INFORMATICA CUANTICĂ

Acad. AȘM, Profesor univ. Sidorenko Anatolie

Institutul de Inginerie Electronica
și Nanotehnologii al UTM

E-mail: sidorenko.anatoli@gmail.com
anatolie.sidorenko@mib.utm.md
Tel./viber *+37369513294*

INFORMATICA CUANTICĂ

Квантовая информатика — раздел науки, возникший в начале XXI века на стыке квантовой механики, теории алгоритмов и теории информации. В квантовой информатике изучаются общие принципы и законы, управляющие динамикой сложных квантовых систем. Моделью таких систем является квантовый компьютер.

Квантовая информатика включает в себя вопросы квантовых вычислений и квантовых алгоритмов, физику квантовых компьютеров, квантовой криптографии и квантовой теории информации, непосредственно касается оснований квантовой теории, в частности, проблемы измерений и описания декогерентности. Важнейшим физическим явлением, которое изучается в квантовой информатике, являются запутанные квантовые состояния и порождаемые ими нелокальные свойства квантовой физики многих тел.

Квантовая информация представляется в кубитах (*quantum bit*). Кубиты могут находиться в состоянии, являющемся суперпозицией 0 и 1. Несколько кубитов могут быть в запутанном состоянии (*entangled*).

Тема 1. Введение. Определение квантовой информатики. Связь с другими науками. Компьютеры с не-фон Неймановской архитектурой. Классические и квантовые приборы. Алгоритмы: классы их сложности. Парадоксы квантовой механики - «Кот Шредингера».

Важнейшие разделы квантовой информатики:

квантовая криптография — этот раздел активно применяется для обеспечения секретности передачи информации;

технологии запутанных состояний —получение, верификация и изучение свойств запутанных состояний до десятка частиц (фотоны, зарядовые состояния электронов и куперовских пар, спины электронов и ядер), есть отдельные приложения в работающих приборах. Работающие прообразы квантового компьютера (малокубитные — до 10 кубитов — квантовые процессоры и многокубитные – более 100 кубитов).

компьютерное моделирование систем многих частиц — новый и наименее разработанный раздел, он включает гипотетический симулятор и моделирование сложных систем на квантовом уровне, вычислительная модель квантового процессора с декогерентностью; моделирование ведётся с использованием классических симуляторов квантового компьютера с большим распараллеливанием, решением квантовой проблемы трех тел.

СВЯЗЬ КВАНТОВОЙ ИНФОРМАТИКИ С ДРУГИМИ ДИСЦИПЛИНАМИ

ТЕОРИЯ ИНФОРМАЦИИ

— раздел прикладной математики, относящийся к измерению количества информации (Шеннон энтропии), её свойств и устанавливающий предельные соотношения для систем передачи данных.

ТЕОРИЯ ВЕРОЯТНОСТЕЙ

— раздел математики, изучающий случайные события, случайные величины, их свойства и операции над ними.

КВАНТОВОАЯ ИНФОРМАТИКА

раздел науки, посвященный использованию квантовых объектов для обработки и передачи информации. Моделью таких объектов является квантовый компьютер.

СТАТИСТИ́ЧЕСКАЯ ФИ́ЗИКА

- раздел теоретической физики, изучающий системы, состоящие из большого числа частиц (молекул, атомов, электронов и т. д.), исходя из свойств этих частиц и взаимодействий между ними. Изучаемые системы могут быть как классическими, так и квантовыми.

РАДИОТЕХНИКА

— наука, изучающая электромагнитные колебания и волны радиодиапазона, методы генерации, усиления, преобразования, излучения и приёма и обработку сигналов, а также применение их для передачи информации.

КВАНТОВАЯ МЕХАНИКА

— фундаментальная физическая теория, которая описывает природу в масштабах атомов и субатомных частиц. Она лежит в основе всей квантовой физики, включающей квантовую химию, квантовую теорию поля, квантовую технологию и квантовую информатику.

КВАНТОВАЯ ОПТИКА

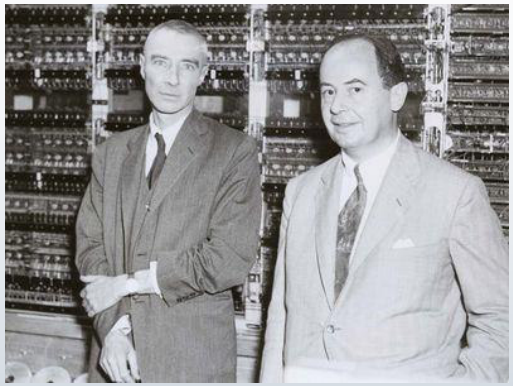
- раздел оптики, занимающийся изучением явлений, в которых проявляются квантовые свойства света. К таким явлениям относятся:тепловое_излучение, фотоэффект, эффект Комптона, эффект Рамана, фотохимические процессы, вынужденное излучение и, соответственно, физика лазеров.

СВЕРХПРОВОДИМОСТЬ

— свойство некоторых материалов обладать *строго нулевым* электрическим сопротивлением при достижении ими температуры ниже определённого значения (критической температуры).

All modern computers, starting from the first generation till the fourth generation have the architecture proposed by John von Neumann

(Neumann János Lajos ; December 28, 1903 – February 8, 1957)



John von Neumann (right) near 30-tons ENIAC (Electronic Numerical Integrator and Computer), 1946.

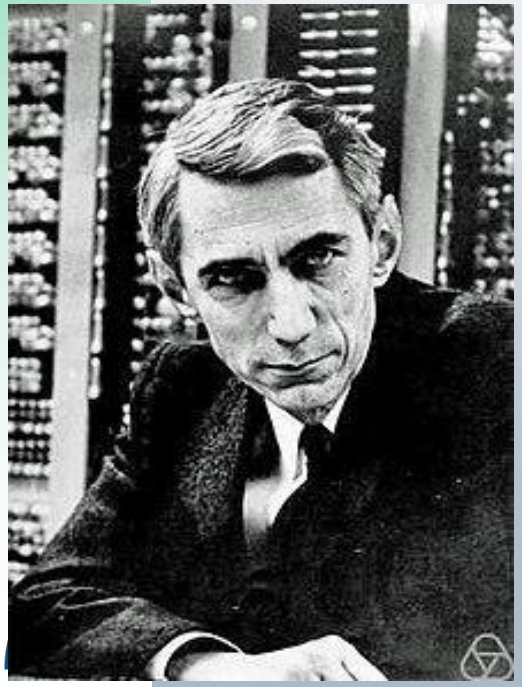
He was the pioneer in building the mathematical framework of quantum physics, in the development of functional analysis, and in game theory, introducing or codifying concepts including cellular automata, the universal constructor and the digital computer – proposed and implemented the "Von Neumann architecture" of the digital computer.

He proposed shared the same memory for code (program) and data, -means, a single-processor, stored-program computer—the widespread architecture now known as a von Neumann machine or von Neumann architecture.

Base elements of the ENIAC

- 18000 vacuum tubes :

Useless machine Шеннона:
1 бит информации — символ или сигнал, который может принимать два значения: включено или выключено, да или нет, высокий или низкий; в двоичной системе исчисления это 1 (единица) или 0 (ноль).



Клод Э́лвуд Ше́ннон (30 апреля 1916, Мичиган, США — 24 февраля 2001, Массачусетс, США) — американский инженер, криптоаналитик и математик.

Является основателем теории информации, предоставил фундаментальные понятия, идеи и их математические формулировки, которые в настоящее время формируют основу для современных коммуникационных технологий. В 1948 году предложил использовать слово «бит» для обозначения наименьшей единицы информации (в статье «Математическая теория связи»). Кроме того, понятие энтропии было важной особенностью теории Шеннона. Он продемонстрировал, что введённая им энтропия эквивалентна мере неопределённости информации в передаваемом сообщении. Статьи Шеннона «Математическая теория связи» и «Теория связи в секретных системах» считаются основополагающими для теории информации и криптографии. Клод Шеннон был одним из первых, кто подошёл к криптографии с научной точки зрения, сформулировал её теоретические основы и ввёл в рассмотрение многие основные понятия. Шеннон внёс ключевой вклад в теорию вероятностных схем, теорию игр, теорию автоматов и теорию систем управления — области наук, входящие в понятие «кибернетика».

Shannon C. E. A Mathematical Theory of Communication // Bell System Technical Journal. — 1948. — Vol. 27. — P. 379—423.
К. Шеннон. Теория связи в секретных системах // Работы по теории информации и кибернетике / Пер. С. Карпова. — М.: ИЛ, 1963. — С. 243—322. — 830 с.

Шеннон ввел понятие информационной энтропии (энтропия Шеннона), аналогичное энтропии Больцмана из термодинамики, которое является мерой неопределённости информации - логарифмическая функция по основанию 2 информации передаваемого сообщения M:

$$I = \mathrm{Log}M$$

и показал её удобство:

1.Она удобна практически. Параметры, важные в инженерных приложениях — такие, как время, пропускная способность, число переключателей и так далее — обычно меняются линейно при логарифмическом изменении числа возможных вариантов. К примеру, добавление одного переключателя удваивает число возможных состояний их группы, увеличивая на единицу его логарифм по основанию 2. Увеличение в два раза времени приводит к квадратичному росту числа сообщений, или удвоению их логарифма, и так далее.

2.Она близка к нашему интуитивному представлению о такой мере. Это тесно связано с предыдущим пунктом, так как мы интуитивно измеряем величины, линейно сравнивая их со стандартами. Так, нам кажется, что на двух перфокартах можно разместить в два раза больше информации, а по двум одинаковым каналам — передать её в два раза больше.

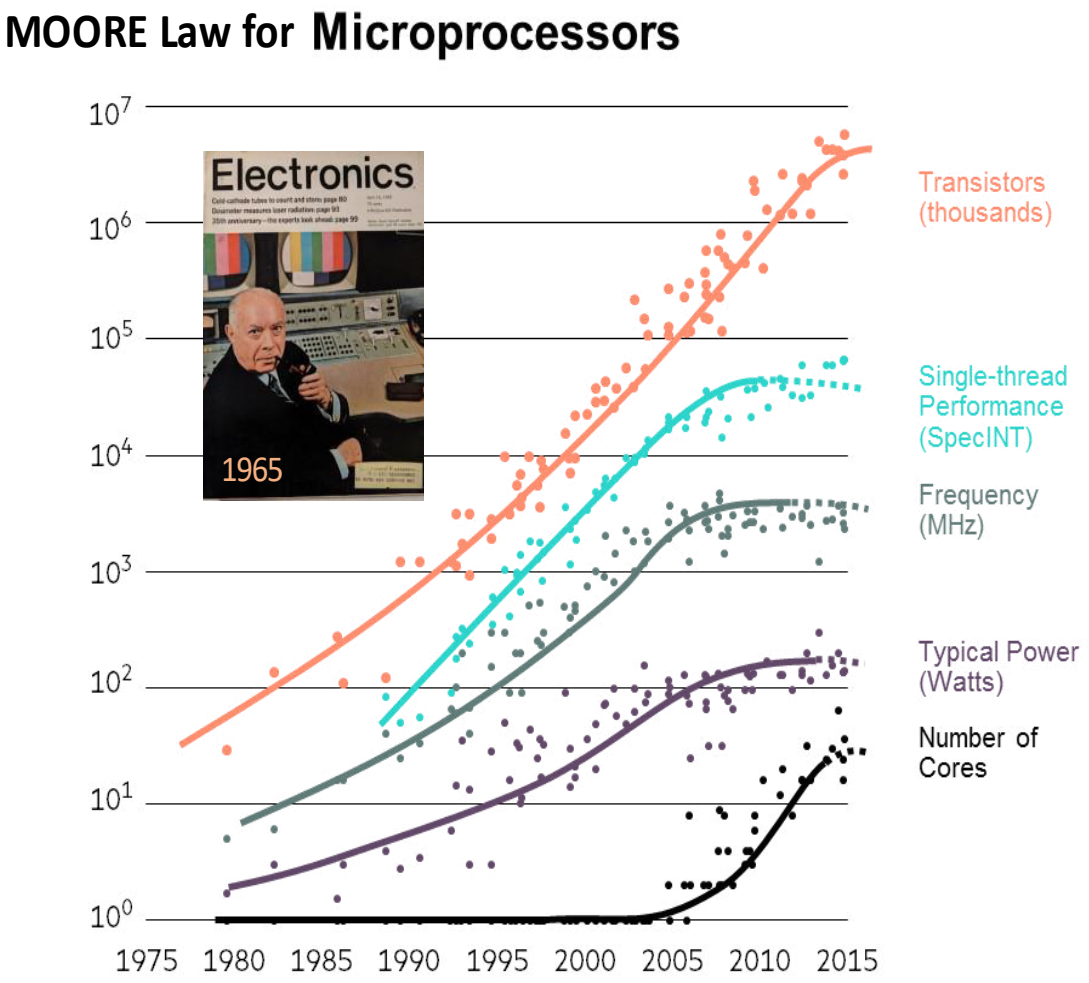
3.Она удобна математически. Многие предельные переходы просты в логарифмах, в то время как в терминах числа вариантов они достаточно сложны.
Также ввел понятие обобщённой системы связи, состоящей из источника информации, передатчика, канала, приемника и пункта назначения. Шеннон разделяет все системы на дискретные, непрерывные и смешанные.

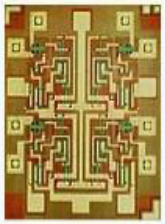
Энтропия является количеством, определённым в контексте вероятностной модели для источника данных. Например, кидание монеты имеет энтропию: -2(1/2log (1/2)) = -Log (½) = log2 = 1 бит информации на одно кидание (при условии его независимости), а

количество **возможных состояний** равно: два в в степени единица = 2 **возможных состояния** (значения) («орёл» и «решка»).

Принцип Ландауэра гласит: **при стирании одного бита информации выделяется энергия Q =kв T log2 =** E_{SNL}
При $T = 300$ K энергия $E_{\mathrm{SNL}} \approx 0{,}017$ эВ $\approx 2{,}7\times10^{-21}$ Дж.

Тема 1. НАРУШЕНИЕ «ЗАКОНА МООРА» И НЕОБХОДИМОСТЬ АЛЬТЕРНАТИВНОЙ АРХИТЕКТУРЫ ОБРАБОТКИ ИНФОРМАЦИИ





MOSFET scaling (process nodes)

10 µm – 1971
6 µm – 1974
3 µm – 1977
1.5 µm – 1981
1 µm – 1984
800 nm – 1987
600 nm – 1990
350 nm – 1993
250 nm – 1996
180 nm – 1999
130 nm – 2001
90 nm – 2003
65 nm – 2005
45 nm – 2007
32 nm – 2009
22 nm – 2012
14 nm – 2014
10 nm – 2016
7 nm – 2018
5 nm – 2020

Future

3 nm – ~2022
2 nm – >2023

(wiki)

Тема 1. НАРУШЕНИЕ «ЗАКОНА МООРА» И НЕОБХОДИМОСТЬ АЛЬТЕРНАТИВЫ

Facebook Data Center, Luleå, Sweden

- 2014 completion target
- Cost: ~760 M$
- Nearby Lule River generates 9% of Sweden's electricity (~4.23 GW)
- Average annual temperature: 1.3 °C

	Specifications
Performance*	27-51 PFLOP/s
Memory*	21-27 PB RAM 1900-6800 PB disk
Power	84 MW avg* (120 MW max)
Space	290,000 ft² (27,000 m²)
Cooling*	~1.07 PUE

* estimated

- D.S. Holmes, B.A. Hamilton, Beyond CMOS Workshop, 2016 April 4-5

Тема 1. НАРУШЕНИЕ «ЗАКОНА МООРА» И НЕОБХОДИМОСТЬ АЛЬТЕРНАТИВНЫ

Ограничения возникающие при наращивании вычислительной мощности

- *Мощность* (возможности электростанций, заведение большой мощности на объект)
- Ограничения по *площади*
- Инфраструктура, требуемая для *охлаждения*

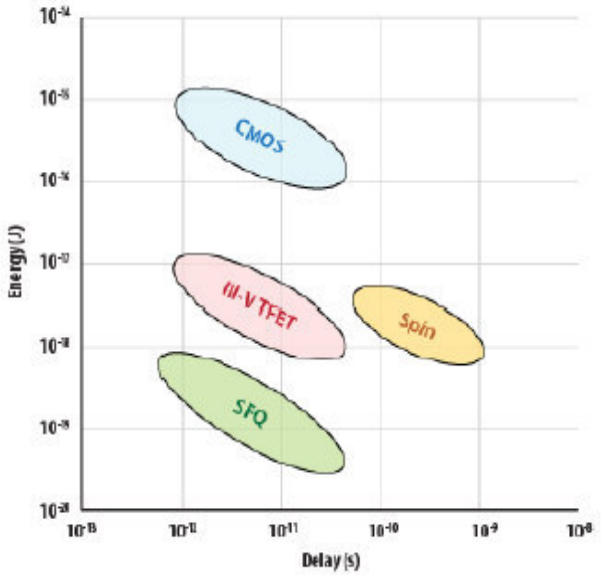
❖ Наращивание мощности в рамках существующих технологий

- Энергопотребление на уровне > 100 МВт

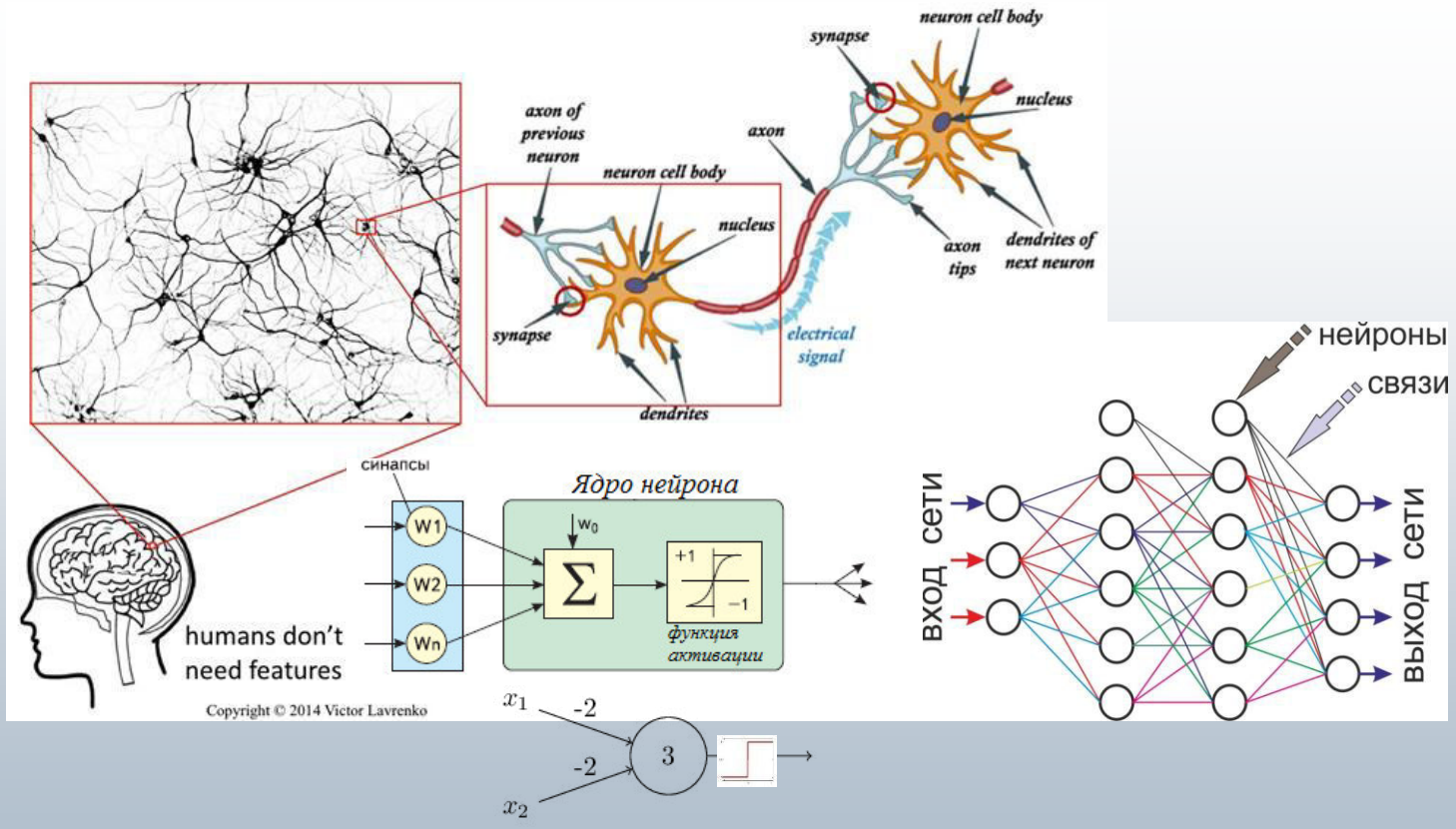
или

- Кардинальная оптимизация всех компонент (?)

❖ Альтернативные технологии вычислений

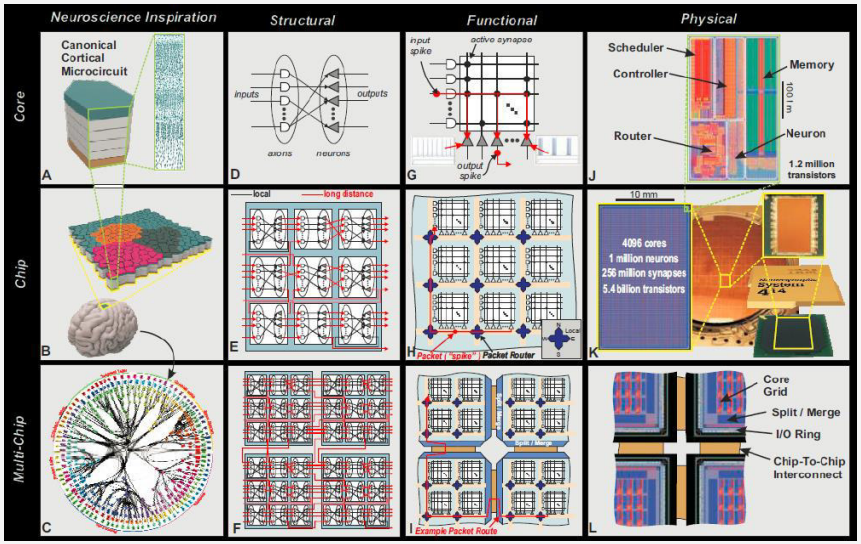


Solution: non-von Neumann architecture, brain-like Artificial Neural Network (ANN) and Quantum Computer (QUBIT)

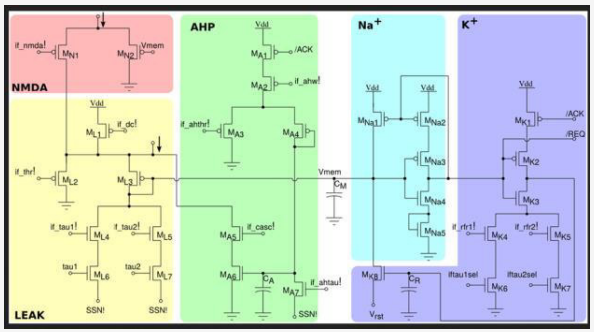


Modern approaches to design the ANN and base elements

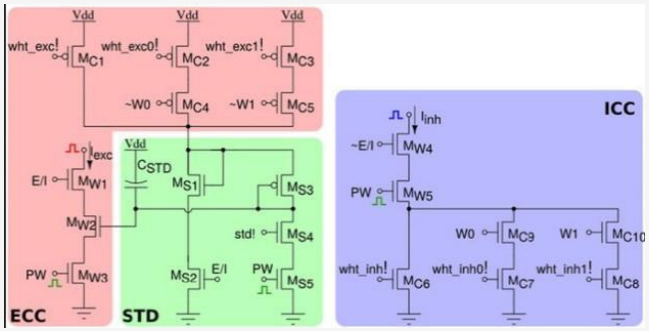
IBM TrueNorth



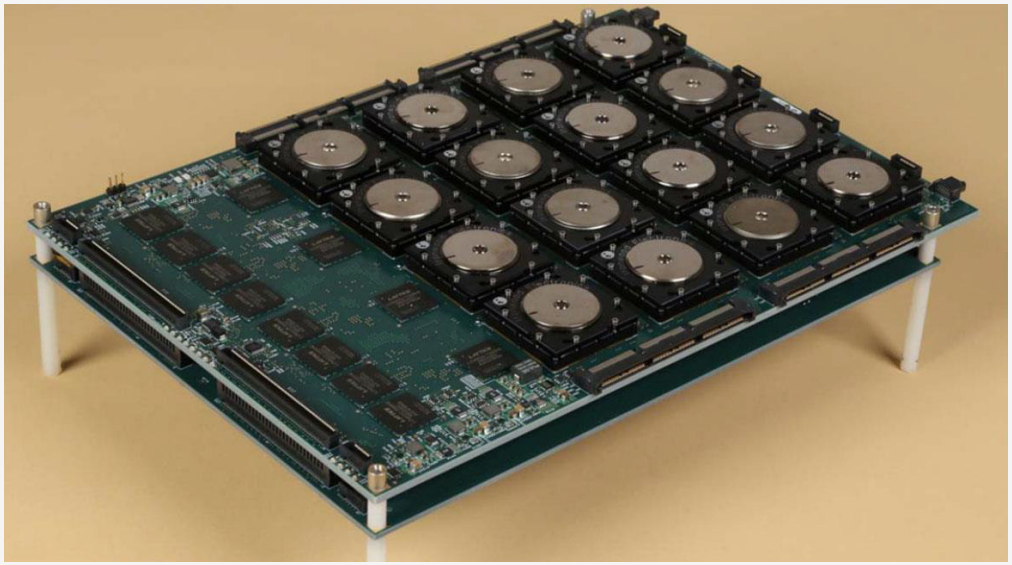
Artificial neuron based on CMOS



Artificial synapse – based on CMOS



Modern approaches to design the ANN



- Отладочная плата с 16 нейроморфными процессорами “IBM TrueNorth”, каждый из которых содержит более 5 млрд транзисторов и имитирует работу до 1 миллиона модельных «нейронов» и до 250 миллионов связей между ними («синапсов»).
  IBM company, August 2014.

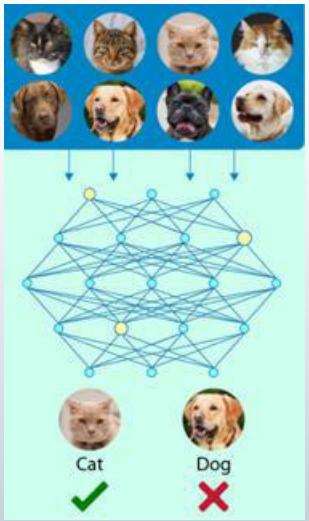
Brain vs neural network

neural network Bert

Power consumption
for training: 1,000 kW h

10^8 tunable synaptic weights

Cat or dog ???
image recognition



Brain:

power consumption: 20 w

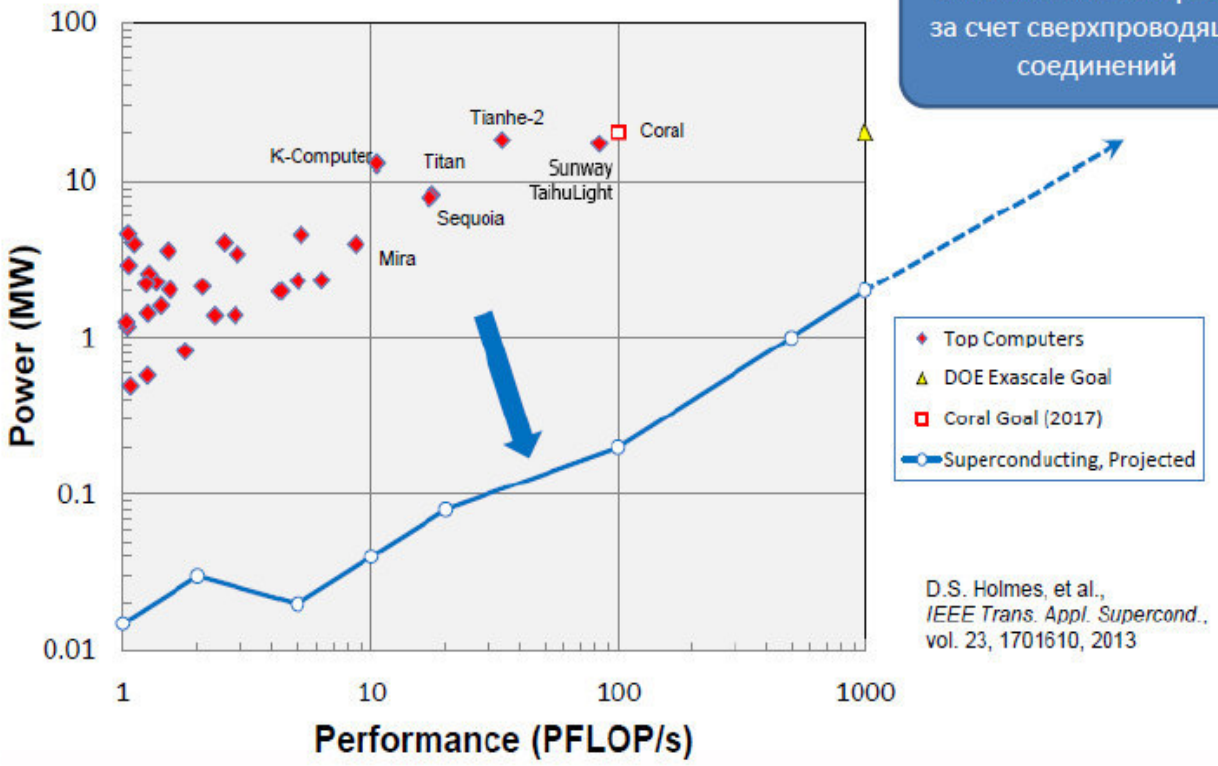
10^{15} synapses and 10^{11} neurons

Тема 1. НАРУШЕНИЕ «ЗАКОНА МООРА» И НЕОБХОДИМОСТЬ АЛЬТЕРНАТИВ

СВЯЗЬ2017
ФУНДАМЕНТ ЦИФРОВОЙ ТРАНСФОРМАЦИИ
ГОСУДАРСТВО. ОБЩЕСТВО. БИЗНЕС

Энергоэффективность вычислений

Наибольший выигрыш – за счет сверхпроводящих соединений



D.S. Holmes, et al., *IEEE Trans. Appl. Supercond.*, vol. 23, 1701610, 2013

- D.S. Holmes, B.A. Hamilton, Beyond CMOS Workshop, 2016 April 4-5

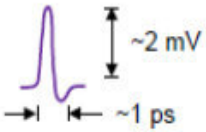
Тема 1. НАРУШЕНИЕ «ЗАКОНА МООРА» И НЕОБХОДИМОСТЬ АЛЬТЕРНАТИВНОЙ ЭЛЕКТРОНИКИ-СПИНТРОНИКИ

СВЯЗЬ2017
ФУНДАМЕНТ ЦИФРОВОЙ ТРАНСФОРМАЦИИ
ГОСУДАРСТВО. ОБЩЕСТВО. БИЗНЕС

Сверхпроводниковая технология вычислений

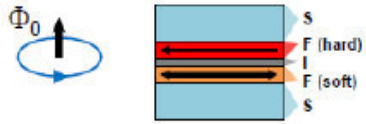
Функционирование при низких температурах (~ 4 К)

- Возможность использования новых физических эффектов
- Коммерчески доступные охлаждающие системы (x400 Вт/Вт - x5000 Вт/Вт)



Логика

- Одноквантовая логика (Single Flux Quantum - SFQ)
- Энергия переключения ~ 10^{-19} Дж



Память

- магнитная память, совместимая с SFQ

Интерконнекты

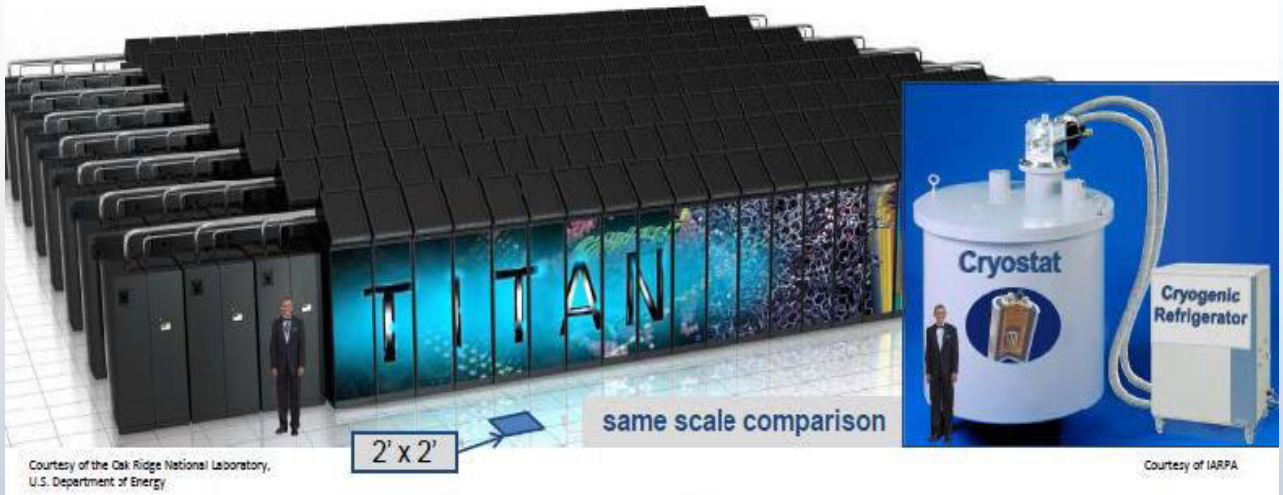
- Сверхпроводящие соединения
- Вход/выход: электрический или оптический

➢ Возможность уменьшения энергозатрат во всех трех областях

Тема 1. НАРУШЕНИЕ «ЗАКОНА МООРА» И НЕОБХОДИМОСТЬ АЛЬТЕРНАТИВ

СВЯЗЬ2017
ФУНДАМЕНТ ЦИФРОВОЙ ТРАНСФОРМАЦИИ
ГОСУДАРСТВО. ОБЩЕСТВО. БИЗНЕС

Концептуальное сравнение (~20 PFLOP/s)



Courtesy of the Oak Ridge National Laboratory, U.S. Department of Energy

Courtesy of IARPA

	Titan at ORNL	Superconducting Supercomputer	
Performance	17.6 PFLOP/s (#2 in world*)	20 PFLOP/s	~1x
Memory	710 TB (0.04 B/FLOPS)	5 PB (0.25 B/FLOPS)	7x
Power	8,200 kW avg. (not included: cooling, storage memory)	80 kW total power (includes cooling)	0.01x
Space	4,350 ft² (404 m², not including cooling)	~200 ft² (19 m², includes cooling)	0.05x
Cooling	additional power, space and infrastructure required	All cooling shown	

* TOP500, 2015-11

- D.S. Holmes, B.A. Hamilton, Beyond CMOS Workshop, 2016 April 4-5

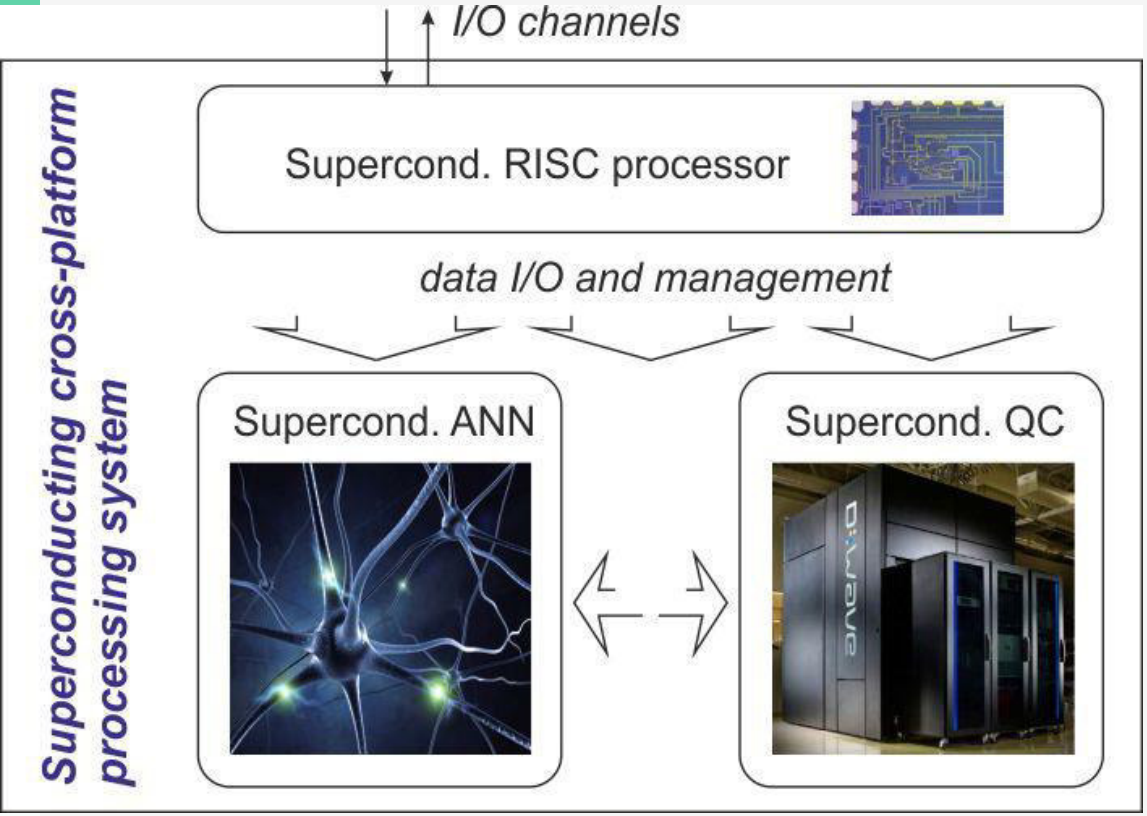
Тема 1. НАРУШЕНИЕ «ЗАКОНА МООРА» И НЕОБХОДИМОСТЬ АЛЬТЕРНАТИВ

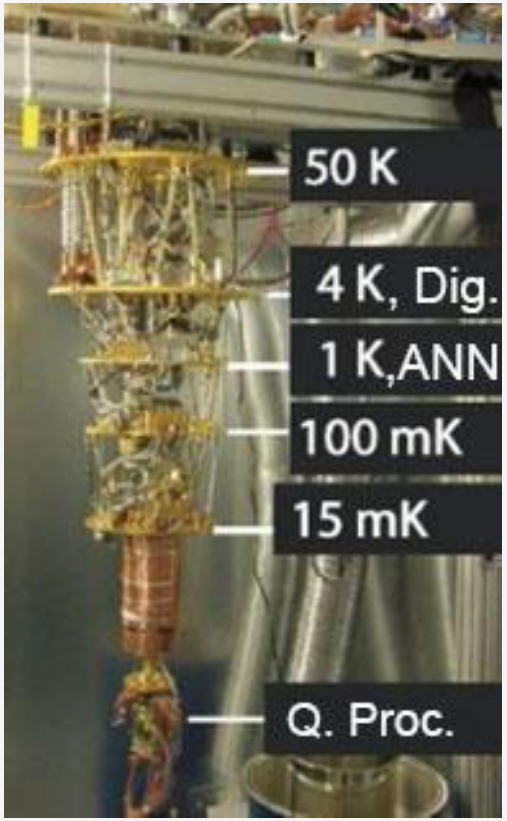
Выводы: в качестве самых энергоэффективных архитектур на сегодняшний момент выступают не-фон Неймановские схемы на базе адиабатической сверхпроводниковой логики. Для таких схем нет нижнего порога энергопотребления на операцию. В настоящее время схемы на базе адиабатической сверхпроводниковой логики активно развиваются и исследуются. Так, в 2020 году был представлен процессор на базе адиабатической сверхпроводниковой логики с суммарным энергопотреблением на операцию ~ 15 фДж на тактовой частоте 5 ГГц, включая затраты на охлаждение, что сравнимо с потреблением 1 транзистора!

Датацентр, собранный из таких процессоров, будет иметь энергопотребление около 10 киловатт (в основном за счет криогенных систем охлаждения процессоров) – по сравнению с таким же полупроводниковым датацентром потребляющим 120 мегаватт, т.е. на 4 порядка меньше энергопотребление!

Тема 1. НАРУШЕНИЕ «ЗАКОНА МООРА» И НЕОБХОДИМОСТЬ АЛЬТЕРНАТИВ

Superconducting solution - **Rapid and energy-efficient platform**
- - neural network and quantum computer with non-von Neumann architecture





Temperature levels of operating ANN and Quantum Computer

Тема 1. Квантовая информатика. Введение.

Квантовая информатика – раздел науки «информатика», посвященный использованию квантовых объектов для обработки и передачи информации.

В настоящее время ведутся интенсивные работы по разработке квантового компьютера. Создаются квантовые базовые элементы, строятся квантовые алгоритмы и разрабатывается архитектура квантового компьютера.

Другое перспективное и уже развитое направление квантовой информатики – квантовая криптография. Квантовые методы передачи данных гарантируют невозможность расшифровки сообщения. Идея создания перепутанных состояний, высказанная в свое время Эйнштейном, Подольским и Розеном (ЭПР алгоритм), позволяет передавать сообщения по квантовому каналу – без непосредственной связи между передатчиком и приемником! Однако один Бит информации должен быть при этом передан по классическому каналу.

Основные постулаты квантовой информатики были сформулированы Эрвином Шредингером в 1935 году в его фундаментальной работе:

1. Schrödinger E *Naturwissenschaften* **23** 807, 823, 844 (1935) [Перевод на русск.: *Успехи химии* **5** 390 (1936); [перевод на англ.: *Proc. Am. Philos. Soc.* **124** 323 (1980)]

Тема 1.Квантовая информатика. Введение.

В работе Шрёдингер анализирует "подводные камни" в описании квантовомеханических процессов измерения и формулирует четыре основных положения, которые сводятся к тому, что состояния объектов квантового мира обладают следующими свойствами:

1. *Суперпозиции*. Состояния описываются линейной суперпозицией базисных состояний.
2. *Интерференции*. Результат измерений зависит от относительных фаз амплитуд в этой суперпозиции.
3. *Entanglement* ("*перепутывания*", "*взаимосопряженности*", "*сцепленности*"). Полное знание о состоянии всей системы не соответствует такому же полному знанию о состоянии ее частей.
4. *Неклонируемости и неопределенности*. Неизвестное квантовое состояние невозможно клонировать, а также наблюдать без его возмущения.

Разберем каждый из четырех постулатов

Тема 1. Парадокс кота Шредингера

2.1. Суперпозиция, парадокс шрёдингеровского кота

Квантовый объект, в отличие от классического, изначально статистический. Однако вероятностный характер квантового объекта не сводится к классически воспринимаемой неопределенности, связанной, например, с неполнотой знания об объекте. Для описания квантового объекта используется понятие *состояние*. Говоря, что объект находится в определенном состоянии, подразумевают, что можно представить к рассмотрению список, каталог (в терминах Шрёдингера), или, что то же самое, волновую функцию, вектор состояния, или матрицу плотности, которые содержат информацию о возможных результатах измерений над этим объектом. Поскольку результаты измерений над объектом, приготавливаемом в одном и том же состоянии, в общем случае меняются от измерения к измерению, вектор состояния должен давать и дает статистическую информацию (функции распределения) результатов ансамбля тех или иных измерений.

Простым примером служит вектор состояния системы, обладающей двумя ортогональными состояниями $|1\rangle$ и $|2\rangle$, например, энергетическими. Состояние такого объекта описывается вектором состояния (волновой функцией)

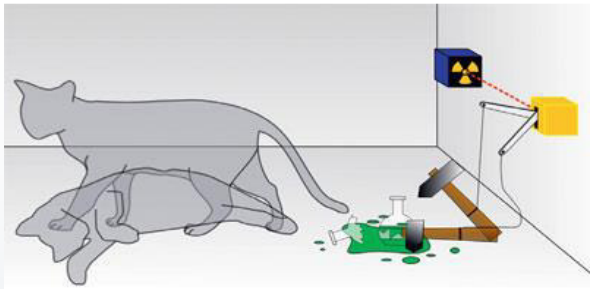
$$|\Psi\rangle = \alpha|1\rangle + \beta|2\rangle\,, \qquad (1)$$

Тема 1. Парадокс кота Шредингера

этот эксперимент Шрёдингером описан так:

«Некий кот заперт в стальной камере вместе со следующей адской машиной (которая должна быть защищена от прямого вмешательства кота): внутри счётчика Гейгера находится крохотное количество радиоактивного вещества, столь небольшое, что в течение часа может распасться только один атом, но с такой же вероятностью может и не распасться; если же это случится, считывающая трубка разряжается и срабатывает реле, спускающее молот, который разбивает колбочку с синильной кислотой. Если на час предоставить всю эту систему самой себе, то можно сказать, что кот будет жив по истечении этого времени, коль скоро распада атома не произойдёт. Первый же распад атома отравил бы кота. Пси-функция – волновая функция системы (уравнение, описывающее квантовое состояние системы) в целом будет выражать это, смешивая в себе или «размазывая» живого и мёртвого кота в равных долях...

В подобных случаях неопределённость, первоначально ограниченная атомным миром, преобразуется в макроскопическую неопределённость, которая может быть устранена путём прямого наблюдения. Это мешает нам принять “модель размытия” как отражающую действительность. Само по себе это не означает ничего неясного или противоречивого. Есть разница между нечётким или расфокусированным фото и снимком облаков или тумана».



Кот Шрёдингера не жив и не мёртв

Состояние радиоактивного атома описывается суперпозицией, то есть смешением двух состояний — распавшегося и не распавшегося. Следовательно, кот и жив, и мёртв одновременно. Но если кто-то откроет крышку (осуществит наблюдение), то квантовое состояние суперпозиции разрушится и наблюдатель увидит либо живого, либо мёртвого кота.

Тема 1. **Классические и квантовые приборы**

1. Классические и квантовые приборы

Лазерная техника основана на знании квантовых спектров электронов в газах, полупроводниках и диэлектриках.

К в а н т о в а я теория зонной структуры спектров электронов в полупроводниках служит базисом физикитранзисторов. Атомная энергетика построена на понимании квантовых законов строения атомного ядра.

Хотя функционирование лазеров и транзисторов основано на использовании квантовых свойств материи, эти приборы, тем не менее, чаще всего работают в классическом режиме. Действительно, токи электронов и напряжения на электродах транзисторов являются классическими величинами, полученными в результате усреднения по большому ансамблю частиц. Аналогично, когерентное лазерное излучение описывается законами классической электродинамики.

"Классичность" лазерного излучения обеспечивается наличием большого ансамбля квантов лазерного излучения. При переходе в режим одиночных фотонов (одноатомные лазеры) лазер становится квантовым прибором в том смысле, что не только его функционирование основано на квантовых законах, но и его излучение представляет собой квантовый объект, - например одиночный фотон. Транзистор в одноэлектронном режиме (так называемый баллистический режим транзистора) может стать квантовым прибором, если динамика электрона описывается квантовым уравнением Шрёдингера $i\hbar\frac{\partial\Psi}{\partial t}=\hat{H}\Psi.$

где $\hat{H}$ – гамильтониан системы.

ψ — комплексно-значная волновая функция

Тема 1. Парадокс кота Шредингера

Таким образом, один и тот же прибор может работать как в классическом, так и в квантовом режиме. Функционирование «классического прибора» описывается уравнениями классической физики для классических переменных.

Под «квантовым прибором» будем понимать прибор, работающий в квантовом режиме - означает, что динамика прибора описывается уравнением Шрёдингера для волновой функции. Аргументами волновой функции выступают квантовые переменные (координаты, импульсы, спины частиц). Волновая функция квантовой системы обладает квантовой когерентностью в том обычном смысле, что она способна к проявлению явлений интерференции при сложении различных компонент волновой функции. Свойство когерентности волновой функции, описывающей квантовый прибор, является его важнейшей отличительной чертой.

Законы классической и квантовой физики имеют принципиальные различия. Поэтому квантово-когерентные приборы и квантовые технологии имеют принципиальные отличия от классических приборов и технологий того же назначения.

1.2. Алгоритмы: классы их сложности

Чтобы решить задачу, компьютер, классический или квантовый, выполняет определенную последовательность операций (инструкций). Описание этой последовательности операций называется алгоритмом решения задачи.

Задача характеризуется ее размером n, равным, например, числу разрядов двоичного числа, над которым выполняется алгоритм.

Алгоритм реализуется некоторой схемой операций N_n зависящей от n; схема N_{n+i} получается из N_n на основе простых правил.

В теории сложности алгоритмов для классическихкомпьютеров принято разделять алгоритмы на эффективные и неэффективные.

Алгоритм относится к классу эффективных, если схема N_n состоит из полиномиального числа операций $O(n^d)$, где d — const, n — размер задачи. Время выполнения эффективного алгоритма возрастает с ростом размера задачи полиномиально: $t_n \propto n^d$

Используемым для решения задачи ресурсом является время работы компьютера. К другим ресурсам относятся объем памяти компьютера и (в случае квантового компьютера) точность выполнения операций. Эффективный алгоритм должен использовать полиномиальное количество ресурсов, являющихся ограниченными. Эффективные алгоритмы называются также полиномиальными (класс P).

Эффективным алгоритмам класса P противопоставляются неэффективные, требующие экспоненциально больших ресурсов (времени, памяти, точности). Например, если $t_n \propto 2^n$, алгоритм причисляется к неэффективным. Приме-ром задачи, для которой не найдено эффективного алгоритма решения на классическом компьютере, является задача о вычислении простых множителей больших *n*-разрядных чисел (задача о факторизации чисел).

Лучший известный вероятностный алгоритм для классических компьютеров требует числа операций:

$$2^{\alpha(n\log_2 n)^{1/2}}$$

В 1994 г. Петер Шор из Белл-Лаб построил алгоритм решения этой задачи на квантовом компьютере, который оказался полиномиальной сложности: необходимое число операций $O(n^2\log_2(\log_2 n \log_2\varepsilon^{-1}))$, где ε – вероятность ошибочного результата вычислений. Сенсационный результат - он опровергает эмпирический закон Чёрча-Тьюринга: все компьютеры эквивалентны в том смысле, что переход от одного компьютера к другому не изменяет класса сложности задачи. Закон был сформулирован для множества классических компьютеров. **Он нарушается, если используются квантовые компьютеры.**

Информация не является только математическим понятием. Наличие глубокой связи между физикой и информацией обнаруживается при сопоставлении термодинамической энтропии в физике и информационной энтропии Шеннона в теории информации: они совпадают с точностью до постоянного множителя.

Физическая теория информации включает в себя классическую и квантовую теории информации, а в более широком смысле (с включением соответствующих технических средств) - классическую и квантовую информатику. К замечательным достижениям классической теории информации относится решение парадокса с демоном Максвелла, нарушающим второй закон термодинамики. Парадокс исчезает, если учесть свойства процесса стирания информации: напомню сказанное в предыдущей лекции, что стирание 1 бита информации сопровождается затратой энергии $E_{\mathrm{SNL}} = kT \ln 2$ и возрастанием энтропии на $k \ln 2$ (принцип Ландауэра, IBM 1961). При $T = 300$ K энергия $E_{\mathrm{SNL}} \approx 0{,}017$ эВ $\approx 2{,}7 \times 10^{-21}$ Дж.

(E_{SNL} Shannon—von Neumann—Landauer, SNL)