УДК 003.26
ББК 32.81
Г79

Гребенников, Вадим Викторович.

Г79 Криптология и секретная связь. Сделано в СССР / Вадим Гребенников. — Москва : Алгоритм, 2017. — 480 с.

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

Массово-политическое издание

Гребенников Вадим Викторович

КРИПТОЛОГИЯ И СЕКРЕТНАЯ СВЯЗЬ
СДЕЛАНО В СССР

Редактор *С.В. Чертопруд*
Художник *И.М. Хотич*

ООО «Алгоритм»

Оптовая торговля:
ТД «Алгоритм» +7 (495) 617-0825, 617-0952
Сайт: http://www.algoritm-izdat.ru
Электронная почта: algoritm-kniga@mail.ru

Өндірген мемлекет: Ресей
Сертификация қарастырылмаған

Подписано в печать 19.09.2017.
Формат 84x108 1/32. Печать офсетная. Усл. печ. л. 25,2.
Тираж экз. Заказ

ISBN 978-5-906979-79-7

9 785906 979797 >

Знак информационной продукции согласно Федеральному закону от 29.12.2010 г. № 436-ФЗ 16+

СОДЕРЖАНИЕ

Кто владеет информацией,
тот владеет миром.
Натан Ротшильд

ПРЕДИСЛОВИЕ

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

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

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

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

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

в группе. Встречались и осложнения этой системы, например, руны в группах перемешивались.

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

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

Символизм, который был заложен в каждую букву, выполнял две функции: во-первых, он скрывал тайны от непосвященных, а во-вторых, напротив, открывал их тем, кто был этого достоин, кто понимал скрытый смысл этих символов. Посвященные жрецы считали святотатством обсуждение священных истин высшего света или божественных откровений вечной Природы на том же языке, который использовался простым народом. Именно из-за этого всеми сакральными традициями мира разрабатывались свои тайные алфавиты.

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

Греческий алфавит, подобно ивриту для евреев, служил грекам одним из средств познания мира. У греков буквы «A», «E», «H», «I», «O», «Y» и «Ω» отвечали семи планетам (небесам). Буквы «B», «Γ», «Δ», «Z», «K», «Λ», «M», «N», «П», «P», «Σ» и «T» при-

писывались 12 знакам Зодиака. Буквы «Θ», «Ξ», «Φ» и «Χ» 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 «Е» (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 от-

крытым текстом. Метод перекручивания и сокрытия открытого текста таким образом, чтобы спрятать его суть, называется шифрованием. Шифрование открытого текста приводит к его превращению в непонятную абракадабру, именуемую шифротекстом. Шифровка позволяет спрятать информацию от тех, для кого она не предназначается, невзирая на то, что они могут видеть сам шифротекст. Противоположный процесс превращения шифротекста в его исходный вид называется расшифровыванием.

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

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

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

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

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

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

Часть 1

РОССИЙСКАЯ ИСТОРИЯ

1.1. Древнерусская тайнопись

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

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

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

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

Второй после системы «иных письмен» системой тайнописи, известной из русских рукописей, была система «измененных знаков», зафиксированная уже в XIV веке. Выделяют две ее разновидности: а) систему знаков, измененных «путем прибавок» к обычным начертаниям; б) построенную на принципе, сходном с греческой тахиграфией, когда вместо буквы пишется лишь часть ее.

Тахиграфия — это изменение написания букв, когда писалась или часть буквы, или наоборот, ее написание допол-

нялось 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 состо-

ял 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 употреб-

ление 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 «монокондил», разные приемы образного и фигурного письма, а также «акростих» (стихотворение, в котором начальные буквы строк образуют слово или фразу). «Акростих» — типичный для европейской средневековой письменной культуры прием организации поэтического 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 стро-

кой. Шифры приходилось выделять в сообщении так же, как и цифры, то есть «титловать» их. Поэтому полностью понятно название шифра «цифрой», то есть текстом, который требует специального прочтения. Впрочем, возможно, что слово «цифирная» в названии палаты была буквальным заимствованием французского слова «chiffre», которое означало как шифр, так и цифру.

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

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

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

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

В 1633 году патриарх Филарет написал «для своих государевых и посольских тайных дел» особенную азбуку и «состав затейным письмом». Сохранился приказ российскому представителю в Швеции Д. Францбекову, из которого видно, что при составлении сообщений царю посол должен был использовать тайнопись. Приказ заканчивался таким образом: «Да что он, Дмитрий [Францбеков], будучи в Свее [Швеции], по сему тайному наказу о тех или иных о наших тайных делах и наших тайных вестей проведает и ему обо всем писать ко государю царю и великому князю Михаилу Федоровичу всея

Руси к Москве по сему государева тайному наказу ~~затейным~~ закрытым письмом».

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

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

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

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

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

Сам царь, очень образованный для своего времени, лично также использовал шифры и в своей приватной переписке. Послы и резиденты всегда обеспечивались шифрами. Например, в 1673 году резидентом в Речь Посполитую (Польшу) был