Комитет по образованию Администрации г. Улан-Удэ
Муниципальное бюджетное общеобразовательное учреждение
«Вечерняя (сменная) общеобразовательная школа № 3»

Конкурс рефератов «Петр I»

в рамках декады МО естественно-математического цикла

Тема: **«Цифирные азбуки» Петра I»**

Автор: Филиппов Александр,
учащийся 10 «б» класса
Руководитель:
Куриганова А.В.,
учитель информатики

2021 г.

Оглавление

Введение

В 2022 году исполнится 350 лет со дня рождения первого российского императора Петра Великого**.** Петр I вошел в историю как великий реформатор. Главным итогом его преобразований стало преодоление отставания России от европейских держав в военной, экономической и политической областях. Он коренным образом изменил структуру государственного управления, создал боеспособную армию и флот, при нем произошел прорыв в экономике страны, было создано множество предприятий, мануфактур, оружейных заводов, металлургических и горнодобывающих предприятий, верфей и т.д. Серьезный импульс к развитию получила внутренняя и международная торговля. По его инициативе была учреждена Академия наук, открывались учебные заведения, сотни молодых людей отправились учиться за границу. С другой стороны, в Россию во множестве приглашались иностранные специалисты.

Разумеется, эффективное государственное управление, военные победы и дипломатические успехи были бы невозможны без активной криптографической деятельности. Петр это отлично осознавал и уделял криптографии как надежному средству сохранения государственных секретов большое внимание.

1. **Защита информации на государственном уровне**

Если говорить о методах защиты информации во времена Петра I, то первое время основным была физическая защита, которая целиком и полностью возлагалась на почтальонов. Россия к концу XVII века стала крупнейшей европейской державой с рассредоточенными по всей огромной территории административными центрами. Поэтому обязанность почтальона по доставке пакетов с ценными документами и нетронутыми печатями кажется не самой легкой.

Широкое реформирование армии поставило перед Петром I задачу развитие систем управления войсками как на маневрах, так и короткие промежутки мирного времени. В 1695 и 1696 годах, во время похода на турок, была организована первая военно-полевая почта под руководством почтмейстера А. А. Виниуса. У всех отправлений этой почты был статус чрезвычайных.

В начале XVIII века простой физической защиты почтальона от посягательств на ценную корреспонденцию стало не хватать, и Петр обратил свой взор на криптографию. Причиной стало появление многочисленных дипломатических представительств Российской империи за рубежом, а также Северная война со Швецией, в ходе которой приходилось управлять войсками на большой территории. И в том, и в другом случаях была велика опасность попадания стратегической информации в руки неприятеля.

Сначала функции криптослужбы выполнял «Посольский приказ», позже параллельно с ним начала функционировать «Посольская канцелярия» при Петре I. 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.

На должности криптографов и шифровальщиков были «переводчики», которые одновременно переводили с иностранного письма и проводили шифровку-дешифровку документов.

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

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

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

Канцлер и вице-канцлер давали указания по созданию новых шифров, замене обветшалых, обеспечению шифрами корреспондентов — дипломатов, военачальников, других государственных деятелей. Непосредственно им

докладывались отчеты о создании новых шифров и добыче иностранных шифров.

Петр I считал шифры монополией царя российского. Он строго наказывал своих подданных за использование «негосударственных» цифирей. Однако частные лица все же пользовались собственными шифрами. Среди них можно указать царевну Софью Алексеевну, которая использовала шифр в переписке со своим фаворитом князем В.В.Голицыным.

При царе Петре I шифрование сообщений для армии и флота было поставлено как следует. В частности, были разработаны и соблюдались строгие меры секретности. Так, ключи от шифров передавали только из рук в руки. Например, ключи для переписки с царем можно было получить только от Петра I лично. В исключительных случаях сам ключ, либо его части можно было получить с нарочными. Их предварительно упаковывали в специальные конверты, опечатывались несколькими сургучными печатями и обязательно указывали имя нарочного. При получении такого сверхсекретного письма корреспондент должен был оповестить о благополучном получении ключей и только после этого канал связи начинал работу.

В 1716 году был принят «Устав воинский», первый в истории России документ подобного рода. В соответствии с Уставом были впервые учреждены должности «адъютантов, ординарцев, курьеров для передачи и доставки секретных донесений», а также обновлены «Правила действия военно-полевой почты». Причем редактуру вносил лично Петр I. Теперь военные почтальоны отвечали за оперативную доставку шифрованной корреспонденции между подразделениями армии, флота и Военной коллегией с Адмиралтейств-коллегией.

Со временем Петр I ввел еще одну инновацию – на флоте появилась служба наблюдения и связи. В качестве связных были скоростные суда, на которые также возлагались разведывательные функции наблюдения за противником. Стрельба, световая индикация и флажки в руках сигнальщика использовались для дистанционной передачи данных, состоящих обычно из

нескольких предложений. Нередко для ускорения передачи могли применять сразу два или три флага, при этом каждый флаг (комбинация флагов) зашифровывал фразу. На пунктах приема были предусмотрены кодовые книги со сводами сигналов для расшифровки. Эти инновации были очень успешно использованы летом 1720 года, когда Россия столкнулась с объединенными военно-морскими силами англичан и шведов на Балтике. Своевременное обнаружение сил противника и оперативное оповещение позволило нашим кораблям эффективно защитить берег. А 28 июня того же года около 60 русских галер атаковали шведов у мыса Гренгам, да так лихо, что англичане побоялись сунуться в эту заварушку. В итоге большая часть шведов побитыми ушла домой, а русский флот пополнился четырьмя трофейными фрегатами. Это была всего лишь одна из славных страниц русского галерного флота – наши моряки регулярно высаживались в тылу шведов, уничтожая материальную базу противника. Все это было возможно благодаря развитой и эффективной морской службе наблюдения и связи.

2 «Пустышки», номенклаторы, «суплементы»…

Теперь рассмотрим шифрсистемы, которые применялись в эпоху Петра I. Как и в прежние годы, основным шифром на Руси была простая замена, то есть знаки открытого текста заменялись на буквы (при этом буквы могли принадлежать как алфавиту открытого текста, так и другой азбуки), цифры или специально придуманные знаки. При этом следует отметить, что в шифрах Петровской эпохи употреблялись только привычные нам арабские цифры, так как в начале XVIII века Петром была выведена из употребления архаичная буквенная кириллическая нумерация, заимствованная у греков. В качестве знаков шифрованного текста употреблялись и буквенные сочетания.

Тексты, которые надо было зашифровать, могли быть написаны на русском, французском, немецком, а иногда даже греческом языках. Как известно Петр прекрасно владел несколькими европейскими языками, в то

же время на государственной службе состояло много иностранцев, именно в переписке с ними в основном использовались немецкий и французский. При этом следует отметить, что с точки зрения стойкости предпочиталось использовать русский язык. За границей было очень мало людей, владевших русским, а знание лингвистических особенностей языка может существенно помочь криптоаналитику в дешифровании.

Новым для российских шифров петровского времени стало наличие во многих из них «пустышек» — знаков шифрованного текста, которым не соответствует никакой знак открытого текста, то есть они не несли никакого смысла. Как правило, пустышек было немного, обычно 5-8 знаков. Пустышки увеличивает стойкость шифра, так как они дают криптоаналитику неверную информацию о количестве знаков в алфавите открытого текста, разбивают структурные лингвистические связи открытого текста и изменяют статистические закономерности, то есть именно те свойства текста, которые используют при дешифровании шифра простой замены.

Кроме того, пустышки увеличивают длину шифрованного текста по сравнению с открытым, что усложняет их взаимное сопоставление. Кроме того, в некоторых случаях отдельные знаки применялись для зашифрования точек и запятых, для этого также могли использоваться пустышки. Это особо оговаривалось в кратких правилах пользования шифром.

Вскоре к обычному алфавиту простой замены стали добавлять обозначения для наиболее употребительных слогов, слов и целых фраз, то есть номенклаторы. Петровские номенклаторы были весьма простыми, они содержали небольшой словарь, называвшийся «суплемент» и содержавший некоторое количество слов (имен собственных, географических наименований или каких-то устойчивых словосочетаний, которые могли часто использовать корреспонденты, использовавшие данный шифр).

Шифр Петровской эпохи представлял собой лист бумаги, на котором от руки был написан ключ – таблица замены (обычно под горизонтально расположенными в алфавитной последовательности буквами кириллицы или

иного алфавита подписаны соответствующие элементы шифроалфавита), а также суплемент (если это был номенклатор). Ниже могли помещаться пустышки и краткие правила использования шифра.

Еще одной особенностью петровских шифров является то, что шифралфавит мог составляться из символов разных типов, например, смеси букв разных алфавитов, цифр и т.д.

Главным новшеством стало применение более сложных, чем простая замена, шифров. Так в 20-х годах XVIII века от шифров простой замены переходят к замене пропорциональной, когда наиболее часто встречающимся знакам открытого текста присваиваются несколько шифробозначений, что затрудняет использование «классического способа» криптоанализа – частотного анализа. Еще раньше, примерно с 1708 года, в России начали применять шифры разнозначной замены – когда для замены одного знака открытого текста используется один или два знака шифртекста. Следует отметить, что шифры такого типа, являясь более стойкими, чем «классическая» простая замена, в то же время и более чувствительны к ошибкам при шифровании.

А в 1719 году русский шифр все-таки вскрыли… И сделали это наши многовековые заклятые друзья британцы в одном из своих «черных кабинетов». Раскрыт был один из шифров простой замены, что, однако, не стало трагедией – в начале 20-х годов в России уже вошли в употребление шифры пропорциональной замены. А на этот алгоритм зубов у англичан тогда не хватило.

Эпоха Петра I стала временем прорыва России в шифровальном деле и криптоаналитической работе. Империя выбилась в мировые лидеры в этой сфере, положительные результаты не заставили себя долго ждать.

3. Высочайший криптоанализ

Именно в Петровскую эпоху свои первые шаги сделал российский криптоанализ, стали развиваться методы тайного перехвата информации, осуществлялась агентурная добыча криптографических секретов противника. При этом особое внимание уделялось добыче открытых текстов шифровок, так как простейший прием «открытый текст – шифрованный текст» в 99% раскалывал любой шифр той эпохи. В этом очень помогли многочисленные трофеи, которые завоевала русская армия на полях Северной войны. Важно отметить, что занимался оценкой стойкости российских шифров не кто-нибудь, а сам царь!

Приведем две цитаты. Петр писал фельдмаршалу Огильви по поводу одного шифра (цифири, как их тогда называли): «А которую вы перво прислали, и та не годна, понеже так, как простое письмо, честь можно». И еще одна нелестная оценка царя: «Сия цифирь зело к разобранию легка».

Стали проявлять в России интерес и к шифрам иностранных государств. О регулярном дешифровании иностранной переписки речь пока не шла, однако заинтересованность в получении информации таким методом уже была. Русским дипломатам, разведчикам и другим представителям за границей предписывалось добывать любую информацию, касающуюся шифров, организации связи, открытых текстов (против атаки «открытый текст – шифрованный текст» подавляющее большинство шифров того времени было не устойчиво). На этих лиц и их зарубежную агентуру также возлагалась задача организации перехвата иностранных сообщений за границами России.

В это время пришло понимание важности такого источника информации, как шифрованная переписка иностранных государств. Полученная информация могла быть весьма полезна российскому руководству, дипломатам, военным. Велся перехват сообщений и внутри России, совершенствовались методы перлюстрации, осуществлялась цензура, вводились ограничения на почтовое сообщение.

Заключение

В петровскую эпоху в России шифрование стало основным средством защиты информации, хотя продолжали использоваться и другие методы: стеганография, физическая защита, условная сигнализация и т.п. При этом, если в прежние времена практически вся шифрпереписка была посвящена дипломатическим вопросам, то при Петре активно шифровалась и военная и внутриполитическая информация.

Для организации связи были созданы ряд учреждений – Кабинет его императорского величества, Посольская канцелярия, Коллегия иностранных дел и т.д. – со строгим разделением функций. Деятельность этих учреждений регламентировалась законодательно. Широко практиковались организационно-административные методы защиты информации, такие как особый подбор кадров для осуществления криптографической деятельности и строгий контроль за их работой, организация пропускного режима в помещения, где производилось шифрование и расшифрование или хранились шифры, обеспечение охраны гонцов и курьеров и т. д. Из новшеств в области связи отметим, что для обеспечения управления флотом и прибрежными районами страны в качестве средства связи стали широко использоваться суда.

В целом отметим, что Петр Великий был первым из российских правителей, кто предельно ясно осознал важность криптографической деятельности для обеспечения безопасности государства. Во время его правления впервые в истории отечественной криптографии к осуществлению криптографической деятельности (в том числе к составлению шифров) привлекалось все высшее руководство России, включая царя.

Список использованной литературы

1. Петр Первый и криптография // BIS Journal. — 2018. — №1(28). — С. 56-59.
2. Астрахан В. И., Гусев В. В., Павлов В. В., Чернявский Б. Г. Становление и развитие правительственной связи в России.
3. Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Криптография: страницы истории тайных операций.
4. Ларин Д. А. Криптографическая деятельность в России при Петре Великом
5. Дзен// Цифирные азбуки Петра I. — [Электронный ресурс].