ШПИОНСКИЙ АРСЕНАЛ
КРИПТОЛОГИЯ И СЕКРЕТНАЯ СВЯЗЬ
СДЕЛАНО В СССР
ВАДИМ ГРЕБЕННИКОВ

Вадим Гребенников

Криптология и секретная связь. Сделано в СССР

«Алгоритм»
2017

УДК 003.26
ББК 32.81

Гребенников В. В.

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

© Гребенников В. В., 2017
© Алгоритм, 2017

Содержание

Предисловие 6
Часть 1. Российская история 10
1.1. Древнерусская тайнопись 10
1.2. «Цифирные азбуки» Петра I 14
1.3. «Черный кабинет» цариц 21
1.4. Секретные «экспедиции» МИД 34
1.5. Таланты Шиллинга 44
1.6. Криптология при Николае II 51
1.7. Перлюстрация и дешифровка 60
1.8. Революционная тайнопись 68
1.9. Военные шифры 83
Конец ознакомительного фрагмента. 86

Вадим Гребенников
Криптология и секретная связь. Сделано в СССР

© Гребенников В.В., 2017
© ООО «ТД Алгоритм», 2017

* * *

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 веч-

ной 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», «Π», «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.* #νάλυσις – 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 поэти-

ческого текста – 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 сообще-

ний 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 зашифровыва-

нию 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 шифросообщению. 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 последовательности 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 Гаврииловича 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 Гаврииловича 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 собственно 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. Долгорукий, 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 – однодва. 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 делу, 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 случае 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 переснимания 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. Каржавин 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 Морениго 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 посто-

ронних 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, пытаясь 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 скопирован-

ных 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».

Сам император Александр II не стеснялся в использовании сведений, полученных в результате дешифровки. Он жаловался Бисмарку, что его, императора, резко критикуют немецкие правители в своих шифрованных посланиях в Россию. Чтение шифропереписки он считал естественным правом самодержца. Здесь нужно отметить, что при использовании сведений, добытых путем дешифровки, стоило обнаруживать особую осторожность, поскольку противник, узнав, что его шифры раскрыты, мог сменить ключ и даже всю шифросистему.

Во второй половине XIX века криптослужба России перестала быть привилегией МИД, поскольку была создана еще в двух ведомствах: военном министерстве и МВД. Этот факт свидетельствовал о росте значения криптологии в деятельности государственных органов, о существенном расширении сфер ее применения.

Развитие внешних и внутренних сетей связи, рост объема шифрованной переписки повлекли за собой увеличение количества действующих шифров и кодов. Появилось достаточно большое разнообразие таких систем. Постепенно выкристаллизовывалась классификация шифров по своему предназначению и цели.

Шифры разделялись прежде всего по языковому принципу. В зависимости от языка шифрованной информации появились русские, французские, немецкие, английские и другие шифры. По отраслевому принципу они делились на шифры МИД, шифры военного ведомства, включая и императорские шифры, шифры жандармерии и созданного в 1880 году в структуре МВД Департамента полиции, а также шифры, которые использовались гражданскими ведомствами для шифрования своей секретной информации (например, министерства финансов). Отдельно выделялись агентурные шифры, которые были предназначены для связи с разведчиками и агентами.

Все шифры делились на секретные и несекретные. Кроме них вводились еще так называемые шифры специального назначения. В одной из инструкций к шифрам МИД говорилось, что несекретными ключами следовало пользоваться во всех тех случаях, когда содержание сообщения само по себе не могло считаться секретным, но когда передача его в незашифрованном виде не представлялась удобной, например, когда желательно было избегать преждевременной огласки таких сообщений в печати и т. п.

Интересное дополнение содержалось в примечаниях к этой инструкции: «Следует полагать, что несекретные ключи известны иностранным правительствам, тем не менее они представляют безусловную тайну для публики и должны храниться если не с секретными ключами, то, во всяком случае, с секретными делами установлений, которые ими снабжены».

Ключи специального назначения использовались для сношений с «различными правительственными установлениями, а также с частными учреждениями и лицами».

Как писал в то время начальник секретной экспедиции МИД Ф. Годениус, в 1862 году было признано необходимым обеспечить русские консульства в Турции русским биграммным шифром. Хотя применение особенностей русского алфавита представляло собой зна-

чительные трудности, экспедиция их преодолела и составленный ею русский биграммный шифр № 334 (в количестве 12 экземпляров) был разослан в консульства. В то же время в эти же консульства были отправлены новые передвижные полоски для русского биклавного шифра № 332 в количестве 90 экземпляров.

Вслед за этим экспедиции был поручен огромный труд, а именно изготовление изобретенного действительным статским советником Г. Гамбургером шифра. После «неусыпных семимесячных трудов» отмеченный шифр был изготовлен и по приказу руководства разослан в 1863 году в главные миссии.

Известно, что в это же время Г. Гамбургером был составлен шифр, получивший название «Chiffre polilexique», на 900 словарных величин. В нем кодовыми обозначениями были трехзначные числа, повторявшиеся 26 раз каждое в зависимости от букв специальных полосок, которые выбирались в особых календарях. Этот шифр был введен в действие в апреле 1862 года и использовался до 1897 года в переписке МИД с посольствами в Европе.

В то же время экспедиция изготовила изобретенный действительным статским советником Румом так называемый «экономический» шифр. Хотя было выдано 30 экземпляров, этот шифр был признан неудобным для применения.

В 1864 году первая «цифирная» экспедиция обеспечила все миссии новым биклавным шифром № 339 для общей связи вместо № 312, находившегося в эксплуатации уже длительное время. Всего было изготовлено 12 экземпляров. Азиатский департамент получил для использования четыре экземпляра русского словарного шифра № 338 для корреспонденции с генерал-губернаторами в Оренбурге и Западной части Восточной Сибири.

В 1865 году были изготовлены и разосланы новые партикулярные биклавные шифры с календарями № 340–345, новый русский биграммный шифр № 347. Кроме того, по требованию министерства финансов туда было выслано 30 экземпляров вновь изготовленного русского словарного шифра № 340.

Следовательно, можно понять, что «цифирная» экспедиция работала активно и напряженно. Однако успех дела зависел от организации деятельности службы в целом, в частности от правильного ведения секретного делопроизводства, соблюдения правил пользования шифрами, условий их хранения. В этих вопросах положение дел оставляло желать лучшего.

Так, например, в 1866 году «цифирная» экспедиция МИД занималась проверкой всех шифров, находившихся в некоторых странах, и всех книг, в которых велись записи о состоянии изготовленных и разосланных экспедицией шифров. При этом было обнаружено, что, с одной стороны, некоторые миссии имели у себя шифры в огромном количестве, из которых многие уже не использовались. С другой стороны, некоторые уже закрытые миссии не вернули шифры, находившиеся у них. Вследствие этого были подготовлены необходимые распоряжения и приняты соответствующие меры по исправлению существующего положения.

В конце XIX века шифровальная служба МИД была организована таким образом. При канцелярии министра функционировал шифровальный департамент с двумя отделениями. В одном отделении шифровались сообщения МИД зарубежным послам и консулам и разбирались получаемые от них сообщения. Во главе этого отделения долгие годы стоял барон Таубе.

Во втором отделении разбирались копии шифротелеграмм, полученных из ЧК Петербурга и других городов Российской империи (Москвы, Варшавы, Киева, Одессы и т. д.), где находились иностранные консулы. Штат этого отделения состоял из 10–12 человек во главе с М. К. Долматовым.

В то время были разработаны также шифры биклавной системы, автором которых был барон Дризен. Эти шифры использовались очень широко в течение XIX века в учреждениях МИД параллельно с биграммными шифрами Шиллинга.

Биклавный шифр был шифром многозначной замены, которая состояла из 26 разных простых замен с достаточно сложным выбором замены каждого знака открытого текста, определяемым двумя ключами. При этом отдельным знакам открытого текста (буквам и знакам препинаний) соответствовали два знака шифротекста. Таким образом длина шифротекста не соответствовала длине открытого текста.

Основу шифра составляли: портфель с 24 передвижными полосками – главная часть двойного ключа, две таблицы (шифровальная и дешифровальная) – вторая часть двойного ключа и календарь набора и разбора.

Каждая полоска была случайным набором с повторениями 20 или менее букв латинского или французского алфавита из 26 букв. Для удобства они записывались группами по четыре буквы в каждой с пропусками. Каждая полоска имела свой номер, обозначенный цифрой или буквой.

Например, полоска «W» имела вид: «qduf kziv akil swkm pzeg».

Шифрующая таблица была квадратом 26 Ч 26, строки которого были обозначены 23 буквами латинского алфавита (без букв k, w, y) и тремя знаками пунктуации, а столбцы были обозначены всеми 26 буквами латинского алфавита. Каждая колонка этой таблицы заполнялась случайным образом 26 знаками, состоявшими из 17 букв латинского алфавита и девяти цифр: 1, 2, 3, 4, 5, 6, 7, 8, 9.

Процесс шифрования осуществлялся таким образом. Открытый текст, предназначенный для шифрования, записывался на транспарант, где каждая строка содержала 24 клетки. Текст писался по четыре знака с пропусками в одну клетку. Таким образом, в каждой строке транспаранта записывалось по 20 знаков, а форма записи отвечала форме шифрованной полоски. Если текст закончился не в конце строки, то добавлялось слово «конец» и еще какие-нибудь произвольные знаки. Каждый транспарант содержал восемь горизонтальных строк.

Таким образом длинное сообщение могло быть записано на нескольких транспарантах. При записи шифротекста на транспарант рекомендовалось сначала выполнить всевозможные сокращения текста, не менявшие смысл сообщения. Далее производилась замена трех букв и некоторых знаков препинаний на знаки, входившие в промежуточный текст, а именно: буква «k» заменялась на «qq», буква «w» заменялась на «vv», буква «y» заменялась на «ii», знак «;» заменялся на «.,» и т. д.

После записи сообщения на транспарант производилось шифрование.

Из 24 полосок в определенном порядке выбирались восемь полосок в соответствии с суточным ключом. Маркантом (специальной меткой или показателем) этого ключа была дата шифрования, которая ставилась в начале сообщения. Первая полоска подставлялась к первой строке сообщения, например, имеем следующий текст и набор знаков на полоске:

uzhg orod and- ukra ine-
W
qduf kziv akil swkm pzeg

Знаки текста с буквами полоски образовывали вертикальные биграммы, которые определяли входы шифровальной таблицы (координаты шифротекста). Например, первая вертикальная пара «uq» определяла знак шифротекста, находившийся на пересечении «u» – строки и «q» – столбца шифровальной таблицы. Таким образом шифровались первые 20 знаков. Следующие 20 знаков шифровались с помощью следующей полоски, определявшейся суточным ключом и т. д. Если шифротекст превышал 20 Ч 8 = 160 знаков, то процедура шифрования повторялась, начиная с первой полоски (в нашем примере «W»).

Дешифровка сообщения производилась в обратном порядке, а открытое сообщение восстанавливалось однозначно при наличии у корреспондента соответствующих ключей.

Таким образом, криптостойкость данного шифра держалась на неизвестном противнику заполнении полосок, определявших выбор последовательности 26 замен, и суточном ключе.

Хотя это число и достаточно большое, однако криптостойкость данной системы шифра ни в коей мере не могла держаться на суточном ключе, поскольку она допускала последовательное опробование полосок шифра одну за другой. Сначала при дешифровке (при известной шифровальной таблице и известных полосках) опробовались одна за другой полоски (24 варианта). Критерием правильности опробования первой полоски было появление открытого (читаемого) текста. Далее опробовалась вторая полоска из числа оставшихся и т. д. Всего выходило $T = (24 + 23 + \ldots + 17) = 164$ элементарных опробования (э. о.). За одно э. о. принималось опробование одного варианта полоски. Если текст шифровался не сначала, а где-то с середины, то число вариантов опробования увеличивалось несущественно: $T = 164 + 10 = 174$ (э. о.).

Содержание полосок, как говорилось выше, было основным ключом. Он действовал значительно дольше, чем суточный ключ, но тем не менее его тоже достаточно часто меняли (полоски менялись обычно дважды в год).

Многие корреспонденты имели разные наборы этих ключей, чем обеспечивалась конфиденциальность переписки и создавалась определенная гарантия от компрометации шифра.

Перешифровальные таблицы, определявшие 26 простых замен, были второй частью ключа. Данный шифр для своего времени можно считать достаточно стойким при сохранении в секрете основного ключа (содержания полосок) и суточного ключа.

Главная слабость этого шифра заключалась в сравнительно коротком периоде T этого шифра (T = 160 букв) и отсутствии разового ключа. Возможно, в те времена за сутки шифровалось не более одного сообщения (в мирных условиях) от конкретного корреспондента, поэтому не было необходимости в введении еще дополнительных разовых ключей. Сами сообщения также не были достаточно длинными, поэтому глубинных перекрытий шифра здесь не ожидалось. Не случайно поэтому шифры этого оригинального типа использовались вместе с биграммными шифрами на протяжении почти сорока лет.

Известны следующие биклавные шифры:

1. Русско-французский ключ № 305. Был изобретен в 1853 году Дризеном и им же напечатан. Предназначался исключительно для переписки миссий в Константинополе с МИД. В 1860 году Дризеном было предложено включить в этот шифр таблицы для шифрования русского текста, а не только французского, как это было сначала. Это предложение было принято «Цифирным» комитетом на заседании 24 марта 1860 года, протокол которого подписали тогдашние члены этого комитета: тайный советник Толстой, тайный советник Гильфердинг, тайный советник Вестман и действительный статский советник барон Дризен. Теперь шифр состоял из двух наборных и разборных таблиц для французского и русского набора. Однако в том же году шифр был выведен из действия.

2. Французский ключ № 306. Был изобретен Дризеном и введен в действие в 1856 году. Предназначался этот шифр для сношений с МИД миссии в Турине (Флоренции). В 1865 году был заменен биклавным ключом № 342, поскольку использовался уже более шести лет. В 1869 году «ввиду устарелой системы» был уничтожен.

3. В 1856 году были введены в действие аналогичные предыдущему и также составленные Дризеном ключи: № 307 – для миссии в Афинах № 308 – для миссии в Стокгольме № 309 – для миссии в Риме № 310 – для миссии в Неаполе и № 311 – для миссии в Мадриде.

4. В том же году был введен в действие французский ключ № 313 для циркулярной связи миссий в Афинах, Берлине, Брюсселе, Константинополе, Копенгагене, Дрездене, Франкфурте, Гамбурге, Ганновере, Лиссабоне, Лондоне, Мадриде, Мюнхене, Неаполе,

Париже, Риме, Стокгольме, Турине, Вене и дипломатической канцелярии в Варшаве. Был сожжен в 1867 году «вследствие устарелости системы».

5. В 1859 году были введены в действие составленные Дризеном русско-французские ключи: № 317 – для переписки МИД с Лондоном; № 318 – с Парижем; № 319 – с Веной; № 320 – с Парижем.

6. В том же году был составлен французский ключ № 322 для переписки князя Горчакова с императором. Однако этот ключ не был своевременно введен в действие и впоследствии, в 1877 году, получил другой номер (364). Им пользовались во время русско-турецкой войны для переписки между главной квартирой Южной армии и МИД.

7. Русский шифр № 322. Был составлен по системе Дризена и введен в действие в 1862 году для переписки МИД с Веной и Константинополем. В 1876 году экземпляры этого шифра были отосланы в Тегеран и Токио, а также великому князю – Главнокомандующему действующей армией в русско-турецкой войне – и генералу Игнатьеву.

8. Французский шифр № 339. Был составлен Дризеном и введен в действие в 1864 году для 28 миссий в Европе и Америке. Использовался в сети общей связи. Кроме корреспондентов МИД экземпляры этого шифра имели в своем распоряжении Походная канцелярия и Императорская главная квартира. Был выведен из действия в конце 1890-х годов «вследствие устарелости системы».

9. Французские шифры № 340–345. Были составлены для телеграфа в 1865 году также Дризеном. Предназначались шифры для сношений в сети общей связи, в которую входили МИД России, а также посольства в Берлине, Вене, Константинополе, Лондоне, Париже, Флоренции. Однако вскоре эти ключи были заменены на более старые ключи той же системы № 305 и № 306.

10. Французский шифр № 348. Был составлен по системе Дризена и введен в действие в 1870 году для миссий в Европе, а с 1871-го по 1882 год использовался также на азиатских линиях связи. Кроме того, экземпляры этого ключа были у министра иностранных дел князя Михаила Горчакова, в Императорской главной квартире, Походной канцелярии, азиатском департаменте МИД, в действующей армии у генерала Игнатьева и барона Фредерикса. На европейских линиях связи этот ключ был выведен из действия лишь в 1891 году.

11. Французские шифры № 350–355. Действовали параллельно с предыдущим ключом на европейских линиях связи. Введены эти ключи в действие были в 1869 году, а выведены из действия лишь в 1891 году.

12. Французский ключ № 357. Был составлен по системе Дризена для телеграфа и введен в действие в 1871 году для переписки МИД с миссией в Вашингтоне. Был сожжен в Вашингтоне в 1884 году.

13. Французский шифр № 364. Был составлен по системе Дризена и введен в действие в 1877 году для переписки с начальником канцелярии при действующей Южной Армии. В 1878 году был отправлен в посольство в Константинополе и в действующую армию барону Фредериксу. Не использовался с 1888 года.

Как видим, биклавные шифры применялись длительное время очень успешно и считались русскими криптологами достаточно надежными. Они были выведены из действия не из-за криптографических изъянов, а по другим причинам. Так, в своем обзоре шифров XIX века Таубе писал в 1901 году: «Система биклавная неприменима в настоящее время ввиду смешанной передачи буквами и цифрами, не допускаемой телеграфными конвенциями». Известно, что некоторое незначительное количество шифров биклавного типа применялись для шифрования секретной почтовой корреспонденции и в начале XX века.

Продолжали активно использоваться в XIX веке также коды и кодовые таблицы. Коды были разных типов, они постепенно видоизменялись и совершенствовались как в эксплуатационном, так и в криптографическом отношении. К концу XIX – началу XX века появи-

лись коды объемом десять тысяч словарных величин и более. До 1917 года наибольшее распространение имели коды именно такого объема.

Большинство кодов России конца XIX – начала XX века были алфавитными, т. е. буквы, слоги, слова, словосочетания кодового словаря располагались в порядке алфавита, а соответствующие им кодовые обозначения представляли собой естественные числовые последовательности. Это обстоятельство в огромной степени облегчило дешифровку, поскольку место каждого кодобозначения определялось местом слова в словаре соответствующего языка эквивалентного объема.

Все эти соображения, естественно, давали возможность опытным криптоаналитикам противника восстанавливать код и дешифровывать сообщение. Применялись и неалфавитные коды, коды пропорциональные и непропорциональные. В зависимости от вида кодобозначений различались цифровые, буквенные и буквенно-цифровые коды. Последние два вида кодов превращались в цифровые, когда сообщения передавались по телеграфу.

С конца XIX века в Европе появились теоретические труды, в которых описывались методы дешифровки алфавитных и неалфавитных кодов. С того времени повсеместно начали использоваться коды с перешифрованием. Перешифрования были разными, от очень наивных, по сути своей чисто маскировочных, до очень сложных. Последние применялись на наиболее важных каналах связи.

Коды и кодовые таблицы интенсивно использовали: МИД, военное ведомство, МВД, министерство финансов и некоторые другие гражданские ведомства. Коды и кодовые таблицы объемом до 1000–1200 словарных величин было принято называть «словарными ключами» и, в зависимости от словаря конкретного кода, называть французскими, русскими, немецкими.

Известны русские словарные ключи XIX века, разработанные бароном Дризеном и другим сотрудником «цифирного» отделения МИД М. Сухотиным:

1. Ключ № 299 на 600 словарных величин. Был введен в действие в апреле 1854 года, а изъят из действия в 1901 году. Предназначался для связи командующих частями Дунайской армии во время Крымской кампании. В 1891 году этим шифром были обеспечены Бухара, Кашгар, Кульджа, Сеул, Пекин, Токио, Иркутск, Омск, Ташкент, Хабаровск, Урга, Чугучак, Владивосток.

2. Ключ № 300 на 600 словарных величин. Был введен в действие в 1855 году, а изъят из действия сразу по окончании Крымской войны в январе 1857 года. Предназначался для главнокомандующего Южной армией и военных и морских сил в Крыму князя Горчакова. В 1860 году этот ключ был отослан в Вашингтон. Не использовался с 1871 года.

3. Ключ № 317 на 1000 словарных величин. Предназначался для секретной переписки по телеграфу и введен в действие в 1859 году. Этим кодом был обеспечен генерал Игнатьев, направленный в Китай, для его переписки с МИД и миссией в Вашингтоне с 25 февраля 1859 года по 11 февраля 1861 года, а также для сношений миссий в Пекине с Вашингтоном и азиатским департаментом МИД. Использовался до 1871 года.

4. Ключ № 326 на 1000 словарных величин. Был введен в действие в 1861 году для переписки МИД с миссиями в Пекине, Урге, Хакодате. Не использовался с 1880 года.

5. Ключ № 330 на 1000 словарных величин. Был введен в действие в 1861 году для переписки Морского министерства с начальником эскадры в Средиземном море. Не использовался с 1888 года.

6. Ключ № 333 на 300 словарных величин. Был введен в действие в 1862 году «для сношений Варшавского военного генерал-губернатора с шестью военными начальниками в Царстве Польском». В 1863 году этот ключ был переделан и напечатан в Варшаве под тем же номером и назван «Шифр Царства Польского. Новый шифр». В свою очередь сам ключ № 333 был переделан из старого ключа № 151.

7. Ключ № 336 на 920 словарных величин. Внешне представлял собой бумажные таблицы, наклеенные на коленкор. Изготовлялся по требованию Морского министерства «для сношений Министерства морского в случае открытых военных действий». Был введен в действие в 1863 году. В 1871 году был послан в Вашингтон, Токио, Пекин, Нагасаки; в 1886 году – в Афины, Фучжоу, Ханькоу, Сеул, Нью-Йорк. Этот ключ был также у военных губернаторов во Владивостоке и Хабаровске. В 1888 году первый экземпляр ключа был украден в Пекине, а в 1891 году – в Вашингтоне. В связи с компрометацией ключа в том же году он был выведен из действия.

8. Ключ № 337. Так же, как и предыдущий, был введен в действие в 1863 году. Сначала служил для переписки наместника на Кавказе с миссиями в Константинополе и Тегеране, потом распространен на консульство в Персии. Был выведен из действия в 1895 году.

9. Ключ № 338 на 900 словарных величин. Был издан в 1864 году. Использовался для переписки азиатского департамента МИД с генерал-губернаторами в Оренбурге, Восточной и Западной Сибири, Туркестане. Не использовался с конца XIX века.

10. Ключ № 346 на 600 словарных величин. Был введен в действие в 1865 году для переписки Министерства финансов с государственными таможнями, Министерством путей сообщения, Государственным контролем. Был выведен из действия в 1867 году в результате утери одного экземпляра.

11. Ключ № 349. Был введен в действие в 1868 году на линиях связи Министерства финансов для телеграфной шифропереписки. Был изъят из действия в 1879 году в результате утери двух экземпляров. В 1901 году снова введен в действие для сношений Министерства финансов с таможнями. Кроме того, этот ключ был введен в действие в 1900 году в Министерстве государственного имущества, в 1902 году – в Порт-Артуре, Харбине, Мукдене. В 1904 году он был отослан в Маньчжурскую армию и действующую армию.

12. Ключ № 368 на 650 словарных величин. Был введен в действие в 1879 году для сношений Министерства финансов с таможнями. Этот ключ также принадлежал к общему типу малых кодов (словарных ключей).

Следует также отметить, что уже в конце XIX века в России были начаты попытки по созданию аппаратов для механического шифрования телеграфных сообщений. Так, в 1879 году главный механик Петербургского телеграфного округа Иван Деревянкин предложил оригинальный прибор по шифрованию телеграмм, который он назвал «Криптограф». Это устройство напоминало известный шифратор эпохи возрождения – диск Альберти. Прибор представлял собой два диска, один из которых был подвижным, однако ни прибор, ни какая-либо информация о нем не сохранились.

1.5. Таланты Шиллинга

Одной из ярких личностей, связанных с российской криптологией начала XIX века, был барон Павел Львович Шиллинг фон Канштадт. Он родился в 1786 году в городе Ревель (ныне – Таллинн, столица Эстонии). Разносторонняя и одаренная личность, полковник российской армии, ученый-востоковед, член-корреспондент Российской Академии наук, изобретатель электромагнитного телеграфа, руководитель «цифирного» отделения МИД – такие наиболее яркие моменты его биографии.

12 июня 1818 года П. Л. Шиллинг был назначен управляющим литографией в МИД. Одновременно он явился инициатором использования этого метода печати для размножения топографических карт и других военных документов. С момента образования в 1823 году «Цифирного» комитета П. Л. Шиллинг стал его членом, работая в «цифирном» отделении, где составлялись шифры. Этим отделением в то время заведовал тайный советник Трефурт. В 1828 году П. Л. Шиллинг назначается на должность начальника «цифирного» отделения.

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

Словарь биграммного шифра содержал двусмысленные буквенные сочетания (французский язык), а кодовыми обозначениями были двух-, трех- или четырехзначные числа, «взятые по два раза каждое для переменной передачи буквенных биграмм то одним, то другим числом». Внешне биграммный шифр был наборно-разборной таблицей, наклеенной на коленкор, при которой имелась инструкция по применению шифра. Буквенные сочетания словаря такого шифра могли быть русскими или французскими, могли быть и двойные русско-французские словари.

Переписка с помощью биграммного шифра, изобретенного П. Л. Шиллингом, велась на французском языке и шифровалась биграммами (двойные сочетания букв и знаков препинаний) французского алфавита. Тип шифра – простая замена, в основном на 992 знака (992 = 32 Ч 31) с пустышками. Важно отметить, что шифровались не идущие подряд биграммы открытого текста, а буквы и знаки, расположенные на длине «Т» периода транспаранта, на котором расписывалось передаваемое сообщение. Биграммы, таким образом, складывались по вертикали из двух строк транспаранта: первая буква – из первой строки, вторая – из второй. Если в конце сообщения не хватало знаков второй строки для образования биграммы, то недостающая часть второй строки заполнялась произвольным образом и шифровались уже отдельные знаки.

Срок действия каждого из таких шифров определялся «Цифирным» комитетом и составлял шесть лет, если в течение этого срока шифр не будет скомпрометирован. Позже в 1858 году этот срок был уменьшен до трех лет. Однако это правило часто нарушалось, что не могло не отразиться на тайне переписки.

Известны некоторые биграммные ключи барона П. Л. Шиллинга. О них есть сведения в «Описи цифирям», составленной Трефуртом, где наряду с данными о других «цифирях», составленных со времени образования «Цифирного» комитета, указывается, что «13 августа 1823 г. от члена оного Комитета Г[осподина] Ст[атского] Сов[етника] Бар[она] Шиллинга фон Канш[тадта] получены его сочинения биграммный ключ № 1 и № 2, № 3 на франц[узском] языке, а также пакет с бумагами, относящимися к составлению этих цифирей».

В феврале 1824 года первый экземпляр биграммного шифра П. Л. Шиллинга был направлен цесаревичу Константину Павловичу; в январе 1826 года тот же первый, а также второй экземпляры были предоставлены князю Меншикову при отправке его в Персию; в 1828 году граф Нессельроде получил третий экземпляр этого шифра при отправке в Америку.

В 1826 году Шиллинг составил шифр для адмирала Синявина. В 1827 году этот экземпляр шифра был передан Нессельроде, в том же году еще три экземпляра этого шифра были направлены в миссию в Вашингтоне. В том же году Шиллинг составил «генеральную цифирь» № 16, «партикулярные цифири» № 4, 5, 6, 8, 9 и 10, а также военный шифр на русском языке № 28.

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

Шиллинг весьма бережно относился к сотрудникам литографии, учитывая важность их работы. Текст одного из его докладов вице-канцлеру Нессельроде свидетельствует: «Литографские ученики Ефимов, Пальцев и Григорьев при хорошем поведении усердным исправлением своей должности, а первый из них сверх того и оказанным искусством в печатании противу своих товарищей, заслуживают внимания начальства, почему долгом поставляю себя испрашивать в Вашего сиятельства в награждение им, первому звание унтер-офицера и 75 рублей, а двум последним по 50 рублей, равно и переплетчику Пазову, занимавшемуся наклейкой цифирных таблиц, 100 рублей».

После смерти Шиллинга в июле 1837 года руководителем первой секретной экспедиции Канцелярии МИД был назначен Артур Миллер. Однако уже через три года его на этом посту заменил действительный статский советник барон Н. Ф. Дризен.

Биграммные шифры Шиллинга в нарушение существующих правил использовались для дипломатической шифропереписки в неизменном виде вплоть до начала XX века, что, естественно, не могло не отразиться на их стойкости. Известны следующие французские биграммные шифры Шиллинга:

1. Телеграфный ключ № 302. Введен в действие в 1856 году, выведен из действия в 1867 году. Использовался «уполномоченным при Парижском конгрессе» бароном Бруновым для сношений с МИД. Выдано было пять экземпляров этого ключа.

2. Ключ № 303. Аналогичен предыдущему. Введен в действие в 1857 году для сношений МИД с миссией в Дармштадте.

3. Ключ № 313. Аналогичен ключу № 302. Введен в действие в 1857 году. Предназначался для консульств на Балканском полуострове (Мостар, Рагуза, Сараево, Белград, Видин, Янина), миссий в Константинополе и Вене, а также использовался для ведения тайной переписки с Азиатским департаментом МИД, Канцелярией и Производной канцелярией. Выведен из действия в 1872 году.

4. Ключи № 314 и № 315. Аналогичны предыдущим. Введены в действие в 1858 году. Ключ № 314 через три года был заменен на биграммный ключ № 328, ключ же № 315 остался в использовании на длительный срок. Использовались для сношений МИД с посольствами и миссиями в Афинах, Берлине, Берне, Бухаресте, Брюсселе, Константинополе, Копенгагене, Дармштадте, Дрездене, Франкфурте, Гамбурге, Ганновере, Гааге, Лиссабоне, Лондоне, Мадриде, Мюнхене, Неаполе, Париже, Риме, Стокгольме, Штутгарте, Турине, Варшаве, Вене, Вашингтоне, Веймаре.

5. Ключ № 316. Введен в действие в 1857 году исключительно для сношений МИД с миссией в Дармштадте. Уничтожен в 1867 году.

6. Ключ № 323. Введен в действие в 1860 году для консульств на Балканах и в Турции (Адрианополь, Битолия, Варна, Белград, Виддин, Вена, Константинополь, Мостар, Рагуза, Сараево, Скутара, Филлипополь, Янина), а также для переписки с МИД генерального консульства в Лондоне. Использовался до начала XX века, когда «Цифирным» комитетом было признано, что и в дальнейшем его можно использовать, но только «для специальной потребности».

7. Ключ № 324. Введен в действие в 1860 году и действовал до начала XX века на линиях связи МИД с Берлином, Константинополем, Лондоном, Парижем, Веной, Бухарестом. Использовался для переписки с генерал-губернатором Одессы.

8. Ключ № 328 был создан как генеральный. Имел словарь меньшего объема, чем вышеперечисленные, – 992 двухбуквенных сочетания. Введен в действие в 1861 году для сношений с МИД и между собой миссий в Афинах, Берлине, Берне, Бухаресте, Брюсселе и других европейских государствах. Выведен в резерв в 1891 году.

9. Ключ № 329. Аналогичен предыдущему. Ключи № 328 и № 329 были введены на замену ключей № 314 и № 315.

В МИД России и других министерствах и ведомствах продолжали активно пользоваться кодами. Коды получили распространение в России с XVIII века и были основным способом шифрования достаточно длительное время. Объем кодов в то время был в пределах от 300 до 1000 словарных величин.

Коды были «привязаны» к словарному языку переписки (дипломатической, военной, торговой и т. д.). При этом наиболее часто употребляемым словам и фразам соответствовало несколько кодобозначений: чем чаще встречался кодовеличина, тем большее количество кодобозначений ей присваивалось. Стойкость такой системы значительно росла за счет «выравнивания» частотной характеристики встречаемости кодобозначений в шифротексте. Таким образом, здесь имело место применение шифра многозначной замены по отношению не к отдельным буквам, а к целым кодовеличинам (словам, фразам и т. п.). В кодах также предусматривались буквенно-составные единицы текста. Характерная черта российских кодов – наличие значительного количества «пустышек».

Коды в основном были алфавитными, а кодовеличины (буквы, слоги, слова, словосочетания) в них располагались по алфавиту. Кодобозначения в основном были цифровыми – от трех до пяти десятичных цифр, расположенных в порядке роста чисел. Практическое удобство такой системы шифрования заключалось в том, что при шифровании и дешифровке применялась одна и та же кодовая книга, в которой и кодовеличины, и кодобозначения располагались в естественном порядке. Однако одновременно это было и слабостью кодирования, поскольку позволяло противнику, узнавшему хотя бы об одном кодобозначении, выдвигать правдоподобные гипотезы о следующих.

Реже применялись неалфавитные коды, а также коды многозначного кодирования. В последнем случае одним кодовеличинам могли соответствовать несколько кодобозначений. Практическое неудобство этих намного более стойких систем заключалось в том, что для повышения оперативности работы шифровальщика были необходимы две книги (кодирование и декодирование), причем в книге декодирования кодобозначения (числа) располагались в порядке их роста, в книге кодирования кодовеличины располагались в лексикографическом порядке, а кодобозначения были произвольными.

Иногда применялось и двойное кодирование разными кодами. При этом первый код не был секретным и использовался для «сжатия» открытого текста (уменьшения его длины), тогда как второй непосредственно обеспечивал его защиту. Достаточно часто кодируемые

тексты дополнительно перешифровывались. Наряду с простыми шифрами (типа простой замены) использовались и достаточно сложные, например «Лямбда».

В 1872 году было введено усовершенствование в структуру биграммных шифров Шиллинга. Разработчик шифров сотрудник шифровального отдела МИД Нелидов предложил существенно уменьшить число букв латинского алфавита и знаков препинаний в открытом тексте с тем, чтобы можно было использовать в качестве шифробозначений латинские биграммы и буквы.

Поэтому французский ключ № 359/360, созданный в 1872 году Нелидовым, получил название биграммно-буквенного. Он содержал биграммные сочетания букв латинского алфавита (кроме k, w, y), знаки препинания (.,-) – 676 величин, а также 26 букв латинского алфавита – всего 702 величины. Шифробозначения – двузначные сочетания из 26 букв латинского алфавита и 26 отдельных букв латинского алфавита, предназначенных для передачи отдельных букв текста. Предназначался он для телеграфа и был введен в действие в 1873 году.

Принцип этой шифросистемы был биграммным с той лишь разницей, что: 1) две буквы текста передавались не тремя числами, как в биграммах, а двумя буквами; 2) при шифровании двухбуквенные сочетания состояли не из букв двух строк переписанного для этой цели по известному транспаранту текста, а из крайних букв каждой строки переписанного по транспаранту текста, двигаясь с двух концов к середине.

Последнее усовершенствование несло и некоторую криптографическую нагрузку. Поскольку на то время стало понятно, что противнику известен принцип шифрования по этой системе, то целесообразно было ввести некоторые изменения в этот принцип, что, конечно, усложняло работу дешифровщиков. Нужно было еще догадаться, в чем заключались эти изменения.

Вторая группа биграммных шифров – это русские биграммные шифры, с помощью которых шифровались сообщения, написанные по-русски. Предназначались они как для внутренней, так и для внешней переписки. Поскольку в русском языке количество биграмм превышало количество трехзначных чисел (вместе со знаками препинаний их было 1296), то разработчики шифров восполняли недостаток чисел шифробозначениями: трехзначных чисел – однозначными, двузначными и четырехзначными.

Известны такие русские биграммные шифры:

1. Ключ № 304. Так называемый «генерал-губернаторский шифр» предназначался «для секретного сообщения из Петербурга с теми из генерал-губернаторов, в местопребывании коих находятся телеграфные станции». Это были такие пункты: Петербург, Москва, Киев, Одесса, Рига, Гельсингфорс, Варшава, Вильно (Вильнюс). Экземпляры этого ключа были у военного министра, министра внутренних дел и шефа жандармов. Шифр был введен в действие в 1857 году. Именно этот ключ был первой попыткой составления русского биграммного шифра.

Впоследствии, когда было введено правило о соединении цифр для передачи по телеграфу сначала в трехзначные, а затем в пятизначные группы, применение этой системы было признано невозможным, и она была заменена сначала сочетаниями из цифр и букв для передачи русских двухбуквенных сочетаний (как, например, в биграммном ключе № 334), а затем уже биграммными ключами, в которых количество букв было сокращено до 28 (ключи № 347, 375, 380, 381 и т. п.). Эти ключи использовались и в начале XX века. Ключ № 304 был выведен из действия (в своем первичном виде) в 1892 году как по указанным причинам, так и в результате потери во время использования большого количества его экземпляров.

2. «Двузначный» ключ № 331. Был составлен по системе биграммных шифров Шиллинга в 1861 году. Этот шифр отличался тем, что не имел двойных чисел в качестве кодобозначений. К 1296 двухбуквенным сочетаниям было добавлено 1296 чисел: 7 однозначных,

75 двузначных, 591 трехзначное и 633 четырехзначных. Использовался этот ключ для шифропереписки между Министерством народного образования и опекунами учебных округов. Выведен из употребления в 1883 году.

3. Ключ № 334. Был составлен Г. Ф. Эстом по системе Шиллинга. Печатал этот шифр, как и другие шифры того времени, Ф. Годениус. Ключ включал 1482 двухбуквенных сочетания. Кодобозначениями служили 1500 трехзначных чисел, из которых 1000 – числа от 000 до 999, 500 – сочетания двузначных чисел с одной из десяти латинских букв, взятых каждая по два раза «для переменной передачи валер [словарных величин]». Шифр этот предназначался для переписки по почте между консульствами в Турции: в Адрианополе, Бейруте, Виталии, Бухаресте, Варне, Виддине, Белграде, Иерусалиме, Коржу, Мостаре, Призряне, Рагузе и др. Выведен из употребления в 1872 году.

Это был первый русский биграммный ключ, в котором двухбуквенные сочетания (словарные величины) передавались при наборе только трехзначными сочетаниями. Но ввиду превышения количества возможных буквенных сочетаний тогдашнего русского алфавита (1396) над количеством трехзначных чисел Г. Ф. Эст, которому была поручена работа над шифром, дополнил недостающие числа сочетаниями из двух цифр и одной из десяти букв французского алфавита. При составлении следующих биграммных шифров для русских текстов уже обошлись без таких сочетаний цифр и букв, поскольку сократили количество двухбуквенных «валер» до 1000, исключив некоторые буквы русского алфавита. Таким образом были составлены, например, ключи № 347, № 356, № 375 и др.

4. Ключ № 347. Введен в действие в 1865 году. Использовался для переписки МИД с консульствами на Балканском полуострове: в Бухаресте, Константинополе, Галаце, Яссах, Измаиле, Тульче, Белграде. В 1871 году был заменен ключом № 356 из-за более чем четырехлетнего применения. Однако в 1903 году этот шифр снова был введен в действие в консульствах Австро-Венгрии, а именно в Будапеште, Сарае, Триесте, Вене и др.

5. Ключ № 356. Введен в действие в 1869 году в консульствах на Востоке, где использовался до 1888 года. Известно, что этот ключ был одним из тех шифров, экземпляры которых были похищены из российской миссии в Пекине 19 августа 1888 года. Вследствие этого он был выведен из употребления, но лишь на некоторое время. Несмотря на очевидность компрометации, в начале 1890-х годов ключ опять ввели в действие, но уже в другом регионе.

В 1894 году ключ № 356 был направлен в Амстердам и Гаагу, в 1896 году – в Берн и Женеву, в 1893 году – в Гаммерфест и Стокгольм. В 1898 году состоялась еще одна компрометация этого шифра: один его экземпляр был утерян начальником адриатической эскадры. Вероятно, именно это событие, наконец, заставило руководителей шифрослужбы окончательно изъять ключ из употребления, как указывалось в соответствующем выводе, «вследствие почти четвертьвекового всемирного использования». Известно, что за весь период применения его использовали в 124 пунктах.

6. Ключ № 361, подобный предыдущему, был составлен Нелидовым в 1876 году. Этот ключ содержал биграммные сочетания из 28 букв упрощенного русского алфавита, знаков препинания и 31 отдельной русской буквы и знака. Всего, таким образом, его словарь содержал 992 величины, которым соответствовали трехзначные кодобозначения. Сначала этот ключ был разослан в консульства на Востоке: в Александрию, Афины, Бухарест, Пекин и др., потом распространен на Австро-Венгрию, Персию, Балканский полуостров и, кроме того, направлен в Тифлис и Одессу.

Во время турецкой войны этот шифр отослали в действующую армию (генералу Игнатьеву, барону Фредериксу, великому князю Михаилу Николаевичу), военному губернатору в Болгарии, адмиралу Лесовскому, контр-адмиралу Крамеру. С 1882 года он использовался в разных консульствах в Европе, а также на международном конгрессе. Несмотря на то, что экземпляр этого шифра был украден в Пекине в 1888 году, его окончательно вывели из упо-

требления лишь в 1903 году. Но и после этого тогдашний начальник шифровального отдела МИД и член «Цифирного» комитета барон Таубе писал: «ключ № 361 может применяться как временный в специальных случаях, кроме Дальнего Востока».

Интересно, что русским криптологам того времени представлялось возможным использовать шифры на линиях связи в каком-то регионе даже в тех случаях, когда они были скомпрометированы в другом регионе. Вероятно, решающим обстоятельством здесь была дальность расстояния. Такое же эйфорическое настроение вселяло в криптологические умы и понятия времени: выведенный из действия в какое-то время шифр, возможно, даже скомпрометированный, мог опять вводиться в действие через значительный промежуток времени. Очевидно, предполагалось, что за давностью времени он будет забыт противником.

Автором французских двухбуквенных ключей № 362 и № 363 также был Нелидов. Разработанные в 1876 году, они были подобны биграммным ключам № 359, № 360 и № 361. Об этих ключах барон Таубе также писал, что их можно использовать и в начале XX века.

Еще одной интересной личностью той эпохи, работавшей в разных российских спецслужбах и занимавшейся криптологией, был Владимир Иванович Кривош. Он родился в 1865 году в Словакии, входившей в состав Австро-Венгерской монархии. По окончании гимназии он владел французским, немецким, венгерским, итальянским, чешским, словацким и хорватским языками. Не являясь по происхождению дворянином, ему удалось поступить в Королевскую Ориентальную (Восточную) Академию в Вене, однако через год, в 1886 году, он был из нее исключен за неуспеваемость. Тем не менее благодаря своим лингвистическим способностям в период учебы в академии В. И. Кривош выучил дополнительно еще английский, сербский, турецкий, арабский и новогреческий языки. В том же году он выехал в Россию и стал слушателем факультета восточных языков Санкт-Петербургского университета.

Одновременно В. И. Кривош вел активную гражданскую, журналистскую и литературную деятельность в разных славянских и словацких обществах Санкт-Петербурга. В 1888 году он получил российское гражданство. Ввиду своего увлечения вышеупомянутой деятельностью и нежеланием «протирать штаны» в университете В. И. Кривош в 1889 году его «бросил», в результате чего высшего образования так и не получил.

В 1891 году он начал работать на Петербургском почтамте, а в 1892 году был назначен переводчиком Санкт-Петербургской почтовой цензуры, т. е. начал заниматься перлюстрацией. Однако спокойная работа на одном месте В. И. Кривоша не устраивала. С 1901 года он начал читать лекции по стенографии в Санкт-Петербургском Технологическом институте (до 1914 года).

С 1904 года В. И. Кривош стал по совместительству работать цензором в Санкт-Петербургском комитете иностранной цензуры (до 1915 года) и переводчиком при Секретном отделении ДП (до 1906 года). С 1906 года он уже заведующий стенографическим бюро Государственной Думы (до 1907 года) и Государственного Совета. С 1907 года – руководитель Секретного бюро Морского генерального штаба и Генерального штаба Военного министерства (до 1911 года).

В начале 1900-х годов В. И. Кривош проявил в области перлюстрации свои творческие способности. Он сделал два изобретения, которыми сотрудники ЧК пользовались в течение десятилетий. Первый заключался в новом способе раскрытия писем с помощью специального аппарата вроде электрочайника. Теперь цензор в левой руке держал конверт над струей пара, а в правой – тонкую иглу, которой осторожно отворачивал клапаны почтового конверта.

Вторым изобретением В. И. Кривош рационализировал технику изготовления состава для поддельных печатей, наносившихся на дипломатическую почту: вместо серебряной амальгамы использовалась медная, более удобная и дешевая. За эти изобретения в 1908 году он получил орден Святого Владимира IV степени и занял должность младшего цензора Санкт-Петербургской цензуры иностранных газет и журналов.

По воспоминаниям самого В. И. Кривоша, благодаря знанию им многих языков его привлекали также к дешифровальной работе в МИД. В 1904 году во время русско-японской войны он был послан в Париж для изучения иностранного опыта по вопросам перлюстрации и раскрытия дипломатических кодов. Французы ввели его «в святая святых» своей тайной полиции «Sыretй Gйnйrale». Там он проработал около десяти дней, пока не был раскрыт четвертый вариант японского кода.

Кроме того, В. И. Кривошу удалось обстоятельно ознакомится с работой парижского ЧК, который, как оказалось, функционировал аналогично петербургскому. Он располагался в частном доме под вывеской какого-то землемерного института. Один из служащих ЧК разбирался в вопросах лесоводства и землеустройства и всегда давал квалифицированную справку частным лицам, интересовавшимся этими вопросами.

Почти все коды французы добывали агентурным путем. Так, они активно использовали для получения криптоматериалов (включая порванные черновики секретных телеграмм, отправлявшихся в зашифрованном виде из этих посольств) подкупленных служащих иностранных посольств. Имели они и некоторые русские коды, что от В. И. Кривоша и не скрывали.

По воспоминаниям В. И. Кривоша, все работники криптослужбы Франции (включая технический персонал: секретарей, машинисток, посыльных и т. п.) должны были быть заинтересованы в своей работе и бояться ее потерять. В секретной части достаточно часто работали жены и сестры служащих. Таким образом, целые семьи сплачивались одной идеей сохранения доверенных им тайн. От этого существенно зависело их семейное материальное благосостояние.

В. И. Кривош стал первым русским криптологом, который получил возможность ознакомиться с работой дешифровальной службы Франции того времени. Полученные им сведения были использованы российскими сотрудниками ЧК в своей практической деятельности.

Вместе с тем с 1910 года русская контрразведка стала подозревать В. И. Кривоша в шпионской деятельности. Кроме того, в то же время его коллеги по службе перлюстрации заподозрили В. И. Кривоша в финансовой небрежности и присвоении казенных денег. В результате в 1911 году он был уволен из Санкт-Петербургской цензуры иностранных газет и журналов, а также из Секретного бюро Морского генерального штаба и Генерального штаба Военного министерства. Как дальше сложилась судьба В. И. Кривоша, будет описано в четвертой части.

1.6. Криптология при Николае II

В период с 1901-го по 1910 год служба перехвата и дешифровки под руководством начальника ЧК МИД Александра Александровича Савинского (1879–1931) получила новый статус, поэтому ее организация значительно улучшилась.

Насколько Николай II интересовался деятельностью ЧК, видно из того, что он однажды собственноручно отобрал три золотых и серебряных портсигара с гербами и бриллиантами в качестве царских подарков и передал их секретному чиновнику для вручения сослуживцам в виде поощрения за полезную деятельность. В этом отношении император Николай II резко отличался от своего отца, императора Александра III. Он, когда ему доложили о «секретной экспедиции» и объяснили ее предназначение, ответил: «Мне это не нужно» и в течение всего своего царствования отказывался читать выписки из перлюстрированных писем, хотя несколько министров делали попытки заинтересовать его этим.

В инструкциях к шифрам МИД неоднократно рекомендовалось применять разные способы повышения стойкости. К этим способам относили: и своевременную смену ключей и кодов, и применение одновременно нескольких кодов в тех местах, где была такая возможность, и применение разного рода приемов типа использования разных вариантов кодообозначений, и, наконец, применение разных способов и систем перешифрования.

Параллельное применение нескольких кодов требовало больших расходов на составление и издание большого их количества и поэтому широкого распространения не получило. В России, как и во многих других странах, применялись разные виды перешифрования кодов: с помощью колонной замены, гаммирования и перестановок. Остановимся на наиболее типичных видах перешифрования.

Все перешифровальные ключи (системы) имели свой порядковый номер и каждому присваивалось наименование по буквам греческого алфавита: Альфа, Бета, Гамма, Дельта, Лямбда и др. Каждое сочетание кодов с перешифрованием перешифровальным ключом также получало свое название. Например, сочетание «Российского консульского ключа № 447» (кода) с перешифрованием перешифровальным ключом № 448 «Лямбда» называлось «Ангарой».

Для одних кодов перешифрование было обязательным, для других – в случаях передачи совершенно секретного сообщения. Разработчики шифров понимали, что коды легко компрометируются (теряют свою стойкость), если содержание зашифрованного с их помощью сообщения становится дословно известным противнику. Поэтому в случаях, если из МИД в какое-либо посольство, консульство или назад передавался какой-то текст, который известен или становился известным, то его необходимо было передавать, в обязательном порядке используя сочетание специальных кодов и перешифрований.

Так, например, в 1916 году для этой цели использовались «Французский общий малый дипломатический ключ № 431» и «Английский малый дипломатический ключ № 407» с обязательным перешифрованием.

Неотъемлемой частью шифров стали лозунги (по современной терминологии – ключи, пароли), меняющиеся в те или другие моменты времени по заранее оговоренным правилам. Лозунгом был более или менее короткий цифровой или буквенный ряд. Ключи были нескольких видов. Одни из них носили название «общих», ими обеспечивались заграничные учреждения определенного региона. Остальные все ключи назывались «специальными». Одни из них предназначались для связи лишь узкого круга корреспондентов или даже для одного посольства с центром (индивидуальные ключи).

При шифровании стандартные словосочетания, включая целые фразы, заменялись условными словами – «постоянными», что делалось для сокращения длины сообщения, и «переменными» – для дополнительного обеспечения секретности.

Рассмотрим некоторые типичные варианты таких шифров.

1. Передвижной условно словарный ключ № 437.

Первое упоминание о нем в документах относится к 1910 году. В «Руководстве» к этому шифру сказано, что он был предназначен для шифрования приведенных в секретных сообщениях выражений общего характера и ссылок, независимо от набора любым секретным ключом (или сочетанием ключей) открытого текста шифрованного сообщения.

Шифр этот состоял из четырех частей. Первая часть была непосредственно кодом (словарным ключом), цифровым, трехзначным, объемом 1000 словарных величин. Вторая часть – перешифровальная – была набором перешифровальных групп. На каждые сутки была своя перешифровальная группа, содержавшая трехзначное число (дополнительный для кода ключ). Под первичным шифрованным текстом, полученным при шифровании по коду, записывалась эта трехзначная перешифровальная группа, и из верхних цифр вычитались нижние по модулю 10. Таким образом, перешифровальная группа была не чем другим, как короткой периодической гаммой с периодом 3.

Третью часть шифра составляла таблица с 1000 передвижных условных выражений (слов), в которой каждое выражение соответствовало трехзначному числу. Таким образом, полученный после перешифрования набор трехзначных чисел заменялся на набор условных выражений. Каждым условным выражением было какое-то латинское слово (или имя собственное, встречавшееся в литературе). Условные латинские выражения располагались в таблице в алфавитном порядке, трехзначные числа – в возрастающем арифметическом порядке, т. е. третью часть шифра можно было назвать обратным алфавитным кодированием. Слово «передвижной» значило, что эта часть должна была со временем меняться и, таким образом, служила секретным ключом шифра.

Четвертую часть шифра составляли 25 таблиц цифровых замен, имевших название «Секунда». В каждой таблице было 20 замен, т. е. всего было 20 Ч 25 = 500 простых замен. Они были предназначены для шифрования чисел в сообщении (дат, ссылок на номер предыдущего или данного сообщения и т. д.). Таким образом, эти числа шифровались не по коду, а с помощью замен «Секунда». Для этого указанные числа открытого сообщения представлялись в виде пятизначных групп с приписыванием слева недостающего до полной пятерки количества нулей.

Далее в начале шифросообщения указывался условный номер выбранной таблицы замены, например, соответствующий первой таблице, и далее производилось шифрование каждой цифры набора пятизначных групп по своей порядковой замене. Первая цифра – первой заменой (столбцом), вторая – второй и т. д. Если количество цифр превышало 20, то следующие цифры после 20 шифровались по второй таблице и т. д.

Таким образом, ключ № 437 был шифром, который можно назвать «код + гамма + обратный код + набор простых замен для шифрования чисел». Методы дешифровки были основаны на использовании цифровой структуры гаммы перешифрования, на ее короткой периодичности и возможности проводить арифметические операции (сложение, вычитание) с цифровыми знаками шифротекста.

Применение в этом ключе обратной операции кодирования практически сводило на нет возможность применения указанных методов дешифровки, по крайней мере до тех пор, пока не удавалось накопить достаточный объем шифроматериала, чтобы с высокой надежностью снять обратный (алфавитный) код.

Что касается применения четвертой части шифра – особого шифрования дат и ссылок, то ее целесообразность можно в какой-то степени объяснить желанием отойти от стандарт-

ного кодирования в сообщении, которое, как известно, служит необходимой помощью для дешифровки кода, особенно в наиболее тяжелый момент начала этой работы. Это объяснение можно подтвердить и тем обстоятельством, что в «Руководстве» рекомендовалось стандартные выражения, входившие в сообщение, не шифровать кодом, а заменять на постоянных условные выражения (в отличие от «передвижных», принимавших участие в третьей части шифрования) и ставить их в начале шифросообщения, отделяя от текста двумя структурными пятизначными группами – группой дня.

В случае передачи сообщения по радиотелеграфу, чтобы весь текст был представлен в виде набора пятизначных цифровых групп, рекомендовалось не применять третью часть шифра – обратное кодирование цифровых групп передвижными условными выражениями. По-видимому, предусматривалось, и не без основания, что и без этого усложнения шифр получался достаточно стойким.

2. Перешифровальный ключ № 448 «Лямбда».

Он предназначался для перешифрования первоначального цифрового шифротекста, полученного при шифровании сообщения с помощью какого-нибудь цифрового кода. Он был шифром колонной замены с периодом десять тысяч суммарных шифров, при этом все подстановки шифра (размера 10 Ч 10) набирались случайно и равновероятно. Все они были напечатаны и сброшюрованы в две книги по 667 страниц каждая. На всех страницах было по 15 вертикальных столбцов, каждый столбец представлял собой лишний ряд подстановки. Все они были пронумерованы цифрами от 1 до 10 тысяч. Кроме того, были пронумерованы все столбцы на каждой странице от 1 до 30 (внутренняя нумерация).

Верхняя строка подстановки менялась и служила одним из ключей. В качестве этой строки выбирался один из столбцов книги. Его порядковый номер указывался «Цифирным» отделением на определенный период и, как правило, менялся дважды в месяц.

Шифровальщик, приступая к работе, выбирал начальный столбец, называемый «исходным» столбцом. Его номер он помещал в криптограмму, предварительно зашифровав с помощью «Особых указательных групп», о которых подробнее будет сказано ниже. Далее он шифровал первоначальный шифротекст, последовательно применяя к каждому знаку текста свою замену. После шифрования заменой с номером 10 000 шифровальщик переходил к столбцу с номером 1 (по циклу).

Для большего удобства пользования такой сложной системой шифра использовался прибор «Скала». Этот деревянный прибор содержал вертикальную целлулоидную ламу с десятью пустыми клетками, размер которых совпадал с длиной шифровальных столбцов в книге. Шифровальщик вписывал в клетки ламы цифры, соответствующие указанному ключу (номеру столбца), и прикладывал прибор последовательно к шифровальным столбцам. Каждый раз выходила подстановка для шифрования.

Номер начального столбца шифровали особо. Для этого шифровальщик три раза подряд выписывал номер начального столбца (3 Ч 4 = 12 цифр) и добавлял дважды записанный номер последнего используемого столбца (с целью, чтобы помочь расшифровать текст при каких-либо сбоях или ошибках). В результате выходил «указательный ряд» из двадцати цифр. Например: 2563 2563 2563 4812 4812. Далее брался столбец, указанный «Цифирным» отделением в качестве ключа (столбец, выписанный на ламе), и столбец, стоявший рядом с ним (10 + 10 = 20 цифрам). Эта последовательность, называвшаяся «календарным» рядом, записывалась под указательной строкой, после чего производилось вычитание по модулю 10. Полученная строка вставлялась в криптограмму в условном месте.

Как видим, данная система перешифрования была значительно сложнее лозунгового гаммирования короткой периодической гаммой и, очевидно, криптографически более стойкой.

Шифром «Лямбда» были обеспечены «центральные и все штатные заграничные учреждения МИД, а равно чиновники МИД при наместнике Е[го] И[мператорского] В[еличества] на Кавказе и начальнике Закаспийской области и чиновники по дипломатической части при Приамурском, Туркестанском и Иркутском генерал-губернаторах». На время войны этим шифром обеспечивалась также дипломатическая канцелярия при штабе Верховного Главнокомандующего.

Во время Первой мировой войны организацией шифросвязи в МИД занимался «Цифирный» комитет. В 1915 году в него входили А. А. Нератов, В. Арцимович, Н. И. Базили, барон К. И. Таубе, Э. Феттерлейн, Ю. А. Колемин, М. Н. Чекмарев, Н. Г. Шиллинг, И. И. Фан-дер-Флит. Члены этого комитета были в курсе всех вопросов, связанных с организацией шифросвязи в России. В частности, члены комитета имели информацию обо всех шифрах, использовавшихся на линиях связи, о действующих системах ключей и т. п.

Война показала, что Россия не смогла предусмотреть опасность затягивания со своевременным введением новых специальных шифров и кодов на военный период по линии МИД. Уже к концу 1914 года стало понятно, что действующие коды не обеспечивали в достаточной мере тайну шифрованной корреспонденции и вместе с тем не позволяли ускорить сам процесс шифрования. Министерством было предложено срочно изготовить для снабжения своих учреждений:

особые словари в десять тысяч знаков, наборных и разборных: дипломатический русский, дипломатический французский, два восточных и консульский;

словарные наборные и разборные таблицы с особыми вертикальными шифрами;

особые ключи для перешифрования.

Однако через два года, осенью 1917-го, в докладе, представленном руководством шифровального отдела Временному правительству, констатировалось, что выполнение этой запланированной в начале 1915 года программы провалилось и пришлось в качестве временных мер вводить более слабые шифры – «трехзначные словари».

5 октября 1917 года руководитель шифровального отделения МИД Юрий Александрович Колемин (1874–1958) подал подготовленную им вместе с его помощником Михаилом Николаевичем Чекмаревым докладную записку на имя министра иностранных дел С. Д. Сазонова. В ней Ю. А. Колемин изложил конкретные предложения по организации корпорации работников криптослужбы, деятельность которой была бы обусловлена соответствующими гарантиями как экономического, так и морального свойства, и, что не менее важно, корпорации, свободной от протекционизма и других изъянов.

Он писал: «Отделение [шифровальное] теперь функционирует. Но я не вижу возможность, чтобы оно оказалось впоследствии жизнеспособным без проведения в жизнь указанных мной принципов, которые, по моему глубокому убеждению, могут быть изменены в частностях, но не по существу». Иначе дело придет «к неминуемому банкротству, последствия которого могут быть для нас бесчисленными».

Необходимость реорганизации деятельности криптослужбы в целом понимали и руководители министерства. Но вопросы пытались решить лишь формально, хотя и был подготовлен проект, в котором была сделана попытка скопировать подобную немецкую специальную службу. В этих условиях и появился документ Ю. А. Колемина.

Деятельность Ю. А. Колемина получила активную поддержку среди служащих шифровального отделения МИД. 8 октября 1917 года состоялось очередное общее собрание служащих шифровального отделения, повестка дня которого, записанная в протоколе, свидетельствовала: «1) выборы двух делегатов на межведомственное совещание для обсуждения проекта Ю. А. Колемина об организации шифровальной службы, 2) выборы пяти лиц в комиссию по организации шифровальной службы, 3) обмен мнениями и текущие дела».

Собрание постановило выразить благодарность от имени всех служащих шифровального отделения Ю. Колемину и М. Чекмареву за их труд по улучшению деятельности отделения и условий службы. 19 октября 1917 года каждый из чиновников шифровального отделения подписал текст присяги, которую составил Ю. А. Колемин для криптологов.

Приведем этот текст:

«Я, нижеподписавшийся (далее следует звание, имя, фамилия и отчество), вступая в исправление моих обязанностей, обещаю, что буду всегда свято и ненарушимо соблюдать перед посторонними лицами молчание о всех материалах, при помощи которых я буду исполнять наложенное на меня ведение секретной переписки Министерства иностранных дел. Обещаю, что буду свято и ненарушимо сохранять в тайне от посторонних лиц все сведения, которые будут проходить через мои руки и перед глазами моими при ведении этой секретной переписки. Обещаю, что буду всегда осторожно, обдуманно и предусмотрительно обходиться с вверенными мне тайными материалами, обещаю, что всегда буду осторожно, обдуманно и предусмотрительно относиться к тем условиям, при которых я могу с сослуживцами по отделению говорить об имеющихся у нас профессиональных сведениях, дабы всеми силами моими содействовать ненарушимости и непроницаемости этих тайн, составляющих собственность немою, а доверяющего их мне Министерства, ведающего при помощи их, через меня, интересами моего Отечества. Обещания сии подкрепляю благородным и честным словом».

Шифры ДП, жандармерии и гражданских ведомств существенно уступали шифрам МИД по своим криптографическим качествам. Так, например, «секретным телеграфным ключом шефа жандармов» 1907 года был набор из 30 простых замен, где буквам открытого текста соответствовали две цифры шифротекста, номер ключа – простой замены – вставлялся в открытом виде в начале сообщения.

При этом адресат, подпись и все числа не шифровались и вставлялись в сообщение в открытом виде, отделяясь от шифробозначений с двух сторон (или с одной стороны – в конце или в начале сообщения) знаками «тире».

Сохранилась даже инструкция к этому жандармскому шифру:

«22 28 37 53 32 65 34 49 39 14 66 18 41 24 67 13 61 26 20 35 30 17 46 36
19 38 42 15 27 31 33 40 21 57 68 50 56 29 64 48 63 47 62 16 54 11 45 23 44 25 52
43 58 10 55 60 59 51 12 ↑ а б в г д е е ж з и к л м н о п р с т у ф х ц ч ш щ ъ ы ю я

[Примечание: буква „е“ фигурирует дважды (она же отвечает за „э“), а весь числовой ряд выписывался в одну равномерную строку.]

1. Составив депешу, необходимо прежде всего в тексте оной подчеркнуть те именно слова, которые, заключая в себе секрет депеши, должны быть зашифрованы. Затем после каждой 12-й буквы шифруемого текста проводится вертикальный штрих.

2. Шифрующий движением азбуки ставит стрелку против желаемого нумера, под которым зашифровывает депешу к передаче телеграфом. Нумер этот состоит из двух букв и пишется в начале каждых 12 букв шифруемого текста.

3. Депеша набирается так. Для составления слов берутся буквы, а к передаче телеграфом пишутся находящиеся под оными цифры, так что каждые две цифры выражают одну букву.

4. По шифровании первых 12 букв стрелка передвигается против другого любого нумера (но только не соседнего) который прописывается и под которым продолжается шифрование следующей группы 12 букв. Затем снова передвигают стрелку произвольно (избегая, впрочем, возвращения в одной и той же депеше к употребленному уже в ней №) и т. д. до конца депеши.

5. Адрес депеши, подпись и цифры в тексте не зашифровываются, а пишутся просто, но при переходе от шифра к цифрам ставится тире, затем каждое произвольное число отделяется точкою или союзом, напр. 6.15 и 350.

6. Разбор депеши. Получивши таковую с телеграфа, разделяют шифрованные цифры запятыми на группы от левой руки к правой попарно и за каждой 13-й парой проводят вертикальный штрих. Потом движением азбуки ставят стрелку против первой пары, т. е. на №, под которым первые 12 букв депеши зашифрованы, а со 2-й пары приискивают цифры впредь до штриха, за сим ставят стрелку на нумер, следующий после штриха, приискивая под ним цифры до следующего штриха и т. д. Затем составляют содержание депеши из букв, под оными находящихся.

7. Секрет этого ключа недоступен, потому что в нем цифры составлены в произвольном порядке и кроме того имеют еще 29 изменений периодически обязательных….

8. В каком именно виде депеши пересылаются:

Саратов. Начальнику Губернского жандармского управления.

Прошу выслать 46382523471925 прежний 63275748273 915465620611446241438174226271515563631361768204405340246713211533, замененный 61262021 новым – 8.57414213243162 – 1871.61152624. Граф Шувалов.

9. Разбор депеши: Саратов. Начальнику Губернского жандармского управления. Прошу выслать в штаб прежний секретный жандармский телеграфный ключ, замененный мною новым, – 8 января 1871 года. Граф Шувалов».

Другой жандармский шифр – это алфавитный цифровой код на 110 величин, одно- и двузначный, с сдвигом, т. е. первые словарные величины (агитатор, администрация фабрики, арестовать и т. д.) имеют соответственно кодовые обозначения: 87, 88, 89 и далее по циклу.

Естественно, очень характерным было лексическое наполнение словарей подобных шифров: беспорядок, бить, буйство, вести себя вызывающе, вина администрации фабрики, вина рабочих, возбуждение дела о забастовке, драка, забастовка, зачинщик, казаки, сжечь, социалистический и т. д.

Среди множества шифров России агентурные шифры всегда занимали особое положение. В соответствии с названием, они предназначались для связи разведчиков и агентов с центром. К сожалению, к настоящему времени сохранилось очень мало сведений об этих шифрах. По инструкции они должны были уничтожаться, как только потребность в них отпадала, и эти правила неуклонно выдерживались. Однако удалось найти некоторые материалы, позволяющие остановиться подробнее на этом вопросе.

Одним из основных требований, предъявляемых к агентурным шифрам, является обеспечение максимально возможной безопасности их пользователю. Поэтому вся документация к шифру (ключи, правила пользования) должна была обладать свойством «скрываемости» или же, в идеале, свойством «безуликовости». Кроме того, сам процесс шифрования должен был быть максимально простым и быстрым, даже если его приходилось осуществлять в самых благоприятных условиях. Эти требования часто входили в противоречие с требованиями высокой криптографической стойкости, и в этих условиях криптографы обычно выбирали какую-то золотую середину. Рассмотрим некоторые виды таких шифров, применявшихся в России в интересующую нас эпоху.

Простыми агентурными шифрами в данный период были также шифры простой замены, в которых используемые простые замены были достаточно структурными и поэтому легко запоминались. Таким образом, это были самые старые «безуликовые» шифры «на память», аналогичные шифру Цезаря с небольшими изменениями: сдвиг шифроалфавита на два, три, четыре и более знаков, замена каждой буквы алфавита следующей по алфавиту буквой, использование лозунга. Обычно ключ определялся датой шифрования сообщения. Очевидно, что эти шифры легко поддавались дешифровке уже в то время.

Более сложным шифром был шифр многозначной замены, получивший название «Прыгающий шифр». Он появился в конце XIX века и криптографически являлся несколькими простыми заменами, которыми агент должен был пользоваться при шифровании сообщения, переходя от одной замены к другой через каждых пять-семь или девять знаков текста. Этот шифр был в действии непродолжительное время, поскольку для агентов он был очень сложен, и они отдавали преимущество шифру Цезаря с часто меняющимися ключами.

В качестве агентурных шифров использовались и книжные шифры. Выбиралась определенная книга, в качестве шифробозначений использовались номера страниц, строк, мест в строках, где находились шифрованные буквы. Этот тип шифра также можно отнести к «безуликовым» шифрам, естественно, при аккуратном пользовании книгой. Книжные шифры обладали несравненно большей криптографической стойкостью по сравнению с шифрами замены.

Однако в ЧК, где дешифровывали такие шифры, было замечено, что шифрознаки, соответствующие большим номерам строк или мест в строке, обозначали, как правило, редко встречающиеся знаки открытого текста. Это была зацепка для раскрытия сообщения и поиска соответствующей книги. Дело в том, что, как правило, каждый корреспондент считает лучшим находить в книге буквы, стоящие неподалеку от начала строки или начала страницы. В противном случае подсчет занимает много времени, и при этом увеличивается достоверность появления ошибки. Редко встречающиеся буквы по необходимости могут оказаться где-то далеко от начала страницы или строки.

Однако, поскольку книга обеспечивала дешифровку всего сообщения, всегда пытались найти используемую книгу. Не случайно при аресте и обыске лиц, подозреваемых в шпионаже, в первую очередь обращали внимание на их библиотеки. Отметим, что книжные шифры широко применялись в России в деятельности нелегальных партий и групп, о чем подробнее будет рассказано ниже.

В начале XX века получили большое распространение в качестве агентурных шифров разные виды шифров перестановок: от старых шифров типа трафарета Кардано до новых шифров типа простых вертикальных перестановок, шахматных и произвольных лабиринтов, прямоугольных и прямолинейных решеток и двойных перестановок.

В шифры перестановок вносились различные усложнения, такие как спиральная выписка, выписка по диагоналям, выписка по лозунгу и распределителю, использование фигурных вертикальных перестановок (со столбцами разной длины).

Как агентурные в России часто использовались шифры вертикальной перестановки с усложнениями. Текст сообщения записывался в таблицу по строкам. Порядок следования столбцов определялся ключом, который пользователи знали на память. Этот ключ должен был меняться достаточно часто (например, не реже, чем один раз в два месяца).

Главное преимущество заключалось в том, что для их использования не нужно было наличия в письменном виде оформленных ключей, которые бы могли скомпрометировать агента. Ключ (лозунг) легко запоминался, а сам алгоритм шифрования был очень простым и доступным для понимания любому агенту.

Приведем упрощенный пример шифра вертикальной перестановки. В качестве секретного ключа используем слово «УЖГОРОД», буквы которого нумеруются по алфавиту (при этом, если буква встречается несколько раз, номера ей присваиваются последовательно):

У	Ж	Г	О	Р	О	Д
7	3	1	4	6	5	2

Эта числовая последовательность является так называемой номерной строкой. Зашифруем фразу: «Информируй о своем плане». При шифровании выписывается номерная строка, а под ним сообщение по строкам:

7	3	1	4	6	5	2
И	Н	Ф	О	Р	М	И
Р	У	Й	О	С	В	О
Е	М	П	Л	А	Н	Е

Шифрование осуществляется выписыванием текста по столбцам по порядку чисел. В первом столбце стоят буквы «ФЙП», во втором – «ИОЕ» и т. д. В результате получим следующий шифротекст: ФЙПИОЕНУМООЛМВНРСАИРЕ.

Дешифровка производилась таким способом. В шифротексте содержится 21 буква, а длина лозунга – 7, следовательно, при шифровании использовалась такая конфигурация:

1	2	3	4	5	6	7

В эту конфигурацию вписывалась номерная строка ключа, после чего по столбцам по порядку вписывался шифротекст:

7	3	1	4	6	5	2
		Ф				И
		Й				О
		П				Е

Таким образом получалось исходное сообщение.

Последующее развитие этого способа шифрования заключалось в использовании двойной вертикальной перестановки: полученный первичный шифротекст опять шифровался по тому же правилу, но другим ключом.

В 1916 году подпоручиком Вави Попазовым было изготовлено шифровальное устройство, впоследствии названное «Прибор Вави». Устройство по своей идее было аналогично цилиндру Джефферсона, но вместо дисков на оси было 20 колец, натянутых на цилиндр впритык друг к другу, которые могли на нем вращаться. На ребрах (цилиндровых поверхностях) колец были нанесены смешанные алфавиты (30 букв), а на первом и последнем кольцах были нанесены по порядку цифры от 1 до 30. При заданном расположении колец на цилиндре ключом шифра являлись: цифра, например 5, и буква, например Б, а также «ключ шага» – две буквы, например, АГ. Сообщение разделялось на части по 17 букв.

Для шифрования фразы «Информируем о плане» на первом кольце отыскивалась ключевая цифра 5. Напротив этой цифры поворотом второго кольца устанавливалась ключевая буква «Б». Потом напротив их поворотами других колец устанавливалась фраза из 17 букв. Эта часть текста заменялась на другие буквы из параллельных строк ключа шага «АГ». «А» – строка, соответствующая букве «А» на втором кольце. Вторая аналогичная строка начиналась с буквы «Г» второго кольца. Буква «И» заменялась буквой «Ж» третьего кольца строки «А», «Н» – буквой «Е» четвертого кольца строки «Г» и т. д. Таким способом зашифрованные буквы брались по очереди, то из строки «А», то из строки «Г».

5	Б	И	Н	Ф	О	Р	М	И	Р	У	Е	М	О	П	Л	А	Н	Е	**5**
6	Я	И	А	Ж	С	Р	Е	П	В	В	Р	О	Б	А	И	В	Ф	Ш	**6**
7	Л	И	Б	Р	Л	О	Д	Ф	Ч	К	Б	Л	Т	Б	Х	Е	Д	Ч	**7**
8	А	Ж	Я	В	А	В	Л	О	Б	Г	Т	К	А	Ф	Н	Ч	Ш	И	**8**
9	Г	Т	Е	А	Ф	Ж	Ю	Д	Ш	Р	О	Ж	И	Т	Д	Х	Г	Ю	**9**

Шифротекст имел вид: ЖЕВФВЮОШГОКИФДЧГИ.

Заметим, что принципиальное отличие системы Попазова от шифра Джефферсона заключалось в единственности выбора шифротекста (по шагу ключа). Однако прибор не нашел широкого применения, потому что преимущество в то время отдавалось ручным шифрам.

1.7. Перлюстрация и дешифровка

С 1870 года официальной «крышей» службы перлюстрации стала Цензура иностранных газет и журналов при крупных почтамтах. С 1881 года в связи с переходом почтового ведомства в состав Министерства внутренних дел (далее – МВД) русский ЧК окончательно уже в 1917 году был подчинен министру внутренних дел. В течение многих лет им руководил непосредственно почт-директор Санкт-Петербургского почтамта. В 1886 году управление перлюстрацией на территории всей империи было впервые возложено на старшего цензора Цензуры иностранных газет и журналов при Санкт-Петербургском почтамте Карла Карловича Вейсмана (1837–1912).

В начале XX века в стране работало восемь перлюстрационных пунктов (далее – ПП) в таких городах: Санкт-Петербург, Москва, Варшава, Казань, Киев, Одесса, Харьков и Тифлис. Позже такие пункты открылись в Вильно, Риге, Томске и Нижнем Новгороде. Однако последние функционировали недолго. В Тифлисе ПП действовал с перерывом с 1905 года по 1909 год, поскольку был разгромлен во время революционных событий 1905 года.

Эти ПП создавались на почтамтах при отделах цензуры иностранных газет и журналов. Официально они назывались «Секретными отделениями». Общее руководство всей перлюстрацией в России возлагалось на старшего цензора Санкт-Петербургского почтамта, который был наделен правами помощника начальника Главного управления почты и телеграфа и в то же время находился в подчинении министра внутренних дел, от которого получал распоряжение и санкции на проведение перлюстрации.

Более тридцати лет, до увольнения в отставку в 1914 году, эту должность занимал действительный тайный советник Александр Дмитриевич Фомин (1845–1917), потом до октября 1917 года – тайный советник Михаил Григорьевич Мардарьев. Перлюстрированные материалы из секретных отделений направлялись в ДП для дешифровки и последующего применения. Старший цензор переписывался с ДП под псевдонимом. Письма, посылаемые на имя «его превосходительства С. В. Соколова», предназначались для отдела цензуры.

Особо тщательным образом подбирались сотрудники ЧК. Как правило, это были всесторонне проверенные люди, «безоговорочно преданные престолу» и давшие подписку о неразглашении тайны. Среди сотрудников ПП в Санкт-Петербурге, кроме цензуры, были люди, служившие в других учреждениях: МИД, банках, университете и т. д., т. е. сохранялась традиция, заведенная еще в середине XVIII века.

Непосредственно перлюстрацией по всей России до 1913 года занималось всего 45 человек, которым помогали отбиравшие письма работники почты. В города, где ПП отсутствовали, в случае необходимости отправлялись чиновники из центрального пункта в Санкт-Петербурге. Но чаще губернские жандармские управления привлекали к этой работе узкий круг местных почтовых чиновников и проводили перлюстрацию сами.

Работа в ЧК была организована таким образом. Письма для вскрытия отбирались по двум спискам. Первый список Особого отдела ДП содержал фамилии лиц, письма которых подлежали просмотру, и адреса, посланные по которым письма подлежали перлюстрации. Также должны были перлюстрироваться письма, освещавшие деятельность съездов, партийных конференций противоправительственных организаций и содержавшие материалы об их подготовке, проведении, деятельности основного партийного состава и членов разных организаций. Второй список составлялся МВД и предписывал перлюстрацию писем общественных и политических деятелей, редакторов газет и журналов, профессоров, членов Государственного совета и Государственной думы, членов царской семьи.

Не подлежали перлюстрации письма только самого министра внутренних дел и царя. В материалах чрезвычайной следственной комиссии Временного правительства, разбирав-

шей в 1917 году вопрос о перлюстрации, имелись данные о том, что в 1910 году командир Отдельного корпуса жандармов П. Г. Курлов обратился к старшему цензору с просьбой, чтобы адресованные ему письма не носили явных следов вскрытия. Такая же просьба высказывалась и сторонником перлюстрации директором ДП С. П. Белецким.

Наибольший поток писем шел через Петербургский почтамт. Ежедневно здесь вскрывалось от двух до трех тысяч писем. Конверты вскрывались особыми косточками или длинными иглами, отпаривались паром, отмачивались в ванночках. Письма с «интересными» сведениями откладывались для снятия копий. Просмотренные письма запечатывались, на обратной стороне в одном из уголков ставилась точка (мушка) – условный знак того, что письмо уже просмотрено и не должно подвергаться перлюстрации повторно.

В ЧК письма задерживались недолго – всего час или два. Лишь в тех случаях, когда их текст был написан симпатическими чернилами или зашифрован, их в оригинале отправляли в ДП, где и подвергали соответствующей обработке. Копии и выписки из писем делали в двух экземплярах. Один экземпляр по списку ДП отправляли директору этого департамента, а второй (и оба экземпляра по списку МВД) шел министру внутренних дел. На местах, в других городах, перлюстрировалась только та корреспонденция, которая шла из этого города или в город, но не транзитная. Копии также делались в двух экземплярах, один из которых направлялся в Санкт-Петербург на имя С. В. Соколова.

Начальник ЧК при Киевском округе связи действительный тайный советник Карл Фердинанд Зиверт изобрел устройство, полностью исключавшее возможность случайной поломки или обгорания печати, которые свидетельствовали бы о вскрытии конверта. Это устройство представляло собой тонкую круглую отполированную палочку размером с вязальную спицу, расщепленную приблизительно до половины. К. Зиверт вводил палочку под клапан конверта, разрезом захватывал письмо, наматывал его на палочку и вытягивал из конверта, не оставляя после себя каких-либо видимых повреждений.

К. Зиверт свыше сорока лет служил в Киеве тайным цензором почты под эгидой царского МВД. В результате он имел возможность вскрывать корреспонденцию, адресованную начальнику русского генерального штаба генералу Михаилу Алексееву, читать письма госпожи Брусиловой жене другого генерала, командующего Киевским военным округом. Он осмеливался даже перлюстрировать официальную переписку военного министра Сухомлинова и графа Бобринского, русского губернатора оккупированной австрийской территории в Галиции.

Печально, что К. Зиверт оказался австро-германским шпионом. Он добрался до самых вершин киевского отдела почтового шпионажа благодаря долгому и умелому шпионажу за высокопоставленными русскими по поручению и в интересах других высокопоставленных русских. От почтового шпионажа не были защищены даже члены императорской семьи – династии Романовых.

Во время Первой мировой войны шпионы, работавшие в ЧК, были разоблачены и арестованы. Главным из них оказался К. Зиверт, проработавший в почтовой цензуре почти пять десятилетий. Он с одинаковым рвением работал одновременно на двух и более хозяев и вообще обнаружил поразительное «беспристрастие» ко всем политическим лагерям в России. Три его главных помощника – Макс Шульц, Эдуард Хардак и Конрад Гузандер – по рождению были немцами, но долго жили в России.

К. Зиверт и его сообщники были осуждены. Военные секреты России, связанные с Киевским округом, он сообщал в Вену еще до начала войны. На суде К. Зиверт признал, что все приспособления, которыми он пользовался при вскрытии писем и для шпионской работы, равно как и фотографические аппараты, которыми пользовались русские цензоры, были немецкими.

По данным ДП, ежегодно по всей стране поддавалось перлюстрации приблизительно 380 тысяч писем, из которых делалось от восьми до десяти тысяч выписок. По более точным подсчетам, в течение 1907–1914 годов наибольшее количество выписок было в 1907 году (11 522), а затем уменьшилось до 7935 в 1910 году. В 1911 году поток опять вырос до 8658, а в 1912 году – до десяти тысяч. Одновременно выросло количество шифрованных писем и писем, написанных химическими чернилами.

Кроме того, шифрами в своей переписке пользовались и члены революционных организаций. Поэтому в число задач, стоявших перед агентами ДП, входила добыча революционных шифров и ключей к ним. Вот выдержка из доклада директору ДП, представленного начальником отделения «по охране общественной безопасности и порядка» в Петербурге 12 ноября 1903 года:

«Вся конспиративная переписка партии эсеров шифруется при помощи известного календаря Гатцука, издаваемого в Киеве… Ключом к переписке с Москвой и Харьковом служит имя „Николай“, с Екатеринославом – „Огюст Кант“, а заграничная переписка шифруется по 8-й книге за август сего года журнала „Мир Божий“. Второму отделению при дешифровании заграничной переписки следует к проставленной на письме дате прибавить число 13, то есть разницу между старым и новым стилем, и полученное число укажет ту страницу в указанной книге, с которой начата шифровка».

Рост революционного движения, постоянно растущий объем перехваченной конспиративной переписки революционеров, важность ее дешифровки для ускорения их розыска и ареста – все это заставило создать криптослужбу при самом Департаменте полиции (далее – ДП).

В 1893 году ДП издал для внутреннего пользования учебник по графологии и криптографии, написанный действительным статским советником Степаном Николаевичем Мардарием. Он был начальником специального департамента корпуса жандармов. В задачу этого подразделения входило создание сети лабораторий по перлюстрации и графологической экспертизе всей подозрительной корреспонденции. В губернских почтовых отделениях и на таможнях появились чиновники, проверявшие письма и всю печатную продукцию.

1 января 1898 года в структуре ДП начал свою деятельность Особый отдел, где был сосредоточен весь политический розыск и преследование революционеров. Его специальное отделение целеустремленно стало заниматься изучениям перехваченных шифрованных писем революционного подполья.

Некоторые сведения о шифрах революционеров, добытых агентурным путем, дают журналы входных документов ДП за 1906–1908 и 1909–1915 годы. Так, например, в 1906 году ДП была агентурным путем получена и дешифрована шифропереписка известных меньшевиков Степана Цосаря, Петра Кирноса, Леонида Комендантова, М. Мандельштама. Из Донского охранного отделения сюда же прислали ключ к шифропереписке комитетов Российской социал-демократической революционной партии (большевиков) (далее – РСДРП(б)) с Центральным комитетом (далее – ЦК), а также ключ к шифру большевика М. Покровского.

В 1907 году ДП получил и дешифровал переписку большевика Николая Буренина, получил ключ к шифру ЦК РСДРП(б) для переписки с Киевской организацией, ключи к шифрам социал-демократов Южного района.

В 1908 году по агентурному доносу был захвачен шифрованный архив Московской военной организации РСДРП(б). Но в журналах есть запись: «Разобрать невозможно». Однако известно, что всего за три года до этого при разгроме полицией редакции газеты «Новая жизнь» в числе других документов была захвачена записная книжка с шифрованными записями, которые были дешифрованы легко и быстро.

В том же 1908 году одесское охранное отделение прислало в ДП ключ к шифру ЦК РСДРП(б), были также получены шифры «Рабочая азбука», «Бородино», ключи к шифрам местных организаций РСДРП(б), например, Полтавской и т. п.

В 1909 году с помощью агентуры ДП получил ключ к шифру политических арестованных, содержавшихся в кутаисской тюрьме, получил и дешифровал переписку известного большевика-химика Александра Чесского из Самары, из Харькова получил ключ к шифру «Грунке», которым пользовались организации РСДРП. Из Екатеринославского охранного отделения сообщили ключ к шифру РСДРП(б) (книжка «Смерть» № 70), из Иркутска поступил ключ к шифрам арестантов тюремного замка Иркутска. Начальник одесского охранного отделения со сводкой агентурных сведений по городу Керчи сообщил ключ к шифру социал-демократического подполья (сборник «Знания» № 17).

Московскому охранному отделению удалось получить ключ к шифру ЦК РСДРП(б) для переписки с Петербургским комитетом. Начальник губернского жандармского управления Самары сообщил ключ к шифру, использовавшемуся в переписке саратовской и уральской социал-демократических организаций. В этом же году ДП получил ключи к шифрам переписки крымской организации с ЦК РСДРП(б), ключи к шифрам пермской организации РСДРП, ключи шифропереписки Московского комитета с ЦК РСДРП(б).

В 1911 году ДП получил и дешифровал переписку Якова Свердлова и его жены К. Новгородцевой, секретаря ЦК РСДРП(б) Н. Агаджановой, агента ЦК по центральному промышленному району В. Яковлевой, а также В. Куйбышева и Р. Пятакова. Были также получены ключи к шифрам социал-демократии Латышского края, шифр для переписки В. Ленина с В. Бажановым, Е. Розмирович, копии шифров Н. Крупской, Р. Петровского и т. д.

В ДП, куда поступали материалы из ЧК и иногда от министра внутренних дел, шла дальнейшая «разработка» перлюстрации: регистрация, дешифровка, проявление химических текстов, копирование и размножение копий. На основании полученных сведений велась переписка с губернскими жандармскими управлениями, выяснялись личности писавших, адреса, «принимались меры». Каждое перехваченное письмо получало свой номер. Простые и «химические» письма регистрировались отдельно: первые просто получали номер, к химическим добавлялась буква «Х».

Фамилии, упоминавшиеся в письмах, вносились в картотечный алфавит. Именные карточки составлялись на автора письма, получателя, на все имена и фамилии, упоминавшиеся в письме. Так детально расписывались только письма революционеров. Письма государственных и общественных деятелей редко проходили такую обработку. Они, как правило, не регистрировались и подшивались в отдельные дела в хронологическом порядке.

В ДП вся перлюстрация сосредоточилась в Пятом отделении Особого отдела ДП, где шла разработка партийных материалов. Копии писем, касавшихся деятельности партии эсеров, анархистов, террористических организаций, поступали во Второе отделение Особого отдела, занимавшееся этими партиями. Материалы по социал-демократическим организациям поступали в Третье отделение, а по национальным организациям – в Четвертое. Здесь же шла последующая разработка этой переписки, но уже розыскного характера, на основании сведений, полученных из писем. Это была кропотливая и сложная работа, которая требовала глубокого знания революционного подполья.

Копии писем посылались в соответствующие охранные отделения и губернские жандармские управления для выявления лиц, принятия мер и установления наблюдения. Эти, уже вторичные копии вместе с материалами по разработке и переписке с соответствующими губернскими жандармскими управлениями группировались в делах по наблюдению за партиями, организациями, отдельными личностями. По социал-демократическому движению эти документы концентрировались в делах по наблюдению за РСДРП.

Прочтением тайнописной и шифрованной переписки революционных партий и групп занимались специальные сотрудники Особого отдела ДП, в частности его Второго и Пятого отделений. Среди них в первую очередь следует отметить, безусловно, выдающегося криптолога Ивана Александровича Зыбина. Родился он в 1865 году и в августе 1887 года в качестве рядового чиновника был принят на службу в ДП. Имея за плечами лишь курс Санкт-Петербургской классической гимназии, благодаря своему исключительному таланту и трудолюбию Зыбин еще к моменту создания Особого Отдела стал ведущим криптологом ДП. В его документах (1902) он именовался «старшим помощником делопроизводителя».

К концу своей службы в ДП (1916) Зыбин официально стал именоваться «делопроизводителем». Работая в сфере дешифровки переписки революционного подполья, Зыбин, естественно, накопил огромный теоретический и практический опыт. Кроме того, будучи от природы высокоодаренной личностью, имея замечательную память, Зыбин был высокообразованным человеком, что позволяло ему получать сведения о шифрах не чисто научно-аналитическим способом, но и с помощью косвенных сведений.

Первое литературное упоминание о Зыбине мы находим в записках о деятельности ЧК бывшего сотрудника ДП Михаила Бакая: «Если встречались письма с шифром, то они расшифровывались специалистом этого дела чиновником Департамента полиции И. А. Зыбиным, который в дешифровке дошел до виртуозности, и только в редких случаях ему не удавалось этого сделать. Зыбин считается единственным своего рода специалистом в этой области, и он даже читает лекции о шифровке и дешифровке на курсах для офицеров, поступающих в отдельный корпус жандармов…

Для Зыбина важно уловить систему ключа, тогда для него не составляет труда подобрать соответствующее значение для букв или цифр… Пользуясь случаем, я обратился к Зыбину с просьбой ознакомить меня со способом разбора шифров и на это получил указание, что письмо с шифрами заранее известных ключей дешифруется очень легко, при этом он мне указал на некоторые ключи революционных организаций, полученные при посредстве провокаторов».

Другой крупный жандарм, глава московского охранного отделения генерал Заварзин в своих заграничных мемуарах вспоминал Зыбина еще более красноречиво: «Простые шифры он разбирал с первого взгляда, зато более сложные приводили его в состояние, подобное аффекту, которое длилось, пока ему не удавалось расшифровать документ».

В 1903 году в ДП разработкой химических и шифрованных документов занималось четыре человека. Один из работников – Владимиров – занимался разбором и переводом химических писем, прокламаций и т. п., написанных на еврейском языке. В. Н. Зверев, ротмистр Мец и И. А. Зыбин вели журналы входящих и исходящих документов, доставляемых цензурой, пополняли алфавит лиц и адресов, упоминаемых в переписке, проявляли и воспроизводили документы, которые подлежали отправке по назначению, вели переписку с цензурой.

В ДП строго хранили криптологические секреты, фамилии сотрудников отделения Зыбина не разглашались. Так, например, в 1908 году из уфимского окружного суда тогдашнему начальнику Особого отдела ДП Е. К. Климовичу были направлены шифрованная записка и ключ к шифру. В сопроводительном письме, подписанном судебным следователем, высказывалась просьба дешифровать письмо, сообщить, какая подпольная организация пользуется таким шифром, и дать возможность допросить в качестве эксперта сотрудника ДП, который будет проводить эту работу. Через неделю в Уфу был направлен ответ. В ней сообщалось содержание записки, которую удалось дешифровать, давалась короткая характеристика шифра (достаточно распространенного), но ДП был категорически против допроса специалиста-криптолога.

Аналогичный случай был в 1915 году. В этот раз допросить криптолога пожелал судебный следователь из Витебского уезда. По приказу директора ДП Брюн-де-Сент-Ипполита было направлено письмо самому прокурору Петроградской судебной палаты с просьбой «одернуть» провинциального следователя. В письме указывалось, что «…разоблачение произведшего дешифровку лица является для Департамента полиции по особым соображениям весьма неудобным».

Отделение Зыбина проводило и экспертизу почерков. Так, например, в сентябре 1910 года «старший помощник делопроизводителя, коллежский советник Зыбин и чиновник для письма ДП коллежский регистратор Жабчинский рассматривали фотоснимки воззвания под заглавием „РСДРП“, начинавшегося словами: „Товарищи! Тяжелое и безотрадное время…“ и подписанного: „Орловская группа РСДРП“, а также протокол допроса ротмистром Шульцем крестьянина Ивана Федоровича Курбатова». Был проведен подробный анализ почерка воззвания и почерка Курбатова и дан очень осторожный вывод «о сходстве букв».

В своей работе Зыбин и его помощники совсем не были «слепыми» исполнителями руководящих указаний начальства. Они постоянно стремились совершенствовать дешифровальную службу ДП, неоднократно писали докладные записки о состоянии ее работы, выходили с предложениями.

Уже в своей докладной записке от 22 мая 1903 года директору ДП Белецкому Зыбин писал, что разрабатывать шифрованные документы с каждым годом становится все тяжелее и тяжелее из-за ряда причин. Во-первых, за последние два года, то есть с 1901-го по 1903 год, их количество стало «огромным», во-вторых, сравнительно легкие приемы шифрования текста, где ключом служило какое-либо слово или стихотворение, постепенно остаются в прошлом, и более «опытные революционные деятели (группа „Искра“ и др.) пользуются для переписки в настоящее время или двойными ключами, или страницами малоизвестных книг и брошюр, избирая для каждого отдельного корреспондента отдельную книгу и избегая повторения страниц, что крайне осложняет работу». Чтобы сделать свои поиски ключей успешнее, криптологи ДП стремились получить несколько писем из одного пункта.

Условия работы дешифровщиков также не способствовали успеху. Из-за тесноты помещений и крайней скученности в них служащих химические тексты приходилось проявлять непосредственно в кабинете заведующего Особым отделом ДП, а наиболее кропотливую работу с ними вообще проводить дома. Дома же сотрудники разбирали и все шифрованные письма.

Еще в 1901 году Зыбин направил начальнику Особого отдела ДП Л. Ратаеву доклад, в котором указывал на то, что резко начал расти поток шифрованных писем, полученных при обысках и арестах. Вместе с тем все эти письма, как правило, для дешифровки направлялись в ДП, поскольку в среде чинов жандармского корпуса своих специалистов по шифрам не было. Основы дешифровки преподавались только в Академии Генерального штаба. Что касается жандармских офицеров, которым такие знания были также необходимы, то они их не получали.

В связи с этим Зыбин предлагал свои услуги для занятий с офицерами штаба Отдельного корпуса жандармов с целью ознакомить их с техникой разбора наиболее употребляемых в революционном подполье шифров. Он считал, что для получения ими необходимых знаний достаточно посвящать этому два часа в неделю. Вместе с ними могли бы заниматься офицеры наиболее важных жандармских управлений и «охранки». «И вскоре можно было бы достичь того, чтобы в каждом из наиболее важных жандармских управлений, а также в охранных отделениях были офицеры, „знакомые“ с приемами дешифровки», – писал Зыбин.

Такие занятия Ивану Александровичу разрешено было проводить. Одновременно с этим он начал преподавать основы дешифровки офицерам Главного военного штаба.

При этом он занимался дешифровкой не только революционной переписки. В функции департамента полиции входила и контрразведка, в том числе и наблюдение за дипломатами и другими иностранцами, находившимися на территории России. Известно, что Зыбин работал с шифропереписки австрийской агентуры в России.

В период Первой мировой войны Зыбин и его коллеги из ДП работали над дешифровкой военных и агентурных сообщений противников России (Германии, Австрии и Турции). К сожалению, дешифровщикам МВД материалы поступали с задержкой, часто это были короткие сообщения, отдельные криптограммы, не передавалась информация о возможном содержании сообщений, обстоятельствах перехвата криптограммы.

Вся перечисленная информация могла бы существенно помочь криптоаналитикам. Но все же сотрудники и агентура ДП и военные старались делать все возможное для помощи своим дешифровщикам. Так известно, что в ходе войны были добыты ряд немецких и турецких военных и агентурных шифров и кодов. Разумеется, велась и аналитическая работа по вскрытию вражеских шифров.

Именно таким образом весной 1915 года команда Зыбина вскрыла ряд криптограмм австрийских и немецких агентов, посланных в Берлин, Вену и Брашов. В этом же году был прочитан ряд австрийских военных сообщений. В результате группа криптоаналитиков ДП во главе с Зыбиным за дешифровку вражеской шифропереписки была награждена денежной премией.

В июле 1915 года был проведен съезд руководителей кабинетов научно-судебной экспертизы при прокурорах судебных палат. На съезде внимание собравшихся было обращено на то, что этим кабинетам нередко приходится иметь дело с дешифровкой документов. Не имея специальной литературы и соответствующего руководства, сотрудникам кабинетов самим приходилось искать способы и приемы дешифровки.

Съезд принял решение о временном командировании чинов кабинетов в ДП, МИД и Военное министерство для ознакомления с практиковавшимися приемами дешифровки, принимая во внимание, что в этих ведомствах накоплен по данному вопросу уже большой опыт. Однако само Министерство юстиции не спешило выполнять решения съезда. Лишь через год, в июле 1916 года, было направлено письмо начальнику Особого отдела ДП Е. К. Климовичу с просьбой допустить сотрудника московского кабинета Русецкого на стажировку в ДП и ознакомить его с наиболее распространенными видами шифров и приемами их разбора. Такое разрешение было дано.

Конечно, в борьбе с революционным подпольем без агентов было не обойтись, но владея техникой раскрытия шифров, можно получить информации намного больше, чем ее давали несколько сотен агентов царской «охранки». Именно Зыбин ввел в практику чинов полиции, проводивших арест или обыск революционеров, обычай тщательным образом искать среди имеющихся книг именно те, которые могли заинтересовать Зыбина-дешифровщика.

Документальных подтверждений тому множество, например: «3.01.1910. Начальнику Санкт-петербургского губернского жандармского управления. Департамент полиции… препровождает при сем Вашему Превосходительству ключ к шифру и разбор шифрованной записки, отобранной по обыску у Якова Свердлова…».

Вот отрывок из его письма от 7 февраля 1910 года начальнику саратовского губернского жандармского управления: «…Отобранные по обыску у мещанина Николая Сергеевича Кузнецова записки зашифрованы 4, 15, 25, 29 и 35-й страницами какой-то неизвестной книги и разбору не поддаются по недостаточности материала. Прошу Ваше Высокоблагородие уведомить в самое непродолжительное время, не было ли обнаружено по обыску у названного Кузнецова, кроме означенных записей, какого-либо издания или легальной книги с пометками на отдельных страницах или загрязненных более других какой-либо страницей

от частого, сравнительно с другими, употребления и, кроме того, не встретилось ли одно и то же издание у прочих лиц, принадлежащих к одной с Кузнецовым организации, так как подобное явление в большинстве случаев указывает, что таковое издание служит ключом для шифрованных сообщений».

Летом 1911 года Зыбин прибыл из Петербурга в Москву для работы с одним из перехваченных революционных шифрованных писем. Успев только поздороваться с Заварзиным, он сразу попросил показать ему письмо. Заварзин уступил столичному гостю свой кабинет, и Зыбин с председателем окунулся в разбор депеши, зашифрованной дробными числами. Когда Заварзин вернулся, чтобы пригласить гостя на обед, ему пришлось дважды обращаться к Зыбину – тот его просто не слышал. За обеденным столом он продолжал удивлять собравшихся.

Доев суп, Зыбин сразу перевернул тарелку и попробовал писать на ней. Но карандаш на фарфоровой тарелке не был виден, поэтому он начал писать на манжетах, не обращая ни на кого внимания и забыв, где находится. Вдруг Зыбин подхватился со стула и закричал: «Тише едешь – дальше будешь!». После этого он опять сел, закончил обед и объяснил Заварзину, что четырехкратный повтор в письме буквы «Ш» дал ему ключ к квадратному шифру террористов. Озвученная им фраза и была нужным ключом.

Зыбину посылались на экспертизу и новые системы шифров, которые планировали использовать на внутренних линиях связи. Вот один из сделанных им выводов, датированный 20 июля 1910 года:

«Предлагаемая система шифрования с помощью двух вращающихся концентрических кругов является мало удобной, во-первых, потому, что по ней подлежащий шифрованию текст предварительно пишется длинными 40-буквенными группами в две строки каждая, последнее возможно лишь в тех случаях, когда весь текст депеши шифруется сплошь, без всяких пропусков; во-вторых, обязательное отделение каждого слова от следующего за ним знаком препинания, причем последний всякий раз обозначается парою цифр, излишне удорожает шифр и др.; в-третьих, сама система концентрических кругов излишне громоздка и не достигает цели в смысле сохранения секрета депеши, так как при любом наложении кругов и при всяких комбинациях для обозначения каждой буквы и каждого знака препинания имеется лишь два числа – четное и нечетное.

Например, буква А всегда будет обозначаться числом 37 или 28; буква Б – 39 или 20 и т. п., вследствие чего круги эти являются совершенно излишними; значения букв гораздо удобнее можно расположить в виде таблицы, как в Департаментском полицейском ключе, в котором, между прочим, для каждой буквы имеется от двух до четырех значений».

Несмотря на многочисленные сигналы «снизу», исходившие не только от рядовых сотрудников, но и от руководителей среднего звена, криптослужба ДП не поддавалась конструктивным изменениям в течение многих лет. Ведь время было совсем не простым, надвигались политические изменения, и это хорошо понимали и Зыбин, и его коллеги.

Главная проблема российской криптослужбы того времени заключалась не в плохой теоретической и практической подготовке кадров и не в использовании устаревших приемов шифрования, а в практическом применении шифросистем, из-за чего вся проделанная криптологами работа становилась бесполезной. И если криптология в России как наука находилась на мировом уровне, то применение ее достижений на практике оставляло желать лучшего.

1.8. Революционная тайнопись

Начиная с XIX века, в России кроме государственных ведомств шифрование активно использовали разные революционные подпольные организации, противодействовавшие власти, такие как «Земля и воля», «Народная воля», «РСДРП», «Бунд» (еврейский рабочий союз), эсеры, анархисты, нигилисты и др. По характеру своего применения шифры подпольщиков были подобны агентурным шифрам, поэтому к ним применялись те же требования: простота, безуликовость, легкая смена ключей у корреспондентов сети связи и т. п.

Необходимость применения шифров подпольными организациями была вызвана требованиями конспирации, потому что правоохранительные органы Российской империи вели с подпольщиками «ожесточенную» борьбу. Выдающийся русский «диссидент» XIX века Александр Герцен в своей переписке использовал достаточно простой прием. Буквы передаваемого текста заменялись на их числовые обозначения в старославянской азбуке.

В то же время широко использовался жаргонный язык, основанный на подмене понятий. Так, например, слово «армяне» значило «евреи», «греки» – «татары», «турки» – «сапожники», «Грузия» – «Тула» и т. п.

В 1860 году в России появилась революционная организация нигилистов (*лат*. nihil – ничто), которые не признавали и отрицали традиции дворянского общества и крепостничества и призывали к их разрушению во имя радикальной перестройки общества. В 1880 году они изобрели собственный шифр перестановки букв.

Их шифр был описан в 78-м томе «Энциклопедии Брокгауза и Эфрона», который вышел в России в 1903 году. Его суть была следующей: буквы, входившие в состав письма, оставались те же, но записывались в другом порядке. Их сначала помещали в клетки квадрата, а затем выписывали из него друг за другом, что определяло ключ к шифру. Далее процитируем саму энциклопедию:

«Нигилисты для нумерации клеток квадрата (по Флейснеру) пользовались определенным словом-секретом; буквы секрета нумеровались сообразно с местом, занимаемым ими в порядке алфавита. Нумера же наносились как на линию языка, так и на секретную линию; числа секретной линии в таком случае обозначали порядок строк, а числа линии языка – порядок букв каждой строки».

Это был шифр, который назывался «двойной перестановкой». Составлялась квадратная таблица по количеству букв ключевого слова. Слово-ключ записывалось сверху и сбоку таблицы. Буквы ключа и соответствующие им столбцы и строки нумеровались в алфавитном порядке. Из одинаковых букв стоящая правее получала высший номер. Шифруемый текст помещался в таблице в соответствии с полученной нумерацией столбцов и строк, а дальше выписывался из нее горизонтальными строками. В случае, когда клетки оставались незаполненными, в них вписывались любые произвольные буквы.

Возьмем следующий секретный ключ (шкалу перестановки): 456321. Его можно было отобразить словом «МОСКВА», каждая буква которого имела порядковый номер согласно месту расположения в алфавите. Открытый текст, например: «ПРОИНФОРМИРУЙТЕ О ТЕРРОРИСТИЧЕСКОМ АКТЕ» вписывался в квадрат размером 6 Ч 6. В соответствии с ключом осуществлялась перестановка столбцов: первый столбец ставился на 6-е место, второй – на 5-е и т. д. Потом по этому же правилу переставлялись строки: первая – на 6-е место, вторая – на 5-е и т. д.

	1	2	3	4	5	6
1	П	Р	О	И	Н	Ф
2	О	Р	М	И	Р	У
3	Й	Т	Е	О	Т	Е
4	Р	Р	О	Р	И	С
5	Т	И	Ч	Е	С	К
6	О	М	А	К	Т	Е

→

	4	5	6	3	2	1
1	И	Н	Ф	О	Р	П
2	И	Р	У	М	Р	О
3	О	Т	Е	Е	Т	Й
4	Р	И	С	О	Р	Р
5	Е	С	К	Ч	И	Т
6	К	Т	Е	А	М	О

→

	4	5	6	3	2	1
4	Р	И	С	О	Р	Р
5	Е	С	К	Ч	И	Т
6	К	Т	Е	А	М	О
3	О	Т	Е	Е	Т	Й
2	И	Р	У	М	Р	О
1	И	Н	Ф	О	Р	П

Шифротекст выписывался по строкам:

РИСОРРЕСКЧИТКТЕАМООТЕЕТЙИРУМРОИНФОРП.

В 1861 году появилась революционная организация «Земля и воля», которая сначала использовала квадратные шифры Полибия и числовые ключи Гронсфельда. Некоторые революционеры пользовались так называемым «пи-шифром»: число $\pi = 3{,}14$ должны были знать все участники сети связи. Из этих трех цифр образовывалась периодическая последовательность с периодом «3-1-4» (гамма шифра), складывающаяся с буквами открытого сообщения. Для этого буквы переводились в числа в алфавитном порядке:

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я
17	18	19	20	21	22	23	24	25	26	27	28	29	30

В результате слово «УКРАИНА» шифруется как «23122104 101804»:

Открытый текст	У	К	Р	А	И	Н	А
Цифровой текст	20	11	17	1	9	14	1
Ключевая гамма	3	1	4	3	1	4	3
Шифротекст	23	12	21	04	10	18	04

Однако постепенно появилась совсем новая шифросистема, получившая название «гамбетовской» по имени премьер-министра Франции Леона Гамбетты. Его взнос в криптологию заключался в отказе от применения приборов шифрования и замене их простыми алгебраическими операциями. Буквы текста и лозунга заменялись числами (в соответствии с порядком их расположения в алфавите), а затем складывались между собой, рождая шифротекст (добавление осуществлялось по модулю, равному мощности алфавита). Именем Гамбетты был также назван основной современный элемент шифрования – «гамма» шифра.

Удобство нового способа криптологии казалось неопровержимым. Исчезала необходимость в составлении обширных буквенных таблиц. Но конкретная реализация идеи Гам-

бетты у революционеров была своя, в чем еще надлежит не раз убедиться. Да и пользовались они одновременно сразу двумя вариантами шифрования.

В гамбетовской шифросистеме ключевое слово, например, «УЖГОРОД» размещалось вертикально в первом столбце таблицы, а с правой стороны выписывались буквы алфавита, которые продолжали его после каждой буквой ключа соответственно. Причем при шифровании использовалась 30-буквенная русская азбука, где буква «Й» стояла в конце алфавита.

После построения таблицы сверху нее выписывался правильный алфавит. Шифрование текста осуществлялась таким образом: буквы его брались из верхнего алфавита, а буквы шифротекста – из строк таблицы по очереди.

А	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**К**	**Л**	**М**	**Н**	**О**	**П**
У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й	А	Б	В
Ж	**З**	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Г	Д	Е	Ж	**З**	И	К	Л	М	Н	О	П	Р	С	Т
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю
Д	Е	Ж	**З**	И	К	Л	М	Н	О	П	Р	С	Т	У

Р	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ы**	**Э**	**Ю**	**Я**	**Й**
Г	Д	Е	Ж	**З**	И	К	Л	М	Н	О	П	Р	С	Т
Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й	А	Б	В	Г	Д	Е
У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й	А	Б	В
Я	Й	А	Б	В	Г	Д	Е	Ж	**З**	И	К	Л	М	Н
А	Б	В	Г	Д	Е	Ж	**З**	И	К	Л	М	Н	О	П
Я	Й	А	Б	В	Г	Д	Е	Ж	**З**	И	К	Л	М	Н
Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й	А	Б	В	Г

В результате слово «УКРАИНА» превращается в шифротекст «ЖРУОШЫД».

Эта система шифра стала основной в течение следующего десятилетия истории российского революционного подполья. Но по сути этот шифр был шифром Виженера, изобретенным еще в XVI веке. Разница заключалась в том, что из большой квадратной таблицы Виженера выписывались друг за другом только те строки, которые соответствовали буквам ключевой фразы.

Но подпольщики быстро поняли, что пользоваться громоздкой таблицей при шифровании не очень удобно. С целью конспирации ее нужно было составлять только в момент работы над криптограммами, а затем приходилось уничтожать. Все это привело к быстрому появлению цифрового варианта той же системы, которая использовала особый цифровой вариант шифра Виженера. Шифрование осуществлялась таким образом: буквы текста и ключа заменялись соответственно номерами их места расположения в алфавите и складывались между собой.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

При использовании ключевого слова «УЖГОРОД» текст «УКРАИНА» превращается в шифротекст «38172015252706»:

Текст	У	К	Р	А	И	Н	А
	19	10	16	1	9	13	1
Ключ	У	Ж	Г	О	Р	О	Д
	19	7	4	14	16	14	5
Шифротекст	38	17	20	15	25	27	06

Именно за таким шифром в революционных кругах окончательно закрепится название «гамбетовского».

В конце лета 1879 года появилась революционная организация «Народная воля», которая также использовала гамбетовский шифр. Но народники при шифровании из всех сумм больше 30 стали вычитать это же самое число (30). Таким образом, вместо 31 писали 1, вместо 45 – 15, а вместо 60 – 30 или 0.

При таком шифровании полностью нарушалось правило – соответствие маленьких сумм начальным буквам, а больших – конечным. При этом совсем отпадала необходимость составления громоздкой таблицы, и все операции можно было производить «в уме». На десятилетие вперед сокращенный гамбетовский шифр станет основным в практике революционеров России.

«Народная воля» применяла также и квадрат Полибия, который нередко называли «шифром узников». Этот шифр был удобен тем, что им можно было легко перестукиваться через стенки тюремных камер. В нем буквы русского алфавита по строкам вписывались в прямоугольник размера 6 Ч 6, и буква заменялась на ее координаты в таблице.

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ж	З	И	И	И	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Ъ	Э	Ю	Я		

Например, буква «Б» стояла в первой строке на втором месте, поэтому передавалась при перестукивании так: удар – длинная пауза – два коротких удара. Еще до народовольцев таким шифром активно пользовался «декабрист» М. Бестужев, находившийся в 1826 году в Алексеевском равелине Петропавловской крепости. Народовольцы использовали этот опыт.

Еще один из способов шифрования народников заключался в том, что составлялась таблица, разделенная продольными и поперечными линиями на девять или десять клеток. В этих клетках записывалась фраза (в каждой клетке по одной букве), которая составляла шифр. Каждый, как продольный, так и поперечный ряд клеток обозначался цифрой так, чтобы каждая клетка, а следовательно, и каждая находившаяся в ней буква соответствовала двум цифрам: одной – продольного ряда клеток, а другой – поперечного ряда. Однако эта система не получила в будущем никакого развития и осталась «памятником» шифровальной мысли революционеров.

За короткий срок от периода «хождения в народ» до покушения на Александра II народниками были реализованы все важнейшие системы шифров революционного подполья. В частности, они творчески развили идею шифра Виженера, создав несколько его оригинальных вариантов. А сокращенный гамбетовский шифр стал визитной карточкой российского подпольщика. Первоначально используемая буквенная запись криптограмм постепенно трансформировалась в цифровую. Главной заслугой народовольцев было усовершенствование многоалфавитного шифра Виженера и разных квадратных систем.

В конце XIX века в России появились разные революционные социал-демократические кружки, в частности марксистская группа «Освобождение труда», продолжавшие широко использовать квадратные и гамбетовские шифросистемы эпохи народничества. Их шифры базировались на коротких ключевых лозунгах, на которых было удобно строить именно квадратные таблицы. Хотя до этого времени они были уже достаточно дискредитированы в глазах старых народовольцев.

По датированному 1895 годом сообщению печально известного полицейского агента, а в будущем – одного из руководителей партии социалистов-революционеров (эсеров) Евно Азефа можно узнать о криптологии тогдашних марксистов: «Слово шифра „Великобритания“. Азбука составлена из первых чисел: 1 – А, 2 – Б, 3 – В и т. д. К каждой букве прибавляется буква слова „Великобритания“ и все цифрами, например, слово „вода“ пишется так:

В – 3 (в) + 3 (в) = 6 (в одной строке), О = цифра, которая отвечает „О“ + цифра для „Е“ и т. д.». В конце XIX века этот шифр получил название «раздельного гамбетовского ключа».

В конце 1901 года появилась партия эсеров, которая ввела в свою практику двойной шифр с использованием цифрового ключа. Эсеры назвали его «вторичным слитным шифром», который фактически был усложненным вариантом известного уже «пи-шифра». Из цифр ключа образовывалась гамма шифра, которая складывалась с цифровыми обозначениями букв сообщения. Для этого буквы переводились в цифры таким образом:

А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О
27	26	25	24	23	22	21	20	19	18	17	16	15	14	13

П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ю	Я	-
12	11	10	9	8	7	6	5	4	3	31	30	29	28	0

Роль «0» сводилась к делению двузначных и однозначных цифр. При использовании ключа «3162» текст «УКРАИНА» превращается в шифротекст «11181729211533»:

Текст	У	К	Р	А	И	Н	А
	8	17	11	27	19	14	27
Ключ	3	1	6	2	3	1	6
Шифротекст	11	18	17	29	21	15	33

Это был один из наиболее стойких видов среди всех действующих криптосистем, используемых революционерами. Правда, в данном случае представлен самый простой его вариант. Таким образом, двойные шифры прочно вошли в практику партии эсеров.

Кроме шифров в эсеровской подпольной практике нашли широкое применение всевозможные виды кодов. Так, в конце 1906 года группой террористов был разработан следующий код. В телеграфной депеше всегда должно было стоять слово «Приезжайте». Слово «Занемог» означало утренние часы от 10 до 12; «Заболел» – вечерние от 5 до 10; «Степан», «Дядя» – Великий князь Николай Николаевич; «Иван», «Отец» – премьер-министр Столыпин. Таким образом, телеграмма: «Приезжайте, занемог Иван» означала, что премьер-министр приезжает к царю на доклад между 5 и 10 часами вечера.

Одновременно в революционную практику начали входить также и другие шифросистемы. Начиная с 1890-х годов появились книжные и стихотворные шифры, что было вызвано в первую очередь недовольством подпольщиков стойкостью прежних шифросистем.

Книжные и стихотворные шифры обеспечивали достаточную стойкость, но имели существенный недостаток: корреспондентам сети необходимо было всегда иметь при себе книгу-ключ. Это нередко было неудобным, и, кроме того, в случае «провала» сети связи противник мог найти ключевую книгу, которая была у всех корреспондентов. Поэтому часто вместо книги использовались легко запоминаемые слова или фразы, по которым воспроизводилась гипотетическая страница книги.

В стихотворном шифре ключом было заранее оговоренное стихотворение, например:

Птичка божия не знает
Ни заботы, ни труда,
Хлопотливо не свивает
Долговечного гнезда.

О процессе шифрования социал-демократ Катин-Ярцев писал так:

«Нужно зашифровать фразу: „Петр арестован“. Первая буква первой строки – „П“, обозначаем 1/1, где числителем будет строка, знаменателем – порядок букв в этой строке. Для „Е“ мы можем взять, например, тринадцатую букву первой строки или двенадцатую третьей и т. д. Рекомендовалось вносить побольше разнообразия, заимствуя букву из разных мест ключа, чтобы затруднить для посторонних специалистов расшифрование написанного. При шифровке в книгах слева отсчитывалась и отмечалась еле заметной карандашной точкой буква, указывающая номер строки в ключе, а справа – порядок букв в строке. В конспиративном отношении предпочтительнее являлось менее общеизвестное стихотворение…».

Об использовании книжного шифра писал и участник питерского марксистского подполья И. Михайлов:

«Распространенный между революционерами шифр заключался в том, что намечалась страница какой-нибудь книги, по ней та или иная буква для нужного слова записывалась двумя цифрами, отделенными запятой: первая цифра показывала строчку сверху или снизу, а вторая – букву в строке слева направо или справа налево, смотря по тому, как условились переписывающиеся. Иной раз в книге записывались адреса разметкой букв в определенном порядке».

Приведем реальный исторический пример стихотворного шифра, который применялся революционерами в начале XX века. Ключом шифра было стихотворение Некрасова «Школьник»: «Ну, пошел же ради бога…». Стихотворение вписывалось в квадрат размером 10 Ч 10, а лишние буквы строки (содержащей более 10 букв) отбрасывались:

	1	2	3	4	5	6	7	8	9	10
1	Н	У	П	О	Ш	Е	Л	Ж	Е	Р
2	Н	Е	Б	О	Е	Л	Ь	Н	И	К
3	Н	Е	В	Е	С	Е	Л	А	Я	Л
4	Э	И	С	А	Д	И	С	Ь	К	О
5	Н	О	Г	И	Б	О	С	Ы	Г	Р
6	И	Е	Д	В	А	П	Р	И	К	Р
7	Н	Е	С	Т	Ы	Д	И	С	Ь	Ч
8	Э	Т	О	М	Н	О	Г	И	Х	Ъ
9	В	И	Ж	У	Я	В	К	О	Г	О
10	Т	А	К	У	Ч	И	Т	Ь	С	Я

Начало зашифрованного текста «Сообщите…» могло иметь разные варианты написания: «3/5 1/4 5/6 2/3 1/5 7/7 7/4 7/2…», «5/7 5/6 8/6 5/5 1/5 5/4 9/9 6/2 …» и т. п. Числитель давал номер строки, а знаменатель – номер столбца. Из-за отсутствия в таблице буквы «Щ» она заменялась на «Ш» (что не мешало правильной дешифровке).

Одна из ошибок революционеров заключалась в частом использовании произведений поэтов-демократов, знакомых полиции. Это облегчало дешифровку секретных посланий, поскольку сама идея шифрования была известна полиции. Защиту обеспечивал лишь ключ – «секретное» стихотворение. Другая ошибка, облегчавшая дешифровку, заключалась в частом употреблении стандартных слов и выражений: «Сообщите…», «Направляю вам…», «явка», «адрес» и т. п. Частое использование одного и того же ключа-стихотворения также облегчало чтение сообщений полицией, которая эффективно использовала эти ошибки.

Иногда заранее оговоренная фраза или начало некоторого стихотворения использовалось в качестве исходной гаммы шифра периодического гаммирования (упомянутый ранее гамбетовский шифр).

Приведем пример:

Небо лазурное в море купалося,
Солнышко ласково морю смеялося…

В соответствии с заранее оговоренным правилом подчеркивались буквы, стоявшие на нечетных местах: 1, 3, 5 и т. д. до 17. Эти буквы выписывались: Н, Б, Л, З, Р, О, В, О, Е.

Потом эти буквы переводились в числа в соответствии с их положением в русском алфавите. Получалось 17 чисел, которые и являлись исходной гаммой шифра. Открытый текст переводился в числа аналогично (по месту букв в алфавите). Исходная гамма периодически записывалась под преобразованным открытым текстом, и шифрованный текст получался в результате сложения буквы (числа) открытого текста и соответствующего знака гаммы шифра. Нетрудно заметить, что данный шифр воспроизводил давно известный шифр Виженера. Этот шифр получил широкое распространение и оказался достаточно стойким при его грамотном использовании.

А вот один из шифров анархистов, описанный идеологом этого движения в России Петром Кропоткиным. Он базировался на десяти словах, которые нужно было запомнить, не записывая:

«Пустынной Волги берег
Чернеют серых юрт рядами
Железный Финогеша Щебальский».

Каждая буква обозначалась двумя числами: номером по порядку следования слова и буквы в слове. Например, буква «П» – 11, «У» – 12, «С» – 13 или 51, или 07 (10-е слово, 7-я буква). Буквы, которые часто встречались («Е» или «А»), обозначались по-разному: «Е» – 32, 34, 42, 72, 86, 02, «А» – 36, 74, 88, 04. Дешифровать такой шифр было невозможно, тем более что писали всплошную, иногда ставя нечетное число букв в начале и конце письма и еще запутывая дешифровку произвольно вставленными «пустыми» парами: 26, 27, 28, 29, 20. Этот шифр был разновидностью книжного шифра, в котором вместо ключа-книги использовались легко запоминаемые фразы (стихотворения).

Кропоткин подчеркивал: «у нас есть специальные шифры для каждого из провинциальных кружков». Таким образом, шифры были индивидуальными для каждого адресата. Одновременно он отмечал и избыточную трудоемкость шифрования: «Мы часто работали ночь напролет, исписывая листы кабалистическими знаками и дробными числами».

Одним из вариантов шифра многозначной замены было построение таблицы замены по заранее обусловленному слову, словосочетанию или фразе. В случае использования ключевого слова «ПРЕКРАСНАЯ» строилась таблица следующего вида (применительно

к современному сокращенному русскому алфавиту): слово-лозунг вписывалось в таблицу по вертикали. Эти вертикали обозначались числами от 1 до 0 (в слове 10 букв). Каждая буква построчно разворачивалась в последовательность букв русского алфавита (циклически). В итоге получался прямоугольник 10 Ч 10, который и являлся гипотетической страницей книги-ключа:

	1	2	3	4	5	6	7	8	9	0
1	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
2	Р	С	Т	У	Ф	Х	Ц	Ш	Ь	Э
3	Е	Ж	З	И	К	Л	М	Н	О	П
4	К	Л	М	Н	О	П	Р	С	Т	У
5	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Ь
6	А	Б	В	Г	Д	Е	Ж	З	И	К
7	С	Т	У	Ф	Х	Ц	Ш	Ь	Э	Ю
8	Н	О	П	Р	С	Т	У	Ф	Х	Ц
9	А	Б	В	Г	Д	Е	Ж	З	И	К
0	Я	А	Б	В	Г	Д	Е	Ж	З	И

В соответствии с этим квадратом осуществлялась замена букв открытого текста на их координаты (первая цифра – номер строки, вторая – номер столбца). Например, буква «П» получала обозначение: 11, 30, или 46 и т. д. Таким образом, слово «УКРАИНА» могло иметь разные шифробозначения: «15, 35, 12, 61, 34, 38, 02» или «87, 90, 84, 91, 99, 44, 61» и т. д. Этот шифр имел уже неплохую криптостойкость.

Дальнейшее усложнение шифра многозначной замены было связано с введением пустышек. Приведем пример согласно вышеупомянутой таблице. Заранее договаривались, что столбцы и строки с номерами 2 и 9 были «пустыми», т. е. вычеркивались. Таким образом, появилась возможность вставлять в шифротекст «пустые» комбинации, содержащие отмеченные цифры (27, 95, 92, 29 и т. д.).

Следующее усложнение заключалось в одновременном использовании нескольких квадратов, полученных по разным ключам-лозунгам. При шифровании квадраты таблицы использовались циклически друг за другом. Иногда переход к следующему квадрату обозначался определенными комбинациями знаков, например трехкратным повтором одной и той же буквы в открытом тексте. Шифр стал более стойким, но менее удобным в применении.

Можно отметить «рациональный» шифр, предложенный одним из лидеров организации «Бунд» Павлом Розенталем в его книге «Шифрованное письмо», напечатанной в Женеве в 1904 году. Он считал его достаточно стойким, но по сути этот шифр был шифром пропорциональной замены. Такие шифры употреблялись ранее, и были известны методы их дешифровки.

Книга П. Розенталя была, по сути, теоретическим исследованием в области криптологии. На конкретных примерах автор подробно продемонстрировал, как можно раскрыть те или другие шифры, какие они имеют изъяны и как их можно избежать. Все это было очень важно в момент быстрого роста революционного движения, когда в его ряды вливались все новые новобранцы. Однако эта книга так и не смогла сломить негативные тенденции в шифропереписке революционеров более позднего времени.

В 1900 году в Женеве в типографии «Союза российских социал-демократов» была опубликована брошюра Владимира Акимова «О шифрах». Своей книгой он также внес весомый вклад в развитие шифровального дела российских революционеров.

В конце XIX века появилась новая революционная партия – РСДРП, членом которой стал будущий «вождь пролетариата» Владимир Ильич Ульянов (Ленин). Его революционная группа в период с 1895-го по 1900 год в своей шифропереписке использовала только страничные книжные ключи.

С конца 1900 года она начала внедрять стихотворные шифры. Способ шифрования был всегда одинаков – числитель шифродроби обозначал нужную строку, а знаменатель – номер нужной буквы этой строки, считая слева направо.

Как пример приведем личный шифр «ленинца» Николая Баумана. Он вписывал в стоклеточный квадрат стихотворение неизвестного поэта следующим образом:

	1	2	3	4	5	6	7	8	9	10	–	12
1	З	в	е	з	д	ы	у	с	ы	п		
2	В	ъ	с	у	м	р	а	к	е	н	е	ж
3	К	а	к	ъ	б	е	з	м	я	т	е	ж
4	Б	л	е	щ	е	т	ъ	и	х	ъ		
5	Т	у	ч	к	и	п	и					
6	Ф	л	о	т	о	м						
7	Д	а	н	а	д	о	с	ч				
8	Н	е	т	ъ	р	а	в	н	о	д	у	ш
9	Б	о	г	ъ	д	а	р	о	в			
10	В	ъ	м	е	с	я	ц	е	и			

Каждая буква при шифровании заменялась дробью по общепринятой системе. При этом вместо первого десятка цифр можно было брать второй или третий. Такие буквы, как «Ж» и «Ш», отсутствовали в основном ключевом квадрате, и был дополнительно введен еще 12-й столбец, где они по тексту стихотворения располагались.

Так, слово «УЖГОРОД» превращается в следующий шифротекст:

5/2 2/12 9/3 6/3 8/5 9/2 1/5.

Важный шаг в развитии стихотворных ключей сделал Александр Малиновский. Главная особенность его шифра заключалась в большом количестве фиктивных дробей (пустышек) в самой криптограмме. Все дроби со знаменателем больше 30 и числителем больше 5 были пустышками. Это определялось размерами стихотворения «Мнение человечества», который служил ключом к шифру.

При отсутствии заранее оговоренного шифра революционеры использовали намеки, иносказания и т. п. Так, в 1900 году соратник Ленина В. Ногин находился в Англии. Ленину было необходимо сообщить Ногину фамилию петербургского издателя книги (революционного содержания) К. Каутского.

Ленин так написал Ногину: «Боюсь доверить фамилию почте – впрочем, передам вам ее таким образом. Напишите имя, отчество (на русский лад) и фамилию Алексея и обозначьте все 23 буквы цифрами по их порядку. Тогда фамилия… будет состоять из букв: 6-й,

22-й, 11-й, 22-й (вместо нее читайте следующую по азбуке букву), 5-й, 10-й и 13-й». Настоящее имя «Алексея», известное обоим корреспондентам, было «Юлий Осиповичъ Цедербаумъ». Пронумеруем его по буквам:

Ю	л	и	й	О	с	и	п	о	в	и	ч
1	2	3	4	5	6	7	8	9	10	11	12
ъ	Ц	е	д	е	р	б	а	у	м	ъ	
13	14	15	16	17	18	19	20	21	22	23	

В результате чтение «шифрованного» сообщения дает фамилию «Смирновъ». Причем при шифровании Ленин допустил ошибку (пропустил букву Р = 18), однако она была легко обнаружена и устранена Ногиным.

Однако стоит подчеркнуть, что подпольщики допускали при использовании шифров серьезные ошибки, приводившие к дешифровке их переписки Департаментом полиции. Примерами таких ошибок были редкая смена ключей, шифрование текста не полностью, а только наиболее «секретной» его части и т. п. Использовались и откровенно слабые шифры (типа простой замены).

Редакция революционной газеты «Искра», обеспокоенная «провалами» своих агентов, в 13-м номере газеты от 20 декабря 1901 года поместила статью «Вниманию революционеров»:

«Добавим со своей стороны, что шифр – оружие обоюдоострое, ибо жандармы легко сумеют раскрыть всякий шифр, если не применять при шифровании особых предосторожностей. Безусловно, необходимо:

1) не отделять слова от слова;

2) не повторять часто одинаковых знаков, особенно знаков для наиболее употребительных букв;

3) писать шифр так, чтобы нельзя было узнать системы шифра;

4) не употреблять слишком известных стихотворений и книг.

Без соблюдения этих правил шифр прямо-таки недопустим».

Однако 4-й пункт «инструкции» противоречил действующей тогда революционной практике, поскольку для шифрования использовались произведения известных классиков русской поэзии Пушкина, Лермонтова, Крылова и Некрасова. Так, за весь период подпольной деятельности Надежды Крупской на должности секретаря разных партийных структур (1901–1905) для стихотворных шифров было использовано свыше 20 произведений Пушкина и столько же Лермонтова, 15 басен Крылова и 16 стихотворений Некрасова.

Особое внимание революционеры уделяли правильному (без ошибок) использованию шифров. Так, в письме (декабрь 1902 года) Ленин писал своему брату: «Ваше письмо получено. Написано оно неизвестным нам ключом, впрочем, мы расшифровали все, за исключением адреса. Не шифруйте иначе, как целыми фразами, иначе очень легко раскрыть ключ…». Здесь речь шла о том, что в секретных письмах часто оставались незашифрованными «несекретные» слова и фразы («клер»), существенно облегчавшие дешифровку.

Аналогичное послание своему корреспонденту в том же году направила Надежда Крупская. Получив плохо зашифрованное письмо, она в ответ возмущалась: «Перво-наперво позвольте вас выругать, что называется на все корки, за небрежную шифровку. Не зная, что вы условились о ключе с Евгением, я недоумевала, каким ключом вы пишете, и, наконец, расшифровала ваше письмо без ключа в какие-нибудь S часа. Это просто скандал. Не повторяйте одних и тех же знаков для одной той же буквы, иначе шифровка никуда не годится».

Таким образом, допускаемые при шифровании ошибки часто сводили на нет все усилия по защите информации. Поэтому ключи шифров и правила их пользования часто менялись. Были введены так называемые «одноразовые ключи», которые менялись с каждой новой шифровкой. Так, например, ключевое стихотворение оставалось тем же, но по простому правилу менялась нумерация его строк (начинать со второй строки, считая ее первой, и т. д.).

Иногда применялась практика смены ключа в процессе шифрования одного послания (по заранее оговоренному условию). Смена шифра практиковалась и в тех случаях, когда возникало подозрение о полицейской дешифровке ранее перехваченных писем. Так, в 1902 году Цедербаум писал в редакцию газеты «Искра»: «Не находит ли Фекла нужным переменить шифр, потому что, очевидно, несколько наших писем к ней пропали».

Но ограничиться исключительно книжными ключами революционеры, понятно, не могли. Слишком непредвиденной была их жизнь, чтобы в любой момент под руками оказалась необходимая книга.

Так, в августе 1903 года «ленинцы» начали использовать уже известный гамбетовский шифр. А связано это было с драматическими событиями, начавшимися сразу по окончании Второго съезда РСДРП, на котором партия «раскололась» на большевиков («ленинцев») и меньшевиков. Единственное усложнение, которое внесли большевики в гамбетовский шифр, заключалось в введении для цифр первого десятка дополнительных чисел «8» и «9»: 6 = 86, 2 = 92, 8 = 98 и т. д.

Известно, что Феликс Дзержинский, один из лидеров «Социал-демократии королевства Польского и Литвы» и будущий организатор советских органов госбезопасности, в 1910-х годах использовал в своей переписке гамбетовский шифр и ключевые фразы «Матка боска ченстоховска», «Когда будет солнце и хорошая погода», «Души человечьи вечно одиноки».

Вместе с тем идея квадратного (координатного) шифра была настолько привлекательна, что подпольщики вновь и вновь обращались к ней. Одним из таких новых вариантов был «круглый» шифр (или, как его называл В. Акимов в своей книге, шифр «по таблице Пифагора»). Он представлял собой прямое усовершенствование квадратного шифра, известного еще со времен народничества.

Составлялась квадратная таблица размером 6 Ч 6, а буквы в ней размещались в алфавитном порядке по схеме графического лабиринта:

	7	8	9	10	11	12
6	–	ч	ц	л	к	а
5	ѳ	ш	х	м	й	б
4	я	щ	ф	н	і	в
3	ю	ъ	у	о	и	г
2	э	ы	т	п	з	д
1	Ѣ	ь	с	р	ж	е

Буква сообщения записывалась как координатная дробь. Причем число можно было увеличивать на цифру 7 или множить на 7 и 10. Поэтому максимальные числа, которые встречались в дробях, – 84 и 120. Все эти новшества должны были озадачить дешифровщиков и маскировать систему шифра. Существовала и фиктивная дробь (пустышка): 6/7 = 7/6 и т. д., соответствующая пустой клетке таблицы. Она также использовалась в качестве знака разделения между словами.

Любую букву можно было зашифровать многими способами, например: А = 6/12 = 12/6 = 12/13 = 19/13 = 60/120 = 13/12 = 13/19 = 12/42 = 42/12 = 19/42 = 42/19.

Это была «вершина криптографической мысли» большевиков к весне 1905 года. Однако этот шифр был очень непрактичен и требовал предельного внимания при работе с ним. Достаточно было допустить ошибку в одном лишь знаке, пропустить цифру или, напротив, приписать лишнюю, как вся криптограмма превращалась в абсолютную «абракадабру». А это, при «химическом» копировании шифра или его некачественном проявлении, происходило всегда и везде.

В 1905 году на волне роста революционного движения в России было основано много новых издательств, которые начали массовыми тиражами выпускать ранее запрещенную литературу. И все эти издания сразу начали использоваться в качестве книжных шифров подполья. Кроме того, книжные шифры постоянно совершенствовались, а фиксированные страницы постепенно уходили в прошлое. В практику вошло правило постоянной смены ключевых страниц. При этом они обозначались определенными дробями, которые ставились в заранее оговоренных местах криптограмм.

Номера страниц определялись разными приемами – чаще всего произведением числителя и знаменателя или их суммой. Иногда их нужно было просто поставить рядом. Так, 2/5 писалось как 25, или же страница книги писалась как дата письма и т. д. Очень широко стали применяться «переменнозначные» книжные системы, где по определенным правилам автоматически менялись страницы ключа.

Среди социал-демократов также были изобретатели шифров. Остановимся на двух из них, принадлежавших к ядру социал-демократической большевистской партии и игравших ведущую роль в революционном движении, а также в ранний послереволюционный период. Это Глеб Иванович Бокий и Варвара Николаевна Яковлева.

При аресте Бокия полиция нашла у него самые обычные ученические тетради, исписанные математическими формулами, а в действительности – записями о подпольных делах, зашифрованными математическим шифром. Шифр этот был изобретением Глеба Ивановича, и ключ к нему был известен только ему одному. Лучшие шифровальщики, которых только имела в своем распоряжении царская «охранка», ломали головы над этими формулами, подозревая в них шифр. Однако раскусить этот орешек они так и не смогли.

Была автором собственных систем шифров и руководитель большевистской организации центрального промышленного района – секретарь московского областного ЦК РСДРП(б) В. Н. Яковлева. Дочь московского купца второй гильдии, она закончила математический факультет Высших женских курсов в Москве. Активная участница революции 1905–1907 годов, она была влиятельным партийным организатором, кандидатом в члены ЦК, автором Устава партии, принятого Шестым съездом РСДРП(б).

Равно как и Бокий, Яковлева создавала шифры, которыми пользовались и другие революционеры. К сожалению, ни тетради Бокия, ни шифры Яковлевой не сохранились. В архивах ДП остались лишь некоторые из шифрованных писем, зашифрованные другими, уже известными нам шифрами.

Как известно, «добыча» шифров и ключей к шифрам революционеров составляла одну из главных задач агентов полиции, действовавших в революционной среде. Получив сведе-

ния о шифрах, агенты немедленно передавали их в полицию или писали о них в своих донесениях. Так, в одном из таких донесений от 21 апреля 1915 года агент по кличке «Пелагея» докладывал ротмистру ДП Ганько:

«…На днях в Москву из Петрограда приехала по поручению ЦК РСДРП(б) какая-то „Татьяна Сергеевна“… „Татьяна Сергеевна“ имеет широкие полномочия по воссозданию на местах социал-демократических большевистских организаций и подготовке почвы к предстоящему летом текущего года созыву партийного съезда или конференции, и с этой целью ей поручено объехать область центрального промышленного района и юг, где она должна по выполнении первой задачи заручиться адресами для транспортировки партийной литературы…

„Татьяна Сергеевна“ почти ежедневно сносится с П[етербургским] К[омитетом], которому сообщает о достигнутых ею результатах и полученных связях, причем пользуется цифровым шифром:

Мы…….. 1
Азбуку…… 2
Весь…… 3
День…… 4
Писали…… 5
Бумаги…… 6
Книжку…….. 7
Извели…… 8
Мы…….. 9
Фыркающих…….. 10
Отвергали……. 11
Эх…… 12
Ящерицу…… 13
Предпочли……. 14
Плешь…… 15

Указанные цифры обозначают только слова ключа, например, 12 – „эх“, нужная же для шифрования буква обозначается порядковой цифрой, занимаемой буквой в слове ключа, так, например, зашифрованная буква „а“ будет обозначена: 2-1, или 5-4, или 6-4, или 10-5, или 11-7.

Однако кроме этих цифр при шифровке между ними вставляются еще произвольные цифры с таким расчетом, чтобы каждая буква была обозначена четырьмя цифрами; так, та же буква „а“ в окончательно зашифрованном виде будет обозначена: 7251, или 3544, или 2634, или 1025, или 1147.

При этом нужно иметь в виду, что между цифрами ключа вставляется только однозначная цифра, поэтому, если зашифрованная буква состоит из двух однозначных цифр, то произвольные цифры вставляются одна перед цифрой ключа, причем нельзя ставить только 1, а другая – между цифрами ключа; если же зашифрованная буква состоит из двузначной и однозначной цифр, как, например, „а“ – 11-7, то вставляется только одна однозначная цифра между ними. Таким образом, зашифрованное слово „Москва“ будет обозначаться так: 392211171534327613873109 5.

Для расшифровки, так как все указанные цифры пишутся подряд, нужно весь зашифрованный текст разбить на группы по четыре цифры, из коих выкинуть произвольно вставленные цифры, имея в виду, что если первая цифра будет „1“, то произвольно вставленная –

только одна цифра между цифрами ключа, то есть по счету третья, в противном случае – вставлено две цифры – первая и третья…»

Вместе с тем шифры были основным, но не единственным средством сокрытия партийных секретов. И чаще всего большевики использовали для написания конспиративных писем так называемый «эзопов язык» и словарный жаргон. Очень широко практиковался язык кодов или условных терминов. Ими обозначались города, партийные предприятия, проведенные мероприятия и т. д. Например: «Акулина» – подпольная типография, «журнал» – чемодан с двойным дном, «магазины» – комитеты партии, «счет» – транспорт литературы и т. п.

Очень популярным был код при переписке телеграфом. Однако этот способ связи был связан со значительным риском. Но намного чаще в телеграммах ограничивались несколькими условными терминами или цифрами. Так, предлагая провести собрание ЦК РСДРП в Стокгольме, Ленин писал в октябре 1905 года своим коллегам в Россию: «Дайте мне телеграмму… За подписью Болеслав с одним числом, которое означает дату, когда я должен быть в Стокгольме (30 = я должен быть до 30 сентября, 2 или 3 = я должен быть до 2 или 3 октября и т. д.)».

Таким образом, буквально все виды почтовой и телеграфной связи в Российской империи использовались революционерами для оперативных контактов между собой.

1.9. Военные шифры

На протяжении всего XVIII и первой половины XIX века криптослужба МИД кроме дипломатических и других шифров разрабатывала шифры и для военного ведомства. Во второй половине XIX века «цифирная» экспедиция МИД также в известной мере обеспечивала это ведомство шифрами, однако уже с конца 1840-х годов в Главном штабе военного министерства была организована и начала работать собственная «цифирная» экспедиция.

Разработанные собственные шифры утверждались военным министром. Экземплярами военных шифров обеспечивались старшие начальники войск и военных управлений, перечисленные в особом списке. В этот список входили император и члены императорской семьи, занимавшие важные военные посты, военный министр, начальники главных управлений военного министерства, командующие войсками в округах, начальники штабов округов, командиры корпусов, коменданты крепостей, атаманы и др.

Естественно, что шифрованная переписка по линии военного министерства велась не только в военный период, но и в мирное время. Зашифровывались сообщения, касавшиеся мобилизационной и военной подготовки, а также готовности армий и крепостей к военным действиям, и некоторые другие сведения.

В военное время из «цифирной» экспедиции МИД в Военное министерство поступали экземпляры тех шифров, которые действовали в сетях общей связи, куда по политическим, военным или иным причинам могли входить дипломатические представители России за рубежом, командующие армиями, военно-морскими силами и др.

Во второй половине XIX века большинство шифров военного министерства было кодами малого (до 1000 словарных величин) объема. Кодовыми обозначениями здесь были трех- и четырехзначные числа. Военные шифры этого типа обычно применялись в течение длительного времени, переделывался лишь быстро устаревающий словарь, что объясняется, например, изменением географии военных действий и т. д. Коды с перешифрованием, созданные в 1860-х годах, использовались еще в начале XX века.

Примером шифра, который использовался во время Крымской войны, был русский словарный ключ № 299 на 600 величин, который был введен в действие в апреле 1854 года. Предназначался он для связи командиров частей Дунайской армии. После войны этот шифр продолжал использоваться. В 1891 году им были обеспечены Бухара, Кашгар, Кульджа, Сеул, Пекин, Токио, Иркутск, Омск, Ташкент, Хабаровск, Ургa, Чугучак и Владивосток. Из действия его вывели только в 1901 году.

Построенная система телеграфной связи была не без успеха применена уже в ходе русско-турецкой войны (1877–1878). Во время этой войны в русской армии применялся французский биклавный ключ № 348, введенный в действие в 1870 году, русский биграммный ключ № 361, составленный в 1876 году, и некоторые другие шифры.

Ключ № 361 имел 992 шифровеличины – 28 букв упрощенного русского алфавита, три знака препинаний, а также всевозможные их биграммные сочетания. Им отвечали трехзначные кодовые обозначения. Этот шифр был сначала послан в консульства на Востоке, а также в Тифлис и Одессу. Французский ключ № 348 использовался на европейских линиях.

Во время русско-турецкой войны оба шифра были направлены в действующую армию. Их экземпляры были у генерала Н. П. Игнатьева и генерала В. Б. Фредерикса. Использовались эти шифры и после войны: французский ключ – до 1891 года, а русский – до 1903 года.

Во время русско-японской войны (1904–1905) применялся русский словарный ключ № 349, введенный в действие в 1868 году на линиях связи Министерства финансов для телеграфной шифропереписки. В 1879 году он был выведен из действия в результате утери двух экземпляров. Но в 1901 году он опять был использован для шифросвязи Министерства

финансов с таможнями. Кроме того, этот шифр был введен в действие в 1900 году в Министерстве государственного имущества, а в 1902 году – в Порт-Артуре, Харбине, Мукдене и, наконец, в 1904 году – в действующей армии.

«Словарные ключи» были наиболее распространенным типом шифров, используемых в конце XIX века в военном ведомстве. Их так и называли «военными ключами». Имея универсальные принципы построения, шифры военного министерства конца XIX – начала XX века отличались друг от друга некоторыми особенностями. Рассмотрим некоторые из них:

1. Ключ военного министерства № 6 1906 года. Был трехзначным многовариантным цифровым кодом с маскировкой и скрытым началом сообщения. Объем составлял 1000 словарных величин. Последними были слова, слоги, буквы русского алфавита. Всем часто встречающимся буквам и наибольшим словам были добавлены по два и больше кодобозначений, остальные словарные величины имели по одному кодобозначению. В правила, кроме того, было введено одно обязательное требование: если в тексте телеграммы встречались одни и те же слова, то их следовало набирать разными способами, избегая повторений кодобозначений. Отдельно были даны перешифровальные цифровые таблицы.

В правила было также введено обязательное требование прятать начало сообщения. С этой целью цифровой зашифрованный текст разбивался справа налево (с конца криптограммы) на группы по пять цифр каждая. В первой с конца группе оставалось четыре цифры. Пятизначные группы на листе отделялись друг от друга с помощью тире. Если в последней группе, соответствующей началу открытого сообщения, оставалось менее пяти цифр, то шифровальщик добавлял необходимое число произвольных цифр. Количество произвольно добавленных цифр указывалось числом, которое ставилось в самом конце цифрового набора, превращая первую с конца четырехзначную группу в пятизначную. Если в начале телеграммы произвольных цифр ставить было не нужно, то в конце последней группы ставился 0.

В шифре была предусмотрена маскировка: в каждой пятизначной группе криптограммы необходимо было переместить вторую и четвертую цифры одну на место другой, оставив без изменений первую, третью и пятую цифры. В результате этой маскировки перемещались цифры, которые принадлежали одной и той же или разным трехзначным кодовым группам. Тем самым нарушались порядковые (алфавитные) связи, если код был алфавитным или содержал какие-то части «с плохо размешанными», неслучайными кодобозначениями.

Указанные усложнения нельзя трактовать как перешифрование кодов, но как маскирующие меры они, естественно, могли существенно усложнить дешифровку противником этих систем.

Конечно, когда дешифровщику становились известными все эти усложнения, он легко от них избавлялся, осуществляя обратные процедуры перестановки знаков и определяя начало сообщения по последней цифре криптограммы.

Полученный номер проставлялся в конце телеграммы, причем он набирался буквами. Если телеграмма была ответом на ранее полученную, то номер последней проставлялся цифрами в начале данной.

Ввиду того, что иногда шифровался не весь текст телеграммы, а отдельные его части, в криптограмме цифровой текст мог перемежаться с открытым текстом. При этом каждая шифрованная его часть оформлялась в группы из пятизначных цифр всякий раз как самостоятельная телеграмма. Указанные правила пользования шифром были подписаны начальником отдела Генерального штаба генерал-майором Марковым и начальником «цифирного» отделения полковником Лео.

2. Ключ военного министерства № 7 1905 года. Был алфавитным трехзначным цифровым кодом на 900 словарных величин, размещенных на 18 таблицах 5 Ч 10. При этом первая

цифра этого кода менялась по ключу в соответствии с маркантом (показателем) так называемой малой таблицы.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.