Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

Восточно–Сибирский государственный университет технологий и управления

(ФГБОУ ВСГУТУ)

Электротехнический факультет

Кафедра «Системы Информатики»

Дисциплина

«Основы программирования»

Отчет по лабораторной работе №2

На тему:

Ветвление и условные операторы

Вариант3

|  |  |
| --- | --- |
| Выполнил: | студент гр. Б661–2 |
|  | Коковихин А.В. |
| Проверил: | преподаватель  Жамбалов Э.Б. |

Улан–Удэ

2021

Введение

Алан Тьюринг, весьма, известное имя в IT индустрии. Сразу вспоминается и «Машина Тьюринга», «Тест Тьюринга» и, наверное, «Рой Тьюринга». И мне стало весьма интересно узнать, кто же этот самый Тьюринг, и почему его именем названо столько изобретений и технологий.

Так же хотелось бы по подробнее изучить все связанные с Тьюрингом технологии, и слегка погрузится в историю изобретения ЭВМ. Ведь даже ноутбук, который я использую для написания этого реферата результат трудов Тьюринга. И пусть его строение мне уже более–менее понятно, но всю равно некое присутствие чего–то магического ощущается, а теперь представите рой самовоспроизводящихся дронов, покоряющий вселенную.

## Биография Алана Тьюринга

Алан Матисон Тьюринг родился 23 июня 1912 года в Лондоне в семье колониального чиновника, служившего в Индии. Его родители – Юлиус Мэтисон Тьюринг и Этель Сара Стоуни познакомились и обвенчались в Индии.

Алан Тьюринг учился в престижной Шерборнской школе (Sherborne Public School) в Англии, где проявил незаурядные способности к математике и химии, затем в 1931 году поступил в Кингз–колледж (King's College) Кембриджского университета.

В 1935 году он защитил диссертацию «Центральная предельная теорема теории вероятности» (которую он самостоятельно пере открыл, не зная об аналогичной предшествующей работе) и был избран членом Научного общества колледжа. В этом же году он впервые начал работать в области математической логики и проводить исследования, которые уже через год привели к выдающимся результатам.

В своей работе «О вычислимых числах, с приложением к проблеме разрешимости» (On the Computable Numbers, with an Application to the Entscheidungsproblem, 1936) Тьюринг ввел математическое понятие абстрактного эквивалента алгоритма, или вычислимой функции, получившее затем название «машины Тьюринга». Это был проект устройства, имеющего все основные свойства современной информационной системы: программное управление, память и пошаговый способ действий.

«Машина Тьюринга» открыла дискуссию по теории автоматов и создала теоретическую базу для работы цифровых компьютеров, которые появились в 1940–е годы.

Тьюринг продолжил учебу в США – в Принстонском университете, где под руководством американского математика и логика Алонзо Чёрча в 1938 году получил степень доктора философии. Затем он вернулся в Великобританию и получил стипендию Кингз–колледжа для занятий логикой и теорией чисел.

В это же время началось его конфиденциальное сотрудничество с правительственной Школой кодов и шифров (Government Code and Cypher School) в Блечли–Парке, где он еще до войны участвовал в работах по раскрытию немецких шифров.

В 1939 году британское военное ведомство поставило перед Тьюрингом задачу разгадать секрет «Энигмы» – специального устройства, использовавшегося для шифровки радиограмм в германском военно–морском флоте и в «люфтваффе». Британская разведка раздобыла это устройство, но расшифровывать перехваченные радиограммы немцев не удавалось. Тьюринг пригласил в созданный им отдел нескольких друзей–шахматистов. Уже через полгода было разработано устройство, названное им «Бомбой», которое позволяло читать практически все сообщения «люфтваффе». А спустя ещё год был «взломан» и более сложный вариант «Энигмы», использовавшийся нацистскими подводниками. Это во многом предопределило военные успехи британского флота.

Тьюринг занимался также разработкой шифров для переписки премьер–министра Великобритании Уинстона Черчилля и президента США Франклина Рузвельта, проведя период с ноября 1942 года по март 1943 года в США.

Заслуги Алана Тьюринга были по достоинству оценены: после разгрома Германии он был удостоен звания кавалера Ордена Британской империи 4–й степени.

В 1945 году Тьюринг был принят в Национальную физическую лабораторию в Лондоне, где возглавил разработку большого автоматического вычислительного устройства АСЕ (Automatic Computing Engine).

Разработанные в 1947 году Тьюрингом «Сокращенные кодовые инструкции» (Abbreviated Code Instructions) положили начало созданию, исследованию и практическому использованию языков программирования.

В 1948 году ученый был назначен заместителем Макса Ньюмена, директора вычислительной лаборатории Манчестерского университета, где создавался компьютер с самой большой по тому времени памятью – манчестерская автоматическая цифровая машина, или «Мадам» (Manchester Automatic Digital Machine), как ее называли в прессе. Тьюринг написал для нее несколько программ, пользуясь буквенно-цифровым кодом.

Тьюринг считается основоположником не только вычислительной техники, но также и искусственного интеллекта. Исключительную роль в развитии этого исследовательского направления сыграла небольшая статья «Вычислительные машины и разум» (Computing Machinery and Intellegence), опубликованная в журнале Mind в 1950 году и впоследствии многократно перепечатываемая, в которой Тьюринг предложил ставший знаменитым мысленный эксперимент (тест Тьюринга) – операциональный способ решения вопроса «мыслит ли машина?».

В 1951 году Алан Тьюринг стал членом Королевского научного общества.

В конце жизни он занялся вопросами биологии, а именно, разработкой химической теории морфогенеза. Эта работа осталась незаконченной. Предварительный доклад 1952 года и отчет, который появился уже после его смерти, описывают только первые наброски этой теории.

В 1952 году Тьюринг попал под суд по обвинению в нетрадиционной сексуальной ориентации. Вскоре скандал стал достоянием публики, ученый подвергся осуждению и потерял право работать в области криптографии.

8 июня 1954 года Тьюринг был найден мертвым в своем доме в Уилмслоу близ Манчестера. Смерть наступила 7 июня от отравления цианидом и была признана самоубийством.

В честь Алана Тьюринга Ассоциация по вычислительной технике (Association for Computing Machnery, АСМ) учредила премию его имени. Первым лауреатом премии Тьюринга в 1966 году стал Алан Перлис, один из создателей языка программирования Алгол, первый президент АСМ.

# Достижения

## Машина Тьюринга

В 1936 г. Аланом Тьюрингом для уточнения понятия алгоритма был предложен абстрактный универсальный исполнитель. Его абстрактность заключается в том, что он представляет собой логическую вычислительную конструкцию, а не реальную вычислительную машину. Термин «универсальный исполнитель» говорит о том, что данный исполнитель может имитировать любой другой исполнитель. Например, операции, которые выполняют реальные вычислительные машины можно имитировать на универсальном исполнителе. В последствие, придуманная Тьюрингом вычислительная конструкция была названа машиной Тьюринга.

Кроме того, предполагается, что универсальный исполнитель должен уметь доказывать существование или отсутствие алгоритма для той или иной задачи.

Машина Тьюринга состоит из бесконечной в обе стороны ленты, разделенной на ячейки, и автомата (головки), которая управляется программой.

Программы для машин Тьюринга записываются в виде таблицы, где первые столбец и строка содержат буквы внешнего алфавита и возможные внутренние состояния автомата (внутренний алфавит). Содержимое таблицы представляет собой команды для машины Тьюринга. Буква, которую считывает головка в ячейке (над которой она находится в данный момент), и внутренне состояние головки определяют, какую команду нужно выполнить. Команда определяется пересечением символов внешнего и внутреннего алфавитов в таблице.

Чтобы задать конкретную машину Тьюринга, требуется описать для нее следующие составляющие:

* Внешний алфавит. Конечное множество (например, А), элементы которого называются буквами (символами). Одна из букв этого алфавита (например, а0) должна представлять собой пустой символ.
* Внутренний алфавит. Конечное множество состояний головки (автомата). Одно из состояний (например, q1) должно быть начальным (запускающим программу). Еще одно из состояний (q0) должно быть конечным (завершающим программу) – состояние останова.
* Таблица переходов. Описание поведения автомата (головки) в зависимости от состояния и считанного символа.

Автомат машины Тьюринга в процессе своей работы может выполнять следующие действия:

* Записывать символ внешнего алфавита в ячейку (в том числе и пустой), заменяя находившийся в ней (в том числе и пустой).
* Передвигаться на одну ячейку влево или вправо.
* Менять свое внутреннее состояние.

Одна команда для машины Тьюринга как раз и представляет собой конкретную комбинацию этих трех составляющих: указаний, какой символ записать в ячейку (над которой стоит автомат), куда передвинуться и в какое состояние перейти. Хотя команда может содержать и не все составляющие (например, не менять символ, не передвигаться или не менять внутреннего состояния).

## Тест Тьюринга

К 1956 году британские учёные уже на протяжении 10 лет исследовали «машинный интеллект». Этот вопрос был обычным предметом для обсуждения среди членов «Ratio Club» – неформальной группы британских кибернетиков и исследователей в области электроники, в которой состоял и Алан Тьюринг, в честь которого был назван тест.

Тьюринг в особенности занимался проблемой машинного интеллекта, по меньшей мере, с 1941 года. Одно из самых первых его упоминаний о «компьютерном интеллекте» было сделано в 1947 году. В докладе «Интеллектуальные машины» Тьюринг исследовал вопрос, может ли машина обнаруживать разумное поведение, и в рамках этого исследования предложил то, что может считаться предтечей его дальнейших исследований: «Нетрудно разработать машину, которая будет неплохо играть в шахматы. Теперь возьмем трёх человек – субъектов эксперимента. А, В и С. Пусть А и С неважно играют в шахматы, а В – оператор машины. Используются две комнаты, а также некоторый механизм для передачи сообщений о ходах. Участник С играет или с А, или с машиной. Участник С может затрудниться ответить, с кем он играет».

Таким образом, к моменту публикации в 1950 году статьи «Вычислительные машины и разум», Тьюринг уже на протяжении многих лет рассматривал возможность существования искусственного интеллекта. Тем не менее данная статья стала первой статьёй Тьюринга, в которой рассматривалось исключительно это понятие.

Тьюринг начинает свою статью утверждением: «Я предлагаю рассмотреть вопрос: «Могут ли машины думать?». Он подчёркивает, что традиционный подход к этому вопросу состоит в том, чтобы сначала определить понятия «машина» и «интеллект». Тьюринг, однако, выбрал другой путь; вместо этого он заменил исходный вопрос другим, «который тесно связан с исходным и формулируется относительно недвусмысленно». По существу, он предлагает заменить вопрос «Думают ли машины?» вопросом «Могут ли машины делать то, что можем делать мы (как мыслящие создания)?». Преимуществом нового вопроса, как утверждает Тьюринг, является то, что он проводит «чёткую границу между физическими и интеллектуальными возможностями человека».

Чтобы продемонстрировать этот подход, Тьюринг предлагает тест, придуманный по аналогии с игрой для вечеринок «Imitation game» – имитационная игра. В этой игре мужчина и женщина направляются в разные комнаты, а гости пытаются различить их, задавая им серию письменных вопросов и читая напечатанные на машинке ответы на них. По правилам игры и мужчина, и женщина пытаются убедить гостей, что все наоборот. Тьюринг предлагает переделать игру следующим образом: "Теперь зададим вопрос, что случится, если в этой игре роль А будет исполнять машина? Будет ли задающий вопросы ошибаться так же часто, как если бы он играл с мужчиной и женщиной? Эти вопросы заменяют собой исходный «Может ли машина думать?».

## «Colossus»

Компьютер «Colossus» создавался для вскрытия шифрованной иностранной переписки, и сам факт его существования более полувека оставался тайной. Эта машина была для своего времени бесспорным чудом, но долгое время о ней знали лишь по слухам и фрагментарным воспоминаниям людей, так или иначе соприкасавшихся с важной тайной Второй мировой войны.

История британского «Колоссуса» началась в первые месяцы 1940 года, когда спецгруппа английской полиции, прослушивавшая радиоэфир для поиска германских шпионов на территории острова, случайно отловила шифрованную немецкую радиопередачу необычного вида. Материал радиоперехвата был отправлен крипто-аналитикам службы GC&CS (Government Code and Cypher School – «Правительственная школа кодов и шифров») в Блечли-Парк, где им чрезвычайно заинтересовались, поскольку он был передан не привычным в ту пору кодом Морзе, характерным и для криптограмм «Энигмы», а телеграфным кодом Бодо. Новая криптосистема противника получила у английских криптографов условное наименование «Рыба» (FISH). Рыбными терминами – «лещ», «макрель», «селедка» – будут названы и перехватываемые линии связи.

Специально под криптосистему FISH в Блечли-Парк было создано отдельное подразделение. Первые полтора года криптоанализ продвигался чрезвычайно тяжело, но 30 августа 1941 года один из германских шифровальщиков совершил чудовищную ошибку. В ответ на просьбу повторить сообщение он еще раз передал длинную (около 4000 знаков) шифр-телеграмму на том же ключе, да еще по лени слегка сократил исходный текст. В руках англичан оказались обе радиопередачи, что позволило им не только полностью дешифровать этот комплект и прочесть текст телеграммы, но и получить очень важную информацию – длинную шифрующую последовательность, генерируемую шифратором. Кроме того, было известно, что в начале каждой шифр-телеграммы немцы дают специфическую последовательность из 12 знаков, поэтому предположили: крипто схема неизвестного шифратора построена на основе 12 шифрующих колес. На основе шифр-колец с шестернями движения разного периода были устроены практически все известные в ту пору шифраторы, включая и немецкие. Вскрытая по комплекту шифр-последовательность давала надежду на полное восстановление логики работы аппарата FISH.

Успех сопутствовал одному из молодых криптографов-математиков GC&CS, Биллу Туту, аккуратно расписавшему пять дорожек вскрытой шифр-последовательности на больших разлинованных листах бумаги – в те времена все подсчеты и поиск повторений крипто-аналитикам приходилось делать исключительно вручную. В одной из дорожек, то есть в череде «точек» и «крестов» (нули и единицы тогда еще не использовали), тот сумел выявить характерные признаки двух шифрующих колес. Развив этот успех, англичане за несколько месяцев сумели взломать шифр-систему, установить общую схему устройства шифратора (см. врезку «Рыба по имени Lorenz SZ») и убедиться, что в принципе переписку такого типа можно вскрывать и читать. Правда, путем чрезвычайно трудоемких вычислений, требовавших до нескольких недель ручного труда на обработку одной телеграммы.

Для того чтобы дешифровать сообщение, аналитикам нужно было решить две главные задачи. Во-первых, «вскрыть колеса», то есть установить точное расположение рабочих и нерабочих штифтов на каждом из 12 шифрующих дисков. Конкретные комбинации штифтов устанавливались в FISH на определенный интервал дат, в течение которого не изменялись и использовались для шифрования всех сообщений, проходящих по данной линии связи. Вторая задача – найти начальное положение («установки») дисков, использованное для конкретной телеграммы. Каждое секретное сообщение зашифровывалось немцами при новых установках, поэтому эта задача решалась лишь после того, как были вычислены штифтовые комбинации на всех дисках.

В Блечли-Парк очень хорошо понимали, что вскрывать такой шифр вручную совершенно неэффективно, ибо за недели кропотливых вычислений утрачивается оперативная ценность столь тяжело добытой информации. Поэтому для автоматизации работ было создано специальное подразделение, получившее шутливое название «Ньюменарий» в честь возглавившего его известного английского математика Макса Ньюмена. Именно здесь чуть позже и родится новаторская идея о большом электронном компьютере, однако появится он далеко не сразу.

Первым проектом по автоматизации дешифрования была опто-механическая специализированная машина-компаратор (сравнивающее устройство) Heath Robinson, названная по имени популярного в довоенных комиксах персонажа-изобретателя странных механизмов. «Робинсон» использовали, но не слишком успешно, для решения задачи о начальных установках колес. Главная проблема была в точной синхронизации двух перфолент, одна из которых содержала германское шифрованное сообщение, а на второй были набиты циклически повторяющиеся последовательности битов, порождаемые штифтовыми комбинациями вскрытых дисков шифратора. Опто-механический считыватель позволял обрабатывать пару перфолент с довольно высокой скоростью – свыше 1000 знаков в секунду – однако перфо-ленточная бумага растягивалась, приводя к сбоям синхронизации и ошибкам в вычислениях. Компьютер Colossus полностью решил эту проблему, поскольку в нем работа дисков шифратора воспроизводилась чисто электронными методами, с помощью ламповых схем. Так что на вводе в устройство осталась лишь одна перфолента с шифр-текстом телеграммы, которая теперь считывалась намного быстрее, со скоростью 5000 знаков (или 12 метров) в секунду, а подсчеты при этом стали значительно надежнее.

Полностью моделировать работу шифратора внутри компьютера, используя ламповые схемы с быстрым временем переключения, предложил инженер-электронщик Томми Флауэрс – сотрудник британского Министерства почт, которого привлекли для помощи крипто-аналитикам. В те времена за механизацию всех государственных коммуникаций отвечал Исследовательский центр министерства почт Dollis Hill в Северном Лондоне, и именно там в период с февраля по декабрь 1943 года Флауэрс и его коллеги построили небывалую по масштабам машину Mark I Colossus, содержавшую в своих схемах около 1500 электронных ламп. В канун Нового года готовый компьютер разобрали и перенесли в Блечли-Парк, где с февраля 1944 года Colossus начал на постоянной основе вскрывать шифро-переписку высшего эшелона германского военного командования. Благодаря надежному и быстродействующему электронному компьютеру время вскрытия телеграмм сократилось с нескольких недель до 2−3 часов. Воодушевленные столь грандиозным успехом англичане в течение 1944 года создали еще более продвинутую версию компьютера под названием Colossus Mark II. Он был примерно в пять раз быстрее своего предшественника, содержал около 2500 электронных ламп и предоставлял возможности программирования. На этом основании Colossus II в целом ряде работ расценивается ныне как первый в мире электронный программируемый компьютер. До конца войны было построено в общей сложности 10 таких машин.

Главный конструктор «Колоссов» Томми Флауэрс, хорошо знавший особенности работы электронных ламп, с самого начала предупреждал, что такие машины лучше вообще не выключать, обеспечив надлежащее охлаждение электроники (чаще всего лампы отказывали и «перегорали» в моменты включения/выключения). Уже первые дни эксплуатации машины полностью подтвердили правоту инженера, так что все компьютеры Colossus, однажды включенные, уже не выключались вплоть до Дня победы.

В общей сложности с помощью «Колоссов» было дешифровано свыше 63 миллионов знаков телеграмм немецкого верховного командования, которые «поставляли» примерно 550 сотрудников (точнее, в большинстве своем сотрудниц) Блечли-Парк плюс, конечно же, службы радиоперехвата.

C приходом мая 1945 года звезда компьютеров Colossus, увы, стремительно закатилась. Машины-гиганты, каждая из которых представляла собой комплекс из 8 крупных двухсторонних монтажных стоек разной ширины, высотой по 2,3 метра и суммарной длиной около 5,5 метра, были слишком специализированы под конкретную задачу. А высшее политическое руководство Великобритании слишком озабочено, чтобы Сталин и быстро формировавшийся вокруг СССР блок просоветских государств ничего не узнали о мощных дешифровальных возможностях недавнего союзника. Уинстон Черчилль лично дал указание, чтобы «Колоссов» разобрали на части размерами «не больше руки человека». Восемь из десяти машин были полностью демонтированы уже в том же 1945 году.

Два последних компьютера сначала перевезли в Лондон, а затем в город Челтнем, где разместилась (и базируется по сию пору) преемница GC&CS, криптографическая спецслужба Великобритании GCHQ, или Штаб-квартира правительственной связи (Government Communications Head-quarters). Здесь, за плотной завесой секретности, эти компьютеры использовались еще полтора десятка лет для тренировочных и вспомогательных криптографических задач. В 1959–1960 годах демонтировали и две последние машины, тогда же были сожжены и все рабочие схемы-чертежи компьютеров Colossus. При этом сам факт существования столь выдающихся для своего времени вычислительных устройств продолжали держать в строжайшей тайне еще многие годы.

Хотя официальной информации о Colossus не публиковалось вплоть до конца XX века, обрывочные сведения об этом компьютере стали появляться с середины 1970-х годов, когда истек стандартный для Британии 30-летний срок хранения государственных секретов. К 1996 году группе энтузиастов при национальном крипто-музее Блечли-Парк даже удалось воссоздать работоспособную копию этой машины, правдами и неправдами накопив достаточное количество подробностей, приватных воспоминаний и эскизов от оставшихся в живых участников проекта.

В таких условиях продолжать делать тайну из того, что так или иначе уже известно всем, стало бессмысленно. В октябре 2000 года власти Великобритании решились наконец рассекретить технический отчет о вскрытии FISH и машинах Colossus, подготовленный в 1945 году сразу по окончании войны. Объемный 500-страничный документ спецслужба GCHQ передала в общедоступный Государственный архив (Public Record Office) в городе Кью.

Заключение

Тьюринг положил начало развитию информационных технологий и активно применял их для выполнения прикладных задач. Помимо этого, он явно грезил в мечтах что его тест когда-то будет пройден машиной, и искусственный интеллект будет работать бок обок с нами.

Что ж это произошло: впервые в истории компьютерной программе удалось пройти тест Тьюринга на «человечность» и убедить 33% судей в том, что с ними общается не машина. Программа «Eugene Goostman», выдающая себя за тринадцатилетнего мальчика по имени Евгений Густман из Одессы, смогла убедить беседовавших с ней людей в том, что выдаваемые ею ответы принадлежат человеку.

А что касаемо искусственного интеллекта… А сейчас из каждого утюга продают курсы по машинному обучению, а большинство компаний обзавелись голосовыми ассистентами с искусственным интеллектом которые с лёгкостью обработают сотни и тысячи звонков одновременно.

Список использованной литературы

1. Биография Алана Тьюринга [Электронный ресурс] – <https://ria.ru/20120623/678612768.html>
2. Машина Тьюринга [Электронный ресурс] –   
   <https://inf1.info/turing>
3. Тест Тьюринга [Электронный ресурс] – <https://ru.wikipedia.org/wiki/Тест_Тьюринга>
4. Что такое тест Тьюринга и почему его так сложно пройти? [Электронный ресурс] – <https://aif.ru/dontknows/eternal/chto_takoe_test_tyuringa_i_pochemu_ego_tak_slozhno_proyti>
5. Колосс британский: Секретный предок компьютеров [Электронный ресурс] – <https://www.popmech.ru/technologies/5472-koloss-britanskiy-sekretnyy-predok-kompyuterov/>