

Глава 1

Начало криптографической деятельности в Русском государстве (до конца Смутного времени)

1.1. Первое упоминание об использовании тайнописи в русской дипломатической переписке. Первое документальное упоминание об использовании цифирной азбуки в дипломатической переписке Московского государства датировано 1590 годом. Представляется знаменательным, что впервые обнаружил этот факт и отметил его важность Николай Михайлович Карамзин, создатель известной 12-томной «Истории государства Российского» (1803–1826).

Описывая плоды просвещения русского общества в конце XVI столетия, Н. М. Карамзин (рис. 1.1) счёл необходимым подчеркнуть: «Тогда же в Посольских бумагах начали мы употреблять тайные цифры»¹. Слово «цифры» здесь означает шифры.

Писатель указал в своей «Истории государства Российского» некоторые подробности: «Гонец Андрей Иванов в 1590 году писал из Литвы к царю вязью, литореею и новою азбукою, взятою у Посла

¹ Карамзин Н. М. История государства Российского. М.: Книга, 1989. Т. 10, с. 148.



Рисунок 1.1 Карамзин Н.М. Художник: А.Г. Венецианов

Австрийского, Николая Варкоча»². «Гонец» здесь означает дипломатический ранг.

В середине XIX века А. Н. Попов уточнил, что в 1589 году приехал в Москву из Австрии посол Николай Варкоч, которому из Москвы к цесарю (императору) приказано было писать *«письмом мудрою азбукою, чтоб опричь (кроме — авт.) Цесарского Величества никто не разумел»*³. Варкоч передал московским дипломатам цифирную, т.е. шифровальную азбуку, и указал способ её применения.

Академик А. И. Соболевский по этому поводу заметил: *«В Москве немедленно переняли эту азбуку и стали пользоваться ею, разумеется, с значительными изменениями»*⁴. И сам эпизод, и содержание шифрованного письма гонца Иванова отражены в Посольской

² Там же.

³ Попов А. Н. Дипломатическая тайнопись времён царя Алексея Михайловича. // Записки Императорского Археологического общества. СПб., 1853. Т. 5, с. 157.

⁴ Соболевский А. И. Славяно-русская палеография. М., 2007, с. 113.

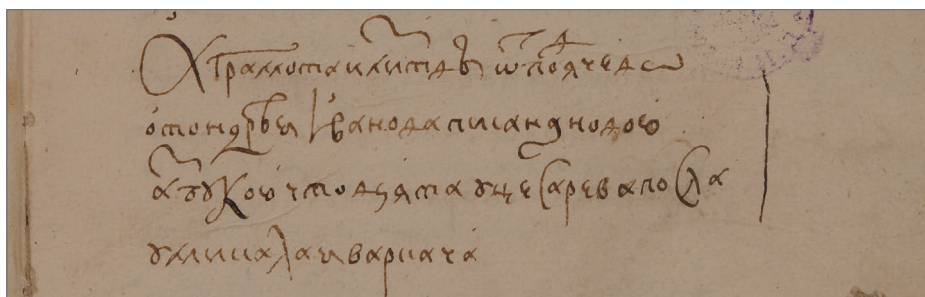


Рисунок 1.2. Запись в Посольской книге (1590 г.)

книге по сношениям с Литвой, фрагмент её страницы⁵ приведён на рис. 1.2. Запись гласит: «Грамота из Литвы от подьячего от Ондreja Иванова писана новою азбукою, что взята у цесарева посла, у Микалая Варкача».

В Приложении 1 приведены образцы скорописного письма букв русского алфавита, позволяющие прочесть эту запись, и дан её разбор.

Именно это место в тексте привлекло внимание Н. М. Карамзина.

Хорошо налаженное делопроизводство Посольского приказа сохранило для нас имя впервые упомянутого в документах русского шифровальщика, расшифровавшего письмо в Москве. Читаем в посольской книге: «... а на низу грамоты подписано по-руски вязью, што тое грамоту перевести латынскому переводчику Якову Заборовскому, и переводил тое грамоту Яков»⁶.

Обратим внимание на 3 момента.

1. От получения азбуки до её применения прошло всего несколько месяцев. А ведь потребовалась её существенная переработка. Можно представить, что азбука Варкоча предназначалась для шифрования букв латинского алфавита. В ней содержались выписанные по порядку знак за знаком шифровые обозначения латинских букв. Гонец Иванов шифровал в Литве своё донесение, написанное

⁵ Российский государственный архив древних актов (РГАДА). Ф. 79. О. 1. Д. 20, л. 52.

⁶ Карамзин Н. М. История государства Российского. М.: Книга, 1989. Т. 10, с. 77, примеч. 438.

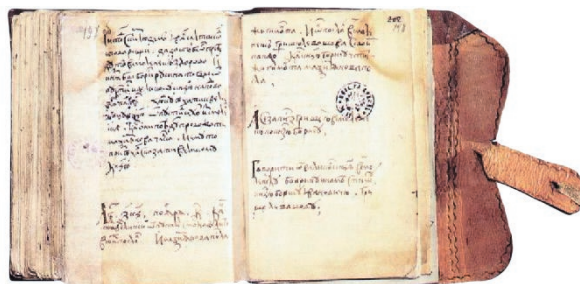


Рисунок 1.3 Одна из посольских книг XVI века

по-русски. В его цифирной азбуке должны были находиться шифровые обозначения для 40 русских букв, составлявших алфавит того времени. Но русских букв значительно больше, чем латинских. Поэтому цифирная азбука Иванова должна была заметно отличаться от азбуки Варкоча. Требовалось время и для обучения гонца.

2. Объём шифрованного письма был велик: описание его содержания в посольской книге занимает более 10 страниц рукописного текста.

3. Н. М. Карамзин указал на использование в посланиях Андрея Иванова ещё и вязи, и литореи. Он добавил также, что «*другое донесение сего подъячего было писано так называемую литорею*»⁷. Литорея (от слова «литера», «буква») — это условная азбука, шифр, тайнопись, а вязь — сплетение нескольких письменных знаков в один. Далее мы рассмотрим вязь и литорею подробнее.

Можно заключить, что гонец Иванов применял в своих сообщениях из Литвы разнообразные средства шифрования. Вместе со сказанным выше это свидетельствует о наличии шифровального опыта в Посольском приказе, пославшем гонца.

Ниже мы рассмотрим более подробно историю с азбукой Варкоча.

Вероятно, справедливо предположение, что и ранее 1590 года криптография использовалась в Московском государстве в важной переписке.

⁷ Там же.

1.2. Исторический рубеж в использовании криптографии.

Представляется, что историческим рубежом в использовании криптографии стала женитьба великого князя Московского Ивана III Васильевича на племяннице последнего византийского императора Софии Палеолог в 1472 г. Известно, что в Москву она приехала, «окружённая толпой образованных греков». *«Невеста имела свой особенный Двор, чиновников и слугителей; к ним присоединились и другие греки, которые надеялись обрести в единоверной Москве второе для себя отечество»*⁸.

Преобразования, начатые Иваном III ещё ранее, с такой поддержкой затронули все стороны государственной жизни Руси. Развернулось каменное строительство в Москве и других крупных городах, свой стимул получили административные перемены и образование. Москва того времени была весьма значительным городом. Уже в начале XVI столетия число дворов в Москве достигало 40 тысяч, по оценке австрийского посла Зигмунда Герберштейна.

В 1497 году новым государственным гербом стал двуглавый орёл (рис. 1.6), бывший византийский имперский герб времени Палеологов. Вскоре появилась и утвердилась идея Москвы как третьего Рима, т.е. третьего центра православного мира после Рима и Константинополя. Государство именовали тогда и до второй половины XVII века Московской, Московским государством или Русским государством, Русией.

Московское государство в лице своих правителей стало ощущать своё преемство от Римской империи. Это преемство признавалось некоторым образом и на Западе, и на Востоке. Так, в 1519 году глава католической церкви папа Римский Лев X писал великому князю Василию Ивановичу: *«Константинополь — отчина московского государя, и если московский государь захочет стоять за неё, то у нас для этого готовы и пути и средства»*⁹.

⁸ Карамзин Н. М. История государства Российского. М.: Книга, 1989. Т. 6, с. 41.

⁹ Костомаров Н. И. Русская история в жизнеописаниях её главнейших деятелей. М., 1996. Кн. 1, с. 363.



Рисунок 1.4. Встреча царевны Софии Палеолог
псковскими посадниками и боярами в устье Эмбаха
на Чудском озере. Художник: Ф.А. Бронников



Рисунок 1.5.
Изображение
Ивана III из «Царского
титulyарника» 1672 г.



Рисунок 1.6.
Малая
государственная печать
Ивана III (прорисовка)

Многое из Византийской империи в Москве рассматривалось как образец. Например, посольская служба. Известно, что Иван III привлекал для организации дипломатической работы знатоков-греков. Именно они стали первыми московскими посланниками в западную Европу. В таком случае естественно предположить, что состоялось знакомство и с криптографией, неотъемлемой составляющей византийской дипломатии.

1.3. Первые московские дипломаты. Великокняжескую канцелярию (казну), ведавшую финансами и внешней политикой, при Иване III возглавляли греки Ховрины и Траханиоты. Братья Траханиоты приехали в свите Софии Палеолог.

Ховрины происходили из византийского императорского рода Комнинов, они внесли заметный вклад и в становление российской государственности. Достаточно упомянуть их потомка, знаменитого дипломата Фёдора Алексеевича Головина. В Москве собирались представители и других знатных византийских родов. Так, в 1485 году из Константинополя приехал Иван Раль с детьми, принадлежавший к ближайшему окружению Палеологов; в 1496 году выехал из Венгрии на жительство в Москву «боярин из Царьграда» (Константинополя) Фёдор Ласкарь с сыном Дмитрием.

Московская служилая элита быстро восприняла опыт приезжих учителей. Уже в 1474 году отправился за границу первый русский по происхождению посланник. Это был Семён Иванович Толбузин. Именно он привёз из Венеции в 1475 году знаменитого у нас зодчего и пушечных дел мастера, строителя современного Московского Кремля Аристотеля Фиораванти, а также других специалистов своего дела (рис. 1.7).

В 1489 году впервые состоялся обмен послами с Австрийской империей, точнее, со Священной Римской империей германской нации — важнейшим европейским государством того времени. Русский посол Юрий Траханиот повёз императору грамоту, в которой Иван III именовал себя государем всея Руси.

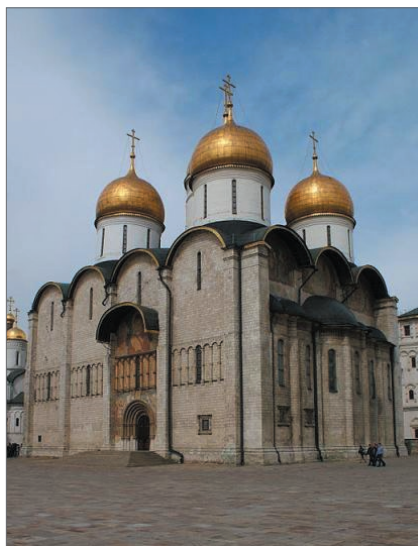


Рисунок 1.7.

Успенский собор в Московском Кремле (1475–1479 гг.), место коронации русских царей и императоров. Архитектор: А. Фиораванти

Всё же, в ту пору вектор московской внешней политики был ориентирован больше в восточном направлении, чем в западном. Взаимный интерес сделал связи на Юге и Востоке глубокими и разносторонними. Н. М. Карамзин писал о путешествии в Индию тверского купца Афанасия Никитина: *«Индийцы слышали об ней (о России — авт.) прежде нежели о Португалии, Голландии, Англии. В то время, как Васка да Гама единственно мыслил о возможности найти путь от Африки к Индостану, наш тверитянин уже купечествовал на берегу Малабара и беседовал с жителями о догматах их веры»*.

Как велик был дипломатический аппарат при великом князе Иване III? Должностные лица в то время именовались дьяками и подьячими, в греческом языке слово «диаконос» означает «служитель». По историческим документам выявлено 28 служителей, подьячих, *«приставленных к посольским делам»* в 43-летний период правления Иоанна III¹⁰.

¹⁰ Дьяки и подьячие Посольского приказа в XVI в. Справочник. Составитель Савва В. И. М., 1983, с. 354.

1.4. Интеллектуальный уровень русского правящего слоя в конце XV — начале XVI столетий. Приехавшие византийцы оказались в культурно и интеллектуально близкой им среде.

Духовное и культурное родство Византии и Руси насчитывало к концу XV века уже полтысячелетия своего развития. Всё это время культурное пространство на Руси создавалось совместными усилиями русских и греков — византийцев. Даже кириллица, с её графикой, ориентированной на греческую, и церковнославянский язык были мудро устроены таким образом, что способствовали восприятию на Руси своей письменности как славянской версии византийской книжной культуры¹¹. В этом проявлялся многовековой опыт византийцев в деле построения империи. И постепенно русская элита впитывала этот имперский опыт.

Уже 5 веков на Руси существовал слой хорошо образованных людей. Одним из них был боярин Фёдор Иванович Карпов, крупный сановник и дипломат времён великого князя Василия Ивановича. Он руководил восточной внешней политикой Русского государства в 1508–1539 годах. Ф. И. Карпов знал греческий, латинский и восточные языки.

Сохранилась его переписка с Максимом Греком, весьма образованным монахом с Афона, приглашённым в Москву для перевода церковных книг и исправления старых переводов. В своих письмах Ф. И. Карпов обнаруживает знание античной литературы, философии, цитирует Аристотеля.

По мнению историка математики Р. А. Симонова, в последние годы усилиями исследователей и, благодаря недавним археологическим находкам, постепенно, но существенно меняются представления об интеллектуальном уровне Древней Руси. Ещё ранее известный историк А. А. Зимин отмечал присущий русским просвещённым интеллектуалам начала XVI века «глубокий интерес к математике, астрономии и медицине».

¹¹ Симонов Р. А. Математическая и календарно-астрономическая мысль Древней Руси. // Памятники религиозно-философской мысли Древней Руси. М., 2007, с. 48.

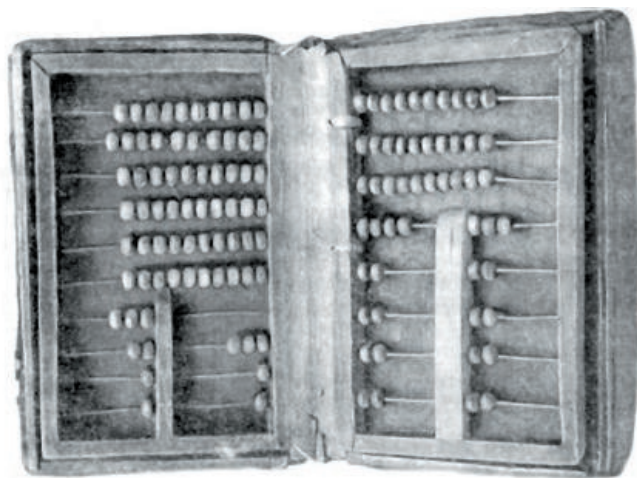


Рисунок 1.8. Дощица счётная (середина XVII века)

Уже в XI столетии на Руси сложилась традиция обучения цифровым знаниям, «существовал свой собственный оригинальный способ обучения арифметике с использованием вычислительного устройства — абака (счёт плодовыми косточками — авт.)... Обучение счёту велось, судя по задачам, очень квалифицированно, с учётом древнерусской денежной системы и с использованием шестизначных чисел»¹².

Историки отмечают и совершенствование на Руси расчётных инструментов. В 50-е годы минувшего века главный хранитель Отдела нумизматики Государственного Эрмитажа И. Г. Спасский установил русское происхождение неведомых Западу счётов. Русские счёты, точнее, «дощица счётная», широко и успешно использовались для целых и дробных вычислений. Они являлись «*организмической, неотъемлемой основой и совершенно необходимым инструментом древнерусской налоговой арифметики*»¹³.

¹² Там же, с. 50.

¹³ Спасский И. Г. Происхождение и история русских счётов. //Историко-математические исследования. М., 1952. Вып.5, с. 61.

Как заметил И. Г. Спасский, о древности счётов на Руси свидетельствует и живой русский язык. Достаточно вспомнить выражения: «сбрасывать со счетов» (не принимать во внимание), «сводить счёты» (выяснять отношения), «скостить» (уменьшить), «выкладка» (обоснованное доказательство) и др. И. Г. Спасский указал: *«В Ашмолеан музеем в Оксфорде хранится вывезенный не позже 1618 года из России, но по недоразумению считающийся китайским, такой немудрящий прибор»*¹⁴. «Дощицу счётную» можно видеть на рис. 1.8.

О вычислительной грамотности и значительном интересе к математическим расчётам свидетельствует берестяная грамота второй половины XII столетия, найденная в Новгороде. Она *«установила существовавшую на Руси традицию математических состязательных посланий»*¹⁵. В задаче, запечатлённой на бересте, требовалось обнаружить некую общность между числами 128 и 96. Исследователи предложили следующее решение:

$$(8 + 8) \times 8 = 128, (8 + \frac{8}{2}) \times 8 = 96$$

Отметим, что в Западной Европе традиция таких посланий существовала в XV–XVI веках: расклеивались или рассылались задачи с вызовом математиков на состязание по их решению.

В XV веке восстанавливаются контакты Москвы с западной Европой, испытывавшей в то время сильное культурное влияние греков — византийцев. Значительно вырос спрос на переводную литературу, потребовались квалифицированные переводчики. В начале XVI века глава русской церкви митрополит Даниил призывал своих юных современников учиться: *«Любомудръствуите, юнии, в хитростех трудящиеся елико по силе: или в писательнемъ художествии, или в учении книжном, или в коем рукоделии аще есть, или ино кое*

¹⁴ Спасский И. Г. Московская математическая рукописная книга середины XVII века и её первый владелец. // Археографический ежегодник за 1979 год. М., 1981, с. 63.

¹⁵ Симонов Р. А. Математическая и календарно-астрономическая мысль Древней Руси. // Памятники религиозно-философской мысли Древней Руси. М., 2007, с. 121.

*художество о Господи»*¹⁶. В современном изложении здесь можно прочесть: *«учитесь с интересом, юные, осваивая профессии по своим способностям: писательское творчество, или учёную специальность, или ремёсла, или художественное творчество»*.

Эту же мысль внушал в те годы и Максим Грек: кто недостаточно хорошо освоил грамматику, стихосложение, риторику и философию, не сможет правильно понимать написанное, тем более заниматься переводом на другой язык.

Академик А. И. Соболевский писал в 1903 году: *«У нас господствует убеждение, что Московское государство XV–XVII веков боялось иноземцев и было как бы отгорожено от западной Европы стеною, до тех пор, пока Пётр Великий не прорубил в Европу окна. Трудно сказать, откуда у нас взялось это убеждение... Борьба с господствующим убеждением не представляет большой трудности, и всякое специальное исследование... даёт в результате длинный ряд крупных и мелких данных, указывающих на тесные связи Москвы с западом Европы задолго до Петра... Первые переводы произведений западноевропейских литератур, сделанные несомненно в Московской Руси, относятся ко второй половине XV века»*¹⁷.

В конце XVI столетия началось распространение печатных книг отечественного издания. В ту пору в Москве существовала крупная государственная типография европейского типа при Печатном дворе.

Подводя итог сказанному, можно констатировать, что русская элита в XV и XVI веках находилась на одном культурно-интеллектуальном уровне с элитой греков — византийцев. Так, рядом с иконописцем Феофаном Греком был великий Андрей Рублёв, рядом с учёным и переводчиком Максимом Греком — дипломат Фёдор Иванович Карпов.

Знания и византийский опыт, в том числе и по криптографии, на Руси было кому оценить, усвоить и творчески использовать.

¹⁶ Бычков В. В. Русская средневековая эстетика. XI–XVII века. М., 1995, с. 306.

¹⁷ Соболевский А. И. Переводная литература Московской Руси XIV–XVII веков. СПб., 1903, с. 38–39.

1.5. Следы греко-византийской криптографии. О греко-византийской криптографии известно немного, в основном — по её следам в исторических источниках других стран.

Есть сведения, что в VIII веке арабскому знатоку языков Абу аль-Яхмади удавалось вскрывать византийские тайнописные послания, если исходный, как ещё говорят, «открытый» текст был греческим.

Немецкий исследователь Гардтгаузен (V. Gardthausen) в своей книге 1879 года привёл три греко-византийских шифровальных азбуки¹⁸. Они показаны на *рис. 1.9*.

Здесь во второй и пятой строках записана азбука 1, т.е. шифровые обозначения для всех перечисленных по порядку в первой и восьмой строках букв греческого алфавита; в третьей и шестой строках выписана азбука 2; в четвёртой и седьмой — азбука 3.

Все эти тайнописные азбуки значковые, составлены из знаков специального вида. Древнейшая из них — третья, её относят к VII веку.

Гардтгаузен отметил также раннее наличие у греков разнообразных цифровых шифров, использовавших числовые значения букв греческого алфавита.

Проявления византийской криптографии в славянских литературных источниках основательно исследовал академик М. Н. Сперанский. Среди его многочисленных сочинений содержится и капитальный труд «Тайнопись в юго-славянских и русских памятниках письма» 1929 года издания, переизданный в 2011 году.

О русских системах изменённых знаков он писал, что они «*не чужды греческой криптографии XV века*». М. Н. Сперанский отметил и пришедшую из Византии цифровую тайнопись. Подробности помещены в *Приложении 2*.

Косвенно о греко-византийской тайнописи можно судить по криптографическим публикациям XV и начала XVI веков в госу-

¹⁸ Gardthausen V. Griechische Palaographie. Leipz., 1879. S. 240.

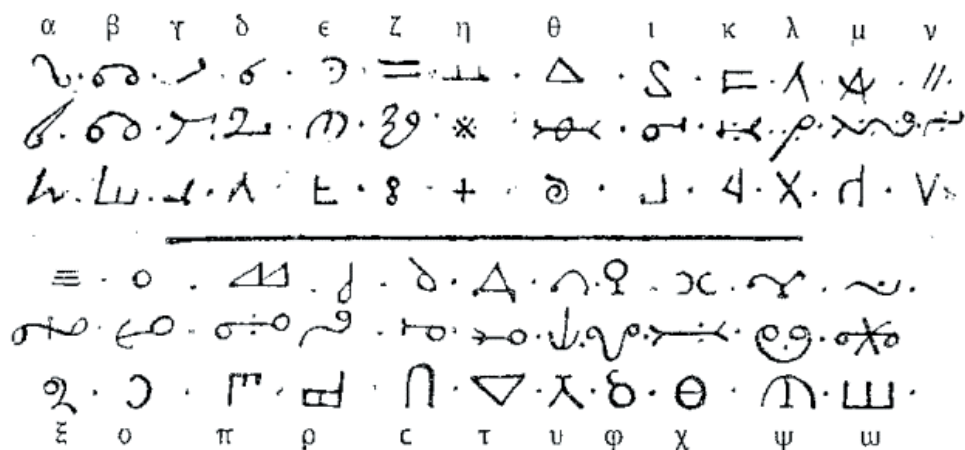


Рисунок 1.9. Три греко-византийские тайнописные азбуки

дарствах, соседствовавших с империей и располагавшихся на территории нынешней Италии. Известен всплеск публикаций, связанных с криптографией, по времени достаточно близкий к 1453 году — моменту окончательной гибели Византийской империи под турецким натиском. Можно предположить наличие связи между этими двумя событиями. Ведь именно в соседних государствах оседали прежде всего и выходцы из империи, и её культурные богатства. Это началось задолго до 1453 года и продолжалось много лет.

М. Н. Сперанский писал: «Для некоторых видов латинской средневековой тайнописи приходится предполагать также и византийское влияние»¹⁹.

В связи со сказанным обращают на себя внимание замечания известного историка криптографии Д. Кана: «В Европе криптография находилась в состоянии застоя вплоть до наступления эпохи Возрождения»; «Нет никаких документальных доказательств того, что криптоанализ попал в христианский мир из исламского»; «Труды Калкашанди (содержательный раздел по крипто-

¹⁹ Сперанский М. Н. Тайнопись в юго-славянских и русских памятниках письма. Л., 1929. Вып. 3–4, с. 1.

графии в 14-томной арабской энциклопедии 1412 года — авт.) ...так и не были переведены на европейские языки»²⁰.

В то же время есть свидетельства резкой деградации арабской криптографии после гибели Византийской империи, этого «*золотого моста между Западом и Востоком*», по образному выражению К. Маркса.

1.6. Вязь и литорей. Вновь обратимся к вязи и литорее, применявшимся в московской дипломатической тайнописи второй половины XVI столетия.

По внешнему виду вязь условно разделяют на простую и сложную. Образцы простой вязи можно наблюдать на иконах: там надписи до сих пор часто делают именно простой вязью. Это древнейший тип вязи. По мнению исследователей, он уже в X веке проник в Россию из Византии. Пример обширной надписи, выполненной простой вязью, даёт нам знамя народного ополчения, собранного К. М. Мининым и Д. М. Пожарским и освободившим Москву в 1612 году. Это историческое шёлковое знамя хранится в Оружейной палате Московского Кремля, оно представлено на *рис. 1.10*. Здесь надпись вязью содержит библейский текст.

Пример сложной вязи приведён на *рис. 1.11*. Расшифровка надписи представляет собой текст молитвы «Достойно есть». В этом можно убедиться, обратившись к *Приложению 3*.

Есть русские образцы сложной вязи, в которых специалисты обнаруживают элементы знаков уйгурской, арабской и даже коптской (египетской) письменности. Видимо, впечатления от знакомства с начертаниями восточных систем письма писцы отражали в своей вязи. Такой пример приведён на *рис. 1.12*. Он взят из статьи Д. А. Морозова²¹, посвящённой оригинально оформленной Псалтири второй половины XV века.

²⁰ Кан Д. Взломщики кодов. М., 2000, с. 15, 22, 25.

²¹ Россия и христианский Восток. М., 2004. Вып. II–III, с. 92.



Рисунок 1.10. Знамя Ополчения 1612 г.



Рисунок 1.11. Запись вязью молитвы «Достойно есть»



Рисунок 1.12. Фрагмент текста Псалтири

По мнению М. Н. Сперанского, тайнопись вязью следует признать русской по происхождению. Такой способ выработался, вероятно, в московских приказах. Об этом свидетельствуют азбуки-прописи, содержащие вместе образцы скорописи и вязи.

Трудно сказать, какой тип вязи использовал гонец Андрей Иванов в своих донесениях в Москву. Бесспорно лишь, что эффективное применение вязи с целью тайнописания предполагало нали-

чие значительного опыта её использования как у исполнителя, так и у читателя.

Обратимся теперь к литорее. Простая литорея представляет собой шифр подстановки. Так называют шифр простой замены, в котором шифруемый алфавит совпадает с азбукой шифровых обозначений. Простая литорея составляется так: согласные буквы русского алфавита записывают в таблицу (подстановку) следующего вида:

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

Шифровыми обозначениями букв первой строки считают подписанные под ними буквы второй строки, и наоборот — в первой строке записаны шифровые обозначения стоящих под ними букв второй строки. Остальные буквы не меняются, т.е. шифровые обозначения этих букв совпадают с самими буквами.

Легко увидеть закономерность в простой литорее: буквы первой строки таблицы записаны по их порядку в алфавите, а буквы из второй строки — в обратном порядке.

Название «литорей» сохраняется и для шифров, отличающихся от приведённого здесь лишь другой разбивкой согласных на пары.

Можно предположить также, что вязь и литорея для зашифрования сообщения применялись вместе.

1.7. Государственное строительство при преемниках Ивана III. Создание действенной системы управления, необходимой для обеспечения жизнеспособности единого государства, неизменно сохранялось как приоритетное направление деятельности при всех преемниках Ивана III.

В XVI столетии в Московском государстве начинает складываться приказная система управления. Постепенно оформляется Посольский приказ.

В 1547 году великий князь Иван IV Васильевич венчался на царство, на него возложили бармы (своеобразное ожерелье, оплечье),