Функционально и конструктивно SG-41 имела некоторое сходство с американской машиной M-209 и шведской BC-38, конструктором которых был знаменитый шведский криптограф Борис Хагелин[15]. Фирма Хагелина не имела патентов в Германии и поэтому его недовольство предполагаемым заимствованием осталось неудовлетворенным. И хотя отдельные удачные конструктивные решения действительно были скопированы с BC-38 в целом SG-41 была новой конструкцией с рядом преимуществ по сравнению с шифраторами Хагелина. В середине 1944 году германское Верховное командование заказало 11 000 машин SG-41 для армии и ещё 2000 машин SG-41Z для шифрования сводок метеорологической службы ВВС Германии. Но из-за нехватки цветных металлов таких, как магний и алюминий и победного шествия советских войск к границам Германии к концу войны было поставлено по разным данным от 500 до 1000 экземпляров, которые использовалась Абвером и немецкими дипломатами с 1944 года. В настоящее время криптографическое превосходство SG-41 в сравнении с машинами Хагелина не доказано, хотя сохранилось два музейных работоспособных экземпляра этого шифратора.

Первая шифрмашина из семейства SZ-40/-42/-43 была разработана в конце 1930-х годов фирмой «Standard Elektrik Lorenz», а обозначение «SZ» означало «SchlusselZusatz» (вставная шифрующая приставка), поскольку наиболее секретный механизм шифратора помещался в блоке, который мог извлекаться из машины в случае опасности. В то время как «Энигма» использовалась полевыми подразделениями на кораблях и подводных лодках, шифрмашина фирмы Lorenz предназначалась для связи высшего руководства Вермахта и Люфтваффе, которое могло использовать тяжелую машину, телетайп и обслуживаемые стационарные линии связи.

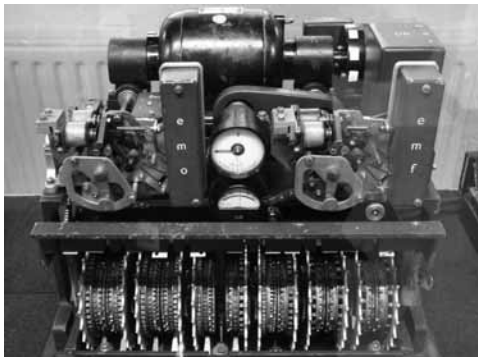


Рис. 11. Шифратор Lorenz SZ-42.

Lorenz использовался в качестве дополнения к телетайпу или коротковолновому радиопередатчику. Габариты сконструированной 12-тироторной машины составляли 51 × 46 × 46 см. Машина фирмы Lorenz вырабатывала псевдослучайный битовый поток группами по 5 битов для суммирования по модулю 2 со знаками кодов Бодо, считываемых с перфорированной ленты телетайпа. Псевдослучайная гамма генерировалась десятью роторами, пять из которых назывались «χ-роторами» и двигались регулярно, а другие пять «ψ-роторов» вращались нерегулярно. Шаговые перемещения «ψ-роторов» управлялись двумя «моторными роторами». Отдельно от перемещений пяти нерегулярных роторов (которые либо двигались вместе или стояли) по сути шифрмашина реализовала пять псевдослучайных генераторов т. о., что не существовало какой-либо связи между пятью линиями. Числа зубцов на всех роторах были взаимно простыми.

Союзники Германии

Подписанный в 1940 году пакт трех держав — Германии, Италии и Японии — гласил: Япония признает и уважает руководство Германии и Италии в деле создания нового порядка в Европе. Германия и Италия признают и уважают руководство Японии в деле создания нового порядка в великом восточно-азиатском пространстве. Помимо Италии в числе европейских государств, принявших сторону Германии, во Второй мировой войне оказались: Болгария, Венгрия, Румыния, Словакия, Финляндия и Хорватия. В боях на Восточном фронте на стороне нацистов участвовали воинские подразделения из Испании и ряда оккупированных Германии стран.

Рассмотрим криптографическую деятельность японцев. История появления японских шифрмашин весьма поучительна. После того как в конце 1920-х годах американский госсекретарь Стимсон (сказав знаменитую фразу о том, что джентельмены чужих писем не читают) ликви-

дировал дешифровальную службу в Госдепартаменте, знаменитый американский криптоаналитик Г. Ярдли остался без работы. Он обратился в японское посольство и предложил продать информацию о методах работы американской дешифровальной службы, в частности о способах дешифрования японских ручных шифров. Японцы купили эти сведения за 7000 (по другим данным 10 000) долларов. Полученная информация послужила стимулом для начала разработки в Японии электромеханических шифрмашин. Также на создание подобных машин повлияло сотрудничество с Францией. Специалист японской разведки по шифрованию секретных сообщений Шин Сакума в 1931 году сотрудничал с французским генералом Анри Картье, который был одним из лучших криптографов своего времени. Во время Первой мировой войны Картье регулярно дешифровывал телеграммы немецкого Генштаба, способствуя победе союзников. Он поделился с японцем некоторыми идеями, которые были использованы при создании первых японских шифрмашин.

Вообще японцы старались получить информацию по криптографии из всех возможных источников. В частности, читать лекции по криптографии японцы пригласили специалиста по кодам капитана польской армии Яна Ковалевского. Позже к нему в Польшу была направлена группа японских студентов, среди которых был Ризобар Ито (впоследствии крупный японский криптограф), занимавшийся разработкой шифров и шифрмашин, а также криптоанализом (в частности, он вскрыл шифрсистему типа «Playfair», которая применялась в 1930 годы на английских линиях связи). Японские шифрмашины были введены в эксплуатацию в начале 1930-х годов[16].

Японцы так же, как и другие страны приобретали коммерческие модели немецких роторных шифрмашин «Энигма», но предпочли разрабатывать свои оригинальные электромеханические модели с использованием других технологий. В частности в Японии был разработан вариант «Энигмы» с горизонтальным расположением четырех роторов (кодовое имя, присвоенное американскими криптографами — GREEN), но он по видимому не был принят на вооружение и очень мало использовался.

В 1931 году была создана экспериментальная шифрмашина «Type No. 91», но она не была принята японским флотом, который предпочитал пользоваться кодовыми книгами. Модифицированная версия «Type 91-A» (Angooki Taipu-A) была принята японским МИДом для использования послами. К концу 1930-х годов американские критпографы «взломали» шифр этой машины, кодовое название которой было «RED — красная».

Рис. 12. Первая японская роторная машина (GREEN).

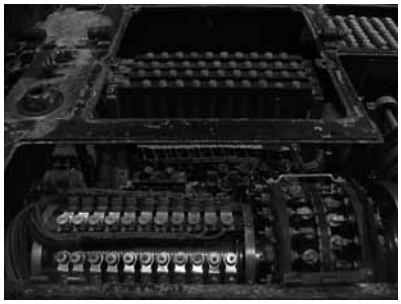


Рис. 13. Японская шифрмашина Angooki Taipu-A («RED»)

Важное место среди японских шифров принадлежит дисковой «пурпурной машине». В 1937 году был разработан новый шифратор «97-shiki O-bun Injiki» (телетайп 97 года для европейских символов; 97 год по японскому календарю соответствует 1937 году) с электрифицированной буквенной клавиатурой. Вместо роторов для шифрования совершенно секретных сообщений использовались 4 электрических шаговых искателя (широко известные шаговые роторные переключатели Strowger uniselector), применявшиеся в телефонных и телеграфных станциях. В классе шифрмашин «Type-97» капитаном ВМС Ризабаро Ито, главным проектировщиком Казуо Танаби и его инженерами Масаджи Ямамото и Эйкиши Сузуки было разработано несколько моделей, для которых американские криптоаналитики использовали кодовые имена RED, JADE, PURPLE и CORAL. Именно Эйкиши Сузуки предложил использовать шаговые переключатели вместо проблемных «классических» роторных.

Рис. 14. Сохранившийся узел японской шифрмашины «Purple» с шаговыми искателями.

Модель Angooki Taipu-B («Type B cipher machine») или PURPLE обладала большей стойкостью к дешифрованию, чем первоначальная модель «Type 97 print machine» или RED, хотя флот Японии и не знал, что сообщения, шифрованные RED читаются американскими криптографами. Машина JADE была захвачена во время операции на Сайпане в 1944 и по видимому PURPLE была во многом на неё похожа.

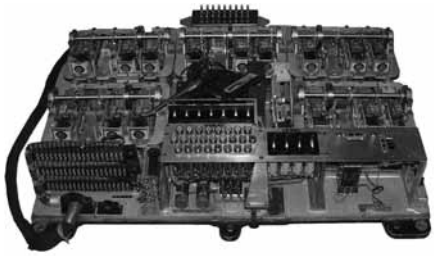


Рис. 15. Японская шифрмашина JADE.

Японцы ещё в апреле 1937 года стали испытывать «пурпурную» машину на некоторых дипломатических линиях связи. Массовое же применение машины началось с февраля 1939 года. Этим шифратором закрывалась наиболее секретная переписка японского МИДа со своими дипломатическими органами в Европе, Азии и Америке, в частности, она применялась посольствами в таких важных пунктах, как Москва, Берлин, Рим, Стокгольм, Мадрид, Берн, Виши, Анкара и др.

«Красные» шифрмашины с криптографическим механизмом «Type 97» стали использоваться японскими послами и консулами с конца 1938 года на линиях радиосвязи Токио-Берлин, а также с Вашингтоном, Лондоном, Москвой и нейтральными странами. Шифровальщик сообщений для установки суточных ключей использовал кодовую книгу «YO GO», чтобы выполнить 26 проводных соединений и поставить 4 ротора заданное начальное положение, а затем печатал текст. Клавиатура шифрмашины была латинской, а не катакана, что позволяло также успешно шифровать информацию и на английском языке. Однако для шифрования цифр и знаков пунктуации шифровальщик должен был их конвертировать в трехбуквенные кодовые слова.

Крупнейший американский криптограф Уильям Фридман после 20 месяцев упорной работы в августе 1940 добился успеха. Задача криптоаналитика состояла в реконструкции сложных внутренних проводных соединений и движений четырех переключателей, чтобы определить стартовые позиции и ежедневные установки. Фридман и его группа криптоаналитиков построили логический эквивалент японской криптомашины с использованием шаговых переключателей известной телефонной фирмы Stroudger и назвали его PURPLE (пурпурная машина). С помощью флота США для проведения дешифровальных работ было построено пять аналогов PURPLE. В конце войны после захвата японских машин 97-B выяснилось, что отличия от американского аналога заключались всего лишь в двух проводных соединениях.

После 1941 года было построено несколько других шифрмашин — CORAL, которые использовались исключительно для связи японского военно-морского атташе и в связи с незначительным объемом перехвата не поддавались дешифрованию до 1943 года. В период 1942–44 годов японский императорский флот использовал другую шифрмашину JADE (кодовое имя криптографов США), подобную CORAL. Главное отличие от CORAL — шифрование сообщений на катакана с использованием алфавита 50 символов.

Благодаря стараниям японцев в их консульствах и посольствах в различных странах мира образцы шифрмашин были уничтожены. Американские оккупационные войска в Японии в 1942–52 годах искали любые оставшиеся от этих машин запасные части[17].

Использовали японцы ручные шифры и коды. Интересно отметить следующий факт. Назначенный в октябре 1940 года японский военный атташе в Швеции полковник Макото Онодэра (к концу войны дослужился на этом посту до звания генерала) не доверял имеющимся в распоряжении японской миссии шифрмашинам. Ещё с 1938 года, когда Онодэра

работал атташе в Риге (Латвия), шифрованием сообщений занималась его супруга Юрико. Она была квалифицированным криптографом и тщательно соблюдала правила конспирации при работе с шифрами. Вот что по этому поводу она позже писала в своих мемуарах: «… научилась аккуратно обращаться с шифрблокнотом и незаметно маскировать его в случае нахождения вне резиденции в складках кимоно»[18]. Переехав вместе с мужем в Швецию, она продолжала пользоваться «трудоемким ручным способом кодирования секретных сообщений между резидентом японской военной разведки и Генеральным штабом. То обстоятельство, что г-жа Онодэра не пользовалась имеющейся в её распоряжении шифровальной машиной… уберегло их секретную корреспонденцию от дешифровки союзническими криптоаналитиками»[19].

Удивительно, но факт: в том, что касалось безопасности связи, японцы возлагали основные надежды не на подготовку персонала или стойкость своих шифров, а больше следили, чтобы своевременно были «вознесены молитвы во имя славных успехов в выполнении священного долга в великой войне в Восточной Азии». К тому же они слишком полагались на малопонятность своего языка, придерживаясь того взгляда, что иностранец не в состоянии выучить многочисленные значения отдельных иероглифов достаточно твердо, чтобы знать японский язык хорошо.

Коммерческие варианты «Энигмы» приобретались союзниками Германии во время Второй мировой войны — Болгарией, Венгрией, Румынией, Финляндией, Италией. В небольших количествах приобретались текстовые шифрмашины фирмы Хагелина. Но эти роторные шифрмашины были по прежнему дорогими и непростыми в эксплуатации. Кроме того уровень криптографических знаний и технологий в этих странах за исключением Италии был недостаточным, чтобы создавать собственные версии роторных шифрмашин.

Для своего флота итальянские криптографы разработали адаптированную версию Энигмы, получившую наименование Navy Cipher D. Печатающая электромеханическая 5-тироторная версия «Энигмы» с наименованием OMI Nistri выпускалась в Риме в 1939–1940 годов итальянской фирмой Ottico Meccanica Italiana S. A. и во время Второй мировой войны применялась в армии, ВВС и ВМФ Италии.

Рис. 16. Итальянский пятироторный клон «Энигмы».

Для шифрования сообщений с временной стойкостью вместо сложных электромеханических систем союзники Германии так же, как, например в США, которые обладали исключительными криптографическими знаниями, в период Второй мировой войны использовались «национальные» ручные средства шифрования. В качестве примера такого устройства на рис. 17. представлено устройство для механического ручного шифрования, созданное венгерскими криптографами, в котором использовался метод суммирования по модулю 26 со «случайной» буквенной гаммой.

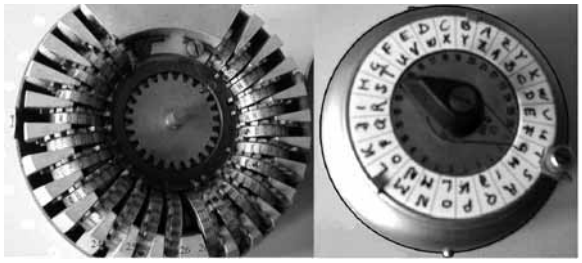


Рис. 17. Венгерская ручная шифрмашина (вид снизу и сверху).

Об успехах советских дешифровальщиков мы рассказали ранее. Здесь же кратко остановимся на успехах криптоаналитиков Великобритании и США. Большинство выше перечисленных шифрмашин Германии и её союзников читалось криптоаналитиками Антигитлеровской коалиции. Регулярное дешифрование перехватов «Энигмы» начали поляки в 1930-х годах. Позже результаты работы польских специалистов были переданы англичанам, что позволило читать «Энигму» в течении всей войны. Кстати первый в современном понимании протокомпьютер был создан во время Второй мировой войны в Англии для решения сложных криптографических задач. Использование этого устройства позволило добиться существенных успехов в дешифровании

«Энигмы». Работа по созданию ЭВМ проходила под руководством знаменитого английского математика А. Тьюринга (1912–1954). Он был членом Лондонского королевского общества. Выполнил цикл работ по математической логике и вычислительной математике. Автор фомализации понятия алгоритма в виде абстрактной вычислительной машины (машины Тьюринга). Машина получила название «Бомба», эти системы выпускались в Англии и США в течение всей войны[20].

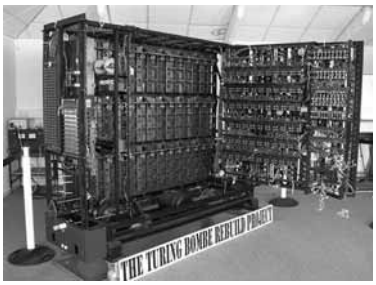


Рис. 18. Вид внутри машины Bombe (музейная реплика 2009 г.).

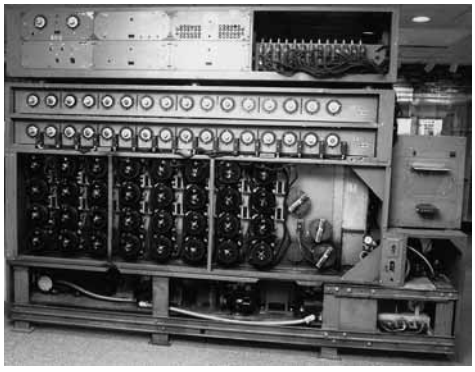


Рис. 19. Самая скоростная дешифровальная машина «US Navy Bombe».

Шифратор Lorenz SZ40/42, использовался для защиты сообщений на коммуникациях лично Гитлера и высшего командования вермахта. О существовании этой шифрмашины англичанам стало известно в первые месяцы 1940 года, когда спецгруппа английской полиции, прослушивавшая радиоэфир для поиска германских шпионов на территории острова, случайно отловила шифрованную немецкую радиопередачу необычного вида. Материал радиоперехвата был отправлен криптоаналитикам службы GC&CS (Government Code and Cypher School — «Правительственная школа кодов и шифров») в Блечли-Парк. Один из ведущих английских криптоаналитиков Джон Тильман обнаружил, что сообщение было передано не привычным в ту пору кодом Морзе, характерным и для криптограмм, зашифрованных «Энигмой», а телеграфным кодом Бодо. Тильман немедленно передал свои сведения коллегам в Блетчли Парк, где шифровальной машине было присвоено кодовое имя Fish («Рыба»), а данному типу сообщений — Tunny («Тунец»). Рыбными терминами — «лещ», «селедка» и т. п. — будут названы и перехватываемые линии связи. Тильман, предположил, что этот шифратор использует шифр гаммирования. Специально под криптосистему FISH в Блетчли Парк было создано отдельное подразделение. Первые полтора года криптоанализ продвигался чрезвычайно тяжело. Тильман разумно рассудил, что до тех пор пока не будет перехвачено два мало отличающихся сообщения с одной кодовой последовательностью, вероятность дешифрования будет нулевой. Оставалось ждать удачного случая.

Это случилось 30 августа 1941 года при передаче сообщения длиной около 4 тыс. символов из Вены в Афины. Получив в ответ из Афин «Не понял, повторите», венский оператор нарушил все возможные инструкции: он еще раз передал длинную шифртелеграмму на том же ключе, да еще по лени слегка сократил исходный текст. В руках англичан оказались обе радиопередачи, что позволило им не только полностью дешифровать этот комплект и прочесть текст телеграммы, но и получить очень важную информацию — длинную шифрующую последовательность, генерируемую шифратором. Этого было достаточно для того, чтобы начать дешифрование — «коготок увяз, всей птичке пропасть». В итоге появилась возможность узнать, как формируется псевдослучайная последовательность ключа. К Тильману подключился выпускник Кембриджа, молодой математик Билл Тьюти, вместе им удалось за четыре месяца восстановить логическую схему Lorenz. Англичанам стало известно, что в начале каждой шифртелеграммы немцы дают специфическую последовательность из 12 знаков, поэтому предположили: криптосхема неизвестного шифратора построена на основе 12 шифрующих колес. На основе этих колес с шестернями движения разного периода были устроены практически все известные в ту пору шифраторы гаммирования, включая и немецкие. Вскрытая по комплекту шифрпоследовательность давала надежду на полное восстановление логики работы аппарата FISH. Успех сопутствовал Тьюти, аккуратно расписавшему пять дорожек вскрытой шифрпоследовательно-

сти на больших разлинованных листах бумаги — в те времена все подсчеты и поиск повторений криптоаналитикам приходилось делать исключительно вручную. В одной из дорожек, то есть в череде «точек» и «крестов» (нули и единицы тогда еще не использовали), Тут сумел выявить характерные признаки двух шифрующих колес. Развив этот успех, англичане за несколько месяцев сумели взломать шифрсистему, установить общую схему устройства шифратора и убедиться, что в принципе переписку такого типа можно вскрывать и читать. Правда, путем чрезвычайно трудоемких вычислений, требовавших до нескольких недель ручного труда на обработку одной телеграммы.

Для того чтобы дешифровать сообщение, аналитикам нужно было решить две главные задачи. Во-первых, «вскрыть колеса», то есть установить точное расположение рабочих и нерабочих штифтов на каждом из 12 шифрующих дисков. Конкретные комбинации штифтов устанавливались в FISH на определенный интервал дат, в течение которого не изменялись и использовались для шифрования всех сообщений, проходящих по данной линии связи. Вторая задача — найти начальное положение («установки») дисков, использованное для конкретной телеграммы. Каждое секретное сообщение зашифровывалось немцами при новых установках, поэтому эта задача решалась лишь после того, как были вычислены штифтовые комбинации на всех дисках.

В Блечли-Парк очень хорошо понимали, что вскрывать такой шифр вручную совершенно неэффективно, ибо за недели кропотливых вычислений утрачивается оперативная ценность столь тяжело добытой информации. Поэтому для автоматизации работ было создано специальное подразделение, получившее шутливое название «Ньюменарий» в честь возглавившего его известного английского математика Макса Ньюмена. Именно здесь чуть позже и родится новаторская идея о большом электронном компьютере, однако появится он далеко не сразу. Первым проектом по автоматизации дешифрования была оптомеханическая специализированная машина-компаратор (сравнивающее устройство) Heath Robinson. Машину назвали по имени известного художника-карикатуриста Хита Робинсона (1872–1944), рисовавшего, в том числе, и «сумасшедшие машины». Конструктором этого аппарата был инженер Чарльз Винн-Вильямс. Идея необычной машины заключалась в суммировании по модулю два содержимого перехваченного кода с подготовленной комбинацией ключей. И то, и другое набивалось на перфоленты, служившие входными данными, далее обе ленты склеивались в петлю и циклически вводились в машину. Изюминкой Heath Robinson был сложный процесс синхронизации ввода лент. Над считанными символами с обеих лент выполнялись арифметические операции. Винн-Вильямс одним из первых в мире предложил использовать для сумматоров электронные схемы на газонаполненных лампах — так называемых тиратронах

В июне 1943 года Heath Robinson был доставлен в «барак № 1» Блечли-Парка, началась практическая работа. Она показала, что избранный замысел и алгоритмические основы совершенно адекватны решаемой задаче. «Робинсон» использовали, но не слишком успешно, для решения задачи о начальных установках колес. Главная проблема была в точной синхронизации двух перфолент, одна из которых содержала германское шифрованное сообщение, а на второй были набиты циклически повторяющиеся последовательности битов, порождаемые штифтовыми комбинациями вскрытых дисков шифратора. Оптомеханический считыватель позволял обрабатывать пару перфолент с довольно высокой скоростью — свыше 1000 знаков в секунду — однако перфоленточная бумага растягивалась, приводя к сбоям синхронизации и ошибкам в вычислениях. Тем не менее, на этой машине удалось отработать процессы ввода и вывода. Однако, для обеспечения надежности нужна была другая машина с меньшим числом механических компонентов. Ею стал Colossus, разработанный совместно Максом Ньюманом и Томми Флоуерсом — эту машину смело можно назвать дедушкой современных компьютеров.

Компьютер Colossus создавался для вскрытия шифрованной иностранной переписки, и сам факт его существования более полувека оставался тайной. Эта машина была для своего времени бесспорным чудом, но долгое время о ней знали лишь по слухам и фрагментарным воспоминаниям людей, так или иначе соприкасавшихся с важной тайной Второй мировой войны. Colossus полностью решил проблему синхронизации, поскольку в нем работа дисков шифратора воспроизводилась чисто электронными методами, с помощью ламповых схем. Так что на вводе в устройство осталась лишь одна перфолента с шифртекстом телеграммы, которая теперь считывалась намного быстрее,

со скоростью 5000 знаков (или 12 метров) в секунду, а подсчеты при этом стали значительно надежнее. Полностью моделировать работу шифратора внутри компьютера, используя ламповые схемы с быстрым временем переключения, предложил инженер-электронщик Томми Флауэрс — сотрудник британского Министерства почт, которого привлекли для помощи криптоаналитикам. В те времена за механизацию всех государственных коммуникаций отвечал Исследовательский центр министерства почт Dollis Hill в Северном Лондоне, и именно там в период с февраля по декабрь 1943 года Флауэрс и его коллеги построили небывалую по масштабам машину Mark I Colossus, содержавшую в своих схемах около 1500 электронных ламп. В канун Нового года готовый компьютер разобрали и перенесли в Блечли-Парк, где с февраля 1944 года Colossus начал на постоянной основе вскрывать шифрпереписку высшего эшелона германского военного командования. Благодаря надежному и быстродействующему электронному компьютеру время вскрытия телеграмм сократилось с нескольких недель до 2–3 часов. Воодушевленные столь грандиозным успехом англичане в течение 1944 года создали еще более продвинутую версию компьютера под названием Colossus Mark II. Он был примерно в пять раз быстрее своего предшественника, содержал около 2500 электронных ламп и предоставлял возможности программирования. На этом основании Colossus II в целом ряде работ расценивается ныне как первый в мире электронный программируемый компьютер. До конца войны было построено в общей сложности 10 таких машин.

В общей сложности с помощью «Колоссов» было дешифровано свыше 63 миллионов знаков телеграмм немецкого верховного командования, которые «поставляли» примерно 550 сотрудников (точнее, в большинстве своем сотрудниц) Блечли-Парк плюс, конечно же, службы радиоперехвата. С приходом мая 1945 года звезда компьютеров Colossus, увы, стремительно закатилась. Машины-гиганты, каждая из которых представляла собой комплекс из 8 крупных двухсторонних монтажных стоек разной ширины, высотой по 2,3 метра и суммарной длиной около 5,5 метра, были слишком специализированы под конкретную задачу. А высшее политическое руководство Великобритании слишком озабочено, чтобы руководство СССР ничего не узнало о мощных дешифровальных возможностях недавнего союзника. Уинстон Черчилль лично дал указание, чтобы «Колоссов» разобрали на части размерами «не больше руки человека». Восемь из десяти машин были полностью демонтированы уже в том же 1945 году.

Два последних компьютера сначала перевезли в Лондон, а затем в город Челтнем, где разместилась (и базируется по сию пору) преемница GC&CS, криптографическая спецслужба Великобритании GCHQ, или Штаб-квартира правительственной связи (Government Communications Head-quarters, в русской транскрипции ШКПС). Здесь, за плотной завесой секретности, эти компьютеры использовались еще полтора десятка лет для тренировочных и вспомогательных криптографических задач. В 1959–1960 годах демонтировали и две последние машины, тогда же были сожжены и все рабочие схемы-чертежи компьютеров Colossus. При этом сам факт существования столь выдающихся для своего времени вычислительных устройств продолжали держать в строжайшей тайне еще многие годы. Хотя официальной информации о Colossus не публиковалось вплоть до конца XXвека, обрывочные сведения об этом компьютере стали появляться с середины 1970-х годов, когда истек стандартный для Британии 30-летний срок хранения государственных секретов. К 1996 году группе энтузиастов при национальном криптомузее Блечли-Парк даже удалось воссоздать работоспособную копию этой машины, правдами и неправдами накопив достаточное количество подробностей, приватных воспоминаний и эскизов от оставшихся в живых участников проекта. В таких условиях продолжать делать тайну из того, что так или иначе уже известно всем, стало бессмысленно. В октябре 2000 года власти Великобритании решились наконец рассекретить технический отчет о вскрытии FISH и машинах Colossus, подготовленный в 1945 году сразу по окончании войны. Объемный 500-страничный документ ШКПС передала в общедоступный Государственный архив (Public Record Office) в городе Кью.

У немцев не было единой национальной дешифровальной службы, каждое ведомство, заинтересованное в получении информации при помощи криптоанализа, создавало свою. При этом некоторое сотрудничество между этими службами было, но в основном они работали самостоятельно и независимо друг от друга.

В начале 1919 года в Министерстве иностранных дел Германии было создано отде-

ление «Z». Его сотрудники стали заниматься криптоанализом дипломатической переписки зарубежных стран. Криптоаналитикам из отделения «Z» накануне и во время Второй мировой войны удалось вскрыть коды и шифры более 30 государств, среди которых были как противники (США, Англия, Франция) так и союзники (Япония, Италия) Германии. Информация, полученная путем дешифрования дипломатической переписки, докладывалась министру иностранных дел Германии Рибентропу и лично Гитлеру.

В вооруженных силах Германии отдельные дешифровальные службы имелись в каждом виде вооруженных сил: вермахте (сухопутные войска), люфтваффе (ВВС) и кригсмарине (ВМС).

В немецкой армии имелись центральный дешифровальный орган, обеспечивающий информацией главное командование, и полевые, работающие непосредственно на передовой в интересах командиров на местах. Например, в знаменитом Африканском корпусе генерала Роммеля имелась специальная рота радиоразведки, которая занималась перехватом и дешифрованием сообщений тактического звена англичан. Специалисты роты снабжали Роммеля ценной информацией с переднего края противника.

Успехи криптоаналитиков вермахта в работе против западных союзников были существенными. Например, доктор Отто Лейберих, бывший глава германской спецслужбы BSI (Bundesamts fur Sicherheit in der Informationstechnik — Федеральная служба безопасности в области информационных технологий), в одном из выступлений отметил, что немецкими криптоаналитиками был вскрыт один из самых массовых американских шифраторов М-209. Американские вооруженные силы закупили и использовали в годы Второй мировой войны около 140 тысяч таких шифраторов. Недавно немецким журналистам удалось разыскать ветерана дешифровальной службы вермахта Райнольда Вебера, в годы войны работавшего в дешифровальном подразделении FNAST-5 в Париже. Из его воспоминаний стало известно, что немцы не только вскрывали шифратор М-209 вручную, но и сконструировали машину-прототип для автоматизации наиболее трудоемких этапов дешифрования. Причем происходило это в 1943–1944 годах — тогда же, когда англичане создавали свой Colossus. Однако компания Dehomag, которой в 1944 году пытались сделать заказ на массовое изготовление аппаратов-дешифраторов для М-209, оценила срок создания серийного образца в два года. Это было слишком долго, время отпущенное Третьему рейху подходило к концу. Поэтому дальше работоспособного прототипа дело так и не пошло. Следует отметить, что шифратор был хорошо знаком немцам, так как некоторое количество С-36 было закуплено в Швейцарии и эксплуатировалось на немецких дипломатических линиях связи.

В интересах люфтваффе дешифрованием занимались в Исследовательском отделе министерства авиации Германии. Эта организация имела неофициальное название «Большое ухо». Она была создана в апреле 1933 года и занималась прослушиванием телефонных переговоров, перлюстрацией и криптоанализом. Интересно отметить, что криптоаналитики Исследовательского отдела работали не только с военной информацией, но и дешифровывали дипломатические сообщения, вели наблюдение за гражданами Германии, оказывая помощь РСХА (Главное управление имперской безопасности — одна из главных спецслужб фашистской Германии). Кстати, и в этой службе имелось небольшое дешифровальное подразделение, однако его возможностей не хватало и приходилось обращаться за помощью в другие ведомства. Отдельное дешифровальное подразделение имелось и у немецкой военной разведки (Абвер). Криптоаналитическая служба также имелась в Министерстве почты[21]. В Кригсмарине дешифровальная служба получила название «служба наблюдения», она была создана в начале 1920-х годов[22].

Теперь рассмотрим работу немецких криптоаналитиков на Восточном фронте. Когда Гитлер принял решение напасть на Советский Союз в 1940 году, у немцев на Востоке не было никаких технических средств для ведения радиоразведки. Перед нападением на СССР главное командование вермахта, планировавшее блицкриг, явно недооценивало советский оборонительный потенциал и довольно легкомысленно отнеслось к организации электронной разведки будущего противника. Вплоть до исхода лета 1941 года никаких технических средств ведения радиошпионажа и соответствующих структур у немцев на Восточном фронте вообще не было. Отрезвление наступило в ходе Смоленского сражения в июле–сентябре 1941 года, когда наши дивизии надолго задержали победный марш группы армий Центр, рвавшейся к Москве. Выдвижение советских резервов из глубины обороны оказалось тогда

для немцев неожиданностью. Поэтому согласно директиве начальника верховного главнокомандования вермахта (ОКВ) генерал-фельдмаршала Вильгельма Кейтеля, в армиях Восточного фронта были созданы радиоразведывательные роты. С присущей им методичностью немцы разбивали линию фронта на отрезки протяженностью 100–150 км, каждый из которых обслуживался 1–2 такими ротами, подчиненных штабу соответствующей армии. Кроме того, в состав радиорот батальонов связи каждой пехотной дивизии были включены радиоразведывательные взводы, а на особо важных участках боевых действий дополнительно размещались стационарные радиоразведывательные пункты, оснащенные пеленгационной аппаратурой. Все эти подразделения вели усиленное наблюдение за советскими радиопередатчиками, чтобы не раскрывая факта осуществления перехвата, выявлять дислокацию его частей, местонахождение штабов, характер действий войск. Наряду с радиоперехватом эти спецподразделения проводили операции по дезинформировании советского командования. Широкое распространение, например, получила подготовка дезориентирующих радиограмм, которые передавались советским частям от имени вышестоящих штабов и командиров. В результате советские радисты занимались приемом и расшифровкой совершенно бесполезных сообщений.

Вот что о ведении немцами войны в эфире пишет советский историк В. Анфилов: «В связи с созданием массовой армии важное значение придавалось развитию средств связи и в особенности радиосвязи. Немецкие танки оснащались надежно работающими ультракоротковолновыми приемо-передатчиками. Этим обеспечивалось гибкое управление танками на поле боя. Для пехоты и артиллерии были созданы портативные радиопередатчики и радиотелеграфные аппараты, которые имели большие преимущества по сравнению с чувствительной к обстрелу проводной связью. Кроме того, создавались средства для ведения так называемой радиовойны. Подслушивание с помощью средств связи, создание помех для радиотелефонных переговоров, а также расшифровка боевых распоряжений и донесений позволяли немецко-фашистским войскам получать важные сведения и затруднять управление войсками своего противника… Радиовойна доставила советским войскам в начале войны большие неприятности. Не говоря уже о нарушениях системы управления, противнику удавалось иногда устанавливать перегруппировки советских войск»[23].

Немецкие армейские подразделения радиоразведки занимались и криптоанализом перехваченных текстов. Однако настоящих специалистов в этой области вермахту катастрофически не хватало. Чаще всего шифротелеграммы, перехваченные радиоразведывательными взводами, пересылались в более крупные подразделения. Однако это занимало слишком много времени, и ценность дешифрованной информации часто терялась. В целом, несмотря на довольно разветвленную систему полевого радиошпионажа, немцы так и не смогли наладить эффективный криптоанализ наших важных сообщений, особенно в оперативном и стратегическом звеньях боевого управления. Тем не менее материалы радиоразведки составляли для Германии до 90% всех разведданных о ходе военных действий на Восточном фронте. Стоит заметить, что во всех предыдущих операциях германской армии, и особенно в весенне–летней кампании 1940 года против Франции и стран Бенилюкса, успехи на этой ниве были не в пример заметнее.

Сообщения советских дипломатов и высшего военного руководства, зашифрованные пятизначным кодом во время войны не читались ни противниками СССР ни союзниками ни нейтралами. С другими системами дело обстояло не так хорошо. В качестве примера рассмотрим годичную деятельность немецкого дешифровального подразделения, приданного группе армий «Север», работавшего по советским шифрам с мая 1943 года по май 1944. Сводные данные приведены в таблице 1.

Как видно из таблицы всего немцам удалось прочитать 13 312 сообщений, зашифрованных с помощью 2-х, 3-х и 4-хзначных кодов из 46 342 перехваченных. Таким образом, немецкие криптоаналитики сумели вскрыть менее трети (28,7 %) перехваченных советских сообщений. Наиболее простые двухзначные системы раскрывались чаще. Обратим внимание, что вскрытых криптограмм, зашифрованных трёхзначной системой меньше чем четырёхзначной, хотя первых перехватывалось больше. Возможно, это объясняется тем, что основные усилия немцев были сосредоточены именно на четырёхзначных криптограммах, которые потенциально содержали более ценную информацию. Кроме того имелось очень

Таблица 1. Сводная таблица дешифровальной работы немецких криптоаналитиков в 1943–44 годах[24].

Месяц	Перехват в среднем за сутки	Общее количество			4-хзначные				3-хзначные				2-хзначные			
		К-во перехваченных криптограмм	К-во дешифрованных	% дешифрованных	К-во перехваченных криптограмм	К-во дешифрованных	% дешифрованных	Вскрыто новых шифрсистем	К-во перехваченных криптограмм	К-во дешифрованных	% дешифрованных	Вскрыто новых шифрсистем	К-во перехваченных криптограмм	К-во дешифрованных	% дешифрованных	Вскрыто новых шифрсистем
1943 г.																
Май	153	4732	1629	34	1813	760	42		1873	201	11		1046	668	64	
Июнь	120	3603	1330	37	1530	789	52		1422	154	11		651	387	59	
Июль	102	3178	1349	42	1114	498	45	6	1396	449	32	8	668	402	60	
Август	67	2079	909	43	619	286	46	3	1163	409	35	5	297	214	72	
Сент.	60	1789	269	15	655	150	23		1009	80	7	5	125	39	31	
Окт.	78	2404	467	19	931	252	27	4	1356	162	11	8	117	53	45	
Ноябрь	78	2182	398	18	850	144	17	1	1210	196	16	15	122	58	46	2
Дек.	91	2810	482	17	1174	242	21	4	1536	194	14	8	100	46	46	6
1944 г.																
Январь	152	4724	1074	23	1593	467	30	8	3005	528	18	15	126	79	63	3
Февр.	178	5175	1217	24	Нет данных											
Март	179	5563	1833	33												
Апрель	130	3897	1000	26												
Май	136	4206	1355	32												
Всего	**117**	**46 342**	**13 312**	**28,7**	**10 279**	**3588**	**34,9**		**13 970**	**2373**	**16,9**		**3252**	**1946**	**59,8**	

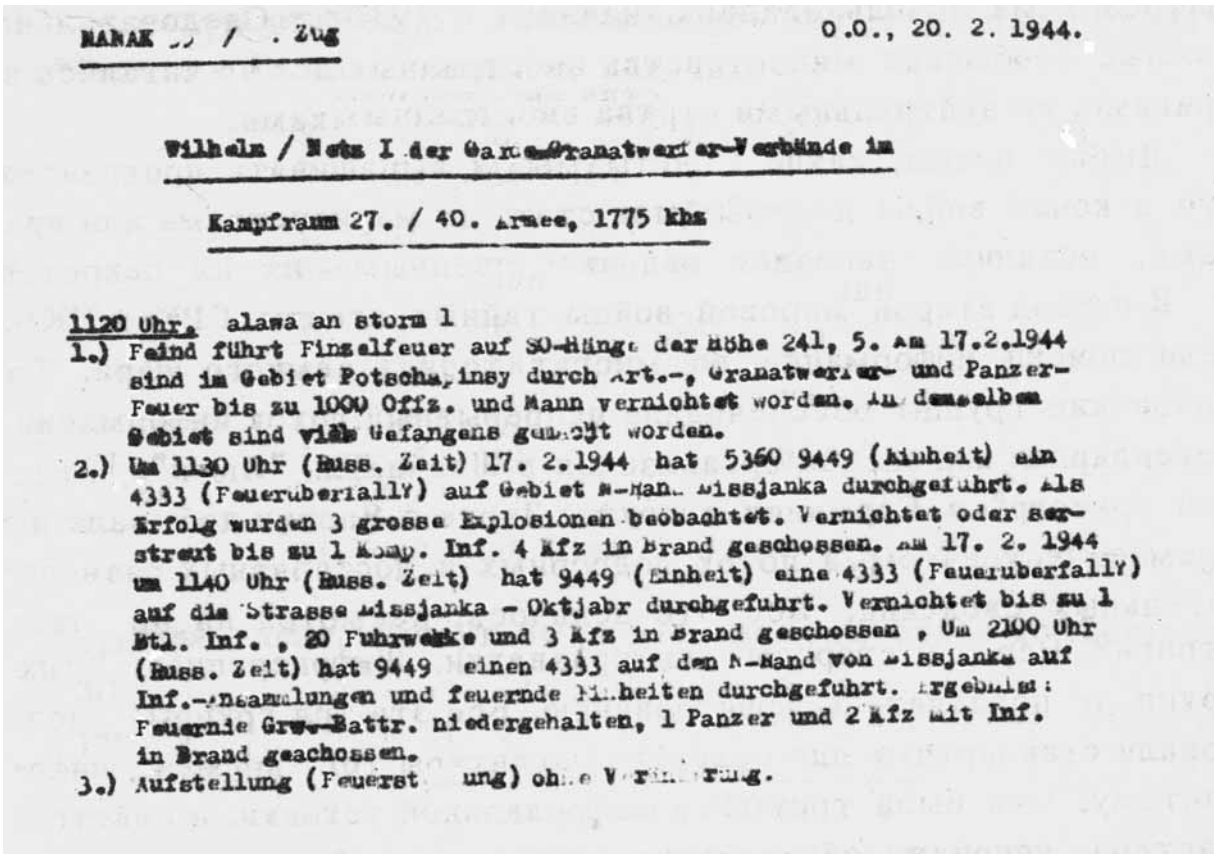
Отсутствие данных в графе «вскрыто новых шифрсистем» означает, что сведений об этом нет.

много вариантов трёхзначного кода, это можно понять анализируя цифры в графе таблицы «вскрыто новых шифрсистем». Так в ноябре 1943 года была вскрыта лишь одна четырёхзначная система, в то время как трёхзначных целых 15, в декабре пропорция изменилась — на 4 четырёхзначных системы приходится всего 8 трёхзначных. В январе 1944 года соотношение сохранилось — вскрыто 8 четырёхзначных и 15 трёхзначных. При этом немецкие дешифровальщики не уточняют количество вновь появившихся советских шифрсистем, которые не были ими вскрыты[25].

Какую же информацию удавалось добывать немцам из наших дешифрованных сообщений? Вот фрагмент из доклада немецких дешифровальщиков об их работе в феврале 1944 года. Из этого документа следует, что «Дешифрованные советские данные… позволили получить сведения об оперативной обстановке, о районах сосредоточения, командных пунктах, потерях и подкреплениях, порядке подчинения и рубежах для атаки (смотри, например, радиограммы 122-й бронетанковой бригады от 14 и 17 февраля). Кроме того, содержание этих сообщений дало возможность выявить семь танковых частей противника и их номера, а также установить наличие ещё двенадцати танковых частей. За редким исключением, весь материал обрабатывался своевременно, и полученные сведения использовались на практике»[26].

После крупнейших поражений под Сталинградом и Курском немецкая авиация утратила господство в воздухе, в связи с этим немцы стали в меньшей степени надеяться на ведение разведки с воздуха и в большей — на

действия своей радиоразведки. Одним из немногих примеров успешной работы немецких криптоаналитиков на Восточном фронте служит деятельность подразделения радиоразведки 48 танкового корпуса в 1943–1944 годах. Во время ожесточенных сражений в октябре 1943 г. начальник штаба этого корпуса полковник Меллентин отмечал: «Лучшим и наиболее надежным источником получения разведывательных данных в настоящее время является наша служба радиоперехвата»[28]. Спустя два месяца 48 танковый корпус принял участие в боях в районе города Радомышля, который находится на территории Украины, западнее Киева, в составе группы армий «Юг» — одной из трех основных военных группировок Германии на Восточном фронте. Перед этой группировкой стояла задача сорвать планировавшееся советское наступление. По планам немцев 48 корпус должен был разгромить советскую 60-ю армию. Немецкая воздушная разведка не смогла добыть какую-либо полезную информацию, а чтобы не насторожить наши войска, командование немецкого корпуса приняло решение группы войсковой разведки не высылать. Наступление, развернутое немцами в 6 часов утра 6 декабря 1943 года, оказалось для советских войск совершенно неожиданным, и они начали беспорядочный отход. Дальнейший успех немцев был напрямую связан с успехами радиоразведчиков. Вот что вспоминал об этом Меллентин: «В те дни, мы успешно осуществляли перехват радиосообщений русских. Эти сообщения немедленно дешифровывались, и их содержание своевременно докладывалось командованию корпуса. Мы всегда были в курсе действии русских, которые предпринимались в ответ на передислокацию наших сил, и в каждом конкретном случае мы вносили соответствующие изменения в наши планы. Вначале русские недооценили важность нанесенного по ним удара и подбросили на наш участок слишком малое количество противотанковых пушек. Затем постепенно русское командование начало проявлять заметное беспокойство. В эфире стали появляться встревоженные запросы: „Срочно уточните, откуда наступает противник“. Ответ: „Узнайте у чертовой бабушки. Как я могу узнать, откуда наступают немцы?“ (Всякий раз, когда в русских радиограммах упоминаются черт и его ближайшие родственники, можно предположить, что назревают серьезные события.)



0.0., 20. 2. 1944.

Wilhelm / Nest I der Gar[illegible]granatwerfer-Verbände im

Kampfraum 27. / 40. Armee, 1775 khs

1120 Uhr. alawa an storm 1

1.) Feind führt Einzelfeuer auf SO-Hänge der Höhe 241, 5. Am 17.2.1944 sind im Gebiet Potscha, insy durch Art.-, Granatwerfer- und Panzer-Feuer bis zu 1000 Offz. und Mann vernichtet worden. In demselben Gebiet sind viele Gefangene gemacht worden.

2.) Um 1130 Uhr (Russ. Zeit) 17. 2.1944 hat 5360 9449 (Einheit) ein 4333 (Feuerüberfall?) auf Gebiet N-Rand Missjanka durchgeführt. Als Erfolg wurden 3 grosse Explosionen beobachtet. Vernichtet oder zerstreut bis zu 1 Komp. Inf. 4 Kfz in Brand geschossen. Am 17. 2. 1944 um 1140 Uhr (Russ. Zeit) hat 9449 (Einheit) eine 4333 (Feuerüberfall?) auf die Strasse Missjanka - Oktjabr durchgeführt. Vernichtet bis zu 1 Btl. Inf. , 20 Fuhrwerke und 3 Kfz in Brand geschossen , Um 2100 Uhr (Russ. Zeit) hat 9449 einen 4333 auf den N-Rand von Missjanka auf Inf.-Ansammlungen und feuernde Einheiten durchgeführt. Ergebnis: Feuernie Grw-Battr. niedergehalten, 1 Panzer und 2 Kfz mit Inf. in Brand geschossen.

3.) Aufstellung (Feuerst[illegible]ung) ohne Veränderung.

Рис. 20. Переведенный на немецкий язык текст советской военной шифрограммы, дешифрованный криптоаналитиками группы армий «Север»[27].

К середине дня 60-я армия русских перестала выходить в эфир, но это уже не имело особого значения, поскольку вскоре наши танки разгромили ее штаб»[29]. Далее события развивались так: к вечеру 6 декабря немцы оттеснили советские войска на 40 километров, и в результате к ночи 9 декабря запланированное советское наступление не состоялось. В течение последующих нескольких дней по советским войскам была нанесена еще целая серия ударов. Меллентин отмечал: «Русские были определенно поражены этими ударами, наносимыми неизвестно откуда, а их радиопереписка неоспоримо свидетельствовала о царившем среди них замешательстве и беспокойстве»[30]. Победа немцев в битве под Радомышлем задержала, но не сорвала наступление советских войск. В рождественские дни группа армий «Юг» была вынуждена начать свое отступление с Украины. Несколько месяцев спустя советские войска уже отбросили немцев на расстояние более чем в тысячу километров. Воодушевлённый успехами своих радиоразведчиков и криптоаналитиков Меллентин писал: «Красная Армия периода Второй мировой войны значительно отличалась от императорской русской армии 1914–1917 гг., однако в двух отношениях русские ничуть не изменились. Они продолжают отдавать предпочтение массированным наступлениям и не перестают проявлять чрезвычайное безразличие к обеспечению безопасности своей радиосвязи»[31]. Однако последний тезис немецкого полковника явно не соответствует действительности.

В тактическом плане сведения, добываемые немцами при помощи радиоперехвата и криптоанализа, безусловно, представляли интерес, однако получить доступ к информации стратегического характера, передававшиеся по советским сетям связи немцам на протяжении всей войны так и не удалось. В связи вышеизложенным один немецкий криптограф заметил, что «Россия проиграла Первую мировую войну в эфире, во время Второй мировой войны она сумела взять реванш за свое поражение»[32]. В целом отметим, что немецкая радиоразведка против СССР во время Второй мировой войны в стратегическом отношении была малоэффективна и не имела какого-либо существенного значения[33].

Об определенных успехах немецких дешифровальщиков иногда удавалось узнать из показаний пленных.

«СООБЩЕНИЕ НАЧАЛЬНИКА 4-ГО ПОЛЕВОГО ОТДЕЛА 5-ГО УПРАВЛЕНИЯ НКГБ СССР ПОДПОЛКОВНИКА Н. К. ВЛАСОВА № 5/4П/425 НАЧАЛЬНИКУ ШТАБА ЮЖНОГО ФРОНТА ГВАРДИИ ГЕНЕРАЛ-ЛЕЙТЕНАНТУ С. С. БИРЮЗОВУ О ДЕШИФРОВАНИИ НЕМЦАМИ ПЕРЕГОВОРОВ КОМАНДОВАНИЯ ВОЙСКОВЫХ СОЕДИНЕНИЙ ФРОНТА

Не ранее 15 сентября 1943 г.

15 сентября 1943 г. пленный перебежчик немец Дюваль Фридрих, переводчик дешифровальной службы 12-й радиоразведывательной роты 549-го полка связи 6 А (6-я немецкая армия второго формирования. Её командующим являлся генерал-полковник К. Холлидт. С середины августа 1943 г. армия входила в группу армий „Юг“ и вела оборонительные бои в районе Донбасса), показал:

Немецкая радиоразведка 6 А за летний период 1943 г. дала командованию армии весьма ценный материал. В основном успешно перехватывалась двух-, трех- и четырехзначная шифрпереписка 5 УА (Ударная армия. — *Авт.*), 2 А (армии. — *Авт.*) и армии, действующей в районе Красного Луча.

В результате дешифрования материала они устанавливали нумерацию войсковых соединений и частей указанных армий, намерение нашего командования и т. п.

Весь отработанный материал помещался в разведсводку, которая выпускалась три раза в день.

Пленный показал, что особенно легко поддаются к дешифрованию наши двух-, трёх-, четырёхзначные коды, у которых ключи менялись через 5–7 дней. На дешифрование такого материала требовалось до двух часов, а после того как откроют все величины кодовой таблицы, то на дешифрование требуется 5–10 минут.

О предыдущем наступлении Южного фронта им было известно из материала дешифрования, в особенности из материалов минометных частей — „Катюш“, которые ранее получали по ½ боекомплекта, то в период наступления получали до 7 боекомплектов.

Из личного состава применяющих кодированную передачу часто встречались Пономарев, Собакин, Зайцев.

Пленный показал, что ими также легко дешифровались переговоры командования войсковых соединений по кодированным картам, которые после кодировки для уточнения координат указывали часто населенные пункты,

таким образом, карта становилась легко читаемая ими. Наш пятизначный шифр, по показанию пленного, не дешифровался.

Вывод. Все показания пленного Дюваль вполне соответствуют действительности, так как дешифровальная служба все указанные слабые стороны использует в своей основной работе.

Предложение. Все кодовые таблицы, выпускаемые войсковыми частями, необходимо утверждать специалистами шифровальной службы, а для крупных войсковых соединений для проверки устойчивости кода привлекать специалистов дешифровальной службы. Располагая некоторым количеством захваченных в прошлом у противника документов — (кодовые таблицы), можно отметить, что они настолько просты, что действительно больше двух часов не потребуется на дешифрование их.

Начальник 4-го полевого отдела
5-го Управления НКГБ СССР
подполковник Власов.
ЦА ФСБ России»[34].

Из данного документа видно, что в начальный период проведения командованием Южного фронта Донбасской наступательной операции (13 августа — 22 сентября 1943 г.) немецким дешифровальным службам удалось добыть определенные данные о дислокации соединений фронта и др. Своевременное информирование о немецких успехах органами госбезопасности командования Южного фронта позволило ему принять соответствующие меры по смене кодовых таблиц, повышению бдительности и боеготовности, что способствовало дальнейшему успешному наступлению советских войск. Войска фронта расчленили 6-ю немецкую армию на две части, нанесли ряд сокрушительных ударов и к 22 сентября 1943 г. вышли на рубеж реки Молочная. В результате Донбасской операции войска Южного и Юго-Западного фронтов продвинулись до 300 км, завершили освобождение Донбасса, разгромили 13 вражеских дивизий. Победа в Донбассе явилась важным этапом в развитии общего наступления Красной Армии[35].

В целом следует отметить, что «немецкая радиоразведка против Советского Союза была малоэффективной. В стратегическом отношении она вообще не имела ни одного сколько ни будь заметного успеха. Немцы оказались не в состоянии вскрыть шифрсистемы, применявшиеся для засекречивания переписки высшего советского военного командования… Таким образом, немецкая дешифровальная служба мало способствовала тому, чтобы в распоряжении верховного командования вермахта было как можно более полное представление о советской стратегии ведения войны против Германии»[36].

Радиоигры и пропаганда немецкой радиоразведки

В предыдущих книгах мы подробно рассказали о радиоиграх с немцами, организованных советскими спецслужбами. Следует отметить, что немцы также пытались вести радиоигры с советской разведкой. Ранее уже упоминалось об этом, в связи событиями, связанными с «Красной Капеллой». Приведём ещё ряд эпизодов. Немецкая разведка активно применяла этот новый вид деятельности своих спецслужб против союзников СССР по антигитлеровской коалиции. Так, арестованный органами ГУКР «Смерш» начальник подразделения немецкой военной контрразведки Абвер-3 Франц фон Бентивеньи на допросе подробно рассказал об исключительно удачной и результативной операции, которую Абвер-3 провел в Голландии. По его словам, в конце 1942 года в Голландии было арестовано 10 английских разведчиков, державших радиосвязь с Лондоном. Пять радистов было перевербовано, а на остальных пяти точках работали немецкие радисты, изучившие почерк англичан. Эта радиоигра продолжалась в течение всего 1943 года. В ходе нее было арестовано большое количество английских агентов и захвачено значительное количество сброшенного с самолетов вооружения, которого хватило бы для оснащения целой дивизии[37]. Данная операция получила у немцев название «Нордпол» (Северный Полюс). Она привела к полному уничтожению сил антифашистского сопротивления на территории Нидерландов[38].

О попытках ведения немцами радиоигр с советской разведкой свидетельствуют документы: