РАДИО о связи
E-mail: mail@radio.ru
ЖУРНАЛ В ЖУРНАЛЕ

История шифровальной машины "Энигма"

Георгий ЧЛИЯНЦ (UY5XE), г. Львов, Украина

Шифровальная машина "Энигма" вошла в анналы истории всемирной разведки. Ей посвящено множество книг и статей-воспоминаний работников спецслужб многих стран мира [1—3].

История электрической роторной переносной шифровальной машины "Энигма" начинается в 1917 г. с патента, полученного голландцем Хьюго Коч (Hugo Koch). Название "Энигма" в переводе с греческого языка означает "Загадка". Её первый вариант осенью 1919 г. Хьюго Коч запатентовал в Голландии. Через несколько лет он передал права на свой патент докторуинженеру из Дюссельдорфа Артуру Шербиусову (Arthur Scherbiusow), который в конструкцию внёс несколько технических изменений и доработок, в основном, по необходимому постоянному изменению ритмичности (такту) вращения валиков "сердца" машины — "шифровального барабана", которое должно было быть в строгом соответствии с аналогичной машиной на другом конце канала радиосвязи.

На первых порах "Энигма" не пользовалась особым спросом в 1926—1928 гг. Рейхсвер (военное ведомство Веймарской республики, которая существовала на территории Германии в 1919—1933 гг. до прихода к власти фашистской диктатуры) приобрёл всего несколько её экземпляров для своего военно-морского флота.

В 1934 г. А. Шербиусов отошёл от этого проекта, но им занялись доктор Рудольф Хеимсоэт и Элсбэт Ринке.

С этого момента начался настоящий бум в продаже этих машин — их торговая фирма ("Heimsoeth & Rinke") с 1935 г. и до второй половины Второй мировой войны поставляла разные модели и модификации "Энигмы" как германским ведомствам (Вермахт, СС, СД, Абвер, полиция, аппарат правительства и МИД), так и своим сателлитам — Испании, Италии и Японии. Всего было продано свыше 1000 экземпляров. Так, например, в немецкой армии они стали единственной моделью применяемых шифровальных машин, начиная со штабов дивизий и бригад в вышестоящие штабы с применением "Энигмы" передавались абсолютно все радиограммы.

М. Реевский, Х. Зыгальский и Й. Розицкий, 40-е годы.

Вполне естественно, что радиоразведки некоторых стран (например, Польша и Франция) сразу столкнулись с проблемой невозможности расшифровки перехватываемых радиограмм.

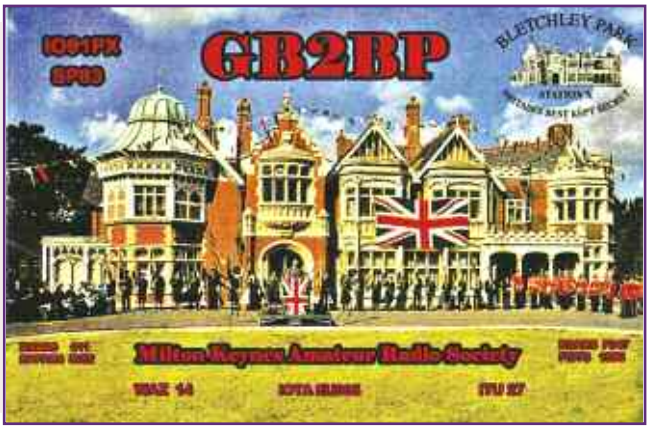
Происходит казусный случай, который в дальнейшем позволил ускорить возможность дешифрования перехватываемых немецких радиограмм. В начале 1928 г. в Варшавскую таможню попадает из Германии посылка. В прилагаемой к ней декларации значится радиопередатчик. Буквально тут же от отправителя приходит запрос-требование на её возврат, как якобы направленной по ошибочному адресу. Заподозрив неладное, польские таможенники информируют об этом свою спецслужбу. Когда открыли ящик, то увидели, что вместо передатчика там находится так называемая "гражданская" модель "Энигмы". Посылку возвращают отправителю, но через подставного посредника спецслужба высылает немецкой фирме заказ на аналогичную модель.

Получив её, польские разведчики поняли, что всё не так просто и зависит от криптологов, которых в распоряжении нет. В 1929 г. в Познаньском университете создаётся кафедра криптологии (греческое слово "крипто" обозначает "тайна", "сокрытие"), на которой начинают обучение двадцать лучших студентов. С 1934 г. она преобразуется в Институт математики.

В конце 1931 г. три студента-математика этой кафедры Марьян Реевский (Marian Rejewski), Хенрик Зыгальский (Henryk Zygalski) и Йержи Розицкий (Jerzy Rozycki) получают задание заняться расшифровкой кодов "Энигмы".

Трудности расшифровки заключались в том, что её нельзя было произвести обычными статистическо-лингвистическими методами, поскольку машина работала как бы хаотически. Марьян и его коллеги каждый день обрабатывали от 80 до 100 перехваченных радиограмм, чтобы постепенно понять основные принципы работы

Трёхроторная военная немецкая шифровальная машина "Энигма".



QSL GB2BP.

QSL HF70E.

машины. Через некоторое время криптологи получили в своё распоряжение ещё один экземпляр "Энигмы", разборка которой позволила изучить механику её "сердца" ("шифровального барабана"). Хотя это и не привело к полной дешифровке кода, но очень приблизило к этому.

Перелом наступил в 1932 г., когда шеф французской разведки капитан Густав Бертранд (Gustaw Bertrand) по согласованию с разведкой Великобритании передаёт польской разведке полученные им от завербованного агента — работника шифровального отдела Рейхсвера (его псевдоним был "Asche", что означает "Пепел") важные материалы: несколько немецких секретных книг с военными кодами ("A", "B", "C", "D", "E" и так называемым "Чёрным кодом") и таблицы их ежемесячных изменений, документы основных мануальных кодов, основы шифров и инструкции по их использованию, образцы шифровок и отвечающие им незашифрованные тексты, а также другие важные документы.

В декабре 1932 г. польские криптологи получают в своё распоряжение секретные инструкции Рейхсвера об основах применения военной модели "Энигма-1", которые были добыты через Эриха Феллгиебла (Erich Fellgiebl; впоследствии — генерала, начальника информационной службы Вермахта).

Королевская чета Великобритании знакомится с экспонатом "Энигмы" в Музее разведки, 90-е годы.

"Энигма-1" имела астрономическое число возможных вариантов кодирования. И самым главным отличием от "гражданской" модели было наличие дополнительной панели со специальными коммутационными гнёздами, контакт каждого из которых имел собственный "ключ". Не имея в своём распоряжении самой машины, по полученным документам, в течение двадцати дней, был произведён теоретико-математический анализ конструкции "шифровального барабана" и коммутационной панели, а также методы и рекомендации по последующей дешифровке перехватываемых радиограмм военного назначения — текстов в виде пятизначных групп.

Через руководителя радиослужбы (отдел BS-4) польской разведки генерала Максимилиана Циецкого (Maksymilian Ciezki) на польских радиопредприятиях "AVA" был размещён заказ на изготовление нескольких экземпляров-аналогов модели "Энигма-1".

С началом Второй мировой войны польские криптологи были перебазированы в Лондон, что позволило союзникам в течение всего периода войны "прикладывать своё ухо ко рту Гитлера". Эта операция по дешифрованию англичанами перехваченных ими немецких сообщений вошла в историю под названием "Ультра". Перехват радиосообщений противника выполняли десятки приёмных станций, имевших кодовое название "Y-station".

В СССР код "Энигмы" был взломан к концу 1940 г. В числе полученной информации были и сведения о подго-

Итальянский диплом.

Кодировочная машина "Фиалка".

товке вторжения в СССР. Несмотря на риск раскрытия источника, сведения были переданы правительству. Однако И. Сталин не поверил в возможность нападения. Несмотря на опасения о возможности Германии слушать советские радиопереговоры, 24 июля 1941 г. У. Черчилль распорядился всё-таки делиться с СССР информацией, получаемой в результате операции "Ультра", при условии полного исключения риска компрометации источника.

С современной точки зрения шифр "Энигмы" был не очень надёжным, но только сочетание этого фактора с наличием множества перехваченных сообщений, кодовых книг, донесений разведки, результатов усилий военных позволило "вскрыть" шифр. После окончания войны все машины были разобраны. Много позже группа из 60 энтузиастов в исследовательских целях воссоздала одну из машин, на что ушло около 10 лет.

"Круглые" даты в истории "Энигмы" не обошли и радиолюбительский эфир. Очевидно, многие коротковолновики имеют в своей коллекции QSL's, работавших в 1999 г. мемориальных позывных: польской — 3Z0ENI, английских — GB60ENI и GB2BP (Музей разведки).

В 2002—2003 гг. в эфире были активны 12 специальных польских позывных: HF70E(N, I, G, M и A) и SN70E(N, I, G, M и A). А SP-DX-Club выдавал и специальный диплом "ENIGMA Award".

В 2014 г. выдавался итальянский диплом.

В сентябре—октябре 2017 г. были активны семь польских спецпозывных (SN0: AP, BP, ENI, NONE, NTWO, RKD и SB).

Если же говорить о СССР, то вскоре после Второй мировой войны была разработана шифровальная машина "Фиалка" (М-125), которая до начала 90-х годов использовалась в странах Варшавского договора. Они выпускались с различными наборами "колёс", как с общими для всех стран, так и для конкретной страны Варшавского договора. Известно обозначение нескольких их модификаций: "0К" — для всех стран (в случае войны), "1К" — для СССР, "3К" — для ПНР, "4К" — для ГДР и "6К" — для ЧССР.

Большая их часть после распада СССР была разобрана или уничтожена. Несколько экземпляров хранятся в частных коллекциях и музеях. Работающая модель представлена в Музее компьютерной истории (Computer History Museum) в США и в Музее разведки, расположенном в Блетчли-Парке (Bletchley Park) в Великобритании.

В истории криптографии до 2005 г. мало что было известно о "Фиалке", поскольку вся информация о её устройстве держалась в секрете. Её более правильное определение — кодировочная машина, она обладала более слабой криптостойкостью, чем шифровальные машины.

ЛИТЕРАТУРА

1. **Dittmer U.** Operacja ENIGMA. — Swiat Radio, 1996, № 10, s. 21—23.

2. **Jarkiewicz S.** (SP2FAP). 3Z0ENI z Kolaczkowa. — MK QTC, 1999, № 9, s. 226, 227.

3. **Маклахлан Д.** Тайны английской разведки (1939—1945) (сокр. перевод с англ. К. Д. Данилова и В. А. Александрова, под ред. А. М. Митрофанова). — М.: Воениздат, 1971, 352 с.