. В 1743 году А. П. Бестужев-Рюмин, не доверяя рядовым копиистам, приказал копировать в ЧК «цифрами писанные» части писем иностранных послов и передавать для дешифровки и перевода Ивану Андреевичу Тауберту (1710–1771).

По этому поводу А. П. Бестужев-Рюмин писал Ф. Ю. Ашу: «Усмотренные в переписываемых унтер-библиотекарусом Таубертом в цифрах писем неисправность причиной, что я Вам особливо рекомендовал, за нужно признать впредь списываемые им копии не токмо в речах, но и в цифрах все нумеры противу оригиналов сходны, с им 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».

По распоряжению А. П. Бестужева-Рюмина почтовые службы должны были раскрывать и копировать все письма зарубежных послов (даже к дамам), пересылаемых через границу. Частные письма, пересекаемые границу, также, по возможности, раскрывались все, но копировались наиболее интересные. Основной массив информации поступал непосредственно А. П. Бестужеву от Ф. Ю. Аша.

Дело перлюстрации писем оказалось чрезвычайно сложным, таким, что требовало терпения, внимания и особых навыков, которые приобретались не сразу. Конверты следовало раскрывать аккуратно, по возможности не нарушая их целостности. Дипломатическое письмо обычно помещали в конверт, который прошивали нитью и опечатывали сургучными печатями. Такое упакованное послание могло укладываться еще в один конверт, который также прошивался и опечатывался.

Технические проблемы безуликового раскрытия писем были очень значительными. Так, Ф. Ю. Аш жаловался А. П. Бестужеву-Рюмину: «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 под печатями находился (кои я искусно снял), однако же не распустился. Следовательно же, я к превеликому моему соболезнованию никакой возможности не нашел оных писем распечатывать без совершенного разодрания кувертов. И тако я оные паки запечатал и в стафету в ея дорогу отправить принужден был…».

Если раскрывал и запечатывал письма лично почт-директор, то копировал их особый секретарь, переводил же особый переводчик. Поскольку письмам необходимо было вернуть их первоначальный вид, то есть заклеить, прошить нитью и опечатать такими же печатями, которыми были опечатаны до вскрытия, то большое значение имело мастерство человека, изготовлявшего печати. Этот мастер-резчик также содержался в штате ведомства Ф. Ю. Аша. Работа его была тонкая и ответственная, ведь использовалось великое множество личных и государственных печатей, которыми дипломаты пользовались при опечатывании своих писем, направляемых в разные адреса.

В то время печать отливалась из свинца по форме, снятой гипсом со сделанного из воска негатива печати. Этот способ, кроме того, что был сложным из-за четырехкратного пересниманий оттиска (негатива – воском, позитива – гипсом, снова негатива – свинцом и, наконец, опять позитива уже на самих письмах – сургучом), давал недостаточно четкие отпечатки. В дальнейшем в середине XIX века один из чиновников МИД изобрел способ изготовления поддельной печати из серебряного порошка с амальгамой. Этот способ был очень простым и быстрым, а печать получалась четкой. Однако она имела существенный недостаток – была очень недолговечной и ломалась от малейшего неосторожного прикосновения.

Ф. Ю. Аш лично проверял все изделия резчика печатей, делал замечания, а затем отправлял готовые образцы для оценки А. П. Бестужеву-Рюмину, который делал уже окончательный вывод. По этому поводу велась переписка.

Из письма Ф. Ю. Аша А. П. Бестужеву-Рюмину от 29 февраля 1744 года: «Печатнорезчик Купи от своей болезни отчасти оправился и уже начало подделыванием некоторых штемпелей учинил, из которых эвон и сегодня два отдал, но один назад взять принужден был, дабы усмотренное мной в нем погрешение поправить, а другой, который барона Нейгауза [австрийского посла в России] есть, я за нарочитой [подходящий] нахожу и оной при чем посылаю…».

Через несколько дней А. П. Бестужев-Рюмин написал Ф. Ю. Ашу ответ:

«На рапорт ваш от 29 февраля здесь в 6 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».

В протоколах докладов императрицы Елизаветы Петровны можно прочитать следующее: «12 февраля 1745 г. 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».

27 февраля 1758 года императрица Елизавета Петровна, разгневанная своеволием канцлера А. П. Бестужева-Рюмина в придворных делах, лишила его графского достоинства, чинов и знаков отличий. Его приговорили к смерти, но государыня заменила этот приговор ссылкой в принадлежащее ему село Горетово под Можайском Московской губернии.

В результате налаженная им служба перлюстрации стала «разваливаться». При отсутствии перехваченных депеш такую же оценку стоит дать и эффективности дешифровки. Тем не менее, несмотря на то, что Х. Гольдбах в это время не имел масштабных успехов в дешифровке, созданные им шифры, насчитывавшие до 3500 цифровых групп, были одними из лучших в Европе.

Ссылка А. П. Бестужева-Рюмина продолжалась до 28 июня 1762 года, когда на троне воцарилась Екатерина II. Он сразу был вызван в Петербург, и императрица возвратила ему графское достоинство, чины, ордена и пожаловала звание генерала-фельдмаршала.

20 ноября 1764 года Х. Гольдбах умер, после чего руководитель КИД граф Никита Иванович Панин пригласил на его место математика и физика, немца по национальности Франца Ульриха Теодора Эпинуса (1724–1802). В обязанности Ф. Эпинуса и его подчиненных входило создание шифров и подбор ключей к шифросистемам перехваченной корреспонденции.

В 1769 году Ф. Эпинус был «пожалован статским советником и определен при Коллегии иностранных дел при особливой должности». За успешную работу в сфере дешифровки в 1773 году он получил чин действительного статского советника. Ф. Эпинус почти всю свою жизнь провел в России, которая стала для ученого второй Родиной.

Пользователями шифров, созданных в КИД, были: императрица (индивидуальные шифры для переписки с избранными лицами), кабинет императрицы (общие и индивидуальные шифры для переписки с высшими чиновниками государства), КИД (общие и индивидуальные шифры для переписки приблизительно с 70 дипломатическими представителями России за рубежом и их между собой; для переписки с иностранными дворами; специальные шифры для переписки с тайными агентами русского правительства), армия и флот.

Перлюстрация была важнейшей наряду с сообщениями платных зарубежных агентов источником информации для принятия внешних политических решений. Перлюстрировалась

вся зарубежная корреспонденция независимо от положения получателя и отправителя. В 1779 году императрица приказала доставлять ей из Санкт-Петербургского почтамта секретно раскрытую корреспонденцию. Чаще всего Екатерина II читала дешифрованные депеши к послам в Санкт-Петербурге даже раньше, чем они сами.

Объем перлюстрации был фантастически большим. В 1771 году количество перехваченных депеш только прусского посла составляло 150 (125 отправленных и 25 полученных), написанных разными шифрами. В 1780 году австрийский посол использовал восемь типов шифров, объемы цифровых текстов достигали 15 страниц перехваченных около 140 депеш. Текущую дешифровку осуществляли «канцелярские служители» с помощью ключей, найденных, перекупленных или похищенных Ф. Эпинусом.

В конце XVIII века дешифровальная служба России также читала французскую дипломатическую переписку. Этот результат было получен в результате сочетания аналитических методов раскрытия шифров, которыми пользовалась криптослужба, и работы агентов русской разведки, добывавших французские шифры. Русское посольство через секретаря посольства А. Машкова завербовало к себе на службу в качестве секретного агента одного из чиновников Министерства иностранных дел Франции.

Таким образом, русский посол во Франции барон Иван Матвеевич Симолин (1720–1799) получал и пересылал в Петербург шифры и ключи к ним, которыми пользовались в своей переписке госсекретарь Франции по иностранным делам граф де Монморен Сент-Эран и французский поверенный в делах в России Эдмонд Жене. В результате Россия получала разведывательную информацию в течение длительного периода, даже после того, как И. М. Симолин вынужден был покинуть революционную столицу Франции после неудачной попытки помочь вывезти Людовика XVI из Парижа.

Кроме дешифровки Ф. Эпинус занимался также и разработкой шифросистем. Его подчиненные готовили конкретные «цифири», которые тиражировались на бланках, печатавшихся в академической типографии. «Цифирные азбуки и разные другие бумаги тайн подлежащие» хранились в КИД в отдельном от пользователей хранилище в идеальном порядке и выдавались для шифрования и дешифровки депеш на считанные часы, указываемые в ведомостях. Эти операции проводились обученными «разборщиками», которые находились на должностях актуариусов.

Шифрование корреспонденции императрицы и Кабинета осуществлял кабинет-министр и его штат, а канцлера – четыре секретаря, работавшие круглосуточно. Одним из них много лет был русский писатель Денис Иванович Фонвизин. Доставка шифров и депеш канцлеру или Кабинету осуществлялась курьерами из сержантов гвардейских полков по жестко регламентируемому времени передвижения.

Задачей несравненно сложнее, чем создание шифров, была для Эпинуса дешифровка текстов. Этим делом Ф. Эпинус занимался лично со своим помощником, выходцем из немцев, Иоганном Георгом Кохом (1739–1805). Начав свою карьеру в 1762 году копиистом в Академии Наук, он был переведен оттуда Ф. Эпинусом в КИД.

Свою деятельность по дешифровке Ф. Эпинус должен был начать с проблемы поистине исторической – найти ключ к «писаным в цифрах» в 1714 году и подписанным Петром I письмам в Амстердам Осипу Соловьеву. В указе Сената от 4 января 1765 года приказывалось «… если возможно отыскать тот азбучный прежний ключ или другим каким по искусству в том средством оные разобрать переписать литерным письмом и взнесть в сенат…».

Результаты «борьбы» Ф. Эпинуса с петровским шифром неизвестны, но есть многочисленные свидетельства успешной дешифровки его службой перлюстрированной корреспонденции, за что он получил звание действительного статского советника.

Значительный вклад в российскую криптологию внесли Ерофей Никитич Каржавин (1719–1772) и его племянник Федор Васильевич Каржавин (1745–1812). Юный Е. Н. Каржа-

вин стремился к знаниям и служению обществу, поэтому в 1748 году тайно отправился во Францию. Там талантливый молодой человек поступил в Сорбонский 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.

16 сентября 1760 года Е. Н. Каржавину, «самовольно отлучившемуся за границу», было разрешено вернуться в Россию, где он начал работать переводчиком и составителем шифров в КИД. В бытность Е. Н. Каржавина в Париже в 1753 году к нему приехал родной племянник Ф. В. Каржавин.

Обучение Ф. В. Каржавина наукам в Париже продолжалось 13 лет. С мая 1763 года он жил 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. В. Каржавин попал под опеку чиновников парижской миссии, где получил работу переводчика. Ф. В. Каржавин был купцом, литератором, путешественником и первым русским, побывавшим в США, на Кубе и Мартинике. Вернувшись в Россию в 1788 году, он так же, как до него Е. Н. Каржавин, стал работать в КИД переводчиком и составителем шифров. Принял он участие и в дешифровальной работе.

С середины XVIII века в России стали использовать новые шифры. Их основные отличия от предыдущих шифров были такими. Во-первых, на русском языке начали активно использоваться коды (номенклаторы) на большое количество букв, слогов, слов, фраз и т. п.; их число достигало 1200 символов. Как правило, это были алфавитные коды с цифровыми шифробозначениями. Наиболее часто используемым буквам, слогам и т. п. соответствовало несколько шифробозначений. Таким образом, применялся шифр гомофонной замены, но на уровне не только букв, но и словосочетаний. Коды менялись регулярно, поскольку ключом такого шифра был сам код-таблица замены.

Во-вторых, увеличилось количество пустышек, которые вставлялись в шифротекст. По этому поводу в одной из инструкций по использованию шифров указывалось: «Пустые числа писать где сколько хочется, только, чтобы на каждой строке было сих чисел не меньше трех или четырех». Так определялся лишь нижний уровень количества пустышек, а верхний уровень не устанавливался. Кроме того, «не начинать пиесы [шифротекст] значащими числами, но пустыми…». Тем самым начало шифротекста в сообщении маскировалось пустышками, что усиливало стойкость шифра.

Кроме того, в шифры вставляли «особые числа», шифробозначения которых обозначали те части шифротекста, которые при дешифровке необходимо было считать пустышкой. Например, знак «+» шифротекста означал, что следующее за ним шифробозначение не имело никакого смысла. Два знака «+ +» говорили дешифровщику, что не следует читать два следующих за ним шифробозначения и т. д. Знак «=» означал, что не следует принимать во внимание все шифробозначения, стоявшие за этим знаком в данной строке шифротекста, а знак «= =» уничтожал весь последующий шифротекст на данной странице. Знак «*» уничтожал предыдущее шифробозначение, два знака «**» уничтожали два предыдущих шифробозначения и т. д.

Таким образом, текст, зашифрованный в результате применения многочисленных пустышек и написания ничего не значимых отрезков, оказывался значительно длиннее открытого текста. Расчет разработчиков шифров именно в том и заключался, чтобы шифротексты были огромными цифровыми массивами, в которых, по их мнению, только знавший ключ мог отделить «зерно от плевел».

Чрезвычайно существенным для шифров этого типа было продолжение в них традиции использования при шифровании одного сообщения разных языков: как правило, все шифры были двуязычными. Их словарь состоял из двух частей: русской и французской (иногда немецкой). Открытый текст депеши составлялся на этих двух языках, при переходе в процессе шифрования 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 шифровании не только практически вдвое увеличивалось количество используемых кодовых обозначений, но, что существеннее всего, смешивались и в известной мере выравнивались статистические характеристики шифротекста. При этом основные правила как для русской, так и для иноязычной части были одинаковыми, т. е. наличие множества пустышек, шифрования больших кусков псевдотекста, уничтожаемых при дешифровке, и т. д.

В правилах к этим шифрам говорилось: «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 полутора, по две и более, а иногда по одному только, по два и по три числа. Иногда пиесы начинаются или оканчиваются самыми значащими. Но во всяком случае часто пишутся пустые в самой середине параграфа и вместо просодии [пробела], а иногда и вмешиваются и в середине фразисов и речений. Да сверх того ставятся между пустыми и самые значащие числа, кои не понадобятся и уничтожаются».

Екатерина II лично уделяла значительное внимание шифрованию сообщений. Так, отправляя генерал-майора Алексея Григорьевича Орлова (1735–1807) в Европу с разведывательным заданием, она обеспечила его «нарочно сочиненным цифирным ключом», прибавив, что «этот ключ используется для корреспонденции вашей с Нами, которая по важности предмета своего требует непроницаемой тайны». Орлову были предоставлены также отдельные шифры на русском, немецком и французском языках для переписки при необходимости с русскими послами «при государственных дворах». Для обеспечения шифрованной переписки Орлов имел надежных и подготовленных «служителей канцелярских».

В тот период в России появились «циркулярные» шифры, т. е. общие шифры у послов и КИД, позволявшие оперативно передавать послам общие указания, приказы и т. п.

Таким образом, к середине XVIII века в России была создана сеть общей шифрованной связи. Общий шифр получил название «генеральная цифирь». Вместе с ним сохранились и «индивидуальные» шифры для связи «центра» с корреспондентами сети. Каждый корреспондент, как правило, имел несколько «индивидуальных» шифров.

Из «Генеральных цифирь» XVIII века известны такие:

в 1762 году на русском языке, с помощью которого обменивались корреспонденцией с КИД и между собой: А. П. Бестужев-Рюмин (Париж), Г. Кейзерлинг (Вена), И. А. Корф (Копенгаген), Н. И. Панин (Стокгольм), А. М. Голицын (Лондон), А. С. Мусин-Пушкин (Гданьск), К. М. Симолин (Митава), И. М. Симолин (Регенсбург), П. С. Салтыков («заграничная армия»), А. М. Обресков (Константинополь);

в 1762 году для тех же корреспондентов, но переписку можно было вести сразу на трех языках: русском, французском и немецком. Дополнительно этот шифр в 1764 году был дан генерал-майору князю Николаю Васильевичу Репнину, который следовал как полномочный министр к прусскому двору, а также генерал-аншефу князю Семену Федоровичу Волконскому;

в 1764 году на русском и французском языках, которая была разослана российским представителям в Вене, Варшаве, Копенгагене, Лондоне, Стокгольме, Берлине, Гааге, Париже, Дрездене, Митаве, Регенсбурге, Гданьске, Мадриде, Гамбурге, Константинополе;

в 1768 году на русском и французском языках, разосланная по тем же 15 адресам;

в 1771 году на французском и русском языках, разосланная 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 Петру Александровичу Румянцеву, генерал-аншефу князю Василию Михайловичу Долгорукову. В 1779 году этот же шифр был дан отправленному в Португалию чрезвычайному послу и полномочному министру графу Максимилиану-Вильгельму-Карлу Нессельроде;

в 1773 году на русском языке под знаком «165», разосланная, по сравнению с предыдущей, по первым 14 адресам;

под знаком «40, 68 и 77» – наиболее известная «цифирь» XVIII века. Она включала две тысячи словарных величин и объединяла КИД с 15 корреспондентами за рубежом: графом Г. О. фон Штакельбергом в Варшаве, князем П. А. Голицыным в Вене, бароном А. Ф. Ассебургом в Регенсбурге, князем И. С. Барятинским в Париже, министром С. С. Зиновьевым в Мадриде, посланником А. М. Белосельским-Белозерским в Дрездене, князем А. М. Голицыным в Гааге, министром И. М. Симолиным в Стокгольме, министром П. П. Долгоруковым в Берлине, министром К. И. Остен-Сакеном в Копенгагене, министром А. С. Мусиным-Пушкиным в Лондоне, резидентом Г. И. Гроссом в Лондоне, послом А. С. Стахиевым в Константинополе, резидентом И. М. Ребиндером в Гданьске, князем Н. В. Репниным в Берлине.

В 1771 году была параллельно организована общая сеть шифрованной связи, охватывавшая абсолютно другой регион. Так, с помощью «Генеральной цифири» в 1771 году под знаком «1631» переписывались между собой и с КИД десять корреспондентов: полномочный министр Я. И. Булгаков в Константинополе, граф С. Р. Воронцов в Венеции, граф А. К. Разумовский в Неаполе, полномочный министр А. С. Мордвинов в Генуе, полномочный министр князь Н. Б. Юсупов в Турине, граф Мореиго во Флоренции, поверенный А. К. Псаро по делам на Мальте, генеральный консул в Смирне коллежский советник И. И. Хемницер, генеральный консул в Молдавии, Валахии и Бессарабии И. И. Северин, коллежский асессор Юлиниц в Сицилии.

В КИД велся тщательный учет всех «цифр». Их перечень, списки лиц, кому они были разосланы, от кого получены назад отдельные экземпляры, на каком языке были составлены, и другие необходимые сведения заносились в особые реестры.

Если экземпляр шифра кем-то из корреспондентов терялся или возникало подозрение, что шифр оказывался известен врагу, то немедленно издавался императорский указ о выведении этого шифра из действия и замене его другим. Этот указ сразу же рассылался всем корреспондентам, входившим в данную сеть связи.

Соблюдению тайны шифропереписки в КИД уделялось большое внимание. Рассуждая «о наилучшем содержании в секрете всех в секретной экспедиции дел», Коллегия еще в 1744 году определила приказать всем служителям этой экспедиции (и архиву) «ни с кем из посторонних людей об этих делах не говорить, не ходить во дворы к чужестранным министрам и никакого с ими обхождения и компании не иметь».

Этот приказ был подтвержден повторно 28 марта 1758 года: «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 конце приказа подтверждался запрет допускать кого-либо постороннего в помещения, занятые секретной экспедицией.

При императрице Екатерине II 15 марта 1781 года КИД в третий раз получил приказ 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 других чинов коллегии не ходил в дома иностранных министров, не имел с ними разговоры о делах, никого из них в своем доме не принимал и ни под каким видом не вел с ними переписку. Тот же запрет был повторен указом от 3 августа 1791 года.

КИД также внимательно следила за хранением шифров. Лично государственный канцлер, а им в тот период был граф Иван Андреевич Остерман (1725–1811), сын вице-канцлера графа Андрея Ивановича Остермана, неуклонно следил за строгим соблюдением правил пользования отечественными шифрами, требовал их своевременной замены. При малейшем подозрении о компрометации шифров он давал указания об их досрочной замене или о внесении в них существенных изменений.

Когда стало известно, что один из канцелярских служащих при после России в Гданьске потерял шифр, Остерман сделал послу Волчкову строгое предупреждение: «…признано здесь за нужно подтвердить вам в то же время единожды навсегда, чтоб вы сами впредь хранили в себя цифирные ключи и заочно не выпускали их из рук, в чем и обязываетесь вы вашею присягой верности Ея Императорскому Величеству».

Постепенно установилась иерархия шифров, когда сложные системы использовали лишь для важнейших сообщений, а со снижением их ранга упрощался и шифр. Если разработка собственных шифросистем, в первую очередь для русского алфавита, еще отставала от Европы, то криптоаналитика была на высоте. С этого времени российская криптология окончательно заняла одну из ведущих позиций в европейской криптологии и стала эффективным оружием в руках дипломатических и военных ведомств страны.

1.4. Секретные «экспедиции» МИД

В начале XIX века в России была сделана реорганизация органов управления страной. В 1802 году Манифестом Александра I вместо коллегий были основаны министерства. В частности, было образовано министерство иностранных дел (далее – МИД), канцелярия которого содержала четыре основных экспедиции и три секретные. Первая секретная – шифровальная, вторая – дешифровальная, третья – служба перлюстрации.

До 1808 года начальником первой экспедиции, куда входила «цифирная» часть, был Андрей Андреевич Жерве (1773–1832). Потом он был назначен руководителем Канцелярии, а начальником этой экспедиции стал Христиан Иванович Миллер. Составлением шифров для секретной корреспонденции и дешифровкой иностранных депеш в этот период заведовал Христиан Андреевич Бек (1770–1853). Сохранились некоторые документы, которые позволяют охарактеризовать деятельность секретной экспедиции Канцелярии МИД периода начала XIX века и войны с Наполеоном.

Письмо от 8 марта 1812 года 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».

Х. И. Миллер и А. Ф. Крейдеман являлись составителями не только лексиконов, т. е. словарей к шифрам, но и самих шифров. Эту работу выполняли и некоторые другие сотрудники. После составления шифра специалистом-криптографом в XVIII веке он набело переписывался от руки специальным секретарем в нужном количестве экземпляров. Позже шифры изготовлялись уже типографским способом. В отношении каждого шифра 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 112S страниц российской наборной азбуки и напечатание по 30 р. за страницу, а за все 112S страниц – 3375 р.

за набор 122S страниц французской наборной азбуки и напечатание по 30 р. за страницу, а за все 122S страницы – 3675 р.

Бумаги:
Александрийской 83 л. по 2 р. 50 к. каждая – 207,50
Итого 9222 р. 50 к.

Коллежск. сов. Хр. Миллер».

В начале XIX века в МИД был создан так называемый «Цифирный комитет», в состав которого вошли наиболее опытные и квалифицированные криптологи. В задачи комитета входил анализ и введение новых систем шифров, контроль за их правильным использованием и хранением, вывод из действия устаревших или скомпрометированных шифров, составления выводов, отчетов и докладов для руководителей МИД и императора по вопросам деятельности шифровальной и дешифровальной служб. Этот комитет был подчинен министру, а возглавлял его «главный член цифирного комитета».

Русская дешифровальная служба еще с середины XVIII века вела успешную борьбу с королевской Францией, практически без особых трудностей, «взломав» ее шифры. Подобное состояние дел перекочевало и в XIX век. Русские дешифровщики и здесь поработали хорошо: царь Александр I имел достаточно информации о переписке наполеоновских генералов.

В законе Российской империи об учреждении Военного министерства от 8 февраля 1812 года было предусмотрено создание Особенной канцелярии, специального органа внешней разведки, директором которой был назначен кадровый офицер русской армии флигель-адъютант полковник Алексей Васильевич Воейков (1778–1825). В начале своей военной карьеры он некоторое время был ординарцем полководца Александра Васильевича Суворова.

Сотрудник Особенной канцелярии полковник Александр Иванович Чернышев (1785–1857), использовавший шифр А. В. Суворова, выполнил в Париже значительную работу по розыску данных о состоянии многочисленной армии Наполеона. В результате своей работы ему удалось завербовать одного сотрудника военного министерства Франции, благодаря которому документы, имевшие стратегическое значение для Франции, Наполеон получал одновременно с Александром I.

Как ни странно, но гений Наполеона остался безразличным к секретам криптологии, хотя обычно император пользовался тайнописью. Применял ее и наполеоновский генералитет, который использовал, например, «книжный» шифр.

В 1812 году русские дешифровщики сыграли значительную роль в разгроме армии Наполеона, начавшего войну против России. В ходе военных действий они раскрыли не только самые простые шифры для связи с небольшими подразделениями, но и «Великий» и «Малый» шифры Наполеона. Несмотря на то, что эти шифры были недостаточно стойкими, французы им полностью доверяли в расчете на то, что русские не смогут их раскрыть.

Русские шифры, применявшиеся в то время на военных сетях связи, по сложности были аналогичны французским, однако русское руководство уделяло намного больше внимания их правильному использованию. Значительные усилия были направлены на развитие службы перехвата и дешифровки. Полученная из дешифрованных сообщений информация вовремя передавалась командованию армии и высшему политическому руководству.

Наполеон же находился на захваченной территории и не имел возможности «партизанского» перехвата сообщений русских военачальников. Он не придавал большого значения криптологии и полностью полагался на мощь своей «непобедимой» армии, поэтому не имел дешифровальной службы в своих войсках. Данные по эффективной дешифровке французами русских военных депеш в истории отсутствуют. Таким образом, можно утверждать, что русская криптология победила в войне с французской.

Американский историк Флетчер Пратт привел такую выдержку из разговора, состоявшегося после войны 1812 года между Александром I и командующим одного из корпусов армии Наполеона маршалом Макдональдом: «Конечно, – сказал император России Александр, пыта-

ясь успокоить маршала на счет 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 царь был удивлен. «Отнюдь нет! Я даю вам честное слово, что ничего подобного не имело места. Мы просто дешифровали их».

В 1823 году при МИД был создан «Цифирный» комитет для руководства шифровальной деятельностью министерства. В это научно-производственное подразделение входили квалифицированные специалисты-криптологи, которые работали в различных департаментах министерства. В задачи комитета входило:

1) изучение различных комбинаций шифров и «обеспечение возможно более полной секретности» дипломатической корреспонденции, разработка новых шифров;

2) контроль за введением новых систем шифров;

3) контроль за обеспечением хранения шифров, вывод устаревших шифров;

4) составление заключений, отчетов по вопросам деятельности шифровальной и дешифровальной служб для руководителя министерства и императора.

В 1828 году в МИД был создан Департамент внешних сношений, в состав которого вошли три секретных экспедиции: шифровальная, дешифровальная и перлюстрации, находившиеся в ведении «Цифирного» комитета. Секретными экспедициями в то время заведовали П. Л. Шиллинг (шифры и литография), Х. А. Бек (дешифровка), Н. С. Лаваль (перлюстрация).

В 1846 году название Департамента внешних сношений было заменено новым – Особая канцелярия МИД. Руководители экспедиций были непосредственно подчинены канцлеру (министру внешних сношений) К. Нессельроде наравне с директорами департаментов МИД. В Особой канцелярии была сосредоточена политическая переписка.

В XIX веке продолжалась практика перехвата и дешифровки иностранных сообщений и переписки антигосударственных организаций в самой России. Этим вопросам придавалось огромное значение на высшем государственном уровне. Так, например, Николай I и Александр II охотно читали выдержки из перлюстрированных писем и, используя эту информацию, принимали важные решения.

Русский ЧК, который был сосредоточен в основном в МИД, постоянно совершенствовал методы, технику перехвата и перлюстрации сообщений иностранных государств. На почтамтах Петербурга, Москвы, Варшавы, Одессы, Киева, Харькова, Риги, Вильно (Вильнюс), Томска и Тифлиса были также созданы ЧК – профессиональные службы по перехвату и перлюстрации дипломатической переписки, где разрабатывались методы быстрого копирования, перлюстрации без улик (подделка печатей и т. п.), оперативного ознакомления с содержанием сообщений и их передачи дешифровальным органам.

Большинство сотрудников ЧК были иностранцами, которые получили российское гражданство. В основном это были немцы, которые говорили по-русски с большим акцентом, поскольку с целью собственной безопасности они вели изолированный образ жизни. Для вскрытия писем, как правило, использовался пар или горячая проволока, с помощью которых снималась восковая печать.

Как утверждал бывший сотрудник ЧК Владимир Иванович Кривош, «иностранная дипломатическая переписка попадала в руки русских „специалистов“ практически полностью. В российском „черном кабинете“ имелся полный набор безукоризненно скопированных печатей для зарубежной переписки всех находившихся в Петербурге посольств и консульств… У российского „черного кабинета“ имелись копии многих шифров иностранных государств».

Успехи российского ЧК признавали даже достаточно высокопоставленные деятели заграничных государств. Так, в конце XIX века «железный канцлер» Германии Отто фон Бисмарк обнаруживал особую обеспокоенность на счет сохранности секретных посланий, которые

отправлялись из Петербурга. Он писал: «…немецкий шифр не остается неизвестным российскому императорскому двору; ведь я знал по опыту, что даже в здании нашей миссии в Петербурге сохранить наши тайны мог не искусно сделанный замок, а только частая смена шифра. Я был уверен, что не мог телеграфировать в Ливадию ничего, что не дойдет до сведения императора».

Конец ознакомительного фрагмента.