
Вадим Гребенніков
Російська криптологія
Гребенніков В.В.
ІСТОРІЯ КРИПТОЛОГІЇ & СЕКРЕТНОГО ЗВ'ЯЗКУ
Історія спецзв'язку

Вадим Гребенников

Російська криптологія

«Издательские решения»

Гребенников В.

Російська криптологія / В. Гребенников — «Издательские решения»,

ISBN 978-5-4493-0780-4

Книга розповідає про історію народження й розвитку російської криптології, телеграфного та радіозв'язку, а також утворення криптологічних служб Російської імперії та їхню боротьбу у «полюванні» за шифрами супротивника у контексті розвитку дипломатичних взаємовідносин з іншими країнами. Книга побудована виключно на відкритих матеріалах, зібраних автором із надрукованих книг та мережі Інтернет. Офіційна веб-сторінка книги: http://cryptohistory.ru

ISBN 978-5-4493-0780-4

Содержание

Російська криптологія
Історія спецзв'язку

Вадим Гребенніков

ISBN 978-5-4493-0780-4
Создано в интеллектуальной издательской системе Ridero
.А.. Б.. В.. Г.. Д.. Е.. Ж.. З……С Т У Ф Х Ц Ч Ш Щ. Ы. Ю.. Я. —
27 26 25 24 23 22 21 20……10 9 8 7 6. 5. 4 3 31 30 29 28 0

Роль «0» зводилася до поділу двозначних і однозначних цифр. При використанні ключа «3162» текст «УКРАИНА» перетворюється у шифротекст «11181729211533»:

1. Стародавній тайнопис

Найбільш ранньою з відомих за староруськими пам'ятниками писемності систем тайнопису була система *«иных письмен»*. У цьому виді тайнопису букви кирилиці замінювалися буквами інших алфавітів: глаголиці, грецької, латинської, пермської абетки.

Вживання грецького тайнопису пов'язують з певною модою, яка прийшла до кінця XVI ст. Поява ж цього способу тайнопису була обумовлена, з одного боку, другим південно-слов'янським впливом, що ніс деякі навики і грецького письма, ближчого півдню слов'янства, ніж Русі, а з іншого – пожвавленням стосунків Московської Русі з греками, що розпочалися з кінця XIV ст.

Вживання латинської азбуки як тайнопису відноситься до пізнішого часу та обумовлене західноєвропейським впливом, що посилився. У розповсюдженні цього виду тайнопису, що трапляється в рукописах XVI і XVII ст., ймовірно, відому роль грала школа з її латинською мовою викладання.

Дещо відособлене місце серед інших алфавітів у застосуванні до тайнопису займає пермська абетка. Ця абетка, що була створена пермським єпископом Стефаном на основах сучасного кириличного й грецького алфавітів, не набула практичного застосування та вже у XV ст., як маловідома, стала тайнописом. Але й в цій якості вона не була широко поширена.

Другою після системи *«иных письмен»* системою тайнопису, відомою з російських рукописів, є система «змінених знаків», зафіксована вже у XIV столітті. Виділяють два її різновиди: а) систему знаків, змінених «шляхом надбавок» до звичайних зображень, б) побудовану на принципі, схожому з грецькою «тахіграфією».

«Тахіграфія» – це зміна написання букв, коли писалася або частина букви, або навпаки, її написання доповнювалося новими елементами. Повідомлення нерідко записували праворуч-ліворуч або догори ногами. Часто «тахіграфія» сполучалася з використанням іноземних алфавітів.

Перший різновид такого тайнопису був відкритий вченим М. Сперанським у Смоленському Псалтирі 1395 року. За його свідченням цей Псалтир Онезького Хресного монастиря зберігався свого часу в Архангельському місцевому відділенні Церковно-археологічного комітету. Його писар, чернець Лука, що чудово володів мистецтвом письма, любив, мабуть, і тайнопис. У цьому рукописі він застосував три види тайнопису: один – змінених зображень, другий – цифра рахункова, третій – система в'язу.

Використовували писарі стародавніх рукописів і систему умовних алфавітів. Як правило, в їх основі лежали вже відомі: грецький, глаголичний, кириличний, в яких привносилися якісь зміни або доповнення. Проте траплялися в рукописах і оригінальні умовні алфавіти, побудовані або за якимсь певним принципом, або абсолютно довільних зображень.

Зразком алфавіту, придуманого спеціально для тайнопису, притому за особливим принципом, може служити ключ до тайнопису, зображений на окремому листі другої половини XVII ст. (Збори Великої Патріаршої бібліотеки №93).

Тут тайнопис полягає в заміні звичайних букв трикутниками і чотирикутниками, запозиченими з грат, складених з двох паралельних ліній, пересічених двома такими ж лініями під прямим кутом. У отриманих клітинках поміщено по чотири й по три букви в порядку азбуки: у тайнописі букви замінюються, при цьому перша – простим косинцем, а наступні – тим же косинцем з однією, двома або трьома крапками, зважаючи на місце букви в нім. Оскільки при такому розміщенні букв у клітинах вся азбука не могла вміститися, то в цьому тайнописі не виявляється знаків для таких букв кирилиці, як «ш», «ь» тощо.

Наступний вид тайнопису, який використовувався писарями в російських рукописах, – це «система замін». Виділяють два види для такого тайнопису: «просту літорею» (від лат.

litera – буква) і «мудру літорею», а також як варіант цієї останньої – тайнопис «в квадратах». «Проста літорея» полягала в тому, що кожен із десяти по порядку азбуки приголосних, поставлених в одному ряду, замінювався відповідною нею буквою в другому такому ж ряду, що складався з останніх десяти приголосних, що йдуть в зворотному (справа наліво) порядку.

Перший документ, який дійшов до нас та містив даний тип криптосистеми, датувався 1229 роком. Однак по-справжньому широке поширення вона здобула наприкінці XVII століття. Ключ до «простої літореї» такий:

.Б..В. Г Д Ж З. К Л М Н

Щ Ш Ч Ц Х Ф Т С. Р П

Слово «УКРАЇНА», записане «літореєю», виглядає так: «УТМАІПА».

Більш складним різновидом «літореї» була так звана «мудра літорея», де всі букви кириличної абетки, включаючи голосні, замінялися на інші букви. До цього ж виду тайнопису, який використувався у XVI – XVII ст., відносився тайнопис «в квадратах», де таблиці заміни букв виписувалися у вигляді квадратів. Нерідко писарі вдавалися до написання фраз у зворотному порядку, складаючи своєрідні криптограми, або не дописували букви -подібний шифр називався *«полусловицей»*.

Цифрова система тайнопису, яку тоді називали *«счётная»* або *«цифирная»,* заснована на вживанні букв як цифр і на різних практичних діях з ними, була дуже поширеною і, до того ж, із досить раннього часу. Слід сказати, що в староруських рукописах траплялися різні її види: проста та складна цифрова система, описова система, система особливого застосування арабських цифр, система значків, тобто з використанням різних значків для позначення цифр-букв. Цифровий тайнопис існував на Русі вже на самому початку XIV ст.

Простий цифровий тайнопис полягав у тому, що для кожної цифри-букви, яка відповідала бажаній в звичайному письмі букві, давалося декілька переважно однакових доданків. Так, щоб отримати потрібну букву, треба було провести складання, а отримана сума, зображена відповідною цифрою-буквою, і була шуканою буквою. Рідше сума складалася з різних цифр-букв, причому кожна група цифр-доданків відділялася яким-небудь знаком або пропуском від сусідніх. Букви, що не мали цифрового значення, залишалися незмінними.

Арабські числа почали використовуватися як тайнопис лише з того часу, як вони почали входити у вживання у російській писемності, тобто з другої половини XVI ст. на російському південному заході і з початку XVII ст. на північному сході.

До інших систем тайнопису, відомих за староруськими рукописами, належав *«моно-кондил»,* різні прийоми образного й фігурного письма, а також *«акростих»* (вірш, в якому початкові букви рядків утворюють слово або фразу). *«Акростих»* – типовий для європейської середньовічної письмової культури прийом організації поетичного тексту – входив в арсенал художньо образотворчих засобів староруських авторів уже з кінця XI ст.

Довгий час державний тайнопис у працях вітчизняних учених, іменувався «дипломатичним тайнописом». Уперше такий термін був введений ученим Поповим, який у 1853 році опублікував працю «Дипломатичний тайнопис часів царя Олексія Михайловича з доповненням до нього». Слідом за ним і інші дослідники російського тайнопису почали називати листування при російському дворі «дипломатичним тайнописом», а шифри, якими воно велося, «дипломатичними».

Слід, проте, відзначити, що таємне дипломатичне листування складало лише частину (правда, велику) шифрованого листування при дворі, яке разом з дипломатичним, стосувалося військових питань, а також внутрішньодержавних справ. Але саме в сфері дипломатії, з властивими їй специфічними рисами і особливостями, в Росії майже впродовж двох сторіч проходило основне становлення криптології як державно-значущої справи. Політична боротьба, політична гра – іншими словами, ведення «великої політики» немислиме без охорони державної таємниці.

Активна зовнішньополітична діяльність царя Івана IV Васильовича (Грозного) та пов'язані з нею війни вплинули на становлення й розвиток тайнописної справи. Роком народження російської криптологічної служби можна вважати 1549 рік, коли була утворена *«Посольская изба»,* пізніше названа «Посольським наказом», при якому працювала *«цифирная»* палата таємних справ. З моменту його утворення в Росії почали активно використовувати криптологічні методи в дипломатичному та військовому листуванні.

Назву «цифирної» палата одержала, можливо, за старою алфавітною системою запису чисел. Виділення цифр та й власних імен у тексті раніше робилося за допомогою «титлу», спеціального знака, який проставлявся над рядком. Шифри доводилося виділяти в повідомленні так само, як і цифри, тобто «титлувати» їх. Тому цілком зрозуміла назва шифру «цифрою», тобто текстом, що вимагає спеціального прочитання. Втім, можливо, що слово «цифирна» у назві палати була буквальним запозиченням французького слова «*chiffre*», що означало як шифр, так і цифру.

З кінця XVI ст. російські посли за кордоном почали отримувати шифри у вигляді таблиць заміни, які потрібно було *«вытвердить гораздо памятно».* У наказі царя Федора Іоановича, даному у 1589 році послу Миколі Воркачу, йому доручалося *«писать письма мудрою азбукою, чтоб оприч Царского величества никто не разумел».* У тій азбуці кожна буква замінювалася своїм особливим знаком.

«Подъячие Посольского приказа», що підтримували зв'язки з царськими представниками закордоном, нерідко користувалися шифрованим листуванням, яке називали *«затейным письмом».* Ключ до розшифрування цих послань не записувався, його заучували напам'ять. Існували різні варіанти таємного письма, але за правилами конспірації ніхто з підданих не повинен був знати усіх варіантів тайнопису.

З початком правління династії Романових (1613) зміцнюються основи феодального ладу. У 1619 році з польського полону повернувся батько царя Михайла Романова Федір, постриженний Борисом Годуновим у монахи під іменем Філарета. Він особисто займався справами «Посольського наказу» та навіть розробляв дипломатичні шифри. Шифри, що використовувались у той час, були шифрами простої заміни та перестановки.

Самі перестановки були достатньо простими. Наприклад, відкритий текст розбивався на склади, після чого в них здійснювалася перестановка букв. Так слово «УЖГОРОД» перетворювалося у слово «ЖУОГДОР».

У 1633 році патріарх Філарет написав *«для своих государевых и посольских тайных дел»* особливу абетку і *«склад затейным письмом».* Зберігся наказ російському представнику у Швеції Д. Францбекову, з якого видно, що при складанні повідомлень царю посол повинен був використовувати тайнопис. Наказ закінчувався таким чином: *«Да что он, Дмитрий [Францбеков], будучи в Свее [Швеції], по сему тайному наказу о тех или иных о наших тайных делах и наших тайных вестей проведает и ему о всем писати ко государю царю и великому князе Михаилу Федоровичу всея Руси к Москве по сему государеву тайному наказу ~~затейным~~ закрытым письмом».*

До наших часів дійшла чернетка цього наказу, у якому слово *«затейным»* закреслене і замінене *«закрытым».* Отже, можна дійти висновку, що в Росії тайнопис перетворився в один із засобів збереження державних таємниць.

Так, в інструкції російському агенту в Швеції Дмитру Андрєєву говорилося: *«Лета 7143 (1653) декабря 15 день… А про те тайные дела и про затейное письмо подъячий Иван Исаков и иной никто отнюдь не ведал, и чёрные 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, подъячий Иван Исаков и иной никто однолично не проведал».*

Приведемо також витяг з присяги перекладача-шифрувальника кінця XVII століття: *«… 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 посиленні центральної влади в роки правління царя Олексія Михайловича (1629—1676) застосування шифрів поширюється. У 1654 році цар утворив *«Приказ великого государя тайных дел»,* яким керував особисто, а бояри до таємних справ не допускалися. Як писав Г. Котошихин, «А *устроен тот Приказ при нынешнем царе, для того чтоб его царская мысль и дела исполнилися все по его хотению, а бояре б и думные люди о том ни о чем не ведали».*

Головна посадова особа наказу – *«тайный дьяк»* – мав титул *«дьяка в государевом имени»,* що означало право підписувати укази від імені царя. Головним завданням наказу був негласний контроль над вищими посадовими особами. *«Подъячие приказа»* наглядали за воєводами під час війни і посилалися з посольствами закордон: *«и те подьячие над послы 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 цар, дуже освічений для свого часу, особисто також використовував шифри і в своєму приватному листуванні. Посли і резиденти завжди забезпечувалися шифрами. Наприклад, у 1673 році резидентом у Річ Посполиту (Польща) був призначений полковник В.М.Тяпкин. По дорозі у Вільно його наздогнав царський гонець і вручив йому *«знаки тайнописи и повеление царское пользоваться ими для донесений».*

У державній криптології отримують розвиток і деякі інші способи тайнопису, відомі за стародавніми російськими рукописами, наприклад, такі як «мудра літорея». Цим способом, зокрема, був зашифрований текст, відлитий на великому дзвоні Саввіно-сторожевського монастиря під Звенигородом. Зашифру-вання тексту, за припущенням учених, здійснив сам цар Олексій Михайлович. Дешифрований він був філологами М.Ф.Калайдовічем, А.І.Єрмолаєвим, князем П.П.Лопухіним і ротмістром М.С.Сурідіним.

А.І.Єрмолаєв з приводу цієї обставини висловився 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…»*

2. Криптологія Петра Першого

Першим із російських царів, який чітко усвідомив важливість шифрування депеш і розвитку шифрувальної справи для забезпечення безпеки держави, був Петро I Великий (1672—1725). Епоха його правління характеризується посиленням Російської держави, всіх його управлінських структур, а також структур виконавчої влади. Петро I здійснив ряд найважливіших реорганізацій: організацію мануфактури, будівництво гірських і заводів зброї, розвиток торгівлі, включаючи міждержавну, створення Сенату – найвищого органу влади у справах законодавства і державного управління, створення колегій.

Активна зовнішньополітична діяльність Петра I вимагала створення постійної криптологічної служби, здатної забезпечити ефективний захист власних повідомлень і розкриття дипломатичного листування інших держав. Спочатку функції криптослужби виконував *«Посольский приказ»,* пізніше паралельно з ним почала функціонувати *«Посольская канцелярия»* при Петрі.

Указом від 18 лютого 1700 року на чолі «Посольського наказу» і наказів, що належали до нього, був офіційно поставлений видатний діяч і дипломат раннього періоду петровського часу Федір Олексійович Головін (1650—1706). Він змінив там думного дяка Є.І.Українцева, який у 1699 році був відправлений послом до Константинополя на російському кораблі, що вперше з'явився у водах Босфору.

При своєму призначенні Головін отримав звання «початкового президента державної посольської канцелярії». Як генерал-адмірал Головін одночасно управляв флотом, очолював збройову палату, монетний двір, малоруський наказ. Окрім особистої участі в переговорах з іноземними державами і укладення договорів з ними, Головін керував діяльністю російських послів за кордоном, робив великий вплив на зовнішню політику Росії в період Північної війни. Під безпосереднім спостереженням Головіна працювало «цифирне» відділення.

Вже на самому початку XVIII ст. Петром I була створена *«Походная посольская канцелярия»,* що зосередила в своєму веденні найважливіше політичне листування. Створення її було викликане частими поїздками Петра. *«Походная канцелярия»* була переважно особистою канцелярією імператора, звідки виходили його найважливіші розпорядження по всіх галузях управління. Сюди стікалися на його вирішення справи зі всіх відомств. Але головною її функцією було ведення дипломатичних справ, чому до її назви додавалося слово *«посольская».*

Перша згадка в документах про «Похідну канцелярію» відноситься до 1702 року. У цей час цар відправився «в похід» до Архангельська. У поїздці його супроводжував начальник *«Посольского приказа»,* перший міністр Ф.О.Головін. Незважаючи на те, що всі державні справи продовжували проходити через *«Посольский приказ»,* а *«печатанье государственной печатью грамот»* повинно було далі знаходитися під контролем бояр, найбільш важливі справи вже вирішувалися в Архангельську у Петра I.

У 1706 році *«Посольский приказ»* очолив Гаврило Іванович Головкін (16601734), який був родичем Петра I по материнській лінії. Після смерті Головіна, 23 вересня 1706 року помічником Головкіна був призначений Петро Павлович Шафіров (1669—1739), який з 1703 року працював «таємним секретарем» при «Похідній канцелярії».

До 1710 року *«Походная канцелярия»* остаточно обґрунтувалася в Петербурзі та з тимчасової установи стала постійною, причому з 1709 року її стали називати просто *«Посольской канцелярией».* Саме там була зосереджена вся робота щодо зашифрування та розшифрування листування Петра I і його наближених з різними кореспондентами, а також утворення шифрів і рекомендацій щодо їх використання.

У період з 1710 по 1718 роки ця Канцелярія стала головним органом зовнішніх стосунків Росії. Компетенція її розширилася у збиток *«Посольскому приказу»,* що залишився в Москві. Зросла чисельність особового складу Канцелярії. У 1709 році Го-ловкін був призначений дер-

жавним канцлером, а Шафіров – віце-канцлером. Саме ці перші особи держави керували діяльністю російської криптослужби.

Канцлер і віце-канцлер давали вказівки щодо створення нових шифрів, заміні застарілих, забезпечення шифрами кореспондентів – дипломатів, воєначальників, інших державних діячів. Безпосередньо їм докладалися звіти про створення нових шифрів і здобич іноземних шифрів.

Стосовно російських *«цифирных азбук»* і ключів 1700-1720-х років, то вони були шифрами заміни, де елементи, відкритого тексту, які надалі будемо називати шифровеличинами, замінюються умовними позначеннями – шифропозначеннями. Тексти, які шифрувались, писалися на російській, французькій, німецькій і навіть грецькій мовах. У різних шифрах шифровеличинами виступали окремі букви, слова і стандартні вирази.

Як шифропозначення використовувалися елементи, як правило, алфавітів, що спеціально складалися з цією метою, які могли бути буквами кирилиці, латиниці, інших абеток (наприклад, глаголиці), цифри, особливі значки. Частина з таких значків, що мали іноді химерні контури, були нейтральні за значенням, інші ж були символами, до нашого часу майже абсолютно забутими та відомими лише вузькому колу осіб, а в ту далеку епоху несли певне смислове навантаження. До цих останніх відносилися й астрологічні символи планет, що одночасно були й символами металів.

У шифрах петровської епохи уживалися тільки індо-арабські цифри, що з'явилося, ймовірно, наслідком того, що саме Петром I на початку XVIII ст. була виведена з уживання архаїчна буквена кирилична нумерація, що застосовувалася до цього. Реформував Петро і кириличне письмо, ввівши новий вигляд шрифтів, які визначають сучасну зовнішність російської писемності. Проте старі графеми продовжували використовуватися як тайнопис.

Вживалися як шифропозначення і буквені поєднання. Таким чином у той час в Росії використовувалися однобуквені, двобуквені, цифрові, буквено-складові шифрозаміни. Перші державні шифри були шифрами простої або взаємно-однозначної заміни, в яких кожній шифровеличині відповідало тільки одне шифропозначення, і кожному шифропозначенню – одна шифровеличина.

У російські шифри даного періоду, як правило, вводяться «пустишки» – шифропозначення, яким не відповідає жодний знак відкритого тексту. Хоча зазвичай для цього використовувалося всього 5—8 шифровеличин як пустушки, зрозуміло, що введення їх у шифротекст, який виходив у результаті заміни елементів відкритого тексту шифропозначеннями, відображало прагнення творців шифрів осмислити дешифрування шифролистування.

Ці пустушки розбивали структурні лінгвістичні зв'язки відкритого тексту і, до певної міри, змінювали статистичні закономірності, тобто саме ті особливості тексту, які використовували, в першу чергу, при дешифруванні шифру простої заміни. Крім того, вони змінювали довжину відкритого повідомлення, що ускладнювало прив'язку тексту до шифроповідомлення. Тому, мабуть, не випадково, за даними Д. Кана, перший такий російський шифр був дешифрований англійцями лише у 1725 році.

Крім того, в деяких шифрах щифропозначення-пустишки могли використовуватися для зашифрування крапок і ком, що містилися у відкритому тексті. Як правило, це особливо обмовлялося в коротких правилах користування шифром, які поміщалися в цих випадках у шифри.

Зовні шифр Петровської епохи являв собою лист паперу, на якому від руки була написана таблиця заміни: під горизонтально розташованими в алфавітній послідовності буквами кириличної або іншої абетки, яка відповідала мові відкритого повідомлення, були підписані елементи відповідного шифроалфавіта. Нижче могли розміщатися пустушки, короткі правила користування, а також невеликий словник, що називався «суплемент» і містив деяку кількість слів (імен власних, географічних найменувань) або якихось стійких словосполучень, які могли

активно використовуватися у текстах, призначених для зашифрування за допомогою даного шифру.

Самим раннім шифром описаного типу була *«цифирная азбука»* 1700 року для листування Колегії закордонних справ (далі – КЗС) з російським послом в Константинополі Петром Толстим. Вона була шифром простої заміни, в якому кириличній абетці відповідав спеціально складений алфавіт. Тут же були два записи. Перший з них: *«Список с образцовой цифирной азбуки, какова написана и послана в Турскую землю с послом и стольником с Толстым сими литеры»*. Другий особливо цікавий: *«Такову азбуку азволнил во 1700 г. написать своею рукою Великий государь по друго диво еси же».* З цього виходить, що автором даного шифру був сам Петро Великий.

У Державному архіві Татарстану знаходиться власноручний лист Петра I Толстому, в якому він пише, що посилає йому шифр для кореспонденцій. Цей шифр мав такі правила користування: «*Сии слова без разделения и без точек и запятых писать, а вместо точек и запятых и разделения речей вписывать из нижеписанных букв…* » (див. таблицю).

А	Б	В	Г	Д	Е	Ж	З	И	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» шифрувалося таким чином: *амнюшнхищахизе*.

Був тут і невеликий словник з іменами деяких державних діячів і найменуваннями декількох військових підрозділів і географічними найменуваннями. Ця обставина також знайшла віддзеркалення в правилах користування, де мовилося: *«Буде же когда случится писать нижеписанных персон имяна и прочее, то оныя писать такими знаки, какия против каждой отмечено, однакож писать все сплош, нигде не оставливая, а между ими ставить помянутыя буквы, которыя ничего не значат».*

Цікавим був і блокнот з шифрами, якими переписувався Петро I. Він був зошитом, листи якого були скріплені мотузком. Розмір зошита: 20х16 см. На кожній його сторінці було записано по одному шифру, всього їх шість:

1) шифр Петра I, який був йому присланий з Колегії закордонних справ до Франції у 1720 році для листування «от *двора ко двору»;*

2) шифр «для *писем к графу Г. и барону П.»;*

3) до князя Долгорукого;

4) до князя Репніна (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.»*

Останній шифр із російським алфавітом відрізнявся від попередніх тим, що як шифропозначення в ньому були використані не букви якого-небудь алфавіту, а числа. Розглянемо ще декілька шифрів раннього типу.

«Азбука, данная из государственной коллегии иностранных дел 3 ноября 1721 г. камер-юнкеру Михаилу Бестужеву, отправленному в Швецию», призначалася для шифрування листів

Бестужева до Петра I і у КЗС. Алфавіт у цьому шифрі був російський із простою буквено-цифрово-значковою заміною без ускладнень. Ця і багато інших *«азбук»* зберігалися в конвертах, на яких були написи про те, для яких цілей призначався даний шифр.

Шифри для листування з царем або КЗС в обов'язковому порядку вручалися всім, хто прямував за кордон з державним дорученням. Це могли бути як дипломати, так і не дипломати. Наприклад, збереглася *«азбука для переписки с господином бригадиром и от гварди майором Семеном Салтыковым, который отправлен к его светлости герцегу Мекленбургскому. Дана Салтыкову 1 декабря 1721 г.».*

Збереглися і шифри канцлера Р.І.Головкіна. Так, шифри, якими користувався канцлер у 1721, 1724 і 1726 роки для листування з різними державними діячами, були підшиті в один зошит. У кореспондентів Головкіна були перші примірники цих шифрів, у канцлера – другі. У цей зошит було включено 17 шифрів. Серед них «Азбука Олексія Гавриловича Головкіна», «Азбука князя Бориса Івановича Куракіна», «Азбука Олексія Бестужева», «Азбука губернатора астраханського пана Волинського», «Азбука Флоріо Беневені» тощо.

Всі ці шифри побудовані однаково, хоча і мають деякі особливості. Так, в «Азбуці Головкіна» російський алфавіт, де кожній приголосній букві відповідало по одному шифропозначенню, а голосній – по два, одне з яких – буква латиниці, а інше – двозначне число. Цікаво, що на відміну від багатьох інших шифрів, цей шифр написаний не в горизонтальних рядках, а по вертикалі у два стовпці. В ньому було 5 пустушок (букви кирилиці), як помічено: *«пустые между слов дабы растановок не знать».* Крім того, були особливі, також буквені позначення для ком і крапок. Таких позначень було також п'ять.

Як умовні позначення використовувалася ціла система цифр, ідеограм, особливих значків, спеціально складених алфавітів. Так, у шифровках Петро I зображував ім'я українського гетьмана Івана Мазепи у вигляді сокири й шибениці після того, як той перейшов до шведського короля Карла XII у жовтні 1708 року, а керівника повстання в 1707—1709 років К. Булавіна – у вигляді шибениці.

Петро I приділяв особливу увагу надійній розсилці шифрів і ключів до них. Він писав одному зі своїх послів: *«При этом посылаем к Вам ключ, и ежели посланный здорово с ним поедет, и о том к нам отпиши, дабы мы впредь нужные письма могли тем ключом писать и посылать».* За указом Петра I кур'єр повинен був *«как можно меньше знать, что он перевозит, и быть довольным оплатой своего труда».* Самому ж кур'єру наказувалося: *«…отнюдь ничьей грамотки не распечатывать и не смотреть».*

Отже, документи свідчать, що в петровську епоху центром, де створювалися шифри, де вони вручалися або звідки вони розсилалися кореспондентам, був спочатку Посольський наказ, потім Посольська похідна канцелярія, а з 1720 року – Перша експедиція КЗС.

Вся діяльність з виготовлення шифрів здійснювалася під безпосереднім керівництвом самого імператора, канцлера і віце-канцлера. Як у майбутньому в КЗС, вже в Посольському наказі існував спеціальний штат, якому доручалося зашифровувати і розшифровувати листування. Текст, який підлягав зашифруванню, переписували належним чином дяки Посольського наказу, а потім перекладачі і секретарі Колегії закордонних справ. Вони ж здійснювали й розшифрування листів.

У ділових паперах нерідко вживалося слово «переклад», коли мова йшла про розшифровані листи, і згадувалися «перекладачі» – особи, що займалися не тільки власне перекладом кореспонденції, але й її розшифруванням. У Посольському наказі, наприклад, перекладачем польських листів був Голембовський. Він же «перекладав», тобто розшифровував листи, написані тайнописом, які приходили з Польщі. П.П.Шафіров, посилаючи Головкіну листа польських міністрів, писав: «А *цифирь такая, чаю, есть у Голембовского».*

Ключ до шифру вручали безпосередньо тій особі, з ким належало листуватися. Проте частини ключа могли пересилатися з нарочними. Для цього їх упаковували в конверт, який

опечатувався декількома сургучними печатками. На конверті іноді писалося ім'я нарочного. Так, у 1709 році Я. У. Полонському було доручено стежити за рухом війська бобруйського старости та не допускати його до з'єднання з корпусом шведського генерала Крассау. Полонський був зобов'язаний застосовувати шифр. «При *этом посылаем к Вам ключ,* – писав Петро, – *и ежели сей посланный здорово с ним поедет, и о том к нам отпиши, дабы мы впредь нужные письма могли тем ключем писать и посылать».*

Повідомлення кореспондентів, отримані КЗС, читалися секретарями експедиції при отриманні їх з пошти, написані шифром розбиралися ними або підпорядкованими ним нотаріусом-реєстратором, канцеляристом і копіїстами. Після цього секретарі були зобов'язані, якщо президента і віце-президента в КЗС не було, посилати ці реляції до них додому, а під час засідань КЗС про них доповідати, записувати резолюції, що накладалися на них, і складати у відповідь рескрипти.

Ці рескрипти прочитувалися на наступному засіданні, причому, згідно з наказом від 5 квітня 1716 року, і чорнові їх списки, і переписані начисто підписувалися всіма членами КЗС та скріплялися секретарем. Потім текст рескрипту зашифровувався та направлявся у відповідну адресу з кур'єром. Вся робота КЗС була строго регламентована. Вхід в апартаменти КЗС дозволявся тільки особам, що там служили. Інструкція від 11 квітня 1720 року, в якій було встановлено побудову КЗС, закінчувалася приписом, як зберігати державні печатки і *«цифирные азбуки».*

Для збереження листа в таємниці застосовувалися відповідні охоронні заходи. Так, лист Петра I до Огильві від 17 лютого 1706 року супроводжувався таким записом: *«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».*

Посилалися в КЗС такі азбуки в конвертах, які опечатувалися червоними сургучними печатками, однак не державними, а особистими відправників. Пересилали шифри досить часто, адже термін їх дії був обмежений і документи, що вийшли з дії, направлялися в КЗС.

Постійно шифроване листування здійснювалося з дипломатичними представниками Росії за кордоном, зокрема: при віденському дворі – Голіциним, Урбіхом, Беклемішевим, Веселовським; при прусському дворі – з Льотом, а потім з Головкіним. Спеціальні шифри для листування з російським двором мали: Матвеєв – посол в Англії, Голландії, Австрії; Куракін – посол в Римі, Лондоні, Нідерландах, Ганновері, Парижі, і багато інших дипломатів, чиї шифри збереглися.

Часто зашифровувалися листи й коронованих кореспондентів – польського короля Августа II, прусського короля Фрідріха, хоча частіше це листування вели міністри і вельможі союзних держав: саксонську – Арнштедт, Флемінг, польську – Шембек, Синявський, Шанявський, Денгоф, данську – Юст Юль. Листування це стосувалося питань міжнародної політики, укладання союзних договорів і військових питань. Шифроване листування прусського короля знаходилося в руках його міністра Кайзерлінга. Існувало таємне листування Росії і Молдавії. Відомі шифровані листи господаря Михайла Раковіци, молдавського «посланця» Георгія Кастріота. Короткочасні дипломатичні місії також супроводжувалися врученням таємної «азбуки» особі, що прямувала з Росії за кордон.

Вищий командний склад армії і флоту також мав шифри для листування з царем. Відомі шифровані листи Петра I до адмірала Апраксіна, фельдмаршала Огильві, фельдмаршала Шереметєва, фельдмаршала-лейтенанта Гольца та їх шифровані відповіді. При цьому Петро I приділяв велике значення якості тайнопису. Так, цар з невдоволенням повідомляв фельдмаршалу Огильві: *«Цыфирь вашу я принял, но оная зело к разобранию легка».*

У своєму листуванні кореспонденти використовували шифри, призначені для шифрування листування на різних мовах. В основному, у цей період застосовувалися так звані російські, німецькі і французькі шифри, в яких як шифровеличини використовувались букви,

склади, слова, словосполучення відповідно російські, німецькі, французькі. Петро I особливо часто використовував французькі шифри.

У одному з листів Огильві скаржився Головкіну, що не зумів прочитати присланих розпоряджень Петра: *«Французские цифирные грамотки нихто читать не может, тако не знаю, что на них ответствовать. Прошу. до извольте мне на все мои письма ответ учинить немецкою цифирью, ибо той француцжкой нихто не разумеет».* Такі ж скарги Огильві адресував і Петру: «*… никого здесь нет, который бы французское ваше мог разуметь, понеже Рен ключ от того потерял… Изволте ко мне через цифирь мою писать, чтоб я мог разуметь…».*

Петро пояснив, чому він перейшов у листуванні тайнописом з німецької мови на французьку: *«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. А и французской ключ послан».*

Вручалися шифри для таємного листування і особам, що отримували спеціальне військове завдання від царя. Найбільш близькою особою до Петра I, як відомо, був Меншиков, якому після Полтавської перемоги цар присвоїв чин генерал-фельдмаршала. Шифроване листування між Петром I і Меншиковим стосувалося надзвичайно важливих питань. Так, Петро I у січні 1708 року послав Меншикову шифроване *«Рассуждение»,* яке розглядалося на військовій раді у місті Вільно 3 лютого, і просив його висловитися з даного питання. У іншому випадку Петро вимагав, щоб Меншиков зі свого боку прислав *«Рассуждение»* цифрою.

Меншиков, у свою чергу, листувався таємною азбукою і з дипломатами Долгорукими, і з підпорядкованими йому особами – генерал-майором Волконським, Боуром, Кропотовим і іншими. Комендант Полтави Келін отримав 19 червня 1709 року, тобто за тиждень до Полтавської битви, шифрований лист Петра I, відправлений до нього в шести примірниках. Цар писав: *«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 чином, військова шифрована кореспонденція супроводжувалася ще й умовною сигналізацією. Самі листи пересилалися в порожнистих бомбах, оскільки облога шведами Полтави не давала можливості листуватися іншим чином. Через 2 дні, 21 червня, Келін зумів повідомити Меншикова у шифрованому листі про тривогу, що спостерігалася у Полтаві, у шведському таборі та про перегрупування військ ворога у зв'язку з переходом російської армії на правий берег Ворскли.

Листування, що стосувалося важливих внутрішньополітичних питань, також шифрувалося. Так, спеціальний шифр був розроблений для листування про повстання на Доні у 1707—1708 роках. Ключ до цього шифру мали: Петро I, що стежив за ходом повстання, Меншиков – командувач кавалерією, адмірал Апраксін, який вів будівництво гаваней і флоту на півдні Росії, де розвивалося повстання, підполковник Преображенського полку Долгорукий, призначений начальником всіх озброєних сил, виставлених проти повстанців, і азовський губернатор Толстой, якому була підпорядкована територія, де знаходився оплот від турецької небезпеки – Азовська фортеця.

Таємне листування, для якого були розроблені особливі шифри, велося з адміністраторами прикордонних районів і губерній – з київським губернатором Голіциним і обер-комендантом Нарви Наришкіним.

У 1711 році для внутрішнього управління державою був створений Сенат. Дуже скоро після цього Петро I почав шифрувати свої листи Сенату. Зашифровані частини цих листів зазвичай стосувалися військових питань.

Таким чином, можна сказати, що урядове, загальнодержавне шифроване листування в петровську епоху активно велося у сфері зовнішньої політики та дипломатії, військової діяльності та вирішення внутрішньополітичних питань.

Разом із тим, Петро чудово розумів, що Росія в значній мірі відстала від провідних європейських держав у сфері криптології, тому ліквідувати це відставання можливо було лише перейнявши європейські шифросистеми та запросивши провідних криптологів Європи для роботи в Росії. Спочатку вибір Петра зупинився на одному з кращих фахівців у цій сфері того часу – Лейбниці, однак через смерть останнього криптослужба Росії ще впродовж довгого часу не могла досягти європейського рівня.

3. «Чорний кабінет» XVIII ст.

У часи перебування на російському престолі Катерини I віце-канцлером Росії і, отже, керівником її криптослужби став Андрій Іванович Остерман (1686—1747). У 1708 році він був прийнятий в число перекладачів Посольського наказу та служив у Похідній канцелярії царя. У липні 1710 року він був посланий до прусського і данського королів. Після повернення до Росії він був призначений секретарем Посольської канцелярії.

В утвореній у 1720 році КЗС він зайняв місце таємного радника канцелярії. Посидючість, працьовитість, дипломатичне мистецтво і знання досконало 4-х європейських мов зробили його незамінним для імператриці. 24 листопада 1725 року вона нагородила Остермана званням віце-канцлера з чином дійсного таємного радника, а на початку наступного року він був призначений членом Верховної таємної ради. У листопаді 1726 року Остерман став головним начальником над поштою (пошт-директором), а 1 січня 1727 року отримав орден Андрія Первозванного.

У створеному 10 листопада 1731 року Кабінеті Міністрів барон Остерман набув першорядного впливу на справи.

Після смерті канцлера Головкіна Остерман отримав звання першого кабінет-міністру та, не зважаючи на відносини, що загострилися між ним і Біроном, зберіг міцне положення при дворі. Імператриця Анна Іоанівна в скрутних випадках радилась з ним, тому сучасники називали його «оракулом» цариці, «душею» кабінету.

При Остермані криптологи Колегії закордонних справ продовжували роботу відповідно до вже сталих традицій. Наукова думка не стояла на місці, постійно велися пошуки нових шифрів. Такими новими шифрами були спочатку алфавітні, а потім неалфавітні коди. У цих кодах словникові величини вміщувалися у декілька розділів: алфавіт, склади, *«суплемент», «счёты», «месяцы».*

Алфавіт у цих шифрах міг бути російський або латинський, залежно від того, на якій мові писалося повідомлення. Склади постійні та характерні для кожної мови, тому ці розділи шифрів для кожної мови були однакові. Наприклад, для російських шифрів це були: ба, бе, би, бо, бу, би, бя, ва, ве, ви, в, ву, ви, вя тощо.

«Суплемент» був достатньо великий і включав не тільки необхідні імена цар-ственних персон, державних діячів («персони») і географічні найменування, як це було раніше, але й іншу активну лексику. У цей розділ, наприклад, могли входити слова: домагання, схильність тощо.

Розділ *«счёты»,* або як його ще називали *«исчисления»,* як правило, у всіх кодах був однаковий. Він включав такі величини: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 00, 000, 0000, 00000, мільйон. Іноді цей розділ якось доповнювався, наприклад, могли бути додані числа 50 000 і 100 000.

Місяці також перераховувалися в особливому розділі, і майже у всіх шифрах це пояснювалося 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 рідкісним винятком шифропозначення – це арабські цифри. Цифри-шифропозначення для різних частин словника завжди мали відмінності. Наприклад, якщо для алфавіту вони могли бути одно-, дво-, тризначні, то для *«суплемента»* тільки три- або чотиризначні, а для інших частин *(месяцы, счёты)* тільки чотиризначні. Крім того, могли бути й інші відмінності. Так, якщо для алфавіту і *«суплемента»* шифропозначеннями могли бути різні числа, то для інших розділів – лише числа, що закінчувалися нулями: 700, 750, 720, 4000 тощо. Взагалі для кожної подальшої частини словника характерна була все зростаюча значність шифропозначень.

Ці шифри мали велику кількість пустушок, що вводилися з метою ускладнення шифру. Могли вводитися помилкові додаткові цифри, що також не мали сенсу, але не входили до числа пустушок. У правилах користування шифрами, хоча вони були ще дуже короткі, явно проступала тенденція до використання при шифруванні навіть невеликих текстів значної частини або навіть більшості словарних величин. Як шифропозначення використовувалися майже виключно цифри на відміну від шифрів першої чверті століття, коли в цій ролі частіше виступали різні ідеограми. У новому типі шифрів вони застосовувалися вкрай рідко та лише для позначення «персон».

Проте разом із цими шифрами продовжували активно використовуватися і шифри старих зразків, в яких був лише алфавіт із шифропозначеннями, – цифрами, буквами або химерними старовинними ідеограмами, такими, наприклад, як у ранній *«цифирной азбуке»* для листування з Григорієм Волковим і князем Куракіним.

Розробники шифрів у цей період вже знали, що частота використання голосних букв у мові вища, ніж приголосних. Тому в 1730-1740-і роки в нових шифрах голосним обов'язково відповідало по декілька шифропозначень, приголосним – одно-два. Спостерігалися спроби запису шифротексту без розділень шифропозначень крапками (що раніше було абсолютне виключено) або з розділенням їх фальшивими крапками. Спосіб розшифрування в правилах обмовлявся заздалегідь. Приклад такого зашифрування наведений у *«цифирной азбуке»* для листування з державним віце-канцлером графом Воронцовим.

Це був шифр простої заміни, де буквам кирилиці відповідали двозначні цифрові шифропозначення, причому голосним додано по шість шифропозначень, приголосним – по два. У правилах сказано: *«Сею цифирью писать двояким образом, без точек, и с фальшивыми точками, которые как бы расставлены не были, токмо для разбору всегда по два номера брать надлежит».*

Шифропозначення в цей період вибиралися завжди за певними порядковими алфавітними схемами, що, зазвичай, не сприяло надійності шифрів. Наприклад, цей шифр виглядав так:

А Б В Г Д Е Ж З И К Л М Н О П Р С Т У…
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29…
40 57 58 59 60 41 74 75 42 80 81 82 83 43 44…
62 …. 63 …. 64 ….. 65 …. 66…
85 …. 86 …. 87 ….. 88 …. 89…
99 …. 98 …. 97 ….. 96 …. 95…
56 …. 55 …. 54 ….. 53 …. 52…

Слово «УЖГОРОД» можна зашифрувати таким чином: 441.7592.426.5.315; 8.974.1.488.266.560 тощо.

З початку 1730-х років у Росії спостерігався перехід від алфавітних кодів до неалфавітних. У алфавітних кодах відкритий текст і шифропозначення (власне код) нумерувалися паралельно один одному. Відхилення від цього порядку хоча і були, але практично дуже незначні і мало впливали на підвищення надійності або, як прийнято говорити, стійкості коду. Мабуть, розробники шифрів відзначили, що такий паралелізм істотно полегшував відновлення відкритого тексту і самого коду, оскільки правильне вгадування деякого числа шифропозначень дозволяло упорядкувати в алфавіті шифропозначення інших словарних величин.

Зрозуміло, що уникнути такої слабкості коду можна було шляхом перемішування шифропозначень. У цих випадках для полегшення процесів зашифрування та розшифрування необхідно було скласти *«шифрант»* і *«дешифрант»* – частини коду, призначені відповідно для зашифрування та для розшифрування. У шифрантів алфавітному порядку розташовувалися

елементи відкритого тексту (шифровеличини), тобто букви, склади, слова, словосполучення, а у дешифрантів порядку зростання – шифропозначення, якщо вони були цифрові. Якщо ж вони були буквені, то у дешифранті шифропозначення також розташовувалися в алфавітному порядку. Проте в шифрах цього другого типу буквені шифропозначення були вкрай рідкісні, вони траплялися лише іноді в окремих частинах шифрів, наприклад, у суплементі.

У цей період у розробників шифрів з'явилося явне прагнення додати кожній букві алфавіту у шифрі якомога більше шифропозначень. Проте всі ці шифропозначення мали одну дуже велику ваду: вони писалися підряд, що давало змогу легко їх розкрити. Так, наприклад, *«цифирная азбука»* для листування з бароном Кейзерлінгом, відправленим до Польщі у грудні 1733 року, мала такий вигляд:

A 11 12 13 14 15
B 16 17 18 19 20
…
Z 131 132 133 134 135

У невеликому суплементі цього шифру кожній величині відповідали по два шифропозначення, вибрані підряд у числовому ряду тризначних цифр: 260, 261 тощо.

А у ще одному шифрі камергера графа Льовенвольда кожній букві латинського алфавіту відповідає навіть по 10 шифропозначень:

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 тощо.

У невеликому суплементі два тризначні цифрові шифропозначення, додані кожній словарній величині, також вибрані підряд. Крапкам і комам відповідали тризначні шифропозначення. Таким чином, традиція вибору різних шифропозначень для різних частин шифру, що склалася у петровську епоху, знайшла своє продовження у цьому другому типі шифрів XVIII ст.

Однотипні по суті, ці шифри другого типу зовні могли оформлятися по-різному. Так, в одних випадках шифрант і дешифрант могли поміщатися на одному розвороті великого листа паперу. У інших випадках шифрант міг виділятися окремо і був листами, зшитими нитками в зошит, а дешифрант писався на окремому розгорненому листі. В обох випадках у шифранті шифровеличини могли поміщатися по-різному: або в порядку алфавіту з виділенням крапок і ком окремо в кінці, або по розділах (словник, складова таблиця, алфавіт, числа – *«счёты»,* календар – *«месяцы»,* пустушки). В цей же час почали поміщати у шифрант, а часто і у дешифрант, правила користування шифром. Ці правила пояснювали ті ускладнення, ті хитрощі, якими відрізнявся даний шифр.

Розглянемо деякі найбільш характерні зразки таких шифрів того часу.

У 1735 році резидент Олексій Вешняков прислав у КЗС *«цифры, которыми он корреспондует с генералитетом и министрами российскими, обретающимися при чужестранных дворах».*

Цифра оформлена у вигляді прошитого нитками зошита. На першій сторінці – заголовок: *«Цифирь секретная, посланная к ея императорского величества господам министрам в Лондон и Дрезден».* Вся сторінка розбита на три вертикальні графи. Перша графа – *«Алфавит для сложения».* У цю графу поміщені букви російського алфавіту, яким відповідають двозначні цифрові шифропозначення (довільні). Сюди ж поміщені в алфавітному порядку найбільш вживані прийменники, займенники, частинки: въ, ізь, як тощо.

Друга графа – *«Разные знаменования»* – містила словник шифру. Цікаво, що разом з тим, що кожному шифропозначенню могли відповідати, як завжди, по одній словниковій величині (наприклад, 100 – *«Ея Императорское Величество»,* 199 – *«двор Ея Императорского Величества»),* деяким з шифропозначень відповідали цілі групи словникових величин, необхідні

величини з яких вибиралися відповідно до контексту (наприклад: 198 – Англійський король, двір, Англія).

Третя графа – *«Для разбору»* – дешифрант. На другому листі тут приведені *«Изъяснения для употребления сей цифири»*.

В *«Изъяснениях»* розкриті хитрощі цього шифру. У шифропозначеннях відсутні цифри 3 і 7, тобто може бути 46, але не 47, 36 тощо. Самі по собі будь-які двозначні або тризначні цифри, що містять 3 і 7, служили для позначення ком і крапок. При цьому рекомендувалося: *«Мешать оныя между всеми как в десятичных, так и в сотенных, яко прибавкою оных число умножится. Следственно знаменательное скроется так, что никакая комбинация открыть не может. Например: А – 29 можно представить: 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 значатъ. Следственно, яко оне бы не были, но едино 29 будет видеть»*.

Писати рекомендувалося всі цифри як без вставок, так і зі вставками підряд *«без роставок буква от буквы и речь от речи»*. Особливо рекомендував автор шифру вводити *«смешения с 3 и 7»* при зашифруванні по буквах, де шифропозначення -двозначні («от *большей части десятеричных надлежит мешать с пустыми»),* бо *«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 писана смешением пустых прилежно»*.

І далі наводився приклад на зашифрування, з якого можна було зробити висновок про те, що голосні легко виділити, *«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»*.

Зберігся також шифр, який Вешняков вручив у січні 1737 року для листування абату Косу, що був російським агентом. На шифрі був напис: *«Цифры с аббатом Косом, данная ему в Каменце от резидента Вешнякова при проезде его от Турской крепости в Россию»*. Цей шифр був побудований за принципом шифрів 1720-х років: російський алфавіт, кожній букві відповідали одно-, дво- і тризначні цифри. Правда, було багато пустишок – 85. Такий же шифр був вручений Вешняковим абату Косу і з латинським алфавітом.

Політичними агентами Росії були не тільки державні іноземні діячі, але й інші особи. Наприклад, в Туреччині російськими агентами у цей період були єрусалимські патріархи Досифей, а пізніше Хрісанф. Через Досифея йшло листування Росії з молдавським правителем. Патріарх Хрісанф запропонував Головкіну таємну «азбуку» для листування, яка була прийнята російським двором з деякими поправками, з приводу чого Хрісанф писав Головкіну: *«Прийняли ми цифру, яка прислана в до-полнку наший, і зело неабияка»*.

Крім того Хрісанф запропонував ввести у таємне листування ще деякі умовності: *«А чтоб нам чащей писать к Великому Государю и к Вашему Высочеству и безопасно сделали мы сию цифирь. Посылаем и образ печати. И как придет к вам какое письмо, в котором есть та печать, ведомо буди, что есть наше писание. А с лица печать какая-нибудь, только бы что была сия внутри. К тому же, которое письмо имеет с лица круг, тое к Великому Государю; а которое имеет треугольный знак, есть к Высочеству Вашему. И сие всегда до будет за подлинное»*.

Введення безлічі пустишок у старі типи шифрів свідчило про виразне розуміння розробниками *«цифирных азбук»* того впливу, який мала на розкриваність зашифрованого тексту частота вживання одних і тих же величин, особливо букв. По мірі ускладнення шифрів кіль-

кість пустушок в них все збільшувалася, деколи їх обсяг у словнику міг перевищувати обсяг його значущих величин.

Так, наприклад, німецький шифр від січня 1744 року, що був отриманий від генерала барона Любераса для листування з ним російських міністрів при іноземних дворах, мав 165 пустушок, а у шифрі від січня 1745 року для листування КЗС з дійсним камергером і надзвичайним посланником у Берліні Петром Чернишовим пустушок взагалі була велика кількість. У звичайній таблиці пустушок було 90 – від 1003 до 1093. Крім того, у примітці було написано: *«Все нумера свыше 3015 служат тако ж пустыми, како пустыми употребляются и те нумеры, которые по порядку до 3015 не доставают».* Значущих величин в даному шифрі було близько 400, таким чином пустушки значно перевищили цю кількість.

У тому ж 1745 році Чернишову був надісланий ще один шифр, у якому було перераховано 90 пустишок, а крім того, вказано: *«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».*

Ще одним прикладом того, що розробники шифрів прагнули в цей період помістити в них якомога більше пустушок, може служити шифр, надісланий у 1747 році до дійсного таємного радника у Берліні Кейзерлінгу. У цьому невеликому за обсягом шифрі для шифропозначень були обрані числа з різних, окрім першої, сотень, а також першою, шостою, сьомою, восьмою тисяч. А як пустишки були вказані такі числа: 1—100, 190—199, 243—299, 327—427, 442—549, 573—674, 682—789, 807—906, 9211000, 5635—7009, 7043—10000. Конверт, у якому доставили цей шифр до Берліна, був опечатаний безліччю сургучних печаток і на ньому був напис про те, що доставлений він лейб-гвардії поручиком Ізмайловим.

У середині XVIII ст. під час царювання Єлізавети Петрівни була створена секретна служба перлюстрації. Результати роботи цієї служби декілька разів на місяць доповідалися цариці, однак це зажадало створення сильної криптоаналітичної служби для «злому» іноземних шифрів. Новий етап у розвитку російської криптослужби (іншими словами – ЧК) був пов'язаний з ім'ям Олексія Петровича Бестужева-Рюміна, призначеного в 1742 році головним директором пошт. Він уперше у вітчизняній практиці залучив до криптоаналітичної діяльності професійних вчених-математиків, причому кращих з них, що були тоді «світилами» європейської математичної науки.

Першим, кого Бестужев-Рюмін залучив до такої роботи, став відомий математик і фахівець з теорії чисел Християн Гольдбах. Іменний указ імператриці Єлізавети про його призначення на «особливу посаду» був датований 18 березня 1742 року, а справа про це названа *«Об определении в Коллегию иностранных дел бывшего при Академии наук профессора юстиц-рата Христиана Гольдбаха статским советником с жалованьем 1500 рублей, о выдаче недоданного ему в Академии наук жалованья и о выдаче ему вперед жалованья».*

Більше року Гольдбах витратив на придбання практичних навичок у новій справі, але перший успіх у дешифруванні цифрових текстів невідомого змісту прийшов до нього лише в липні 1743 року. З липня по грудень 1743 року ним був дешифрований 61 лист «міністрів прусського й французького дворів». Навесні 1744 року він уже міг «ламати» шифри підвищеної складності. На Гольдбаха посипалися всілякі милості імператриці, але необхідно відзначити головне – владні особи відчули, що математика для держави та для них особисто, це не щось престижно-декоративне, а «щит і меч», що охороняли їхні безпосередні інтереси.

Збереглися російські копії дешифрованих листів 1742 року: від *«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 також копії деяких інших документів.

Найбільшого успіху Гольдбах домігся у перших числах червня 1744 року, коли ним була прочитана шифрована депеша французького посла Шетарді до Парижа. Цей випадок став хрестоматійним в історії криптології. Знаючи, що його листи на пошті розкривалися, Шетарді був упевнений, що прочитати його шифр було неможливо й тому легковажно писав про імператрицю, що вона цілком віддавалася своїм задоволенням, була несерйозна, дурна та розпусна.

Бестужев-Рюмін, який став канцлером, спритно використав саме цей текст у боротьбі проти «французької» придворної партії (раніше в нього вже були дешифровані тексти практично всіх листів цього посла). Він розіграв перед Єлізаветою сцену дешифрування депеші, «вимушено» вимовляючи *«поносные слова».* В результаті 17 червня Шетарді був вигнаний із країни, а робота Гольдбаха на терені дешифрування не залишалася без уваги та високо була оцінена імператрицею.

У 1744 році вона дала вказівку про видачу йому надалі річної платні у 2000 рублів із статс-контори. У 1760 році Гольдбах отримав звання таємного радника з щорічною платнею у 4500 рублів. Це було одне з найвищих звань в російській державі, і нагороджувалися ним дворяни за особливі заслуги перед Вітчизною. Відзначимо, до речі, що Леонарду Ейлеру, незважаючи на його видатні наукові досягнення та постійне заступництво з боку російського двору, вказане звання так і не було подароване.

Саме з моменту появи Гольдбаха в штатах КЗС директору Санкт-Петербурзького поштамта Фрідріху Ашу почали поступати розпорядження Бестужева-Рюміна ретельно копіювати листи цілком, у жодному випадку не опускаючи в них шифротексту. Не довіряючи рядовим копіїстам, Бестужев-Рюмін наказав копіювати в ЧК *«цифрами писанные»* частини листів професору математику Тауберту.

З цього приводу Бестужев-Рюмін писав Ашу: *«Усмотренные в переписываемых унтер-библиотекарусом Таубертом в цифрах писем неисправность причиною, 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 ним 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».*

За розпорядженням Бестужева-Рюміна поштові служби повинні були розкривати й копіювати всі листи закордонних послів (навіть до дам), що пересилалися через кордон. Приватні листи, що перетинали кордон, так само, по можливості, розкривалися всі, але копіювалися найцікавіші. Основний масив інформації надходив безпосередньо до Бестужева від Аша.

Справа перлюстрації листів виявилася надзвичайно складною, такою, що вимагала терпіння, уваги і особливих навиків, які отримувалися зовсім не відразу. Конверти слід було розкривати акуратно, по можливості не порушуючи їх цілісності. Дипломатичний лист зазвичай поміщали в конверт, який прошивали ниткою та опечатували сургучними печатками. Таке упаковане послання могло вкладатися ще в один конверт, що також прошивався та опечатувався.

Технічні проблеми безулікового розкриття листів були дуже значними. Так, Аш скаржився Бестужеву-Рюміну:». *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 несолько часов держал, никак распуститься и отстать не мог. Да и тот клей который под печатями находился (кои я искусно снял) однако ж не распустился. Следовательно же, я к превеликому моему соболезнованию никакой*

возможности не нашёл оных писем распечатывать без совершенного разодрания конвертов. И тако я оные паки запечатал и стафету в ея дорогу отправить принужден был…».

Якщо розкривав і запечатував листи особисто пошт-директор, то копіював їх особливий секретар, переводив же особливий перекладач. Оскільки листам необхідно було надати їх первинний вигляд, тобто заклеїти, прошити ниткою та опечатати такими же печатками, якими вони були опечатані до розтину, то велике значення мала майстерність людини, що виготовляла печатки. Цей майстер-різьбяр також містився у штаті відомства Аша. Робота його була тонка й відповідальна, адже вживалася велика кількість особистих і державних печаток, якими дипломати користувались при опечатуванні своїх листів.

У той час печатка відливалася зі свинцю за формою, знятою гіпсом з негативу печатки, зробленого з воску. Цей спосіб, крім того, що був складний через 4-крат-не перезнімання відтиснення (негативу – воском, позитиву – гіпсом, знов негативу – свинцем і, нарешті, знову позитиву вже на самому листі – сургучем), давав не достатньо чіткі відбитки. В подальшому у середині Х!Х ст. один з чиновників МЗС винайшов спосіб виробництва підробленої печатки зі срібного порошку з амальгамою. Цей спосіб був дуже простий і швидкий, а печатка виходила чіткою. Проте вона мала істотний недолік – була дуже недовговічною та ламалася від щонайменшого необережного дотику.

Аш особисто перевіряв всі вироби різьбяря печаток, робив зауваження, а потім відправляв готові зразки для оцінки Бестужеву-Рюміну, який давав вже остаточний висновок. З цього приводу велося листування.

З листа Аша Бестужеву-Рюміну від 29 лютого 1744 року: *«Печатнорезчик Купи от своей болезни отчасти оправился и уже начало подделыванием некоторых штемпелей учинил, из которых он и сегодня два отдал, но один назад взять принужден был, дабы усмотренное мною в нем погрешение поправить, а другой, который барона Нейгауза есть, я за нарочитой нахожу и оной при чем посылаю…».*

Через декілька днів Бестужев-Рюмін написав Ашу відповідь:

«Из Государственной коллегии иностранных дел санкт-петербургскому почт-директору господину Ашу.

На рапорт Ваш от 29-го февраля здесь в 6-е 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 нейгау-зова не весьма хорошего мастерства».

У протоколах доповідей імператриці Єлізаветі можна прочитати таке: *«В Санкт-Петербурге. 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».*

Петро ІІІ, вступивши на престол, одержав службу перлюстрації вже в стані повного розвалу. При відсутності перехоплених депеш таку ж оцінку варто дати й ефективності дешифрування. Потрібно сказати, що якщо Гольдбах у цей час не мав масштабних успіхів у дешифруванні, то створені ним шифри, що нараховували до 3500 цифрових груп, були одними з кращих у Європі.

20 листопада 1764 року помер Гольдбах, після чого керівник КЗС граф Микола Панін запросив на його місце математика і фізика, німця за національністю Франца Ульріха Теодора Епінуса. В обов'язки Епінуса та його підлеглих входило створення шифрів і підбір ключів до шифросистем перехопленої кореспонденції.

У 1769 році Епінус був «*пожалован статским советником и определен при Коллегии иностранных дел при особливой должности*». За успішну роботу на терені дешифрування у 1773 році він отримав чин дійсного статського радника. Епінус майже все своє життя провів у Росії, яка стала для вченого другою Вітчизною.

Користувачами шифрів, створених в КЗС, були: імператриця (індивідуальні шифри для листування з обраними особами), кабінет імператриці (загальні й індивідуальні шифри для листування з вищими чиновниками держави), КЗС (загальні й індивідуальні шифри для листування, приблизно з 70 дипломатичними представниками Росії за кордоном та їх між собою; для листування з іноземними дворами; спеціальні шифри для листування з таємними агентами російського уряду), армія та флот.

Перлюстрація була найважливішим поряд з повідомленнями платних закордонних агентів джерелом інформації для прийняття зовнішньополітичних рішень. Перлюструвалася вся закордонна кореспонденція незалежно від положення одержувача та відправника. У 1779 році імператриця наказала доставляти їй з Санкт-Петербурзького поштамту таємно розкриту кореспонденцію. Найчастіше Катерина II читала дешифровані листи до послів у Санкт-Петербурзі навіть раніше, ніж вони самі.

Обсяг перлюстрації був фантастично великим. У 1771 році кількість перехоплених депеш тільки прусського посла становила 150 (125 відправлених та 25 отриманих), написаних різними шифрами. У 1780 році австрійський посол використовував 8 типів шифрів, обсяги цифрових текстів досягали 15 сторінок перехоплених близько 140 депеш. Поточне дешифрування здійснювали «канцелярські служителі» за допомогою ключів, знайдених, перекуплених або викрадених Епінусом.

У кінці XVIII ст. дешифрувальна служба Росії також читала французьке дипломатичне листування. Цей результат був отриманий в результаті поєднання аналітичних методів розкриття шифрів, якими користувалася криптослужба, і роботи агентів російської розвідки, що здобували французькі шифри. Російське посольство через секретаря посольства Мешкова завербувало до себе на службу як секретного агента одного з чиновників Міністерства закордонних справ Франції.

Таким чином, російський посол у Франції барон Смолін отримував і пересилав до Петербурга шифри та ключі до них, якими користувалися у своєму листуванні міністр закордонних справ Франції граф Монморсі і французький повірений в справах в Росії Дружині. В результаті Росія отримувала розвідувальну інформацію протягом тривалого періоду, навіть після того, як Смолін вимушений був покинути революційну столицю Франції після невдалої спроби допомогти відвезти Людовика XVI з Парижа.

Крім дешифрування Епінус займався також і розробкою шифросистем. Його підлеглі готували конкретні «*цифири*», які тиражувалися на бланках, що друкувалися в академічній друкарні (аркуші обліковувалися). «*Цифирные азбуки и разныя другия бумаги тайн подлежащие*» зберігалися в КЗС в окремому від користувачів сховищі в ідеальному порядку та видавалися для шифрування й дешифрування депеш на лічені години, що були вказані у відомостях. Ці операції проводилися навченими «розбирачами», які перебували на посадах актуаріусів.

Шифрування кореспонденції імператриці й Кабінету здійснював кабінет-міністр та його штат, а у Канцлера – чотири секретарі, які працювали цілодобово. Одним з них багато років був російський письменник Денис Іванович Фонвізін. Перевезення шифрів і депеш до Канцлера або Кабінету здійснювалося кур'єрами з сержантів гвардійських полків із жорстко нормованим часом руху.

Завданням незрівнянно більш складним, ніж створення шифрів, було для Епінуса дешифрування текстів. Цією справою Епінус займався особисто зі своїм помічником, вихідцем з німців, Йоганом Георгом Кохом. Розпочавши свою кар'єру в 1762 році копіювальником в Академії Наук, він був витягнутий звідти Епінусом у КЗС.

Свою діяльність з дешифрування Епінус повинен був почати з проблеми воістину історичної – знайти ключ до «писаного в цифрах» у 1714 році і підписаних Петром I листах до Амстердама Осипу Соловйову. В указі Сенату від 4 січня 1765 року наказувалося *«…если возможно отыскать той азбучной прежней ключ или другим каким по искусству в том средством оные разобрать переписать литерным письмом и взнесть в сенат…»*.

Результати протиборства Епінуса з петровським шифром невідомі, але є численні свідчення успішного дешифрування його службою перлюстрованої кореспонденції. За успішну діяльність він отримав звання дійсного статського радника.

Значний внесок у російську криптологію зробили Єрофей Каржавін і його племінник Федір Каржавін, які навчалися у Парижі, працювали на посадах перекладачів КЗС і займалися складанням шифрів та дешифруванням. Вони стали першими вітчизняними професійними криптологами в Росії.

З середини XVIII ст. в Росії стали використовувати нові шифри. їхні основні відмінності від попередніх шифрів були такими. По-перше, на російській мові розпочали активно використовуватися коди («номенклатори») на велику кількість букв, складів, слів, фраз тощо; їх число досягало 1200 символів. Як правило, це були алфавітні коди з цифровими шифропозначеннями. Буквам, складам тощо, що найбільш часто використовувались, надавалося декілька шифропозначень. Таким чином, застосовувався шифр гомофонної заміни, але на рівні не тільки букв, а й словосполучень. Коди мінялися регулярно, оскільки ключем такого шифру був сам код-таблиця заміни.

По-друге, збільшилась кількість пустушок, що вставлялися у шифротекст. З цього приводу в одній з інструкцій з користування шифрами вказувалося: «*Пустые числа писать где сколько хочется, только чтобы на каждой строке было сих чисел не меньше трёх или четырёх*». Так визначався лише нижній рівень кількості пустушок, а верхній рівень не встановлювався. Крім того, «*не начинать пиесы значащими числами, но пустыми…* ». Тим самим початок істинного шифротексту у повідомленні маскувався пустушками, що посилювало стійкість шифру.

Крім того, у шифри вставляли «особливі числа», шифропозначення яких визначало ті частини шифротексту, що при розшифруванні необхідно було вважати пустушкою. Так, зашифрований знак «+» означав, що наступне за ним шифропозначення не мало ніякого значення. Два знаки «++» говорили дешифрувальнику, що не слід читати два наступні за ним шифропозначення тощо. Знак «=» означав, що не слід брати до уваги всі шифропозначення, що стояли за цим знаком в даному рядку шифротексту, а знак «=» знищував весь подальший шифротекст на даній сторінці. Знак «*» знищував попереднє шифропозначення, два знаки «**» знищували два попередні шифропозначення тощо.

Таким чином, текст, зашифрований в результаті застосування численних пустушок і написання нічого не значущих відрізків, виявлявся значно довшим за відкритий текст. Розрахунок розробників шифрів саме і полягав у тому, що шифротексти були величезними цифровими масивами, у яких, на їх думку, лише той, хто знав ключ, міг відокремити «*зерно от плевел*».

Надзвичайно істотним для шифрів цього типу було продовження в них традиції використання при зашифруванні одного повідомлення різних мов: як правило, всі шифри були двомовними. Словник їх складався з двох частин: російською та французькою (рідше німецькою). Відкритий текст депеші складався на цих двох мовах, при переході у процесі зашифрування

з однієї мови на іншу ставилися особливі, заздалегідь обумовлені в правилах числа, яких для кожного шифру було декілька.

Цей прийом, коли різні частини однієї і тієї ж депеші писалися на різних мовах, приводив до того, що при зашифруванні не тільки практично удвічі збільшувалася кількість використовуваних кодових позначень, але, що найістотніше, змішувалися і певною мірою вирівнювалися статистичні характеристики шифротексту. При цьому основні правила як для російської, так і для іншомовної частини були однаковими, тобто наявність безлічі пустушок, зашифрування великих шматків псевдотексту, які при розшифруванні знищувалися, тощо.

Як мовилося у правилах до цих шифрів: *«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 полуторе, по две и более, а иногда по одному только, по два и по три числа. Иногда пиесы начинаются или оканчиваются самыми значущими. Но во всяком случае часто пишутся пустые в самой середине параграфа и вместо просодии, а иногда и вмешиваются и в середине фразисов и речений. Да сверх того ставятся между пустыми и самые значущие числа, кои не понадобятся и уничтожаются».*

Катерина II особисто приділяла значну увагу шифруванню повідомлень. Так, відправляючи Олексія Орлова до Європи з розвідувальним завданням, вона забезпечила його «*нарочно сочинённым цифровым ключом*», додавши, що «*этот ключ используется для корреспонденции вашей с Нами, которая по важности предмета свого требует непроницаемой тайны*». Орлову були надані також окремі шифри на російській, німецькій та французькій мовах для листування при необхідності з російськими послами «*при государственных дворах*». Для забезпечення шифрованого листування Орлов мав надійних і підготовлених «*служителей канцелярских*».

У той період у Росії з'явилися «циркулярні» шифри, тобто загальні шифри у послів і КЗС, що дозволяло оперативно передавати послам єдині вказівки, накази тощо.

Таким чином, до середини XVIII ст. в Росії була створена мережа загального шифрованого зв'язку. Загальний шифр отримав назву «*генеральная цифирь*». Разом із ним збереглися й «індивідуальні» шифри для зв'язку «центру» з кореспондентами мережі. Кожний кореспондент, як правило, мав декілька «індивідуальних» шифрів.

З *«генеральных цифирь»* XVIII ст. відомі такі:

– 1762 року на російській мові, за допомогою якої обмінювалися кореспонденцією з КЗС і між собою: Бестужев-Рюмін (Париж), Кейзерлінг (Відень), Корф (Копенгаген), Панін (Стокгольм), Голіцин (Лондон), Пушкін (Гданьськ), А. Симолін (Мітава), Д. Симолін (Регенсбург), Салтиков («закордонна армія»), Обрізків (Константинополь);

– 1762 року, що об'єднувала тих же кореспондентів, але листування по ній можна було вести відразу на 3-х мовах: російській, французькій і німецькій. Додатково цей шифр у 1764 році був даний генерал-майору князю Репніну, що прямував як повноважний міністр до прусського двору, а також генерал-аншефу князю Волконському;

– 1764 року на російській і французькій мовах, яка була розіслана російським представникам у Відні, Варшаві, Копенгагені, Лондоні, Стокгольмі, Берліні, Гаазі, Парижі, Дрездені, Мітаві, Регенсбурзі, Гданьську, Мадриді, Гамбурзі, Константинополі;

– 1768 року на російській і французькій мовах була розіслана у ті же 15 адрес;

– 1771 року на французькій і російській мовах, яка була розіслана у Мітаву, Гданьськ, Берлін, Дрезден, Париж, Мадрид, Гаагу, Лондон, Гамбург, Копенгаген, Стокгольм, Відень, Регенсбург, Варшаву, командувачу 1-ою і 2-ою арміями генерал-фельдмаршалу графу Румянцеву, генерал-аншефу князю Долгорукову. У 1779 році цей же шифр був даний відправленому до Португалії надзвичайному послу і повноважному міністру графу Нессельроде;

– 1773 року на російській мові під знаком «165», яка була розіслана, у порівнянні з попередньою, у перші 14 адрес;

– під знаком «40, 68 і 77» – найбільша з відомих цифр XVIII ст. Вона включала 2000 словникових величин і об'єднувала КЗС з 15 кореспондентами за кордоном: Стакель-бергом у Варшаві, міністром Голіциним у Відні, міністром Ассебургом у Регенсбурзі, міністром Барятінським у Парижі, міністром Зіновьєвим у Мадриді, послом Белосельським у Дрездені, послом Голіциним в Гаазі, міністром Симоліним у Стокгольмі, міністром Долгоруковим у Берліні, міністром Сакеном у Копенгагені, міністром Мусіним-Пушкіним у Лондоні, резидентом Гроссом у Лондоні, послом Стахієвим у Константинополі, резидентом Ребіндером у Гданьську, князем Репніним у Берліні.

У 1771 році була паралельно організована загальна мережа зв'язку, що охоплювала абсолютно інший регіон. Так, за допомогою «*генеральной цифири*» 1771 року під знаком «1631» переписувалися між собою і з КЗС 10 кореспондентів: повноважний міністр Булгаков у Константинополі, граф Воронцов у Венеції, граф Разумовський у Неаполі, повноважний міністр Мордвінов у Генуї, повноважний міністр князь Юсупов у Турині, граф Мореніго у Флоренції, Псаро – повірений у справах на Мальті, колезький радник Хемніцер у Смірні, генеральний консул у Молдавії, Валахії і Бесарабії Северін, колезький асесор Юліниц у Сицилії.

У КЗС вівся ретельний облік всіх цифр. Перелік цифр, списки осіб, кому вони були розіслані, від кого отримані назад окремі примірники, на якій мові шифри складені, та інші необхідні відомості заносилися в особливі реєстри.

Якщо примірник шифру кимось з кореспондентів втрачався або виникала підозра, що шифр виявлявся відомий ворогу, то негайно видавався імператорський указ про виведення цього шифру з дії та заміну його іншим. Цей указ відразу ж розсилався всім кореспондентам, що входили в дану мережу зв'язку.

Дотриманню таємниці шифролистування в КЗС приділялася велика увага. Міркуючи *«о наилучшем содержании в секрете всех в секретной экспедиции дел»,* Колегія ще у 1744 році визначила наказати всім служителям цієї експедиції (і архіву) *«ни с кем из посторонних людей об этих делах не говорить, не ходить на дворы к чужестранным министрам и никакого с ними обхождения и компании не иметь».*

Цей наказ був підтверджений повторно 28 березня 1758 року: «*Для сохранения вящего секрета при нынешних военных и всяких важных обстоятельствах*» секретарям таємної експедиції ставилося в обов'язок суворо наглядати за перекладачами, «*чтобы дела, им порученные, по столам не лежали и чтобы товарищи их не читали этих дел*». Наприкінці наказу підтверджувалася заборона кого-небудь стороннього пускати в апартаменти, зайняті таємною експедицією.

При імператриці Катерині II 15 березня 1781 року КЗС утретє отримала наказ не допускати знайомства *«чинов департамента иностранных дел»* з іноземними міністрами та їх свитою. При цьому імператриця вказала, щоб, окрім *«министров департамента иностранных дел, каковыми ее величество почитает канцлера (или без сего звания управляющего оным департаментом), вице-канцлера и членов секретной экспедиции»,* ніхто з інших чинів колегії не ходив у будинки іноземних міністрів, не мав з ними розмов про справи, нікого з них у своєму будинку не приймав і ні під яким виглядом не вів з ними листування. Та ж сама заборона була повторена указом від 3 серпня 1791 року.

КЗС також уважно стежила за збереженням шифрів. Особисто державний канцлер, а ним у той період був граф Іван Остерман (син Андрія Остермана), неухильно стежив за суворим дотриманням правил користування вітчизняними шифрами, вимагав їх своєчасної заміни. При щонайменшій підозрі про компрометацію шифрів він давав вказівки про їх дострокову заміну або про внесення в них істотних змін.

Коли стало відомо, що один із канцелярських службовців при послові Росії у Гданську загубив шифр, Остерман зробив послу Волчкову суворе попередження: *«…признано здесь за нужно подтвердить Вам в то же время единожды навсегда, чтоб Вы сами впредь хранили у себя цифирнык ключи и заочно не выпускали их из рук, в чем и обязываетесь Вы Вашею присягою верности Ея Императорскому Величеству».*

Поступово встановилася ієрархія шифрів, коли складні системи використовували лише для найважливіших повідомлень, а зі зниженням їхнього рангу, спрощувався й шифр. Якщо складання власних шифросистем, насамперед для російського алфавіту, ще відставало від Європи, то криптоаналітика була на висоті. З цього часу російська криптологія остаточно зайняла одну з провідних позицій у криптології європейській та стала ефективним знаряддям у руках дипломатичних і військових відомств країни.

4. Криптологія першої половини XIX ст.

На початку XIX ст. у Росії була зроблена реорганізація органів керування країною. У 1802 році Маніфестом Олександра I замість колегій були засновані міністерства. Зокрема, було утворене міністерство закордонних справ (далі – МЗС), канцелярія якого містила чотири основні експедиції та три таємні. Перша таємна – шифрувальна, друга – дешифрувальна, третя – служба перлюстрації.

До 1808 року начальником першої експедиції, куди входила *«цифирная»* частина, був Жерве. Потім він був призначений керівником Канцелярії, а начальником цієї експедиції, перетвореної у відділення, став Міллер. Дешифрувальну частину у цей період очолював Християн Бек. Збереглися деякі документи, що дозволяють охарактеризувати діяльність таємної експедиції Канцелярії МЗС періоду початку XIX ст. та війни з Наполеоном.

Лист від 8 березня 1812 року Міллеру:

«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».

Міллер і Крейдеман були не тільки розробниками «лексиконів», тобто словників до шифрів, але й самих шифрів. Цю роботу виконували і деякі інші співробітники. Після складання шифру фахівцем-криптографом у XVIII ст. він начисто переписувався від руки спеціальним секретарем в потрібній кількості примірників. Тепер шифри виготовлялися вже друкарським способом. Відносно кожного шифру завідувачам таємною експедицією при цьому складалася доповідна записка такого змісту:

«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 напечатани-ем, 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 112 1/2 страниц российской наборной азбуки и напечатание по 30 р. за страницу, а за все 112 1/2 страниц – 3375 р.

за набор 122 1/2 страниц французской наборной азбуки и напечатание, по 30 р. за страницу, а за все 122 1/2 страницы – 3675 р.

Бумаги:

Алексан др и йеной 83 л. по 2 р. 50 к. кажд ая – 207,50
Итого 9222 р. 50 к. Коллежск. сов. Хр. Миллер».

На початку XIX ст. у МЗС був організований так званий *«Цифирный комитет»,* до складу якого увійшли найбільш досвідчені та кваліфіковані криптографи. У завдання комітету входив аналіз і введення нових систем шифрів, контроль за їх правильним використанням і зберіганням, вивід з дії застарілих або скомпрометованих шифрів, складання висновків, звітів і доповідей для керівників МЗС і імператора з питань діяльності шифрувальної та дешифрувальної служб. Цей комітет був підпорядкований міністру, а очолював його *«главный член цифирного комитета».*

Конец ознакомительного фрагмента.