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:

«ИЗ СПЕЦСООБЩЕНИЯ УНКВД ПО ЛЕНИНГРАДСКОЙ ОБЛАСТИ СЕКРЕТАРЮ ЛЕНИНГРАДСКОГО ОБКОМА ВКП(б) М. Н. НИКИТИНУ О ПОПЫТКАХ НЕМЕЦКИХ КОНТРРАЗВЕДЫВАТЕЛЬНЫХ ОРГАНОВ ИСПОЛЬЗОВАТЬ РАДИОИГРЫ В ЦЕЛЯХ ДЕЗИНФОРМАЦИИ КОМАНДОВАНИЯ КРАСНОЙ АРМИИ

Апрель 1943 г.

Из ряда перехваченных документов противника… устанавливается, что немецкие контрразведывательные органы придают серьёзное значение вопросу… дезинформации командования Красной Армии и подготовки условий для борьбы с партизанскими отрядами (перехват связистов и пр.).

Дезинформация осуществляется противником посредством радиоигр, которые с ведома штаба „Валли“ проводятся непосредственно контрразведывательными командами и группами в контакте с командованием соответствующих подразделений немецкой армии.

Против участков Ленинградского, Волховского и Северо-Западного фронтов контролирует и руководит радиоиграми находящаяся в г. Пскове 304-я контрразведывательная команда, на учёте которой имеется до 30 радиоигр… причём некоторые радиоигры продолжаются до настоящего времени.

В целях своевременного предотвращения попыток противника дезинформировать посредством радиоигр командование Красной Армии и вести работу на перехват выбрасываемых в тыл немецкой армии наших разведчиков, связистов и партизанских групп прошу дать указание Вашему аппарату:

1. Немедленно давать исчерпывающие ответы на запросы КРО УНКВД по Ленинградской области, связанные с выявленными провалами выброшенных в тыл противника партизанских групп и одиночек.
2. Одновременно информировать КРО о всех выявленных в процессе работы провалах и о разведчиках, подозреваемых в связи с немцами, с целью их учета и проверки по материалам КРО.
3. В тех случаях, когда в процессе радиообмена будет вскрыта радиоигра противника и представится возможным продолжить её в контрразведывательных целях, передать в КРО все необходимые для продолжения радиоигры материалы (состав группы, её связи за линией фронта, задание, технические радиоданные и проведенный уже радиообмен).

Начальник УНКВД
по Ленинградской области
комиссар госбезопасности III ранга
Кубаткин
ЦА ФСБ России»[39].

А вот немецкий документ, посвященный данному вопросу:

«ИЗ ОТЧЕТА НАЧАЛЬНИКА 304-й АБВЕРКОМАНДЫ О РЕЗУЛЬТАТАХ КОНТРРАЗВЕДЫВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ЗА АПРЕЛЬ 1944 г.

8 мая 1944 г.

…**Радиоигры „Секретная связь“.**

В настоящее время абверкомандами проводятся 4 радиоигры „Секретная связь“, 2 из которых („Аня“ и „Вапс“) возобновлены в отчетном месяце. Радиоигра „Аня“ началась 15 апреля 1944 г. в абверкоманде-301.

Схваченный вражеский радист принадлежал к группе разведотдела 2-го Прибалтийского фронта численностью 10 человек. Группа была заброшена 26 марта 1944 г. с заданиями проводить разведку противника и осуществлять диверсии.

Радиоигра „Вапс“ началась 22 апреля 1944 г. в абверкоманде-326, а также в VAO-326 (имеется в виду абвергруппа-326) в Ревеле (ныне город Таллин, Эстония. — *Авт.*). Игра ведется с эстонским НКВД, который 7 апреля 1944 г. через Центральный штаб эстонских партизан забросил группу в составе 2 человек с заданиями проводить разведку и подрывную работу в районе Феллин — Тарту.

Проводившаяся в VAO-326 радиоигра „Морская чайка“ была в отчетном месяце прервана, так как с середины января 1944 г. она велась безрезультатно.

Давно подозревавшиеся связи, тянущиеся с территории Прибалтики через Финляндию к шведской и английской разведслужбам, подтверждены благодаря случаю, установленному КОР (германский разведывательный и контрразведывательный орган „Кригсорганизацион Финляндия“. — *Авт.*).

На основании материала, захваченного у задержанного курьера, явилась возможность обнаружить эстонскую тайную организацию, которая наряду с политической деятельностью в духе националистических устремлений к самостоятельности, занималась шпионажем против германского вермахта и поставляла разведматериал в разведцентр эстонских эмигрантов

в Стокгольме как непосредственно, так и через Финляндию; данный разведцентр работает на Англию. Благодаря вмешательству полиции безопасности к настоящему времени удалось задержать около 100 лиц, которые сейчас допрашиваются; допросы прольют свет на обстоятельства, связанные с деятельностью организации.

Удавшееся независимо от этого случая нападение на литовского подполковника, у которого кроме документов были найдены инструкции по нелегальной радиосвязи между Каунасом и Стокгольмом, дало в руки факт существования разведывательной организации противника, работающей в Каунасе. Допросы с целью выяснения всех обстоятельств ещё ведутся…

Начальник команды
майор Гезенреген
ЦА ФСБ России, перевод с немецкого»[40].

Отметим, что немцы использовали радио и для проведения психологических операций. Так на переднем крае используя усилители большой мощности немцы вели пропаганду и склоняли красноармейцев к сдаче в плен. Часто передачи вели недавно сбежавшие изменники, которые обращались к своим бывшим товарищам по имени и фамилии и рассказывали как хорошо в плену, мол, немцы хорошо относятся к пленным, обеспечивают их хорошим питанием и кругом царят образцовая чистота и порядок. Делалась ставка и на вредные привычки, говорили, что немцы дают пленным сколько угодно шнапса и нередко к ним приезжают девочки. К сожалению, в начальный период войны некоторые красноармейцы поддавались на подобные провокации. Но после успехов нашей армии на фронтах, эффективность подобной пропаганды резко упала[41] [en.wikipedia].

В 1944 году подразделения пропаганды вермахта совместно с полком СС «Курт Эггерс» провели в полосе ответственности группы армий «Северная Украина» самую крупную психологическую операцию периода Второй мировой войны под названием «Восточный скорпион». Ее наиболее активная фаза пришлась на сентябрь–октябрь 1944 года. В ней были задействованы 93 офицера, более 1300 унтер-офицеров и рядовых. В их распоряжении имелись 16 мощных звуковещательных станций, поезд-типография, передвижной широковещательный КВ-передатчик мощностью 80 кВт и две стационарные радиостанции. Несмотря на военные трудности того времени, военно-воздушные силы предоставили необходимое количество самолетов для распространения печатных пропагандистских материалов. К участию в операции привлекались также подразделения РОА[42]. Однако ввиду общей неблагоприятной для немецких войск обстановки на фронте, операция «Восточный скорпион», несмотря на частично достигнутые положительные результаты, не смогла оказать существенного влияния на ход боевых действий[43].

В заключение данной главы подведём некоторые итоги. Несомненное первенство Германии (до и во время войны) в конструировании и практическом применении роторных шифровальных машин побудило потенциальных противников Германии включиться в развитие собственных методов и аппаратуры шифрования и криптоанализа. С начала Второй мировой войны дешифрование сообщений противника приобрело чрезвычайно для союзников по антигитлеровской коалиции важное значение, так как немецкое командование в условиях блицкрига при быстром перемещении своих войск для передачи приказов преимущественно использовало радиосвязь. Союзникам жизненно необходимо было разработать совершенно новые способы криптоанализа и технических средств для дешифрования передач многочисленных шифрмашин типа «Энигма» и других.

По мнению англо-американских историков, если бы не взлом немецких шифровальных кодов, война длилась бы на два года дольше, потребовались бы дополнительные жертвы, также возможно, что на Германию была бы сброшена атомная бомба. Взлом «Энигмы», других немецких шифровальных машин, ручных шифров и кодов обеспечил союзникам не только доступ к военно-тактической информации, но и к информации МИДа, полицейской, СС-овской и железнодорожной и т. д. Сюда же относятся сообщения стран «оси», особенно японской дипломатии, и итальянской армии. Дешифрование японских шифрсообщений сыграло значительную роль в победе союзников на Дальнем Востоке.

Взлом немецкой шифртехники для хода войны имел исключительно важное значение, т. к. союзники благодаря получаемой дешифрованной информации имели существенные преимущества. Однако далеко не все модификации роторных шифрмашин поддавались практическому взлому. Для таких работ требовались исключительно большие человеческие (для разработки теоретических основ машинной криптологии) и вычислительные ресурсы, кото-

рые могут себе позволить себе только страны, обладающие исключительно высоким криптографическим потенциалом. Потенциально высокие криптографические характеристики механических и электрифицированных роторных шифрмашин, созданных во время войны, позволили эксплуатировать их вплоть до конца 1980-х годов. Разработка и эксплуатация новых моделей роторных электромеханических криптомашин со значительно увеличенной стойкостью против возможного дешифрования продолжалась в различных странах и после окончания войны (помимо Восточной Германии и ФРГ также в СССР, США, Канаде, Италии, Швейцарии, Швеции, Польше и ряде других стран.

Появление миниатюрных электронных схем ознаменовало собой переворот в сфере шифровальных технологий. С последних десятилетий XX века наблюдается неуклонный рост мирового спроса на компактные и простые в эксплуатации шифровальные средства со все более высоким уровнем безопасности не только в правительственном и военном, но также и в гражданском, коммерческом секторе. Этим объясняется быстрое возрастание сложности современной криптографической науки и техники, идущих вслед за развитием новых электронно-вычислительных технологий. Эра механических шифрмашин времен Второй мировой войны с её криптографическими победами и поражениями закончилась. Однако захватывающее знакомство со страницами ушедшей великой мировой криптографической войны может оказаться не только интересным, но и поучительным для грядущего.

Теперь несколько слов о судьбе немецких криптографов в послевоенное время. По заданию специально созданного союзниками органа TICOM («Target Intelligence Committee» — «Комитет по целевой разведке») в последние месяцы войны две сотни ведущих криптографов Германии были тайно переброшены в Великобританию. В марте 1945 года шесть специально подготовленных англо-американских групп были отправлены в Германию с первоначальной задачей найти и захватить немецкие криптографические центры, местоположение которых было установлено, главным образом, благодаря дешифровавшейся в Блетчли-Парк «Энигме». Главная задача групп TICOM состояла в том, чтобы захватить столько германского криптооборудования, сколько будет возможно и вывезти его вместе с обслуживающим персоналом. Одна из групп была послана для захвата замка в Саксонии, где находился архив радиоразведки министерства иностранных дел. В результате успешной операции весь этот объект, включая и штатных сотрудников, был переправлен в Британию.

Эта же группа TICOM захватила конвой грузовиков, в котором перевозили четыре германских шифратора «Fish», группу техников-шифровальщиков и командовавшего ими офицера. Всю эту технику вместе с людьми также отправили в Англию. Добытые в Германии материалы дали англо-американским союзникам информацию о том, какие из их собственных шифров были вскрыты немцами. В частности, оказалось, что Германия успешно читала «Шифр ВМС № 3», использовавшийся британскими и американскими конвоями в Атлантическом океане. Именно по этой причине конвои столь часто становились жертвой атак немецких подводных лодок. Собранные TICOM данные позволили впоследствии читать секретную переписку по крайней мере 35 стран, включая Францию, Италию, Японию, Испанию, Швейцарию и Ирландию[44].

---

1 http://en.wikipedia.org

2 Лайнер Л. Погоня за «Энигмой», М.: Молодая гвардия, 2004. С. 27.

3 Enigma Family Tree. Version 0.14–10 September 2009.//cryptomuseum.com/

4 А. Шербиус никогда не узнал о беспрецедентном успехе своего шифратора «Энигмы» так как погиб в дорожно-транспортном происшествии 12 мая 1929 года. См. Лайнер Л. Указ. соч. С. 28.

5 Kruh Louis, Deavours Cipher A. The Commercial Enigma: Beginnings of Machine Cryptography. Cryptologia, vol. 26, № 1, January 2002, p.1–16.

6 Лайнер Л. Указ. соч. С. 313.

7 GC183VZ Darwin Enigma Challenge (Unknown Cache) in Northern Territory, Australia created by gib — Microsoft Internet Explorer.

8 Межутков А. Исторический экскурс. DigitalSecurity 2003.

9 http://en.wikipedia.org/wiki/Siemens&Halske T52

10 Weierud Frode. Bletchley Park's Sturgeon, the Fish that Laid No Eggs. The Rutherford Journal, vol 1, December 2005. //www.Cryptocellar.org/

[11] Более подробную информацию об устройстве данных шифрмашин, а также работе по их дешифрованию шведами и англичанами можно получить из следующих ичточников: Бутырский Л. С., Гольев Ю. И., Ларин Д. А., Никонов Н. В., Шанкин Г. П. Криптографическая деятельность в Швеции в первой половине XX века // Защита информации. INSIDE. № 4, 2007. С. 88–96, Стефанович А. В. История успехов и неудач шведской радиоразведки (1914–1944 гг.) // www. agentura.ru., Beckman, Bengt: A Swedish Success: Breaking the German Geheimschreiber during WW2. Monograph produced by Forsvarets Radioanstalt, Stockholm, Sweden (1997), Beckman Bengt. Tr., Kjell-Ove Widman. Codebreakers: Arne Beurling and the Swedish Crypto Program during World War II. Providence, RI: American Mathematical Society, 2002, Davies Donald W. The Siemens and Halske T52e Cipher Machine. Cryptologia, vol.6, № 4, October 1982, p.289–308, Davies Donald W. The Early Models of the Siemens and Halske T52 Cipher Machine. Cryptologia, vol.7, № 3, July 1983, p.235–253, Davies Donald W. New Information on the History of the Siemens and Halske T52 Cipher Machine. Cryptologia, vol.18, № 2, April 1994, p.141–146, www.fra.se — официальный сайт шведской радиоразведки (FRA), www.hem.passagen.se — сайт шведского историка Торбьона Андерссона (Torbjörn Andersson).

[12] www.hem.passagen.se. Указ. сайт.

[13] Schmeh Klaus. Die Enigma wurde wie andere Maschinen geknackt, aber kaum bekannt ist, dass die Nazis gegen Ende des Krieges an weiterer Verschlusselungsmschinen gearbeitet haben. //www.heise.de/tp/r4/artikel/17/17995/1.html.

[14] Черняк Л. Colossus, победивший Lorenz. Открытые системы, № 10, 2004 // www.osp.ru/os/2004/10/184688

[15] Краткий очерк о его вкладе в мировую криптографию содржится в статье Бутырский Л. С., Гольев Ю. И., Ларин Д. А., Никонов Н. В., Шанкин Г. П. Криптографическая деятельность в Швеции. От викингов до Хагелина // Защита информации. INSIDE. № 3, 2007. С. 88–96.

[16] Подробнее об этом можно прочитать в книгах: Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Криптография: страницы истории тайных операций. М.: Гелиос АРВ, 2008, Соболева Т. А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002, Kahn D. The codebreakers. N- Y: Macmillan Publ. Co., 1967.

[17] Подробнее о японских шифрмашинах и работе американцев по их дешифрованию можно прочитать в книгах Ландер И. И. Негласные войны. История специальных служб 1919–1945. Одесса, «Друк» 2007. http://www.lander.odessa.ua и Kahn D. Указ. соч., а также на сайте http://en.wikipedia.org.

[18] Забелин А. Центр японского шпионажа в Скандинавии // Независимое военное обозрение №6, 2008. С. 7.

[19] Забелин А. Указ. соч.

[20] О дешифровании «Энигмы» написаны десятки книг и сотни статей, привести их все в рамках данной книги не представляется возможным, так что приведем наиболее доступные источники по данному вопросу на русском языке: Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Указ. соч. С. 167–219, Лайнер Л. Указ. соч., Ларин Д. А., Шанкин Г. П. Вторая мировая война в эфире: Некоторые аспекты операции «Ультра» // Защита информации. INSIDE. № 1, 2007. С. 91–96, № 2, 2007. С. 87–96., Уинтерботем Ф. Операция «Ультра». М. Военное издательство, 1978.

[21] Подробнее о её деятельности см. Бутырский Л. С., Ларин Д. А. История цифровых систем засекречивания речевого сигнала в США // Защита информации. INSIDE. № 3, 2006. С. 82.

[22] Подробнее о деятельности этой службы можно прочитать в статье Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Служба наблюдения Кригсмарине // Защита информации. INSIDE. № 5, 2006. С. 70–74, № 6, 2006. С. 90–94.

[23] Анфилов В. А. Провал «Блицкрига». М.: Наука 1974, 616 с. // http://www.mgimo.ru/publications/?id=25007. 8.01.2012.

[24] Kahn D. Указ. соч. P. 648.

[25] Kahn D. Указ. соч. P. 647.

[26] Кан Д. Указ. соч. С. 235–236.

[27] Kahn D. Указ. соч. P. 649.

[28] Кан Д. Указ. соч. С. 233.

[29] Кан Д. Указ. соч. С. 234.

[30] Кан Д. Указ. соч. С. 235.

[31] Кан Д. Указ. соч. С. 235.

[32] Кан Д. Указ. соч. С. 236.

[33] Пронин Александр. Без грифа «секретно»: Нацистские взломщики кодов. Журнал «Братишка», Ноябрь № 11, 2005 // www.bratishka.ru/archiv/2005/11/9.php.htm

[34] Органы, 1995. Том 4. Книга 2.

[35] Органы, 1995. Том 4. Книга 2.

[36] Кан Д. Указ. соч. С. 232.

[37] Старков Б. А. Радиоигры ленинградских контрразведчиков. Ученые записки Петрозаводского государственного университета, 2008, Август, № 2.

[38] Более подробную информацию о ходе данной операции можно, в частности, получить из следующих источников: Бутырский Л. С., Гольев Ю. И., Ларин Д. А., Шанкин Г. П. История криптографической деятельности в Нидерландах // Защита информации. INSIDE. № 5, 2008. С. 91–96, № 6, 2008. С. 79–86, Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Указ. соч., Kahn D. Указ. соч.

[39] Органы, 1995. Том 4 книга 1.

[40] Органы, 1995. Том 5 книга 1.

[41] http://en.wikipedia.org

[42] Созданная немцами из предателей русская освободительная армия — её бойцы более известны под названием «власовцы».

[43] Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт). Изд. Минск, 1999.

[44] http:.// www.nsa.gov/public__info/_files/european_axis_sigint/volume.2_notes_on_german.pdf.