УДК 621.3

ЭЛЕКТРОМЕХАНИЧЕСКИЕ ШИФРОВАЛЬНЫЕ МАШИНКИ ВРЕМЁН ВТОРОЙ МИРОВОЙ ВОЙНЫ

Коротченков Е.С., Гук Т.А.
Научный руководитель – старший преподаватель Михальцевич Г.А.

Данная научно-познавательная работа направлена на ознакомление и изучение принципа работы шифровальных машин времен Второй мировой войны. Период между двумя мировыми войнами характеризуется, помимо всего прочего, интенсивными работами по разработке и последующему внедрению и использованию шифровальных машин всевозможных конструкций.

Немецко-фашистские войска в боевых действиях на суше и на море до определенного момента вполне успешно применяли машину «Энигма» («Enigme»). Японцы в ходе войны на Тихом океане использовали шифровальную машину, прозванную американцами «Пурпур». Сами американцы шифровали свои сообщения с помощью машины «SIGABA», а англичане применяли устройство под названием «Type X». СССР разработал шифровальную машину с роторным шифратором К-37 «Кристалл», а затем, в 1942 году на смену Кристаллу пришла не менее надёжная машина – М-101 «Изумруд». Эти машины оказали серьёзное влияние на ход и результат многих боевых операций.

Из них, как минимум для «SIGABA» и «Type X» «Энигма» является прототипом. «Энигма» – портативное устройство 20-х годов выпуска снаружи выглядело как чемодан, подобно обычным печатным машинкам того времени. Помимо стандартной клавиатуры и валиков, двигающих лист бумаги обычной пишущей машинки, в «Энигма» значительную часть пространства занимали электронная и механическая часть. Шифровальный механизм состоял из роторов шириной около 1 сантиметра, с вытесненными по их окружности буквами латинского алфавита; соответственно, их было 26, и они соответствовали 26 электрическим контактам. Контакты с обеих сторон барабана соединялись попарно случайным образом 26 проводами (перепайками), создававшими замену символов. Эти «случайно» выполненные соединения в каждом из роторов являлись долговременным секретным криптографическим ключом, возможность определения которого противником должна быть исключена. Роторы были связаны шестеренками. При нажатии клавиши один из роторов приходил в движение, другие тоже начинали вращаться, но с разными скоростями. Шифрование каждой буквы осуществлялась с помощью электрических импульсов, которые, проходя подряд через все роторы, отражались от рефлектора и выходили через зигзагообразные промежутки, получаемые разными положениями роторов по отношению друг к другу. Роторы касались друг друга подпружиненными контактами, которые и обеспечивали прохождение электрического тока сквозь весь пакет (существовали модели «Энигма» как с тремя, так и с четырьмя роторами). Результат шифрования фиксировался лампочкой, подсвечивающей соответствующую букву (рисунок 1) и записывался вручную на лист бумаги.

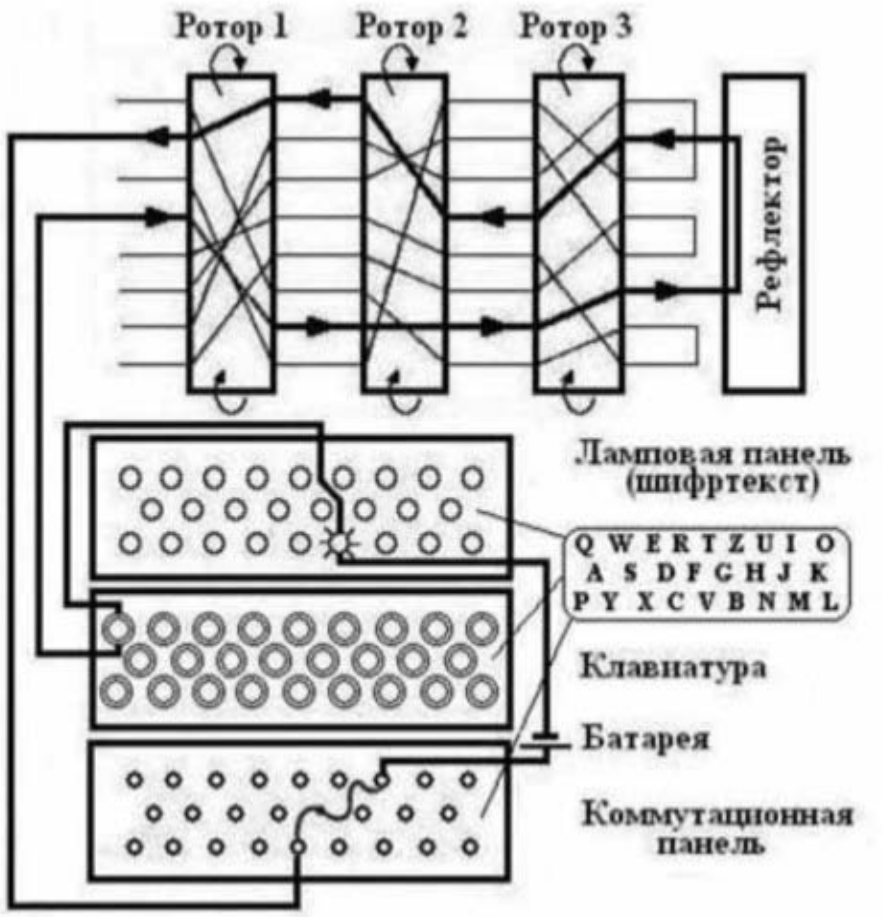

Рисунок 1 – Блок-схема 3-роторного» лампового шифратора «Энигма»

Ключ к шифру на определенный период, определялся первоначальным положением каждого ротора, которое легко менялось. Перед началом работы роторы поворачивались так, чтобы устанавливалось выбранное кодовое слово (пароль) из 3-х букв, а при нажатии клавиши и кодировании очередного символа правый ротор поворачивался на один шаг. После того как он делал полный оборот, на один шаг поворачивался следующий ротор – как в электросчетчике. Следовательно, получался ключ заведомо более длинный, чем текст сообщения. Такой механизм обеспечивал миллионы вариантов шифра простой замены, определяемого текущим положением роторов. Для затруднения дешифрования роторы периодически переставлялись местами или заменялись на другие роторы, имевшие отличающиеся перепайки внутренних соединений. Последующие усовершенствования машины состояли в смене линейного вращения роторов на более хаотичное вращение, и в увеличении их числа сначала до 4, а потом до 5, 6, 8-ми и более.

Минусов у такого способа шифрования было несколько, и одним из главных была невозможность шифрования какого-либо символа через самого себя.

Так же, как и «Энигма», английский аналог – «Type x» был роторной машиной. Но, в отличие от «Энигма», он состоял из пяти роторов, что на два-три больше чем в Энигме. Так же, как и в немецкой машинке, в «Type x» было возможным отправлять сигнал через роторы дважды, используя «отражатель» на

конце ротора. Так же, для повышения надёжности машины, электрический контакт был удвоен.

Из пяти роторов, как правило, первые два были фиксированными, что позволяло обеспечить дополнительное шифрование механизмов поворота ротора. Их назначение было подобно блокам в Энигме, они способны были осуществлять дополнительную рандомизацию с возможностью её регулирования, именно оттуда пошёл принцип «Random».

В отличие от «Энигмы» сообщения «Type x» нужно было напечатать, а зашифровка и передача происходили автоматически всего за один шаг, тогда как сообщения «Энигма» было необходимо написать, зашифровать, передать, получить, расшифровать и записать снова.

В японской шифровальной машине «PURPLE» вместо роторов применялись телефонные коммутаторы. Аппарат состоял из сложной хитроумной комбинации кабелей и контактной панели, что позволяло создать миллионы шифровальных комбинаций. При шифровании сообщения сначала нужно было установить выбранный ключ, а затем, с помощью клавиатуры электрической пишущей машинки ввести в шифровальную машину открытый текст. Текст обрабатывается различными электрическими и контактными устройствами, после чего на электрическом печатном устройстве распечатывалось уже закодированное сообщение.

Перед началом Второй мировой войны криптографические службы всех ведущих мировых держав были оснащены электромеханическими шифровальными машинами, которые имели относительно высокую для того времени скорость обработки информации, обеспечивали требуемую стойкость шифров и были весьма разнообразны. Одно время даже высказывалось мнение, что расшифровать криптограммы, создаваемые с помощью таких машин, невозможно. Однако в ходе войны это мнение было быстро опровергнуто.

Литература

1. Книга шифров. Тайная история шифров и их расшифровки / С. Сингх; – Астрель, 2007. – 72 с.

2. Страна Восходящего Солнца и ее шифровальные машины / [Электронный ресурс] – Режим доступа: https://habr.com/ru/company/ua-hosting/blog/385605/?fl=ru%2Cen. – Дата доступа: 19.03.2019

3. Enigma Simulator v7.0/ [Электронный ресурс] – CIPHER MACHINES AND CRYPTOLOGY. Режим доступа: http://users.telenet.be/d.rijmenants/en/enigmasim.htm. – Дата доступа: 21.03.2019