

УДК 947

## **“БОМБА” ДЛЯ ГИТЛЕРОВСКОЙ ГЕРМАНИИ**

*Маштакова А.Ю., студентка 1 курса факультета ветеринарной медицины  
Научный руководитель - Войнатовская С.К., старший преподаватель  
ФГБОУ ВПО «Ульяновска ГСХА им. П.А. Столыпина»*

**Ключевые слова:** война, бомба, исход войны, Алан Тьюринг, компьютеры

*Работа посвящена известному криптографу Алану Тьюрингу, который создал дешифровальную машину, которая называлась «Бомба». Во время Второй мировой войны Машина Тьюринга позволила взломать шифровальную машину немцев «Энигма», код которой шифровал все сообщения фашистов. Это позволило выиграть войну раньше и спасти миллионы жизней.*

«Бомба» - электромеханическая машина, разработанная во время Второй мировой войны Аланом Тьюрингом и Гордоном Уэлчманом. Опираясь на доведенную работу легендарного польского криптографа Мариана Реевски, Тьюринг изобрел машину, сумевшую взломать код Энигмы, благодаря чему Блетчли-Парк превратился из загородного дома в огромный завод криптографии. Тьюринг также обязался за двадцать месяцев взломать надежную защиту шифра машины Энигма, на который полагались подводные лодки Северо-Атлантического флота. Тьюринг и его команда криптографов взломали сообщения, связывающие немецкие подводные лодки и их базы в июне 1941 года. Позже Черчилль - лидер Великобритании во время войны, признался: «Единственное, что действительно испугало меня в военное время- это угроза атаки подлодок соперника». Работа Тьюринга наконец дала надежду на предотвращение этой угрозы. Немецкие подводные лодки своими сообщениями раскрывали собственные позиции, благодаря чему появилась возможность перенаправить Британский флот и корабли союзников. Это был самый простой, но очень эффективный метод [1].

Позже Бомба была усилена, так называемым, плетением, изобретенным криптографом Гордоном Уэлчманом, что значительно сократило количество шагов, необходимых для взлома шифра. Вторая Бомба с диагональю Уэлчмана получила название «Агнус Ди», позже была переименована в более короткое «Агнесс» или «Агги». Первую машину «Победа» также оснастили диагональю Уэлчмана.

В ходе войны было построено более 200 Тьюриг-Уэлчманских «Бомб». Во избежание риска потерять эти машины во время бомбардировок их распределили между Блетчли-Парком и, так называемыми, базами в Уэвендоне, Адстоке, Гейхерсте, которые находились под управлением Женских Королевских морских сил и гражданской обороны [3].

Метод Тьюринга - один из трех великих вкладов в войну. Наряду с Бомбой и взломом сообщений шифровальной машины Энигма в Блетчли-Парке был создан систематический метод, позволивший взломать кодированные сообщения, создаваемые «Тунцом»- шифровальной машиной немцев. Тунец - хай-тек преемник Энигмы и гитлеровской «Блэкберри». Он был использован для шифрования секретных сообщений на самом высоком уровне. Основываясь на работе, проделанной в одиночку своим молчаливым другом Виллиамом Тутте, Тьюринг взломал систему Тунца. Использование метода Тьюринга позволило Блетчли-Парку читать секретные сообщения между берлинскими генералами и командующими армиям на фронте, а также разговоры, которые раскрыли военную стратегию Германии [2].

Могут ли историки подтвердить тот факт, что машины Тьюринга оказали влияние, решившее исход войны? Конечно, они не могут с большой уверенностью сказать, что Тьюринг сократил войну, в отличие, например, от атомной бомбы, которая очень хорошо иллюстрирует это влияние. Но в XXI веке мы можем, по крайней мере, подтвердить описание огромного вклада Тьюринга в войну за время службы в Блетчли-Парке, чего не могли сказать историки XX века в связи с соображениями о безопасности и засекреченности данных.

Изобретение Тьюринга было далеко от совершенства, но оно породило целую новую область исследований, которая получила название “Машины Тьюринга”. Сегодня мы называем их “Компьютеры”.

### **Библиографический список**

1. Bombe [Электронный ресурс]. – Режим доступа: <http://ru.wikipedia.org/?oldid=69789674>
2. Bombe - Crypto Museum [Электронный ресурс]. – Режим доступа: // Cryptomuseum. URL: <http://www.cryptomuseum.com/crypto/bombe>
3. How Different Would the World Be Today if Turing Had Not Broken the German-Codes? [Электронный ресурс]. – Режим доступа: <https://www.bigquestionsonline.com/content/how-different-would-world-be-today-if-turing-had-not-broken-german-codes>

## **THE BOMBE FOR HITLER'S GERMANY**

*Mashtakova A. Yu.*

**Key words:** *war, bombe, the outcome of the war, Alan Turing, computers*

*The study investigates the famous codebreaker Alan Turing, who invented a decoding machine called «The Bombe». During the Second World War Turing machine allowed to break German cipher machine Enigma, which ciphered all exchanges of fascist. This enabled to win the war earlier and save millions of lives.*