

ИСТОРИЧЕСКИЕ ОЧЕРКИ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЁ ПРИЛОЖЕНИЯМ

DOI 10.17223/20710410/18/7

УДК 519.7

ОБ ИСТОРИИ КРИПТОГРАФИИ В РОССИИ¹

Н. Н. Токарева

*Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск***E-mail:** tokareva@math.nsc.ru

Представлен материал по истории криптографии в России. До сих пор она остаётся мало изученной и во многом засекреченной; в то же время к ней наблюдается повышенный интерес. Кратко рассмотрен период с середины XVI века до настоящего времени. Иногда хронологический порядок изложения нарушается, внимание обращается к отдельным событиям и людям, повлиявшим на ход истории криптографии или своеобразно его отразившим.

Ключевые слова: *криптография, криптоанализ, история России, П. Л. Шиллинг, В. И. Кривош-Неманич, Г. И. Божий, В. А. Котельников.*

1. Появление криптографии в России

Первые профессиональные криптографы на Руси появились при Иване Грозном (1530–1584). Они находились на службе в Посольском приказе, созданном им в 1549 г. и отвечавшем за внешнюю политику страны. Криптографы разрабатывали так называемые «азбуки», «цифири», «цифры» или шифры, как они стали называться позднее. Сначала это были простые шифры замены.

Но всё-таки, как отмечает в своей книге [43] исследователь истории шифровального дела Т. А. Соболева, первым из российских государей, осознавшим всю важность криптографии для безопасности страны, стал Пётр I (1672–1725). Он поставил шифровальную службу действительно на профессиональную основу. С 1700 г. вся работа по созданию шифров, шифрованию и расшифрованию велась в цифирном отделении Посольского приказа, а позднее, с 1709 г., — в Посольской канцелярии. Криптографическая служба в это время находилась под постоянным и непосредственным контролем государственного канцлера Гавриила Ивановича Головкина и вице-канцлера Петра Павловича Шафирова. Ими же заслушивались отчеты о перехваченных иностранных шифрах, что может свидетельствовать и о начале криптоаналитической деятельности. Затем криптографическая работа велась в Первой экспедиции Коллегии иностранных дел, где она стала строго регламентироваться и засекречиваться.

Типичным шифром того времени был шифр простой замены: каждая буква алфавита заменялась новым знаком, буквой или сочетанием букв. Кроме того, добавлялись «пустышки» — незначащие символы, а также вводились специальные обозначения для

¹Исследование выполнено при поддержке РФФИ (проекты № 10-01-00424, 11-01-00997, 12-01-31097) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0429).

часто употребляемых в определённом контексте слов или словосочетаний (такой словарь назывался «суплемент»). Авторство некоторых цифирей принадлежало лично Петру I.

У Петра I имелся даже специальный блокнот с шестью шифрами, которыми он активно пользовался. Однако в переписке случались и некоторые казусы. В книге [43] приводится такой пример. Пётр I часто употреблял французские шифры. В одном из писем фельдмаршал Г. Б. Огильви жаловался Головкину: «Французские цифирные грамотки никто читать не может, тако не знаю, что на них ответствовать...» и писал напрямую Петру I: «...никого здесь нет, который бы французское ваше мог разуместь, понеже Рен ключ от того потерял... Изволте ко мне через цифирь мою писать, чтоб я мог разуместь...», на что Пётр I отвечал: «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». Кажется, что потеря ключа в то время не сильно озадачивала переписчиков. Однако позднее к Огильви был приставлен А. И. Репнин, доверенное лицо Петра I, которому было поручено наблюдать за действиями фельдмаршала.

Методы шифрования и сама шифрованная переписка петровской эпохи наиболее полно представлены в многотомном издании «Письма и бумаги императора Петра Великого» (под редакцией А. Ф. Бычкова и И. А. Бычкова).

2. Чёрные кабинеты

Криптографическую службу России продолжал курировать вице-канцлер. С 1725 г. этот пост занимал Андрей Иванович Остерман. При нём шифры становятся неалфавитными — кодируются уже комбинации букв, а в качестве шифробозначений теперь используются исключительно цифры. В 1741 г. с приходом к власти Елизаветы Петровны (1709–1761) вице-канцлером и главным директором почт назначается Алексей Петрович Бестужев-Рюмин. С его именем связано появление в России службы перлюстрации (тайного вскрытия почты). Осуществляется эта деятельность в «чёрных кабинетах» — тайных комнатах, имевшихся во всех крупных почтовых отделениях.

Вскрывать письма было непросто. Нужна была необыкновенная аккуратность и изобретательность. А иной раз ничего и не выходило. Например, об одной своей неудаче сообщал перлюстратор Ф. Аш в письме к Бестужеву-Рюмину: «...на письмах нитка таким образом утверждена была, что оный клей от пара кипятка, над чем письма я несколько часов держал, никак распуститься и отстать не мог. Да и тот клей, который под печатями находился (кои я хотя искусно снял), однако ж не распустился. Следовательно же я к превеликому моему соболезнованию никакой возможности не нашел оных писем распечатать без совершенного разодрания кувертов. И тако я оные паки запечатал и стафету в ея дорогу отправить принуждён был...» [43]. Со временем в чёрных кабинетах появился целый штат сотрудников: одни вскрывали и запечатывали письма, другие прошивали их ниткой и подделывали печати, третьи копировали содержимое, четвёртые переводили, пятые занимались дешифрованием и т. д. Их деятельность держалась в строгом секрете.

Государственные интересы оказывались выше доводов морали. И не только в России. Надо сказать, что в европейских странах чёрные кабинеты начали свою работу лет на сто раньше.

В 1742 г. на «особливую должность» в Коллегию иностранных дел был принят первый профессиональный криптоаналитик. Им стал математик Христиан Гольдбах (1690–1764), получивший через год первые успехи на новом поприще. Он дешифро-

вал ряд французских дипломатических шифров. Позднее криптоанализом занимались математики Ф. Эпинус и И. Тауберт; русские криптографы братья Ерофей и Фёдор Коржавины и другие [36].

3. Первая половина XIX века

С начала XIX века вся криптографическая деятельность, а также руководство службой перлюстрации осуществляются в Канцелярии только что созданного (1802 г.) Министерства иностранных дел. Непосредственно руководит Канцелярией (с 1810 г.) статс-секретарь Карл Васильевич Нессельроде, позднее ставший министром иностранных дел и государственным канцлером.

К числу ярких успехов того времени относится дешифрование военной переписки Наполеона. Этот факт сыграл важную роль в исходе Отечественной войны 1812 г. и поражении наполеоновской армии.

— Нам очень сильно помогло то, что мы всегда знали намерения вашего императора из его же собственных депеш <...>

— Я считаю очень странным, что Вы смогли их прочесть. Кто-нибудь, наверное, выдал Вам ключ?

— Отнюдь нет! Я даю Вам честное слово, что ничего подобного не имело места. Мы просто дешифровали их.

(Из разговора, состоявшегося после войны между императором Александром I и командующим одним из корпусов армии Наполеона маршалом Макдональдом.)

Интересно, что выдающийся русский учёный Павел Львович Шиллинг (1786–1837) — электротехник, изобретатель первого электромагнитного телеграфа² и электрической мины, собиратель ценнейших коллекций китайских и японских рукописей, учёный-востоковед, отважный военный, участвовавший в сражениях Отечественной войны 1812 г. и награждённый одной из самых почётных наград — саблей с надписью «За храбрость», блестящий игрок в шахматы, «весельчак, отличный говорун» и, кстати, петербургский знакомый А. С. Пушкина и К. Н. Батюшкова — был, кроме того, одним из крупнейших криптографов XIX века! И эта особая сторона его многогранной деятельности долгое время оставалась засекреченной. Даже сейчас она ещё не исследована должным образом.



Рис. 1. П. Л. Шиллинг. Портрет и мини-портрет на советской марке

²Получивший распространение телеграф С. Морзе был запатентован в 1837 г. — спустя пять лет после изобретения П. Л. Шиллинга.

Известно, что с 1803 г. П. Л. Шиллинг работал в МИД, в которое он вернулся и после окончания Отечественной войны. Именно он организовал министерскую литографию — способ плоской печати, только что входивший в употребление в Европе. До этого шифрдокументы копировались от руки. С 1818 г. барон Шиллинг стал заведующим цифирной экспедицией Канцелярии МИД, занимающейся разработкой шифров. Ему принадлежит изобретение биграммного шифра, в котором шифровались не отдельные буквы, а их двойные сочетания, биграммы. При этом некоторые статистические зависимости снимались за счёт того, что в биграммы объединялись буквы, находящиеся друг от друга на большом расстоянии [43].

4. Шифры второй половины XIX века

Во второй половине XIX века криптографическая служба России перестала быть привилегией МИД и была создана ещё в двух ведомствах: военном и Министерстве внутренних дел. Тем самым существенно расширялись сферы использования криптографии, её значение в жизни государства неуклонно росло. Появилась классификация шифров по их назначению и области применения. Были выделены шифры военного ведомства (включая императорские), шифры жандармерии, гражданские шифры (например, Министерства финансов), агентурные шифры, предназначенные для связи с разведчиками.

Активно использовались биграммные шифры, введённые бароном Шиллингом; биклавные шифры — шифры многозначной замены, определяемой двумя ключами (автор — барон Н. Ф. Дризен); шифровальные коды — шифры, использовавшие цифры в качестве шифралфавита; коды с перешифровкой.

Термины «шифр» и «ключ» тогда ещё были синонимами. Ключом назывался, по сути, принцип шифрования сообщения, его алгоритм. Раскрытие ключа было равносильно гибели всей криптографической системы. Не так будет обстоять дело в XX веке, когда ключ станет сменной частью сложной криптосистемы. Раскрытие ключа не будет приводить к краху шифра, а будет означать лишь то, что ключ необходимо поменять.

Цифирный комитет устанавливал предельный срок действия каждого шифра в среднем от трёх до шести лет. Но любопытно, что многие шифры использовались и по истечении их «срока годности», что, несомненно, сказывалось на тайне переписки. Кроме того, имели место серьёзные нарушения. Так, представлялось возможным снова использовать скомпрометированные шифры в других регионах или спустя некоторое время. Например, русский биграммный ключ № 356 использовался почти 25 лет! История его такова. Он был введен в действие в 1869 г. «в консульствах на Востоке». В 1888 г. его экземпляр был украден из Российской миссии в Пекине. Вследствие этого шифр был выведен из употребления, но лишь на некоторое время. Несмотря на очевидность компрометации, в начале 90-х годов XIX века шифр вновь ввели в действие, но уже в другом регионе. Он был направлен в Амстердам, Гаагу, Берн, Женеву, Стокгольм и другие города. В 1898 г. произошла ещё одна компрометация этого шифра: один его экземпляр был потерян начальником Адриатической эскадры. Вероятно, именно это событие, как пишет Т. А. Соболева [43], наконец заставило руководителей шифрслужбы окончательно изъять ключ № 356 из употребления. В соответствующем заключении было указано: «вследствие почти 1/4-векового всемирного использования». Лучше и не скажешь.

Но в целом криптографическая служба России в то время находилась на достаточно высоком профессиональном уровне. Очень быстро и эффективно работали чёрные

кабинеты. «Сохранить тайну шифра в Петербурге особенно трудно», — отмечал канцлер Германской империи Отто фон Бисмарк [13].

Один из бывших сотрудников спецслужбы перлюстратор С. Майский вспоминал: «Иностранная дипломатическая переписка попадала в руки российских специалистов практически полностью. „Чёрные кабинеты“, разумеется, существовали везде, даже в самых демократических республиках Америки и Старого Света. Но справедливость требует сказать, что нигде в мире „чёрный кабинет“ не работал так чисто, как в России, и в особенности в Петрограде» [13].

Интересно, что император Александр III в течение всего своего правления отказывался читать выписки из писем, добытые в чёрном кабинете. После вступления на престол и знакомства со службой перлюстрации он заявил: «Мне этого не нужно». Не так поступали другие императоры.

В Военном ведомстве второй половины XIX века чаще всего использовались «словарные ключи». Работали они так. Составлялся словарь небольшого объёма (до 1 000 словарных величин), каждому слову которого соответствовал код — трёх- или четырёхзначное число. Шифрование велось непосредственной заменой по словарю. Такие «военные ключи» действовали длительное время, при этом относительно часто менялся словарь.

Подобными (словарными) шифрами пользовался и Николай II. Примечательно, что словари Его Императорского Величества, предназначенные для деловой переписки, содержали множество слов с эмоциональной окраской. Например, такие: «бескорыстный», «безотрадный», «благородный», «болезненный», «ни под каким видом», «молва», «нелепый», «неправдоподобный» и др. [43].

Особое положение занимали *агентурные шифры*, использовавшиеся разведчиками и агентами царской охранки. Одним из основных требований, предъявляемых к таким шифрам, была «скрываемость», «безуликовость» их документации. Ключ должен был запоминаться или легко извлекаться из «окружающих предметов» (например, распространённых книг), наличие которых никак не компрометировало агента. Сам процесс шифрования должен был быть быстрым и простым. К числу таких шифров относились варианты шифра Цезаря, книжные шифры, шифры перестановок.

Книжный шифр при правильном использовании мог быть действительно очень надёжным и безуликовым. Выбиралась определённая книга, в которой номера страниц, строк и букв в строках служили шифробозначениями для шифруемых букв. Подобные шифры массово использовались и в русском подполье конца XIX века. Однако сотрудники «чёрных кабинетов» обнаружили несколько «зацепок» к раскрытию таких шифров. Оказалось, что корреспонденты предпочитали находить в книгах буквы, стоящие неподалеку от начала строки или страницы. Так, подсчёт номера буквы занимал меньше времени, да и риск ошибки был ниже. А вот редкие буквы обычно имели большие номера, так как в начале строк они попросту не попадались. Другой «зацепкой» было изъятие и внимательное изучение личной библиотеки каждого подозреваемого.

Подробнее о российской криптографии XIX века и начала XX века можно прочитать в [6–10, 14–21].

5. Криптограф-соловчанин

В 1898 г. сотрудник российской криптографической службы, коллежский регистратор Владимир Иванович Кривош (1865–1942) был послан в Париж для изучения иностранного опыта в делах перлюстрации. В том числе устройства местного чёрного кабинета.

Любопытно описание этого учреждения, которое приведём по книге [43]. «Парижский чёрный кабинет был устроен аналогично петербургскому. Эта „секретная часть“ находилась в частном доме. Официальная вывеска на нём гласила, что здесь располагается землемерный институт. Один из служащих „секретной части“ действительно знал толк в лесоводстве, и если какой-то частный человек туда забредал, то ему давалась вполне квалифицированная справка. В передней комнате, куда мог прийти с улицы кто угодно, на стенах висели карты, планы земельных участков, а на столах лежали свежие газеты и письменные принадлежности. Из этой комнаты была дверь в следующую, в которой также не было ничего секретного, но был шкаф, служивший дверью в третью комнату. Таким образом, чтобы пройти в действительно секретную часть, необходимо было идти через шкаф, зная, как его открыть (наступить одновременно на две дощечки на полу и нажать одно из украшений шкафа). Дверь автоматически сама запиралась за прошедшим через неё. В следующей комнате была перлюстрационная часть, имевшая сообщение пневматической почтой с главным почтамтом. Все прибывающие в Париж дипломатические пост-пакеты прежде всего отправлялись сюда. Здесь проводилась их регистрация и передача в кабинеты дешифровальщикам, занимавшимся с ними по двое. После дешифрования и фотографирования письма вновь заклеивались и отправлялись по той же трубе пневматическим способом на почтамт. Для президента ежедневно выпускался „листок“ со всеми полученными за сутки сведениями — нечто вроде дипломатической газеты».

Поездка не прошла даром. Вместе с французскими специалистами были раскрыты шифры, использовавшиеся Японией, Англией и Германией. В. И. Кривош, словак по происхождению, стал одним из ведущих российских криптографов. За предложенные им усовершенствования российской криптографической службы он получил орден Святого Владимира 4-й степени из рук П. А. Столыпина. Владимир Иванович постоянно приглашался для ведения заседаний государственных комиссий различного уровня секретности.

Удивительна судьба этого человека. В. И. Кривош родился в одной из деревень Австро-Венгерской монархии. Он рос вблизи строящейся железной дороги и мечтал: когда дорога будет достроена, он уедет в далёкие края. Какими же суровыми и фантастическими они оказались...

Его родители были мелкими предпринимателями, которым хватило средств отправить на учёбу только одного сына, Владимира. Его одарённость открыла ему поистине удивительные перспективы. Сначала были гимназии: немецко-словацко-венгерская и итальянско-хорватская. Потом с поразительной быстротой — Королевская Ориентальная Академия, Петербургский университет, парижская Сорбонна. В 1890 г. Владимиру Ивановичу 25 лет. Он блестяще образован, изучил математику и статистику, владеет пятнадцатью языками (к концу его жизни это число достигнет сорока!), написал диссертацию по арабской литературе и уже стал незаменимым российским специалистом в области криптографии и стенографии. Вскоре он становится Главным цензором газет и журналов Российской империи и занимает множество «особых» и «сверхсекретных» должностей. Царское правительство использует его талант в самых разных областях.

Однако в 1915 г. он попадает под подозрение в шпионаже. За этим следует разжалование и ссылка в Сибирь. И возвращение в революционный Петербург в 1917-м. Встреча и работа с В. И. Лениным, который зачисляет В. И. Кривоша в состав наркомата иностранных дел. Так начинается новый, советский, период его жизни.

А дальше, как пишет Любомир Гузи [23], исследователь жизни и творчества выдающегося криптографа, «жизненный путь этого человека напоминает шутку потерявшие

го всякую объективность биографа-графомана». Кривоша арестовывают: его прошлое дискредитирует советскую власть. Но расстрелять лучшего специалиста не решаются. Из тюрьмы он переводится на службу в разведку, потом становится переводчиком-дешифровальщиком Особого отдела ВЧК. Новый арест. И последовавший затем перевод в Спецотдел на разработку сложнейших шифров и их дешифрование. Вскоре «за принятие мер к выезду из страны» Кривош арестовывается и приговаривается к расстрелу. Но снова помилован. В мае 1922 г. — очередное освобождение и очередное назначение в контрразведку. Год спустя — опять арест «за несанкционированные контакты с представителями чехословацкой миссии». В тюрьме он ожидает то расстрела, то ссылки в лагерь. Кривош временно теряет зрение, но, когда оно возвращается, с радостью читает тюремную библиотеку и занимается переводами. Он приговаривается к 10-летнему заключению в концлагере, который ему разрешают выбрать самому — выбирает Соловки³. Главным образом потому, что первую волну заключённых составили преимущественно интеллектуалы бывшего режима.

На Соловках Кривош выбирает псевдоним «Тот, у которого ничего нет», что по-словацки звучит как «Нема нич». Он работает ботаником, зоологом, орнитологом, переводчиком, преподаёт иностранные языки, основывает оркестр, становится председателем научной комиссии по фауне и флоре Севера России.

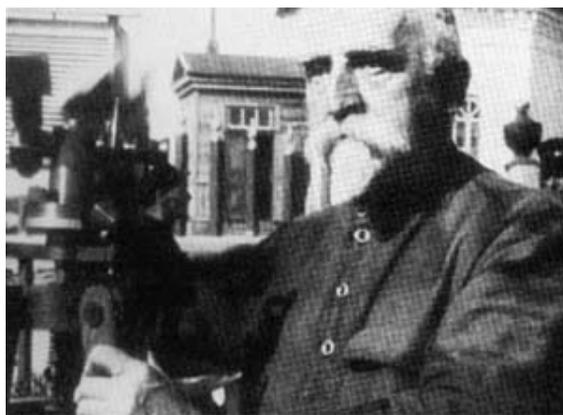


Рис. 2. В. И. Кривош-Неманич, узник СЛОНа

В 1928 г. Кривош-Неманич выходит на свободу. Дома его встречает жена, которая не отказалась от мужа во время всех преследований. До 1936 г. этот удивительный человек (принявший фамилию Кирпичников) работает в Министерстве иностранных дел, но вернуться на словацкую родину ему не удается. Во время войны он живет в эвакуации в Уфе, где преподаёт иностранные языки. Умер Кривош-Неманич в августе 1942 г. Хоронил его сын, однако через несколько лет останки выдающегося криптографа царской и советской России были перемещены в братскую могилу, следы которой затерялись [45]...

6. Первая мировая война

Общий недостаточный уровень подготовки России к войне отразился и на работе криптографической службы.

³Соловки, или СЛОИ, — Соловецкий лагерь особого назначения — первый концентрационный лагерь Советской России. Организован в 1923 г. на базе древнего Соловецкого монастыря, расформирован в 1933 г.

В то время в российской армии практически отсутствовала надёжная проволочная телеграфная связь, поэтому основное взаимодействие между частями велось по радиосвязи. Но никакого отлаженного механизма использования шифрованной радиосвязи не было. Вследствие беспорядка с распределением и согласованием шифров радиостанции часто «не понимали» друг друга. Им приходилось передавать свои сообщения открытым текстом...

«Такое легкомыслие очень облегчало нам ведение войны на Востоке, иногда лишь благодаря ему и вообще возможно было вести операции», — вспоминал немецкий военачальник М. Гофман, позднее — командующий германскими войсками на Восточном фронте.

«Русские пользовались своими аппаратами так легкомысленно, как если бы они не предполагали, что в распоряжении австрийцев имеются такие же приемники, которые без труда настраивались на соответствующую волну. Австрийцы пользовались своими радиостанциями гораздо экономнее и осторожнее и, главным образом, для подслушивания, что им с успехом удавалось. Иногда расшифровка удавалась путём догадок, а иногда при помощи прямых запросов по радио во время радиопередачи. Русские охотно помогали „своим“, как они считали, коллегам» — из отзыва М. Ронге — начальника разведывательного бюро австрийского генштаба (см. [13]).

Всё это очень грустно.

Ошибка с передачей специального военного шифра сыграла определённую роль в поражении армии А. В. Самсонова на Мазурских островах у Танненберга [43]. Во время восточно-прусской операции в августе 1914 г. две армии (Самсонова и Ренненкампа), выступив до завершения мобилизации, должны были оттянуть на себя часть немецких сил, тем самым сорвав основное наступление Германии против Франции. Но сценарий реализовался другой. При взаимодействии двух армий оказалось, что в армии П. К. Ренненкампа новый шифр уже получен, а старый уничтожен, а в армии Самсонова ещё действовал старый шифр. Поэтому радиопереговоры между ними велись в открытую, чем не могло не воспользоваться немецкое командование. Кроме того, армия Самсонова не имела запасов телеграфной проволоки, командованию и разведке приходилось использовать для связи даже телефоны местных жителей. В то же время посылаемые приказы командующего фронтом о своевременном отходе армий к определённым рубежам просто не доходили до Самсонова. Его армия попала в окружение и героически сражалась, оставшись без какой-либо поддержки. К ней на помощь должна была прийти армия Ренненкампа, но не пришла: по оценкам историков, это было фактическое предательство. В результате армия Самсонова была уничтожена. Потери составили десятки тысяч убитыми, ранеными и пленными [43]...

В сентябре 1914 г. российскому командованию всё-таки удалось обеспечить войска шифровальными средствами. Однако новый шифр был без труда раскрыт дешифровальной службой Австро-Венгрии уже через пять дней после его введения! Наши противники бесперебойно читали шифрпереписку русской армии. Потом они настолько привыкли к этому, что даже не отдавали приказов до тех пор, пока не получали очередной порции информации от своих дешифровальщиков.

В целом «войну в эфире» мы проиграли. Причинами этого послужили плохая организация шифрованной радиосвязи царских армий, слабость российских шифров и нарушения в их использовании. К этому необходимо добавить и то, что до войны в России не существовало военных дешифровальных отделений (они были только у Франции и Австро-Венгрии). Когда такие отделения были созданы, им не хватало со-

ответствующих специалистов и оборудования — например радиостанций пеленгации и перехвата.

Отметим и ряд успехов нашей криптографической службы. Перед войной и во время войны дешифровальная служба МИД работала довольно результативно. Ею читалась переписка многих иностранных государств (в первую очередь Австрии, Германии, Болгарии, Италии, Турции и др.). Позднее число перехваченных и дешифрованных телеграмм снизилось в связи с тем, что Германия и Австро-Венгрия стали чаще использовать телеграф, а не радиосвязь. В недавно созданных военных дешифровальных отделениях достаточно быстро вскрывались ключи немецкого морского шифра, что позволяло читать немецкие сообщения и приказы.

К числу успешных относится и операция по захвату кодовых книг с затонувшего немецкого крейсера «Магдебург» в 1914 г.

Приведём эту историю, следуя книге [13]. «В августе 1914 года наскочил на мель в восточной части Балтийского моря у острова Оденсхольм лёгкий немецкий крейсер „Магдебург“. Русские моряки сумели достать с этого крейсера кодовые книги ВМС Германии. Для того чтобы скрыть факт захвата кодовых книг с „Магдебурга“ от немцев, русские провели следующую операцию. Немцы не знали, что командир „Магдебурга“ Хабенихт при аварии был тяжело ранен и умирал в госпитале. В операции было решено использовать двойника командира немецкого крейсера. В Шлиссельбурге под охраной жил офицер русского флота И. И. Ренгартен. Он свободно говорил по-немецки и был внешне похож на Хабенихта. Как и рассчитывало русское командование Балтфлотом, немцы сумели выйти с ним на связь. Это было сделано с помощью немецких газет, которые „командир“ заказывал в шведском посольстве. Над буквами одной из статей Ренгартен обнаружил еле видные точки. Помеченные буквы складывались в следующий текст: «Где книги? Если уничтожили их, сообщите так: если утопили, попросите журнал „Иллюстрированные новости“, если сожгли, то „Шахматный журнал Кагана“ — номер, соответствующий номеру котла на „Магдебурге“». Ренгартен заказал „Шахматный журнал Кагана“ номер 14. Именно в этом котле крейсера русскими были сожжены фальшивые кодовые книги и подлинные обложки в свинцовом переплёте. На следующий день к сидящему на камнях „Магдебургу“ подошла немецкая подводная лодка. Высадившаяся из неё на крейсер группа извлекла пепел от „сгоревших кодовых книг“, остатки переплёта и кожи от обложек. Русские подводную лодку „не заметили“. Так немцы убедились в том, что кодовые книги с „Магдебурга“ уничтожены. В результате свой код они не сменили» [13].

Для России это был большой успех. Захваченными шифрами русские поделились с англичанами. Уинстон Черчилль, получивший доступ к этим документам, назвал их «бесценными». Англичане эффективно использовали русский подарок. Они не только дешифровывали ценные телеграммы, но и посылали сообщения от имени германского командования. Одно из таких сообщений привело к крупной победе англичан на море: была уничтожена немецкая эскадра под командованием генерала Шпее осенью 1914 г. недалеко от Южной Америки.

7. «На грани крушения»

Глубокий кризис, который переживала российская криптографическая служба, особенно остро ощущался самими криптографами. Многие из них искренно переживали за судьбу не только своей службы, но и России в целом. Юрий Александрович Колемин, управляющий шифровальной частью МИД, писал в своей докладной записке министру иностранных дел С. Д. Сазонову о необходимости немедленной реорганиза-

ции криптографической службы, находящейся, по его словам, «на грани крушения». Он писал о ничтожных окладах её сотрудников, об их «второсортном положении», а по сути об их ненужности государству. «На каком именно основании, — пишет Колемин, — они должны чувствовать солидарность с интересами своего дела?», ведь «добросовестность нельзя безнаказанно эксплуатировать». В его записке встречаются такие слова, как «крах», «безнадёжность», «банкротство»... Пользуясь активной поддержкой своих служащих, он предлагает организацию нового Отделения, детально разрабатывает принципы его устройства, вкладывает в это дело «всю свою душу»! Но этим планам не суждено было реализоваться. На пороге стоял 1917 год. И история начиналась совсем другая.

8. Глеб Бокий и начало советской криптографии

По ночам Самбикин долго не мог заснуть от воображения труда на советской земле, освещённого сейчас электричеством. Он вставал с кровати, зажигал свет и ходил в волнении, желая предпринять что-либо немедленно. Он включал радио и слышал, что музыка уже не играет, но пространство гудит в своей тревоге, будто безлюдная дорога, по которой хотелось уйти.

А. Платонов. Счастливая Москва

Пятого мая 1921 г. при ВЧК был создан Спецотдел, заведовавший криптографическими делами. Отдел находился на особом положении: его действия координировались непосредственно Политбюро. Распоряжения Спецотдела по всем вопросам шифрования были обязательными к исполнению всеми ведомствами РСФСР. Возглавил новую криптографическую службу Глеб Иванович Бокий (1879–1937), соратник В. И. Ленина.

Об этом человеке трудно найти какую-либо информацию. Особенно непротиворечивую. Историк Т. А. Соболева в своей книге [43] пишет: «Даже в моём собственном окружении, в той самой службе КГБ, которая была детищем Бокия и которую он возглавлял 17 лет, о нём почти никто ничего не знал».



Рис. 3. Г. И. Бокий

Дворянин Г. И. Бокий вступил в Российскую социал-демократическую рабочую партию (РСДРП) в 1900 г. Кстати, его партийный билет был номер 7. «Бокий, как и Сталин, в предреволюционный и революционный период входил в ядро, руководящую верхушку большевистской партии» [43]. На протяжении 20 лет (с 1897 по

1917 г.) он являлся одним из руководителей петербургского большевистского подполья. За это время Бокий двенадцать раз подвергался арестам, провёл полтора года в одиночной камере, два с половиной года — в сибирской ссылке, от побоев в тюрьме получил травматический туберкулёз [37]. Параллельно с революционной деятельностью он учился в Петербургском горном институте, работал гидротехником и горным инженером. Основательно изучал философию и политэкономия. «Работал над своим образованием настолько упорно, что позволял себе спать не более четырёх часов в сутки» [43].

Максим Горький писал о нём так: «Человек из породы революционеров-большевиков старого, несокрушимого закала. Я знаю почти всю его жизнь, всю работу и мне хотелось бы сказать ему о моём уважении к людям его типа, о симпатии лично к нему. Он, вероятно, отнёсся бы к такому „излиянию чувств“ недоумённо, оценил бы это как излишнюю и, пожалуй, смешную сентиментальность» [22].

В советский период Г. И. Бокий не только руководил Спецотделом, но и был членом ВЧК, затем коллегии ОГПУ и НКВД, входил в состав «троек» ОГПУ. Он был одним из активных создателей системы ГУЛАГ, в частности уже упоминавшегося Соловецкого лагеря. Именем Бокия был назван пароход, в трюме которого в Соловки привозили новых заключённых. Известный советский учёный-филолог Дмитрий Сергеевич Лихачёв, узник Соловков, вспоминал свою поездку на пароходе так: «Вывели нас на пристань с вещами, построили, пересчитали. Потом стали выносить трупы задохшихся в трюме или тяжело заболевших: стиснутых до перелома костей, до кровавого поноса...» [33]. А однажды на пароходе прибыл и сам «куратор Соловков». Но это был его рабочий визит. Заключённые лагеря сочинили тогда такие строки [45]:

«В волнение все, но я спокоен.
Весь шум мне кажется нелеп:
Уедет так же, как приехал,
На „Глебе Боком“ — Бокий Глеб».

На службе у Бокия работали некоторые криптографы царской России. Был здесь В. И. Кривош-Неманич, И. А. Зыбин, дешифровавший в своё время переписку Ленина, И. М. Ямченко, бывший начальник врангелевской радиостанции. В создании службы участвовали и люди, ранее не работавшие в области шифрования. Зять Бокия, писатель Лев Разгон, вспоминал: «В спецотделе работало множество самого разного народа, так как криптографический талант — талант от Бога. Были старые дамы с аристократическим прошлым, был немец с бородой почти до ступней» и множество других непонятных людей.

К работе на Спецотдел Бокий привлек и учёного-мистика А. Барченко, исследовавшего биоэлектрические явления в жизни клетки, в работе мозга и в живом организме в целом. Свои лабораторные опыты Барченко совмещал с должностью эксперта Бокия по психологии и парапсихологии. В частности, им разрабатывалась методика выявления лиц, склонных к криптографической работе. Учёный выступал консультантом при обследовании всевозможных знахарей, шаманов, гипнотизёров и прочих людей, утверждавших, что они общаются с призраками. С конца 1920-х годов Спецотдел активно использовал их в своей работе. Как отмечается в книге [37], исследования и методика Барченко применялись и в особенно сложных случаях дешифрования вражеских сообщений — в таких ситуациях проводились сеансы связи с духами.

Первый успех новой криптографической службы относится к 1921 г.: был раскрыт немецкий дипломатический код. С этого времени и вплоть до 1933 г. контролировалась переписка многих линий дипломатической связи Германии и её консульств в СССР.

С 1921 г. читалась переписка внутренних линий связи Турции. В 1924 г. были вскрыты два шифра польского разведотдела генерального штаба, которые использовались для связи с военными атташе в Москве, Париже, Лондоне, Вашингтоне и Токио. В 1927 г. началось чтение японской переписки, в 1930 г. — переписки некоторых линий связи США. Разрабатывались коды и других стран.

Одновременно со «взломом» чужих шифров шла напряжённая работа по созданию своих. В 1924 г. на основе 52 различных шифров был создан так называемый «русский код», дешифровать который не удалось никому. В литературе по истории криптографии об этом коде нет информации. По одним источникам, «на десятилетия он стал основным шифром для всех служб СССР», по другим — такого кода никогда не было.

Несмотря на большой спектр решаемых задач, спецотдел в ВЧК, а затем в ОГПУ был в их структуре самым засекреченным. Его сотрудникам запрещалось даже родным говорить, где они работают.

В 30-е годы руководство криптографической службой сменилось, а Глеб Бокий был расстрелян.

Его жизнь окружена множеством легенд. Кто-то их подтверждает, кто-то яростно опровергает. Часто говорится о связи Г. И. Бокия с представителями тайных обществ, о его поисках Шамбалы — страны вечных мудрецов, по преданию, затерянной где-то в Азии. В 1925 г. он даже планировал туда научную экспедицию, но запретило Политбюро.

Одни считали Бокия «страшным человеком», устраивавшим тайные оргии на своей даче. Вспоминали, что некоторые сотрудники спецотдела, принимавшие в них участие, потом заканчивали жизни самоубийством. Атмосферу созданной им «дачной коммуны» сравнивали с атмосферой Великого бала у сатаны в романе его современника М. А. Булгакова «Мастер и Маргарита». Только в действительности, вспоминали очевидцы, было ещё страшнее. Другие с возмущением отвергали подобные «байки», считая их «версией, которую пустили в обиход после ареста Бокия». Эти люди вспоминали Бокия как «интеллигентного и весьма скромного человека, никогда и никому не пожимавшего руки и отказывавшегося от всех привилегий». Как человека, который «на сделку с совестью не шёл никогда».

9. Секретная связь во время Великой Отечественной войны

В этом и следующих разделах речь пойдёт о методах секретной связи и криптографии в СССР во время Великой Отечественной войны и в период подготовки к ней. Это и секретная телефонная связь, и радиосвязь, и создание текстовых шифраторов.

Первые разработки аппаратов секретного телефонирования в СССР относятся к 1927–1928 гг., когда в Научно-исследовательском институте связи РККА были изготовлены для погранохраны и войск ОГПУ шесть телефонных аппаратов ГЭС (конструктор Н. Г. Суэтин). В 1930-х годах в области секретной телефонии вели работы семь организаций: НИИ НКПиТ (наркомата почт и телеграфа), НИИС РККА, завод имени Коминтерна, завод «Красная Заря», НИИ связи и телемеханики ВМФ, НИИ № 20 Наркомата электропромышленности (НКЭП), лаборатория НКВД.

ВЧ-связь. В 1930 г. заработали первые линии междугородной правительственной высокочастотной связи (ВЧ-связи) Москва — Ленинград и Москва — Харьков. Отметим, что сама технология ВЧ-связи без применения аппаратуры шифрования была совершенно ненадёжна и могла защитить только от прямого прослушивания. В 1935–1936 гг. на заводе «Красная Заря» было создано устройство автоматического засекречивания телефонных переговоров — *инвертор ЕС* (названный по фамилиям разра-

ботчиков К. П. Егорова и Г. В. Старицына) — и налажен его выпуск для каналов телефонной ВЧ-связи. Практически на всём протяжении Великой Отечественной войны и позднее для организации ВЧ-связи успешно использовались устройства этого типа. К 1941 г. в СССР функционировало 116 ВЧ-станций и 39 трансляционных пунктов, а число абонентов высшего партийного и государственного руководства достигло 720.

К первому периоду войны относится разработка портативной, исполненной в виде чемодана, засекречивающей аппаратуры СИ-15 («Синица») и САУ-16 («Снегирь»), которая использовалась в основном при выездах высшего командного состава в пункты, не имевшие ВЧ-станций.

В 1938–1939 гг. в Центральном научно-исследовательском институте связи были созданы две лаборатории по засекречиванию телеграфной и телефонной информации. Возглавил их выдающийся учёный Владимир Александрович Котельников. Это человек, сыгравший ключевую роль в организации надёжной секретной связи самого высокого уровня во время Великой Отечественной войны и после неё.

Секретная телеграфная связь. В. А. Котельниковым впервые в СССР были разработаны принципы построения телеграфной засекречивающей аппаратуры путём наложения на сообщение знаков гаммы (аппаратура «Москва»).

Как приводится в работе [11], «Сам шифратор, сконструированный на электромеханических узлах, был сложным и громоздким. В основе конструкции лежал барабан, заполненный шариками. При вращении барабана через систему штырей из щелей шарики случайным образом скатывались по шести вертикальным трубкам на две движущиеся телеграфные ленты, которые были наложены одна на другую через „копирку“. В результате на обеих лентах получался одинаковый рисунок — „дорожки“ из случайно расположенных пятен. Затем по этим меткам ленты перфорировались. Эти ленты образовывали случайный ключ и рассылались на пункты установки аппаратуры».

Сама схема наложения гаммы на открытый текст была уже хорошо известна к тому времени благодаря изобретению Гильберта Вернама 1917 г. Она оказалась очень привлекательной и долгое время использовалась в аппаратуре последующих поколений.

Секретная телефонная связь. В 1939 г. В. А. Котельникову было поручено решение важной государственной задачи — создание шифратора для засекречивания речевых сигналов с повышенной стойкостью к дешифрованию.

В лаборатории Котельникова было установлено, что для хорошей маскировки речевого сигнала необходимо использовать *частотные преобразования* и *временные перестановки* отрезков речи одновременно [12]. Эти принципы легли в основу новой разработанной под руководством Котельникова сложной засекречивающей аппаратуры С-1 («Соболь») [28], которая стала широко использоваться в действующей армии. Несмотря на все трудности, уже к осени 1942 г. сотрудники лаборатории Котельникова изготовили несколько образцов оборудования «Соболь-П». Согласно работе [11], это была самая сложная аппаратура засекречивания информации, не имевшая аналогов в мире. «Соболь-П» использовался для обеспечения секретной связи самого высокого уровня (Ставки Верховного Главнокомандующего со штабами фронтов), причём впервые такая связь осуществлялась с помощью радиоканала. Заменить относительно безопасный проводной канал связи на радиоканал для связи такого уровня оказалось возможно только благодаря *исключительной стойкости* использованного шифрования.

Как вспоминали ветераны ВОВ, применение шифраторов Котельникова в ходе решающих боев на Курской дуге в значительной степени определило успешный исход битвы [11]. По сведениям советской разведки, Гитлер заявлял, что за одного крип-

тоаналитика, способного «взломать» советскую радиосвязь, он не пожалел бы трёх отборных дивизий.

Уже в то время В. А. Котельников понимал, что для обеспечения высокой стойкости и уровня маскировки речевого сигнала необходимо сначала проводить сжатие речи [12]. Поэтому параллельно с разработкой «Соболя-П» В. А. Котельников проводил работы по созданию *вокодера* — устройства, обеспечивавшего компрессию спектра речи примерно в 10 раз. К октябрю 1941 г. вокодер начал «говорить». В ноябре 1941 г. лаборатория продолжила свою работу в Уфе, куда была эвакуирована.

За создание шифраторов В. А. Котельников и его коллеги по лаборатории (И. С. Нейман, Д. П. Горелов, А. М. Трахтман, Н. Н. Найдёнов) получили в марте 1943 г. Сталинские премии I степени. Все разработки были жёстко засекречены. Сотрудник лаборатории Е. В. Руднев передает атмосферу секретности в своих стихах-воспоминаниях [39]:

«В 43-м весною, по радио
Мы узнали — трудились не зря.
Золотыми нагрудными знаками
Удостоена эта работа была.
Первый том был написан В. А.
Мой четвёртый — последний,
Между ними два тома Д. Б. и Ю. С.
Все четыре — под грифом С. С.»

Аппаратура «Соболь-П» очень активно использовалась в дальнейшем. После окончания Второй мировой войны она получила применение и на дипломатических линиях связи Москвы с Хельсинки, Парижем и Веной при проведении переговоров по заключению мирных договоров, а также при проведении Тегеранской, Ялтинской и Потсдамской конференций и для связи с Москвой нашей делегации во время принятия капитуляции Германии в мае 1945 г. За дальнейшие разработки в области шифраторов Котельникову и его группе в 1946 г. была повторно присуждена Сталинская премия I степени.

Одновременно с созданием аппаратуры засекречивания в СССР проводились и работы по её дешифрованию. Было установлено, что аналоговая аппаратура шифрования мозаичного типа теоретически дешифруема. Для того чтобы получить недешифруемую аппаратуру засекречивания телефонных переговоров, речь необходимо переводить в *цифровую форму*.

В 1941 г. Владимир Александрович доказал, что можно создать *математически недешифруемую систему* засекречивания, если каждый знак сообщения будет засекречиваться выбираемым случайно и равновероятно знаком гаммы. Параллельно и независимо к этим идеям пришёл выдающийся американский учёный Клод Шеннон. Подобные системы он стал называть *совершенно секретными шифрами*. Такие системы, как показал В. А. Котельников, должны быть цифровыми, а преобразование аналогового сигнала в цифровую форму должно основываться на доказанной им *теореме отсчётов* (другое название — *теорема дискретизации*). Эта теорема, как и другие результаты В. А. Котельникова, прочно вошла в Золотой фонд классических результатов современной теории информации.

Теорема Котельникова. Если аналоговый сигнал $s(t)$ имеет ограниченный спектр, то он может быть восстановлен однозначно и без потерь по своим дискретным отсчётам, взятым с частотой не менее удвоенной максимальной частоты спектра.

Другими словами, теорема говорит о возможности восстановления непрерывных функций с ограниченным спектром по их значениям через определённые интервалы времени. Заслуга Котельникова состоит в том, что он первый осознал возможности приложений этого математического факта и осуществил удачный выбор класса функций для дискретизации. В зарубежной литературе эта теорема более известна как теорема Найквиста — Шеннона.

С этих результатов В. А. Котельникова, представленных в секретной научной работе «Основные положения автоматической шифровки» (1941) и независимо полученных К. Шенноном в 1945 г., и началась криптография как наука. Для криптографических методов впервые за всю историю их развития был разработан строгий математический аппарат.

Необходимо отметить, что результаты К. Шеннона были опубликованы в открытой печати, тогда как работы В. А. Котельникова долгое время оставались засекреченными. Поэтому приоритет в этой области по праву закреплён за К. Шенноном.

После войны, 21 января 1948 г., была создана секретная Марфинская лаборатория [28] для работы над следующими проблемами:

- дискретизация непрерывного речевого сигнала;
- увеличение скорости передачи двоичных сигналов;
- разработка высокоскоростного шифратора;
- создание нового направления — криптографического анализа.

Однако В. А. Котельников отказался возглавить лабораторию; он только её курировал. В это время он продолжал работать в Московском энергетическом институте (МЭИ). Руководил Марфинской лабораторией А. М. Васильев.

В новой лаборатории вместе с вольными работала заключённые спецтюрьмы № 16 МГБ СССР. На проведение всех работ руководство страны поставило сверхкороткий срок — полтора года! Атмосфера была очень напряжённой. Марфинская криптографическая лаборатория описана в романе А. И. Солженицына «В круге первом». Правда, как вспоминал в 2003 г. В. А. Котельников, «Солженицын не слишком правильно описал атмосферу в лаборатории. „Вольным“ приходилось работать больше, чем заключённым, и кормили их много хуже. Усложняла работу и обстановка излишней секретности. Закрытость и секретность вообще много вреда принесли нашей науке» [26].

10. В. А. Котельников

Владимир Александрович Котельников (1908–2005) родился в Казани, в семье университетского профессора — известного математика Александра Петровича Котельникова. Его дед, Пётр Иванович Котельников, также всю жизнь проработал математиком в Казанском университете и, между прочим, был первым математиком, который открыто поддержал смелые работы Н. И. Лобачевского о неевклидовой геометрии.

В 1926 г. Владимир Александрович поступил в Московское высшее техническое училище им. Баумана, на последних курсах перешел в отделившийся от училища Московский энергетический институт, который и окончил в 1930 г., получив звание инженера-электрика. Однако научная деятельность В. А. Котельникова началась раньше — в 1930 г. в НИИ связи Красной Армии, куда он был зачислен в качестве инженера. Одновременно с научной деятельностью с 1931 по 1941 г. В. А. Котельников преподавал на кафедре радиотехники МЭИ. В конце 30-х годов и в годы войны Владимир Александрович занимался разработкой специальной шифровальной аппаратуры связи. Достигнутые им криптографические успехи без преувеличения внесли огромный

вклад в нашу победу, а сам В. А. Котельников снискал себе негласный титул «патриарха секретной телефонии».

В конце 40-х годов Владимир Александрович организовал Особое конструкторское бюро МЭИ, ставшее впоследствии одним из ведущих предприятий в области космической техники. С 1954 г. В. А. Котельников возглавил недавно созданный Институт радиотехники и электроники (ИРЭ), получивший при нём мощное развитие.

В 90-е годы В. А. Котельников был одним из шести основателей Академии криптографии. Он принимал активное участие в работе её советов и комиссий.

Обширные научные интересы Владимира Александровича включали в себя общую и прикладную физику; радиофизику, радиотехнику и электронику; теорию информации, в частности — методы защиты информации от помех в системах радиосвязи и криптографию, практические вопросы разработки специальной аппаратуры связи; исследования космоса, в особенности созданное им направление планетной радиолокации и многое, многое другое. Во всех этих областях В. А. Котельников получил существенные результаты.

В. А. Котельников — лауреат Ленинской премии, дважды лауреат Государственной премии СССР, дважды Герой Социалистического труда. Он награждён шестью орденами Ленина, орденом «За заслуги перед Отечеством» I степени, другими орденами и медалями, в частности орденом «За заслуги перед Москвой». Хоть и с большим опозданием, его научные заслуги были признаны во всем мире. В 1999 г. ему были присуждены высшие международные награды — премия Э. Рейна и Золотая медаль А. Белла. Решением Международного астрономического союза астероид № 2726 носит имя «Kotelnikov». Президент Международного института электронной и электрической инженерии Брюс Эйзенштейн (США) признавал самый существенный вклад Котельникова в развитие радиосвязи и криптографии, он говорил: «Over the years the West had its Shannon; and the East had its Kotelnikov».



Рис. 4. В. А. Котельников

Полученные звания и награды не стали препятствием основному делу его жизни: Владимир Александрович сохранил научную активность до самого последнего времени. Его творческий и земной путь завершился на 97-м году жизни почти законченной, но не опубликованной работой «Модельная квантовая механика».

Коллеги В. А. Котельникова отмечали его выдающиеся личные качества. «Прежде всего, это необычайная серьёзность в подходе к решению любого вопроса, будь то государственная проблема или личная проблема сотрудника. Далее, неизменная доброжелательность, обязательность в выполнении обещанного, стремление всегда решить

вопрос, не откладывая на завтра, — вот те замечательные качества, которые характеризовали Владимира Александровича как руководителя и как человека» (директор ИРЭ академик Ю. В. Гуляев) [24].

На работе и в жизни Владимир Александрович был скромен и прост. Он умел видеть главное и быть требовательным. Читая воспоминания [30] тех, кому посчастливилось работать с ним, отмечаешь, что в присутствии Владимира Александровича людям неожиданно становилось... стыдно. За себя, за недостатки в своей работе. И они старались работать лучше, не позволяя себе «халтуры», и сами менялись к лучшему.

11. Немного о советских шифрмашинах

Когда речь заходит о шифровальной технике времён Второй мировой войны, то, как правило, вспоминают знаменитую немецкую шифровальную машину «Энигма» — изобретение инженера Артура Шербиуса 1918 г. Этим дисковым шифратором с 1926 г. стали оснащаться вооружённые силы и спецслужбы Германии. Наиболее востребованной «Энигма» стала после прихода к власти Гитлера и особенно во время войны. По некоторым оценкам, для вооружения немецкой армии было выпущено до 100 000 её экземпляров.

Вспоминают тайную работу по дешифрованию «Энигмы», которая велась в разных странах и увенчалась успехом. На протяжении войны немецкие сообщения тайно читались англичанами, американцами, русскими и др.

Первый математический аппарат для дешифрования «Энигмы» разработали выпускники Познаньского университета (Польша) Мариан Раевский, Генрих Зыгальский и Ежи Розицкий (см. подробнее [13, 29, 42]). В 2008 г. в Познани о них был снят документальный фильм [46]. Результатами польских криптоаналитиков воспользовались англичане. Ими была спланирована масштабная операция «Ультра», нацеленная как на аналитическое дешифрование сообщений «Энигмы», так и на захват её действующих кодовых книг. Об этой успешной операции и её главном криптографическом центре в Блетчли-парке написано довольно много. Большой объём сведений можно найти и о самой «Энигме».

А какими были советские шифрмашинны?

До последнего времени информации о них практически не было.

«...кто возьмет в плен русского шифровальщика, либо захватит русскую шифровальную технику, будет награждён Железным крестом, отпуском на родину и обеспечен работой в Берлине, а после окончания войны — помещён в Крыму».

«Эти проклятые русские шифровальные машины, мы никак не можем их расколоть!»

Многое дают понять эти слова Гитлера. Он инициировал настоящую охоту за советскими шифровальщиками. Однако немцам так и не удалось дешифровать сообщения, зашифрованные с помощью советской техники. С 1942 г. эти сообщения перестали перехватывать. Благодаря разработанной перед войной шифровальной технике Советскому Союзу удалось скрыть свои стратегические планы. Это был огромный успех нашей шифровальной службы!

В подтверждение приведём несколько цитат.

«Ни одно донесение о готовящихся военно-стратегических операциях нашей армии не стало достоянием фашистских разведок» (начальник Генштаба Маршал Советского Союза А. М. Василевский).

«Хорошая работа шифровальщиков помогла выиграть не одно сражение» (зам. Верховного Главнокомандующего Маршал Советского Союза Г. К. Жуков).

В своих показаниях начальник штаба при ставке верховного главнокомандования немецких вооружённых сил генерал-полковник А. Йодль сообщал: «Радиоразведка играла особую роль в самом начале войны, но и до последнего времени не теряла своего значения. Правда, нам никогда не удавалось перехватить и расшифровать радиограммы вашей ставки, штабов фронтов и армий. Радиоразведка, как и все прочие виды разведок, ограничивалась только тактической зоной» [32].

Первая попытка создать текстовый электромеханический шифратор в СССР была предпринята в 1923 г. в Особом техническом бюро по военным изобретениям специального назначения. Найти какую-либо информацию об этой попытке достаточно трудно.

В 30-е годы образцы советской шифровальной техники создавались под руководством талантливого инженера Ивана Павловича Волоска. Шифрмашины того времени реализовывали наложение случайной последовательности (гаммы) на открытое текстовое сообщение. Даже сейчас такой подход абсолютно современный и при выполнении некоторых условий может обеспечивать гарантированную стойкость шифрования.

В-4, М-100 — одни из первых советских шифрмашин, реализующих шифры гаммирования. В 1938 г. началось их серийное производство.

«Шифровальная машина М-100 состояла из трёх основных узлов: клавиатуры с контактными группами, лентопротяжного механизма с транзиттером и приспособления, устанавливаемого на клавиатуру пишущей машинки, и семи дополнительных блоков. Общий вес комплекта достигал 141 кг. Только одни аккумуляторы для автономного питания электрической части машины весили 32 кг. Тем не менее данная техника выпускалась серийно и в 1938 г. была успешно испытана в боевых условиях во время гражданской войны в Испании (1936–1939 гг.), на Халхин-Голе (1939), во время советско-финской войны (1939–1940 гг.). Шифрованная связь в этих военных конфликтах осуществлялась в звене Генеральный штаб — Штаб армии» [11].

Позднее появились и более компактные машины, например К-37 («Кристалл»), М-101 («Изумруд») и другие. Наряду с шифрами гаммирования применялись и шифры многоалфавитной замены. После войны в СССР использовались такие шифрмашинки, как М-105 «Агат», М-125 «Фиалка» и др.

Широко использовалось и ручное шифрование. Телеграммы отправлялись с помощью лёгких, весом в три килограмма, радиостанций «Север», или «Северок», как их ласково называли военные связисты. Эта техника, быстро завоевавшая симпатии наших разведчиков и партизан, выпускалась в блокадном Ленинграде.

На машинную шифросвязь в годы войны легла основная нагрузка при передаче секретных телеграмм. И с этой нагрузкой, как уже отмечалось выше, наша шифровальная служба справилась блестяще. Только в 8-м Управлении Красной Армии за период с 1941 по 1945 г. было обработано свыше 1,6 миллионов шифротелеграмм.

Не будем забывать про эти успехи.

Известно много примеров героического поведения наших шифровальщиков на войне [32]. Офицеры спецсвязи на грани жизни и смерти, часто с тяжелейшими ранениями уничтожали шифровальные документы перед приходом врага. В большинстве случаев это было то последнее, что они успевали сделать перед смертью. Советские шифровальщики под страшными пытками не выдавали ни наших кодовых таблиц, ни особенностей использования нашей шифровальной техники. Без этого личного героизма секретная работа даже самой надёжной шифровальной техники была бы невозможна.

Успехи нашей дешифровальной службы во время войны требуют отдельного исследования. Приведём лишь один пример. Как отмечает в своём интервью Н. Н. Андреев,

бывший руководителем 8-го Главного Управления КГБ, с 1992 по 1998 г. — президент Академии криптографии РФ, «во время войны мы читали японскую дипломатическую переписку, анализ которой позволил сделать вывод о том, что Япония не намерена начинать военные действия против СССР, что дало возможность перебросить значительные силы на германский фронт» [27].

12. После войны

О том, как развивалась отечественная криптография после войны, есть только обрывочные сведения.

Ещё с 1 сентября 1939 г. в СССР велась подготовка военных криптографов. С момента образования Спецотдела ВЧК и вплоть до Великой Отечественной войны каких-либо стационарных учебных заведений (кроме краткосрочных курсов и школ) для подготовки профессионалов-криптографов не было. В эти годы основы криптографии преподавались в Военно-инженерной академии имени В. В. Куйбышева и в Военной академии связи в Ленинграде.

В Спецотделе разрабатывались и первые учебники по криптографии. Среди них — пособие «Шифры и их применение» (1933), учебник «Криптография (шифрование и дешифрование)» (авторы А. И. Копытцев, С. Г. Андреев, С. С. Толстой, Б. А. Аронский, 1939). В эти же годы был подготовлен, а в 1951 г. издан учебник «Введение в криптографию» (автор М. С. Одноров). Учебник состоял из четырёх частей (общим объёмом 737 страниц), содержал большое количество примеров, построенных на реальных материалах (подробнее см. [38]).

В 1940 г. при ОГПУ была создана криптографическая школа особого назначения (ШОН), которая с началом войны перебазировалась в Уфу. Именно там, в криптографической школе, преподавал иностранные языки удивительный В. И. Кривош-Неманич. Кстати, языковой подготовке в СССР уделялось очень большое внимание. Считалось, что каждому криптографу следует владеть хотя бы одним иностранным языком.

В начале 1946 г. при Высшей школе НКГБ были организованы криптографические курсы, которые позднее послужили основой подготовки криптографов на закрытом отделении механико-математического факультета МГУ. Такое отделение было создано в 1949 г. и просуществовало до 1957 г.; его возглавлял Георгий Иванович Пондопуло (1910–1996).

Как вспоминает выпускник закрытого отделения мехмата В. Н. Сачков, «в послевоенные годы в связи с резким увеличением информационного обмена и необходимостью его надёжной защиты, а также с целью повышения эффективности дешифровальной работы возникла потребность существенного усиления криптографических служб ведущих держав. С этой целью в Советском Союзе в 1949 г. было создано Главное управление специальной службы (ГУСС), а в США в 1952 г. — Агентство национальной безопасности (АНБ). Деятельность как ГУСС, так и АНБ протекала в условиях строгой секретности» [41].

19 октября 1949 г., в год четырёхсотлетия российской криптографической службы, были созданы Главное управление Специальной службы и *Высшая школа криптографов* (ВШК). ВШК стала первым и единственным в стране высшим учебным заведением такого профиля. Впоследствии она была преобразована в Высшую школу криптографов 8-го Управления МВД СССР, затем — в Высшую школу криптографов КГБ при Совете Министров СССР, затем — в технический факультет Высшей школы 8-го Главного управления КГБ при СМ СССР, а в 1992 г. — в *Институт крипто-*

графии, связи и информатики (ИКСИ). Все эти годы днём рождения ИКСИ и его предшественников считается 19 октября [38].

Позволим небольшое отступление от хронологии: 19 октября — это день рождения ещё одного учебного заведения — Царскосельского лицея, особо почитаемый его первыми выпускниками. Помните у А. С. Пушкина:

«Кому ж из нас под старость день лицея
Торжествовать придется одному?»

«Торжествовать» пришлось Александру Михайловичу Горчакову (1798–1883), российский дипломату, министру иностранных дел России с 1856 по 1882 г. Любопытно вспомнить его здесь как человека, на самом высоком уровне причастного к криптографической деятельности. Ведь именно министр иностранных дел в XIX веке контролировал шифровальную службу.

С 40-х годов XX века криптографические задачи стали существенно сложнее и математичнее. В ряде институтов, таких, как Математический институт им. В. А. Стеклова, были созданы закрытые отделы для их решения. Например, в терминах теории вероятностей и математической статистики решалась задача о критерии открытого текста. Она заключалась в том, чтобы из всевозможных «хаотических» вариантов, которые получаются при дешифровании перехваченного сообщения, выделить единственный верный вариант. Для этого нужно было очень тонко учитывать статистические особенности, присущие неизвестному «правильному» тексту, составленному на том или ином языке.

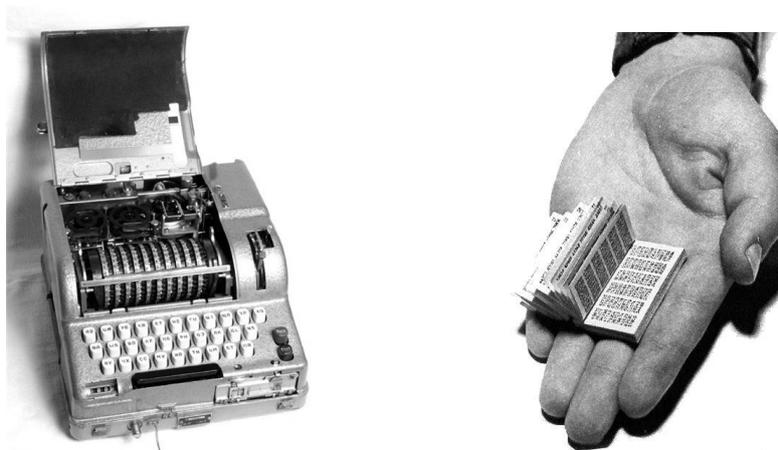


Рис. 5. Шифрмашинa M-125 «Фиалка»; кодовая книга советского разведчика (одноразовый блокнот)

Как отмечается в книге [38], в 50-е годы в Высшей школе активизировалась работа по подготовке специалистов-криптографов. В 1955 г. в ВШ был создан учёный совет, стали готовиться научные работы и диссертации. Большой творческий вклад в подготовку научных кадров внёс член-корреспондент Академии наук СССР Владимир Яковлевич Козлов (1914–2007) — им подготовлено более 25 кандидатов и докторов наук [4]. Забота о становлении, развитии и укреплении дневного отделения подготовки криптографов (создано в 1962 г.) легла на плечи Ивана Яковлевича Верченко (1907–1995), очень уважаемого студентами преподавателя, декана технического факультета Высшей школы КГБ [40].

По заказам оборонных предприятий криптографические исследования проводились во многих вузах страны (см., например, [2]). Результаты исследований публи-

ковались в закрытых сборниках, о которых и сейчас мало информации. Попытки опубликовать криптографические результаты в открытой печати, предпринимавшиеся отдельными исследователями, были безуспешны. Так, рукопись А. Д. Закревского «Метод автоматической шифрации сообщений» 1959 г. была не принята к печати из-за её высокой секретности; автору пришлось сменить область своих исследований. Спустя 50 лет рукопись была опубликована в журнале «Прикладная дискретная математика» [25].

В целом, специалисты-криптографы высоко оценивали работу нашей шифровальной службы послевоенного времени. Американский криптограф Дэвид Кан так описывает криптографические успехи СССР 50–60-х годов: «Россия сама по себе остаётся загадкой, овеянной тайной из тайн. То же самое касается и её средств связи. Одно-разовые шифроблокноты обеспечивают надёжную защиту для сообщений российских разведчиков, военных, дипломатов и работников тайной политической полиции. Грамотно сконструированные шифраторы навечно сохраняют в секрете от врагов России её наиболее важную дипломатическую, агентурную и военную переписку. В период „холодной войны“ русские сумели вскрыть шифры американского посольства в Москве. Такие подвиги свидетельствуют об их осведомлённости, базирующейся на глубоком понимании шифровального дела и криптоанализа. Так или иначе русские вознесли достижения своей страны в криптологии до высоты полёта её космических спутников» [29].

Однако не всё было гладко. С начала 40-х годов и вплоть до 1 октября 1980 г. в контрразведке США действовал проект Venona, направленный на дешифрование советских сообщений. Успехи американцев привели к раскрытию нескольких советских разведчиков и утечке секретных сведений. Официально проект был рассекречен в США в 1995 г.

В отличие от других стран, в СССР все исследования по криптографии были сильно засекречены. Почти вплоть до распада Союза «упоминание слова „криптография“ в открытой печати даже в невинном контексте часто вызывало в инстанциях резкие возражения и обычно под тем или иным предлогом приводило к запрещению этого упоминания» [31].

До сих пор большинство архивов по истории российских спецслужб (в том числе по истории криптографии) остаются закрытыми. Более того, как отмечается в книге А. Солдатова и И. Бороган [44], «некоторые архивы, открытые в 1990-е, были вновь засекречены в недавнее время».

13. Современность

«Остановиться бы тогда, в конце 80-х годов, снять с глаз тёмные очки и оглядеться вокруг на окружающую действительность. Была же ведь реальная возможность побороться за мировые рынки сбыта наукоёмкой криптографической продукции, программ и алгоритмов, была возможность даже в каком-то смысле стать законодателями криптографической моды. Были и идеи, и отличные молодые специалисты...», — так рассуждает в своей книге «Криптография и свобода» [34] криптограф М. Е. Масленников, выпускник 4-го факультета Высшей школы, с 1979 по 1993 г. сотрудник 8-го Главного управления КГБ, ныне — свободный житель Южной Кореи.

Но возможность была упущена. Тогда, в конце 80-х, криптографическая служба России была не готова к переменам. Как в далёком 1917 году, она переживала тяжёлые времена.

И всё же они миновали. Страна выдержала. Выдержала и обновилась криптографическая служба. Начиная с 90-х годов в России стала развиваться гражданская криптография. Теперь криптография изучается в гражданских вузах, многие статьи и книги по криптографии публикуются в открытой печати, широко используются криптографические средства защиты информации.

Отметим лишь некоторые события последних десятилетий в области российской криптографии и защиты информации.

В 70–80-х годах был разработан блочный шифр ГОСТ 28147-89, ставший с 1990 г. государственным стандартом России. Он был рассекречен в 1994 г.

В 1991 г. было создано Федеральное агентство правительственной связи и информации при Президенте РФ (ФАПСИ). Упразднено в 2003 г.

В 1992 г. в России была создана Академия криптографии. Её первым президентом стал Н. Н. Андреев. Идею создания Академии поддержали академики и члены-корреспонденты РАН: В. А. Котельников, Ю. В. Прохоров, В. Я. Козлов, В. К. Левин, Б. А. Севастьянов. Академия решает задачи государственной важности по обеспечению национальной безопасности и обороноспособности страны [27].

В 90-е и 2000-е годы защиту информации и криптографию начали изучать в гражданских вузах страны.

В 1995 г. был издан Указ Президента РФ от 03.04.1995 г. № 334 о мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации. Согласно Указу, был наложен запрет на использование, разработку, производство, реализацию и эксплуатацию шифровальных средств юридическими и физическими лицами без наличия лицензий ФАПСИ.

В настоящее время криптографическая деятельность в России также подлежит обязательному лицензированию (см. Приказ ФСБ России от 09.02.2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение пкз-2005)», Постановление Правительства РФ от 29.12.2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»).

В 1997 г. была образована «Лаборатория Касперского». Её возглавляет Евгений Касперский — выпускник 1987 г. технического факультета Высшей школы КГБ СССР. Сейчас компания является одним из мировых лидеров в сфере программных решений для информационной защиты конечных пользователей.

В 1999 г. Институт криптографии, связи и информатики отметил своё 50-летие. Ко дню рождения вышла книга [38] об истории ИКСИ, ставшая библиографической редкостью.

В 1999 г. была создана Российская криптографическая ассоциация «РусКрипто», аналог международной организации IACR.

В 2003 г. на базе ФАПСИ была создана Служба специальной связи и информации Федеральной службы охраны РФ (Спецсвязь России).

В 2010 г. шифр ГОСТ был заявлен в качестве участника конкурса Международной организации по стандартизации (ISO) на приобретение статуса Всемирного стандарта шифрования (Worldwide Industrial Encryption Standard).

В апреле 2011 г. вступил в силу Закон об электронной подписи в РФ, согласно которому каждый гражданин России может завести себе электронную подпись.

В 2013 г. в 15-й и соответственно в 12-й раз пройдут российские конференции Рус-Крипто и SIBECRYPT по криптографии.

Вместо заключения

О советской криптографии сняты несколько документально-публицистических фильмов. Среди них:

- «Открытая закрытая связь» (режиссёр Д. Скворцов, 2006) — фильм об истории создания секретной телефонной связи в СССР.
- «Код Верченко» (режиссёр А. Трофимов, 2007) — фильм о советском криптографе И. Я. Верченко (1907–1995), сотруднике Марфинской лаборатории, позднее — декане технического факультета Высшей школы КГБ.

Для более глубокого знакомства с историей криптографии в России можно рекомендовать книги Т. А. Соболевой «История шифровального дела в России» [43], Ю. И. Гольева, Д. А. Ларина, А. Е. Тришина, Г. П. Шанкина «Криптография: страницы истории тайных операций» [13], А. В. Бабаша, Г. П. Шанкина «История криптографии» (часть 1) [5], Д. Кана «Взломщики кодов» [29], С. Сингха «Книга шифров. Тайная история шифров и их расшифровки» [42], главы по истории в книгах А. П. Алфёрова, А. Ю. Зубова, А. С. Кузьмина, А. В. Черёмушкина [3], В. И. Нечаева [35], В. М. Фомичёва [47]. Российской криптографии XIX века и начала XX века посвящены статьи А. В. Бабаша, Ю. И. Гольева, Д. А. Ларина, А. Е. Тришина, Г. П. Шанкина [6–10, 14–21]. О вкладе Х. Гольдбаха и Ф. Эпинуса в российскую криптографию можно прочитать в работе В. К. Новика [36]. Дополнительно о В. И. Кривоше-Неманиче см. публикации [23, 45]. О криптографии во время Великой Отечественной войны, В. А. Котельникове, Марфинской лаборатории можно прочитать в статье Д. А. Ларина [32], сборнике «В. А. Котельников. Судьба, охватившая век» [30], книге К. Ф. Калачёва [28]. О криптографии в XX веке — в сборнике об истории ИКСИ [38], статьях и интервью Н. Н. Андреева [4, 27], В. А. Котельникова [26], В. Н. Сачкова [41], А. Д. Закревского [25], Г. П. Агибалова [2], сайте фонда им. И. Я. Верченко [40], публикациях сайта [1], отчёте лаборатории МГУ [31], книге [34] и других. На английском языке истории российской криптографии посвящены некоторые публикации журнала «Cryptologia», среди них — статьи Т. R. Hamant [49–51], D. Kahn [52], D. Schimmelpenninck [54], J. Bury [48], Z. J. Carera [53] и другие.

Автор выражает глубокую благодарность В. М. Фомичёву за ценные замечания и обсуждения.

ЛИТЕРАТУРА

1. Агентура.ру. Российский интернет-ресурс, посвященный проблемам спецслужб, разведки и борьбы с терроризмом // www.agentura.ru.
2. Агибалов Г. П. 50 лет криптографии в Томском государственном университете // Прикладная дискретная математика. 2009. № 2. С. 104–126.
3. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черёмушкин А. В. Основы криптографии. М.: Гелиос АРВ, 2005. 480 с.
4. Андреев Н. Н., Зубков А. М., Ивченко Г. И. и др. Владимир Яковлевич Козлов (к девяностолетию со дня рождения) // Дискретная математика. 2004. Т. 16. № 2. С. 3–6.
5. Бабаш А. В., Шанкин Г. П. История криптографии. Ч. 1. М.: Гелиос АРВ, 2002. 240 с.

6. *Бабаш А. В., Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* О развитии криптографии в XIX веке // Защита информации. Конфидент. 2003. № 5. С. 90–96.
7. *Бабаш А. В., Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптографические идеи XIX века // Защита информации. Конфидент. 2004. № 1. С. 88–95; 2004. № 2. С. 92–96.
8. *Бабаш А. В., Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптографические идеи XIX века. Русская Криптография // Защита информации. Конфидент. 2004. № 3. С. 90–96.
9. *Бабаш А. В., Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Шифры революционного подполья России XIX века // Защита информации. Конфидент. 2004. № 4. С. 82–87.
10. *Бабаш А. В., Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптография в XIX веке // Информатика. 2004. Т. 466. № 33. С. 17–23.
11. *Бабиевский В. В., Бутырский Л. С., Ларин Д. А., Шанкин Г. П.* Советская шифровальная служба: 1920–40-е // <http://www.agentura.ru>
12. *Букашкин С. А.* В. А. Котельников — основоположник секретной телефонии // Сб. «В. А. Котельников. Судьба, охватившая век». Т. 1. Воспоминания коллег. М.: Физматлит, 2011. С. 21–24.
13. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Криптография: страницы истории тайных операций. М.: Гелиос АРВ, 2008. 288 с.
14. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Криптографическая деятельность в период наполеоновских войн // Защита информации. Конфидент. 2004. № 5. С. 90–95.
15. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Научно-технический прогресс и криптографическая деятельность в России XIX века // Защита информации. INSIDE. 2005. № 2. С. 67–75.
16. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Начало войны в эфире // Защита информации. INSIDE. 2005. № 3. С. 89–96.
17. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Криптографическая деятельность во время Гражданской войны в России // Защита информации. INSIDE. 2005. № 4. С. 89–96.
18. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Криптографическая деятельность революционеров в 20–70-х годах XIX века в России: успехи и неудачи // Защита информации. INSIDE. 2005. № 5. С. 90–96.
19. *Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптографическая деятельность организаций «Земля и воля» и «Народная воля» в России в 1876–1881 годах // Защита информации. INSIDE. 2005. № 6. С. 80–87.
20. *Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптографическая деятельность революционеров в России. 1881–1887 годы: агония «Народной воли» // Защита информации. INSIDE. 2006. № 2. С. 88–96.
21. *Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптографическая деятельность революционеров в России в 90-е годы XIX века // Защита информации. INSIDE. 2006. № 4. С. 84–91.
22. *Горький М.* По союзу советов. Очерк V. Соловки // Собрание сочинений в тридцати томах. Т. 17. М.: ГИХЛ, 1952. С. 201–220.
23. *Гузи Л.* Узник Соловецких островов Владимир Кривош-Неманич // Кафедра русистики, ФФ ПУ Прешов. Словакия. Специально для «Соловки Энциклопедия». 15.11.2005. Доступно по адресу http://www.solovki.ca/camp/_20/scientists.php.
24. *Гуляев Ю. В.* Краткая научная биография академика В. А. Котельникова. www.cplire.ru/alt/Kotelnikov/index.html.
25. *Закревский А. Д.* Метод автоматической шифрации сообщений // Прикладная дискретная математика. 2009. № 2. С. 127–137.

26. Интервью: «Владимир Котельников: „Радио — главное открытие XX века“» // С. Лесков. <http://fbm2000.ru/tp/in/rd.htm>.
27. Интервью: «Н. Н. Андреев: Россия остаётся в числе лидеров мировой криптографии» // <http://www.ssl.stu.neva.ru/psw/crypto/Andreev23.html>.
28. *Калачев К. Ф.* В кругу третьем: Воспоминания и размышления о работе Марфинской лаборатории в 1948–1951 годах. М.: Машмир, 2001. 129 с.
29. *Кан Д.* Взломщики кодов. М.: Центрполиграф, 2000. Перевод книги *Kahn D.* The codebreakers. 1967.
30. В. А. Котельников. Судьба, охватившая век. В 2 т. / сост. Н. В. Котельникова. М.: Физматлит, 2011. 312 с.
31. Лаборатория МГУ по математическим проблемам криптографии 1990–2000. Материалы к заседанию межведомственного междисциплинарного семинара по научным проблемам информационной безопасности 30 ноября 2000 г. М.: МГУ, 2000. 48 с.
32. *Ларин Д. А.* Советская шифровальная служба в годы Великой Отечественной войны // Изв. УрФУ. Сер. 1: Проблемы образования, науки и культуры. 2011. Т. 86. № 1. С. 69–80. <http://proceedings.usu.ru/>
33. *Лихачёв Д. С.* Избранное: Великое наследие. Заметки о русском. СПб.: Logos, 1998. 560 с.
34. *Масленников М. Е.* Криптография и свобода. <http://lib.rus.ec/b/145611>
35. *Нечаев В. И.* Элементы криптографии (Основы теории защиты информации). М.: Высшая школа, 1999. 109 с.
36. *Новик В. К.* Христиан Гольдбах и Франц Эпинус (из истории шифровальных служб России XVIII века) // Математика и безопасность информационных технологий. Материалы конф. в МГУ 23–24 октября 2003 г. М.: МЦНМО, 2004. С. 87–110.
37. *Первушин А. И.* Оккультный Сталин. М.: Яуза, 2006.
38. Пятьдесят лет Институту криптографии, связи и информатики. Исторический очерк / под ред. Б. А. Погорелова. М., 1999. 272 с.
39. *Руднев Е. В.* О нашей юности и сверстнике моём // Сб. В. А. Котельников. Судьба, охватившая век: в 2 т. М.: Физматлит, 2011. Т. 1. Воспоминания коллег. С. 19–20.
40. Сайт благотворительного фонда им. И. Я. Верченко. www.verchenko.ru
41. *Сачков В. Н.* Вклад выпускников МГУ в развитие теоретической криптографии в России во второй половине XX века // Московский университет и развитие криптографии в России. Материалы конф. в МГУ 17–18 октября 2002 г. М.: МЦНМО, 2003. С. 250–257.
42. *Сингх С.* Книга шифров. Тайная история шифров и их расшифровки. М.: АСТ Астрель, 2006. 447 с.
43. *Соболева Т. А.* История шифровального дела в России. М.: ОЛМА-ПРЕСС, 2002. 512 с.
44. *Солдатов А., Бороган И.* Новое дворянство: Очерки истории ФСБ. М.: ООО «Юнайтед Пресс», 2011. 298 с.
45. Соловки-энциклопедия. Digest project. www.solovki.ca.
46. ENIGMA. Poznan mathematicians success. Познаньский университет, Польша. Фильм, 2008. Реж. J. Malinowska.
47. *Фомичёв В. М.* Из истории развития шифров. Раздел в учеб. пособии «Математические основы современной криптологии». М.: Финансовый университет при Правительстве РФ, 2013 (в печати).
48. *Bury J.* Operation Stonka. An Ultimate Deception Spy Game // Cryptologia. 2011. V. 35. No. 4. P. 297–327.
49. *Hammant T. R.* Russian and Soviet cryptology I — Some communications intelligence in tsarist Russia // Cryptologia. 2000. V. 24. No. 3. P. 235–249.

-
50. *Hammant T. R.* Russian and Soviet cryptology II — The Magdeburg incident: the Russian view // *Cryptologia*. 2000. V. 24. No. 4. P. 333–338.
 51. *Hammant T. R.* Russian and Soviet cryptology III — Soviet Comint and the Civil War, 1918–1921 // *Cryptologia*. 2001. V. 25. No. 1. P. 50–60.
 52. *Kahn D.* Soviet Comint in the Cold War // *Cryptologia*. 1998. V. 22. No. 1. P. 1–24.
 53. *Kapera Z. J.* Summary Report of the State of the Soviet Military Sigint in November 1942 Noticing “ENIGMA” // *Cryptologia*. 2011. V. 35. No. 3. P. 247–256.
 54. *Schimmelpenninck van der Oye D.* Tsarist Codebreaking some Background and some examples // *Cryptologia*. 1998. V. 22. No. 4. P. 342–353.