Против «Энигмы»

При рассказе о деятельности советских криптоаналитиков во время Великой Отечественной войны разумеется нельзя обойти тему знаменитого немецкого шифратора «Энигма». Подробнее об этом шифраторе мы еще расскажем.

Задолго до начала Второй мировой войны на войсковых линиях связи немцы ввели трёхдисковую обратимую машину «Энигма» с постоянным коммутатором. Удельный вес шифрпереписки, зашифрованной этими машинами, составлял в немецкой армии примерно 70%. Исследования машины «Энигма» велись по нескольким направлениям, однако раскрыть её до конца войны так и не удалось.

В ходе боевых действий Второй мировой войны в руки советских специалистов попадали экземпляры основной шифровальной машины Германии, а также ключи к ней. Первые два шифратора этого типа были захвачены нашими войсками ещё в 1941 году, один из них — в начале декабря 1941 года во время наступления на Клин. Также в этом году в советский плен попали несколько немецких шифровальщиков. Ещё три «Энигмы» были получены при ликвидации Сталинградского котла и опять среди военнопленных было несколько шифровальщиков, которые были привлечены к сотрудничеству.

Рис. 17. Немцы работают с «Энигмой». С биноклем — Гудериан.

Кстати немцы весьма высоко оценивали возможности советских дешифровальщиков. В январе 1943 года специалисты Управления связи вермахта (немецкие сухопутные войска) пришли к выводу о вскрытии «Энигмы» советскими криптоаналитиками, так как в расположении окруженной под Сталинградом группировки немецких войск находилось 26 шифраторов этого типа, а подтвердить факт их уничтожения в условиях окружения не представлялось возможным и имелась вероятность попадания «Энигмы» к русским. Кроме этого, среди тысяч пленных, захваченных советскими войсками под Сталинградом, могли оказаться шифровальщики[243]. В дальнейшем немцы применяли усовершенствованный вариант «Энигмы». При этом немецкие связисты отдали должное предполагаемым успехам советских криптоаналитиков, когда в решении, принятом на конференции офицеров связи в 1943 году, записали: «Запрещается каким-либо образом выделять передаваемые по радио послания фюрера»[244].

30 июля 1944 года малый охотник МО-105 потопил немецкую подводную лодку U-250. И, не ожидая ничего особенного, просто на всякий случай, водолазы во главе с капитаном III ранга И. В. Прохатиловым попытались проникнуть в потопленную лодку, найти в ней секретные документы. Благо лежала она на глубине всего около тридцати метров. Не тут-то было! Каждый раз, когда какое-либо судно оказывалось в районе потопления U-250, береговые батареи гитлеровцев открывали огонь. Дважды немецкие торпедные катера пытались прорваться к этому месту, но их отбивали советские катерники. Стало известно, что фашисты намереваются сбросить на лодку глубинные бомбы, поставить вокруг нее мины заграждения. Естественно, советское командование пришло к выводу: на подводной лодке есть нечто такое, что враг пытается уничтожить. Несмотря на трудные условия, водолазы сумели поднять важные судовые документы. Между прочим, нашли фотографию командира U-250, почему-то в летной форме. Оказалось, что раньше капитан-лейтенант Вернер Шмидт служил в авиации, принимал участие в бомбежках Лондона, Белграда и Москвы. На флот перешел потому, что морякам платили больше. Спасся Шмидт с лодки

подлым способом: перепустил воздух высокого давления в рубку и вместе с несколькими членами экипажа выбросился на поверхность, оставив остальных погибать. Всплывших моряков подобрал катер МО-105. Увидев поднятые документы, бывший командир U-250 заявил, что саму лодку поднимать нельзя, что она при этом взорвется. И все-таки водолазы продолжали работу. Лодку подняли, привели в Кронштадт, поставили в док, а Шмидт продолжал твердить, что она взорвется, едва ее сдвинут.

Рис. 18. Подлодка U-250 в кронштадтском доке.

Действительно, лодка U-250 была одной из новейших в гитлеровском флоте, и сюрпризов от нее следовало ожидать. Но обошлось. Собственными руками Шмидт отдраил люки, горловины, открыл торпедные аппараты. Были найдены секретные шифры, коды, инструкции, шифровальная машина «Энигма», а кроме того, две новейшие самонаводящиеся торпеды Т-5. Секрет их был раскрыт, и это сыграло большую роль в дальнейшем. После войны многочисленные трофейные «Энигмы» широко использовались в качестве учебных пособий при подготовке советских криптографов[245].

Вышеперечисленные ранние трофеи были тщательно изучены. Это дало свои результаты. В конце 1942 года научные сотрудники специальной группы дешифровальной службы ГРУ с помощью агентуры выявили возможность дешифрования немецких криптограмм, зашифрованных «Энигмой», и приступили к конструированию специальных механизмов, ускоряющих процесс дешифрования. Советские специалисты сумели построить математическую модель немецкого шифратора. Выявили слабости, которые могли способствовать процессу дешифрования. Кстати эта информация была использована при совершенствовании советских шифрмашин, недостатки присущие «Энигме», были исключены в принципе. Заслуги отечественных криптоаналитиков отражены в представлении к награждению орденами группы офицеров дешифровальной службы военной разведки, которое было подписано начальником ГРУ генералом И. Ильичевым 29 ноября 1942 года. К наградам были представлены 14 офицеров: полковник Малышев Ф. П., подполковник Тюменев А. А. и капитан Яценко А. Ф. — к ордену Красного Знамени; майор Уханов И. И., военинженеры III ранга Одноробов М. С. и Баранов А. И., а также капитан Шмелев А. И. — к ордену Красной Звезды. Были награждены и другие офицеры[246]. Однако дешифровать удалось только старые радиоперехваты потому, что в январе 1943 года немцы ввели ряд дополнительных уровней защиты. Преодолеть эти новинки советские криптоаналитики не смогли из-за понятной отсталости электронной техники военного периода.

Вообще следует отметить, что от определения того, можно ли принципиально дешифровать роторную шифрмашину до практических результатов — дистанция огромного размера. Возможно, удавалось эпизодически вскрывать некоторые сообщения, однако о массовом чтении «Энигмы» в СССР говорить нельзя. Но это было закономерно, так как наши криптографы не обладали той исходной информацией, которая имелась у англичан, а также из-за отсутствия достаточных человеческих и материальных ресурсов, а также слабого развития «машинных» средств обработки информации. Следует признать, что Д. Кан[247] и другие источники, утверждающие о постоянном практическом дешифровании «Энигмы» советскими специалистами ошибаются.

А теперь самое главное — огромный массив информации, касающейся дешифрования англичанами «Энигмы», в первую очередь содержание дешифрованных криптограмм, советское руководство получало по линии агентурной разведки. Исходя из этого, разумно предположить, что руководители СССР и отечественных дешифровальных служб решили не тратить наши весьма ограниченные силы на «Энигму», так как в данном случае за нас всю необходимую работу делали англичане.

Основное внимание советские криптографы уделяли армейским «ручным» шифрам и кодам Германии, а также шифрмашинам других типов. На этом поприще им удалось достичь значительных результатов.