Заключение

Грамотно сконструированные шифраторы навечно сохраняют в секрете от врагов России её наиболее важную дипломатическую, агентурную и военную переписку…так или иначе русские вознесли достижения своей страны в криптологии до высоты полета её космических спутников[1]
Дэвид Кан

СССР как главный победитель в войне понес невиданные доселе материальные и людские потери: более 27 миллионов своих граждан; уничтожено 32 тысячи промышленных предприятий; разрушены сотни городов и свыше 70 тысяч сел и деревень, 98 тысяч колхозов, 1876 совхозов, 2890 машинно-тракторных станций; сметены с лица земли десятки тысяч больниц, школ, вузов, осталось без крова 25 миллионов человек. Вслед за этим западные страны и США со своими доктринами «сдерживания», «балансирования на грани войны» развязали затяжную «холодную войну», стремясь добиться осуществления своих собственных прогнозов, делая ставку на военную силу.

Испытание в 1949 году в СССР атомной бомбы стало отрезвляющим фактором в созданной ими мировой политической обстановке. К этому времени в стране уже убедительных успехов добились определяющие отрасли экономики: металлургия, энергетика, авиастроение, станкостроение, сельскохозяйственное машиностроение и другие. Становилось прочно на ноги ракетостроение. Но в развитии средств связи, вычислительной техники, радиоаппаратостроения, радиоэлектроники, как специальной, так и бытовой был очевиден большой пробел. Страна отставала в развитии и применении как низовой, так и магистральной защищенной связи в Вооруженных силах и Военно-морском флоте. В это же время в странах, не так сильно пострадавших от войны, радиотехника и радиоэлектроника получили активное развитие и явились катализатором научно-технического прогресса.

Понимая сложившуюся ситуацию в области специальной связи, оставшиеся после демобилизации немногочисленные военные криптографы обратились через голову своего могущественного шефа — Лаврентия Берия — к И. В. Сталину. Обращение было услышано и советская криптография была принята под крыло самого мощного органа Советского Союза — ЦК ВКП(б). Осенью 1949 года Политбюро ЦК приняло ряд важнейших для советской криптографии решений, суть которых сводилась к следующему:

— на базе 6-го Управления МГБ и дешифровально-разведывательной службы Генштаба Вооруженных Сил Постановлением Политбюро ЦК ВКП(б) № П71/426 от 19 октября 1949 года было создано Главное управление Специальной Службы (ГУСС) при ЦК ВКП(б) с одновременным выделением больших средств для его становления и развития;
— были приняты меры к привлечению наиболее сильных ученых, как для выполнения оперативных задач криптографической службы, так и в роли преподавателей для подготовки новых высококвалифицированных кадров;
— для выполнения последней цели создавались Высшая школа криптографов и закрытое отделение механико-математического факультета МГУ[2].

ЦК КПСС и СМ СССР Постановлением № 5275–2282 от 22 декабря 1951 года передавало 25 заводов из других министерств в полувоенное Министерство промышленности средств связи. МПСС развивалось как одно из самых

динамических министерств и на его базе за два с половиной десятилетия выросло три крупнейших министерства: электронной промышленности, радиотехнической промышленности и промышленности средств связи СССР.

Реализация этих решений за каких-то три с небольшим года позволила коренным образом изменить лицо советской криптографии. Для дальнейшего развития техники криптографической информации в СССР в период 1950-х годов были созданы и начали функционировать промышленные научно-исследовательские и проектные организации, которые включились в процесс разработки и обеспечения промышленного выпуска аппаратуры криптографической защиты телефонных переговоров и телеграфной информации и определили начало процесса активного использования и развития научного и производственного потенциала промышленности в интересах оснащения структур государства техникой защиты информации. К середине 1951 года на территории СССР функционировали 199 ВЧ-станций, обслуживавшие 2465 абонента, и за рубежом 24 ВЧ-станции с обслуживанием 439 абонентов[3].

12 января 1952 года постановлением Совета Министров СССР был создан ГосНИИ № 2, преобразованный затем в предприятие п/я37, переименованное в 1966 году в Научно-исследовательский институт автоматики (НИИА). Цель создания — выполнение важнейших исследований по разработке и построению техники для засекреченной связи. В 1950–1960 годы в НИИА было создано первое поколение отечественной шифраппаратуры, главными разработчиками которой были А. П. Петерсон, К. Ф. Калачев, И. С. Нейман, А. М. Нанос, Н. Б. Петров, Ю. Я. Волошенко, Н. Н. Найденов, Ю. А. Солдатихин, А. М. Васильев, А. Н. Кабатов, Б. А. Николаев, Г. В. Кукушкин, А. Ф. Носов, В. А. Никитин, В. П. Дементьев и др. Первая серийная аппаратура систем засекреченной связи была создана в НИИ уже в 1954 году и установлена на линиях Москва–Берлин и Москва–Пекин. На то время этот самый протяженный засекреченный канал связи обеспечивал не только высокую стойкость, но и качество связи[4]. В 1950–1960-е годы в институте были разработаны шифровальные аппараты первого поколения, позволявшие защищать речевые переговоры по телефонным и коротковолновым каналам связи: «М-803–5», «Лиана», «Алмаз», «Булава» и др. В дальнейшем разрабатываются специальные комплексы технических средств засекречивания связи и управления: «Кавказ», «Роса» и «Интерьер»[5].

Начиная с 1956 года завод п/я 64 в Запорожье (с 1966 г. завод «Радиоприбор», предприятие п/я А-1405) был определен головным по производству аппаратуры закрытия каналов связи, разрабатывавшейся Московским НИИ-2. Первыми из этого направления осваивались изделия «Брусок» (главный конструктор Личидов Ю. Я.), «Ландыш» (главный конструктор Николаев Б. А.), «Сирена», «КУ-ЛС», затем «Север-М» (главный конструктор Мартынов И. Д.), «Лотос-В», «Стрела», а за ними вокодерная аппаратура «Булава» (главный конструктор Петерсон А. П.) в подвижном и стационарном вариантах, на основе которого родились «Группировка», «Карпаты», а также «чемоданный оперативный вариант»[6].

Во второй половине 1960-х годов в полевую сеть правительственной связи внедрена аппаратура засекречивания временной стойкости «Коралл» и гарантированной стойкости «Лагуна». В эти же годы в странах социалистического лагеря (Чехословакия, Венгрия, Монголия, Польша, ГДР) организованы свои сети правительственной связи, для чего им переданы станции и аппаратура ВЧ-связи и аппаратура засекречивания, шифры для которой изготовлялись в СССР и направлялись к местам назначения диппочтой[7].

Несмотря на принятые меры, все еще имело место несоответствие между потребностями заказчиков в лице Министерства Обороны, КГБ и других ведомств и возможностями промышленности, что определило актуальность создания дополнительных НИИ и заводов, расширяющих ресурсы в области разработки и промышленного изготовления новых видов техники защиты информации специального назначения. Учитывая это, в городе Пензе приказом Госкомитета по радиоэлектронике при СМ СССР от 18 января 1958 г. № 34 для указанных целей был образован НИИ-3 (будущий ПНИЭИ), «дочернее» предприятие для НИИ-2, из которого в Пензу были приглашен коллектив сильных конструкторов. Позднее НИИ-3 был назначен головным по разработке аппаратуры шифрования телеграфной информации и данных[8].

Успехи нашей Спецслужбы особенно весомы в свете того, что в условиях «холодной войны» ей приходилось противостоять не только европейским спецслужбам, но и мощному Агентству национальной безопасности США. АНБ было создано в 1953 году в обстановке чрезвычайной

секретности на базе нескольких криптографических и радиоразведывательных органов различных американских министерств. С истинно американской скоростью АНБ развернуло по всему миру, и прежде всего вблизи границ нашей страны, сеть станций радиоперехвата[9].

В послевоенные годы в СССР на смену прежним электромеханическим машинам для предварительного шифрования текстов пришли практически такие же громоздкие и тяжелые печатающие электромеханические модели М-104 «Аметист», «Аметист-2» и М-105 «Агат», обеспечивавшие высокий, «гарантированный» уровень засекречивания[10]. Несмотря на конструирование шифрмашин нового поколения с использованием транзисторной электроники интерес к роторным шифрмашинам, относящимся к классу криптографических решений, применявшихся в семействе немецких шифрмашин «Энигма» и считавшихся устойчивыми в работе к электромагнитным и жестким поражающим излучениям, на которые негативно реагирует полупроводниковая электроника, не был утрачен.

Ряд моделей отечественной роторной шифрмашины М-125 «Фиалка» были разработаны в период холодной войны вскоре после окончания войны. На эксплуатацию она была поставлена с начала 1960-х годов в качестве основной шифрмашины для засекреченной связи между дипломатическими кругами стран Варшавского Договора в период до начала 1990-х годов. Новая печатающая шифрмашина предварительного шифрования М-125 была взята на вооружение Советской Армией в 1965 году и получила кодовое наименование FIALKA («Фиалка»), под которым она стала впоследствии хорошо известна за рубежом, где её криптографические характеристики оценивались очень высоко. По сравнению с наиболее распространенными 3-х или 4-хроторными «Энигмами» количество роторов в «Фиалке» было увеличено до 10-ти с дополнительными возможностями вращения роторов в противоположных направлениях и изменения внутрироторных проволочных соединений в полевых условиях. Каждая из стран Варшавского Договора располагала собственным криптографическим вариантом М-125–3хх (символы «хх» указывали на собственную «национальную» криптографическую версию)[11].

Отечественные конструкторы и криптографы широким фронтом продолжают усовершенствование прежних и разработки новых технических средств защиты информации передаваемой по всевозможным каналам связи. «Старейшее» головное предприятие России — «НИИ Автоматики» (бывший НИИ-2) за выдающиеся достижения в области науки и техники был награжден Орденом Ленина ещё в 1978 году. В период с 1993 по 2005 гг. институтом разрабатывается семейство технических средств специальной связи, реализующее качественно новые принципы и технологии создания шифраппаратов. Суть этих подходов состоит в построении функциональных узлов спецаппаратов на основе методов цифровой обработки сигналов с последующей реализацией каждого функционального узла (речепреобразующего устройства, спецблока, модема) на вычислителях реального времени, построенных

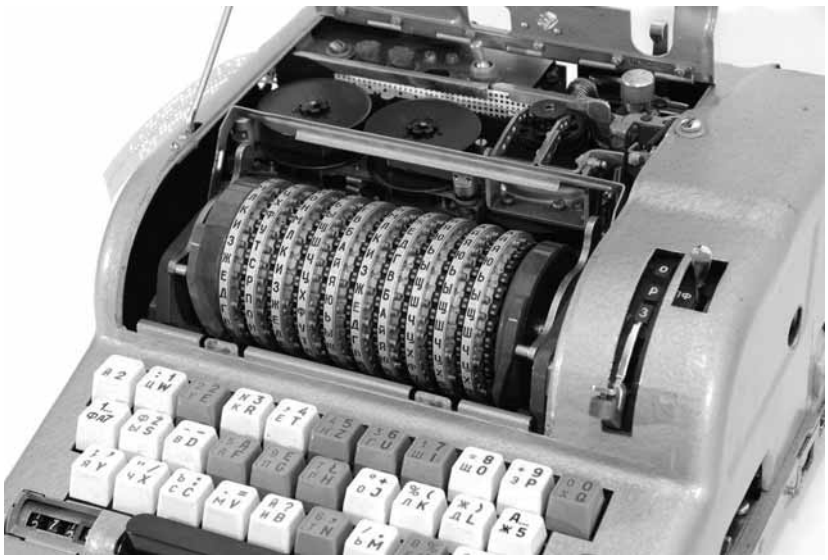

Рис. 1. Вид на роторы, клавиатуру и печатающий механизм «Фиалки»

на цифровых процессорах обработки сигналов. В соответствии с современной мировой криптографической политикой НИИА разрабатывает семейства шифраппаратуры, предназначенные для зарубежных и коммерческих продаж[12].

Столь же динамично развивается ПНИЭИ (бывший НИИ-3), являющийся одним из крупнейших предприятий России, разрабатывающим и производящим технику криптографической защиты информации, телекоммуникационного оборудования для сетей специальной связи министерств и ведомств, включая предприятия и организации любой формы собственности.

В современном противоречивом мире помимо постоянных военных конфликтов идет глобальная транснациональная информационная война по всем средам и каналам передачи открытых, дезинформирующих, шифрованных сигналов. Необходимость наращивания таких составляющих информационную войну технологий, как разведка, радиоконтроль и радиоперехват, дешифрование и т. д. постоянно усиливается. Поэтому по прежнему остаются актуальными слова нашего вероятного противника Адмирала Томаса Х. Морера (бывшего Председателя Объединенного Комитета начальников штабов США): «Если начнется Третья мировая война, то победителем будет та сторона, которая сможет лучше действовать и обращаться с электромагнитным спектром»[13].

---

1 Кан Д. Взломщики кодов. — Пер. с англ. А. Ключевского. — «Секретная папка» — М.: М.: ЗАО Изд-во Центрполиграф, 2000. С. 172.

2 Кузьмин Л. А. ГУСС — этап в развитии советской криптографии // Защита информации. Конфидент. № 4, 1998. С. 89–94.

3 Краткая хроника истории органов и войск правительственной связи (часть вторая: 1945–1969 гг.). http://www.radioscanner.ru/info/article283

4 http://niia.ru>document/history.htm

5 Рузайкин Г. И. Отечественные криптографические технологии. Computerworld, № 47, 2002 г.

6 Крохмаль В. М. О предприятии. Запорожское государственное предприятие «Радиоприбор» 1951–2001 гг. http://www.RADIOPRIBOR.narod.ru.

7 Краткая хроника. Указ. соч.

8 http://www.pniei.penza.ru/company/history.htm.

9 Кузьмин Л. А. Указ. соч.

10 http://www.scz.bplaced.net/m105.html M-104 AMETHYST-2, M-105 N AGAT.mht

11 Perera T., Hamer D. General Introduction: Russian Cold War Era M-125 and M-125–3MN Fialka Cipher Machines. http://www.w1tp.com/enigma museum

12 http://niia.ru Указ. сайт.

13 Arcangelis M. Radio-electronic War. — London: Blandford Press Ltd, 1985. Русский перевод Ю. Репка : Марио де Арканжелис. Радиоэлектронная война (от Цусимы до Ливана и Фолклендских островов), 2000 г.