А.В. Бабаш, Е.К. Баранова
(Российский государственный социальный университет;
e-mail: babash@yandex.ru)

СПЕЦИАЛЬНЫЕ МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В ПЕРИОД МЕЖДУ ПЕРВОЙ И ВТОРОЙ МИРОВЫМИ ВОЙНАМИ

Чтобы обеспечивать информационную безопасность, полезно знать историю противостояния криптографов и взломщиков шифров. Читателю предлагается цикл из пяти статей о специальных методах добывания информации, что во многом связано с историей криптографии. Это третья статья цикла о специальных методах криптографической деятельности. Проведён обзор специальных методов в криптографической деятельности в период между Первой и Второй мировыми войнами.

Ключевые слова: информация, криптология, тайна, шифр.

A.V. Babash, E.K. Baranova

SPECIAL METHODS TO CRYPTOGRAPHIC ACTIVITY AT PERIOD OF BETWEEN FIRST AND SECOND WORLD WAR

To ensure information security, it is useful to know the history of confrontation and crackers cryptography ciphers. The reader is invited to a series of five articles on special methods of collecting information, which is largely associated with the history of cryptography. This is a third article of the cycle about special method of cryptographic activity. A review of special techniques in cryptographic activity in the period between the First and Second World Wars.

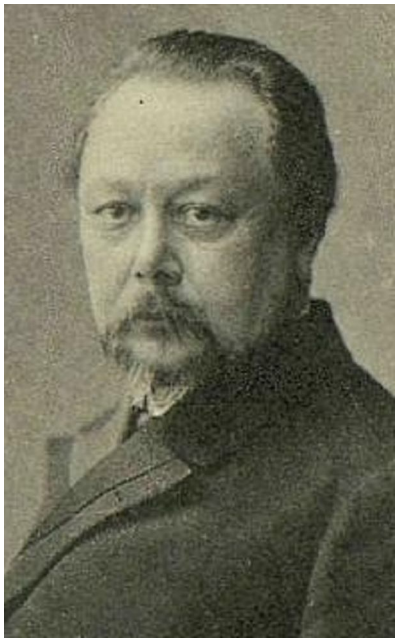
Key words: information, cryptology, secret, cipher.

Статья поступила в редакцию Интернет-журнала 12 января 2011 г.

Если периоды мировых конфликтов – это время активного использования специальных методов в криптографической деятельности и накопления оперативного материала, то периоды между мировыми войнами – это периоды обработки накопленных материалов, их анализа и активной разработки новых методов и средств в криптологии.

Летом 1919 года ВЧК РСФСР раскрыла подпольную контрреволюционную организацию **"Национальный центр"**. Эта организация была создана в мае – июне 1918 в Москве с целью координации действий антибольшевистских сил в стране. Организация объединяла бывших членов "Правого центра", представителей запрещённых партий кадетов, октябристов и других.

Руководителями "Национального центра" были Д.Н. Шипов, М.М. Фёдоров, Н.Н. Щепкин, среди активных деятелей – П.П. Рябушинский, Д.В. Сироткин и ряд других крупных политических фигур. В мае 1919 г. **Николай Николаевич Щепкин** возглавлял деятельность организации в Москве. Также он входил в состав группы из шести человек, которая координировала деятельность всех московских антисоветских организаций, так называемый "Тактический центр", был членом военной комиссии "Тактического центра" [1]. При обыске у Н.Н. Щепкина была обнаружена "жестяная коробка, содержащая шифрованные и нешифрованные записки, шифр, рецепты проявления химических чернил …". Эти материалы оказали существенную помощь в расследовании деятельности организации.



Н.Н. Щепкин

Арестованный по этому делу П.М. Мартынов рассказал об используемом шифре следующее: "Возьмите русское евангелие от Луки, главу 11 (где "Отче наш") – текст пишется цифрами в два и три цифровых знака; цифра справа всегда означает порядок буквы в стихе, а остальные цифры означают номер стиха. Так, например: 311, 26, 46, 41, 311, 54 означает, первая буква в 31-м стихе – Ц, шестая буква во 2-м стихе – А (пробелы между словами учитываются – авт.) и т.д. Все слово означает "царица"…".

31 Царица южная восстанет на суд с людьми рода сего и осудит их, ибо она приходила от пределов земли послушать мудрости Соломоновой; и вот, здесь больше Соломона. 3Цар 10:1, 4; 2Пар 9:1; Мф 12:42

2 Он сказал им: когда молитесь, говорите: Отче наш, сущий на небесах! да святится имя Твое; да приидет Царствие Твое; да будет воля Твоя и на земле, как на небе; Мф 6:9

Евангелие от Луки
стих 31 и 2

Таким образом, подпольщиками использовалась одна из разновидностей книжного шифра.

В 20-х годах **англичане** предприняли силовую акцию по захвату документов торгового общества **"Аркос"**. 12 мая 1927 г. полиция произвела обыск в помещении советского торгового представительства в Лондоне и англо-советского акционерного общества "Аркос", заподозренного в шпионаже в пользу СССР. Все служащие "Аркоса" и торговой делегации были задержаны и подвергнуты личному обыску. В тот же день поверенный в делах СССР в Лондоне обратился к Министру иностранных дел Великобритании сэру Остину Чемберлену с нотой протеста.

Сэр Остин Чемберлен

Изъятые при обыске документы не содержали никаких компрометирующих сведений, но, несмотря на это, были использованы британским правительством в качестве основания для обвинения Советского Союза в "подрывной" деятельности в Великобритании, разрыва дипломатических отношений и расторжения всех торговых соглашений. Среди захваченных секретных документов оказались и советские шифры. Эта находка дала англичанам возможность читать шифрпереписку советских дипломатов в Англии. Опубликованные дешифрованные сообщения возбудили общественное мнение и позволили оправдать разрыв дипломатических отношений Великобритании с Россией, которые были восстановлены только в октябре 1929 г.

В начале 20-х годов **российской контрразведке** (КРО ОГПУ СССР) удалось добыть ключевую документацию к ряду шифров и кодов иностранных государств, что позволило ОГПУ контролировать телеграфные сообщения ряда иностранных посольств в Москве.

В августе 1921 г. **Спецотдел ВЧК** (государственный криптографический орган России – авт.) издал приказ, в соответствии с которым все подразделения в центре и на местах должны были направлять в отдел обнаруженные при обысках и арестах шифры, ключи к ним и шифрованные сообщения.

Работа Спецотдела началась с детального изучения архивов дешифровальных служб дореволюционной России. Среди архивных документов были обнаружены подлинники и копии шифров Болгарии, Германии, Китая, США и Японии, а также отчеты о работе по их вскрытию и учебные пособия. Этот факт сыграл важную роль в подготовке специалистов – криптографов в послереволюционной России.

Одной из операций **русской разведки** с целью добычи шифра была операция по изъятию шифра из китайского посольства в 20-х годах, проведенная **Петром Леонидовичем Поповым**, талантливым разведчиком-самоучкой, по профессии судовым механиком с канонерской лодки "Манджур", охранявшей в царское время рыбные промыслы в районе Камчатки. Об этом оставшимся малоизвестным российском разведчике, обладавшим аналитическим складом ума и необыкновенной смелостью, поднявшимся до уровня высококвалифицированного профессионала, подробно рассказал в своей книге В. Гоголь [3].

Пользуясь завоеванным авторитетом у китайских властей и посла Китая в СССР Ли Тьяо, Попов получил свободный доступ в китайское посольство в Москве. Изучив обстановку, он составил план получения слепков с ключей от сейфа, в котором находились шифрдокументы. Отключив отопление в здании посольства перед очередным визитом туда, Попов, по просьбе хозяев, занялся проверкой всей отопительной системы и получил доступ в зону безопасности. Проверяя там отопительные батареи, он улучил момент и снял нужные слепки с ключей, лежавших на столе шифровальщика. Имея ключи от сейфа, изъятие шифра было осуществлено без затруднений.

В начале 1924 г. резидентом **советской разведки** в Ковно (в то время столица Литвы – авт.) стал **Игорь Константинович Лебединский**. Находясь там в течение двух лет, он проявил себя умелым организатором разведывательной работы, располагал связями с французской, эстонской и латвийской мис-

сиями. Один из информаторов Лебединского, получивший псевдоним **"Василий"**, работал курьером в аппарате военного атташе Франции, через этого курьера советская разведка получала черновики секретной переписки атташе с Парижем, что помогло в раскрытии французских шифров.

Работа курьера, под псевдонимом "Василий", продолжалась до конца 30-х годов. Сам И.К. Лебединский в дальнейшем работал в Австрии и Германии.

С мая 1924 г. по ноябрь 1927 г. военным атташе при полпредстве СССР в Персии (Иране) был **Ардальон Александрович Бобрищев** – бывший офицер царской армии в 1918 г. добровольно вступивший в Красную Армию и состоявший на дипломатической службе. Во время работы в Персии Бобрищев завербовал себе на службу практически всех шифровальщиков Главного штаба Персии. В результате был получен богатый материал, проливавший свет на внутреннюю и внешнюю политику этой страны.

В 1930 г. по идеологическим соображениям перешел на сторону противника начальник контрразведывательного отдела российской спецслужбы ГПУ (Главное политическое управление – авт.) **Георгий Сергеевич Агабеков**. Он рассказал о некоторых методах работы ГПУ, связанных с дешифрованием дипломатической переписки. В частности, он раскрыл детали проникновения ГПУ к афганским дипломатическим шифрам (через переводчика афганского консульства в Ташкенте), а также к правительственным шифрам Персии, путем вербовки шифровальщика при Совете Министров Персии [4].

Георгий Агабеков – уникальный исторический персонаж, чья жизнь напоминает авантюрный роман, был первым крупным разведчиком-чекистом, который, выступил на Западе с разоблачением деятельности ОГПУ. Агабеков сотрудничал со спецслужбами Бельгии, Англии, Франции, Голландии, Германии, Румынии, Болгарии. В эмиграции Агабеков опубликовал книги "ГПУ. Записки чекиста" (Берлин, 1930) и "ЧК за работой" (Берлин, 1931). По приговору советского суда в 1937 г. был ликвидирован агентами НКВД.

Обложка книги Георгия Агабекова, букинистическое издание (1996 г.)

Мемуары Г. Агабекова – это уникальное свидетельство непосредственного участника многих событий, происходивших в 20-е годы. В предисловии А.В. Шаврова к книге "ЧК за работой", например, приводятся следующие факты.

"Основным методом работы секретных резидентов была вербовка людей, имевших доступ к секретной информации. Особое внимание чекистов при этом привлекали западные дипломатические миссии, и наибольших успехов ОГПУ достигло именно в перлюстрации дипломатической почты.

Агабеков подробно описал технику такой работы, практиковавшуюся в Иране, когда давал показания представителям западных спецслужб. Глава бельгийской разведки барон Ферхюльст сначала не поверил, что вся бельгийская

дипломатическая почта в Персии перлюстрировалась ГПУ. По свидетельству барона, Агабеков в ответ на это предложил провести эксперимент. Ему был дан запечатанный и прошитый конверт, он вышел в соседнюю комнату и через полчаса вернул его в целости и сохранности, при этом сообщив точное содержание бывшего в пакете документа. Ферхюльст был буквально "покорен" высоким профессионализмом работы бывшего советского резидента. Для Интеллидженс сервис (англ. Intelligence service – собирательное наименование сети разведывательных и контрразведывательных служб Великобритании – авт.) также было полной неожиданностью, что с 1926 г. советская разведка имела в своем распоряжении копии почти всех сообщений из Англии, адресованных в Тегеран и даже в Индию. Всего люди Агабекова, работавшие в Мешхеде (город на северо-востоке Ирана – авт.), вскрывали ежемесячно свыше пятисот секретных дипломатических писем. Для англичан и бельгийцев это была весьма малоприятная новость, тем более что им было вполне ясно – аналогичные службы ОГПУ успешно действовали в большинстве советских полпредств по всему миру. Советская разведка, видимо, затрачивала на подобные операции небольшие деньги. Во всяком случае, в Мешхеде за каждое переданное ОГПУ английское или персидское письмо местные почтовые чиновники получали всего два доллара, а за любое другое – один доллар. После того, как Агабеков раскрыл эту систему, англичане и их бельгийские коллеги смогли принять меры для прекращения систематической перлюстрации дипломатической почты" [4].

В 1925 г. пришёл в советскую разведку незаконнорожденный сын графа А.Н. Толстого **Дмитрий Александрович Быстролётов**. Будучи чрезвычайно одаренным человеком. Д.А. Быстролётов имел задатки для того, чтобы стать литератором или художником. Были у него склонности и к естественным наукам.

Д.А. Быстролётов

Гимназию Д.А. Быстролётов окончил в России, в Константинополе – колледж, в Праге получил диплом доктора права, в Цюрихе стал доктором медицины. Он владел более чем двадцатью языками. В 1937 г. был принят в Союз художников. В 1938 г. – репрессирован. В 1956 г. – реабилитирован. Скончался Д.А. Быстролётов 3 мая 1975 г.

В 1930 г. Быстролётов стал агентом-нелегалом в Европе. Именно в этом году он обосновался в Германии и наладил регулярное снабжение СССР шифрами европейских стран.

Обладая незаурядной внешностью, он вовлекал в свою работу женщин, представлявших интерес для советской разведки.

Наиболее интересная операция была проведена Бысролётовым в первой половине 30-х годов. В советском посольстве в Париже работал на высокой должности поверенного в делах **Григорий Зиновьевич Беседовский**, он перешел на сторону французов, украв деньги и наиболее важные документы. Бесе-

довский выдал все секреты посольства и подпольных работников, каких только знал. Погибли люди, делу был нанесен огромный ущерб. Изменник опубликовал книгу. Так случилось, что её внимательно прочитал И.В. Сталин и написал на полях единственное слово: *"Возобновить"*. Оно появилось напротив рассказа об одной истории, разыгравшейся в парижском посольстве и разглашенной предателем.

Беседовский писал, что в 1928 г. в советское посольство в Париже явился небольшого роста человек, брюнет с красным носом. Незнакомец предложил купить у него шифры Италии за 250 тысяч французских франков, обещая в случае вступления в силу новых продавать и их, но опять за 250 тысяч. По словам "носика", главная ценность сотрудничества с ним заключалась в возможности пользоваться этим источником многие годы. Рассчитывая на долговременное сотрудничество, и уверенный в ценности своего предложения он заявил: "Вы располагаете, конечно, на парижской почте своей агентурой и собираете всякие шифрованные телеграммы, в том числе и итальянского посольства. Я вам доверяю. Возьмите книги, отправляйтесь в свой шифровальный кабинет и дешифруйте пару итальянских шифртелеграмм. Когда убедитесь в подлинности принесенных мною документов, давайте произведем расчёт".

Атташе вышел в соседнюю комнату, убедился в подлинности шифров, сфотографировал их, а потом, желая сэкономить деньги, обвинил незнакомца в мошенничестве и выгнал. В Москву фотокопии были посланы с победной реляцией об удачной операции, открывшей советской разведке тайны политики Муссолини, и о сбереженной для советского государства большой сумме денег. Атташе получил орден за хорошую работу, а итальянцы немедленно сменили шифр, поступление новых шифров из-за обмана посредника стало невозможным. Сталин приказал ОГПУ восстановить контакт с посредником, для этого из Норвегии в Москву срочно был отозван Быстролётов.

По прибытии в Москву Быстролётов получил в руки злополучную книгу Беседовского с пометкой вождя вместе с распоряжением найти человека, посетившего парижское посольство со столь необычным предложением. Ему открыли неограниченный кредит и приказали выехать из Москвы в ту же ночь. Это было чрезвычайно сложное задание – найти неизвестного человека, который один раз показался на глаза советскому военному атташе в Париже и про которого только и известно, что он маленького роста, с красным носом. Быстролётов проанализировал ситуацию и, исключая одну страну за другой, нашел отставного офицера швейцарской армии, итальянца по фамилии Росси, с большими связями в Риме. Перед Быстролётовым стояла серьезная проблема, ведь признаться "носику", что перед ним – советский разведчик, было невозможно из-за обмана, произошедшего в Париже. Быстролётов решил выдать себя за японского шпиона, что было возможно, поскольку японцы не могли сами вести разведывательную работу в Европе из-за характерной внешности и поэтому пользовались услугами европейских наемников, которым хорошо платили.

При встрече с Быстролётовым Росси рассказал, что торговлю шифрами наладил сам министр иностранных дел Италии **граф Галеаццо Чиано**, женатый на дочери итальянского диктатора Муссолини. По его поручению Росси объезжал все великие державы и, собрав пару миллионов, переходил на средние по величине государства, которым продавал те же шифры дешевле, а объехав средние, опускался до мелких и загонял им шифры за пустяки. Когда все заинтересованные державы читали итальянскую дипломатическую переписку, граф Чиано менял шифр и Росси пускался в новый обход клиентуры.

Граф Галеаццо Чиано

После опубликования книги Беседовского Чиано организовал провокацию с исчезновением шифровальных книг в одном из итальянских посольств, нагрянул туда с ревизией и обвинил в краже случайного человека. Невиновный был уничтожен, а Чиано прослыл неукротимым борцом с коррупцией и изменой. Росси стал продавать итальянские шифры Быстролётову, при этом иногда делая "представителю японской разведки" весьма оригинальные предложения. Однажды он предложил начать печатать в Японии фальшивые доллары и был согласен получать не 200 тысяч настоящих франков, а миллион фальшивых долларов.

Следует отметить, что Росси отличался хитростью, изворотливостью и сообразительностью. Пользуясь географической удаленностью Японии и обширностью своих связей, он сначала продавал итальянские шифры японцам в Токио, а затем – их "агенту" Быстролётову в Берлине. Вскоре Росси удалось вычислить, что Быстролётов – советский разведчик, и он решил расправиться с ним. Росси заманил Быстролётова к себе на виллу, жизнь советского разведчика подверглась реальной опасности, но Быстролётов проявил хладнокровие. Услышав на улице автомобильный гудок, он заявил Росси, что это условный сигнал и если через 10 минут он не выйдет, то на помощь ему придут товарищи, которые ожидают в машине около дома Росси. Не предвидя такого оборота событий, Росси пошел на попятную и согласился на дальнейшее сотрудничество с Быстролётовым, правда, запросив увеличить ему оплату, на что Быстролётов согласился. В дальнейшем, в качестве компенсации за происшествие на вилле, Росси познакомил Быстролётова с одним французским шпионом, который ради установления дружеских отношений с японской разведкой передал её "агенту" несколько шифров.

В 1930 г. Быстролётов принял участие в разработке шифровальщика британского МИДа капитана Эрнеста Олдхама (псевдоним **"Арно"**).

В 1929 г. **Эрнест Холлоуэй Олдхам** продал за две тысячи долларов советской разведке английский дипломатический шифр. Этот эпизод так описан в книге Олега Гордиевского и Кристофера Эндрю.

"Эрнест Холлоуэй Олдхам, шифровальщик Управления связи Министерства иностранных дел Великобритании, находившийся в тот момент в Париже с британской торговой делегацией, пришёл в советское посольство, представился как Скотт и попросил, чтобы его принял военный атташе.

Вместо этого он был принят офицером ОГПУ Владимиром Войновичем, представившимся как "майор Владимир". Олдхам заявил, что работает в Форин Оффисе (англ. Foreign Office – Министерство иностранных дел Великобритании – авт.) и принес с собой британский дипломатический шифр, который и предлагает купить у него за две тысячи долларов США. Войнович взял шифр и исчез с ним в соседней комнате, где шифр сфотографировали. Возможно, подозревая провокацию, Войнович вернулся к ожидавшему Олдхаму, разыграл возмущение, бросил шифр на колени Олдхаму, обвинил его в мошенничестве и выгнал из посольства. Дешифровщики объединенного подразделения по радиоперехвату ОГПУ определили достоверность шифра, принесенного Олдхамом. Центр сделал Войновичу выговор за то, что тот не заплатил "Скотту" деньги и не установил с ним связь; приказал выдать тому две тысячи долларов и настоял на повторном контакте. К стыду Войновича, офицер ОГПУ, следивший за Олдхамом, когда тот возвращался домой, записал неверный адрес и не смог найти его. Потребовались долгие усилия Ганса Галлени, нелегала ОГПУ в Голландии, известного среди своих агентов как "Ганс", прежде чем Олдхама нашли в Лондоне в 1930 г." [5].

В течение трех лет работы с Олдхамом от него были получены шифры, коды, дешифровальные таблицы, еженедельные сборники шифрованных телеграмм британского МИД и другая секретная информация. Однако в дальнейшем Олдхам не выдержал психологической нагрузки, связанной с агентурной работой, и покончил жизнь самоубийством. Используя информацию, переданную Олдхамом, советской разведке удалось завербовать еще несколько сотрудников МИД Великобритании.

Обложка книги Д.А. Быстролётова, букинистическое издание (1993 г.)

В 1930-1936 годах Быстролётов получил германские шифры и установил оперативный контакт с сотрудником военной разведки Франции. От последнего были получены австрийские, итальянские и турецкие шифрованные материалы, секретные документы нацистской Германии [6].

Эффективная работа Быстролётова по добыванию западноевропейских шифров позволила советской разведке получать чрезвычайно важную информацию о действиях и намерениях западноевропейских государств в 30-40-х годах.

Дмитрий Александрович Быстролётов оставил большое наследие – 16 книг и сценарий многосерийного фильма [7, 8].

В 1927 году произошёл крупный провал **советской разведки** в Тегеране (Иран). В результате три завербованных разведкой шифровальщика Главного штаба иранской армии были расстреляны, а один приговорён к пятнадцати годам тюрьмы.

В конце 20-х начале 30-х годов **агент советской резидентуры** в Токио (псевдонимы **"Кротов"**, **"Крот"**, **"Костя"**) регулярно добывал шифровальные таблицы и книги не только японской военной разведки, но и аналогичные материалы из США, Германии и Китая.

Такая эффективность "Кротова" объясняется тем, что он являлся сотрудником одной из спецслужб Японии. Его настоящее имя до сих пор не рассекречено.

Позднее морально-психическое состояние агента стало вызывать подозрения. В одном из донесений токийской резидентуры отмечалось, что "... К. на последние встречи приходит рассеянный, объясняя это усталостью, большой занятостью по работе. Один раз явился пьяный...". Связь с "Кротовым" было решено прервать, агента "законсервировать" на неопределенное время.

Генерал-майор
Эрнст Кёстринг

В 1935 году на должность военного атташе посольства Германии в СССР был назначен генерал-майор **Эрнст Кёстринг**. Эрнст Кёстринг родился в 1876 г. в Тульской губернии, где его отец владел имением Серебряные Пруды. Окончив в Москве гимназию, будущий генерал вермахта поступил в Михайловское артиллерийское училище, прослужил некоторое время в русской армии и перед Первой мировой войной выехал в Германию, где вскоре стал начальником разведки при Главном штабе немецкой армии.

По возвращении в СССР в качестве военного атташе посольства Германии он сразу же попал в поле зрения Главного управления государственной безопасности НКВД СССР. Контрразведчикам удалось внедрить в кабинет атташе аппаратуру слухового контроля.

Спустя много лет участник этой операции **Василий Степанович Рясной** вспоминал её детали: "В полуподвал жилого дома рядом с особняком Кёстринга пришли строители. Жильцам объяснили, что произошел разрыв труб и нужен серьёзный ремонт. На самом деле с торца дома прорыли подземный ход в подвал особняка, оттуда проникли в кабинет атташе, наставили повсюду "жучков" и успешно замели все следы своего визита" [9].

В.С. Рясной

Благодаря этой операции удалось получить важную разведывательную информацию. По своей значимости она не уступала информации, поступавшей от советских разведчиков в Германии. Помимо этого, перехваченная информация давала возможность поставлять немцам дезинформацию, что в итоге сыграло важную роль в стратегических просчётах рейха при планировании предстоящей войны против СССР.

В 1934 г. **советской** разведкой был завербован шифровальщик Управления связи британского МИД капитан **Джон Герберт Кинг** (псевдоним **"Маг"**), в результате чего советская разведка получила доступ ко всем секретам британской дипломатии. Кинг передавал не только шифры и ключи к ним, но и копии секретных государственных телеграмм. Они передавались непосредственно И.В. Сталину. Разведка англичан разоблачила Кинга с помощью перебежчика Вальтера Кривицкого (настоящее имя – Гинзберг Самуил Гершевич), ответственного сотрудника НКВД. Кинг был приговорен к десяти годам лишения свободы, но досрочно выпущен за примерное поведение.

Арнольд Дейч

Вербовкой Джона Кинга занимался **Арнольд Генрихович Дейч** (он же Стефан Григорьевич Ланг)**.** Его имя долгое время хранилось в глубокой тайне и стало известно только после развала СССР. А между тем это был выдающийся советский разведчик. Коллеги по работе звали его Стефаном Лангом. Имя "Стефан" было и оперативным псевдонимом разведчика, которым он подписывал свои сообщения в Центр. Впервые о Дейче было упомянуто лишь в 1990 г. на страницах журнала "Курьер разведки" в связи с рассказом о созданной им группе советских агентов, получившей название "Кембриджская пятерка". [13]

За период работы в Англии Дейч привлек к сотрудничеству с советской разведкой свыше двадцати человек, в том числе и членов знаменитой "Кембриджской пятерки": Ким Филби, Дональд Маклейн, Гай Берджес, Энтони Блант и Джон Кернкросс.

Все завербованные Дейчем члены "Кембриджской пятерки" успешно работали на Москву в течение длительного времени. Филби стал высокопоставленным сотрудником английской разведки. Блант в период Второй мировой войны работал в контрразведке Великобритании. Кернкросс служил в британской дешифровальной службе, затем координировал деятельность английской разведки в Югославии. Маклейн и Берджес занимали высокие посты в английском МИДе. Они снабжали Кремль ценнейшей информацией о решениях и мероприятиях правительства Великобритании, о деятельности МИД и спецслужб. Американские историки Норманн Полмар и Томас Аллен в своем капитальном труде "Энциклопедия шпионажа" так оценивают деятельность "Кембриджской пятерки":

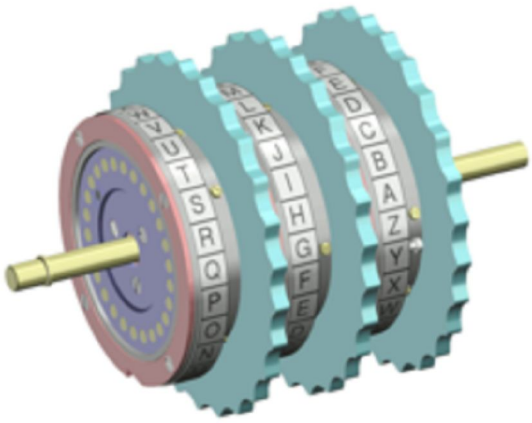
"Эти люди стали одними из самых удачливых тайных вражеских агентов за всю историю США и Великобритании. Им удалось глубоко внедриться в государственные структуры и долгое время добывать сверхсекретную информацию стратегической важности на самых высших эшелонах власти этих двух стран" [10].

Ниже речь пойдет об одном из наиболее известных, в рассматриваемый период, шифраторе **"Энигма".**

Внешний вид шифровальной машины "Энигма"

"Энигма" (Enigma – загадка, головоломка) – портативная шифровальная машина. Более точно, "Энигма" – целое семейство электромеханических роторных машин, применявшихся ещё с 20-х годов. Шифратор был изобретен в 1917 г. Эдваром Хеберном. Промышленная версия создана чуть позже берлинским инженером Артуром Кирхом (в некоторых источниках Артуром Шербиусом – авт.). Хотя шифр "Энигмы", с точки зрения криптографии, был достаточно слаб, но на практике лишь сочетание этого фактора с другими, такими, как ошибки операторов, процедурные-изъяны и захваты экземпляров "Энигмы" и шифровальных книг, позволило английским криптоаналитикам вскрывать сообщения, зашифрованные шифром "Энигмы".

На каждой стороне диска "Энигмы", представлявшего собой зубчатое колесо, по окружности располагалось 26 электрических контактов, столько же, сколько букв в латинском алфавите. Контакты с обеих сторон соединялись внутри диска случайным образом 26-ю проводами, формировавшими замену символов. Диски складывались вместе и их контакты, касаясь друг друга, обеспечивали прохождение электрических импульсов сквозь весь пакет дисков на регистрирующее устройство. На боковой поверхности дисков был нанесен алфавит. Перед началом работы диски поворачивались так, чтобы установилось кодовое слово. При нажатии клавиши и кодировании очередного символа левый барабан поворачивался на один шаг. После того, как диск делал полный оборот, на один шаг поворачивался второй барабан, после полного поворота второго – третий, как в счетчике электроэнергии.



Три последовательно соединенных ротора "Энигмы"

Пройдя через три диска, сигнал с клавиатуры поступал на так называемый рефлектор – систему проводников, соединяющую каждый контакт с другим контактом на задней стороне третьего диска. Таким образом, рефлектор посылал сигнал обратно через диски, но уже по другому пути. Когда сигнал выходил из системы дисков, он поступал на лампочку-индикатор. Как правило, с "Энигмой" работали три человека. Один зачитывал открытый текст, другой набирал его на клавиатуре, третий считывал шифртекст с ламп и записывал его.

В 1930 г. "Энигма" была модернизирована путём включения в её конструкцию штепсельной панели из 26 пар розеток и штепселей. С её помощью осуществлялась дополнительная замена перед тем, как знаки открытого текста поступали с клавиатуры на систему дисков, и после того, как они её покидали.

Ключами шифратора "Энигма" являлись:

- коммутация дисков (долговременный ключ);
- выбор дисков из комплекта и взаимное расположение их в шифраторе (всего в комплекте имелось пять дисков, в шифратор устанавливались три);
- начальное положение дисков.

До Второй мировой войны и во время нее были выпущены десятки тысяч экземпляров шифратора "Энигма", они применялись во всех видах германских вооруженных сил, а также в "Абвере" и службе безопасности.

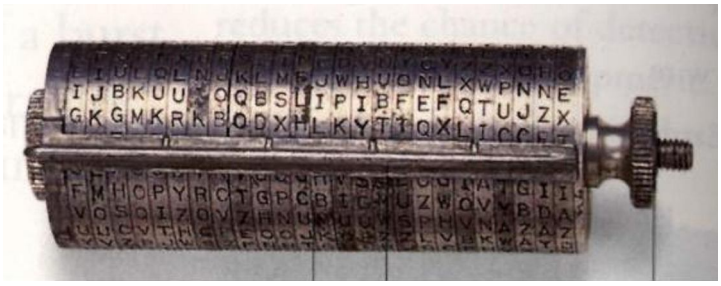
В 1931 г. сотрудник шифрбюро министерства обороны Германии **Ганс-Тило Шмидт** начал передавать французской разведке материалы по шифрам "Энигмы". Он предоставил им ключевую документацию, инструкцию по эксплуатации и ряд других ценных документов. Однако французские специалисты на основании этой информации сделали категорический вывод о невозможности вскрытия шифратора. Лишь в 1939 г., после прибытия во Францию польских криптографов, они смогли вскрыть один из ключей "Энигмы", чем доказали ошибочность представлений о невскрываемости шифра.

В середине 30-х годов польская спецслужба обнаружила завод в Юго-Восточной Германии, на границе с Польшей, где немцы производили шифрмашину "Энигма" – основной шифратор Германии во Второй мировой войне. В 1933 г. поляки-подпольщики начал изучать то, что производилось на заводе. Эта информация дала возможность польскому генштабу разобраться в устройстве шифратора. В июле 1939 г. поляки передали все материалы англо-французским союзникам вместе с двумя экземплярами аппаратуры. Полученная информация позволила англичанам провести крупнейшую дешифровальную операцию во время Второй мировой войны – операцию **"Ультра"** (дешифрование "Энигмы"). Об этой операции написаны отдельные монографии. Результаты операции "Ультра" существенно повлияли на ведение боевых действий Англии и США во время Второй мировой войны.

В конце 30-х годов важные разведывательные материалы начал передавать советской разведке сотрудник МИД Великобритании Джон Кернкросс – один из членов ранее упоминавшейся "Кембриджской пятерки". Наиболее ценная информация – это материалы, связанные с операцией "Ультра", к которым Кернкросс получил доступ. Советское руководство получило возможность изучать важные дешифрованные материалы нацистской Германии. За свою работу Джон Кернкросс был награжден орденом Красного Знамени. В 1951 г., в связи с возникшими у английской спецслужбы подозрениями, Кернкросс покинул Великобританию, в которую вернулся только в 1995 г., где вскоре умер.

В 30-е годы американским специалистам удалось получить открытые тексты телеграмм военного атташе Японии в Лиссабоне (Португалия). Они были извлечены из корзины для мусора. Имея эти тексты, американцы без особого труда раскрыли коды японского посольства.

В те же годы военно-морской флот США широко применял так называемый **"полосковый шифр"** (шифр **"полоски"**). Еще в начале XX века трудами Паркера Хитта (США) была технологически усовершенствована идея дискового шифратора Томаса Джефферсона (XIX век).



Шифратор Джефферсона

Шифратор Джефферсона представлял собой цилиндр, разрезанный на 36 дисков. Эти диски насаживались на одну общую ось таким образом, чтобы они могли независимо вращаться на ней. Исходный текст набирался вдоль линейки по одной стороне цилиндра, а шифртекст считывался вдоль такой же линейки с противоположной стороны. Для латиницы количество ключей такого шифратора (36!×26!), то есть порядка 10^{60}.

Усовершенствованный шифратор Паркера Хитта принял вид "полоскового шифра", значительно более простого в изготовлении. Полоски с удвоенным алфавитом, закрепленные в рамку, гораздо более технологичны, чем диски с алфавитом. Смысл шифрования и расшифрования остался тем же, что и в изобретении Джефферсона, однако сложные диски были заменены на легко воспроизводимые "полоски" из твердого материала, например, картона, металла или пластмассы. Такой шифратор отличался компактностью, его можно было носить в кармане пиджака. Полоски были сменными, их было до сотни, а выбор тридцати действующих полосок задавался таблицей ключей (суточный ключ).

В конце 1937 г. **японцы** осуществили секретную выемку в здании американского консульства в Кобе (Япония) и перефотографировали американский посольский полосковый шифр. Однако эффективно воспользоваться этой добычей они не смогли, поскольку стойкость шифра определялась ключевой системой, в которую, кроме "полосок", входили еще их выбор и расположение на планшете.

В конце 30-х годов **советская** разведка завербовала сотрудника МИД Германии **"Винтерфельда"**, имевшего доступ к шифрам. Были получены важные материалы, но впоследствии "Винтерфельд" стал разделять идеи нацистов и прервал связи с советской разведкой.

Рихард Зорге

В конце 30-х годов известный советский разведчик **Рихард Зорге**, работавший в Японии под видом немецкого журналиста, заведя любовную связь с секретаршей немецкого посла в Токио, получил возможность знакомиться с шифрперепиской между Берлином и немецким посольством в Японии. Это позволило Зорге постоянно получать важную разведывательную информацию, которую он сообщал в Москву.

Еще в годы Первой мировой войны Зорге служил в вооруженных силах Германии. После демобилизации поступил в Гамбургский Университет на факультет политологии, где успешно защитил докторскую диссертацию. В 1919 г. Рихард Зорге познакомился с немецкими коммунистами и в том же году вступил в Компартию Германии [12].

В первой половине 1930-х годов под псевдонимом **"Рамзай"** Зорге работал в Шанхае. За годы работы в Китае под видом немецкого журналиста и "истинного арийца", Зорге хорошо зарекомендовал себя в нацистских кругах и в 1933 г. вступил в нацистскую партию. Когда Зорге стал видным партийным функционером, Коминтерн направил его в фашистскую Японию, где он работал помощником немецкого посла генерала Югена Отто. С вторжением японских войск в 1931 г. в Манчжурию коренным образом изменилось соотношение сил на азиатском континенте. Япония сделала серьезную заявку на статус азиатской супердержавы, поэтому интересы советских разведчиков переключились на Страну Восходящего солнца.

В Японии Зорге стал ведущим немецким журналистом, часто публиковался в нацистской прессе. Накануне войны сумел занять пост пресс-атташе германского посольства в Токио. Всесторонне образованный, с прекрасными манерами и знанием многих иностранных языков Зорге завел широкие связи в немецких кругах, был вхож в высшие круги нацистского посольства. Создал в Японии разветвленную разведывательную коммунистическую организацию.

В 1935 г. Зорге по вызову начальства кружным путем через Нью-Йорк добирается до Москвы и получает от нового начальника Четвертого управления Урицкого очередное задание – выяснить, способна ли Япония по своим материальным и людским ресурсам напасть на СССР. Тогда же было решено заменить радиста Зорге, им стал Макс Клаузен, знакомый Рихарда еще по Шанхаю.

Примечательно, что шифр, используемый Клаузеном, не удалось расшифровать ни японским, ни западным дешифровщикам. В качестве ключа Зорге, со свойственным ему остроумием, применял статистические ежегодники рейха, позволяющие варьировать шифр до бесконечности. Кроме того, инфор-

мация по конспиративным каналам передавалась в Центр на микропленках. Особо важные снимки, например военных объектов или образцов вооружения, с помощью специальной аппаратуры уменьшали до размеров точки, которую специальным составом приклеивали в конце строки письма самого обычного содержания. Как мы сейчас бы определили – использовали методы стеганографии (скрытия самого факта передачи сообщения).

В октябре 1937 г. отказался вернуться в Советский Союз директор Лондонского отдела Интуриста **Арон Шейнман**, бывший нарком внешней торговли СССР. Он передал англичанам сведения об организации советской шифрсвязи.

В июне 1938 г. начальник Управления НКВД по Дальневосточному краю **Люшков Генрих Самойлович**, испугавшись сталинских репрессий, перебежал к **японцам**. Здесь он выступил с рядом статей и интервью, где подробно говорил о массовых репрессиях в СССР. Кроме того, он передал японцам сведения об организации шифрсвязи. Люшков стал гражданином Японии под именем **Ямогочи Тосикадзу**. Однако в 1945 г. при вступлении советских войск в Манчжурию его ликвидировали сами японцы как нежелательный источник информации о методах работы японской разведки.

В 1939 г. в районе Халхин-Гола японские войска вторглись на территорию Монголии, имевшей договор об оказании военной помощи с СССР.

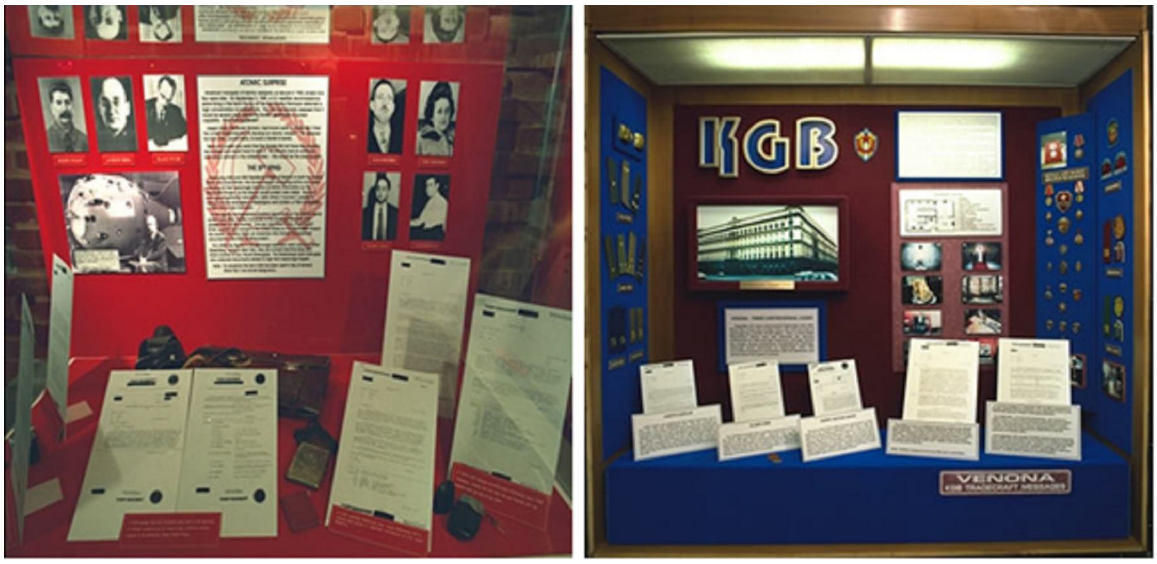
Командующий советскими войсками маршал **Георгий Константинович Жуков** разработал план оперативно-тактического обмана противника перед наступлением войск, один из пунктов которого включал вопросы дезинформации противника.

Маршал Г.К. Жуков

Он вспоминает: "Мы знали, что противник ведет радиоразведку и подслушивает телефонные разговоры, и разработали в целях дезинформации целую программу радио и телефонных сообщений. Переговоры велись только о строительстве обороны и подготовке её к осеннее-зимней кампании. Радиообман строился главным образом на коде, легко поддающемся расшифровке".

В результате японцы поверили в то, что советские войска укрепляют свою оборону и наступать не собираются. Это стало их грубым просчётом.

Одна из крупнейших операций **американских спецслужб** в области дешифрования советской переписки получила наименование **"Венона"**. Успехи этой операции во многом определялись полученными американцами оперативно-агентурными материалами. Корни этой операции уходят в конец 30-х годов.



Стенды музея АНБ США, посвященные операции "Венона"

Во время советско-финской войны 1939-1940 годов финны на поле боя захватили шифровальные блокноты НКГБ. В ноябре 1944 г. они продали их американцам. Американцы, скопировав блокноты, вернули оригиналы своему союзнику – СССР. И хотя в мае 1945 г. шифры были заменены, тем не менее, блокноты помогли американцам дешифровать перехваченные до мая 1945 г. шифрсообщения агентуры НКГБ. Это имело весьма серьёзные последствия для советских спецслужб.

Литература

1. ***Думова Н.Г.*** Кадетская контрреволюция и её разгром (октябрь 1917-1920). М., 1982.
2. ***Спиридонович А.И.*** Записки жандарма. М., 1991.
3. ***Гоголь В.*** Бомба для Сталина. М., 1996.
4. ***Агабеков Г.*** ЧК за работой. М.: Ассоциация "Книга. Просвещение. Милосердие", 1992.
5. ***Гордиевский О., Эндрю К.*** КГБ. История внешнеполитических операций от Ленина до Горбачева. М., 1992.
6. ***Шварев Н.*** Разведчики-нелегалы СССР и России. Кн. 1. М.: Родина, 2006.
7. ***Быстролётов Д.А.*** Пир бессмертных. М.: Граница, 1993.
8. ***Быстролётов Д.А.*** Путешествие на край ночи. М.: Современник, 1996.
9. ***Залесский К.А.*** Империя Сталина. Биографический энциклопедический словарь. М.: Вече, 2000.
10. ***Норманн П., Томас А.*** Энциклопедия шпионажа. М.: Крон-Пресс, 1998.
11. ***Дамаскин И.А.*** Сто великих операций спецслужб. М.: Вече, 2004.
12. ***Колесников М.С.*** Таким был Рихард Зорге. М.: Военное издательство МО СССР, 1965.
13. **http:**//www.jewish.ru/history/press/2009/03/news994272810.php.