ИНФОРМАТИКА: СТРАНИЦЫ ИСТОРИИ

https://doi.org/10.29003/m1850.978-5-317-06529-4/469-474

Злобин Е.В.
Москва

Зачем был построен компьютер Колоссус (неизвестные страницы истории информатики)

Аннотация. В статье описано использование первого в мире компьютера Колоссус для взлома шифров верховного немецкого командования, включая Гитлера. Источником послужили уникальные мемуары взломщика кодов, работавшего в годы войны в центре дешифровки в Блечли-Парке. Ввиду абсолютной секретности проекта в течение 60 лет, воспоминания были написаны после его рассекречивания в начале 2000-х. Изданы после смерти автора.

Ключевые слова: История информатики, первый компьютер, шифрование, дешифровка, взлом шифров, Блечли-Парк.

Evgenii Zlobin
Moscow

Why was the Colossus computer built? (unknown pages of the history of computer science)

Abstract. In the article is described the use of the 1st world computer Colossus for the breaking of the ciphers of supreme German command, including Hitler. The unique Memoirs of the codebraker, who worked during the years of war in the center of decoding in the Bletchley Park, served as source. In view of the absolute secrecy of project in time of 60 years, Memoirs were written after project declassification in the early 2000s. Memoirs were published after author death.

Keywords: History of informatics, First computer, coding, decoding, codebracking, Bletchley Park.

Создание и использование англичанами в годы второй мировой войны первого в мире компьютера Колоссус (Colossus) – один из наиболее секретных британских проектов, сравнимых по степени закрытости пожалуй только с делом Гесса. Более полувека данные материалы оставались недоступны, и были окончательно рассекречены только в начале 2000-х годов. К этому времени оказалось, что в английских архивах материалов сохранилось немного – к примеру вся техническая документация на компьютер была уничтожена [1]. Значительно более полная коллекция документов отложилась в архивах ЦРУ [2], с её помощью энтузиасты воссоздали работающую модели этого уникального устройства, о которой мы уже писали [3].

В немногочисленных публикациях, которые вышли после первых упоминаний о Колоссусе еще до его полного рассекречивания и сразу после, приводятся сведения об устройстве компьютера, его элементной базе, и о главном предназначении – взломе шифров т.н. «Лоренца», шифровальной машины SZ42, использовавшйся в переписке верховного командования рейха во главе с Гитлером [4]. Однако до недавнего времени в публикациях обходился вопрос о том, а каким образом взламывались эти шифры, по каким алгоритмам работал и что именно считал первый в мире компьютер. Прежде чем коснуться этого вопроса, опишем кратко что из себя представлял, кем и как был взломан самый секретный немецкий шифратор.

SZ42, которых было изготовлено всего несколько сотен, использовал стандартную телетайпную 5-ти позиционную перфоленту как носитель текста, и шифр Вернама (Vernam) – к двоичному коду символа текста прибавлялись по модулю 2 коды двух случайных символов. При дешифровке эти же два символа снова прибавлялись по модулю два, и на выходе получался исходный текст. Полученная перфолента распечатывалась на стандартном буквопечатающем аппарате. Широкое применение данного шифратора началось в 1940 г.

Шифратор включал 3 группы дисков или роторов – всего их было 12 (для сравнения в другой взломанной англичанами шифровальной машине Энигма – 3 или 4) – пять «chi» (чи), два «моторных» и пять –«psi» (пси). Увеличение числа роторов больше чем в три раза по замыслу конструкторов обеспечивало потенциальную невзламываемость шифра. Однако «человеческий фактор» – ошибка оператора, передавшего в 1942 г. подряд два больших по объёму сообщения без смены установки роторов, позволил дешифровщикам получить статистически значимый объём текста для взлома структуры устройства. В течение 3 месяцев Билл Тат (Tutte), криптоаналитик из Блечли-Парка – самого секретного места Великобритании в годы войны, анализируя этот массив текста, сумел определить логическую структуру SZ42, которую англичане называли «Рыбой» (Fish) [5, p. 72–75]. Основываясь на его результатах был построен электромеханический эмулятор шифратора, получившая название «Тунец» (Tunny). Всего их было построено 15, все они были уничтожены после войны, один восстановлен после рассекречивания в 2011 г. [6] Меняя его установки штекерами на коммутационной панели, имитирующими изменения положение роторов, дешифровщики получили возможность просматривать результаты различных вариантов расшифровки.

По оценке генерала армии Дуайта Эйзенхауэра, верховного главнокомандующего экспедиционными силами союзников в Европе, а впоследствии президента США, взлом шифров криптоаналитиками из Блечли-Парка приблизил окончание войны как минимум на два года [5, p. 17]. Поразительным является тот факт, что до конца войны в руки союзников не попала ни одна шифровальная машина Лоренц, в отличие от Энигмы. Шифратор, который в настоящее время экспонируется в музее криптографии в Блечли-Парке, использовался фельдмаршалом Кессельрингом, командующим немецкими войсками в Италии. В конце войны его конвой при возвращении в Германию был перехвачен союзными силами в начале мая 1945 года, и перенаправлен в Блечли-Парк. И уже там, разбирая попавшие к ним трофеи, дешифровщики обнаружили шифратор Лоренца и смогли «вживую» увидеть то устройство, работающую модель которого они успешно создали на основе своих умозрительных заключений. И если сам шифратор – относительно небольшой и по размеру сопоставим с типичным буквопечатающим телеграфным аппаратом, то его английский аналог – стойка аппаратуры выше человеского роста.

Решаемые в ходе дешифровки первым компьютером практические задачи впервые были описаны в изданной в 2017 году книге воспоминаний другого взломщика кодов, капитана Джерри Робертса (Jerry Roberts) [5]. Свои записки он начал писать в 87 лет, после того, как появились первые публикации о Колоссусе и был официально рассекречен проект по взлому Лоренца (2002 г.). До этого на протяжении всего послевоенного периода, и об этом неоднократно упоминается в книге, он никогда и ни с кем, включая родителей и бывших сослуживцев, не обсуждал свою работу дешифровщика в силу секретности. Поскольку в этом почтенном возрасте он уже имел проблемы со зрением, то в основном надиктовывал текст, который затем практически не правился и не редактировался. В книге много повторов, используются разговорные выражения и пр. Поэтому в какой-то степени его мемуары можно отнести к т.н. «oral history». Автор скончался в марте 2014 года вскоре после завершения работы над книгой в возрасте 94 лет. Издание было подготовлено к печати его вдовой Мей. Робертс стал единственным из сотрудников дешифровальных подразделений Блечли-парка, кто написал книгу воспоминаний. И только он спустя полвека в 2012 году был награждён за взлом шифра Гитлера став кавалером (MBE – самая младшая степень) ордена Британской империи (для сравнения – одновременно с ним высшей степени ордена – рыцарской – был удостоен известный

велогонщик). Главная задача, которую Робертс перед собой ставил, принимаясь за мемуары – восстановление исторической справедливости, необходимость отдать должное английским дешифровщикам, внесшим существенный вклад в достижение победы над фашизмом.

Если верить его воспоминаниям, собственно взлом каждого сообщения включал 7 этапов, при этом компьютер выполнял первые два этапа. Как мы уже упоминали шифратор Лоренц включал 3 группы шифродисков или роторов (названия группам дал Тат) – пять «chi» (чи), два «моторных» и пять – «psi» (пси). Последовательность взлома шифровок с помощью Колоссуса была следующей. Первоначально исходный текст, записанный на стандартную бумажную ленту от телетайпа, считывался оптическим устройством и обрабатывался на компьютере в котором псевдослучайный ключ генерировался электронными схемами на тиратронах. Обработка шла параллельно на пяти счётчиках с суммарной скоростью считывания до 20000 символов в минуту. Методом простого перебора возможных комбинаций компьютер вычислял т.н. гамма-функцию, которая позволяла определить установку роторов первой группы – чироторов. При этом оператор, управляющий работой машины, с коммутационного пульта мог менять направления подсчёта функции.

После этого чи-роторы выставлялись в нужное положение на Тунце. Закодированное сообщение еще раз обрабатывалось на нём, и получался частично расшифрованный, т.н. де-чи текст. Дальнейшая работа производилась уже вручную, для чего, по воспоминаниям Робертса, ему надо было держать в памяти возможные 992 комбинации из 32 символов по 3 [5, p. 87]. Дешифровщики вычисляли положение двух оставшихся групп роторов, и после их установки на Тунце можно было получить полностью расшифрованное сообщение.

Использование компьютера для первичного взлома сделало возможным ускорить первичный взлом сообщений и позволило существенно убыстрить процедуру дешифровки, сократив её с недель и месяцев до дней и часов. С течением времени всё возрастающие объёмы обмена информацией в радиосетях немецкого командования потребовали постройки новых машин. К концу войны успешно функционировало уже 10 компьютеров, на них работали и их обслуживали 26 криптоаналитиков, 28 инженеров, 275 техников, которые работали круглосуточно в три смены заряжая и меняя бумажные ленты. Всего с помощью в том числе и этой команды, было перехвачено и расшифровано документов Верховного немецкого главного

командования объёмом 64 млн (!) символов, или около 35 000 машинописных страниц. Число перехваченных и расшифрованных сообщений составило по годам: 1942 – 872, 1943 – 3454, 1944 – 4724, 1945 – 4475, всего более 13 500. Основываясь на своих воспоминаниях, Робертс составил примерную таблицу вклада компьютерной расшифровки в общий объём выполненных работ [5, p. 119].

Таблица 1

Примерный вклад компьютера в расшифровку

Период	Условия дешифровки	Вклад Колоссуса
Май 1942 – середина 1943	7 этапов расшифровки, только вручную	100% вручную
Июль 1943 – февраль 1944	5 этапов расшифровки, 90% вручную	10% с помощью Колоссуса
Февраль 1944 – май 1945	5 этапов расшифровки, 75–80% вручную	20–25% с помощью Колоссуса
Всего	5 этапов расшифровки, 75–80% вручную	20–25% с помощью Колоссуса

Всего по расчётам Робертса вручную выполнено 78% работы, с помощью компьютера – 22%. Столь незначительная оценка вклада компьютерных технологий может обьясняться, во-первых, тем, что сам Робертс служил в конкурирущем подразделении названном по имени начальника, майора Ральфа Тестера (Ralph Tester), «Тестери» (Testery). Его служащие занимались только ручной дешифровкой. А Колоссус был построен и все действующие компьютеры эксплуатировались в подразделении Макса Ньюмана (Max Newman) – «Ньюменри» (Newmanry). Между этими подразделениями существовало определенная конкуренция в оценках их вклада в дело дешифровки. Строгий режим секретности внутри Блечли-Парка также не способствовал распространению лишней информации о происходящем буквально в соседней комнате. Во-вторых, спустя 60 лет речь может идти о самой приближеннойэкспертной оценке суммарного общего вклада в расшифровку сообщений, поскольку каких-либо отчётных документов не сохранилось, а память могла легко подвести ветерана. В то же время, сопоставляя процедуры ручной и машинной дешифровки, Робертс упоминает также о том, что он слышал якобы, что в конце войны компьютер смогли запрограммировать таким образом, что он полностью расшифровывал поступающие сообщения, но это, по его мнению, «highly unlikely» [5, p. 120].

Таким образом, с помощью первого в мире компьютера Колоссус производились вычисления, существенно убыстряющие взлом и дешифровку переписки немецкого верховного главнокомандования. Его использование позволило британским криптографам обеспечивать командование экспедиционными войсками союзников в Европе важнейшей информацией для принятия стратегических решений. Тем самым был внесён существенный вклад в обеспечение победы во Второй мировой войне.

Библиография

1. Account of the methods used for breaking German teleprinter cypher messages. Ref. HW 25/4. – The National Archives, UK.

2. Small A. W. Special Fish Report. National Archive and Records Administration. – RG 457, Historical Collection. – Box 1417. – Nr 4628 (1944); Campaigne H. Report on British Attack on “Fish”. National Archives and Records Administrations. – RG 457, NSA Historical Collection. – Box 457. – Nr. 1407 (1945).

3. Злобин Е.В. К истории информатики – как был утрачен и восстановлен первый в мире компьютер (казус Тони Сэйла) // Современные информационные технологии и ИТ-образование. Сборник научных трудов II Международной научной конференции и XII Международной научно-практической конференции. – М.: 2017. – С. 76–81.

4. Paul Gannon. Colossus. Bletchley Park’s Greatest Secret. – London: Atlantic Books, 2006. – 562; B.Jack Copeland and others. Colossus. The secrets of Bletchley Park’s Codebreaking Computers. – Oxford: University Press, 2006. – 462 p.

5. Captain Jerry Roberts. Lorenz. Breaking Hitler’s top secret code at Bletchley Park. – Brimscombe Port: The History Press, The Mill, 2017. – 240 p.

6. Codebreaking Tunny machine rebuilt for Bletchley Park. – URL: https://www.bbc.com/news/uk-england-beds-bucks-herts-13559856. (дата обращения: 25.08.2020).