

*Китайский иероглиф,  
означающий «кризис»,  
состоит из двух знаков:  
«опасность» и «возможность».*  
*Роберт Макки*



# Технологический кризис ИТ и прогнозы на будущее

В последние годы произошел потрясающий прогресс в информационных технологиях. За 20 лет быстродействие вычислительной техники увеличилось в 1000 раз, пропускная способность каналов возросла в 10000 раз, уже более 30 лет действует закон Мура (удвоение плотности активных элементов на кристалле каждые полтора года).

45 лет тому назад были заложены основы Интернет, который изменил более чем на порядок одну из важнейших переменных, определяющих темп научно-технического прогресса: задержку между моментом появления новой научной идеи или факта и временем, когда эти данные становятся доступны всем заинтересованным лицам. Число объектов в Интернете продолжает увеличиваться (рис. 1). Число Интернет-объектов сегодня превысило 4 млрд. На одного человека приходится ~1–3 Интернет-объекта.

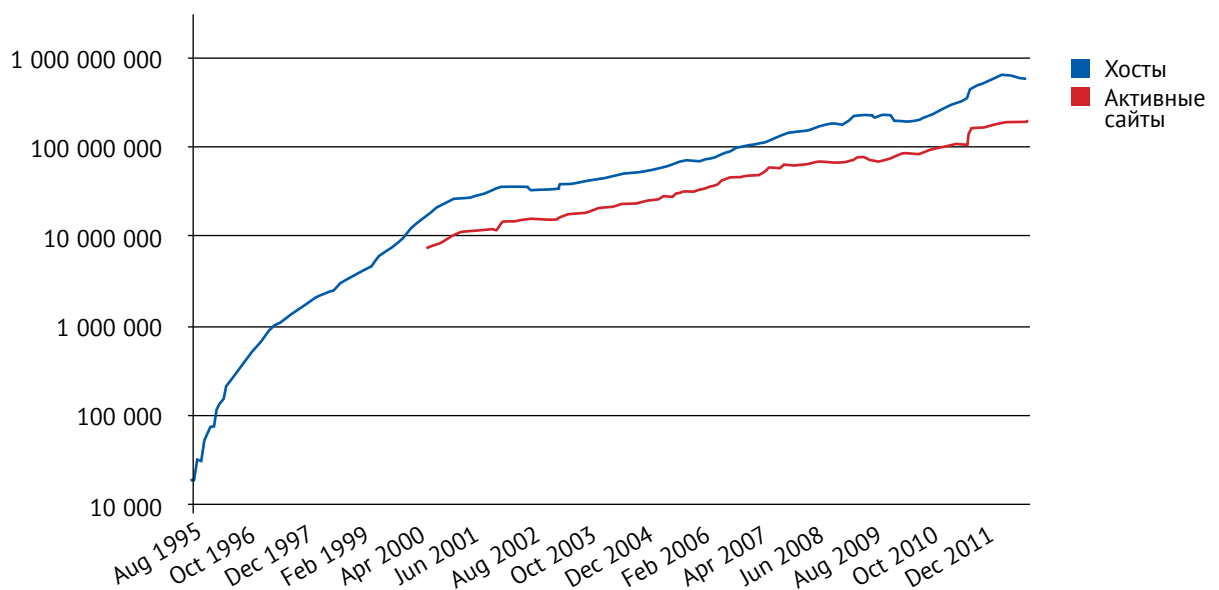
Уместно задать вопрос: можно ли ожидать аналогичный темп развития в дальнейшем? К сожалению, ответ на него будет, скорее всего, отрицательным, если ориентироваться на существующие технологии. Причем ожидается, что критических значений технологии достигнут уже весьма скоро – в 2020–2025 годах.



#### Юрий Семенов

Заместитель заведующего кафедры «Телекоммуникационные сети и системы» МФТИ, заместитель заведующего кафедры «Информатики» ФНТИ МФТИ, начальник лаборатории «Инфокоммуникационных технологий» Института теоретической и экспериментальной физики (ИТЭФ)

**Рис. 1.**  
Рост числа узлов WWW  
в 1994–2012 гг.



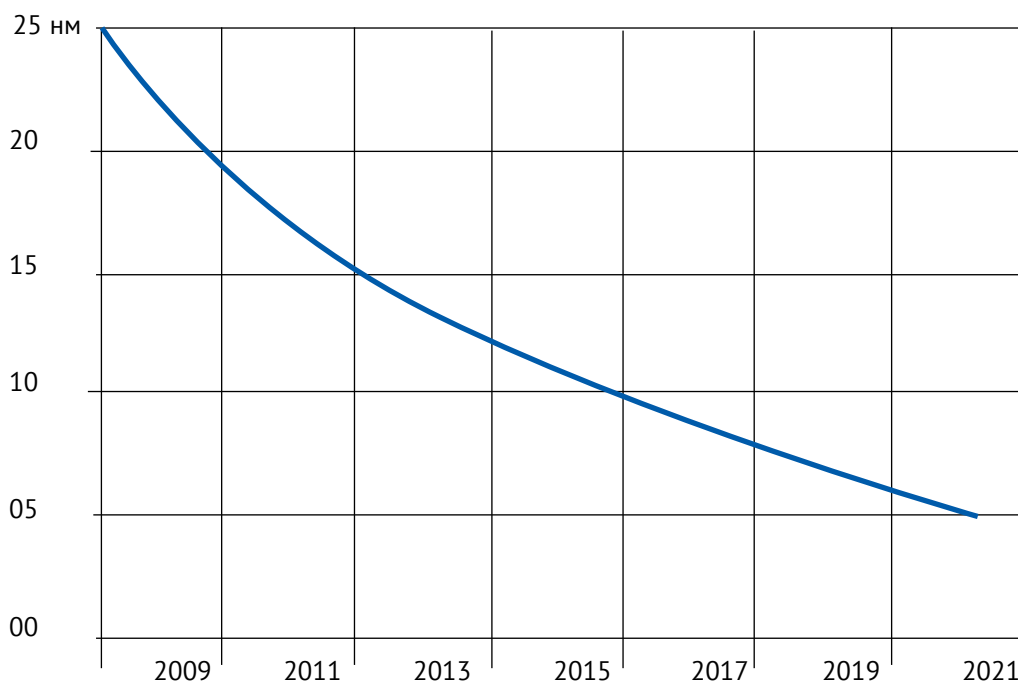
## Ограничения роста мощности вычислительных систем

Первая и одна из самых важных причин технологического кризиса – физические ограничения на дальнейший рост мощностей вычислительных систем. Тут можно выделить два фактора:

- ограничения разрешения технологического процесса производства полупроводников;
- ограничения роста частоты.

**Разрешение технологического процесса производства полупроводников.** Используемая технология на кремнии позволяет работать с разрешением ~15 нм. На подходе мемристоры и графеновые транзисторы (5 нм), но постоянная кристаллической решетки кремния ~0,1 нм. Да и совместить технологию на кремнии с графитом будет непросто. Понятно, что запас повышения разрешения менее 10, и при темпе, определяемом законом Мура, возможности роста будут исчерпаны уже к 2020 году (на рис. 2 показана ситуация с возможностями технологического процесса полупроводникового производства на сегодняшний день и прогноз на будущее при условии, что закон Мура останется справедливым). К 2020 году технология выйдет на разрешение порядка 5 нм (флэшки на мемристорах не в счет, так как там высокая однородность структуры), но для размеров <5 нм возникнут проблемы отношения сигнал–шум. Недаром квантовые компьютеры работают при температуре 0,01 кельвина. Заметьте, это ограничение не технологии, а физики; ограничение дальнейшего роста плотности элементов на кристалле процессора связано не с технологией, а с физикой.

Аналогичное ограничение есть и в технологиях хранения информации. Традиционные системы памяти большого объема базируются, в основном, на жестких дисках. Это накладывает определенные ограничения на время доступа к данным. Со временем альтернативой им могут стать твердотельные системы памяти. У этих устройств время выборки может быть в 100 раз меньше, чем у HDD. Но твердотельные системы памяти пока обеспечивают ограниченное число циклов записи/чтения (~10 000), да и удельная стоимость их пока выше, чем у традиционных жестких дисков.



**Рис. 2.**  
Эволюция разрешения нанотехнологий

**При темпе, определяемом законом Мура, возможности роста будут исчерпаны уже к 2020 году**



Повышение емкости памяти вызывает миниатюризацию ячеек памяти, а уменьшение размера уменьшает заряд, там хранящийся, что приводит к ухудшению отношения сигнал–шум. Неслучайно первый квантовый компьютер работает при температуре 10 мК<sup>0</sup>.

Замечу, что прогресс в области цифрового ТВ и DVD-видео был связан с повышением эффективности сжатия информации. Алгоритмы сжатия данных без потерь вышли на энтропийный предел еще около 10 лет назад.

**Рост частоты.** Тактовая частота процессора достигла 5 ГГц, и заметный дальнейший рост проблематичен. По этой причине уже в 2004 году производители процессоров перешли на многоядерную схему. Но и здесь ресурсы не беспредельны – уже сегодня на кристалле около 70 % поверхности занимают проводные соединения между активными элементами, да и делать кристаллы размером с книгу вряд ли целесообразно. Кроме того, производительность вычислений растет в среднем пропорционально логарифму числа процессоров.

Ярким примером сложившейся ситуации может служить рекордсмен супер-ЭВМ (10 петафлоп/с, Fujitsu, Япония), которая занимает 800 стоек и требует для своего питания и охлаждения 5 МВт (это мощность первой АЭС в Обнинске). А это самая энергоэффективная машина на сегодняшний день (2,2 Гфлопс/Вт). Чем же будет супер-ЭВМ следующего поколения – машиной размером с небольшой город?

К слову, в 2005 году вычислительные машины потребляли 1,2–1,5 % производимой в США энергии. Большая часть из этой доли приходится на настольные машины и небольшие серверы. Известно, что полезная мощность составляет примерно половину

всех энергозатрат. Вторая часть представляет собой потребление вспомогательных структур вычислительного центра, включая системы питания и охлаждения. Именно столь высокий объем энергопотребления привел к формированию направления green computing.

### Проблемы надежности

Следующий важный фактор – проблемы надежности. Человечество уже не может жить без машин и сетей. Машины управляют потенциально опасными технологиями, авиалайнерами, энергетическими системами, проектируют новые лекарства, на очереди встраивание чипов в человеческий организм и т.д. Но ведь машины и используемое ими программное обеспечение имеют конечную надежность. Среднее число ошибок (после отладки) на 1000 строк кода для современного ПО равно 15–50. Для Linux это число равно 7. Продукты Microsoft после отладки характеризуются цифрой около 0,5 ошибок на 1000 строк кода<sup>1</sup>. Современное ядро ОС содержит от 50 до 250 млн. строк кода (Windows XP содержит около 50 млн. строк). Значит, на любом компьютере имеется 1000–50 000 программных ошибок. Согласно существующим оценкам, в дистрибутиве Debian содержится около 3 млн. ошибок (на 350 млн. строк кода). А еще есть приложения...

По этой причине жизненно важным становится поиск решений, которые бы гарантировали приемлемый результат даже на ненадежной машине с ошибками в программном обеспечении. Замечу, что в 2000 году программы в автомобиле имели до миллиона строк кодов, к 2010 это число возросло в 100 раз, ожидается, что в 2020 г. программы в автомобиле будут содержать 10 млрд. строк кода. Разработчики программного обеспечения стремятся сделать программы более дружелюбными для пользователя. Но это ведет к их усложнению. Сформулирован закон Никласа Вирта (Niklaus Wirth), который гласит:

<sup>1</sup>Рекордно низкие значения имеют программные продукты NASA JPL (навигационные программы для космических объектов), имеющие 0.003 ошибки на 1000 строк кода.



**Жизненно важным становится поиск решений, которые бы гарантировали приемлемый результат даже на ненадежной машине с ошибками в ПО**

**Новое поколение программы требует настолько больших ресурсов, что она работает медленнее, чем старая.**

То есть скорость работы новых программ понижается быстрее, чем увеличивается быстроедействие вычислительного оборудования. При этом усложнение программ делает их уязвимее, а требование к их надежности растет день ото дня.

## Проблемы объема информации

Объем информации увеличивается очень быстро. В 2000 г. полный трафик Интернет составлял более 1 эксабайта, а в 2010-м достиг 256 эксабайт, что соответствует темпу роста в 70 % в год. По оценкам журнала Economist объем данных каждый год увеличивается на 60 %. Эта точка зрения подтверждается аналитиком компании IDC, который предсказывает, что «цифровая вселенная» вырастет до 1,8 зетабайт (10<sup>21</sup> байт) в 2011-м, то есть на 47 % по отношению к 2010 г., и превысит 7 зетабайт к 2015-му. 1 зетабайт эквивалентен содержанию 50 библиотек Конгресса США. В 2020 году будет генерироваться в 200 раз больше данных, чем в 2008 году. Более того, ожидается, что стоимость определения генома отдельного человека составит около 100 долларов, и это добавит к содержанию медицинской карты еще несколько гигабайт

В связи со столь значительным ростом возникают два вопроса:

- 1. Где хранить эту информацию?** Ожидается, что к 2020 году память будет стоить \$0,5 за терабайт. Однако, несмотря на все более дешевую память, зазор между потребностями и возможностями со временем только увеличится (200 петабайт в год). Рост информационных объемов и доступной памяти показан на рис. 3. Причин такому отставанию много. Это и оцифровка библиотек и архивов, создание разнообразных баз данных, видеозапись мониторинга (банкоматы, эскалаторы метро, банки), частные аудио- и видеотеки и т.п. Активная эволюция мобильных средств еще более усугубит проблему. **Чтобы сохранить существующий стиль жизни, к 2020 году человечеству потребуется еще одна планета!**



**Только 15 % компаний способны эффективно использовать данные и такая ситуация сохранится до 2015 года**



**Рис. 3.** Рост потребности и возможности хранения информации.

**Таблица 1.**  
Распределение объемов  
данных, хранимых  
компаниями, по отраслям.

| Отрасли                             | Сохраненные данные<br>в 2009 году, петабайт | Среднее количество данных<br>на компанию <sup>1</sup> , терабайт |
|-------------------------------------|---|--|
| Дискретное производство             | 966   | 967  |
| Государственное управление          | 848   | <b>1312</b>  |
| Медиа и коммуникации                | 715   | <b>1792</b>  |
| Непрерывное производство            | 694   | 831  |
| Банковские услуги                   | 619   | <b>1931</b>  |
| Здравоохранение                     | 434   | 370  |
| Услуги безопасности<br>и инвестиций | 429   | <b>3856</b>  |
| Профессиональные услуги             | 411   | 278  |
| Розничная торговля                  | 364   | 697  |
| Образование                         | 269   | 379  |
| Страховые услуги                    | 243   | 870  |
| Транспорт                           | 227   | 801  |
| Дистрибуция                         | 202   | 535  |
| Энергетика                          | 194   | <b>1507</b>  |
| Добыча природных ресурсов           | 116   | 825  |

**2. Как ее использовать?** Количественный рост объемов и потоков данных привел к проблеме нахождения нужной информации в хранилищах и выделения ее в потоках. Для решения проблемы нахождения нужной информации в хранилищах разработана специальная разновидность баз данных NoSQL.

Появился термин «технологии больших объемов данных» (Big Data Technologies) – это новое поколение технологий и архитектур, разработанных для эффективного извлечения нужной информации из гигантских объемов данных, относящихся к различным типам. Не следует думать, что большие объемы данных – это то, с чем имеет дело только Google или Facebook. В таблице 1 показано распределение объемов данных по отраслям в США в 2009 году.

По оценкам 90 % данных, генерируемых в 2012 году, являются неструктурированными (видео, изображения и WEB). И только 15 % компаний способны эффективно использовать данные. Предположительно такая ситуация сохранится до 2015 года. Доклад Gardner за 2011 год утверждает, что 40 % бизнес-трафика в США не имеет никакого отношения к бизнесу. 42 % всех корпоративных данных оказываются задублированными, съедая ресурсы компании.

<sup>1</sup>Учитывались компании,  
в которых более 1000  
сотрудников.

### Информационная емкость потока информации

Потоки информации растут, но можно ли утверждать, что информация, содержащаяся в 1 гигабайте, в 1000 раз больше мегабайта? Среднее количество информации  $E$  на один произвольный символ (или сообщение) равно:

$$E = -\sum_i p_i \log_2 \left( \frac{1}{p_i} \right),$$

где  $p_i$  – вероятность появления  $i$ -го символа (или сообщения).  $\log_2 (1/p_i)$  определяет число бит, характеризующих данную информацию (сколько бит мы должны послать, чтобы передать эту информацию). Отсюда следует, что сообщение, которые имеют большую вероятность, несут в себе меньше информации. Пожалуй, интерес людей к сенсациям диктуется интуитивным стремлением получить информационно более емкий материал.

## Проблемы безопасности

**В 2012 году доходы киберпреступников превысили доходы от наркотрафика.** Более тысячи различных типов атак угрожают смартфону или планшетному ПК, с которыми вы работаете. Новую атаку можно ожидать каждый день. **Вследствие полиморфности современные антивирусные системы детектируют только 24 % всех вредоносных кодов.** Это обстоятельство понижает эффективность IDS/IPS-защиты. В последнее десятилетие многообразие вредоносных кодов ежегодно увеличивалось на 50 %. В день появляется 50 000 новых сигнатур в дополнение к 6–20 млн. уже известных. В докладе 2012 WEB Security Report (Blue Coat) сообщается об увеличении числа вредоносных сайтов на 240 %, в среднем любая организация ежемесячно сталкивается с 5000 новыми угрозами. Компания считает, что пришло время унификации и стандартизации средств противодействия сетевым атакам и защиты данных.

Сетевая безопасность находится в состоянии близком к хаосу. 70 % часто посещаемых WEB-сайтов содержат вредоносные коды и заражают посетителей. Рекордный размер botnet достиг 12 млн. машин. Впрочем, самая большая botnet – это совокупность машин с ОС Windows (ведь мы не знаем, какие программы туда заносятся при автоматическом обновлении ОС). После того как поставщики годами продавали точечные решения, закрывающие отдельные проблемы, но не гарантирующие безопасности, а атакеры имели практически полную свободу, нечего удивляться тому, что они преуспели. От многих атак просто нечем защититься. Последние полтора года постепенно возникло понимание проблемы. Стало ясно, что нужны стандарты для безопасности, а предлагаемые решения должны быть масштабируемыми. Ожидаемый прирост инвестиций в компьютерную безопасность составляет 9,6 %.

Гари Дэвис (Gary Davis) из фирмы McAfee привел пример, когда система водоснабжения Южной Калифорнии наняла хакера проверить надежность ее сети управления. Хакер за час добился доступа и полного контроля над системой и осуществил добавление оговоренных химических веществ в воду. Это иллюстрирует, насколько уязвимы современные системы управления. Возможно, столь критические для жизни системы не должны иметь доступа через Интернет, однако и это не гарантирует полной безопасности.

В 2008 году в мире использовалось 350 млн. USB-флэш модулей памяти, что создает определенные угрозы. За последние два года 52 % предприятий пострадали от утраты конфиденциальных данных, хранившихся на USB-драйвах. Например, компьютеры Международной космической станции были заражены вирусом через флэш-память. На рынке появились приборы, которые требуют аутентификации для доступа к таким устройствам.

Тенденции в мире киберпреступности очень тревожны. Формируются стабильные киберармии. Например, Iranian Cyber Army, Pakistan Cyber Army, ChinaHonker Group и т.д. Создаются такие группы в Палестине, Северной и Южной Кореех и некоторых других государствах. Во многих странах в 2012 году продолжилась разработка новых видов кибероружия и средств противодействия. Понятно, что страны с продвинутой ИТ инфраструктурой более уязвимы. В США в июле 2011 создан Department of Defense Strategy for Operating in Cyberspace и начата разработка доктрины кибербезопасности.

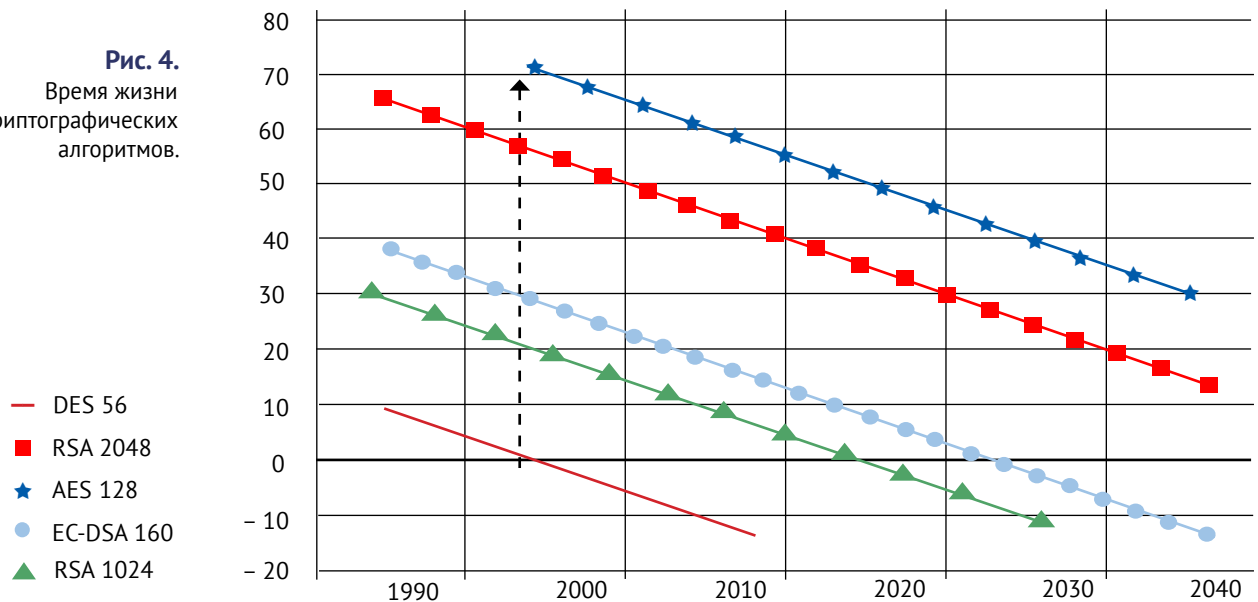
Еще один аспект безопасности. Дело идет к тому, что любая информация, как хранящаяся, так и передаваемая, будет криптографически защищена. Но для алгоритмов защиты не доказаны теоремы криптографической прочности. Прогнозируемое время жизни криптографических алгоритмов показано рис. 4<sup>3</sup>. А современные вычислительные технологии, в частности графические процессоры, сокращают срок жизни криптографических ключей. С учетом этого обстоятельства кривые можно опустить вниз на 10 единиц.



**В день появляется 50 000 новых сигнатур в дополнение к 6–20 млн. уже известных, сетевая безопасность близка к хаосу**

<sup>3</sup>Network Security, Issue 12 (декабрь) 2004.

**Рис. 4.**  
Время жизни  
криптографических  
алгоритмов.

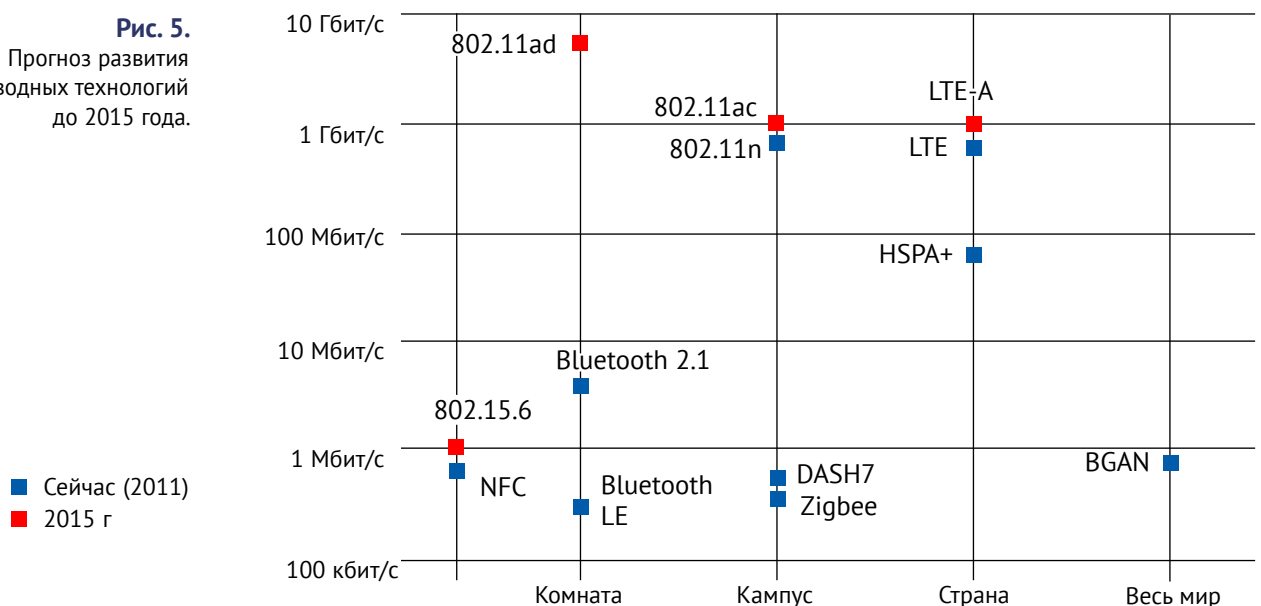


### Технологические тенденции

При всем этом ИТ развивается так, как будто не видит этих тенденций. Прогнозируются, что процессоры будут встроены в различные окружающие нас предметы. Изображение экрана будет проектироваться с помощью специальных очков непосредственно на глазное дно, а сенсорная клавиатура будет проектироваться на любые поверхности, которые окажутся под рукой. Активно развиваются беспроводные технологии (рис. 5.). В последние два года появились сообщения о внедрении техники OpenFlow (сетевая технология нового поколения), Bitcoin (новая платежная система), NFC, управление голосом, многопортовые приложения (P2P, Skype и др.) и т.д.

В последние годы появляется все больше сообщений о разработках интерфейса между человеческим мозгом и компьютером (Brain-Computer Interfaces for Communication and Control, BCI). Такие интерфейсы пытаются использовать для управления протезами конечностей человека и даже для восстановления зрения. Но им найдется применение и в системах управления, где выполнение той или иной операции может быть инициировано мыслью человека. Первые сообщения о BCI относятся к 1970-м годам (Jacques Vidal of the University of California). Суть технологии в том, что электрические сигналы, генерируемые мозгом (электроэнцефалограмма), считываются, усиливаются, фильтруются, анализируются и используются для целей управления. Эти операции и выполняют

**Рис. 5.**  
Прогноз развития  
беспроводных технологий  
до 2015 года.





BCI. Сигналы мозга можно получать с помощью электродов, установленных на коже головы. Хотя в этом случае электроды и мозг разделяют кости черепа и скальп, получаемые сигналы оказываются детектируемыми. Разумеется, эти электроды воспринимают сигналы не только мозга, но и, например, наводки силовой сети переменного тока.

Но как же те тенденции о которых мы говорили выше? Исходя из приведенных выше тенденций, можно сформулировать наиболее важные направления разработок будущих информационных технологий:

1. язык для описания проблемы, а не алгоритма ее решения;
2. средства для выявления некорректных решений и блокировка их реализации;
3. надежные системы сертификации и верификации программ;
4. разработка мультимедийных поисковых систем;
5. разработка методов объективной оценки количества информации;
6. безопасные и надежные ОС для целей SCADA; программы для роботов;
7. распределенные системы управления потенциально опасными производствами;
8. разработка надежных алгоритмов распознавание сетевых атак нулевого дня;
9. моделирование работы биологических объектов, включая органы человека (например, биомолекул в качестве ячеек памяти);
10. искусственный интеллект.

### Компьютеры на новых принципах

Емкость памяти современных машин (~1 Тбайт) по порядку величины сравнялась с числом нейронов в мозге человека. Сигналы в человеческом теле распространяются со скоростью менее 130 м/с. Машины же выполняют миллион миллиардов операций в секунду, но конкурировать с человеком при выполнении творческих заданий пока не могут. Видимо для этого необходимы какие-то другие принципы их организации. В 2011 году на рынке появился первый квантовый компьютер. Он умеет распознавать фотографии известных достопримечательностей. При этом он занимает площадь 10 кв. м, работает при температуре  $T=0,01$  К0 и на привычный нам компьютер не похож.

