Введение

У каждой страны нет ничего более секретного, чем её шифры, поскольку их раскрытие другим государством повлечет за собой утечку многих тысяч секретов, закрываемых этими шифрами… Пока существуют государства, будет оставаться и необходимость в защите государственных секретов.
Н. Н. Андреев[1]

Л. С. Бутырский*, Д. А. Ларин**, Г. П. Шанкин***

Из многочисленных работ, посвященных многовековой истории развития мировой *криптографии* или *криптологии* — науке передачи ценной политической, военной и другой текстовой информации в тайной форме (защищенной от всех кроме конкретного адресата, владельца секретного ключа) известно, что за прошедшие столетия она получила развитие и практическое применение во многих странах. Криптография ровесница письменности. Эта наука прошла путь от папируса до компьютера и по возрасту старше Египетских пирамид. Она в своем развитии прошла через этапы: «криптография как искусство» и «криптография как ремесло» к этапу «криптография как наука». Криптография всегда развивались в тесном взаимодействии с математикой. Эти науки взаимно дополняли и обогащали друг друга.

Ряд древних систем шифрования возник одновременно с идеографической (пиктографической, клинописной, иероглифической) письменностью в Древнем Шумере в конце IV — начале III тысячелетия до н. э. Затем они употреблялись в Вавилонском царстве, в Ассирии, в Древнем Персидском государстве, Египте, Китае, Индии, т. е. существовали независимо на протяжении многих веков и даже тысячелетий у разных народов, на разных территориях. Одними из первых криптографию стали использовать различные государственные структуры для защиты правительственных, военных, дипломатических сообщений. Фактически, как только где-то на Земле происходило становление того или иного государства как тут же начиналась криптографическая деятельность, с развитием государственных институтов учреждались специальные криптографические службы. Вообще считается, что признаками великой державы являются наличие у страны ядерного оружия, успехов в освоении космоса и достижений в области криптографии.

Перед началом Второй мировой войны *все ведущие страны* уже имели на вооружении электромеханические шифрсистемы, обладающие высокой скоростью обработки информации и высокой стойкостью к дешифрованию. Одно время считалось даже, что существующие на то время шифрсистемы невозможно дешифровать, и что наступил конец эпохи криптоанализа. Но уже в ходе войны это мнение было опровергнуто.

* **Леонид Сергеевич Бутырский** — полковник, почетный радист России, историк криптографиии.

** **Дмитрий Александрович Ларин** — полковник, доцент кафедры ИТС МГТУ МИРЭА, к.т.н.

*** **Генрих Петрович Шанкин** — полковник, д.т.н., профессор.

При оценке влияния криптографии на те или иные события мировой истории следует использовать более широкое понятие — криптографическая деятельность. Под криптографической деятельностью понимается не только шифрование и дешифрование, но и организация каналов передачи сообщений (системы связи), использование различных методов защиты информации (криптография, стеганография, физическая защита собственных линий связи и т. д.), организация перехвата шифрованной информации противника. Дешифрование без перехвата невозможно. Разумеется, сюда входят меры по добыванию информации, облегчающей дешифрование (добывание ключей, описания шифрсистем и т. д.). С другой стороны, при разработке методов и средств защиты информации необходимо учитывать возможные аналогичные действия противника и предпринимать соответствующие меры для их пресечения. Если действия по добыванию информации связаны с разведывательными операциями, то при защите главную роль играют контрразведывательные мероприятия. Поэтому криптографические службы работают в тесном контакте с разведкой и контрразведкой.

Во все времена решающим условием успешной деятельности разведчика была и остается надежная связь (защищенная от перехвата и понимания её противником) с центром. В военной обстановке, когда ситуация может мгновенно и радикально изменяться, а своевременно добытые данные о предполагаемом маневре противника способны спутать все его карты, значение четко работающей связи возрастает во сто крат.

Вообще криптографическая деятельность является составной частью информационного противоборства, которое включает в себя организацию пропаганды и информационного воздействия на потенциального и реального противника и своего населения (поддержка патриотического духа, разъяснение политики государства и т. д.), ведение контрпропаганды, проведение операций по дезинформации противника. В случае проведения операций по информационному воздействию на противника нередко используется криптография. С одной стороны, узнав о дешифровании своих секретных сообщений, можно не усиливать защиту, а продолжать использовать тот же шифр, передавая дезинформацию, которую другая сторона будет принимать за истинную информацию. Такая ситуация называется дезинформацией «под шифром». В этом случае для передачи настоящей информации следует использовать другие шифры и другие каналы связи. С другой стороны, тайно захватив шифры и ключи противника (или вскрыв их аналитическим путем), можно попытаться от имени истинного отправителя передать противнику дезинформацию.

Таким образом, агентурные радиостанции и эфирная дальняя связь с их помощью являются обоюдоострым оружием для корреспондентов, находящихся на передающей и принимающей сторонах. В военное, да и в мирное время передаваемое радиосообщение может содержать как исключительно ценную адресную информацию, так и ложную дезинформацию, приводящую впоследствии к трагическим результатам для того, кто не имеет средств для выявления истинного положения вещей в «информационной войне». Одним из наиболее надежных средств для решения двух главных задач практики: (1) сокрытие (защита от посторонних) смысла передаваемой информации; (2) установление подлинности (аутентификации) и истинных намерений корреспондента считается кодирование и шифрование сообщения, что требует применения криптографических методов и средств их реализации с привлечением как «ручных», так и «механических» технологий.

Во время Второй мировой войны больших успехов в дешифровании немецких и японских сообщений удалось добиться криптоаналитикам Англии и США. Появление компьютеров оказало большое влияние на криптографию с их помощью стали создаваться как стойкие алгоритмы шифрования, так и разрабатываться новые методы криптоанализа. Кстати первый в современном понимании компьютер был создан в о время Второй мировой войны в Англии для решения сложных криптографических задач. Использование этого устройства позволило добиться существенных успехов в дешифровании шифрмашины «Энигма» — одного из основных немецких шифраторов. Содержание последней главы книги показывает какие колоссальные человеческие и машинные ресурсы потребовались Англии и США для взлома германских шифрмашин. Напротив, в годы войны штат дешифровально-разведывательных служб СССР был достаточно небольшим. Однако они показали удивительную результативность и эффективность во взломе машинных и ручных шифров противника. Главные события Второй мировой

разумеется происходили на Советско-германском фронте.

В этой книге рассматривается противостояние советских криптографов с соответствующими специалистами Германии, Японии и их союзников. Советские люди героически сражались на земле, в небесах и на море. Криптографы вели свою войну в особом измерении — радиоэфире. В ходе войны советские дешифровальные службы предоставили политическому и военному руководству СССР большое количество важнейшей информации. Эта информация поступала во время всех важнейших сражений (в т. ч. битвы за Москву, Сталинградской битвы, сражения на Курской дуге и т. д.) и способствовала нашим победам. В то же время шифровальная служба не позволила противнику получить сведения о наших замыслах и действиях. Итак, рассмотрим криптографическую во время Великой Отечественной войны подробнее.

История техники защиты правительственной связи

Создание и развитие собственной шифровальной службы в СССР началось после окончания Гражданской войны. Так называемые «ручные» системы кодирования и шифрования не могли справиться со все возрастающими потоками информации по причине неизбежно низкой скорости её обработки. Кроме того, армейские и дипломатические службы Германии, Японии, США, России и других стран пользовались довольно простыми шифрами. Актуальность разработки механических и электромеханических машин для шифрования текстов, а также электрических шифраторов для радио и телефонных переговоров стала исключительно высокой.

В конце 1920-х годов в условиях жесткой централизации созрела острейшая необходимость создания эффективной системы управления страной и её самой главной составляющей — связи высшего партийного руководства. Особенность её состояла в том, что она должна была быть специально выделенной элитарной системой, обеспечивающей коммуникационную оперативность и конфиденциальность передаваемой информации[2].

До этого времени считалось, что использование защищенных переговорных пунктов (станций), отдельных аппаратных помещений, прямых проводов и ручных коммутаторов для телефонной связи даёт возможность…«главе государства оперативно решать по телефону вопросы государственной важности, сохраняя при этом секретный характер переговоров»[3]. Защита правительственной корреспонденции решалась посредством проволочного телеграфа с использованием предварительной криптографической обработки текстов. Право на разрешение предоставления прямых проводов являлось исключительной прерогативой наркома почт и телеграфов, а разрешение на право ведения переговоров оформлялось в виде мандата. Считалось также, что *автономия* — единственно приемлемая форма эксплуатация сети связи Кремля. К концу 1920-х годов длина телефонно-телеграфных проводов в стране приближалась к миллиону километров, а телефонная связь на большие расстояния стала возможной лишь благодаря применению промежуточных трансляционных усилителей, производство которых было освоено ленинградским заводом «Красная заря».

Первая отечественная одноканальная аппаратура высокочастотного телефонирования была разработана и изготовлена в 1926 году сотрудниками Ленинградской научно-испытательной станции под руководством П. А. Азбукина при участии Я. И. Великина и установлена на линии Ленинград — Бологое. В 1926 году под руководством В. Н. Листова была создана аппаратура, дающая возможность организовать три телефонных канала на воздушных цветных цепях. В 1930 году появилась постоянная линия ВЧ-связи от Москвы до Харькова через Тулу, Орел и Курск. В 1934 году станцию правительственной связи открыли в Киеве. Только за 1938 год было построено 32 станции правительственной ВЧ-связи. В конце 1920-х и первой половине 1930-х годов применение принципа ВЧ-телефонирования (переноса разговорного частотного спектра в область частот выше десяти или нескольких десятков килогерц*) считалось гарантом обеспечения конфиденциальности* ведущихся телефонных переговоров[4]. Недостаточная развитость радиотехнической