П. В. Генюш, А. Э. Барчук

СОВЕТСКАЯ И ГЕРМАНСКАЯ СИСТЕМЫ ШИФРОВАНИЯ: ОСОБЕННОСТИ И ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ В ГОДЫ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ

Раскрывается роль шифровальной связи как важнейшего фактора стратегического противостояния в годы Великой Отечественной войны. Показано, что эффективность отечественных шифровальных систем являлась одним из ключевых элементов обеспечения безопасности связи и управления войсками в военный период.

Великая Отечественная война стала не только битвой армий, но и противостоянием умов, развернувшимся в невидимом фронте – в сфере шифровальной связи. Информация превратилась в важнейший стратегический ресурс, а способность защитить свои секреты и раскрыть чужие нередко играла решающую роль в исходе масштабных операций.

Шифровальная машина «Энигма» является одним из наиболее известных символов криптографического противостояния Второй мировой войны. В вооружённых силах нацистской Германии для защиты оперативно-тактической связи использовалась её модификация, получившая официальное обозначение Wehrmacht Enigma («Энигма I»).

Конструкция «Энигмы I» базировалась на трёх роторах, каждый из которых представлял собой набор из 26 входных и 26 выходных контактов, соединённых внутри проводами. Выходные контакты предыдущего ротора соединялись с входными следующего. При нажатии клавиши ток последовательно проходил через три ротора, после чего поступал на неподвижный отражатель. Отражатель также представляет собой диск с проводами внутри, но его отличие от шифратора состоит в том, что он не вращается, а провода входят с одной стороны и затем выходят с той же стороны. Поступающий в отражатель сигнал идет обратно через те же три шифратора, но уже по другому пути. После этого на световом табло загоралась лампа, соответствующая зашифрованной букве [1].

Несмотря на кажущуюся неуязвимость шифровальной машины, она была взломана, и это обстоятельство сыграло ключевую роль в ходе войны. «Надежную машину» взломал польский математик Мариан Реевский. Уже через несколько месяцев польские специалисты создали шесть дешифрующих устройств, получивших наименование «Бомба». Впоследствии Алан Тьюринг взял за основу польскую идею и значительно усовершенствовал её, добавив метод поиска ключей. В итоге успешной дешифровки была получена большая часть разведывательной информации об авиационных налётах в период с 10 июля по 30 октября 1940 года в ходе «Битвы за Британию». Кроме того, были перехвачены приказы штаба Германа Геринга, касавшиеся подготовки люфтваффе к атаке на военно-воздушные базы Англии. Позднее, в 1943 году, британская разведка передала советскому командованию расшифрованные данные, раскрывавшие планы немецкой операции «Цитадель».

В арсенале германских криптографов существовали и другие средства защиты информации. Одним из них была система одноразовых шифроблокнотов, известная как шифр Вернама. Это простейший шифр на основе бинарной логики, который обладает абсолютной криптографической стойкостью [2]. Принцип действия шифра Вернама заключается в наложении на исходный текст случайного ключа той же длины посредством логической операции «исключающее ИЛИ». Для реализации этого метода обе стороны связи должны обладать идентичными блокнотами, страницы которых содержат уникальные ключи и подлежат уничтожению после однократного использования. Однако широкое применение данной системы сдерживалось логистическими сложностями: необходимостью безопасной передачи блокнотов и трудоемкостью ручной генерации случайных последовательностей.

Германские специалисты усовершенствовали шифр Вернама и на его основе была создана шифровальная машина «Лоренц», которая обеспечивала передачу в эфир или в проводные каналы закодированной информации в стандартном коде Baudot teleprinter code. Эта система считалась абсолютно надежной, пока операторы не допустили критическую ошибку: при повторной передаче длинного сообщения они не сменили настройки ключа. Это позволило перехватить два связанных шифротекста и восстановить принцип работы шифратора. Однако даже после раскрытия структуры расшифровка вручную занимала недели, из-за чего данные быстро устаревали. Проблему решило создание специализированной вычислительной техники. Первые электромеханические машины ускорили процесс, но лишь появление компьютера сократило время взлома с нескольких недель до нескольких часов.

Развитие машинного шифрования в СССР началось в межвоенный период, когда привычные ручные методы постепенно уступали место электромеханическим устройствам. Уже к концу 1920-х годов советские специалисты начали создавать аппараты для автоматизации шифрования и расшифровки, закладывая основы будущих высокозащищенных систем.

Одним из первых шагов стало усовершенствование методов временной перестановки сегментов речевого сигнала, предложенное М.А. Бонч-Бруевичем в 1920 году. Идея заключалась в систематическом перемещении частей сообщения по заранее определённым схемам, что значительно усложняло дешифровку при перехвате. В 1927–1928 годах в НИИС РККА были изготовлены первые аппараты секретного телефонирования для органов ОГПУ и пограничных войск. В

1930-е разработки велись сразу в нескольких организациях, что обеспечивало комплексное развитие криптографических технологий [3].

В 1931 году была создана отдельная сеть междугородной высокочастотной связи с аппаратами защиты сообщений, а в 1934 году завод «Красная Заря» начал серийное производство трёхканальной СМТ-34, обеспечивавшей качественную связь на расстоянии до 2000 км. В середине 1930-х создавались устройства автоматического засекречивания телефонных переговоров типа «ЕС». Эти аппараты применяли метод инверсии сигнала с добавлением мешающего тона, что существенно повышало уровень секретности [4].

Для текстовой информации был создан шифратор «В-4» с методом гаммирования: каждая буква текста заменялась числом и суммировалась с элементами ключевой последовательности (гаммы). В 1939–1940 годах «В-4» модернизировали в «Изумруд», а позже появились дисковые шифраторы К-37 «Кристалл», применявшиеся на оперативно-тактическом уровне и ускорявшие обработку шифротелеграмм при сохранении высокого уровня секретности. Шифромашины К-37 и «В-4» использовались в разных районах боевых действий, обеспечивая надёжную связь, снижая риск. К началу войны имелось более 150 комплектов К-37.

Особое значение защита каналов связи приобрела во время Сталинградской битвы, когда секретность сообщений напрямую влияла на исход боевых действий. Советские войска использовали шифраторы «В-4» и дисковые машины «К-37» для передачи приказов, разведданных и координат подразделений. Надёжность этих устройств позволяла фронтовому командованию быстро и безопасно направлять распоряжения между армиями без риска перехвата немецкими криптоаналитиками. Ключевую роль играли специалисты по криптоанализу, проверявшие уязвимости каналов связи и усиливавшие защиту, что обеспечивало конфиденциальность стратегических решений и повышало эффективность действий советских войск [5].

Под руководством В.А. Котельникова была создана система С-1 «Соболь», основанная на перестановке коротких временных отрезков и двухчастотной инверсии сигнала, управляемой генератором гаммы с частотой 10 раз в секунду. Аппаратура использовалась в действующей армии и для связи с Москвой во время переговоров о капитуляции Германии в мае 1945 года. За её создание Котельников и его команда были награждены Сталинскими премиями I степени.

В целом советская криптографическая система в годы Великой Отечественной войны представляла собой комплексный подход к защите информации. В то время как германская школа делала упор на математическую сложность одной машины, что оборачивалось уязвимостью при малейших ошибках операторов, советская система использовала эшелонированную организацию защиты. Эффективность этих систем, совместно с работой криптоаналитиков и разработчиков шифровальных машин, сыграла ключевую роль в обеспечении стратегического преимущества СССР.

Список литературы

1. Книга шифров: тайная история шифров и их расшифровки / Саймон Сингх ; пер. с англ. А. Галыгина. – М. : АСТ : Астрель, 2009. – 447 с.
2. Криптография Второй мировой войны [Электронный ресурс]. – Режим доступа: https://podcast.lib33.ru/kriptografiya-vtoroj-mirovoj-vojny. – Дата доступа: 25.03.2026
3. Ларин, Д. А. Этапы криптографической деятельности в России / Д. А. Ларин // История и архивы. – 2011. – № 13 (75). – С. 45-58.
4. Токарева, Н. Н. Об истории криптографии в России / Н. Н. Токарева // Прикладная дискретная математика. – 2011. – № 4 (18). – С. 98-107.
5. Ларин, Д. А. Защита информации и криптоанализ в СССР во время Сталинградской битвы / Д. А. Ларин // История и архивы. – 2012. – № 14 (94). – С. 11–28.

Генюш Полина Викторовна, студентка 1 курса ФИТУ БГУИР, pgenus2@gmail.com
Барчук Алина Эдуардовна, студентка 1 курса ФИТУ БГУИР
Научный руководитель: Галицкая Елена Михайловна, преподаватель