Человеческое общество по мере своего развития овладевало не только веществом и энергией, но и информацией. С появлением и массовым распространение компьютеров человек получил мощное средство для эффективного использования информационных ресурсов, для усиления своей интеллектуальной деятельности. С этого момента (середина XX века) начался переход от индустриального общества к обществу информационному, в котором главным ресурсом становится информация. Возможность использования членами общества полной, своевременной и достоверной информации в значительной мере зависит от степени развития и освоения новых информационных технологий, основой которых являются компьютеры. На сегодняшний день реальный «интеллект», демонстрируемый самыми сложными нейронными сетями, находится ниже уровня дождевого червя, однако, как бы ни были ограничены возможности нейронных сетей сегодня, множество революционных открытий, могут быть не за горами.

Однако для начала я предлагаю разобраться в семантике слова ЭВМ и узнать историю вычислительных машин в целом и в частности пройтись по пути развития ЭВМ.

**Электро́нная вычисли́тельная маши́на** (сокращённо **ЭВМ**) — комплекс технических, аппаратных и [программных](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) средств, предназначенных для автоматической обработки информации, вычислений, [автоматического управления](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F). При этом основные функциональные элементы (логические, запоминающие, индикационные и др.) выполнены на [электронных элементах](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B8%D0%BA%D0%B0). Термин *машина* означает устройство, выполняющее механические движения. Современные компьютеры не являются машинами, название сохранилось за ними от простых счетных машин. Основным отличием вычислительной машины от таких счетных устройств, как счеты, арифмометр, калькулятор, заключается в том, что вся последовательность команд на вычисление предварительно записывается в память вычислительной машины и выполняется последовательно автоматически.

Если отметить основные вехи развития вычислительных машин, то основной период развития выпадает на 17 век.

Ещё в 1623 году немец [Вильгельм Шиккард](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D0%BA%D0%BA%D0%B0%D1%80%D0%B4,_%D0%92%D0%B8%D0%BB%D1%8C%D0%B3%D0%B5%D0%BB%D1%8C%D0%BC) создал так называемые «[Считающие часы](https://ru.wikipedia.org/wiki/%D0%A1%D1%87%D0%B8%D1%82%D0%B0%D1%8E%D1%89%D0%B8%D0%B5_%D1%87%D0%B0%D1%81%D1%8B_%D0%92%D0%B8%D0%BB%D1%8C%D0%B3%D0%B5%D0%BB%D1%8C%D0%BC%D0%B0_%D0%A8%D0%B8%D0%BA%D0%B0%D1%80%D0%B4%D0%B0)», которые сегодня принято считать первым автоматическим [калькулятором](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BB%D1%8C%D0%BA%D1%83%D0%BB%D1%8F%D1%82%D0%BE%D1%80). В письмах к [Иоганну Кеплеру](https://ru.wikipedia.org/wiki/%D0%9A%D0%B5%D0%BF%D0%BB%D0%B5%D1%80,_%D0%98%D0%BE%D0%B3%D0%B0%D0%BD%D0%BD) Шиккард объяснял, как можно использовать его машину для расчёта [астрономических таблиц](https://ru.wikipedia.org/wiki/%D0%90%D1%81%D1%82%D1%80%D0%BE%D0%BD%D0%BE%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%82%D0%B0%D0%B1%D0%BB%D0%B8%D1%86%D1%8B). Машина Шиккарда умела [складывать](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5) и [вычитать](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%87%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D0%B5) шестизначные [числа](https://ru.wikipedia.org/wiki/%D0%A7%D0%B8%D1%81%D0%BB%D0%BE), оповещая звонком о переполнении. Более сложные вычисления выполнялись с помощью набора [палочек Непера](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D0%BB%D0%BE%D1%87%D0%BA%D0%B8_%D0%9D%D0%B5%D0%BF%D0%B5%D1%80%D0%B0), установленного на корпусе механизма. Оригинал машины был потерян при пожаре ещё до начала двадцатого столетия. В [1960 году](https://ru.wikipedia.org/wiki/1960_%D0%B3%D0%BE%D0%B4) на основе сохранившихся чертежей была построена копия этого вычислителя, подтвердившая его существование и работоспособность.

В [1642 году](https://ru.wikipedia.org/wiki/1642_%D0%B3%D0%BE%D0%B4) машину, помогающую в сложении чисел, изобрёл [французский](https://ru.wikipedia.org/wiki/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D0%B8%D1%8F) учёный [Блез Паскаль](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%81%D0%BA%D0%B0%D0%BB%D1%8C,_%D0%91%D0%BB%D0%B5%D0%B7" \o "Паскаль, Блез). «[Паскалина](https://ru.wikipedia.org/wiki/%D0%A1%D1%83%D0%BC%D0%BC%D0%B8%D1%80%D1%83%D1%8E%D1%89%D0%B0%D1%8F_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0_%D0%9F%D0%B0%D1%81%D0%BA%D0%B0%D0%BB%D1%8F" \o "Суммирующая машина Паскаля)», как назвал свою конструкцию изобретатель, представляла собой механическое устройство в виде ящичка, наполненного многочисленными [шестерёнками](https://ru.wikipedia.org/wiki/%D0%A8%D0%B5%D1%81%D1%82%D0%B5%D1%80%D0%BD%D1%8F). Складываемые числа вводились в машину за счёт соответствующего поворота наборных колёсиков. На каждом из этих колёсиков, соответствовавших одному [десятичному](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%81%D1%8F%D1%82%D0%B8%D1%87%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) [разряду](https://ru.wikipedia.org/wiki/%D0%A7%D0%B8%D1%81%D0%BB%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D0%B0%D0%B7%D1%80%D1%8F%D0%B4), были нанесены деления с [цифрами](https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%B0) от 0 до 9. При вводе числа колёсики прокручивались до соответствующей цифры. При завершении полного оборота избыток над цифрой 9 переносился на соседний разряд (на 1 позицию сдвигалось соседнее колесо) и так далее. «Машина Паскаля» позволяла выполнять не только сложение, но и другие [операции](https://ru.wikipedia.org/wiki/%D0%90%D1%80%D0%B8%D1%84%D0%BC%D0%B5%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8), однако при этом требовала применения довольно неудобной процедуры повторных сложений.

В [1673 году](https://ru.wikipedia.org/wiki/1673_%D0%B3%D0%BE%D0%B4) другой известный учёный — [Готфрид Вильгельм Лейбниц](https://ru.wikipedia.org/wiki/%D0%9B%D0%B5%D0%B9%D0%B1%D0%BD%D0%B8%D1%86,_%D0%93%D0%BE%D1%82%D1%84%D1%80%D0%B8%D0%B4_%D0%92%D0%B8%D0%BB%D1%8C%D0%B3%D0%B5%D0%BB%D1%8C%D0%BC) изготовил механический [калькулятор](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BB%D1%8C%D0%BA%D1%83%D0%BB%D1%8F%D1%82%D0%BE%D1%80_%D0%9B%D0%B5%D0%B9%D0%B1%D0%BD%D0%B8%D1%86%D0%B0), позволявший легко выполнять вычитание, [умножение](https://ru.wikipedia.org/wiki/%D0%A3%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5) и [деление](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)).

[1723 год](https://ru.wikipedia.org/wiki/1723_%D0%B3%D0%BE%D0%B4) — немецкий [математик](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA) и [астроном](https://ru.wikipedia.org/wiki/%D0%90%D1%81%D1%82%D1%80%D0%BE%D0%BD%D0%BE%D0%BC) [Христиан Людвиг Герстен](https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D1%80%D1%81%D1%82%D0%B5%D0%BD,_%D0%A5%D1%80%D0%B8%D1%81%D1%82%D0%B8%D0%B0%D0%BD_%D0%9B%D1%8E%D0%B4%D0%B2%D0%B8%D0%B3) на основе работ Лейбница создал [арифметическую машину](https://ru.wikipedia.org/w/index.php?title=%D0%90%D1%80%D0%B8%D1%84%D0%BC%D0%B5%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0_%D0%93%D0%B5%D1%80%D1%81%D1%82%D0%B5%D0%BD%D0%B0&action=edit&redlink=1). Машина высчитывала [частное](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)) и [произведение](https://ru.wikipedia.org/wiki/%D0%A3%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5) (за счёт последовательно выполняемых операций сложения). Кроме того, в ней была предусмотрена возможность контроля за правильностью ввода данных.

В [1820 году](https://ru.wikipedia.org/wiki/1820_%D0%B3%D0%BE%D0%B4) француз [Тома де Кольмар](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D1%8C%D0%BC%D0%B0%D1%80,_%D0%A8%D0%B0%D1%80%D0%BB%D1%8C_%D0%9A%D1%81%D0%B0%D0%B2%D1%8C%D0%B5_%D0%A2%D0%BE%D0%BC%D0%B0_%D0%B4%D0%B5) наладил промышленный выпуск [арифмометров](https://ru.wikipedia.org/wiki/%D0%90%D1%80%D0%B8%D1%84%D0%BC%D0%BE%D0%BC%D0%B5%D1%82%D1%80).

Разработанная в [1823 году](https://ru.wikipedia.org/wiki/1823_%D0%B3%D0%BE%D0%B4) [разностная машина англичанина Чарльза Бэббиджа](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B7%D0%BD%D0%BE%D1%81%D1%82%D0%BD%D0%B0%D1%8F_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0_%D0%A7%D0%B0%D1%80%D0%BB%D1%8C%D0%B7%D0%B0_%D0%91%D1%8D%D0%B1%D0%B1%D0%B8%D0%B4%D0%B6%D0%B0) предназначалась для расчётов математических таблиц.

Изучение работ Бэббиджа и его советы помогли [шведскому](https://ru.wikipedia.org/wiki/%D0%A8%D0%B2%D0%B5%D1%86%D0%B8%D1%8F) изобретателю [Перу Георгу Шойцу](https://ru.wikipedia.org/wiki/%D0%A8%D1%83%D1%82%D1%86,_%D0%93%D0%B5%D0%BE%D1%80%D0%B3) начиная с [1854 года](https://ru.wikipedia.org/wiki/1854_%D0%B3%D0%BE%D0%B4), построить несколько разностных машин, а в [1859 году](https://ru.wikipedia.org/wiki/1859_%D0%B3%D0%BE%D0%B4) даже продать одну из них канцелярии [английского](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D1%8F) правительства.

Ещё одна «Разностная машина», построенная вскоре, также была в своей основе улучшенной версией машины Чарльза Бэббиджа и использовалась для расчёта и публикации печатных [логарифмических таблиц](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%82%D0%B0%D0%B1%D0%BB%D0%B8%D1%86%D0%B0).

К [1890 году](https://ru.wikipedia.org/wiki/1890_%D0%B3%D0%BE%D0%B4) [американцем](https://ru.wikipedia.org/wiki/%D0%A1%D0%A8%D0%90) [Германом Холлеритом](https://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D0%BB%D0%BB%D0%B5%D1%80%D0%B8%D1%82,_%D0%93%D0%B5%D1%80%D0%BC%D0%B0%D0%BD) была разработана электрическая [табулирующая система](https://ru.wikipedia.org/wiki/%D0%A2%D0%B0%D0%B1%D1%83%D0%BB%D1%8F%D1%82%D0%BE%D1%80_%D0%A5%D0%BE%D0%BB%D0%BB%D0%B5%D1%80%D0%B8%D1%82%D0%B0), которая использовалась в [переписях населения](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%BF%D0%B8%D1%81%D1%8C_%D0%BD%D0%B0%D1%81%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) [США](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D1%91%D0%BD%D0%BD%D1%8B%D0%B5_%D0%A8%D1%82%D0%B0%D1%82%D1%8B_%D0%90%D0%BC%D0%B5%D1%80%D0%B8%D0%BA%D0%B8) в [1890](https://ru.wikipedia.org/wiki/1890) и [1900 годах](https://ru.wikipedia.org/wiki/1900_%D0%B3%D0%BE%D0%B4).

В [1938 году](https://ru.wikipedia.org/wiki/1938_%D0%B3%D0%BE%D0%B4) немецкий [инженер](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80) [Конрад Цузе](https://ru.wikipedia.org/wiki/%D0%A6%D1%83%D0%B7%D0%B5,_%D0%9A%D0%BE%D0%BD%D1%80%D0%B0%D0%B4) на квартире родителей построил свою первую машину, названную [Z1](https://ru.wikipedia.org/wiki/Z1_(%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0)). Это была пробная модель полностью механической программируемой цифровой вычислительной машины. В том же году Цузе приступил к созданию машины [Z2](https://ru.wikipedia.org/wiki/Z2). А в [1941 году](https://ru.wikipedia.org/wiki/1941_%D0%B3%D0%BE%D0%B4) Цузе создаёт первую вычислительную машину, обладающую всеми свойствами современного компьютера [Z3](https://ru.wikipedia.org/wiki/Z3).

Теперь перейдем непосредственно к теме моего сегодняшнего доклада.

Начиная с 1950 года, каждые 7-10 лет кардинально обновлялись конструктивно-технологические и программно-алгоритмические принципы построения и использования ЭВМ. В связи с этим правомерно говорить о поколениях вычислительных машин. Условно каждому поколению можно отвести 10 лет.

ЭВМ проделали большой эволюционный путь в смысле элементной базы (от ламп к микропроцессорам) а также в смысле появления новых возможностей, расширения области применения и характера их использования. Деление ЭВМ на поколения - весьма условная, нестрогая классификация вычислительных систем по степени развития аппаратных и программных средств, а также способов общения с ЭВМ.

Основные идеи, по которым долгие годы развивалась вычислительная техника, были сформулированы в 1946 г. американским математиком Джоном фон Нейманом. Они получили название архитектуры фон Неймана. В 1949 году была построена первая ЭВМ с архитектурой фон Неймана – английская машина EDSAC. Годом позже появилась американская ЭВМ EDVAC. В нашей стране первая ЭВМ была создана в 1951 году. Называлась она МЭСМ — малая электронная счетная машина. Конструктором МЭСМ был Сергей Алексеевич Лебедев. Серийное производство ЭВМ началось в 50-х годах XX века.

Первое поколение ЭВМ — ламповые машины 50-х годов. Скорость счета самых быстрых машин первого поколения доходила до 20 тысяч операций в секунду. Для ввода программ и данных использовались перфоленты и перфокарты. Поскольку внутренняя память этих машин была невелика (могла вместить в себя несколько тысяч чисел и команд программы), то они, главным образом, использовались для инженерных и научных расчетов, не связанных с переработкой больших объемов данных. Это были довольно громоздкие сооружения, содержавшие в себе тысячи ламп, занимавшие иногда сотни квадратных метров, потреблявшие электроэнергию в сотни киловатт.

Логические схемы создавались на дискретных радиодеталях и электронных вакуумных лампах с нитью накала. В оперативных запоминающих устройствах использовались магнитные барабаны, акустические ультразвуковые ртутные и электромагнитные линии задержки, электронно-лучевые трубки (ЭЛТ). В качестве внешних запоминающих устройств применялись накопители на магнитных лентах, перфокартах, перфолентах и штекерные коммутаторы.

Программирование работы ЭВМ этого поколения выполнялось в двоичной системе счисления на машинном языке, то есть программы были жестко ориентированы на конкретную модель машины и "умирали" вместе с этими моделями.

В середине 1950-х годов появились машинно-ориентированные языки типа языков символического кодирования (ЯСК), позволявшие вместо двоичной записи команд и адресов использовать их сокращенную словесную (буквенную) запись и десятичные числа. В 1956 году был создан первый язык программирования высокого уровня для математических задач - язык Фортран, а в 1958 году - универсальный язык программирования Алгол.

ЭВМ, начиная от UNIVAC и заканчивая БЭСМ-2 и первыми моделями ЭВМ "Минск" и "Урал", относятся к первому поколению вычислительных машин.

Во втором поколении ЭВМ логические схемы строились на дискретных полупроводниковых и магнитных элементах (диоды, биполярные транзисторы, тороидальные ферритовые микротрансформаторы). В качестве конструктивно-технологической основы использовались схемы с печатным монтажом (платы из фольгированного гетинакса). Широко стал использоваться блочный принцип конструирования машин, который позволяет подключать к основным устройствам большое число разнообразных внешних устройств, что обеспечивает большую гибкость использования компьютеров. Тактовые частоты работы электронных схем повысились до сотен килогерц.

Стали применяться внешние накопители на жестких магнитных дисках и на флоппи-дисках - промежуточный уровень памяти между накопителями на магнитных лентах и оперативной памятью.

В 1964 году появился первый монитор для компьютеров - IBM 2250. Это был монохромный дисплей с экраном 12 х 12 дюймов и разрешением 1024 х 1024 пикселов. Он имел частоту кадровой развертки 40 Гц.

Создаваемые на базе компьютеров системы управления потребовали от ЭВМ более высокой производительности, а главное - надежности. В компьютерах стали широко использоваться коды с обнаружением и исправлением ошибок, встроенные схемы контроля. В машинах второго поколения были впервые реализованы режимы пакетной обработки и телеобработки информации.

Первой ЭВМ, в которой частично использовались полупроводниковые приборы вместо электронных ламп, была машина SEAC (Standarts Eastern Automatic Computer), созданная в 1951 году. В начале 60-х годов полупроводниковые машины стали производиться и в СССР.

В 1958 году Роберт Нойс изобрел малую кремниевую интегральную схему, в которой на небольшой площади можно было размещать десятки транзисторов. Эти схемы позже стали называться схемами с малой степенью интеграции (Small Scale Integrated circuits - SSI). А уже в конце 60-х годов интегральные схемы стали применяться в компьютерах.

Логические схемы ЭВМ 3-го поколения уже полностью строились на малых интегральных схемах. Тактовые частоты работы электронных схем повысились до единиц мегагерц. Снизились напряжения питания и потребляемая машиной мощность. Существенно повысились надежность и быстродействие ЭВМ.

В оперативных запоминающих устройствах использовались миниатюрнее ферритовые сердечники, ферритовые пластины и магнитные пленки с прямоугольной петлей гистерезиса. В качестве внешних запоминающих устройств широко стали использоваться дисковые накопители.

Появились еще два уровня запоминающих устройств: сверхоперативные запоминающие устройства на триггерных регистрах, имеющие огромное быстродействие, но небольшую емкость (десятки чисел), и быстродействующая кэш-память.

Начиная с момента широкого использования интегральных схем в компьютерах, технологический прогресс в вычислительных машинах можно наблюдать, используя широко известный закон Мура. Один из основателей компании Intel Гордон Мур в 1965 году открыл закон, согласно которому количество транзисторов в одной микросхеме удваивается через каждые 1,5 года.

Ввиду существенного усложнения как аппаратной, так и логической структуры ЭВМ 3-го поколения часто стали называть системами.

Так, первыми ЭВМ этого поколения стали модели систем IBM (ряд моделей IBM 360) и PDP (PDP 1). В Советском Союзе в содружестве со странами Совета Экономической Взаимопомощи (Польша, Венгрия, Болгария, ГДР и др.) стали выпускаться модели единой системы (ЕС) и системы малых (СМ) ЭВМ.

В вычислительных машинах третьего поколения значительное внимание уделяется уменьшению трудоемкости программирования, эффективности исполнения программ в машинах и улучшению общения оператора с машиной. Это обеспечивается мощными операционными системами, развитой системой автоматизации программирования, эффективными системами прерывания программ, режимами работы с разделением машинного времени, режимами работы в реальном времени, мультипрограммными режимами работы и новыми интерактивными режимами общения. Появилось и эффективное видеотерминальное устройство общения оператора с машиной - видеомонитор, или дисплей.

Большое внимание уделено повышению надежности и достоверности функционирования ЭВМ и облегчению их технического обслуживания. Достоверность и надежность обеспечиваются повсеместным использованием кодов с автоматическим обнаружением и исправлением ошибок (корректирующие коды Хемминга и циклические коды).

Модульная организация вычислительных машин и модульное построение их операционных систем создали широкие возможности для изменения конфигурации вычислительных систем. В связи с этим возникло новое понятие "архитектура" вычислительной системы, определяющее логическую организацию этой системы с точки зрения пользователя и программиста.

Революционным событием в развитии компьютерных технологий третьего поколения машин было создание больших и сверхбольших интегральных схем (Large Scale Integration - LSI и Very Large Scale Integration - VLSI), микропроцессора и персонального компьютера. Начиная с 1980 года практически все ЭВМ стали создаваться на основе микропроцессоров. Самым востребованным компьютером стал персональный.

4-е поколение: Логические интегральные схемы в компьютерах стали создаваться на основе униполярных полевых CMOS-транзисторов с непосредственными связями, работающими с меньшими амплитудами электрических напряжений (единицы вольт), потребляющими меньше мощности, нежели биполярные, и тем самым позволяющими реализовать более прогрессивные нанотехнологии (в те годы - масштаба единиц микрон).

Оперативная память стала строиться не на ферритовых сердечниках, а также на интегральных CMOS-транзисторных схемах, причем непосредственно запоминающим элементом в них служила паразитная емкость между электродами (затвором и истоком) этих транзисторов.

Первый персональный компьютер создали в апреле 1976 года два друга, Стив Джобс (1955 г. р.) - сотрудник фирмы Atari, и Стефан Возняк (1950 г. р.), работавший на фирме Hewlett-Packard. На базе интегрального 8-битного контроллера жестко запаянной схемы популярной электронной игры, работая вечерами в автомобильном гараже, они сделали простенький программируемый на языке Бейсик игровой компьютер "Apple", имевший бешеный успех. В начале 1977 года была зарегистрирована Apple Соrр., и началось производство первого в мире персонального компьютера Apple.

Кратко основную концепцию ЭВМ пятого поколения можно сформулировать следующим образом: компьютеры на сверхсложных микропроцессорах с параллельно-векторной структурой, одновременно выполняющих десятки последовательных инструкций программы. Компьютеры с многими сотнями параллельно работающих процессоров, позволяющих строить системы обработки данных и знаний, эффективные сетевые компьютерные системы.

Линия в развитии ЭВМ пятого поколения, это — суперкомпьютер. Машины этого класса имеют быстродействие сотни миллионов и миллиарды операций в секунду. Суперкомпьютер – это многопроцессорный вычислительный комплекс.

Разработки в области вычислительной техники продолжаются. ЭВМ шестого поколения — это машины недалекого будущего. Основным их качеством должен быть высокий интеллектуальный уровень. В них будет возможным ввод с голоса, голосовое общение, машинное «зрение», машинное «осязание».

Машины шестого поколения — это реализованный искусственный интеллект.

**Появление «Загадки»**

Разработка семейства шифровальных машин «Энигма» стартовала сразу после Первой мировой, еще в 1918 году. Немец Артур Шербиус получил патент на роторную шифровальную машину, которая, по сути, являлась первым вариантом «Загадки» (так Enigma переводится с немецкого). В 1923 Шербиус вместе с компаньоном организовал предприятие со сложнопроизносимым названием Chiffriermaschinen Aktiengesellschaft, наладившее серийный выпуск шифровальных аппаратов.

Первые две модели «Энигмы», A и B, пользовались умеренным успехом. Настоящим прорывом в 1925 году стала модель С — с рефлектором, гораздо более компактная, чем ее предшественники. Enigma C весила всего лишь 12 кг при размере 28 на 34 на 15 см, тогда как предыдущие модели весили около 50 кг, имея габариты 65 на 45 на 35 сантиметров. Модель С практически сразу стали использовать на судах немецкого флота.

В 1928 году военные специалисты по заказу Вермахта переработали конструкцию гражданских шифровальных машин, сконструировав модель Enigma-G, которую двумя годами позже модифицировали в версию Enigma-I. Именно этот аппарат 1930 года стал основой для множества версий, которые во время Второй Мировой использовали самые разные военные службы. Существовали варианты Enigma с количеством роторов от 3 до 8. Правда, восьмироторная версия, созданная специально для высших армейских структур, довольно быстро была выведена из эксплуатации из-за ненадежности.

## «Слив», не превратившийся во взлом

Хотя «Энигма» была одобрена высшими чинами немецкой армии в том числе и за свою эффективность и надежность, секретность шифруемых на ней сообщений оказалась под угрозой очень скоро. Виной тому стал агент Аше — он же Ганс-Тило Шмидт, с 1931 года сотрудник шифровального бюро минобороны Германии — агент французской разведки. Шмидт передавал французам вышедшие из употребления коды, которые обязан был уничтожать, а также «слил» инструкцию по использованию военного варианта шифровальной машины.

К информации «агента Аше» французская разведка отнеслась довольно прохладно. Иметь своего агента в стане потенциального противника было полезно, но **«Энигма» считалась настолько надежной машиной, что взломать ее во Франции даже не попытались**. Зато в Польше, которой французы передали материалы от своего немецкого агента, нашлись гении криптографии, разобравшиеся с шифром.

## «Польский Тьюринг»

**«Надежную машину» взломал Мариан Реевский, 27-летний математик, окончивший секретные курсы криптографии.**Хотя в польском Бюро шифрования он работал не один, работать над расшифровкой Enigma I доверили только Реевскому. Мариан сразу же активно начал искать уязвимости ключа сообщений, выбирая из ежедневных шифрограмм первые шесть букв и составляя таблицы соответствий.

Сначала ему удалось обнаружить 4 повторяющиеся последовательности букв в шифрах. А затем благодаря информации о том, что у «Энигмы» только три барабана, а начальная настройка состоит из трех букв латинского алфавита, Реевский установил количество возможных кодовых цепочек. Оно оказалось во много раз меньше, чем предполагали ранее: 3!263 против 26!. Это дало возможность в течение года составить полный каталог всех цепочек.

Видимо, догадавшись о том, что их шифры могут быть прочитаны, немецкие криптографы начали гораздо чаще менять конфигурацию положения роторов машины. А осенью 1938 года принцип шифрования был изменен, что сделало невозможным распознавание шифрограмм на основе прежних методов. Однако Реевский со своими коллегами раскусил эту уловку, состоявшую в так называемом удвоении ключа и являвшуюся, по сути, криптографической ошибкой.

**Уже через несколько месяцев поляки создали аппарат под названием «Бомба Реевского»**, названный так то ли за характерный звук тиканья при работе, то ли в честь круглых пирожных, которые Мариан очень любил. Устройство проводило поиск по шаблону, учитывая, что парам первой и четвертой, второй и пятой, третьей и шестой букв шифрованного текста соответствовали одинаковые буквы текста нешифрованного.

Криптологическая «бомба» Реевского. 1 — роторы для подбора ключей, 2 — двигатель для вращения роторов, 3 — индикаторная тумба, сигнализирующая об успешном подборе кода

Именно работы Мариана Реевского стали основой успеха Алана Тьюринга. Хотя нельзя сказать, что британец всего лишь присвоил себе чужой успех. Да, поляки в 1939 году при нападении войск Третьего Рейха передали все наработки местных дешифровщиков агентам британской разведки. Но методика Реевского к этому времени была бесполезна для работы с «Энигмой».

## Погоня за ошибками и перебор вариантов

Уже в декабре 1938 года к трем роторам машины добавили еще два, и количество возможных позиций роторов увеличилось в 10 раз. Вместо 6 «бомб Реевского» полякам уже тогда требовалось 60 дешифрующих устройств. А в мае 1940 года немцы отказались от идеи удвоения ключа, и сам концепт польского дешифрующего аппарата оказался бесполезным. Так что Тьюринг проделал огромный пласт работы, чтобы разгадать усовершенствованную «Загадку» — тем более что польские криптоаналитики уничтожили «бомбы» в сентябре 1939 года, после вторжения немецких войск в страну.

Реевский был гением, но допустил ошибку, постоянно выискивая чужие ошибки. Методика польского дешифровщика состояла в выявлении уязвимостей «Энигмы». Но сами немцы постоянно совершенствовали свою машину, вынуждая молодого математика все время находиться в позиции догоняющего.

Англичанам уже не подходила «бомба Реевского», которая для подбора ключа использовала перебор всех возможных комбинаций.

Тьюринг предложил более простой и менее трудозатратный способ расшифровки: **учитывать в работе то, что часть исходного текста известна**. Несмотря на хитроумность немецкого шифра, несмотря на все предосторожности, немецкие солдаты чаще всего общались между собой короткими стереотипными фразами, которые можно было «узнать». Точное место отдельных фраз в шифровке можно было определить механическим перебором 26 букв латинского алфавита. Дополнительным облегчением было и то, что в шифре «Энигмы» ни одна из букв исходного сообщения не кодировалась той же самой буквой.

**«Бомба» для Третьего Рейха**

На основе этой методики были разработаны «Бомбы Тьюринга». Первую запустили 18 марта 1940 года — для каждого возможного исходного положения роторов она выполняла сверку с известным фрагментом текста и формировала логические предположения. Если в этих предположениях обнаруживались нестыковки, вариант «отбраковывался». Таким образом, из огромного множества вариантов — 1019 возможных комбинаций для обычного варианта «Энигмы» или 1022 для версии, использовавшейся подводниками — оставались лишь несколько логически непротиворечивых, на основе которых машина и подбирала шифр.

Восстановленная «Бомба Тьюринга» в Блетчли-Парке

Весной 1940 года британским криптографам удалось разгадать шрифт сухопутного варианта «Энигмы». Еще через полгода была расшифрована продвинутая версия, которая использовалась на подводных лодках Рейха.

Команда дешифраторов круглосуточно, в несколько смен работала в роскошном особняке под названием Блетчли-Парк в городке Милтон Кейнс в 72 км от Лондона. Сотрудники обрабатывали тысячи сообщений ежедневно, выделяя в шифрограммах так называемые подсказки — приветствия, цифры, повторяющиеся куски текста. На основе этих фрагментов машина и строила свои предположения.

Иногда случалось так, что информации оказывалось недостаточно для разгадки шифра. Особенно критично это было накануне крупных операций немцев. Тогда британские войска прибегали к приему под названием «гарденинг» (возделывание). Для этого британские ВМС проводили демонстративные минирования отдельных участков моря, а в Блетчли-Парке затем определяли известный текст на основе докладов противника о разминированиях.

**Гений, которого оценили слишком поздно**

Тьюринг сделал все для того, чтобы Англия не сдалась под натиском немецкого флота и авиации, а у СССР в союзниках осталась не только Америка. Как сказал однажды один из коллег Алана: «Не берусь утверждать, что мы выиграли войну благодаря Тьюрингу. Однако без него могли бы ее и проиграть».

Алан Тьюринг считается одной из самых важных фигур в истории криптографии. Но его работа по дешифровке «Энигмы» едва ли повлияла на развитие данной науки — как бы странно это ни звучало. Все дешифровальные аппараты из Блетчли-Парка после Второй Мировой были уничтожены, а сам факт попыток дешифровки — успешных и не очень — держали в секрете до 1970 годов. Сам ученый уже в 1952 году из неизвестного героя превратился в объект публичного позора: Тьюринга обвинили заставили проходить курс гормональной терапии, от которого «победитель Энигмы» впал в глубокую депрессию и через два года покончил жизнь самоубийством.

В 2013 году королева Великобритании Елизавета II официально помиловала Тьюринга, который был обвинен в «непристойности».

И тем не менее: сегодня имя Тьюринга знакомо большинству людей. В честь гения назван принцип полноты по Тьюрингу, тест Тьюринга и машина Тьюринга, а также одна из самых престижных премий в области информатики. В кино Алана сыграл жутко модный Бенедикт Камбербэтч, а в Манчестере ему поставлен памятник.