Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
Национальный исследовательский ядерный университет «МИФИ»
Саровский физико-технический институт – филиал НИЯУ МИФИ
Физико-технический факультет
Факультет информационный технологий и электроники
Кафедра философии и истории
XXIX студенческая конференция по гуманитарным и социальным наукам
XII студенческая онлайн-конференция по истории
«Ядерный университет и духовное наследие Сарова:
Великая Победа-75»
3,4 июня 2020 г.

Машина «Bombe» Алана Тьюринга и битва за Атлантику

Доклад:
студентов группы ПМ 19, ЭП 19
С. Кузяева (руководитель), В. Арсенова, В. Кароткина
Преподаватель:
кандидат исторических наук, доцент
О.В. Савченко

Саров-2020

Аннотация.

Наш доклад посвящён машине «Bombe», разработанной английским математиком Аланом Тьюрингом, которая помогала расшифровывать немецкие сообщения, закодированные машиной «Энигма».

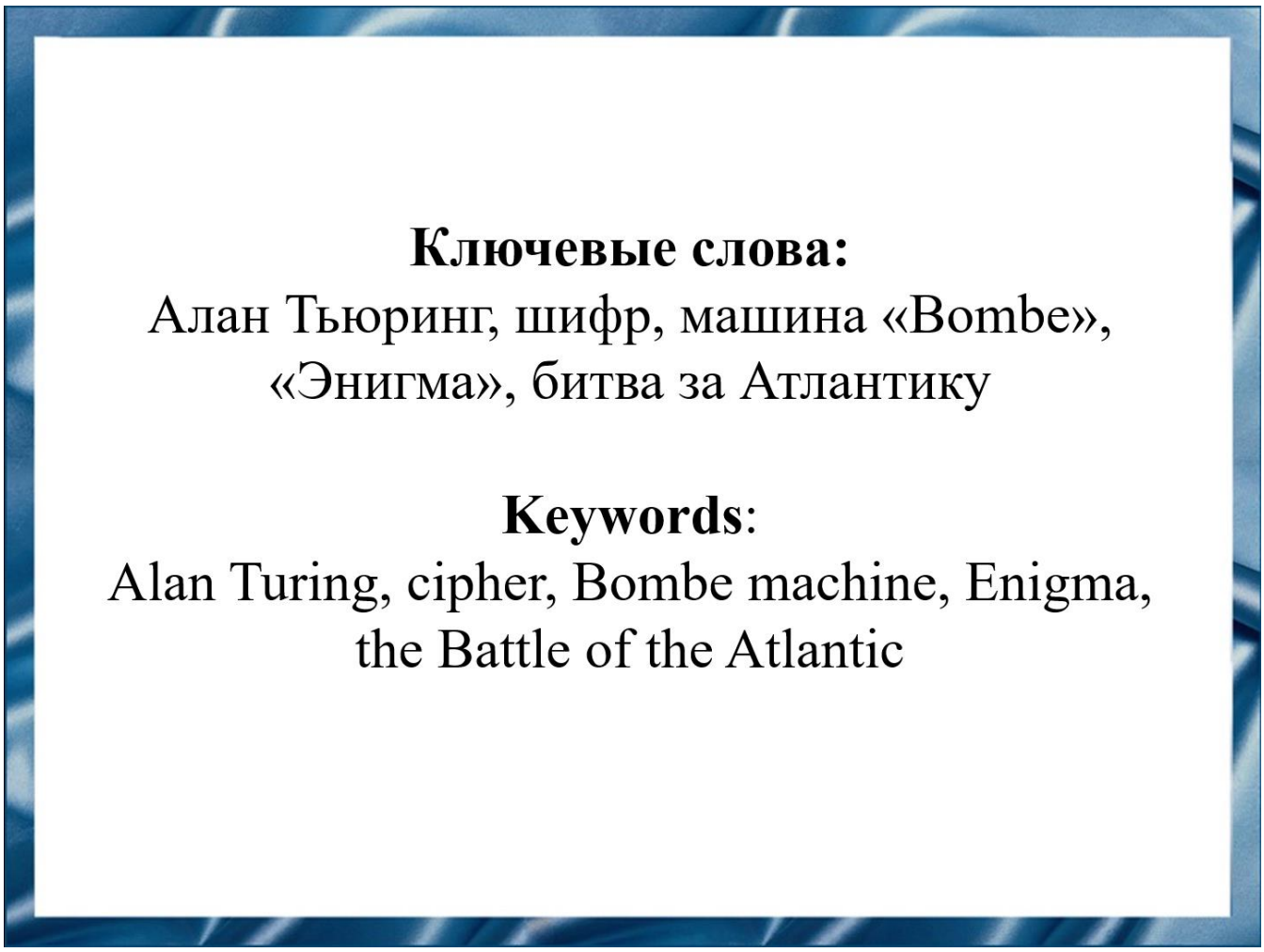
Во время Второй мировой войны в Англии для расшифровки сообщений, зашифрованных с помощью «Энигмы», была создана машина с кодовым названием «Turing Bombe», оказавшая значительную помощь антигитлеровской коалиции. Вся информация, полученная криптоанализом с её помощью, имела кодовое название «Ultra».

В нашем докладе показано применение информации, полученной при дешифровании немецких сообщений на примере битвы за Атлантику. Во время битвы за Атлантику нацисты использовали «Энигму» для передачи информации о предстоящих атаках немецких подводных лодок, главной целью которых было устранение конвоев Великобритании и кораблей антигитлеровской коалиции. Рассмотрены события, которые отражают результаты использования Великобританией машины «Bombe» Алана Тьюринга во Второй мировой войне.

Слайд 1.

Добрый день!

Мы представляем доклад о машине «Bombe» Алана Тьюринга, которая взломала нацистский шифр «Энигма» во время Второй мировой войны.

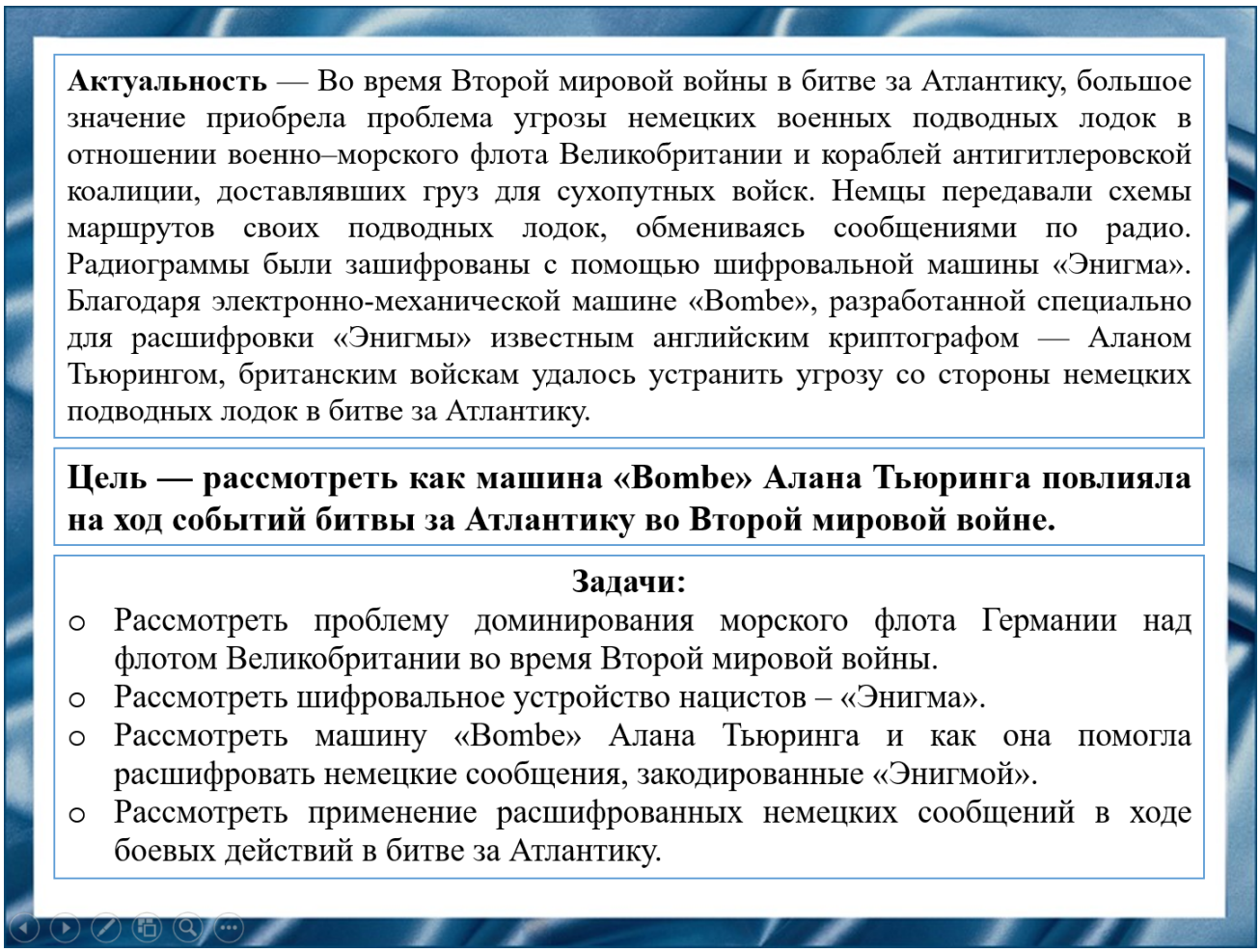


Слайд 2.

Во время Второй мировой войны в битве за Атлантику, большое значение приобрела проблема угрозы немецких военных подводных лодок в отношении военно–морского флота Великобритании и кораблей антигитлеровской коалиции, доставлявших груз для сухопутных войск.

Немцы передавали схемы маршрутов своих подводных лодок, обмениваясь сообщениями по радио. Радиограммы были зашифрованы с помощью шифровальной машины «Энигма».

Благодаря электронно-механической машине «Bombe», разработанной специально для расшифровки «Энигмы» известным английским криптографом — Аланом Тьюрингом, британским войскам удалось устранить угрозу со стороны немецких подводных лодок в битве за Атлантику.



Слайд 3.

Цель данной работы – рассмотреть как машина «Bombe» Алана Тьюринга повлияла на ход событий битвы за Атлантику во Второй мировой войне.

Слайд 4.

Боевые действия германских подводников в период Второй мировой войны представляют собой непрерывную цепь сражений практически на всех просторах мирового океана (от Ньюфаундленда до Австралии и от Арктики до мыса Доброй Надежды). Наиболее известным из этих сражений является Битва за Атлантику – боевые действия подводных лодок на атлантических коммуникациях в период 1939–1944 годов.

После войны премьер–министр Великобритании - Уинстон Черчилль признался на страницах своей книги «Вторая мировая война», что именно германские подводные лодки, а не асы Люфтваффе (германские военно-воздушные силы), были главной угрозой Великобритании.

Слайд 5.

Поначалу многие немецкие командиры старались следовать условиям Лондонского протокола 1936 года об ограничениях военно–морских вооружений, но вскоре командиры английских подводных лодок стали сообщать, что встреченные ими одиночные немецкие суда активно используют установленные на своих палубах артиллерийские орудия и немедленно передают в эфир особый сигнал при обнаружении английского судна.

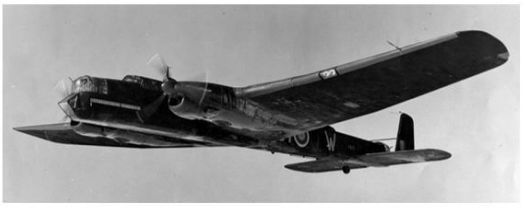
Задачей немецких подлодок было устранение английских конвоев - отрядов торговых судов, перевозивших стратегические грузы (главный путь, по которому двигались конвои, начинался в канадском порту Галифакс, проходил по Северной Атлантике и завершался в западных портах Великобритании). С сентября 1939 года и протяжении нескольких лет Англия теряла от немецких торпед на много больше судов (в первую очередь транспортных), чем могли построить ее верфи.

Слайд 6.

Справится с английскими конвоями нацистам позволяла тактика «Волчья стая», разработанная главнокомандующим немецким подводным флотом Карлом Дёницом. Имея приблизительные данные о маршруте движения конвоя, группа подлодок численностью 6—9 единиц рассредоточивалась веером на его пути. Командир, первым заметивший добычу, немедленно передавал в эфир радиограммы и ожидал, когда подтянутся остальные охотники.

Контрстратегия Великобритании

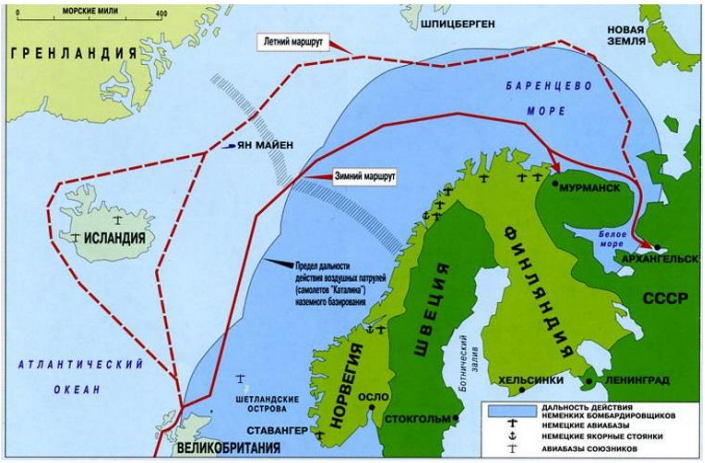
Для борьбы с немецкими подлодками англичанами с июля 1941 года была введена на северном маршруте от Ньюфаундленда до Великобритании система «сквозного конвоя». Вместе с этим флот США и авиация взяли на себя защиту коммуникаций, примыкающих к Исландии. Но со временем, потери союзников благодаря усовершенствованию системы противолодочной обороны, стали снижаться.



Британский “Armstrong Whitworth AW23”, снимок сделанный в мае 1940 г .

Британский “Short Sunderland”, патрулирующий прибрежную зону, 1941 г

Тем не менее, до октября 1942 года нацистам удалось потопить суда общим водоизмещением более 14 млн. рег. тонн. Тогда единственной надежной было попытаться расшифровать немецкие сообщения, взломав «Энигму».



Карта: Северный путь Арктических конвоев, доставлявшие в СССР грузы по ленд-лизу (государственная программа, по которой Соединенные Штаты Америки поставляли своим союзникам во Второй мировой войне боевые припасы, технику, продовольствие, медицинское оборудование и лекарства, стратегическое сырье, включая нефтепродукты) во время Второй мировой войны. Отправлялись из портов Англии и Шотландии. Проход конвоев сопровождался упорными боями британского и немецкого флотов

Слайд 7.

Стратегия «Волчья стая» помогла немцам за небольшие потери добиться успехов в подводной войне, прирастив тоннаж союзных потерь. Это стало толчком для англичан для создания контрстратегии, которая позволила бы снизить, а в дальнейшем и вовсе исключить наносимый Великобритании урон. В первую очередь англичане наладили прибрежное авиационное патрулирование, что заставило «волчьи стаи» перебраться дальше в океан.

Но несмотря на это, подводные немецкие лодки дальше продолжали топить корабль за кораблём и при этом могли уже не днями, а неделями преследовать своих жертв.

Слайд 8.

Решением проблемы нападения «волчьих стай» стало бы установление их место нахождения, а так как командование подводных лодок знало о том, что кто-то из “стаи” нашёл жертву, следовательно поддерживалась связь. Эта связь осуществлялась путём передачи сигналов по радио, зашифрованных машиной «Энигма», которая была установлена на каждом борту немецких подводных лодок.

Устройство этой шифровальной машины довольно простое. В один из ее отделов вводят незашифрованное сообщение. Пройдя через машину, под воздействием различных электрических импульсов оно превращается в зашифрованный текст и выводится из другого отдела машины. Ключом, который постоянно меняется, обладает другая «Энигма», принимающая сообщение. Через нее оно проходит в обратном направлении, и текст из зашифрованного превращается в обычный.

Слайд 9.

Ещё до начала Второй мировой войны союзник Великобритании - Польша, зная о об агрессивных намерениях немцев в отношении Польши стремилась вызнать больше о планах противника. Благодаря польским математикам под руководством Мариана Реевского, были определены механические процессы, происходящие в «Энигме» и создано устройство, получившее название «Криптологическая бомба».

Для этого потребовалось четыре года напряженной работы, помощь французских разведданных (в лице «купленного» Ганса-Тило Шмидта, из минобороны Германии, который «слил», пусть и устаревшие, коды трехроторной «Энигмы», которые позволили понять принципы шифрования).

Устройство поляков преуспело благодаря дефекту немецкого шифрования, который дважды шифровал первые три буквы в начале каждого сообщения, что позволило взломщикам кода искать необходимые шаблоны.

За тридцать семь дней до Второй мировой польские инженеры сделали союзникам Польши подарок – подарили по одной «Крипто-Бомбе». Французы не смогли воспользоваться подарком, зато англичане развернули на базе польского устройства целую программу противодействия «Энигме», с кодовым названием «Ультра»

К 1939 году немецкие шифровальщики обнаружили и устранили слабость двойного шифрования. Тогда британцам потребовалось более продвинутое решение, и к работе подключился Тьюринг и его команда.

Слайд 10.

Тьюринг Алан Матисон (1912-1954 гг.) – английский математик, логик, криптограф, оказавший существенное влияние на развитие информатики.

В годы Второй мировой войны Тьюринг Алан Матисон работал в британской Правительственной школе кодов, которая располагалась Блетчли – парке. В этой школе ученые трудились над поиском методов, позволяющих «взломать» шифры и коды, используемые странами нацистского блока. Математик возглавлял группу Hut 8, отвечающую за криптоанализ сообщений военно-морского флота нацистов.

Используя информацию, предоставленную поляками, Тьюринг начал взламывать сообщения «Энигма» с помощью своего собственного «компьютера». Его методы основывались на предположении, что в каждом сообщении содержится шпаргалка – известный фрагмент немецкого открытого текста в знакомом месте сообщения.

В одном примере это был прогноз погоды в Атлантике, который каждый день записывался в одном и том же формате. Оборудование для определения местоположения на прослушивающих станциях позволило взломщикам кода определить откуда исходит сообщение, и если оно совпадает с расположением метеостанции, вполне вероятно, что слово «wettervorhersage» будет присутствовать в каждом сообщении. Другой любопытной подсказкой была неспособность «Энигма» закодировать букву как саму себя.

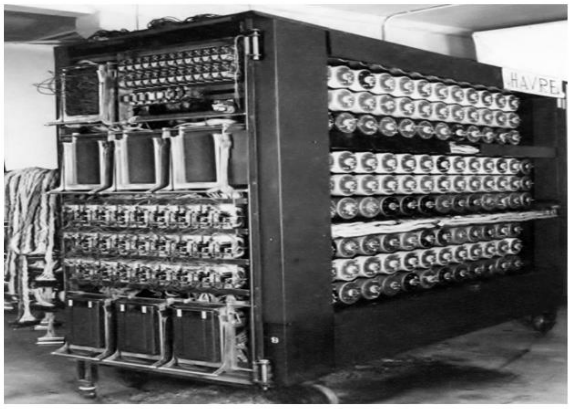
Машина «Bombe» Алана Тьюринга

Первая «Бомба» Алана Тьюринга была запущена 18 марта 1941 года.

Как и польский вариант, новая «Bombe» так же работала методом «переборки» всех возможных вариантов кода. «Бомба» помогала находить ежедневные настройки «Энигм», главным образом – позиции роторов, так как именно это определяло ключи шифра. Перебор ключей выполнялся за счет вращения механических барабанов. Для каждого возможного значения ключа, заданного положениями роторов, «Бомба» выполняла сверку с известным открытым текстом .

С помощью проверочной машины процесс повторялся до тех пор, пока не был найден правильный ответ. Это дало взломщикам часть ключа, но не весь. Затем приходилось использовать полученные знания и выяснить остальную часть ключа.

Гарольд Кин (1894 – 1973 гг .) — британским инженер, собрал механизм машины «Bombe» по чертежам Алана Тьюринга



Фотографии “Turing Bombe” : слева запечатлён вид машины снаружи , справа — вид машины внутри .

Слайд 11.

Получившийся механизм начал работать с марта 1940-го. Это бы агрегат длиной три метра, высотой два с небольшим метра и шириной чуть больше полуметра. Вес составлял около двух с половиной тонн. Сто восемь барабанов (соединенных по три и объединенные в три секции по двенадцать таких «строенных «барабанов) соответствовали ста восьми роторам «Enigma».

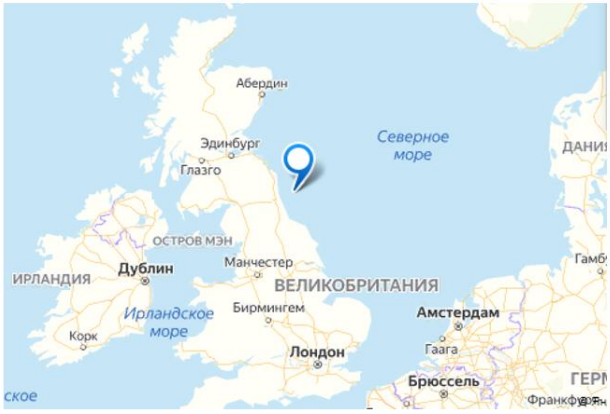
Роторы и барабаны имели одинаковую систему внутренних проводом, а рефлектор «Enigma» моделировался в «Bombe» простым дублированием контактов с проводами. Работал механизм так: верхний ряд барабанов вращался со скоростью сто двадцать об/м. После полного оборота поворачивался средний ряд, после оборота среднего – нижний. Такое вращение длилось до того, как будет получен сигнал «стоп» или, все барабаны не вернутся в начальное положение. Сигнал «стоп» машина выдавала в случае совпадения дешифрованного сообщения с шифрованным.

Первые сообщения, расшифрованные машиной “Bombe”

Фото: английские моряки поднимаются на палубу поврежденной немецкой подводной лодки U-559

Разгадать тайны морского варианта «Энигмы» помог случай. В октябре 1942 года в Восточном Средиземноморье английским морякам удалось подняться на палубу поврежденной немецкой подводной лодки U-559. Там они обнаружили шифровальные книги для морской версии «Энигмы». В результате в Блетчли Парк с помощью этой книги смогли читать все сообщения немецкого флота в северной Атлантике. И это произошло в то время, когда немецкие подводные лодки каждый месяц топили десятки кораблей союзников с жизненно необходимыми для Великобритании грузами.

Одним из примеров полученных сообщении было сообщение 1942 г. : **MWMSAICTAISOAWAI, которое расшифровали как : “Эсминец Ягуар "А" - в пункт точки 53 градуса 24 минуты северной широты и "А" в пункт 1 градус западной долготы, Хай Гитлер”,** расшифровав данное сообщение Британия отдала приказ корабельным составам конвоев с провизией подобрать курс, не проходящий через это местоположение, что позволило сохранить жизнь 500 людям находящимся на борту.



Место, координаты которого были указаны в расшифрованном сообщении, на карте .

Слайд 12

Благодаря информации, приобретенной с помощью машины «Bombe» стало возможным изменять курсы конвоев, а также пока противник был полностью уверен в надёжности своего «нерушимого» кода, разрабатывать дальнейшие стратегии против немецких действий. Одним из примеров полученных сообщении было сообщение, которое расшифровали как: «Эсминец Ягуар «А» -в пункт точки 53 градуса 24 минуты северной широты и «А» в пункт 1 градус западной долготы, Хай Гитлер», расшифровав данное сообщение Британия отдала приказ корабельным составам конвоев с провизией подобрать курс, не проходящий через это местоположение, что позволило сохранить жизнь 500 людям находящимся на борту.

Слайд 13.

Благодаря расшифрованным сообщениям, уже в марте 1941 года в Северной Атлантике в течение нескольких дней англичанам удалось потопить сразу 4 немецкие лодки, причем тремя из них командовали такие немецкие асы, как Гюнтер Прин (U-47), Йоахим Шепке (U-100) и Отто Кречмер (U-99). Лодки Шепке и Кречмера были потоплены в одну ночь эсминцами «Уокер» и «Ванок» при атаке английского конвоя HX-112.

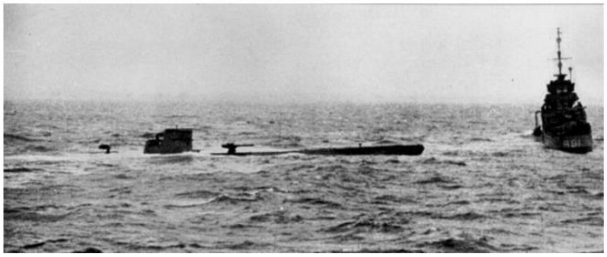
В мае 1941 г. командованием немецкого военно-морского флота была спланирована операция «Рейнские учения» (Rheinübung), согласно которой линкор «Бисмарк» (Bismarck) и тяжёлый крейсер (карманный линкор) «Принц Ойген» (Prinz Eugen) должны были совершить прорыв в Атлантику через Датский пролив, чтобы затем действовать на морских коммуникациях союзников и топить их торговые суда.

Таким образом, потеря лучших асов и такого количества лодок за короткий период нанесла серьезный урон Кригсмарине и уже точно положила конец «Счастливому времени» Германии.

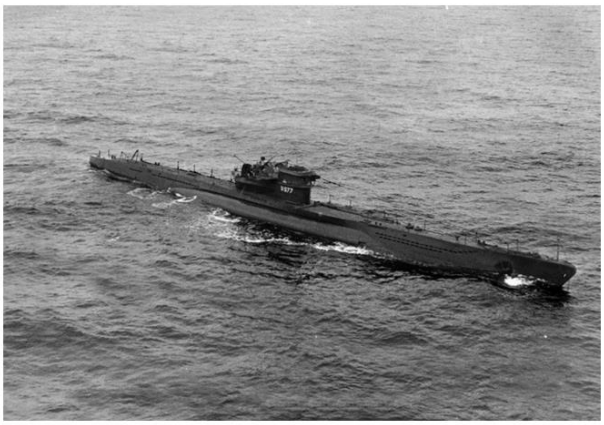
Многочисленные потери подводного флота Германии

1943 год принес Германии самые большие потери в Битве за Атлантику.

После капитуляции Германии 159 подводных лодок сдалось в плен. Остальные 203 были потоплены их командами. За пять с половиной лет войны Германия построила 1157 подводных лодок и захватила 15 иностранных. Немцы потеряли 789 подводных лодок. 500 из 632 подводных лодок, потопленных в море, было 428 уничтожено английскими кораблями и авиацией. Из общей суммы потерь союзников от подводных лодок 61% составляют суда, шедшие вне конвоев; 9% — отставшие от конвоев и только 30% — шедшие в составе конвоев.



Сдача немецкой подводной лодки U-110 в плен к англичанам, 9 мая 1943г.



Немецкая подлодка U-977, которая сдалась последней – в августе 1945 года.

С помощью машины “Bombe” англичане заранее узнавали о предстоящих атаках “волков” и передавали информацию союзникам. Самолеты союзников, оснащенные радиолокаторами, постоянно дежурили в Бискайском заливе. После обнаружения вражеских суден бетонные авиабомбы «Толлбой», запросто разрушали линкоры и подлодки.

Слайд 14

Узнав, о предстоящей атаки “волчьей стаи” с помощью машины «Bombe», флоту Великобритании удалось потопить 5 подводных лодок, в то же время ни одного судна потеряно не было. Одновременно немецкие подлодки атаковали английский конвой, где потеряли две лодки, также не добившись какого-либо результата.

В мае 1943 года Дёниц потерял 43 лодки - самые большие потери в битве за Атлантику, также 1943 год стал фактической точкой в Битве за Атлантику из которой англичане вышли победителями, а Дёниц был вынужден отозвать свои лодки.

Окончательная победа Великобритании в битве за Атлантику

Карл Дёниц
(1891 — 1980 гг.)
немецкий военный и государственный деятель, гроссадмирал .

Бетонная авиабомба "Толлбой"

Теперь «волки Дёница» все реже получали шанс для атаки конвоев и были озабочены проблемой собственного выживания. Германскому подводному флоту не помогали ни совершенные радиолокаторы, ни усиленное бронирование, не помогали и новые самонаводящиеся акустические торпеды, и зенитное вооружение. Положение усугублялось еще и тем, что противник уже давно имел возможность читать немецкие шифрограммы.

«Противник держит козырную карту, покрывает все районы с помощью дальней авиации и использует способы обнаружения, к которым мы не готовы. Противнику известны все наши секреты, а мы ничего не знаем об их секретах!» - писал Карл Дёниц.

К концу 1944 года немцы уже окончательно проиграли «Битву за Атлантику».

Слайд 15

Бесчисленные самолеты союзников, оснащенные радиолокаторами, постоянно дежурили в Бискайском заливе, который стал настоящим кладбищем немецких подлодок. Убежища из армированного бетона, стали уязвимыми после разработки англичанами 5-тонных бетонобойных авиабомб «Толлбой», превратились для подлодок в ловушки.

Теперь «волки Дёница» все реже получали шанс для атаки хорошо защищенных конвоев и все чаще были озабочены проблемой собственного выживания. Зачастую англо-американским эсминцам не хватало жертв, и они сворой гончих псов накидывались на любую обнаруженную подлодку, буквально засыпая ее глубинными бомбами. Такова, к примеру, была участь U-546, которую одновременно бомбили сразу восемь американских эсминцев. До недавнего времени грозный германский подводный флот не спасали ни

совершенные радиолокаторы, ни усиленное бронирование, не помогали и новые самонаводящиеся акустические торпеды, и зенитное вооружение.

Положение усугублялось еще и тем, что противник уже давно имел возможность читать немецкие шифрограммы. А ведь германское командование до самого конца войны пребывало в полной уверенности в том, что коды шифровальной машины «Энигма» взломать невозможно.

К концу 1944 года немцы уже окончательно проиграли «Битву за Атлантику».

Слайд 16.

«На протяжении всей войны битва в Атлантике являлась доминирующим фактором» – писал Уинстон Черчилль, поэтому чтобы более эффективней взламывать немецкие шифрограммы, было выпущено 210 бомб Тьюринга, которые могли дешифровать около трех тысяч немецких сообщений в день.

По окончании войны Черчилем был издан приказ по программе «Ultra» о полном уничтожении всех устройств Тьюринга. Все, что было связано с операцией «Ultra», десятилетиями оставалось под грифом секретности. Рассекречивание своей разновидности «Bombe» американскими властями началось только в 1974 году, несколько позже в этот процесс включилась и Англия. Образцы американского оборудования хорошо сохранились, а вот к оборудованию, которое работало в Блетчли-парке, судьба оказалась не так благосклонна. По какой-то причине его большая часть была уничтожена, и гриф секретности был снят намного позже. Сейчас в сохранившемся поместье Блетчли-парк можно увидеть восстановленные «Bombe».

Роль машины Тьюринга в победе Великобритании над Германии в битве за Атлантику

Успех команды Алана Тьюринга в разгадке сообщений «Энигмы» помог союзникам одержать победу в битве за Атлантику. Благодаря машине “Bombe”, существенно увеличилась скорость декодирования перехваченных немецких сообщений, что позволило силам Великобритании реагировать на секретные данные нацистов в течение нескольких часов и своевременно устранять угрозу со стороны немецких подводных лодок.

Связь была одним из важных звеньев победы.

Гибель линкора «Bismarck». 27 мая 1941 г.

Слайд 17.

В заключении, мы можем отметить, что своевременный перевод полученной информации немецких сообщений помогал командирам всех

рангов принимать правильные, взвешенные решения, что в результате помогало сохранять жизни огромному количеству людей, это можно точно проследить на примере незаметного обхода «волчьих стай» в Битве за Атлантику.

Победа над нацистской Германией – это заслуга участвующих войне стран «Антигитлеровской коалиции», находящихся в тылу и оккупации, и в частности, это победа совершенства системы точного расшифрования сообщений «Энигмы» с помощью машины Алана Тьюринга.

Данный случай в истории показал, как умение предвидеть действия противника нейтрализует грубую силу оружия.

Список литературы и источников

1. Бивор Э. Вторая мировая война. М., 2016.
2. Дёниц К. Немецкие подводные лодки во второй мировой войне. Пер. с нем. М., 1964.
3. Левин Р. Утра идет на войну: Секретная история. Лондон, 2001.
4. Морисон С.Э. Битва за Атлантику выиграна. Май 1943 - май 1945. Пер. с англ. М., 1959.
5. Роскилл С. Флот и война. Пер. с англ. М., 1967.
6. Тьюринг А.М. Вычислительные машины и разум. Пер. с англ. М., 2018.
7. Харрис Р. «Энигма». Пер. с англ. М., 2001.
8. Черчиль У. Вторая мировая война. Пер. с англ. М., 1997.
9. Эббинхауз Г. Машины Тьюринга и рекурсивные функции. Пер. с нем. М., 1972.
10. «Энигма», или как разгадывались тайны Третьего Рейха. // https://clck.ru/MKG8N

Слайд 18.

Наш доклад основывается на данных источниках и литературе.

Слайд 19.

Спасибо за внимание!

Резюме для СМИ.

В нашем докладе рассмотрена Машина «Bombe», разработанная британским математиком Аланом Тьюрингом, и её значение для победы в битве за Атлантику во время Второй мировой войны. Изобретение Тьюринга помогло взломать немецкие сообщения, закодированные легендарной машиной «Энигма».

Устройство Алана Тьюринга существенно увеличило скорость декодирования перехваченных немецких сообщений. Это позволило силам Великобритании реагировать на секретные данные в течение нескольких часов.

Благодаря расшифрованным сообщениям, британские войска могли предугадать атаки нацистов и устранять угрозу со стороны немецких подводных лодок.