Криптография в России.

Вопрос о том, использовались ли криптографические методы сокрытия информации в Древней Руси до сих пор остается дискуссионным.

Чаще всего для сокрытия информации на Руси использовали некириллические азбуки, чаще всего греческую, а с XVI-XVII вв. латинскую. Сообщение просто записывалось греческими буквами, но на русском языке, что представляло весьма примитивный способ шифрования сообщения.

Другой весьма распространенной системой сокрытия информации сообщения была **тахиграфия** – изменение начертаний букв, когда писалась или часть буквы, или наоборот, ее написание дополнялось новыми элементами. Сообщение нередко записывали справа налево или вверх ногами. Часто тахиграфия совмещалась с использованием иностранных алфавитов.

Существовали и шифры простой замены, примером которых может служить «**литорея**», предполагавшая замену согласной на противоположную (б-щ, в-ш), при этом замена гласных не производилась. Первый дошедший до нас документ, содержащий данный тип криптографической системы, датируется 1229 годом. Одним из видов литореи была «**мудрая литорея**», предполагавшая замену не только согласных но и гласных

Использовалась на Руси и система цифровых обозначений. Так как каждой цифре кириллического алфавита в то время соответствовала буква, то для того, чтобы зашифровать сообщение, обычно каждую букву незашифрованного текста представляли в виде двух букв, дающих в сумме исходное значение. Буквы, не имеющие цифровых обозначений, оставались незашифрованными.

Информации об использовании криптографии до XVI века в дипломатии и военном деле на Руси нет. Дошедшие до нас криптографические приемы были изобретением переписчиков книг и ученых монахов и не имели значительно практической ценности. В этот период не было особой необходимости в криптографических средства защиты письменных сообщений, однако со формированием единого централизованного государства, потребность в них значительно возросла.

Активная внешнеполитическая деятельность Ивана Грозного и связанные с ней войны оказали значительное влияние на становление и развитие тайнописного дела.

Активная внешнеполитическая деятельность Петра требовала создания регулярной криптографической службы, способной обеспечить эффективную защиту собственных сообщений и вскрытие дипломатической переписки других государств. Однако отсутствие опыта в этой области и незначительное число достаточно образованных для подобного рода деятельности людей, не позволяло быстро выйти на европейский уровень криптографии. Первоначально, функции криптографической службы выполняет Посольский приказ, позже параллельно с ним начинает функционировать Походная посольская канцелярия при Петре. С учреждением Коллегии иностранных дел, в ней были сконцентрированы все основные криптологические службы страны.

Складывавшейся криптологической службе России требовался опыт, который мог быть приобретен лишь со временем, поэтому, несмотря на все усилия Петра, российская криптология, хоть и сделала гигантский рывок вперед, по сравнению с предшествующим периодом, вышла на европейский уровень лишь в 40-е годы XVIII века.

Новый этап в развитии русской криптографической службы связан с именем А.П. Бестужева-Рюмина. Это потребовало создания сильной криптоаналитической службы, для взлома иностранных шифров, в чем и состоит основная заслуга Бестужева. Он впервые в отечественной практике привлекает к криптоаналитической деятельности профессиональных ученых-математиков,

Однако в течение второй половины XVIII века никаких существенных изменений в Российской криптологии не происходило, что отражало общеевропейскую тенденцию. Шел лишь количественный рост криптологических знаний, усложнялись шифры В середине XVIII века русская криптологическая служба достигла европейского уровня и в некоторых моментах превосходила его. Если составление собственных шифрсистем, прежде всего для русского алфавита, еще отставало, то криптоаналитика была на высоте. С этого времени русская криптология окончательно занимает одну из ведущих позиций в криптологии европейской

и является эффективным орудием в руках дипломатических и военных ведомств страны.

В первой половине XIX века главой русского криптологического ведомства П.Л. Шиллингом был создан первый русский биграммный шифр. Вследствие сложности этот шифр применялся лишь для наиболее значимой дипломатической переписки и был весьма устойчив ко взлому. Позже был создан биклавный шифр – сложная разновидность шифра многозначной замены с использованием 2 ключей, продолжавший использоваться на протяжении всего XIX века.

Появившаяся в начале XX века радиосвязь значительно повышала требования к стойкости армейских шифров, в условиях когда почти каждое сообщение могло быть перехвачено противником. К началу Первой мировой войны для русской армии был создан сложный шифр двойной перестановки с частой сменой ключей, представлявший проблему для самых опытных криптоаналитиков того времени, но этот шифр к началу войны поступил лишь в некоторые части, что вызвало колоссальную неразбериху – ведь в одних частях все еще действовал старый шифр, а в других он был уничтожен и приходилось передавать сообщения открытым текстом. Только в 1916 году удалось более-менее наладить своевременное снабжение частей новым шифрами и установить в вопросе секретной связи некоторое взаимодействие, однако события 1917 года и последовавшая гражданская война привели к почти полной ликвидации криптографических служб России

В результате к 1920-м годам в России не существовало криптологичекого центра, способного обеспечить еще более возросшую потребность в защите информации. Предстояло воссоздать подобные службы практически с нуля, поэтому в мае 1921 года на базе криптографического отдела ВЧК был создан Спецотдел по криптографии при данном ведомстве (восьмой спецотдел). Спецотдел играл роль центрального криптографического органа.

С окончанием Второй мировой войны, Советский Союз вступил в острое противостояние с Западом, что в значительной степени способствовало развитию отечественной криптологии, занявшей лидирующие позиции в XX веке.