В.Д. Мунистер

Компьютерные сети

IoT & межмашинное взаимодействие

Издание Первое

Учебно-теоретическое издание

«Компьютерные сети. IoT и межмашинное взаимодействие»

Хрестоматия

2020 г.

GLÜCKSRITTER
MUNISTER

§ INSCRIPTUM

Вторая половина XX века подарила человечеству великое множество замечательных достижений в области цифровой электронной вычислительной техники - технической базы информационных технологий (ИТ). Благодаря появлению компьютеров информация, которой владеет человечество, стала своеобразным "сырьем" для производства множества "продуктов": новых знаний, управленческих решений, научных прогнозов, статистических сведений, всевозможных рекомендаций, заключений и т.д. Причем, в отличие от физического сырья (полезных ископаемых и др.), информация по мере использования не только не исчезает, а наоборот, пополняется новой, являя собой неисчерпаемую "сырьевую" базу интеллектуального труда.

Современными успехами компьютеризации и информатизации мировое сообщество обязано миллионам тружеников - ученым, инженерам, рабочим, создавшими новые поколения компьютеров, их программное обеспечение, мощные информационные сети.

Однако тех, кто закладывал фундамент компьютерной науки и техники, было не так много. На их долю выпало самое трудное - создать то, чего еще никогда не было. Среди них были ученые, инженеры и математики многих стран. Вторая мировая война и последовавшие за ней десятилетия "холодной" войны привели к разобщению ученых и засекречиванию работ, поскольку компьютеры (электронные вычислительные машины ЭВМ) - создавались прежде всего для военных целей.

Вследствие этих факторов имена создателей вычислительной техники и их творческий вклад были известны лишь узкому кругу специалистов.

За рубежом в странах Западной Европы и США этот пробел в литературе о становлении и развитии цифровой электронной вычислительной техники уже восполнен. Здесь появилось много книг, статей в периодических изданиях, созданы музеи с экспонатами ЭВМ первых поколений.

В странах бывшего Советского Союза этот процесс затянулся. Лишь в поздние девяностые и нулевые годы двадцать первого века, то есть, уже в наше время, началось рассекречивание многих ранее выполненных в данной отрасли работ и появилась возможность исследовать и оценить огромный творческий вклад ученых, инженеров, производственников в мировой процесс становления и развития вычислительной техники, информатики, ИТ.

И я хочу посвятить это учебно-теоретическое издание этим людям: родоначальникам компьютерных наук. Это необходимый шаг, так как многие из тех, кто будет упомянут, получили признание, выраженное в виде медали «Пионера компьютерной техники» (англ. Computer Pioneer Award) - самой престижной награды Компьютерного общества IEEE уже посмертно.

К сожалению, наш с вами Нобель или Пулитцер, стал вручаться относительно недавно – всего тридцать с небольшим лет назад. Да и к тому же, вручается он за выдающиеся достижения в компьютерных науках, с условием, что основной вклад должен был быть совершён более пятнадцати лет назад. Таким образом, медаль, выполненная из бронзы, на аверсе медали выполнен барельеф Чарльза Бэббиджа, является примерно тем, чем для художника признание – невероятной редкостью при жизни.

Я хочу начать с наших соотечественников, людей, говоривших на русском языке, сделавших так много, чтоб в конце концов стереть все границы и барьеры, стоящие на пути мгновенного и общедоступного общения между людьми, посредством информационных технологий. К сожалению, формат книги не позволит рассказать историю их жизни, трудовых и научных и даже боевых подвигов, голодных и бессонных дней, но не назвать их, я их не могу. Так как благодарен всем им своим основным призванием по жизни.

Эта книга посвящается: Лебедеву Сергею Алексеевичу, Ляпунову, Алексею Андреевичу, Глушкову Виктору Михайловичу, Лопато Георгию Павловичу, Столярову Геннадию Константиновичу, Никлаусу Вирту, Линусу Торвальду, Фридриху Бауэру, Питеру Науру, Джону Атаносову, Артуру Самуэлю, Маршиану Хоффу, Килби Джеку, Эриху Блоху, Кену Олсену, Рейнолду Джонсону, Дугласу Энгельбардту, Алану Перлису, Гради Бучу, Эдварду Фейгенбауму, Джину Бартику, Ирвину Джону Гуду, Кену Томпсону, Томасу Курцу, Джону Макарти, Айленду Сазерленду, Джеффри Чуан Чу, Барбаре Лисков, а также всем сотрудникам Института инженеров электротехники и электроники — IEEE и членам «Зала Славы Интернета».

Мунистер В.Д.

§ СОДЕРЖАНИЕ

Содержание курса. Система интер-отклика посредством QR.

Данное издание предназначено для восполнения недостающих теоретических знаний по дисциплинам, междисциплинарным курсам, связанных с принципами организации межсетевого взаимодействия, архитектуры информационных систем: («Организация, принципы построения и функционирования компьютерных систем», «Математический аппарат для построения компьютерных систем», «Дизайн архитектуры распределенных сетей», «Инфокоммуникационные системы и сети», «Информационные технологии», «Внедрение и поддержка программного обеспечения компьютерных систем», «Компьютерные и телекоммуникационные сети») студентов, осваивающих программы среднего и высшего профессионального обучения.

Получение недостающих знаний – серьезный инструмент общего процесса актуализации: поддержания практических и теоретических знаний индивидуума в актуальном состоянии, т.е. приведение их в соответствие с состоянием отображаемых объектов предметной области будущего специалиста в сфере информационных технологий и вычислительной техники. Я отождествляю вкладываемый смысловой контекст данной книги с понятиями необходимого и достаточного условий — известных вам по изучаемым математическим дисциплинам.

Учебное издание «Компьютерные сети. IoT и межмашинное взаимодействие» и выступает в роли достаточного условия процесса снятия информационной энтропии, касающегося профессионального ориентирования студентов вышеперечисленного профиля подготовки.

Издание содержит в себе ряд перспективных т.н. «Рабочих предложений» (RFC) от IETF, IEEE, и иных организаций, занимающихся сертификацией технологий в рассматриваемой области человеческой деятельности, а также статей с верифицированных иностранных и отечественных научных и публицистических изданий. Часть информации подана в явном компрессированном виде, и неявном – полноценном. Все это достигается за счет внедрения на страницы издания печатных QR-кодов с ссылками на те или иные интернет-ресурсы. Таким образом, книга получает куда более расширенное функционально-интерактивное предназначение.

Надеюсь, что тщательно подобранные, переработанное и адаптированные к чтению, материалы данного учебного курса (вместе с планируемым дополнением, выраженным в виде курса лабораторных работ в сетевом эмуляторе Cisco Packet Tracer) станут путеводной звездой для поколения новых инженеров – архитекторов Интернета завтрашнего дня.

От ARPANET до модели OSI/ISO.

Мы можем назвать имена создателей парового двигателя, самолёта или кинематографа. Однако в создании сети Интернет принимали участие множество блестящих учёных и коллективы целых университетов. Технология развивалась достаточно медленно, поэтому в разные годы вклад в становление «глобальной паутины» вносили самые разные люди. Как и большинство других, передовых для своего времени технологий, Интернет появился как военная разработка. Первые попытки создать беспроводное средство связи начались в самый разгар холодной войны. Руководство США было обеспокоено успехами СССР в освоении космоса. По мнению ряда американских военных специалистов, космические технологии сделали бы Советский Союз абсолютно неуязвимым в случае вооруженного столкновения. Поэтому сразу после успешного запуска советского «Спутника-1» в 1957 году, в Америке начались разработки новой системы для передачи данных. Все исследования велись под эгидой Министерства обороны США и держались в глубочайшем секрете. В создании новой технологии принимали участие технические кафедры лучших университетов страны.

В 1962 году сотрудник Массачусетского университета, по совместительству работавший в Управлении перспективными исследовательскими проектами при Министерстве обороны США (ARPA), — Джозеф Ликлайдер — предложил своё решение проблемы. Ликлайдер полагал, что осуществлять связь можно через компьютеры. Под его руководством в 1960-е годы началась работа над проектом, получившим название ARPANET. Планировалось, что сообщения в такой сети будут передаваться целиком, но подобная передача имела несколько серьёзных изъянов: невозможность взаимодействия большого количества пользователей, дороговизна, неэффективное использование пропускной способности сети, неспособность нормально функционировать при разрушении отдельных компонентов сети. Над устранением этих недостатков стал работать учёный из Калифорнийского университета — Пол Бэран. Итогом его работы стал новый способ передачи информации — коммутация пакетов. Фактически каждое сообщение разбивалось на несколько пакетов, каждый из которых шёл к адресату по своему каналу. Благодаря этому техническому решению, новая сеть передачи данных становилась практически неуязвимой.

В конце 1969 года состоялось историческое событие — по ARPANET было передано первое сообщение.

Сеанс связи осуществлялся между Калифорнийским и Стенфордским университетами и увенчался успехом только со второй попытки.

Для того чтобы передать на расстояние 640 км короткое слово «login», потребовалось полтора часа. На тот момент к сети было подключено всего 4 компьютера, расположенные в разных университетах Америки.

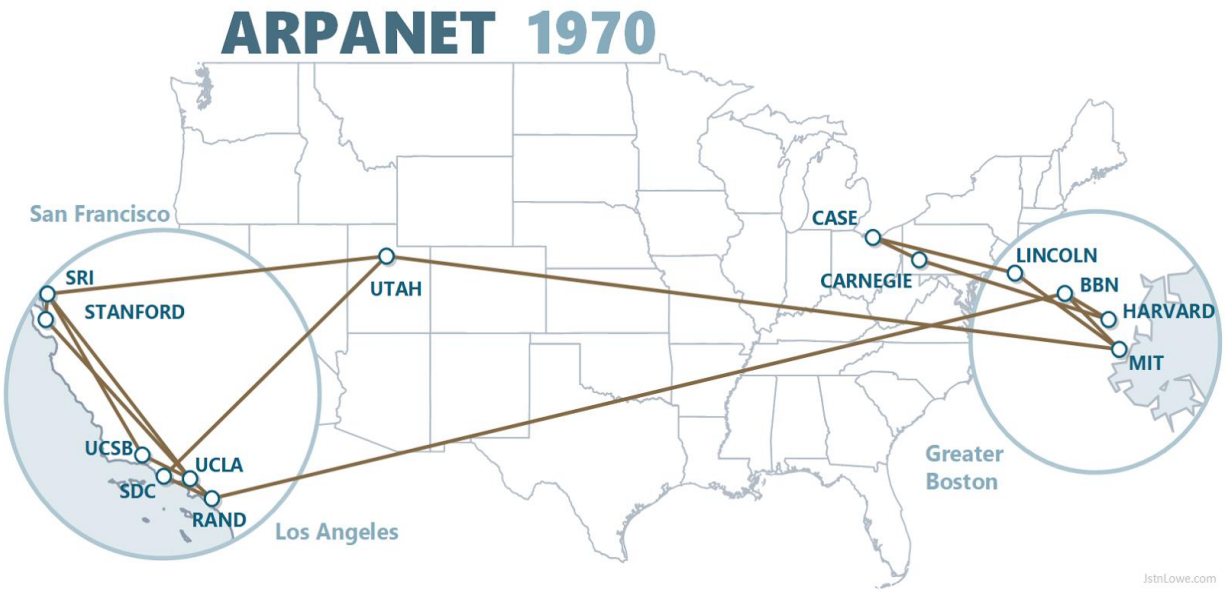


Рис. 1 – Сеть ARPANET в 1970м году.

К началу 1970-х была налажена электронная почта, позволяющая обмениваться сообщениями внутри сети. И в это же время интернет перестал быть исключительно американской системой. К сети подключились университеты Великобритании и Норвегии. По мере роста числа компьютеров в сети, их взаимодействие становилось всё более медленным и рассинхронизированным.

Налаживанием интеграции компьютеров в единую сеть занялся ещё один учёный, работавший в ARPA, — Винстон Сёрф. Сёрф разработал два протокола: протокол управления передачей (TCP); и дополнительный интернет-протокол (IP). Благодаря совместной работе двух протоколов, стало возможным наладить связи между множеством компьютеров, расположенных по всему миру.

В 1980-е годы ARPANET уже был достаточно удобным инструментом, с помощью которого между собой могли общаться университеты, научно-исследовательские лаборатории и институты. В 1984 году возникла система доменных имён. Каждому из компьютеров, включённых в сеть, было присвоено своё доменное имя. Со временем эта система изменилась: домен стал просто составной частью множества электронных адресов, а не именем конкретного устройства. Для удобства имена пользователя и домена стали отделять друг от друга символом — @.

Позднее появился и новый способ общения в сети: владельцы компьютеров могли не просто пересылать друг другу файлы, но и общаться в режиме реального времени в специальных чатах.

Для того чтобы упростить обмен электронной почтой в 1991 году появилась первая соответствующая программа. Однако всё это время Интернет оставался лишь набором каналов для передачи данных с одного компьютера на другой, и пользовались им только ведущие учёные Европы и США. Революционным решением, сделавшим Интернет достоянием всех владельцев компьютеров, стало появление и дальнейшее развитие системы WWW.

В начале 1990-х годов английский физик и программист Тим Бернерс-Ли начал работу над открытой системой, которая позволяла бы размещать в сети различные данные, таким образом, чтобы любой пользователь мог иметь к ним доступ. Изначально планировалось, что эта система позволит обмениваться нужной информацией учёным-физикам. Так появилась хорошо знакомая нам глобальная сеть — World Wide Web (WWW). Для размещения и поиска данных в цифровой сети потребовалось создание дополнительных инструментов: протокола передачи данных HTTP языка HTML. Ну а дальше…

И вот прошло еще два полных десятилетия. И количество подключенных устройств к глобальной сети – единой среде взаимодействия уже больше миллиарда. Значительно больше. На порядок. Десять миллиардов хостов – вопрос времени.

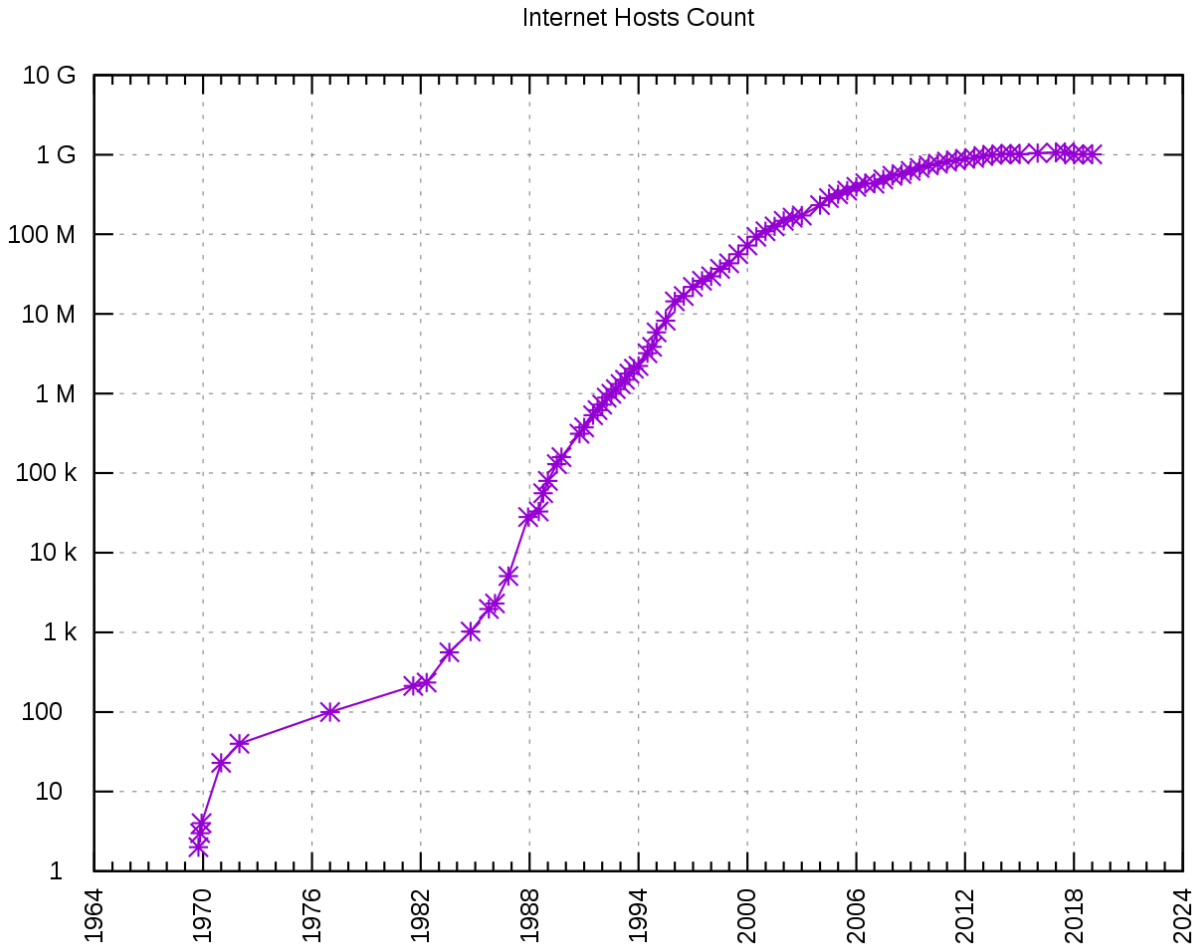


Рис. 2 - Количество Интернет-узлов по всему миру (логарифмическая шкала)

Если в 1970ом году, еще в пору становления ARPANET, было четыре узла, то сейчас их столько, что их количество можно подсчитать лишь по косвенным признакам. Для всей этой громады необходимо было предусмотреть программную, а как следствие, и аппаратную платформу взаимодействия, работающую по единому признаку. И не просто предусмотреть… А и внедрить. На базисе предустановленности.

Ведь, еще, в карикатуре Питера Штейнера, опубликованной 5 июля 1993 года на страницах литературно-публицистического еженедельника «The New Yorker» был подчеркнут самый интересный атрибут нового явления нашей жизни, заключающейся в фразе: «В Интернете никто не знает, что ты собака».

Данную фразу можно интерпретировать по-разному. Понятно, что речь идет не только об анонимности. Напрашиваются как вполне логичные и явные, так и не совсем, аллегории и суждения. Но мало кто вспоминает, что именно WWW десакрализировал роль человека в управлении – по его же и согласию. Вычислительные машины общаются между собой даже тогда, когда мы об этом и не просим. Благодарить за это надо общепринятую эталонную модель межсетевого взаимодействия OSI/ISO, и, термин, известный каждому, а именно «протокол».

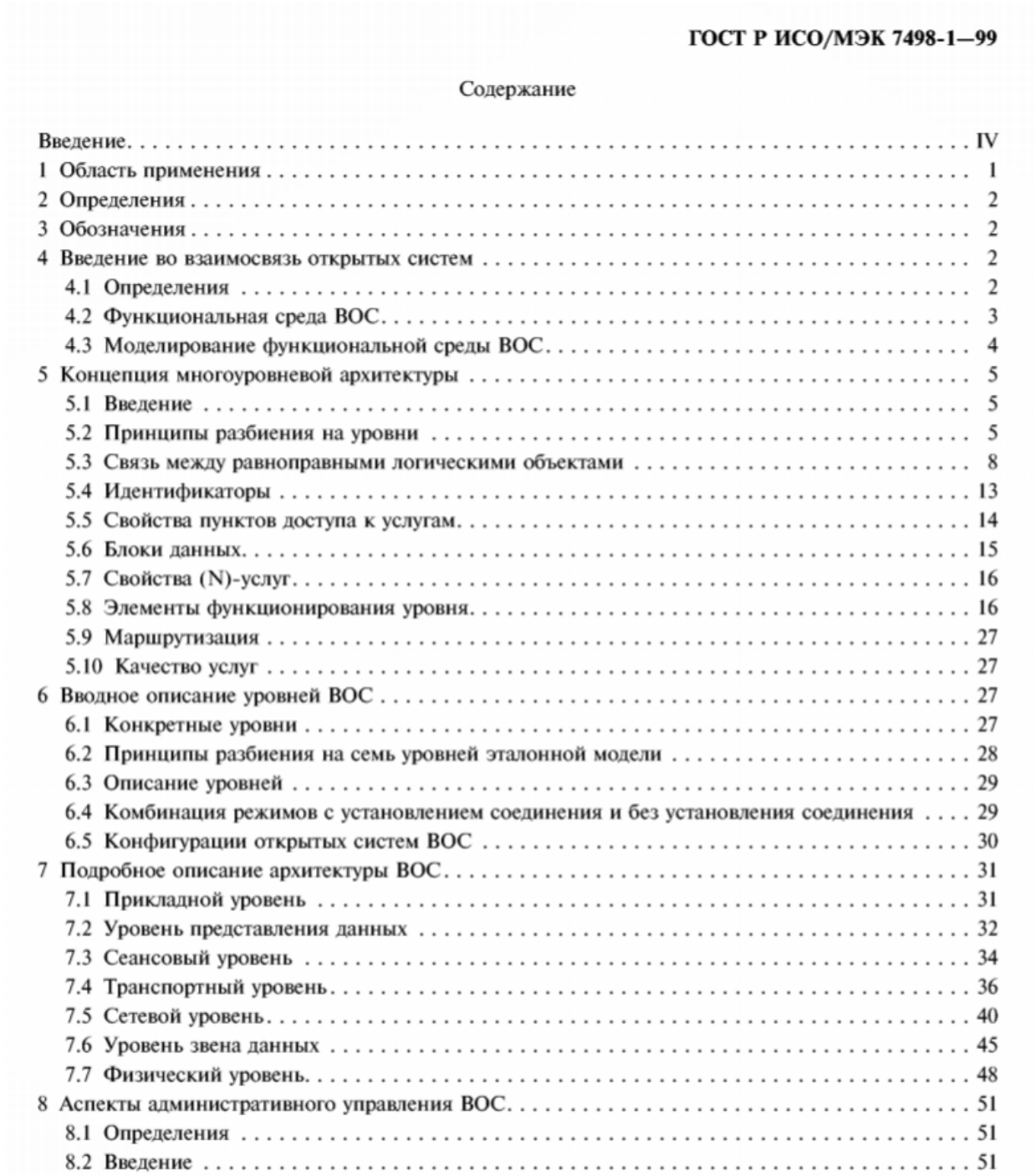
"On the Internet, nobody knows you're a dog."

Когда речь идет о данной модели – то в голове напрашивается поиск должной аналогии. Для создания хорошего ассоциативного эффекта у изучающего. Но так уж получилось, что человечество, создав довольно близкий к идеальному механизм инкапсуляции данных, предоставления их на нужном уровне разным ресурсам, не смогло реализовать такое на практике, отделавшись, давней, и совершенной близко не похожей, при детальном рассмотрении, системой государственной власти (практически любой из современных), и вовсе, казалось бы, наиболее схожей, системой документооборота.

Несмотря на большое значение данной системы, теоретическому описанию принципов работы набора сетевых протоколов, взаимодействующих друг с другом в рамках модели OSI/ISO было суждено предоставить не мне. Прежде чем ознакомится с содержимым данной книги, рекомендую считать QR-код, расположенный на этой страницы.

ГОСТ Р ИСО МЭК 7498

Считав этот код, и перейдя на портал Федерального Агентства по Техническому регулированию и метрологии, вы получите доступ к полному изложению следующего наименования: «Информационная технология. Взаимосвязь открытых систем. базовая эталонная модель. Базовая модель»:



ГОСТ Р ИСО/МЭК 7498-1—99

Содержание

Рисунок 3 – Содержимое QR-кода

У вас все получилось, и вы получили доступ к полному изданию стандарта? Тогда я вас поздравляю – только что был достигнут завершающей стадии обмена, процесс взаимодействия двух машин, т.е, прошлое базовое межмашинное взаимодействие: между вашим смартфоном и экраном монитора компьютера (если вы читаете электронный вариант издания).

Компьютерная сеть — это совокупность ПК и других устройств, объединяемых вместе с помощью сетевых кабелей таким образом, что они могут взаимодействовать друг с другом с целью совместного использования информации и ресурсов.

Принято иметь весьма стандартизованные, академические представления о типах компьютерных сетей. Мы считаем, что сети отличаются размерами и по топологическому признаку: некоторые размещаются внутри одного офиса, другие охватывают несколько зданий и даже весь земной шар.

Смею заметить, что данный подход к определению несколько устарел. Виновником это стал небезызвестный фактор, выраженный как закон Мура — эмпирическое наблюдение, изначально сделанное Гордоном Муром, согласно которому (в современной формулировке) количество транзисторов, размещаемых на кристалле интегральной схемы, удваивается каждые 24 месяца.

Казалось бы – причем тут это. Да и закон, сформулированный еще почти полвека назад, уже давно оспаривается в научном мире. В частности, в последние годы. Такое мнение форсируется преимущественно публицистическими изданиями. И с этим совершенно не согласен Институт инженеров электротехники и электроники (IEEE).

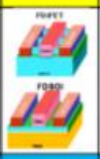
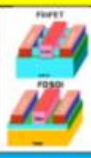
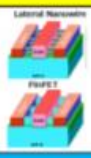
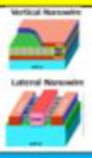
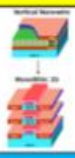
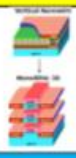
YEAR OF PRODUCTION	2015	2017	2019	2021	2024	2027	2030
Logic device technology naming	P70M56	P54M36	P42M24	P32M20	P24M12G1	P24M12G2	P24M12G3
Logic industry "Node Range" Labeling (nm)	"16/14"	"11/10"	"8/7"	"6/5"	"4/3"	"3/2.5"	"2/1.5"
Logic device structure options	finFET FDSOI	finFET FDSOI	finFET LGAA	finFET LGAA VGAA	VGAA, M3D	VGAA, M3D	VGAA, M3D
							
DEVICE ARCHITECTURE & MODULES							
Starting substrate	Si, SOI	Si, SOI	Si,SOI, SRB, QW	Si,SOI, SRB, QW	Si,SOI, SRB, QW	Si,SOI, SRB, QW	Si,SOI, SRB, QW
N-channel	Si	sSi	sSi, Ge	sSi, sGe, IIIV	sSi, sGe, IIIV	sSi, sGe, IIIV	sSi, sGe, IIIV
P-channel	Si	Si,SiGe	Si,SiGe	Si,SiGe	Ge	Ge	Ge
Channel formation	Etch	Etch, EPI	Etch, EPI	Etch, EPI	Etch, EPI	Etch, EPI	Etch, EPI
Contact material	Silicide	Low-SBH	Low-SBH	Low-SBH	Low-SBH	Low-SBH	Low-SBH
Contact integration	EPI	EPI	EPI WAC	WAC	WAC		
DEVICE PERFORMANCE BOOSTERS							
Main performance booster	SCE finHeight Vt	SCE finHeight Vt	Parasitics finHeight	Parasitics finHeight	Low Vdd 3D		
Scaling focus	Perf	Power	Power	Power	Function		
Channel strain	Yes	Yes	Yes	Yes	Yes		
S/D strain	Yes	Yes	Yes	Yes	Yes		
Transport scheme	DD	Quasi Ballistic	Quasi Ballistic	Ballistic	Ballistic TFET, JFET, NCMOS		

Рисунок 4 – Дорожная карта из брошюры IEEE по прогнозированию продолжения работы законы Мюра на 2015-2030 гг.

А ведь связь напрашивается очевидная – технологический процесс изготовления полупроводниковых (п/п) изделий и материалов прямо связан и с сетевыми технологиями. Правда, про это не желают упоминать. Надеясь на смекалку.

Если говорить очень упрощённо, возвращаясь к архитектуре компьютерных систем, то процессор, не нуждающийся в каком-либо представлении, — это миллиарды крошечных транзисторов и электрических затворов, которые включаются и выключаются при выполнении операций.

И, например, «7 нм тех.процесс» — это размер этих транзисторов в нанометрах. Для понимания масштабов стоит напомнить, что в одном миллиметре миллион нанометров, а человеческий волос толщиной 80000-110000 нанометров. Транзистором, напомню, называют радиоэлектронный компонент из полупроводника (материал, у которого удельная проводимость меняется от воздействия температуры, различных излучений и прочего), который от небольшого входного сигнала управляет значительным током в выходной цепи. Он используется для усиления, генерирования, коммутации и преобразования электрических сигналов. Сейчас транзистор является основой схемотехники подавляющего большинства электронных компонентов и интегральных микросхем. Размер транзистора полезно знать специалистам для оценки производительности конкретного процессора, ведь чем меньше транзистор, тем меньше требуется энергии для его работы.

Собственно, только благодаря поступательному развитию в этом направлении, в усилиях по уменьшению технологического процесса, стал возможным полноценный беспроводной обмен в рамках технологий семейства GSM/3GPP/LTE. А однокристальные системы (SoC) - электронные схемы, выполняющие функции целого устройствами размещённые на одной интегральной схеме стали такими популярными (рис. 5).

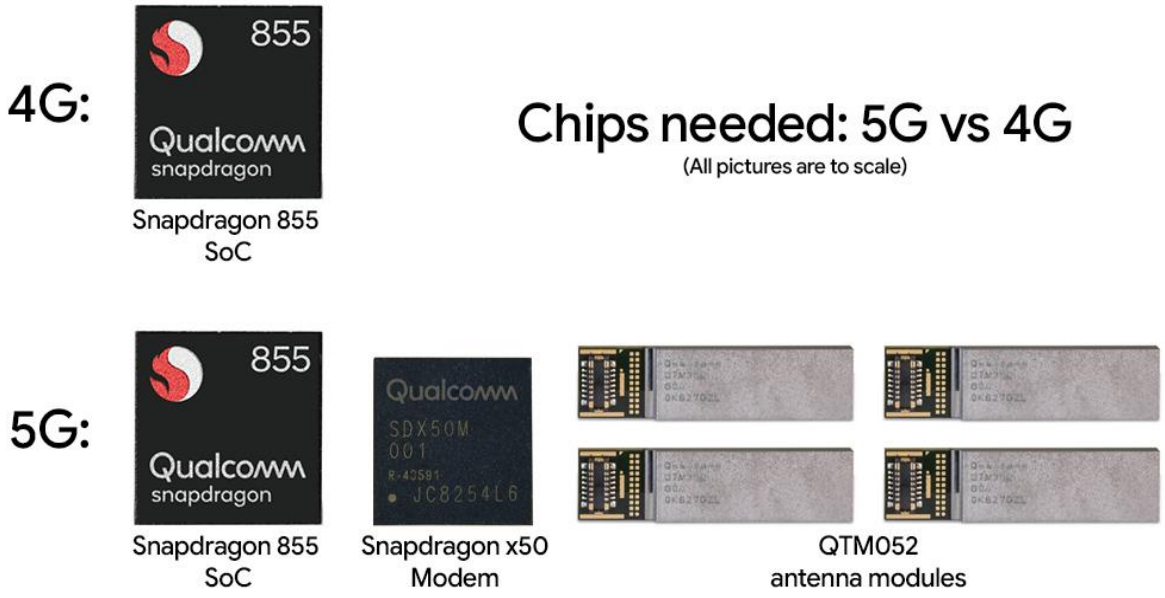


Рис.5 – SoC с поддержкой беспроводных сетевых технологий

Сегодня, в 2020 году на крохотной площадке в 49мм^2 (Qualcomm Snapdragon 855) помещается полноценная компьютерная система. И данный представитель SoC интегрирован в смартфон. Не в специализированное устройство, а в обычный смартфон. В нем есть всё, что есть в обычных компьютерах – CPU, GPU, RAM, ROM и многое другое: от полноценной реализации контроллера оперативной памяти, сигнального процессора (DSP) и до сопроцессора обработки изображений (рис.6).

Характеристики Qualcomm Snapdragon 855	
Техпроцесс	7 нм (TSMC)
Архитектура	64 бита
Центральный процессор	8 ядер Kryo 485 (1+3+4) 1 ядро Cortex A76 до 2,84 ГГц 3 ядра Cortex A76 до 2,42 ГГц 4 ядра Cortex A55 до 1,8 ГГц
Контроллер памяти	LPDDR4x 4-канальный (64 бита) 2133 МГц, до 34,13 ГБ/с До 16 ГБ
Графический процессор	Adreno 640 384 ядра DirectX 12, Vulkan, OpenGL 3.2, OpenCL 2.0 ≈ 1 TFLOPS (FP32)
Экран	4K внутренний, 4K внешний (до 2 шт.), HDR 10+, до 120 Hz
Сигнальный сопроцессор (DSP)	Hexagon 690
Сопроцессор обработки изображений (ISP)	Spectra 380, двойной, 14-битный сигнал Аппаратное ускорение машинного зрения
Фотокамера	Одиночная – до 48 Мп (с MFNR, ZSL) Двойная (одновременная работа) – до 22 или 16+16 Мп (с MFNR, ZSL) Максимальное разрешение – 192 Мп
Запись видео	До 4K 60 FPS, эффект боке, HDR10, HLG, Rec. 2020 Slow-Mo 720p 480 FPS
Воспроизведение видео	H.265 (HEVC), H.264 (AVC), HLG, HDR10, HDR10+, VP8, VP9
Мобильная связь	GSM, HSPA, CDMA, LTE Cat 20 до 2 Гбит/с (загрузка) / Cat. 13 до 384 Мбит/с (передача) Поддержка дискретного модема 5G Snapdragon X50
Wi-Fi	802.11a/b/g/n/ac/ad/ay/ax-ready, диапазоны 2,4, 5 и 60 ГГц, до 10 Гбит/с
Bluetooth	5.0
Навигатор	GPS, BeiDou, Galileo, QZSS, ГЛОНАСС, SBAS, двухчастотный
USB	3.1
Быстрая зарядка	4+

Рис.6 – Характеристики SoC Qualcomm Snapdragon 855

И что наиболее важно – данная SoC имеет на своем миниатюрном борту исправно работающий тандем из устройств, представляющих информационный обмен посредством технологий: Bluetooth (IEEE 802.15.1), Wi-Fi (IEEE 802.11), LTE (4G), и 5G. Кажется, что все это время мы недооценивали смартфоны, пренебрежительно относились к носимой электронике. Необходимо дать трезвый отчет тому, что с точки зрения детализированного подхода к определению роли практически любого гаджета появилась большая и стремительно увеличивающаяся информационная энтропия. И общая проблема заключается в том, что необходимо трактовать смартфоны, умные часы, устройства IoT как самостоятельные информационные системы, самоорганизующиеся сети[1], а не только как оконечные узлы.

[1] Самоорганизующаяся сеть – сеть, не имеющая определенной структуры, меняющаяся и распределяющая функции между узлами при подключении нового устройства, изменении характера трафика и т.д.

В иноязычной литературе данный пробел в познании рамок сетевого инжиниринга был решен за счет внедрения дополнительных типов сетей (по территориальному признаку).

На данный момент принято делить все сети по вышеперечисленному признаку на следующие типы (подвиды), которым и необходимо дать более детальную характеристику в актуальном формате:

BAN (Body Area Network — нательная компьютерная сеть) — сеть надеваемых или имплантированных компьютерных устройств.

PAN (Personal Area Network) — персональная сеть, предназначенная для взаимодействия различных устройств, принадлежащих одному владельцу.

LAN (**ЛВС,** Local Area Network) — локальные сети, имеющие замкнутую инфраструктуру до выхода на поставщиков услуг. Термин «LAN» может описывать и маленькую офисную сеть, и сеть уровня большого завода, занимающего несколько сотен гектаров. Локальные сети являются сетями закрытого типа, доступ к ним разрешён только ограниченному кругу пользователей, для которых работа в такой сети непосредственно связана с их профессиональной деятельностью.

CAN (Campus Area Network) — кампусная сеть, объединяет локальные сети близко расположенных зданий. Диапазон CAN составляет от 1 км до 5 км. Если два здания имеют один и тот же домен, и они связаны между собой сетью, то это будет рассматриваться только как CAN. Хоть и CAN в основном используется для корпоративных кампусов, канал передачи данных будет иметь высокую скорость.

MAN (Metropolitan Area Network) — городские сети между учреждениями в пределах одного или нескольких городов, связывающие много локальных вычислительных сетей.

WAN (Wide Area Network) — глобальная сеть, покрывающая большие географические регионы, включающие в себя как локальные сети, так и прочие телекоммуникационные сети и устройства. Пример WAN — сети с коммутацией пакетов (Frame relay), через которую могут «разговаривать» между собой различные компьютерные сети. Глобальные сети являются открытыми и ориентированы на обслуживание любых пользователей.

Большой прогресс в физиологических аппаратах, маломощных интегрированных схемах и беспроводных коммуникациях сделал возможным новое поколение т.н. беспроводных сенсорных сетей, ныне используемых для таких целей, как мониторинг пробок, урожая, инфраструктур и здоровья. Нательная компьютерная сеть позволяет провести недорогой и продолжительный мониторинг тела в реальном времени через Интернет. Несколько интеллектуальных физиологических аппаратов могут быть интегрированы в надеваемые устройства, которые могут использоваться для компьютерной реабилитации или заблаговременного обследования состояния здоровья. Эта область основывается на возможности имплантации очень маленьких датчиков внутрь человеческого тела, которые очень удобны и не нарушают нормальную деятельность человека. Имплантированные в тело аппараты будут отслеживать различные физиологические изменения, чтобы контролировать состояние здоровья пациента независимо от его местоположения. Эта информация будет передана по беспроводному каналу. Устройство будет мгновенно передавать всю информацию в режиме реального времени врачам во всем мире. Если обнаружена экстренная ситуация, врачи сразу же проинформируют пациента через компьютерную систему посредством отправки соответствующих сообщений или аварийных сигналов. Хотя технология все ещё находится в своей начальной стадии, она широко исследуются, и после её принятия ожидается прорыв в области здравоохранения.

BAN устройства могут быть встроены в тело, имплантированы, прикреплены к поверхности тела в фиксированном положении или совмещены с устройствами, которые люди носят в различных местах (в карманах, на руке или в сумках). Несмотря на уменьшение размера устройств, т.к. сети, состоящие из нескольких миниатюрных сенсорных блоков (BSU), объединяются с единым центральным блоком тела (BCU) устройства размером более дециметра (планшеты, КПК), по-прежнему играют большую роль, выступая, в таком случае, концентраторами информации, предоставляя пользовательский интерфейс для обзора и управления BAN приложениями «на месте».

Разработка технологии BAN началась еще в конце 90х годов прошлого века на основе идеи использования беспроводных персональных сетей для реализации связи «на», «рядом», и «вокруг» человеческого тела. Около десяти лет спустя термин BAN стал обозначать системы, где связь полностью «в пределах», «на» или «в непосредственной близости» от человеческого тела.

BAN может использовать беспроводные технологии в качестве шлюзов для достижения больших расстояний. Через шлюзы можно соединять надеваемые на человеческое тело устройства через Интернет. Таким образом, мед. работники могут получить доступ к данным о пациенте онлайн, используя Интернет вне зависимости от местоположения пациента.

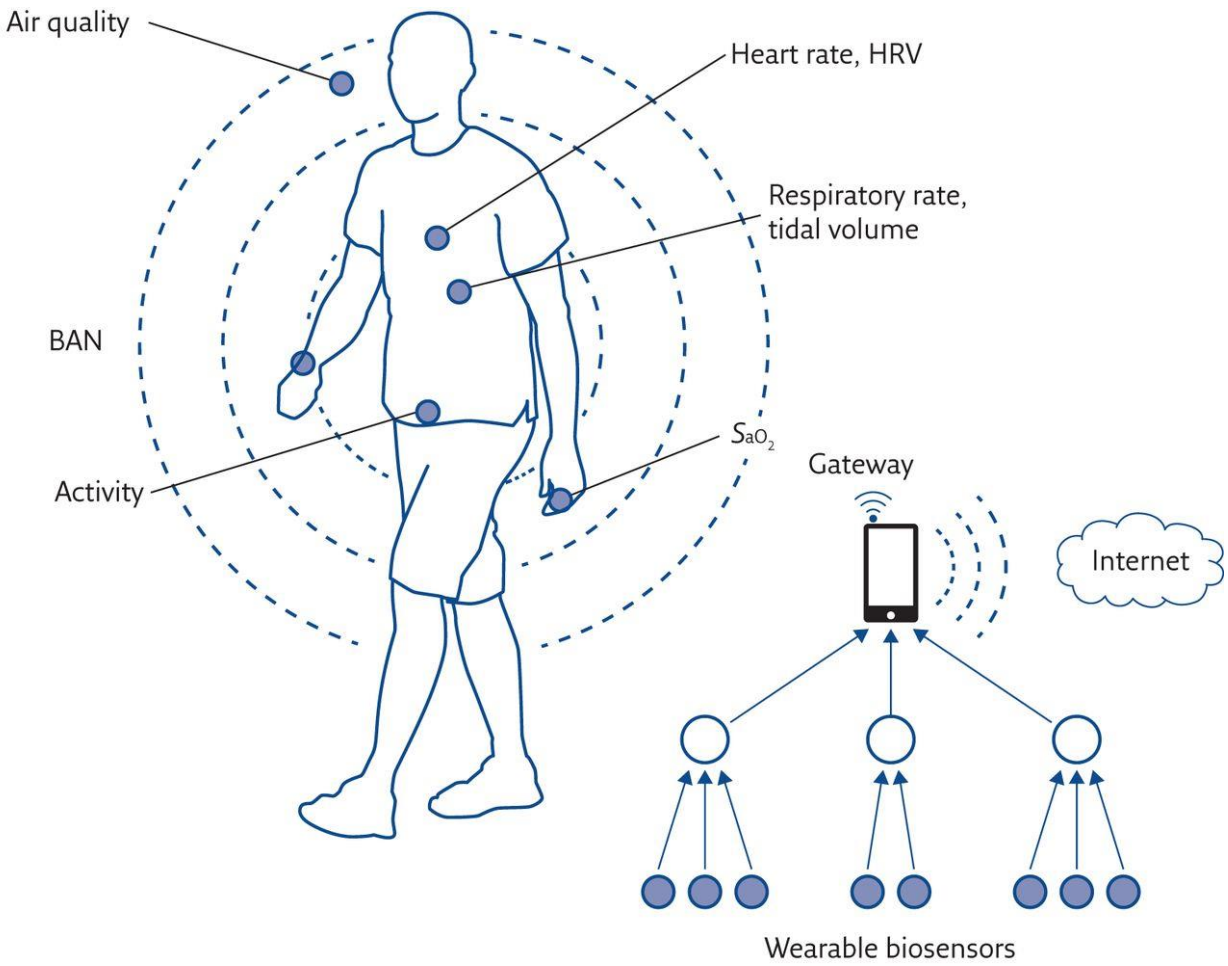


Рис.7 – BAN как носимая (Wearable) технология

Первоначальные применения нательной компьютерной сети тела прежде всего ожидаются в области здравоохранения, особенно для непрерывного мониторинга и записи важных данных о пациентах, страдающих от хронических заболеваний, таких как диабет, астма и сердечные приступы (см. рис.7).

Нательная компьютерная сеть может предупредить по сети больницу даже прежде, чем у пациента случится сердечный приступ, путём слежения за важными изменениями человека.

Также, технология позволяет автоматически вводить инсулин больным диабетом, как только уровень инсулина снижается.

Технология также применима в спорте, военном деле или охране безопасности. Продвижение технологии в новых областях поможет беспроводным обменом информацией и между людьми и машинами.

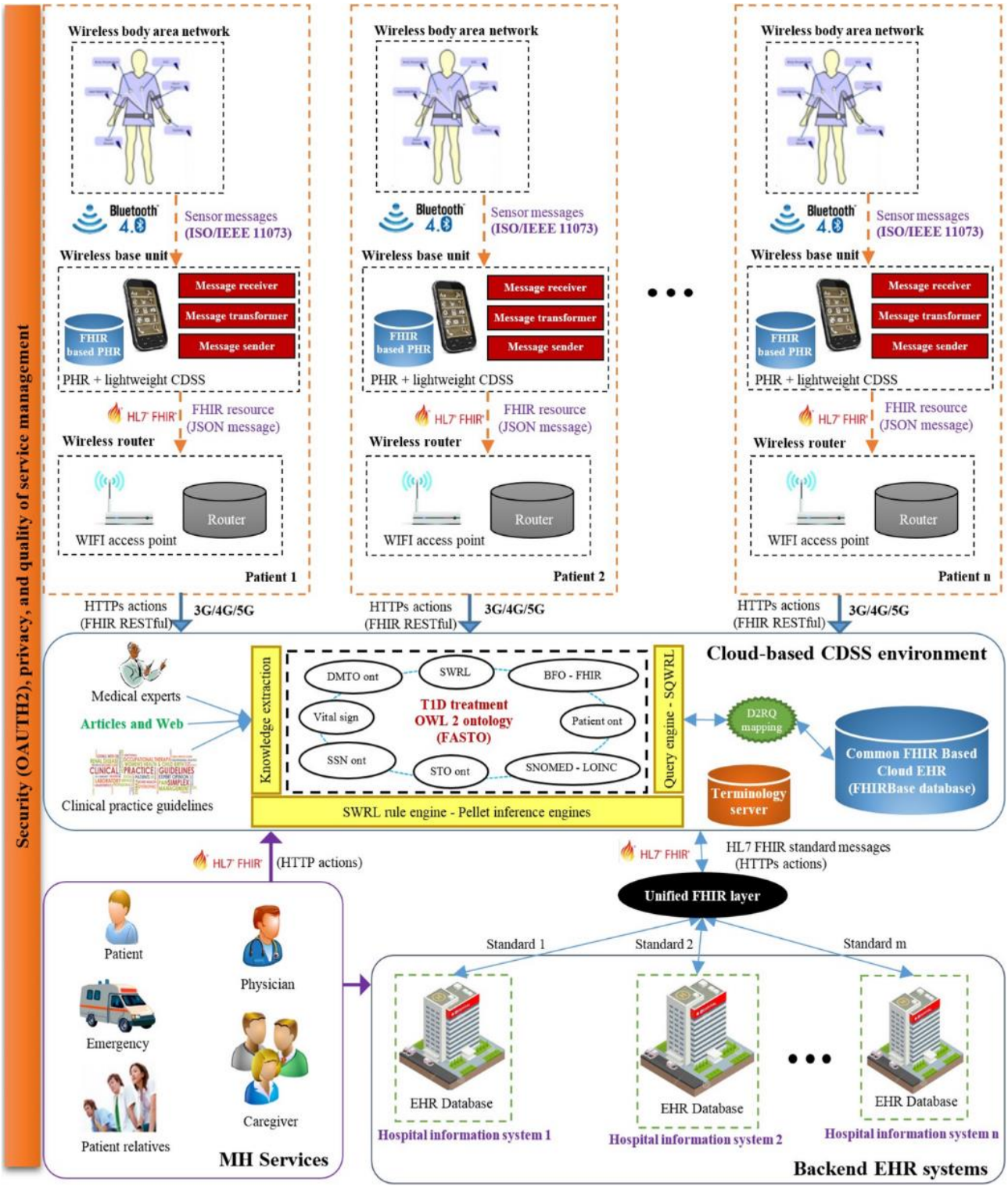


Рис.8 – Инфологическая карта применения BAN технологий в медицине

На рисунке 8, показана модель взаимодействия между тремя BAN/WBAN и неуказанной в явном виде, но явно более глобальной (по территориальному признаку) сети, т.е информационной системы, в которой, в упрощённом виде главным информационным субъектом является видовая составляющая трёх типов электронной медицинской карты, которые определены на рисунке по следующим аббревиатурам:

Electronic Health Record (EHR) — хранит информацию относительно всех медицинских заболеваний, хранителем является специально авторизованный центр (Health Authority). Медицинские записи являются официальными данными, могут быть доступны для других авторизованных центров и подобных представителей медицинских услуг, а также лабораторий, гос. учреждений и т.п. для улучшения качества здравоохранения.

Electronic Medical Record (EMR/MH Services) – хранит информацию относительно конкретной медицинской области (например, стоматология), хранителем является клиника или практикующий врач. Обычно это электронная версия истории болезни пациента в данном конкретном учреждении.

Personal Health Record (PHR) – хранит какую-то медицинскую информацию, хранителем, а точнее ответственным за полноту и качество информации, является сам пациент (или его представителя, например, член семьи).

Данная схема является примером практической реализации сети такого плана. Все те же, классические HTTP-запросы, клиент-серверная архитектура и топологическая организация.

Проблемы с использованием технологий и решений на базе BAN могут заключаться в:

Взаимодействии: BAN системы должны обеспечивать беспрепятственную передачу данных через стандарты такие, как Bluetooth, ZigBee и т. д., чтобы способствовать обмену информацией между взаимодействующими устройствами. Кроме того, эти системы должны быть масштабируемыми, обеспечивать эффективный переход между сетями и предлагать непрерывное соединение.

В системных устройствах: Датчики, используемые в Wireless BAN должны быть низкой сложности, небольшие по размеру, легкие в весе, мощные, легкие в использовании и перенастраиваемые. Кроме того, устройства хранения данных должны облегчить дистанционное хранение устройств и просмотр за пациентами, а также доступ к внешним средствам обработки и анализа через Интернет.

В системной и аппаратной безопасности: Требуются значительные усилия, чтобы сделать BAN безопасной и точной. Мы должны быть уверены, что данные о пациентах не могут перепутаться.

В вторжении в личную жизнь: Люди могут рассматривать технологию BAN как потенциальную угрозу для их свободы, если исследования выйдут за рамки безопасности здоровья. Общественное признание стало бы ключом к этой технологии, находящим более широкое применение.

В проверке (опросе) датчика: Распространенным устройствам зондирования свойственны аппаратные и сетевые ограничения. Это может привести к ошибочным данным, передаваемым обратно к конечному пользователю. Имеет первостепенное значение, особенно в области здравоохранения, проверка показаний датчиков. Благодаря этому можно сократить число ложных созданий сигналов тревоги и определить возможные слабые места в рамках аппаратного и программного обеспечения.

В согласованности данных: Данные, находящиеся на нескольких мобильных устройствах и беспроводных аппаратах пациентов, должны быть собраны и проанализированы. В BAN жизненно важные данные пациента могут проходить через множество узлов, сетей и компьютеров. Если мобильное устройство практикующего врача не содержит всю известную информацию, то качество медицинской помощи может снизиться.

В вмешательстве: беспроводная связь, используемая для датчиков тела, должна минимизировать помехи и повысить сосуществование узлов сенсорных устройств с другими сетевыми устройствами, доступными в окружающей среде. Это особенно важно для реализации крупномасштабных систем BAN.

В управлении данными: BAN генерирует данные в больших объёмах, поэтому управление информацией имеет первостепенное значение.

Помимо аппаратно-ориентированных задач, следующие вопросы, касающиеся человека, должны учитываться в развитии BAN:

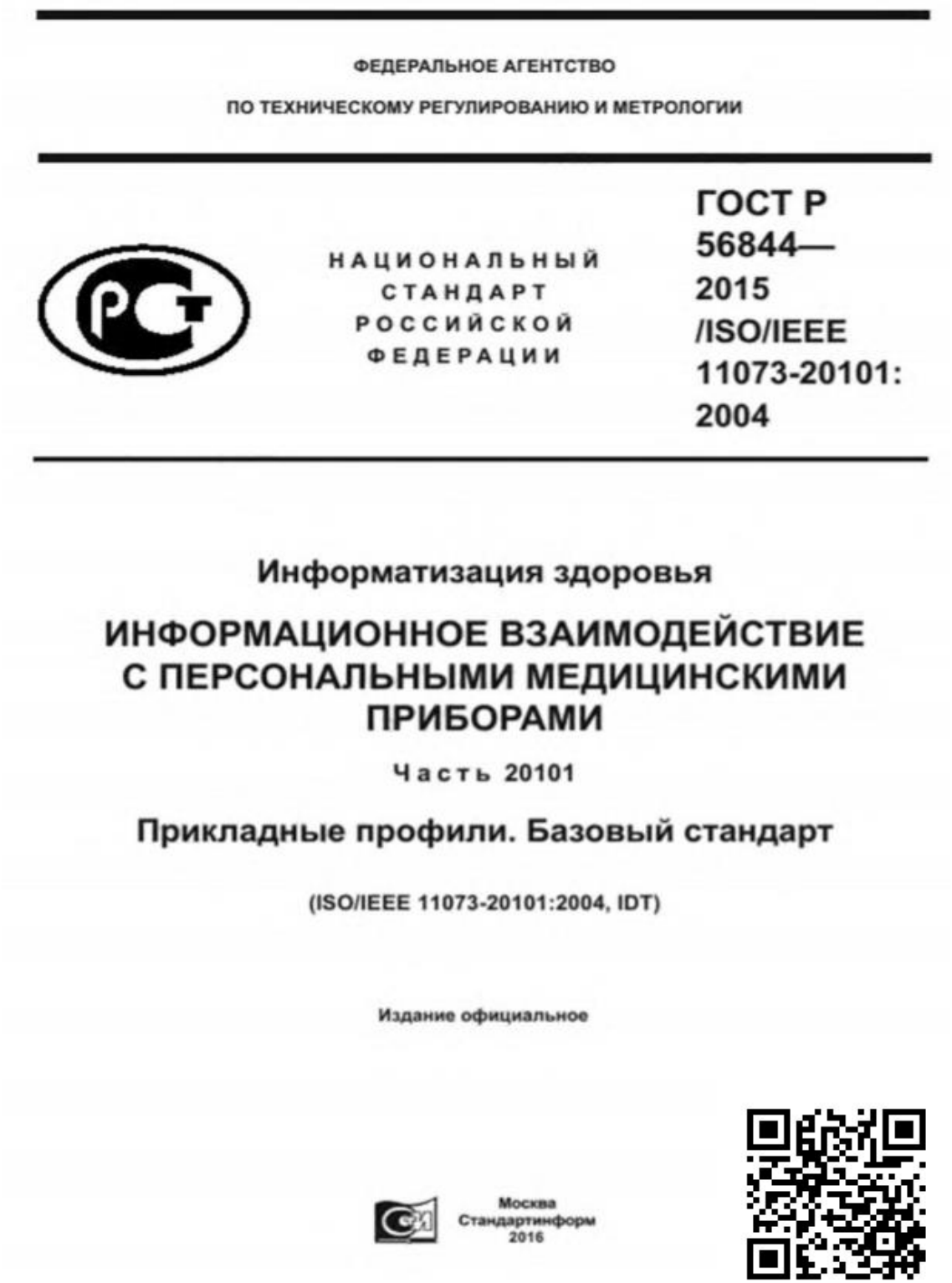
Стоимость: В наши дни потребители ожидают низких цен для мониторинга здоровья, которые должны сочетаться с высоким функционалом.

Постоянный мониторинг: Пользователям могут потребоваться различные уровни мониторинга, например, тем, кто подвержен риску ишемической болезни, необходимо, чтобы BAN постоянно работал, в то время как другим группы риска может потребоваться только контроль BAN'а, когда они ходят или двигаются. Уровень мониторинга влияет на количество требуемой энергии и определенный заряд энергии.

Размещение: BAN должен быть удобным для надевания, легким, ненавязчивым. Он не должен изменять повседневную деятельность пользователя, обременять его. Технология должна в конечном счете быть удобной для пользователя, выполнять свои задачи мониторинга без его ведома.

Производительность: Производительность BAN должна быть стабильной. Измерения датчиков должны быть точными, даже если BAN выключается и включается снова. Беспроводные каналы связи должны быть надежными и работать под различными средами пользователей.

Таким образом, нательные компьютерные сети – по-прежнему прерогативны для будущего, для технологий завтрашнего дня. Но техническое регламентирование информационного взаимодействия в отдельных отраслях уже вполне доступно не только для обозрения, а и для проектировочной и пуско-наладочной деятельности. Как например, семейство стандартов IEEE/ISO 11073:



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56844— 2015 /ISO/IEEE 11073-20101: 2004

Информатизация здоровья

ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ С ПЕРСОНАЛЬНЫМИ МЕДИЦИНСКИМИ ПРИБОРАМИ

Часть 20101

Прикладные профили. Базовый стандарт

(ISO/IEEE 11073-20101:2004, IDT)

Издание официальное

Москва Стандартинформ 2016

Рис. 9 - Стандарты комплекса ISO/IEEE 11073 определяют взаимосвязь между медицинскими приборами и внешними компьютерными системами

Общие положения сферы применения WBAN (BAN) отражены в стандарте IEEE 802.15.6.

Стандарт **IEEE 802.15.6** направлен на обеспечение конфиденциальности, аутентификации, целостности, защиты конфиденциальности и защиты воспроизведения. Все узлы и концентраторы должны выбрать три уровня безопасности: незащищенная связь (уровень 0 , аутентификация, но без шифрования(уровень 1) и аутентификация и шифрование (уровень 2). В процессе сопоставления безопасности узел и концентратор должны совместно выбрать подходящий уровень безопасности.

Все узлы и концентраторы в WBAN должны пройти определенные этапы на уровне MAC перед обменом данными. А ассоциация по вопросам безопасности это процедура для идентификации узла и концентратора друг к другу, чтобы установить новый мастер-ключ (MK) совместно используемый между ними, или активировать существующий MK предварительно совместно используемый между ними**. Ассоциация безопасности**[2] в стандарте IEEE 802.15.6 основана на четырех ключевых протоколах соглашения, которые имеют проблемы безопасности. В опубликованной академической литературе есть несколько интересных предложений, которые соответствующим образом решают проблемы безопасности и конфиденциальности текущих процедур.

WBAN поддерживает разнообразие в реальном масштабе времени контроль здоровья и применения бытовой электроники. Последним международным стандартом для WBAN является стандарт IEEE 802.15.6 который направлен на обеспечение международного стандарта для низкой мощности, короткого диапазона и чрезвычайно надежной беспроводной связи в пределах окружающей области человеческого тела, поддерживая широкий диапазон скоростей передачи данных для различных приложений. В настоящем стандарте указываются краткосрочные беспроводные средства связи в непосредственной близости или внутри человеческого тела (но не только для людей).

Он использует существующие промышленные научные медицинские (ISM) полосы, а также частотные полосы, одобренные национальными медицинскими и / или регулирующими органами.

---

[2]Ассоциация безопасности - это симплексное соединение, которое позволяет предоставлять услуги безопасности для трафика, переносимого этим соединением. Услуги безопасности предоставляются ассоциации безопасности посредством использования протоколов идентификации (МСЭ-Т Y.1281).

Второй ступенью развития компьютерных сетей по территориальному признаку (по возрастанию) являются так называемые Personal Area Networks.

Персональная сеть (англ. Personal Area Network, PAN) — это сеть, построенная «вокруг» человека. PAN представляет собой компьютерную сеть, которая используется для передачи данных между устройствами, такими как компьютеры, телефоны, планшеты и персональные карманные компьютеры (КПК). Персональные сети могут использоваться как для информационного взаимодействия отдельных устройств между собой (интерперсональная коммуникация), так и для соединения их с сетями более высокого уровня, например, глобальной сети Интернет (восходящая линия связи), где одно "первичное" устройство берет на себя роль интернет-маршрутизатора.

Беспроводная персональная сеть (WPAN) является маломощной PAN, которая организуется на небольшом расстоянии с использованием беспроводных сетевых технологий, таких как: IrDA, Bluetooth, Z-Wave, ZigBee, Piconet.

Радиус действия WPAN составляет от нескольких десятков сантиметров до нескольких метров, так что все устройства находятся в одной рабочей области. PAN также может организовываться с использованием проводных компьютерных шин, таких как USB и FireWire.

Хотя, использование мобильного телефона в качестве точки доступа для других устройств через Wi-Fi соединение может быть использовано только одним пользователем, всё же такая сеть не считается PAN.

Беспроводная персональная сеть (WPAN) это та же самая персональная сеть, однако в ней, все соединения являются беспроводными. Беспроводной PAN основан на стандарте **IEEE 802.15**. В WPAN используются два вида беспроводных технологий. Это Bluetooth и Infrared Data Association.

Беспроводные персональные сети применяются для связи различных устройств (как портативных, так и настольных), включая компьютерную, бытовую и оргтехнику, средства связи и т. д. Такие сети могут иметь и более специализированное назначение, например, в медицине.

Ключевым понятием в технологии WPAN является "подключение". В идеальном случае, когда любые два WPAN-оборудованные устройства находятся в непосредственной близости (в пределах нескольких метров друг от друга) или на расстоянии нескольких километров от центрального сервера, они могут общаться, как будто соединены с помощью кабеля. Другой важной особенностью является способность каждого устройства выборочно блокировать связь с другими устройствами, с целью предотвращения несанкционированного доступа к информации.

Технология WPAN сейчас находится в стадии становления и переживает бурное развитие. На данный момент в цифровом режиме предлагаются рабочие частоты порядка 2,4 ГГц. Цель, которую хотят достичь в этой технологии - обеспечить стабильную и бесперебойную работу всех систем, использующих WPAN. Каждое устройство в WPAN будет иметь возможность подключиться к любому другому устройству в той же WPAN, при условии, что они находятся в зоне видимости друг друга. Кроме того, в будущем, во всем мире все беспроводные персональные сети будут взаимосвязаны. Так, например, археолог на сайте в Греции сможет использовать карманный компьютер для прямого доступа к базам данных в университете Миннесоты в Миннеаполисе, и передать результаты этой базе данных.

Беспроводные персональные сети **обычно охватывают диапазон** от нескольких сантиметров до 10 метров (33 фута). Эти сети можно рассматривать как особый тип (или подмножество) **локальных сетей**, которые поддерживают одного человека вместо группы.

Связь ведущего-ведомого устройства может иметь место в PAN, где несколько устройств подключаются к «главному» устройству, называемому ведущим. Ведомые реле передают данные через ведущее устройство. С Bluetooth такая настройка может достигать 100 метров (330 футов).

Хотя PAN, по определению, **личные**, они могут по-прежнему получать доступ к Интернету при определенных условиях. Например, устройство в пределах PAN может быть подключено к локальной сети, которая имеет доступ к Интернету, которая является глобальной сетью. Чтобы каждый тип сети был меньше следующего, но все они могут быть в конечном счете тесно связаны.

Личные сети могут быть беспроводными или сконструированы с помощью кабелей. USB и FireWire часто соединяют проводную PAN, в то время как WPAN обычно используют Bluetooth (и называются piconets) или иногда инфракрасные соединения.

Пример: клавиатура Bluetooth подключается к планшету для управления интерфейсом, способным достичь близкой «умной» лампочки.

Кроме того, принтер в небольшом офисе или доме, который подключается к ближайшему настольному компьютеру, ноутбуку или телефону, считается существующим в PAN. То же самое можно сказать о клавиатурах и других устройствах, использующих IrDA (Инфракрасная ассоциация данных).

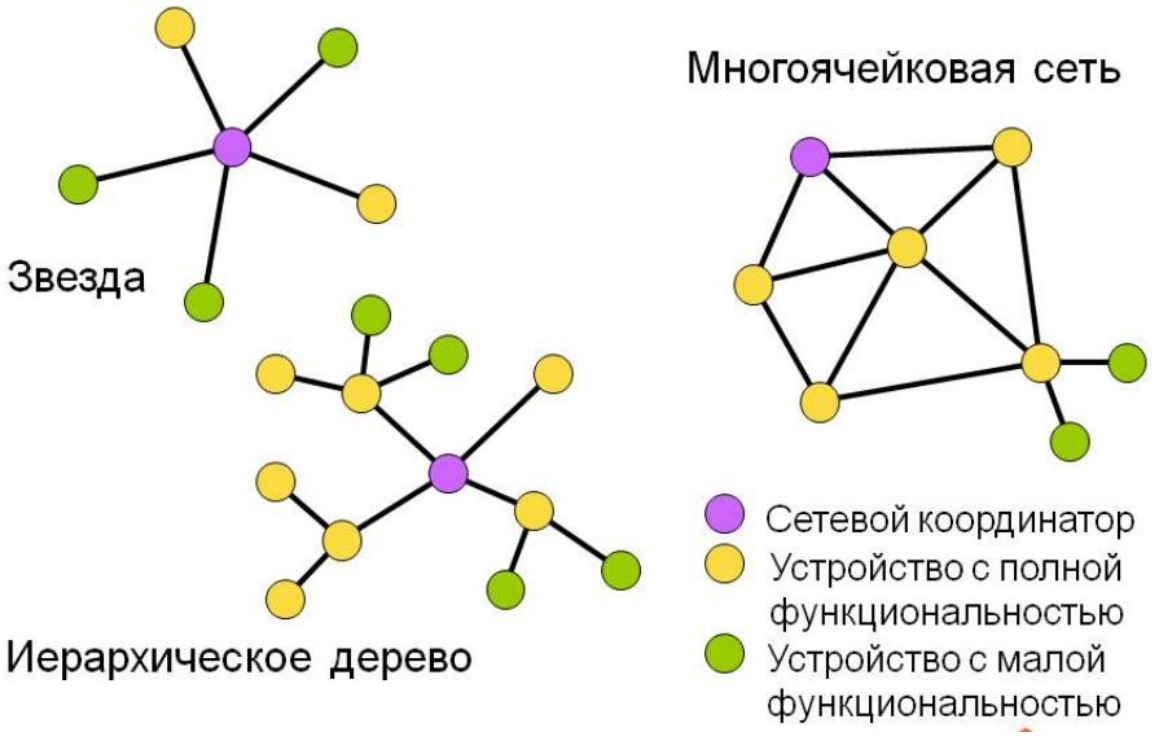
Преимущества персональной сети:

PAN для личного использования, поэтому преимущества могут быть более понятны, чем при разговоре о глобальных сетях, например, описывающих Интернет. Благодаря личным сетям ваши личные устройства могут соединяться для более удобного общения. Нет необходимости, чтобы все сообщения передавались через более крупную сеть только для того, чтобы их принимали люди в нескольких футах от них. PAN позаботится об этом.

Пример, упомянутый выше, — это беспроводная клавиатура или даже мышь. Устройствам такого типа не нужно управлять компьютерами в других зданиях или городах, поэтому они вместо этого строятся, чтобы просто общаться с ближайшим, как правило, устройством прямой видимости, таким как компьютер или планшет.

Поскольку большинство устройств, поддерживающих связь на коротком расстоянии, могут блокировать соединения, которые не являются предварительно авторизованными, WPAN считается защищенной сетью.

В топологическом плане PAN-сети обладают весьма большими возможностями (рис.10): возможно построение сетей на базе физических топологий «звезда», «дерево», «Mesh» (решетка).



Однако архитектура PAN, описанная в IEEE 802.15 подразумевает и особенности, которые необходимо учитывать при выборе той или иной топологии – зачастую, в PAN, из-за жестких рамок по электропитанию, часть носимых сетевых устройств не могут иметь полную функциональность в информационном обмене.

Поэтому, Сети PAN строятся из базовых станций трех основных типов: координаторов, маршрутизаторов и конечных устройств.

Координаторы запускает сеть и управляет ею. Он формирует сеть, выполняет функции центра управления сетью и доверительного центра (trust-центра) – устанавливает политику безопасности, задает настройки в процессе присоединения устройств к сети, ведает ключами безопасности.

Маршрутизатор PAN (устройство с полной функциональностью) транслирует пакеты, осуществляет динамическую маршрутизацию, восстанавливает маршруты при перегрузках в сети или отказе какого-либо устройства. При формировании сети маршрутизаторы присоединяются к координатору или другим маршрутизаторам, и могут присоединять дочерние устройства – маршрутизаторы и конечные устройства. Маршрутизаторы работают в непрерывном режиме, имеют стационарное питание и могут обслуживать «спящие» устройства. Маршрутизатор может обслуживать до 32 устройств (ZigBee).

Конечное устройство (устройство с малой функциональностью) может принимать и отправлять пакеты, но не занимается их трансляцией и маршрутизацией. Конечные устройства могут подключаться к координатору или маршрутизатору, но не могут иметь дочерних устройств.

Конечные устройства могут переводиться в спящий режим для экономии заряда аккумуляторов. Именно конечные устройства имеют дело с датчиками, локальными контроллерами и исполнительными механизмами.

Не зря, ранее в книге было упомянуто понятие **самоорганизующихся сетей.**

Сеть PAN – самоорганизующаяся, и ее работа начинается с формирования. Устройство, назначенное при проектировании координатором персональной сети (PAN координатор), определяет канал, свободный от помех, и ожидает запросов на подключение.

Устройства, пытающиеся присоединиться к сети, рассылают широковещательный запрос. Пока PAN координатор – единственное устройство в сети, отвечает на запрос и предоставляет присоединение к сети только он. В дальнейшем присоединение к сети могут предоставлять также присоединившиеся к сети маршрутизаторы.

Устройство, получившее ответ на широковещательный запрос, обменивается с присоединяющим устройством сообщениями, чтобы определить возможность присоединения. Возможность определяется способностью присоединяющего маршрутизатора обслужить новые устройства в дополнение к ранее подключенным.

Вступление в сеть (присоединение)

Существует два способа присоединения: MAC ассоциация и повторное сетевое присоединение (NWK rejoin).

MAC ассоциация

MAC ассоциация доступна любому устройству ZigBee и осуществляется на MAC уровне. Механизм MAC ассоциации следующий:

Устройство, позволяющее присоединиться к нему, выставляет на MAC уровне разрешение на присоединение.

Устройство, вступающее в сеть, выставляет на MAC уровне запрос на присоединение и передает широковещательный запрос маячка.

Получив «маячок» от устройств, готовых подключить присоединяемое устройство, последнее определяет, в какую сеть и к какому устройству оно желает присоединиться, и выставляет на MAC уровне требование о вступлении с флажком «повторное присоединение» в значении FALSE.Затем вступающее устройство направляет на выбранное для присоединения устройство запрос присоединения и получает ответ с присвоенным ему сетевым адресом.При MAC ассоциации данные передаются не зашифрованными, поэтому MAC ассоциация не является безопасной. Повторное сетевое присоединение вопреки названию может применяться и при первичном присоединении. Оно выполняется на сетевом уровне. При этом, если вступающее устройство знает текущий сетевой ключ, обмен пакетами может быть безопасным. Ключ может быть получен, например, при настройке.

При повторном подключении присоединяющееся устройство выставляет на сетевом уровне запрос присоединения и обменивается с подключающим устройством пакетами «запрос присоединения» – «ответ на запрос присоединения». Кроме случаев присоединения новых устройств структура сети меняется и в случаях, когда устройства покидают сеть и повторно присоединяться в других местах (это происходит, например, в случае перезагрузки устройства).

На рисунке 11 – пример переподключения. Устройство с адресом «0E3B» переподключается как «097D», а затем как «0260». Каждый раз оно присоединяется к другому маршрутизатору и получает адрес из имеющегося в распоряжении присоединяющего маршрутизатора диапазона адресов.

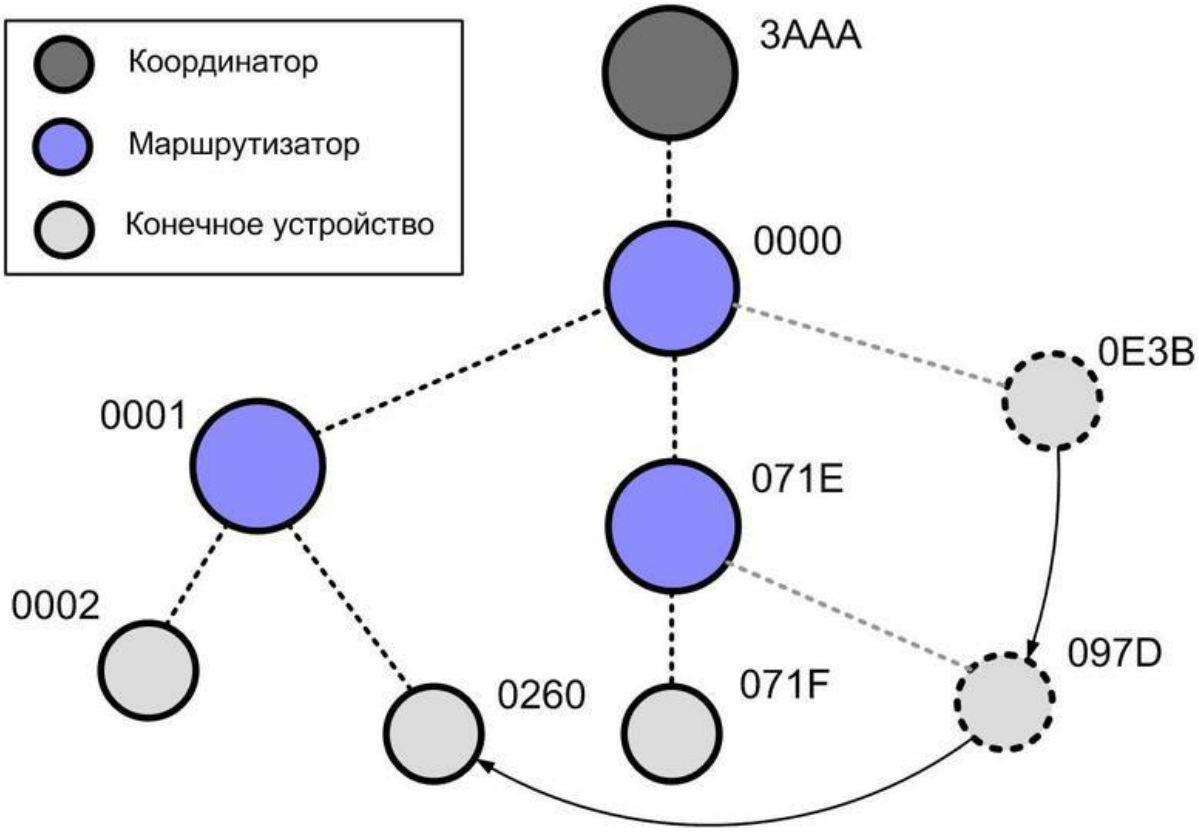


Рис.11 - Переподключение конечного устройства в древовидной сети

Таким образом, можно дать определение WPAN сетям в полном виде.

Беспроводная ad-hoc-сеть (беспроводная динамическая сеть, беспроводная самоорганизующаяся сеть) — децентрализованная беспроводная сеть, не имеющая постоянной структуры. Клиентские устройства соединяются «на лету», образуя собой сеть. Каждый узел сети пытается переслать данные, предназначенные другим узлам. При этом определение того, какому узлу пересылать данные, производится динамически, на основании связности сети. Это является отличием от проводных сетей и управляемых беспроводных сетей, в которых задачу управления потоками данных выполняют маршрутизаторы (в проводных сетях) или точки доступа (в управляемых беспроводных сетях).

Первыми беспроводными самоорганизующимися сетями были сети «packet radio» начиная с 1970-х годов, финансируемые DARPA после проекта ALOHAnet.

WLANs или WPANs?

WPAN определена в контексте личного рабочего пространства (POS - Personal Operating Space), которое обычно распространяется в радиусе до 10 метров и окружает человека или объект, находящийся в покое или в движении. WPAN также подразумевает низкую стоимость и **низкое энергопотребление**. Узел WPAN имеет небольшие размеры, что позволяет встраивать его в портативные устройства, такие как мобильные телефоны и КПК.

С другой стороны, WLAN представляет из себя систему более широкого радиуса действия и имеет более высокую сложность.

WLAN включает в себя центральный узел, называемый точкой доступа(AP - Access Point), который предоставляет доступ к каналу связи некоторому количеству конечных узлов. Типичный узел WLAN представляет из себя карту, устанавливаемую в персональные компьютеры и ноутбуки.

Локальная сеть представляет собой, по сути, сеть, используемую в одном здании или отдельном помещении, таком как квартира, для обеспечения взаимодействия используемых в них компьютеров и программ. Локальные сети, расположенные в разных зданиях, могут быть соединены между собой с помощью спутниковых каналов связи или волоконно-оптических сетей, что позволяет создать глобальную сеть, т.е. сеть, включающую в себя несколько локальных сетей.

Если используется одноранговая сеть, то все компьютеры, входящие в нее, имеют одинаковые права. Соответственно, любой компьютер может выступать в роли сервера, предоставляющего доступ к своим ресурсам, или клиента, использующего ресурсы других серверов.

В сети, построенной на архитектуре клиент/сервер, существует несколько основных компьютеров — серверов. Остальные компьютеры, которые входят в сеть, носят название клиентов, или рабочих станций.

ЛВС применяются для решения таких проблемы как:

Распределение данных. Данные в локальной сети хранятся на центральном ПК и могут быть доступны на рабочих станциях. В связи с этим не надо на каждом рабочем месте иметь накопители для хранения одной и той же информации.

Распределение ресурсов. Периферийные устройства могут быть доступны для всех пользователей ЛВС. Такими устройствами могут быть, например, сканер или лазерный принтер.

Распределение программ. Все пользователи ЛВС могут совместно иметь доступ к программам, которые были централизованно установлены на одном из компьютеров.

Существует ряд причин, для объединения отдельных персональных компьютеров в ЛВС:

Во-первых, совместное использование ресурсов позволяет нескольким ПК или другим устройствам осуществлять совместный доступ к отдельному диску (файл-серверу), принтерам, к сканерам и другому оборудованию, что снижает затраты на каждого отдельного пользователя.

Во-вторых, кроме совместного использования дорогостоящих периферийных устройств ЛВЛ позволяет аналогично использовать сетевые версии прикладного программного обеспечения.

В-третьих, ЛВС обеспечивает новые формы взаимодействия пользователей в одном коллективе, например работе над общим проектом.

В–четвертых, ЛВС дают возможность использовать общие средства связи между различными прикладными системами (коммуникационные услуги, передача данных и видеоданных, речи и т.д.).

Можно выделить **три принципа** LAN:

1) Открытость – возможность подключения дополнительных компьютеров и других устройств, а так же линий (каналов) связи без изменения технических и программных средств существующих компонентов сети.

2) Гибкость – сохранение работоспособности при изменении структуры в результате выхода из строя любого компьютера или линии связи.

3) Эффективность – обеспечение требуемого качества обслуживания пользователей при минимальных затратах.

У **локальной сети** есть следующие отличительные признаки:

- Высокая скорость передачи данных (до 10 Гб/с), большая пропускная способность;
- Низкий уровень ошибок передачи (высококачественные каналы передачи);
- Эффективный быстродействующий механизм управления обменом данных;
- Точно определенное число компьютеров, подключаемых к сети. В настоящее время трудно представить какую либо организацию без установленной в ней локальной сети, все организации стремятся модернизировать свою работу с помощью локальных сетей.

Так как учебно-теоретическое издание «Компьютерные сети. Интернет вещей и межмашинное взаимодействие» определено на интер-отклик систему взаимодействия с читателем с расстановкой приоритетов в подаче явного и неявного контента, то более детальную информацию по LAN вы сможете получить в учебном издании (QR-код представлен на текущей странице, как и содержимое) Уральского федерального университета им. Первого президента России Б.Н. Ельцина «Основы сетевых технологий» за авторством Руденкова Н.А. и Долинера Л.И.

Частный случай LAN: технологии семейства WLAN (IEEE 802.11) будут расмотрены более детально в Главе VI. Архитектура Internet of things (IoT).

CAN (Campus Area Network — кампусная сеть) — это группа локальных сетей, развернутых на компактной территории (кампусе) какого-либо учреждения и обслуживающие это учреждение - университет, промышленное предприятие, порт, оптовый склад и т.д. При этом сетевое оборудование (коммутаторы, маршрутизаторы) и среда передачи (оптическое волокно, медный завод, Cat5 кабели и др.) данных принадлежит арендатору или владельцу кампуса, предприятия, университета, правительства и так далее.

Кампусом называется группа компактно расположенных зданий или корпусов, например, промышленные предприятия, научные институты и вузы, студенческие городки, гостиничные комплексы, больницы. Для того чтобы создать единое информационное пространство организации, имеющей кампусную структуру, необходимо наличие сетевой интегрированной инфраструктуры, объединяющей отдельные здания.

На базе современных цифровых технологий пользователям кампусной сети предоставляются **следующие возможности**:

Поддержка мультимедийных приложений (голос, видео).

Поддержка широкополосных приложений (голосовые конференции, видео конференции, системы видеонаблюдения).

Увеличение емкости полосы пропускания для сетей, уже развернутых на базе традиционной технологии разделяемого Ethernet.

Поддержка любых новых приложений, которые могут внедряться в кампусе, независимо от специфики используемых сетевых протоколов.

Объединение пользователей с общими интересами (отдел, департамент), которые территориально расположены в различных частях кампуса, в единую виртуальную команду (виртуальную локальную сеть) и контроль доступа к информации, с которой работает группа.

Создание специализированных информационных центров, в которых происходит обработка и хранение данных, необходимых различным группам пользователей. Доступ к таким общим информационным ресурсам должен быть одинаково легким из любой точки кампуса.

Простой механизм подключения к единой сетевой инфраструктуре новых корпусов (зданий), не требующий перестройки существующей сетевой структуры. Высокая производительность и масштабируемость сетевой инфраструктуры, обеспечивающая растущие потребности пользователей в доступной полосе пропускания каналов связи.

Оперативное восстановление работоспособности сети при сбоях.

Сравнительно невысокая цена инсталляции и обслуживания сети при высокой надежности ее функционирования.

Правильно построенная кампусная сеть предприятия представляет собой **иерархическую структуру, состоящую их трех уровней**:

1. магистральный уровень (Core);
2. уровень распределения (Distribution);
3. уровень доступа (Access).

Уровень ядра – находится на самом верху иерархии и отвечает за надежную и быструю передачу больших объемов данных. Трафик, передаваемый через ядро, является общим для большинства пользователей. Сами пользовательские данные обрабатываются на уровне распределения, который, при необходимости, пересылает запросы к ядру.

Для уровня ядра большое значение имеет его отказоустойчивость, поскольку сбой на этом уровне может привести к потере связности между уровнями распределения сети.

Уровень распределения, который иногда называют уровнем рабочих групп, является связующим звеном между уровнями доступа и ядра. В зависимости от способа реализации, уровень распределения может выполнять следующие функции:

· обеспечение маршрутизации, качества обслуживания сети;

· агрегирование каналов;

· переход от одной технологии к другой (от 100Base-TX к 1000Base-T).

Уровень доступа занимается предоставлением доступа пользователей и рабочих групп к ресурсам объединенной сети. Основной задачей уровня доступа является создание точек входа/выхода пользователей в сеть. Уровень выполняет следующие функции:

· управление доступом пользователей и политиками сети;

· создание отдельных доменов коллизий (сегментация);

· подключение рабочих групп к уровню распределения;

· использование технологии коммутируемых локальных сетей.

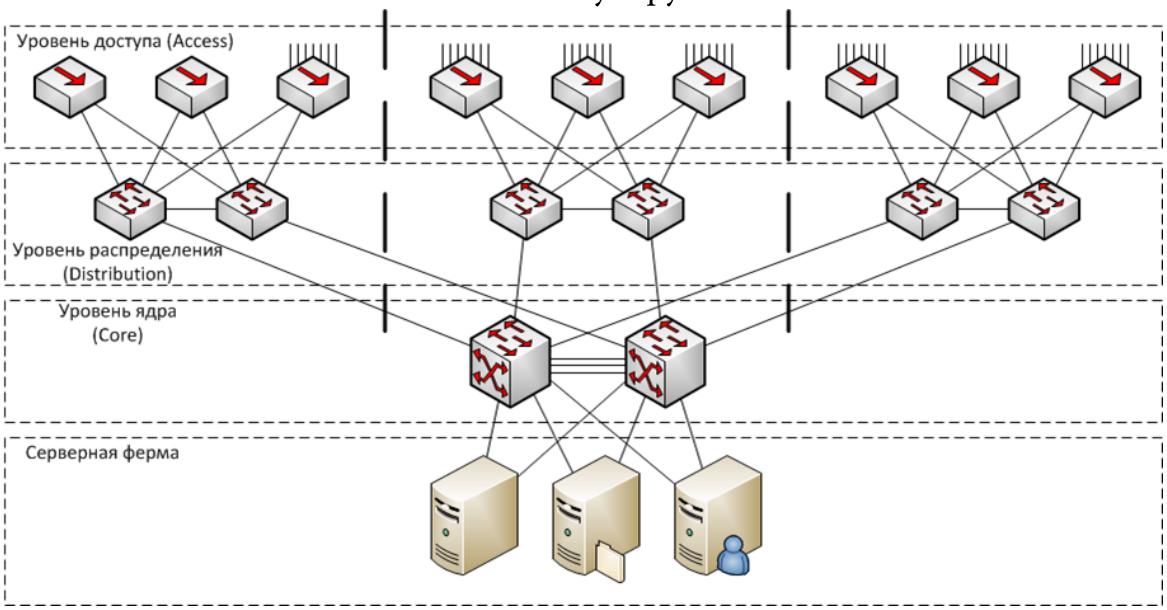


Рис. 12 – Иерархическая структура CAN

Такой подход к описанию CAN дает возможность выбрать оборудование, наиболее точно удовлетворяющее функциональным потребностям конкретной сетевой структуры.

Современная сетевая инфраструктура является разделяемым ресурсом, обеспечивающим работу широкого спектра информационных подсистем.

Эффективность и безопасность деятельности любого современного предприятия напрямую зависит от качества работы информационной инфраструктуры, отвечающей за обслуживание технологических и бизнес процессов.

При проектировании кампусной сети необходимо использовать модульный подход. Данный подход позволяет сформулировать требования по функциональности и защищенности для каждого модуля по отдельности. Построение сети связи с использованием модульного подхода обеспечивает большую гибкость решения и удобство при дальнейшем масштабировании.

Как правило, современная информационная инфраструктура предприятия состоит из следующих составных блоков (рис.13).

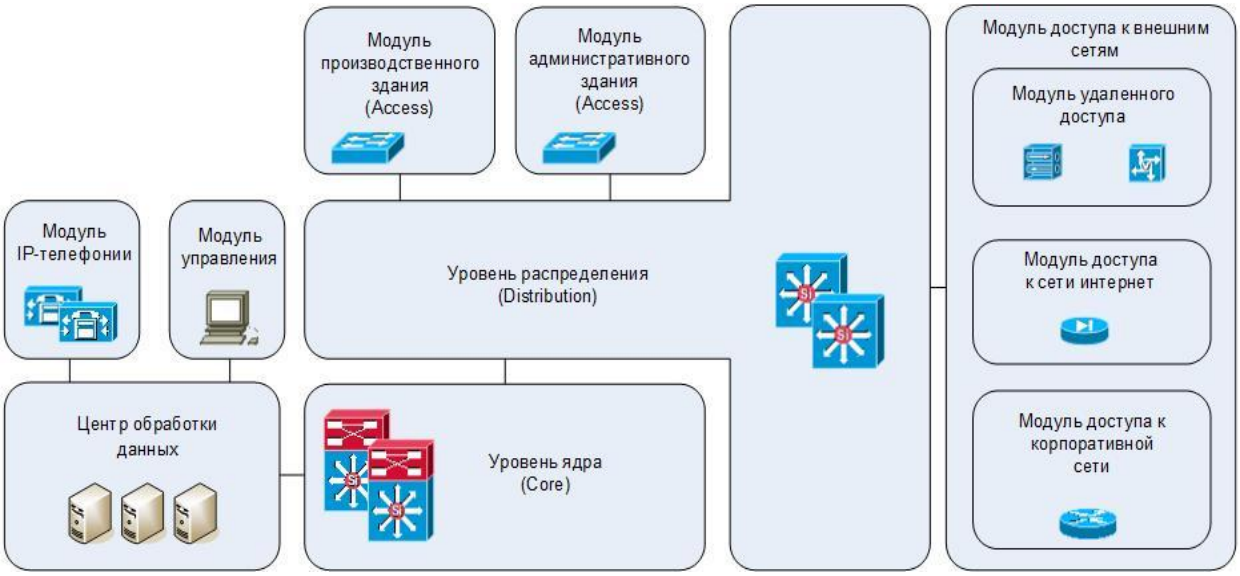


Рис. 13 – Логическая (модульная) схема типовой CAN-сети

1. Модуль управления сетью;
2. Модуль IP-телефонии;
3. Центр обработки данных;
4. Модуль производственного здания (включает в себя коммутатор доступа, рабочие станции и технологические контроллеры);
5. Модуль административного здания (включает в себя один или несколько коммутаторов и рабочие станции);
6. Модуль распределения;
7. Модуль ядра сети;

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ КАМПУСНОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ.

! Магистральный уровень.

Здания или различные части кампуса объединяются высоконадежной коммутируемой магистралью. Высокая надежность ядра достигается за счет резервирования соединений между магистральными сетевыми устройствами и резервирования соединений, идущих от корпусов к ядру сети.

В составе ядра сети используются высокопроизводительные **коммутаторы третьего уровня сетевой модели OSI/ISO**, которые обеспечивают:

маршрутизацию на скорости среды передачи данных (десятки гигабит в секунду); быстрое восстановление при сбоях; балансировку нагрузки;

дополнительные сервисы, например безопасность, диагностику, управление, поддержку мультимедийных приложений в масштабе всей сети, что реализуется за счет встроенного интеллектуального программного обеспечения.

Для использования в качестве среды передачи данных наиболее эффективны две технологии, взаимно дополняющие друг друга и способные удовлетворить требованиям практически любого кампусного дизайна: оптоволоконные линии связи

Оптоволоконные линии связи могут связать кампусные городки, территориально разнесенные на десятки километров, и увеличить пропускную способность ядра сети до десятков гигабит в секунду. Экономически наиболее выгодно использовать оптоволоконные линии связи в компактных кампусах, где требуется обеспечить полную скорость доступа пользователей в любую точку кампуса.

Использование стандартных технологий **10-40GE** или Gigabit Ethernet позволяет гибко регулировать стоимость конечного решения в зависимости от эффективного радиуса кампуса: от сотен метров до 100 км.

Радиодоступ используется в случаях, когда требуется соединить корпуса, между которыми прокладывать физическую проводку неоправданно дорого или просто нецелесообразно, например, для подключения небольших корпусов, складских по мещений.

Идеальным решением в этом случае становится технология радио-Ethernet (все семейство беспроводных стандартов Ethernet IEEE 802.11), предоставляющая следующие возможности:

передавать данные на скорости до 1000 Мбит/с на расстояние до 50 км; быстро организовывать канал связи: для соединения двух корпусов достаточно установить два радиомоста, соединенных с коммутаторами в зданиях.

! Уровень распределения.

На уровне распределения обычно располагаются центральные коммутаторы здания – чаще всего высокопроизводительные коммутаторы. С ядром сети эти коммутаторы соединяются агрегированными каналами Gigabit Ethernet, 10G Ethernet. Каналы, ведущие к ядру сети, дублируются, осуществляется балансировка загрузки основных и дублирующих каналов. Коммутаторы рабочих групп соединяются с коммутаторами здания агрегированными каналами Gigabit Ethernet или Fast Ethernet.

Серверная группа (ферма) (рис.12) обычно располагается в одном из центральных корпусов, которые снабжены несколькими физическими каналами связи с другими корпусами кампуса. Коммутаторы, подключенные к серверам, поддерживают режим балансировки нагрузки на серверы. Для крупных серверных групп также используются дополнительные устройства кэширования информации, которые позволяют снизить загрузку серверов.

! Уровень доступа.

На уровне доступа используются коммутаторы второго уровня, предназначенные для рабочих групп. Они снабжаются высокоскоростными портами Fast Ethernet или Gigabit Ethernet (рис.14), служащими для подключения к центральным коммутаторам здания. Соединения с центральными коммутаторами здания резервируются. Возможно изменение баланса нагрузки, что позволяет повысить эффективность использования резервного канала связи.

Название	Скорость	Кабель	Стандарт
Ethernet	10 Мб/с	«Толстый», «тонкий» коаксиал, Витая пара	802.3
Fast Ethernet	100 Мб/с	Витая пара, оптика	802.3u
Gigabit Ethernet	1 Гб/с	Витая пара, оптика	802.3z, 802.3ab
10G Ethernet	10 Гб/с	Витая пара, оптика	802.3ae, 802.3an

Рис 14. – Типы стандартов Ethernet

Рабочие места пользователей подключаются к коммутируемым портам Fast Ethernet. Высокопроизводительные рабочие станции и серверы могут подключаться к коммутатору с помощью агрегированных каналов Fast Ethernet или по каналу Gigabit Ethernet. Агрегированные каналы позволяют плавно увеличивать производительность сетевого соединения путем объединения нескольких физических интерфейсов в один логический.

Кампусные сети, должны в обязательном порядке проектироваться с учетом требованиям к СКС (структурированным кабельным системам), описанным в ГОСТ Р 53245-2008 «Информационные технологии (ИТ). Системы кабельные структурированные» и ГОСТ Р 53246-2008 «Монтаж основных узлов системы. Методы испытания» и сопутствующих документах.

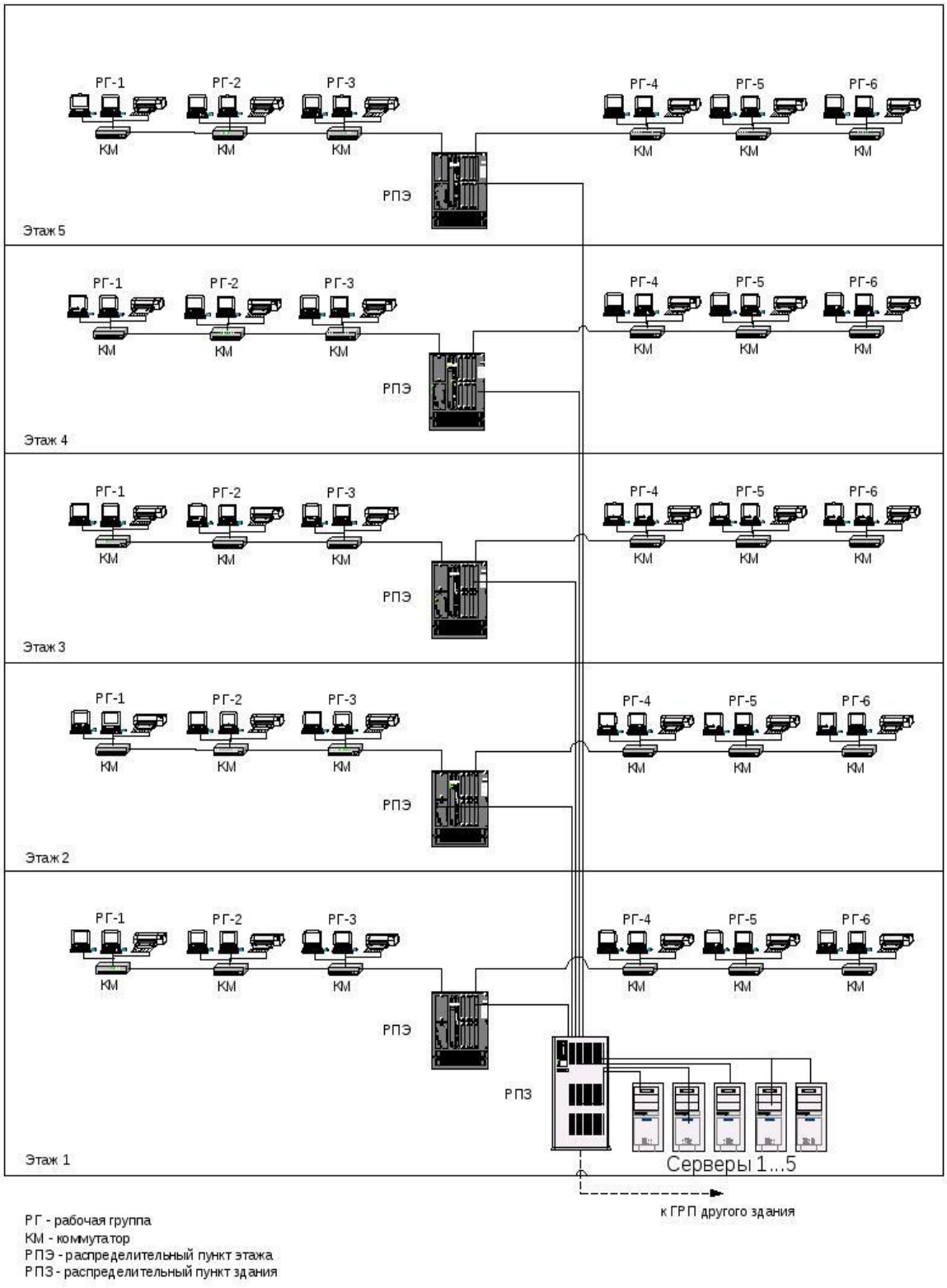


Рис. 15 – Принципиальная схема структурированной кабельной системы CAN

MAN: городские сети.

Городская вычислительная сеть (Metropolitan area network, MAN) (от англ. «сеть крупного города») объединяет компьютеры в пределах города, представляет собой сеть, по размерам меньшую, чем WAN, но большую, чем LAN. Является частным случаем совокупности CAN, объединенных между собой.

Самым простым примером городской сети является система кабельного телевидения. Она стала правопреемником обычных антенных сетей в тех местах, где по тем или иным причинам качество эфира было слишком низким. Общая антенна в этих системах устанавливалась на вершине какого-нибудь холма, и сигнал передавался в дома абонентов через кабельные сети.

Когда Интернет стал привлекать к себе массовую аудиторию, операторы кабельного телевидения поняли, что, внеся небольшие изменения в систему, можно сделать так, чтобы по тем же каналам в неиспользуемой части спектра передавались (причём в обе стороны) цифровые данные. С этого момента кабельное телевидение стало постепенно превращаться в MAN.

MAN — это не только кабельное телевидение. Недавние разработки, связанные с высокоскоростным беспроводным доступом в Интернет, привели к созданию других MAN, которые описаны в стандарте IEEE 802.16, описывающем широкополосные беспроводные ЛВС.

MAN (Metropolitan Area Network) — **опорная сеть провайдера**. То есть точки, связанные скоростными каналами. Расстояние — от 1 до 10 км. Это ещё не WAN, но точно MAN-решения.

MAN применяется для объединения в одну сеть группы сетей, расположенных в разных зданиях. В диаметре такая сеть может составлять от 5 до 50 километров.

Как правило, MAN не принадлежит какой-либо отдельной организации, в большинстве случаев её соединительные элементы и прочее оборудование принадлежит группе пользователей или же провайдеру, кто берёт плату за обслуживание. Об уровне обслуживания заранее договариваются и обсуждают некоторые гарантийные обязательства.

MAN часто действует как высокоскоростная сеть, чтобы позволить совместно использовать региональные ресурсы (подобно большой CAN). Это также часто используется, чтобы обеспечить общедоступное подключение к другим сетям, используя связь с WAN (глобальной сетью).

Информационные технологии — широкий класс дисциплин и областей деятельности, относящихся к технологиям создания, сохранения, управления и обработки данных, в том числе с применением вычислительной техники. В последнее время под информационными технологиями чаще всего понимают компьютерные технологии. В частности, ИТ имеют дело с использованием компьютеров и программного обеспечения для создания, хранения, обработки, ограничения к передаче и получению информации.

Согласно определению, принятому ЮНЕСКО, ИТ - это комплекс взаимосвязанных научных, технологических, инженерных дисциплин, изучающих методы эффективной организации труда людей, занятых обработкой и хранением информации; вычислительная техника и методы организации и взаимодействия с людьми и производственным оборудованием, их практические приложения, а также связанные со всем этим социальные, экономические и культурные проблемы.

Сами ИТ требуют сложной подготовки, больших первоначальных затрат и наукоемкой техники. Их внедрение должно начинаться с создания математического обеспечения, моделирования, формирования информационных хранилищ для промежуточных данных и решений. **Телекоммуникации** - это любые формы связи, способы передачи информации на большие расстояния. Телекоммуникации - это также процессы передачи, получения и обработки информации на расстоянии с применением электронных, электромагнитных, сетевых, компьютерных и информационных технологий. Человечество занималось обработкой информации тысячи лет, а первые информационные технологии основывались на использовании счетов и книгопечатания. Ускорившееся за последние 40 лет развитие информационной технологии в первую очередь связано с появлением компьютеров. Успехи интегральной микроэлектроники обусловили ее проникновение почти во все стороны повседневной жизни, а также привели к многообразному переплетению различных ее отраслей.

Узкий смысл термина «информационная технология» определился к концу 1970-х годов, когда его стали употреблять в связи с использованием современной электронной техники для обработки информации. Информационная технология охватывает всю вычислительную технику и технику связи и отчасти — бытовую электронику, телевизионное и радиовещание. Она находит применение в промышленности, управлении, торговле, образовании, медицине, науке и военной сфере.

В последние 15 лет довольно популярным стало понятие новая информационная технология. Наблюдаются различные подходы к трактовке этого термина.

Под новыми информационными технологиями понимают совокупность внедряемых («встраиваемых») в системы организационного управления принципиально новых методов, способов и средств обработки данных, представляющих собой целостные технологические системы и обеспечивающих целенаправленное создание обработки, передачу, хранение и отображение информационного продукта (данных, идей, знаний) с наименьшими затратами и в соответствии с закономерностями той социальной среды, где развивается эта информационная технология. Новейшие информационные технологии- это специальные термин, характеризующий использование новейших для данного этапа развития достижений науки и техники в области информатизации. Понятие «новая» является относительным и может использоваться на определенном отрезке времени. Так называемую «новизну» информационной технологии придает использование принципиально новых методов и средств преобразования информации.

Принципиальное значение современной информационной технологии состоит в замене машинно-бумажного процесса обработки данных на безбумажный, в котором не только не используются промежуточные носители данных, но и снижается объем фиксации данных на обычных документах. В подобной технологии впервые наблюдается феноменальное явление - процессы обработки информации отделены от процесса переноса массы. Только при обмене между человеком и машиной могут использоваться (но не обязательно) механические перемещения устройств.

Объектом исследования в информационной технологии являются не механические и программные средства, а деятельность человека, т.е. взаимодействие его в системе: **человек — ЭВМ — социальная среда**. Речь идет о создании и преобразовании моделей человеко-машинных систем. В этих моделях деятельность по созданию, использованию и совершенствованию сливается воедино и неразрывно взаимосвязана.

Предметом исследования выступают закономерности становления и развития методов информационной технологии, а также закономерности построения и функционирования средств ее реализации.

В настоящее время **информационная технология** обрела три наиболее характерные функции:

1)персонализация вычислений на основе компьютерных систем и систем интеллектуального интерфейса конечного пользователя с ПК;

2) использование баз данных и баз знаний;

3) применение вычислительных сетей.

3) применение встроенных компьютерных систем;

Эти функции реализуются посредством создания универсальных и специализированных информационных (информационно-технических, информационно-технологических) систем и комплексов.

История развития информационной технологии:

Принципиальное отличие информационной технологии от производственной состоит в следующем:

Информационная технология не может быть непрерывной , так как она соединяет работу рутинного типа (счетоводство, снятие копий, оперативный учет, и т.п.) и работу творческую, не поддающуюся пока формализации (принятие решений). Технология производства непрерывна и отражает строгую последовательность всех операций для выпуска продукции (конвейеризация процесса). Используемые в производственной сфере технологические понятия (норма, норматив, технологический процесс и т.п.) могут быть в настоящее время распространены только на рутинные операции над информацией.

Из всех видов технологий информационная технология сферы управления предъявляет самые высокие требования к «человеческому фактору», оказывая принципиальное влияние на квалификацию работника, содержание его труда, физическую и умственную нагрузку, профессиональные перспективы и уровень социальных отношений. Социальный подход ко всем новациям в информационной технологии особенно важен при внедрении человеко-машинных систем и переносе достижений компьютерной революции из одной социальной сферы в другую.

1. Информационная технология в своем развитии прошла несколько этапов. До второй половины XIXв. основу информационной технологии составляли перо, чернильница и бухгалтерская книга. Коммуникация (связь) осуществлялась путем направления пакетов (депеш). Продуктивность информационной обработки была крайне низкой: каждое письмо копировалось отдельно вручную; помимо счетов, суммируемых также вручную, не было другой информации для принятия решений.

2. На смену «ручной» информационной технологии в конце XIX в. пришла «механическая». Изобретение пишущей машинки, телефона, диктофона, модернизация системы общественной почты –все послужило базой для принципиальных изменений в технологии обработки информации, и, как следствие, в продуктивность работы. По существу , «механическая» технология проложила дорогу к формированию организационной структуры существующих учреждений.

3. 40-60-е годы XX в. характеризуются появлением «электрической» технологии, основанной на широком использовании электрических пишущих машинок со съемными элементами, копировальных машин на обычной бумаге (типа ксерокса), портативных диктофонов.

Они улучшили учрежденческую деятельность за счет повышения качества, количества и скорости обработки документов. Многие современные учреждения базируются на «электрической» технологии.

4. Появление во второй половине 60-х годов больших производительных ЭВМ на периферии учрежденческой деятельности (в вычислительных центрах) позволило сместить акцент в информационной технологии на обработку не формы, а содержания информации. Это было началом формирования «электронной», или «компьютерной» технологии. Как известно, информационная технология управления должна содержать как минимум три важнейших компонента обработки информации: учет, анализ и принятие решений. Эти компоненты реализуются в «вязкой» среде – бумажном «море» документов, которое становится с каждым годом все более необъятным.

5. Сложившиеся в 60-х годах концепции применения АСУ не всегда и не в полной мере отвечают задаче совершенствования управления о неограниченных возможностях «кнопочной» информационной технологии. Методологически эти концепции вычислительной мощности систем АСУ и применении наиболее общих имитационных моделей, которые в ряде случаев далеки от реального механизма оперативного управления.

Название «автоматизированная система управления» не совсем корректно отражает функции, которые такие системы выполняют: точнее было бы «автоматизированная система обеспечения управления (АСОУ), ибо в существующих АСУ понятие «система» не включает решающего

Звена управления-пользователя. Игнорирование этого принципиального обстоятельства, по-видимому, привело к тому, что расширение сет АСУ и повышение мощности их вычислительных средств обеспечили благодаря большим массивам первичных данных улучшение в основном учетных функций управления (справочных, статистических, следящих). Однако учетные функции отражают только прошлое состояние объекта управления и не позволяют оценить перспективы его развития, т.е. обладают низким динамизмом. В других компонентах технологии управления наращивание мощности АСУ не дало ощутимого эффекта. Отсутствие развитых коммуникационных связей рабочих мест пользователя с центральной ЭВМ, характерный для большинства АСУ пакетный режим обработки данных, низкий уровень диалоговой поддержки – все это фактически не обеспечивает высокого качества анализа пользователями данных статистической отчетности и всего интерактивного уровня аналитической работы. Тем самым эффективность АСУ на нижних ступенях управленческой лестницы, т.е. именно там, где формируются информационные потоки, существенно падает вследствие значительной избыточности поступающей информации при отсутствии средств агрегирования данных.

Именно по этой причине, несмотря на ввод дополнительных систем АСУ, с каждым годом возрастает количества работников, занятых учетными функциями: на сегодняшний день шестую часть всех работников аппарата управления составляет учетно-бухгалтерский персонал.

6. Начиная с 70-х годов сформировалась тенденция перенесения центра тяжести с развития АСУ на фундаментальные компоненты информационной технологии (особенно на аналитическую работу) с максимальным применением человеко-машинных процедур. Однако по-прежнему вся эта работа проводилась на мощных ЭВМ, размещаемых централизованно в вычислительных центрах. При этом в основу построения подобных АСУ была положена гипотеза, согласно которой задачи анализа и принятия решений относились к классу формализуемых, поддающихся математическому моделированию. Предполагалось, что такие АСУ должны были повысить качества, полноту, подлинность и своевременность информационного обеспечения лиц, принимающих решения, эффективность работы которых будет возрастать благодаря увеличению числа анализируемых задач.

Однако внедрение подобных систем дало весьма отрезвляющие результаты. Оказалось, что применяемые математические модели имеют ограниченные возможности практического использования: аналитическая работа и процесс принятия решений происходят в отрыве от реальной ситуации и не подкрепляются комммуникационным процессом формирования. Для каждой новой задачи требуется новая модель, а поскольку модель создавалась специалистами по математическим методам, а не пользователем, то процесс принятия решений происходит как бы не в реальном масштабе времени, и теряется творческий вклад самого пользователя, особенно при решении нетиповых управленческих задач. При этом вычислительный потенциал управления, сосредоточенный в вычислительных центрах, находится в отрыве от других средств и технологий обработки информации вследствие неэффективной работы нижних ступеней т необходимости непрерывных конверсий информации. Это также понижает эффективность информационной технологии при решении задач на верхних ступенях управленческой лестницы. К тому же для сложившейся в АСУ организационной структуры технических средств характерны низкий коэффициент их использования, значительные сроки (не всегда выполняемые) проектирования автоматизированных систем и невысокая их рентабельность из-за слабого воздействия результатов автоматизации на эффективность управления.

7. С появлением ПК на «гребне микропроцессорной революции» происходит принципиальная модернизация идеи АСУ: от вычислительных центров и централизации управления к распределенному вычислительному потенциалу, повышению однородности технологии обработки информации и деценрализации управления.

Такой подход нашел свое воплощение в **системах поддержки принятия решения** (СППР) и **экспертных системах** (ЭС), которые характеризуют новый этап компьютеризации технологии организационного управления, по существу, -этап **персонализации АСУ**. **Системность** - основной признак СППР и признание того, что самая совершенная ЭВМ не может заменить человека. В данном случае речь идет о структурной человеко-машинной единице управления, которая оптимизируется в процессе работы: возможности ЭВМ расширяются за счет структуризации пользователем решаемых задач и пополнения ее базы знаний, а возможности пользователя- за счет автоматизации тех задач, которые ранее было нецелесообразно переносить на ЭВМ по экономическим или техническим соображениям. Становится возможным анализировать последствия различных решений и получать ответы на вопросы типа « что будет, если…?», не тратя времени на трудоемкий процесс программирования.

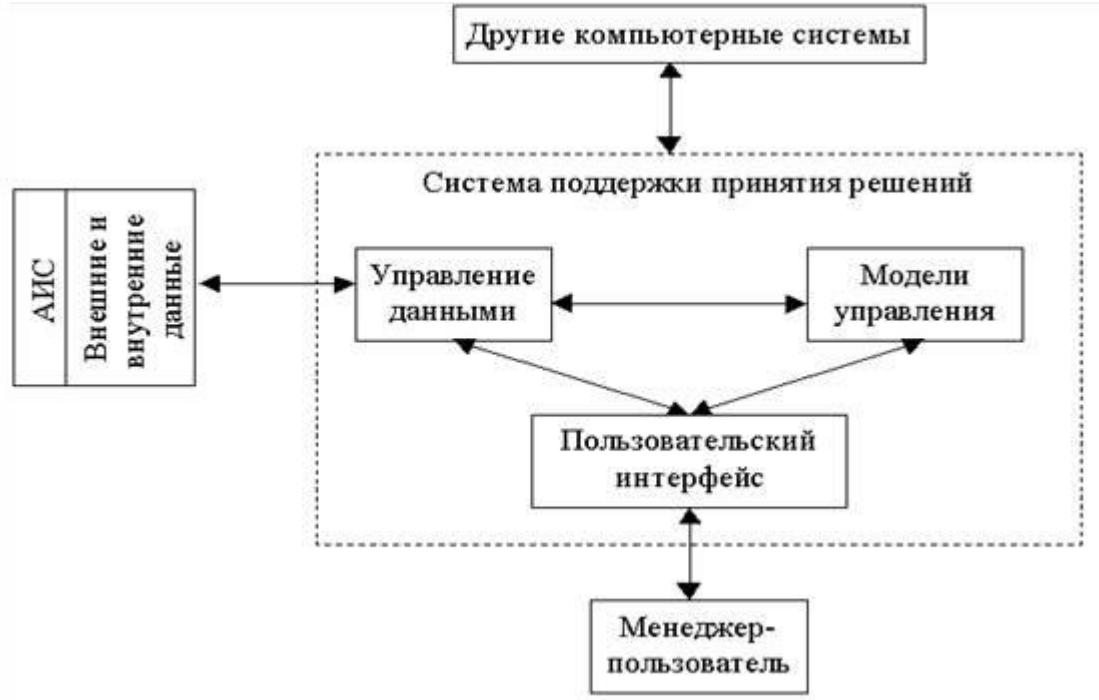


Рис. 16 - Система поддержки принятия решения

Важнейший аспект внедрения СППР (рис.16) и ЭС – рационализация повседневной деятельности работников управления. В результате их внедрения на нижних ступенях управления существенно укрепляется весь фундамент управления, уменьшается нагрузка на централизованные вычислительные системы и верхние ступени управления, что позволяет сосредоточить в них вопросы решения крупных долгосрочных стратегических задач. Естественно, что «компьютерная» технология. СППР должна использовать не только ЭВМ, но и другие современные средства обработки информации.

Концепция СППР требует пересмотра существующих подходов к управлению трудовыми процессами в учреждении. По существу на базе СППР формируемся новая человеко-машинная трудовая единица с квалификацией труда, его нормированием и оплатой. Она аккумулирует знания и умение конкретного человека (пользователя СППР) с интегрированными знаниями и умением, заложенным в ПЭВМ (экспертные системы, системы принятия решений, системы обеспечивающей технологии и др.).

В заключение раздела кратко остановимся на состоянии и тенденциях развития ИТ в США, странах Западной Европы, Японии можно охарактеризовать следующими тезисами:

1. Наличие большого количества промышленно функционирующих БД большого объема, содержащих информацию практически по всем видам деятельности общества.

2. Создание технологий, обеспечивающих интерактивный доступ массового пользователя к этим информационным ресурсам. Технической основой данной тенденции явились государственные и частные системы связи и передачи данных общего назначения и специализированные, объединенные в национальные, региональные и глобальные ИВС.

3. Расширение функциональных возможностей информационных систем, обеспечивающих параллельную одновременную обработку Баз Данных (БД) с разнообразной структурой данных, мультиобъектных документов, гиперсред, в том числе реализующих технологии создания и ведения гипертекстовых БД. Создание локальных, многофункциональных проблемно-ориентированных информационных систем различного назначения на основе мощных ПК и локальных сетей ПК.

4. Включение в информационные системы элементов интеллектуализации интерфейса пользователя с системами, экспертных систем, систем машинного перевода, индексирования информации и других технологических средств. Ведущие промышленно развитые страны имеют государственную политику в области развития ИТ и соответствующие программы, которые субсидируются правительством, государственными учреждениями, частными фирмами и ассоциациями.

§ IV. Микроархитектура компьютерных сетей.

I. Эталонный подход: Friend-to-friend и Peer-to-Peer обмен.

Архитектура сети – это набор параметров, правил, протоколов, алгоритмов, карт, которые позволяют изучать сеть.

Протокол – это набор семантических и синтаксических правил, определяющий поведение функциональных блоков сети или передачи данных. Другими словами, протокол – это совокупность соглашений относительно способа представления данных, обеспечивающего их передачу в нужных направлениях и правильную интерпретацию данных всеми участками процесса информационного обмена. Поскольку информационный обмен – это процесс многофункциональный, то протоколы делятся на уровни. За каждым уровнем закрепляется группа родственных функций. Для правильного взаимодействия узлов различных вычислительных сетей их архитектура должна быть открытой (известной). Существует несколько систем межсетевого взаимодействий, как например известная вам модель OSI/ISO, снискавшая массовое распространение во всем мире. Однако, модель OSI/ISO дает достаточно плоские, поверхностные представления, к самим сетям, к разности подхода обмена между конечными устройствами. Стек (реже именуемый моделью) протоколов TCP/IP еще более узконаправлен в своих функциях.

Сеть — базис, на который опирается всё, и производить изменения на ней довольно сложно — сервисы не терпят, когда сеть лежит, равно как и наоборот. Зачастую вывод из эксплуатации одного узла может сложить большую часть приложений и повлиять на много клиентов. Отчасти поэтому сетевой инжиниринг сопротивляться любым физическим изменениям — «потому что сейчас оно как-то работает (мы, возможно, даже не знаем как), а тут надо что-то новое настроить, и неизвестно как оно повлияет на сеть». А еще чаще необходимо расширить возможности передачи информации. И на помощь этому приходит **логическая архитектура передачи данных**:

Оверлейная сеть (от англ. Overlay Network) — общий случай **логической сети**, создаваемой поверх любой другой компьютерной сети. Узлы оверлейной сети могут быть связаны либо физическим соединением, либо логическим, для которого в основной сети существуют один или несколько соответствующих маршрутов из физических соединений.

Примерами оверлеев являются сети VPN и одноранговые сети, которые работают на основе интернета и представляют собой «надстройки» над классическими сетевыми протоколами, предоставляя широкие возможности, изначально не предусмотренные разработчиками основных протоколов. Коммутируемый доступ в интернет фактически осуществляется через оверлей (например, по протоколу PPP), который работает «поверх» обычной телефонной сети. Основное преимущество оверлейных сетей заключается в том, что они позволяют разрабатывать и эксплуатировать новые крупномасштабные распределённые сервисы без внесения каких-либо изменений в основные протоколы сети. Распространённым недостатком оверлеев являются повышенные затраты при передаче информации из-за дополнительного уровня обработки пакетов или неоптимальных маршрутов.

Одноранговая, децентрализованная, или пиринговая (англ. peer-to-peer, P2P — равный к равному) сеть — оверлейная компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются все пиры.

Впервые фраза «peer-to-peer» была использована в 1984 году при разработке архитектуры Advanced Peer to Peer Networking (APPN) фирмы IBM.

Устройство одноранговой сети

В сети присутствует некоторое количество машин, при этом каждая может связаться с любой из других. Каждая из этих машин может посылать запросы другим машинам на предоставление каких-либо ресурсов в пределах этой сети и, таким образом, выступать в роли клиента. Будучи сервером, каждая машина должна быть способной обрабатывать запросы от других машин в сети, отсылать то, что было запрошено. Каждая машина также должна выполнять некоторые вспомогательные и административные функции (например, хранить список других известных машин-«соседей» и поддерживать его актуальность).

Любой член данной сети не гарантирует своего присутствия на постоянной основе. Он может появляться и исчезать в любой момент времени. Но при достижении определённого критического размера сети наступает такой момент, что в сети одновременно существует множество серверов с одинаковыми функциями.

Идея классического peer-to-peer обмена заключается в том, что каждый peer знает и поддерживает информацию о других участниках. Когда новый клиент подключается к сети, он может узнать у любого пира информацию о том, где и какие файлы сейчас доступны.

Когда клиент начинает скачивает файл себе на компьютер, то скачанные части этот файла сразу становятся доступны для скачивания другим пользователям. Никто не даёт гарантию, что каждый сервер будет находиться длительное время в сети и давать скачивать информацию, напротив - ситуация, когда сервер пропадает в процессе загрузки, является естественной. В данном случае будет найден новый сервер, который может продолжить передачу данных.

Для поддержания списка активных peer-ов каждый сервер посылает другим серверам heartbeat. **Heartbeat (удар сердца)** - это сообщение, которое один сервер посылает другому, чтобы сказать ему, что он жив. Соответственно, если heartbeat долго не приходит, значит этот сервер нужно удалить из списка активных peer-ов. Постоянно обмениваться heartbeat-ом с большим количеством серверов трудоёмко. Поэтому у каждого сервера есть два параметра -- нижняя и верхняя граница на размер списка активных серверов. Когда это количество становится ниже нижней границы, запускается поиск новых участников. Сервер запрашивает у других серверов список активных peer-ов и добавляет некоторых из них в свой список, но при этом следит за тем, чтобы размер списка не превысил верхнюю границу.

В некоторых peer-to-peer сетях кроме равноправных узлах присутствуют сервера, которые выполняют административные функции, такие как поддержка базы онлайн пользователей. К частично децентрализованным сетям относятся например eDonkey, BitTorrent, Direct Connect, The Onion Router.

Одна из областей применения технологии одноранговых сетей — обмен файлами. Пользователи файлообменной сети выкладывают какие-либо файлы в папку общего доступа («расшаренную» от англ. share — делиться) на своём компьютере, содержимое которой доступно для скачивания другим пользователям. Какой-нибудь другой пользователь сети посылает запрос на поиск какого-либо файла. Программа ищет у клиентов сети файлы, соответствующие запросу, и показывает результат. После этого пользователь может скачать файлы у найденных источников. В современных файлообменных сетях информация загружается сразу из нескольких источников. Её целостность проверяется по контрольным суммам.

Friend-to-friend (друг-к-другу, F2F) — разновидность одноранговой сети (P2P), в которой пользователи устанавливают прямые соединения только с заранее выбранными пользователями (друзьями, англ. friend). Для аутентификации могут использоваться цифровые подписи или пароли.

В отличие от других типов приватных P2P-сетей, пользователи F2F-сети не знают, кто за пределами их круга друзей пользуется сетью. Этим обеспечивается анонимность пользователей. RetroShare, GNUnet и Freenet — примеры ПО, на основе которого можно создать F2F-сеть (GNUnet по умолчанию не настроен для работы в режиме F2F-сети). Термин «friend-to-friend-сеть» (F2F-сеть) был предложен Даниэлем Бриклином в 2000 году.

Преимущества F2F

1. Использование F2F-сетей позволяет избегать атак типа MITM, то есть пользователи могут без опасений обмениваться секретными данными (например, крипто-ключами) со своими друзьями. **Атака посредника**, или атака «человек посередине» (англ. Man in the middle (MITM)) — вид атаки в криптографии и компьютерной безопасности, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом. Является методом компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию. Одним из примеров атак типа «человек посередине» является активное прослушивание, при котором злоумышленник устанавливает независимые связи с жертвами и передаёт сообщения между ними. Тем самым он заставляет жертв поверить, что они разговаривают непосредственно друг с другом через частную связь, фактически же весь разговор управляется злоумышленником. Злоумышленник должен уметь перехватывать все передаваемые между двумя жертвами сообщения, а также вводить новые. В большинстве случаев это довольно просто, например, злоумышленник может вести себя как «человек посередине» в пределах диапазона приёма беспроводной точки доступа (Wi-Fi)

2. При использовании F2F-сетей пользователь может настроить фаерволл так, чтобы доступ к порту программы, обеспечивающей подключение к сети F2F, был разрешён только друзьям (так как IP-адреса друзей заведомо известны). Благодаря этому случайные люди не смогут доказать, что с IP-адреса пользователя можно было получить доступ к обсуждаемым файлам.

3. Поскольку программы, обеспечивающие подключение к сети F2F (как например Gnutella на рисунке 17), шифруют данные, передаваемые между соседними узлами сети, и используют неполное шифрование при передаче данных между оконечными точками, пользователи промежуточных узлов могут отслеживать, какого рода файлы передаются через них.

4. То, что соединения возможны только между доверенными узлами (между друзьями), защищает пользователей от взломщиков, которые могли бы использовать уязвимость.

Недостатки F2F-обмена:

В настройках программного обеспечения, обеспечивающей подключение к сети F2F, нужно вручную указывать список всех своих друзей. Ситуация усугубляется, если пользователь хочет опробовать несколько различных программ. Обычно не так много друзей (пиров (peer)) готовы участвовать в сети в режиме 24/7.

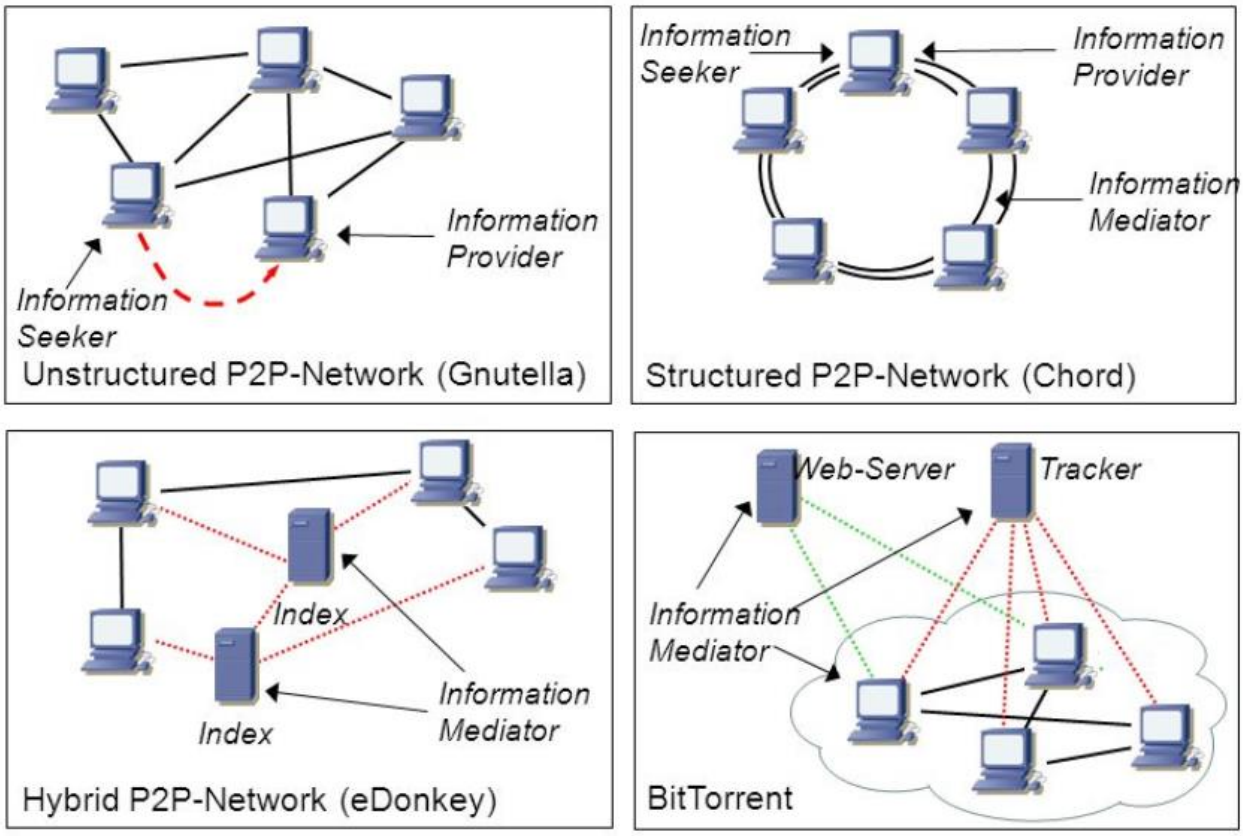


Рис. 17 – P2P/F2F решения

§ V. Беспроводные сенсорные сети.

I. **Интеллектуальные системы на базе сенсорных сетей.**

Беспроводная сенсорная сеть, или беспроводная датчиковая сеть, — **распределённая, самоорганизующаяся** сеть множества **датчиков** и **исполнительных** устройств, объединённых между собой посредством радиоканала. Область покрытия подобной сети может составлять от нескольких метров до нескольких километров за счёт способности ретрансляции сообщений от одного узла к другому.

Одним из первых прообразов сенсорной сети можно считать **SOSUS**, предназначенную для обнаружения и идентификации подводных лодок.

В середине 1990-х годов технологии беспроводных сенсорных сетей стали активно развиваться, в начале 2000-х годов развитие микроэлектроники позволило производить для таких устройств достаточно дешёвую элементную базу. Беспроводные сенсорные сети начала 2010-х годов в основном базируются на стандарте **ZigBee,** который будет рассматриваться в следующей главе. .

Многие отрасли и сферы деятельности (промышленность, транспорт, коммунальное хозяйство, охрана) заинтересованы во внедрении сенсорных сетей, и число потребителей непрерывно увеличивается. Тенденция обусловлена усложнением технологических процессов, развитием производства, расширяющимися потребностями частных лиц в сегментах безопасности, контроля ресурсов и использования товаро-материальных ценностей. С развитием микроэлектронных технологий появляются новые практические задачи и теоретические проблемы, связанные с применениями сенсорных сетей в промышленности, жилищно-коммунальном комплексе, домашних хозяйствах.

Использование недорогих **беспроводных сенсорных устройств** контроля параметров открывает новые области для применения систем телеметрии и контроля, такие как: Своевременное выявление возможных отказов исполнительных механизмов, по контролю таких параметров, как вибрация, температура, давление и т. п.; Контроль доступа к удалённым системам объекта мониторинга в режиме реального времени; обеспечение охраны музейных ценностей; обеспечение учёта экспонатов; автоматическая ревизия экспонатов; Автоматизация инспекции и технического обслуживания промышленных активов; Управление коммерческими активами; Применение как компоненты в энерго- и ресурсосберегающих технологий; Контроль экологических параметров окружающей среды.

Беспроводные сенсорные сети состоят из миниатюрных вычислительных устройств — **мотов**, снабжённых датчиками (например, температуры, давления, освещённости, уровня вибрации, местоположения и т. п.) и передатчиками, работающими в заданном радиодиапазоне. Гибкая архитектура, снижение затрат при монтаже выделяют беспроводные сети интеллектуальных сенсоров среди других беспроводных и проводных интерфейсов передачи данных, особенно когда речь идет о большом количестве соединенных между собой устройств, сенсорная сеть позволяет подключать до 65 000 устройств. Постоянное снижение стоимости беспроводных решений, повышение их эксплуатационных параметров позволяют постепенно перейти с проводных решений в системах сбора телеметрических данных, средств дистанционной диагностики, обмена информации на беспроводные.

Технология ретранслируемой ближней радиосвязи 802.15.4/ZigBee, известная как «Сенсорные сети», является одним из современных направлений развития самоорганизующихся отказоустойчивых распределенных систем наблюдения и управления ресурсами и процессами. Сегодня технология беспроводных сенсорных сетей, является единственной беспроводной технологией, с помощью которой можно решить задачи наблюдения и контроля, которые критичны к времени работы сенсоров. Объединённые в беспроводную сеть датчики образуют территориально-распределённую самоорганизующуюся систему сбора, обработки и передачи информации.

Основной областью применения является контроль и наблюдение измеряемых параметров физических сред и предметов. Принятый стандарт IEEE 802.15.4 описывает контроль доступа к беспроводному каналу и физический уровень для низкоскоростных беспроводных личных сетей, то есть два нижних уровня согласно сетевой модели OSI.

Сенсорные сети могут состоять из различных типов датчиков, например, сейсмических, датчиков определения магнитного поля, тепловых, инфракрасных, акустических, которые в состоянии осуществлять самые разнообразные измерения условий окружающей среды.

Военное применение

Беспроводные сенсорные сети могут быть неотъемлемой частью военного управления, связи, разведки, наблюдения и систем ориентирование (C4ISRT). Быстрое развертывание, самоорганизации и отказоустойчивость – это характеристики сенсорных сетей, которые делают их перспективным инструментом для решения поставленных задач.

Поскольку сенсорные сети могу быть основаны на плотном развертывании одноразовых и дешевых узлов, то уничтожение некоторых их них во время военных действий не повлияет на военную операцию так, как уничтожение традиционных датчик. Поэтому использование сенсорных сетей лучше подходит для сражений. Перечислим еще некоторые способы применение таких сетей: мониторинг вооружения и боеприпасов дружественных сил, наблюдение за боем; ориентация на местности; оценка ущерба от битв; обнаружение ядерных, биологических и химических атак. Мониторинг дружественных силы, вооружения и боеприпасов: лидеры и командиры могут постоянно контролировать состояние своих войск, состояние и наличие оборудования и боеприпасов на поле боя с помощью сенсорных сетей. К каждому транспортному средству, оборудованию и важным боеприпасам могут быть прикреплены датчики, которые сообщают их статус. Эти данные собирается вместе в ключевых узлах, и направляются руководителям.

Данные также могут быть переадресованы на верхние уровни иерархии командования для объединения с данными из других частей. Наблюдения боя: критические участки, пути, маршруты и проливы могут быть быстро покрыты сенсорными сетями для изучения деятельности сил противника. Во время операций или после разработки новых планов сенсорные сети могут быть развернуты в любое время для наблюдения за боем. Разведка сил противника и местности: Сенсорные сети могут быть развернуты на критических территориях, и могут быть собраны в течении нескольких минут ценные, подробные и своевременные данные о силах противника и местности, прежде чем враг сможет их перехватить. Ориентация: сенсорные сети могут быть использованы в системах наведения интеллектуальных боеприпасов. Оценка ущерба после боя: непосредственно перед или после нападения, сенсорные сети могут быть развернуты в целевой области для сбора данных об оценке ущерба. Обнаружение ядерных, биологических и химических атак: при применении химического или биологического оружия, использование которого близко к нулю, важное значение иметь своевременное и точное определение химических агентов.

Могут быть использованы сенсорные сети в качестве систем предупреждения химических или биологических атак и данные собранные в короткие сроки помогут резко уменьшить количество жертв. Также можно использовать сенсорные сети для подробной разведки, после обнаружения таких атак. Например, можно осуществлять разведку в случае радиационных заражений, не подвергая людей радиации.

Экологическое применение

Некоторые из направлений в экологии, где применяют сенсорные сетей: отслеживание движения птиц, мелких животных и насекомых; мониторинг состояния окружающей среды, с целью выявления ее влияния на сельскохозяйственные культуры и скота; орошения; широкомасштабный мониторинга земли и исследования планет; химическое / биологическое обнаружение; обнаружение лесных пожаров; метеорологические или геофизические исследования; обнаружение наводнений; и исследование загрязнения. Обнаружение лесных пожаров: поскольку моты могут быть стратегически и плотно развернуты в лесу, то они могут ретранслировать точное происхождение огня до того, как пожар станет неконтролируемым. Миллионы датчик могут быть развернуты на постоянной основе. Они могут быть оснащены солнечными батареи, т.к. узлы могут быть оставлены без присмотра на месяцы и даже годы.

Моты будут работать сообща для выполнения задач распределенного зондирования и преодоления препятствий, таких как деревья и скалы, которые блокируют работу проводных датчиков. Отображение биосостояния окружающей среды [требует сложных подходов к интеграции информации во временных и пространственных масштабах. Прогресс в области технологии дистанционного зондирования и автоматизированный сбор данных, позволили значительно снизить затраты на исследования. Преимущество данных сетей в том, что узлы могут быть соединены с Интернетом, который позволяет удаленным пользователям осуществлять контроль, мониторинг и наблюдения за окружающей средой.

Хотя спутниковые и бортовые датчики являются полезными в наблюдении за большим разнообразием, например, пространственной сложности видов доминирующих растений, они не позволяют наблюдать за мелкими элементами, которые составляет большую часть экосистемы. В результате возникает потребность в развертывании на местах узлов беспроводных сенсорных сетей.

Одним из примеров применения это составление биологической карты окружающей среды в заповеднике в Южной Калифорнии. Три участка покрыты сетью, в каждой их которых по 25-100 узлов, которые используются для постоянного наблюдения за состоянием окружающей среды. Обнаружение наводнений: примером обнаружения наводнений является система оповещения в США.

Несколько типов датчиков, размещенных в системе оповещения, определяют уровень осадков, уровень воды и погоду.

Научно-исследовательские проекты, такие как COUGAR Device Database Project в Корнельском университете и проект DataSpace в Университете Rutgers, изучают различные подходы к взаимодействию с отдельными узлами в сети для получения снимков и долго собираемых данных. Сельское хозяйство: преимуществом сенсорных сетей также является возможность контролировать уровень пестицидов в воде, уровень эрозии почвы и уровень загрязнения воздуха в режиме реального времени.

Применение в медицине

Одним из применений в медицине является устройства для инвалидов; мониторинг пациентов; диагностика; мониторинг использования медикаментов в больницах; сбор физиологических данных человека; и мониторинга врачей и пациентов в больницах. Мониторинг физиологического состояния человека: физиологические данные, собранные сенсорными сетями могут храниться в течение длительного периода времени и могут использоваться для медицинского исследования. Установленные узлы сети могут также отслеживать движения пожилых людей и, например, предупреждать падения. Эти узлы невелики и обеспечивают пациенту большую свободу передвижения, в тоже время позволяют врачам выявить симптомы болезни заранее. Кроме того, они способствуют обеспечению более комфортной жизни для пациентов в сравнении с лечением в больнице. Для проверки возможности такой системы на факультете медицины Grenoble–France был создан “Здоровый умный дом ".

Мониторинг врачей и пациентов в больнице: каждый пациент имеет небольшой и легкий узел сети. Каждый узел имеет свою конкретную задачу. Например, один может следить за сердечным ритмом, в то время как другой снимает показания кровяного давления. Врачи могут также иметь такой узел, он позволит другим врачам найти их в больнице. Мониторинг медикаментов в больницах: Узлы могут быть присоединены к лекарствам, тогда шансы выдачи неправильного лекарства, могут быть сведены к минимуму. Так, пациенты будут иметь узлы, которые определяют их аллергию и необходимые лекарства. Компьютеризированные системы, как описано выше, показали, что они могут помочь свести к минимуму побочные эффекты от ошибочной выдачи препаратов.

Применение в доме

Автоматизация дома: смарт-узлы могут быть интегрированы в бытовые приборы, например в пылесосы, микроволновые печи, холодильники и видеомагнитофоны. Они могут взаимодействовать друг с другом и с внешней сетью через Интернет или спутник.

Это позволит конечным пользователям легко управлять устройствами дома как локально, так и удаленно. Умная окружающая среда: дизайн смарт-среды может иметь два различных подхода, т.е., ориентированного на человека или на технологии. В случае первого подхода, смарт-среда должна адаптироваться к потребностям конечных пользователей с точки зрения взаимодействия с ними. Для технологически-центрированных систем должны быть разработаны новые аппаратные технологий, сетевые решений, и промежуточные приложения. Примеры того, как узлы могут быть использованы для создания смарт-среды описана в . Узлы могут быть встроены в мебель и технику, они могут общаться друг с другом и сервером комнаты. Сервер комнаты может также общаться с другими серверами комнат, чтобы узнать о услугах, которые они могут предложить, например, печать, сканирование и работа с факсом. Эти сервера и сенсорные узлы могут быть интегрированы в существующие встраиваемые устройства и составлять самоорганизующиеся, саморегулируемые и адаптивные системы, основанные на модели теории управления, как описано в работе.

Факторы, влияющие на разработку моделей сенсорных сетей.

Разработка сенсорных сетей зависит от многих факторов, которые включают в себя отказоустойчивость, масштабируемость, издержек производства, вид операционной среды, топологию сенсорной сети, аппаратные ограничения, модель передачи информации и потребление энергии. Эти факторы рассматриваются многими исследователями. Однако ни в одном из этих исследований полностью не учтены все факторы, которые влияют на разработку сетей. Они важны, поскольку служат в качестве ориентира для разработки протокола или алгоритмов работы сенсорных сетей. Кроме того, эти факторы могут быть использованы для сравнения различных моделей.

II. Беспроводные самоорганизующиеся сети.

С точки зрения инженера-электронщика, датчик или сенсор – это устройство, которое используется для сбора информации о физическом процессе или физическом явлении и преобразования его в электрические сигналы, которые можно обрабатывать, измерять и анализировать. Термин «физический процесс», используемый в приведенном определении датчика, может быть любой реальной информацией, такой как температура, давление, свет, звук, движение, положение, поток, влажность, излучение и т. д. Что же из себя представляет беспроводная сенсорная сеть в реальности?

Как упоминалось ранее, в предыдущей статье, типичная сенсорная сеть состоит из датчиков, контроллера и системы связи. Если система связи в сенсорной сети реализована с использованием беспроводного протокола, то эти сети называются беспроводными сенсорными сетями или просто **WSN** (Wireless Sensor Networks).

Типичная беспроводная сенсорная сеть может быть разделена на два элемента: **сенсорный узел** (рис.18) и **сетевая архитектура** (рис.19).

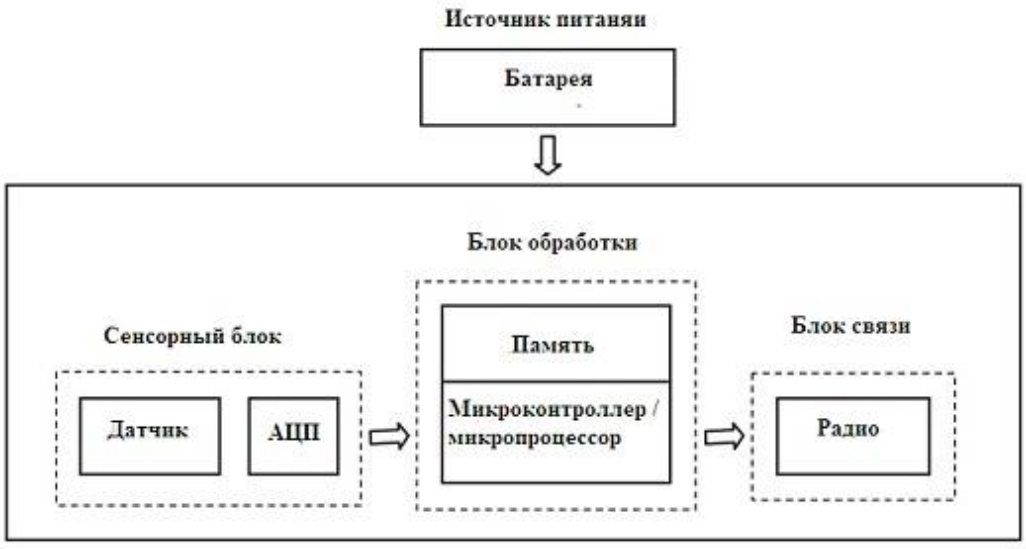


Рис. 18 – Сенсорный узел

Датчик собирает аналоговые данные из физического мира, и АЦП преобразует эти данные в цифровые данные. Основной процессор, который обычно является микропроцессором или микроконтроллером, выполняет интеллектуальную обработку данных и манипулирование ими.

Система связи состоит из системы радиосвязи, обычно радиостанции ближнего действия, для передачи и приема данных. Поскольку все компоненты являются устройствами с низким энергопотреблением, для питания всей системы используется небольшая батарея, такая как CR-2032 (такая используется в модуле часов реального времени (RTC) в вашем компьютере).

Несмотря на название, сенсорный узел состоит не только из сенсорного компонента, но и из других важных функций, таких как устройства обработки, связи и хранения. Благодаря всем этим функциям, компонентам и усовершенствованиям узел датчика отвечает за сбор данных физического мира, анализ сети, корреляцию данных и объединение данных другого датчика с собственными данными.

Архитектура беспроводной сенсорной сети

Когда большое количество сенсорных узлов развернуто в большой области для совместного мониторинга физической среды, объединение в сеть этих сенсорных узлов одинаково важно. **Сенсорный узел** в WSN не только связывается с другими сенсорными узлами, но также и с базовой станцией, используя беспроводную связь.

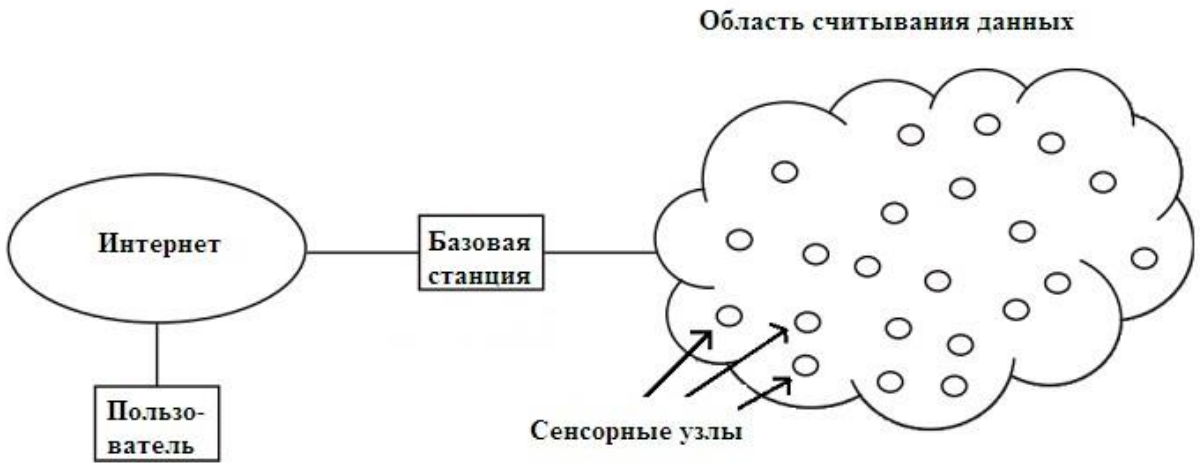


Рис.19 – Архитектура беспроводной сенсорной сети в общем виде

Базовая станция отправляет команды на сенсорные узлы, а сенсорные узлы выполняют задачу, взаимодействуя друг с другом. После сбора необходимых данных сенсорные узлы отправляют данные обратно на базовую станцию. Базовая станция также действует как шлюз для других сетей через Интернет. После приема данных от узлов датчиков базовая станция выполняет простую обработку данных и отправляет обновленную информацию пользователю через Интернет.

Если каждый узел датчика (сенсорного узла – см. рис 20) подключен к базовой станции, он известен как архитектура сети с одним переходом (или **<u>односкачковая архитектура – рис. 21</u>**). Хотя передача на большие расстояния возможна, потребление энергии для связи будет значительно выше, чем для сбора и вычисления данных.

Рис.20 – Практическая реализация сенсорного узла

Следовательно, **многоскачковая** сетевая архитектура обычно используется в серьезных приложениях. Вместо одной единственной линии связи между узлом датчика и базовой станцией данные передаются через один или несколько промежуточных узлов.

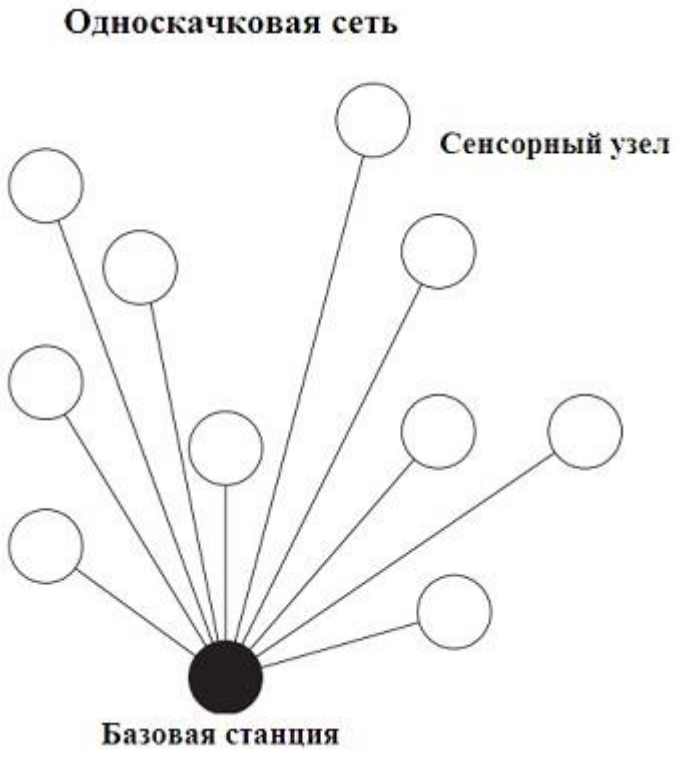


Рис.20 – Схема односкачковой сенсорной сети

Это может быть реализовано двумя способами: Архитектура плоской сети и архитектура иерархической сети.

В **плоской архитектур**е базовая станция отправляет команды всем сенсорным узлам, но сенсорный узел с совпадающим запросом ответит, используя свои равноправные узлы через **многоскачковый путь.** В иерархической архитектуре группа сенсорных узлов формируется в виде кластера, и сенсорные узлы передают данные в соответствующие головы кластера. Затем головы кластера могут передавать данные на базовую станцию (рис.21).

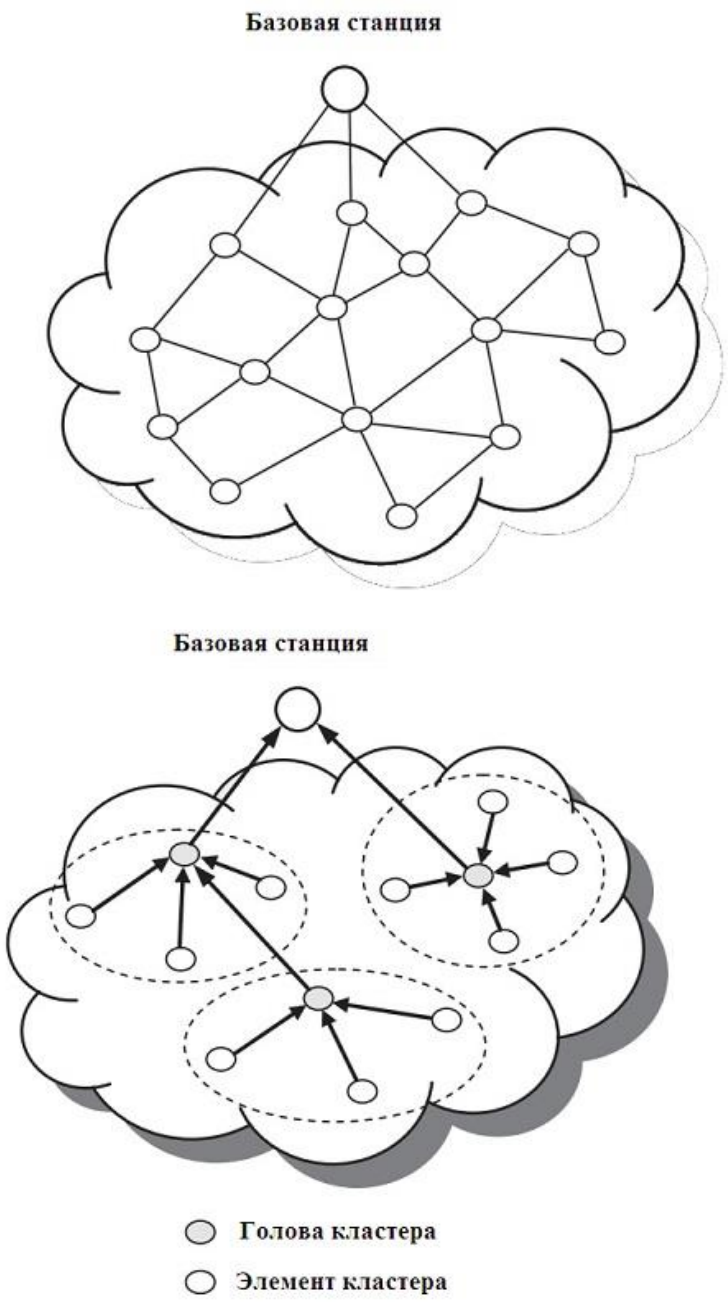


Рис. 21 – Процесс обмена

Топология сети – важная модель состояния сети, поскольку неявно она дает много информации об активных существующих узлах и связности сети. Так как **беспроводные сенсорные сети** обладают ограниченными энергетическими ресурсами, алгоритмы сбора информации о топологии должныпредполагать низкое энергопотребление.

В зависимости от требований предметной области формирование топологии сенсорной сети может происходить в двух режимах: топология типа "звезда" (иерархическая топология), либо топология типа "точка-точка" (однородная топология). В случае топологии типа "звезда" предполагается, что сеть состоит из объектов двух типов: полнофункциональные объекты и объекты с уменьшенной функциональностью (мы это рассматривали в главе **PAN**).

Объекты второго типа могут вести общение только с объектами первого типа. Ввиду повышенных нагрузок полнофункциональные устройства могут быть стационарными и иметь питание от внешних источников.

Такой способ организации сети может быть востребован для решения ограниченного спектра задач, например, в промышленности.

Второй вариант организации работы сети – "однородная" топология, когда не требуется разбиение сети сегменты (кластеры) и все объекты могут вести общение между собой в пределах области видимости, при этом вся сеть может разбиваться на сегменты, управляемые координаторами, а может и нет. Данный подход к формированию сети позволяет организовывать более сложные конфигурации сети, адаптировать такие сети к решению более сложных и нестандартных задач. Подобная гибкость достигается благодаря тому, что при таком подходе отдельные объекты могут самостоятельно организовываться сеть и адекватно реагировать на изменения в топологии сети со временем.

Кроме того, в рамках такой сети может быть реализована маршрутизация сообщений, когда объекты, не являющиеся непосредственными соседями, могут общаться между собой. Именно этот способ зачастую неявно подразумевается в большинстве печатных трудов, когда тематика работы непосредственно связана с понятием "сенсорная сеть".

Каждый координатор выбирает уникальный идентификатор подсети. Этот идентификатор обеспечивает связь между устройствами в сети с помощью коротких адресов и позволяет передавать данные между устройствами через независимые подсети. Все сети топологии «звезда» работают независимо от других сетей. После того, идентификатор выбран, координатор разрешает узлам подключаться к сети.

Количество статей, мнений, разработок, касающихся беспроводных сенсорных сетей уже достаточно велико, но всё это не дает представление о БСС как о единой структуре. Уже сегодня сенсорные сети нуждаются в первом шаге к направлению о представлении их как единой сложной системы.

Многообразие информации уже дает возможность собрать пазл эффективной, универсальной сенсорной сети, которая будет является отдельной, независимой технологией. Но простое (аддитивное) объединение отраслей (систем), которые содержит БСС не нерационально. С развитием вычислительной техники и средств связи наступила эра беспроводных сетей и распределенных вычислений. Пройдет еще несколько лет, и беспроводные технологии свяжут между собой огромные количество цифровых устройств, превратив Информационные Технологии во всепроницающую и вездесущую силу эпохи Информационного Общества. В свою очередь, беспроводные сенсорные сети, как элемент инфокоммуникационной структуры, позволяет расширить инфокоммуникационные возможности на периферию, давая возможность пользователю получить доступ к ранее недоступным услугам наблюдения состояния физических параметров контролируемого объекта или явления.

Изучение теоретических основ создания, развития, реализации БСС (беспроводных сенсорных сетей) на практике – залог карьерного успеха в будущем, когда все крупные компании, как полагают многие ученые, устремляться занять нишевые позиции на рынке информационных систем технологий. В следующей главе учебно-теоретического издания мы рассмотрим частный случай PAN/BAN сетей: Internet of things (IoT), содержащей в себе элементы концепции БСС (WSN) и, что немаловажно, уже активно внедряемый в нашу повседневную в жизнь уже сегодня.

I. Средства и технологии передачи данных: IEEE 802.15, Zigbee.

Семейство стандартов IEEE 802.15 образует беспроводную сеть WPAN (Wireless Personal Area Network) которая обеспечивает беспроводную связь между различного типа устройствами на небольших растояниях. Стандарты, которые входят с это семейство – это **Bluetooth** (IEEE 802.15.1), IEEE 802.15.3, **ZigBee** (IEEE 802.15.4) и UWB (Ultra Wideband) (IEEE 802.15.4a/b).

Беспроводная технология **Bluetooth**, основана на стандарте **IEEE 802.15.1**, является стандартом, определяющим функционирование компактных систем связи на небольших расстояниях между мобильными персональными компьютерами, мобильными телефонами и иными портативными устройствами. Bluetooth представляет собой недорогой радиоинтерфейс с низким энергопотреблением (мощность передатчика всего порядка 1 мВт) для организации персональных сетей, обеспечивающий передачу в режиме реального времени как цифровых данных, так и звуковых сигналов.

Изначально дальность действия радиоинтерфейса закладывалась равной 10 метрам, однако сейчас спецификациями Bluetooth уже определена и вторая зона около 100 м. Для работы радиоинтерфейса Bluetooth используется так называемый нижний (2,45 ГГц) диапазон ISM (industrial, scientific, medical), предназначенный для работы промышленных, научных и медицинских приборов. Радиоканал обладает полной пропускной способностью в 1 Мбит/с, что обеспечивает создание асимметричного канала передачи данных на скоростях 723,3/57,6 Кбит/с или полнодуплексного канала на скорости 433,9 Кбит/с. Если данные не передаются, то через Bluetooth-соединение можно передавать до 3-х дуплексных аудиоканалов по 64 Кбит/с в каждом направлении.

Возможна также и комбинированная передача данных и звука. В части организации обмена данными Bluetooth соответствует спецификации стандарта локальных сетей IEEE 802 и использует сигналы с расширением спектра путем скачкообразной перестройки частоты (FHSS) по псевдослучайному закону со скоростью 1600 переключений в секунду в полосе 2400-2483,5 МГц.

Bluetooth работает как многоточечный радиоканал, управляемый, аналогично сотовой связи GSM, многоуровневым протоколом с поддержкой обратной зависимостью. На данный момент актуальными версия этой технологии являются 4.0, 4.1, 4.2, 5.0 (рис.21).

	4.1	4.0	3.0	2.x	1.x
Базовая скорость	1 Мбит/с	1 Мбит/с	1 Мбит/с	1 Мбит/с	1 Мбит/с
Повышенная скорость передачи (EDR)	3 Мбит/с	3 Мбит/с	3 Мбит/с	3 Мбит/с	нет
High Speed	54 Мбит/с	54 Мбит/с	54 Мбит/с	нет	нет
Дальность (макс./мин. мощность)	100 м/ 10 м	100 м/ 10 м	100 м/ нет	100 м/ нет	100 м/ 10 нет
Режим низкого потребления	да	да	нет	нет	нет
Двойной профиль (одновременно Master и Slave)	да	нет	нет	нет	нет
Поддержка IPv6	готовится	нет	нет	нет	нет
Сопряжение NFC	да	да	да	да	нет
128-битное шифрование AES	да	да	нет	нет	нет

Рис. 21 - Сравнительная таблица версий (поколений) Bluetooth.

Первый чип с поддержкой Bluetooth 3.0 был выпущен компанией Sony в конце 2009 года. В настоящее время выпускается большое количество мобильных устройств с поддержкой этого стандарта.

Bluetooth 4.1

В конце 2013 года Bluetooth Special Interest Group (SIG) представила спецификацию Bluetooth 4.1. Одно из улучшений, реализованных в спецификации Bluetooth 4.1, касается совместной работы Bluetooth и мобильной связи четвёртого поколения LTE Стандарт предусматривает защиту от взаимных помех путём автоматического координирования передачи пакетов данных.

Bluetooth 4.2

3 декабря 2014 Bluetooth Special Interest Group (SIG) представила спецификацию Bluetooth 4.2. Основные улучшения — повышение конфиденциальности и увеличение скорости передачи данных.

Bluetooth 5.0

16-17 июня 2016 года Bluetooth Special Interest Group (SIG) представила спецификацию Bluetooth 5.0.Изменения коснулись в основном режима с низким потреблением и высокоскоростного режима. Радиус действия увеличен в 4 раза, скорость увеличена в 2 раза.

Посредством Bluetooth можно объединить как два, так и сразу несколько устройств. В первом случае подключение осуществляется по схеме «точкаточка», во втором — по схеме «точка-многоточка». Независимо от применяемой схемы одно из устройств является ведущим (master), остальные — ведомыми (slave). Ведущее устройство задает шаблон, который будут использовать все ведомые устройства, а также синхронизирует их работу. Соединенные таким образом устройства образуют пикосеть (piconet). В рамках одной пикосети могут быть объединены одно ведущее и до семи ведомых устройств. Кроме того, допускается наличие в пикосети дополнительных ведомых устройств (сверх семи), которые имеют статус заблокированных (parked): они не участвуют в обмене данными, но при этом находятся в синхронизации с ведущим устройством.

Несколько пикосетей можно объединить в распределенную сеть (scatternet). Для этого устройство, работающее в качестве ведомого в одной пикосети, должно выполнять функции ведущего в другой (см. вторую схему). При этом пикосети, входящие в состав одной распределенной сети, не синхронизированы друг с другом и используют разные шаблоны.

Относительная универсальность является как преимуществом, так и недостатком Bluetooth. Во-первых, не все адаптеры поддерживают все профили (именно по этой причине универсальность Bluetooth является относительной). Во-вторых, в некоторых ситуациях эта самая универсальность может оказаться излишней (например, могут возникнуть трудности при нахождении устройства в сети с большим числом подключений).

Одним из главных недостатков сетей Bluetooth является обеспечиваемый уровень безопасности. Слабости защиты bluetooth, в частности, вызваны тем, что эта технология делает сильный упор на опознание устройств для безопасного обслуживания, а также на контроль, которым обладает пользователь над устройствами bluetooth и их конфигурацией. Современная bluetooth-технология не предлагает никакого средства опознания пользователя, что делает bluetooth-устройства особенно уязвимыми к так называемым spoofing-нападениям (радиодезинформации) и неправильному применению опознавательных устройств. Особенно слабым аспектом bluetooth является процесс «спаривания» (pairing) устройств, при котором происходит обмен ключами в незакодированных каналах. Если нападающий перехватит передачу процесса спаривания, то он сможет получить ключ инициализации путем калькуляции этих ключей для любого возможного варианта пароля и сравнения результатов с перехваченной передачей. Ключ инициализации используется для расчета ключа связи. Рассчитанный хакером ключ связи сравнивается с перехваченной передачей с целью узнать, верен он или нет.

Также причиной уязвимости является возможность использования коротких, а также заурядных/распространенных паролей (ситуация аналогична использованию простых паролей системными администраторами компьютерных сетей). Такие пароли значительно упрощают инициализацию. Именно это делает ключи связи очень простыми для извлечения из перехваченных передач.

Во многих приложениях требуются беспроводные сети связи (БСС), не обладающие высокой скоростью передачи, но **надежные**, живучие (способные к самовосстановлению), простые в развертывании и эксплуатации. Сети типа Bluetooth все же не, являются **надежными из-за вышеперечисленных причин**. Важно также, чтобы оборудование таких сетей допускало длительную работу от автономных источников питания, имело низкую стоимость, и было компактным. Пример такого приложения – «умный дом».

Такому сочетанию требований еще 10 лет назад не отвечал ни один из сетевых стандартов, что и привело к созданию стандартов IEEE 802.15.4 и **ZigBee**, описывающих устойчивые масштабируемые многошаговые беспроводные сети, простые в развертывании и поддерживающие самые разные приложения.

Стандарт IEEE 802.15.4 (ZigBee) ориентирован, главным образом, на использование в качестве средства связи между автономными приборами и оборудованием. В корпоративном секторе это могут быть, например, складские системы, системы автоматизации производства, различные датчики, сенсоры, сервоприводы, электронные метки, а в домашних условиях – персональные компьютеры, игровые приставки, системы безопасности, освещения, кондиционирования, радиофицированные игрушки.

Стандарт IEEE 802.15.4 определяет спецификации **физического слоя** (**PHY**) и **протокол управления доступом** (MAC), предлагая поддержку различных топологий сетей. Схемы сетевой маршрутизации призваны обеспечить сохранение энергии и кратчайшие задержки, укладывающееся в гарантированный временной интервал, а за счет наличия нескольких маршрутов к каждому узлу в сетях ZigBee предполагается предотвратить возможность "сбоя в одной точке".

Ключевые функции PHY включают в себя контроль за энергией и качеством звеньев, а также оценку каналов для более успешного сосуществования с сетями других беспроводных операторов.

MAC определяет автоматическое подтверждение получения пакетов, обеспечивает возможность передачи данных в определенные временные интервалы и поддерживает 128-битные функции-безопасности AES. Если в пределах досягаемости ZigBee-устройств окажется оборудование Wi-Fi или Bluetooth, их каналы могут быть использованы как туннель для трафика ZigBee.

Стандарт IEEE 802.15.4 предусматривает **радиус покрытия** от 10 до 75 м и пропускную способность канала - до 250 кбит/с. Передача на этой скорости ведется в диапазоне 2,4 ГГц. Небольшая мощность и скорость обусловлены малыми энергоресурсами связываемых устройств. Доступны также диапазоны 858 МГц (20 кбит/с) и 902-928 МГц(40 кбит/с). То есть 3 частотных диапазона.

Возможности: до 255 подчиненных устройств в сети и до 100 параллельно работающих сетей. Данный стандарт, активно продвигаемый организацией Альянсом ZigBee, заполнит вакуум в спектре беспроводных сетевых технологий, поскольку он предлагает разработчикам возможность создавать недорогие продукты с очень низким потреблением мощности и чрезвычайно гибкими функциями поддержки беспроводных сетей (рис.22).

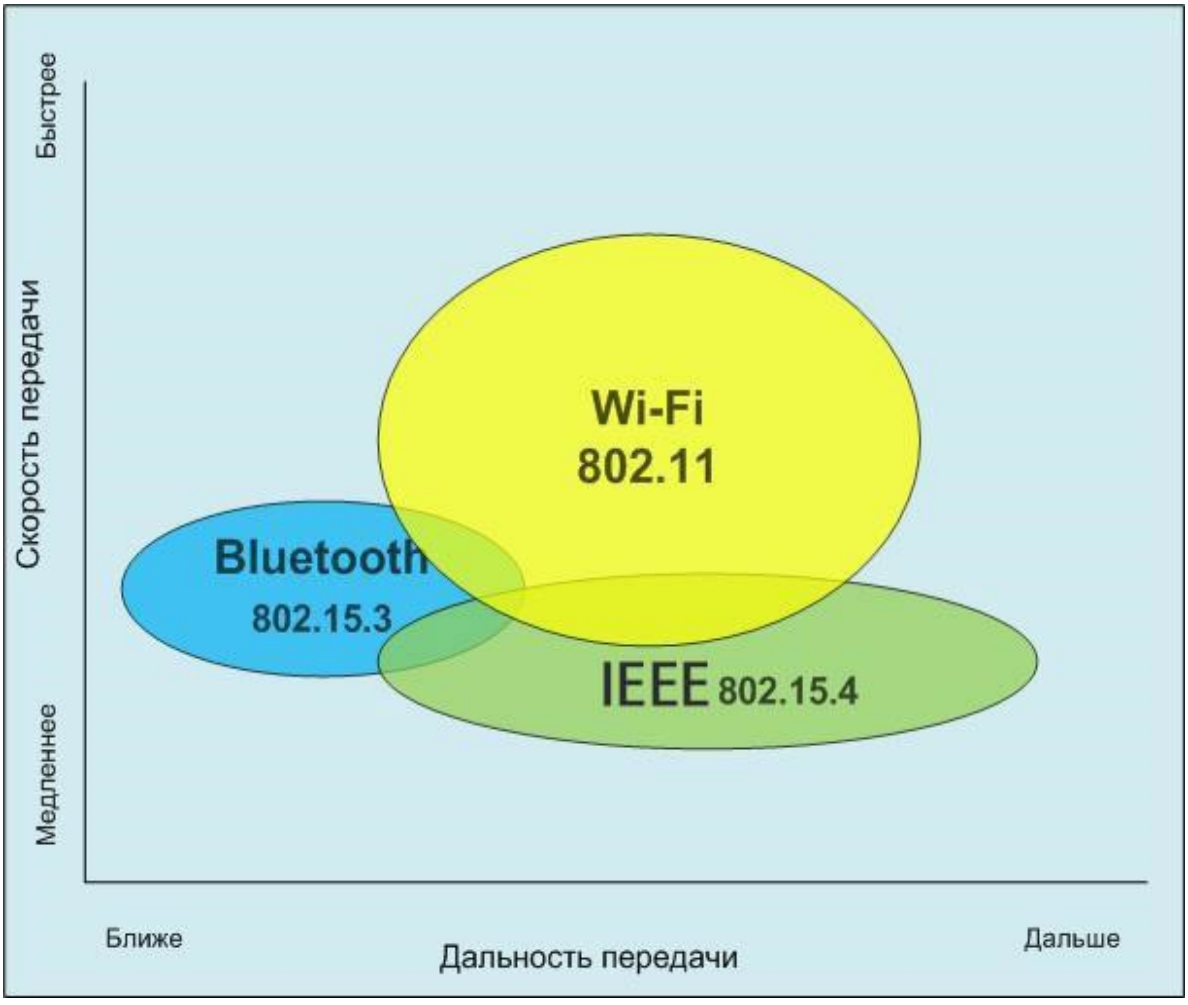


Рис. 22 - Сравнительная характеристика IEEE 802.15, 802.11, 802.15.3

Главные отличия и преимущества ZigBee от других беспроводных технологий: **ZigBee** работает по **ячеистому типу**, в то время как Wifi и Bluetooth присоединяются к центральному роутеру (топология «звезда») (рис.23). При отсутствии связи с роутером узел не может подключиться к другим членами сети. Например, если телевизор выходит в интернет через модем, то он не сможет воспроизвести фильм или получить его с планшета, если роутер не подключен к сети. В ячеистой структуре узлы связаны напрямую. Благодаря этому обрыв связи не является помехой для передачи данных. Этот механизм намного надежнее и применяется в самой сети интернет. Для реализации технологии «Умный дом» этот фактор очень важен. При аварии сигнал по Wifi может не передаться на большую дальность через бетонные стены.

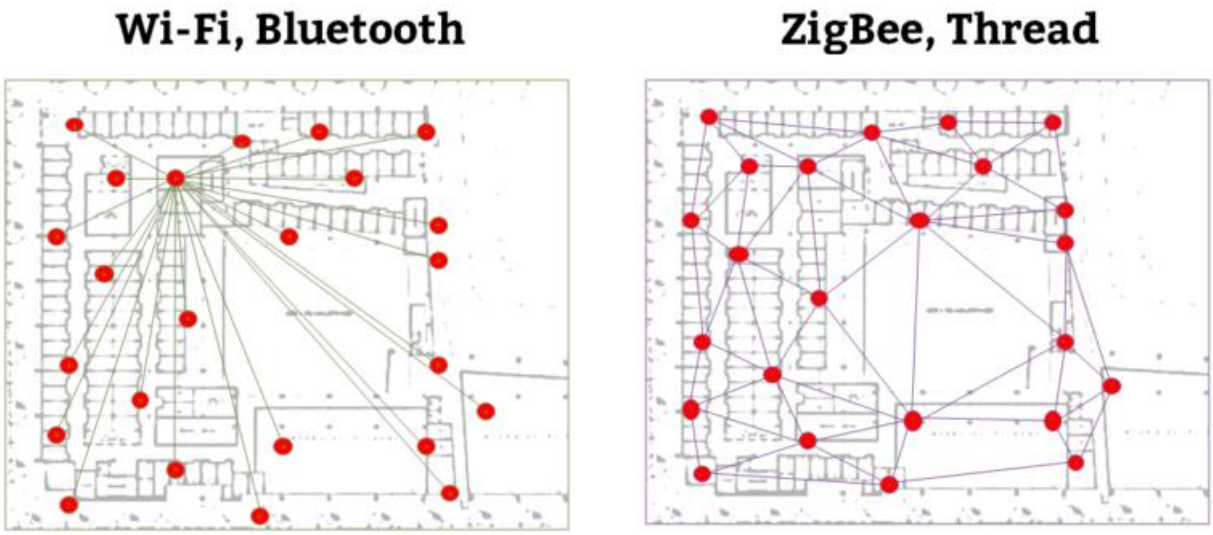


Рис. 23 – Ячеистый тип технологии передачи данных

ZigBee устройства потребляют минимальный объем энергии, поскольку функционируют в спящем режиме. Пропускная возможность Зигби (250 Кбит/секунду) намного ниже, чем у Wifi (300–1000 Мбит/секунду). Это связано с тем, что Зигби доставляет маленькие пакеты данных, а Wifi позволяет получить крупные файлы (видео и т.д.).

Скорость: Период задержки передачи сигнала Зигби **намного меньше**, чем у Bluetooth (несколько секунд) и составляет 30 миллисекунд. Показатель Зигби примерно равен времени от нажатия выключателя и возникновения света в люстре. В связи с этим, в последнее время Bluetooth стал меньше использоваться при установке системы «Умный дом».

Количество узлов: у Zigbee намного больше. Теоретически, к сети Wifi может присоединиться от 300 до 1000 участников. Но пользователи отмечают, что при работе уже с несколькими устройствами происходят задержки в работе и вряд-ли удастся проверить показатель. ZigBee система функционирует при любом количестве участников, что необходимо при установке «умного дома» на больших площадях.

Цена. Стоимость модуля ZigBee на порядок дешевле, чем цена Wifi модема.

На современный рынок, выпускается много ZigBee устройств: к ним относится розетка, диммер, лампочка, датчики движения, сенсоры контроля воды, температуры, и другие. На данный момент (январь 2020 года) по большому количеству причин среди производителей устройств на протоколе ZigBee лидирует китайская компания Xiaomi.

II. Средства идентификации, измерения, передачи данных LPWAN

Мы познакомились с стандартами беспроводной передачи информации, работающих на относительно небольших дистанциях (Bluetooth до 20 метров при условии прямой видимости, Wi-Fi и ZigBee на расстояния, не превышающие нескольких сотен метров при благоприятных условиях, с потерей эффективности передачи для конечных устройств). В завершении экскурса необходимо дать представление о новых беспроводных сетях – LPWAN.

LPWAN (англ. Low-power Wide-area Network — «энергоэффективная сеть дальнего радиуса действия») — беспроводная технология передачи небольших по объёму данных на дальние расстояния, разработанная для распределённых сетей телеметрии, межмашинного взаимодействия и интернета вещей. LPWAN является одной из беспроводных технологий, обеспечивающих среду сбора данных с различного оборудования: датчиков, счётчиков и сенсоров.

В основе принципа передачи данных по технологии LPWAN на физическом уровне PHY лежит свойство радиосистем — увеличение энергетики, а значит и дальности связи при уменьшении скорости передачи. Чем ниже битовая скорость передачи, тем больше энергии вкладывается в каждый бит и тем легче выделить его на фоне шумов в приёмной части системы. Таким образом, низкая скорость передачи данных позволяет добиться большей дальности их приёма.

Подход, используемый для построения LPWAN-сети, схож с принципом работы сетей мобильной связи. LPWAN-сеть использует топологию «звезда», где каждое устройство взаимодействует с базовой станцией напрямую. Сети городского или регионального масштаба строятся с использованием конфигурации «звезда из звезд».

Устройство или модем с LPWAN-модулем передает данные по радиоканалу на базовую станцию. Станция принимает сигналы от всех устройств в радиусе своего действия, оцифровывает и передаёт на удалённый сервер, используя доступный канал связи: Ethernet, сотовая связь, VSAT (спутниковая связь).

Полученные на сервере данные используются для отображения, анализа, построения отчетов и принятия решений.

Управление устройствами, обновление программного обеспечения происходит с использованием обратного канала связи.

Для передачи данных по радиоканалу, как правило, применяется нелицензируемый спектр частот, разрешенных к свободному использованию в регионе построения сети: 5,0 ГГц, 2,4 ГГц, 868/915 МГц, 433 МГц, 169 МГц.

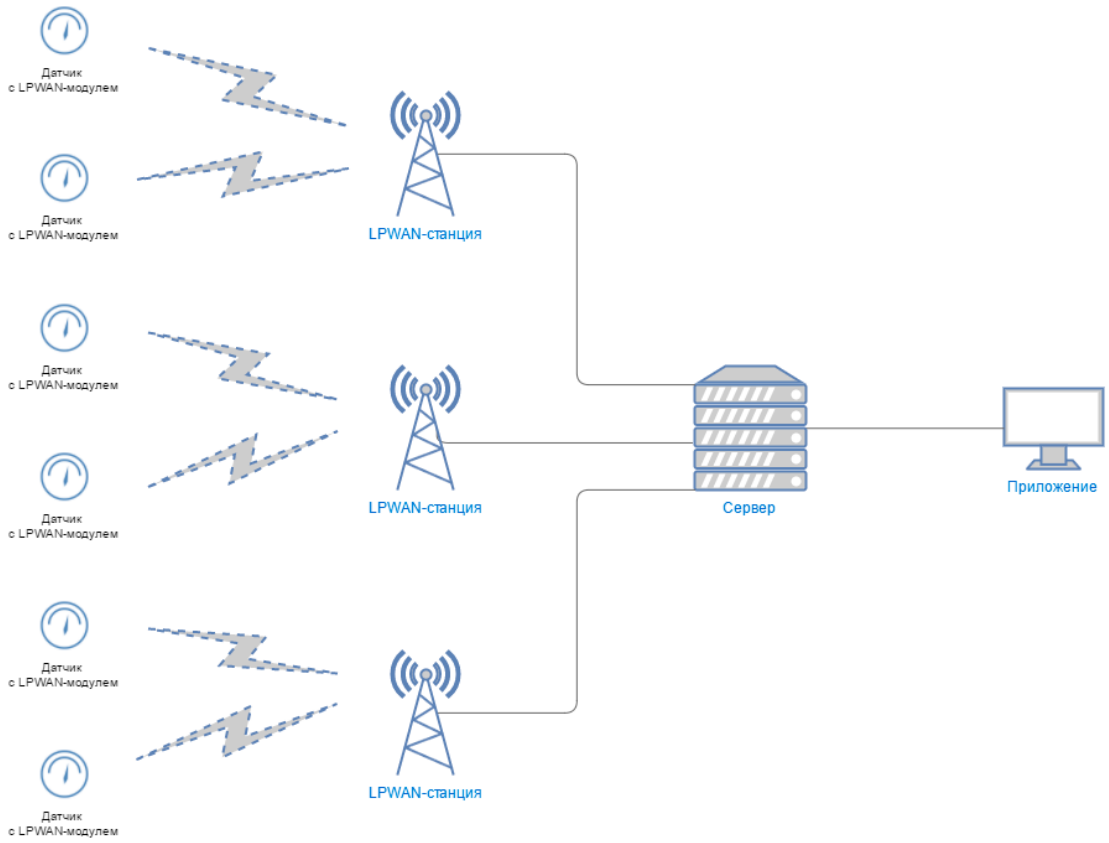


Рис. 24 – Топология LPWAN-сетей

Преимущества LPWAN

Большая дальность передачи радиосигнала по сравнению с другими беспроводными технологиями используемыми для телеметрии GPRS или ZigBee, достигает 10—15 км.

Низкое энергопотребление у конечных устройств, благодаря минимальным затратам энергии на передачу небольшого пакета данных.

Высокая проникающая способность радиосигнала в городской застройке при использовании частот суб-гигагерцового диапазона. Высокая масштабируемость сети на больших территориях. Отсутствие необходимости получения частотного разрешения и платы за радиочастотный спектр, вследствие использования нелицензируемых частот (ISM band).

Недостатки LPWAN

Относительно низкая пропускная способность, вследствие использования низкой частоты радио канала. Варьируется в зависимости от используемой технологии передачи данных на физическом уровне, составляет от нескольких сотен бит/с до нескольких десятков кбит/с.

Задержка передачи данных от датчика до конечного приложения, связанная с временем передачи радиосигнала, может достигать от нескольких секунд до нескольких десятков секунд.

Отсутствие единого стандарта, который определяет физический слой и управление доступом к среде для беспроводных LPWAN-сетей.

Технология LPWAN также, как и описанные ранее технологии, ориентирована на приложения, требующие гарантированной передачи небольшого объёма данных, возможности длительной работы сетевых устройств от автономных источников питания, большого территориального охвата беспроводной сетью. Основными областями применения технологии LPWAN являются беспроводные сенсорные сети, автоматизация сбора показаний приборов учета, системы промышленного мониторинга и управления.

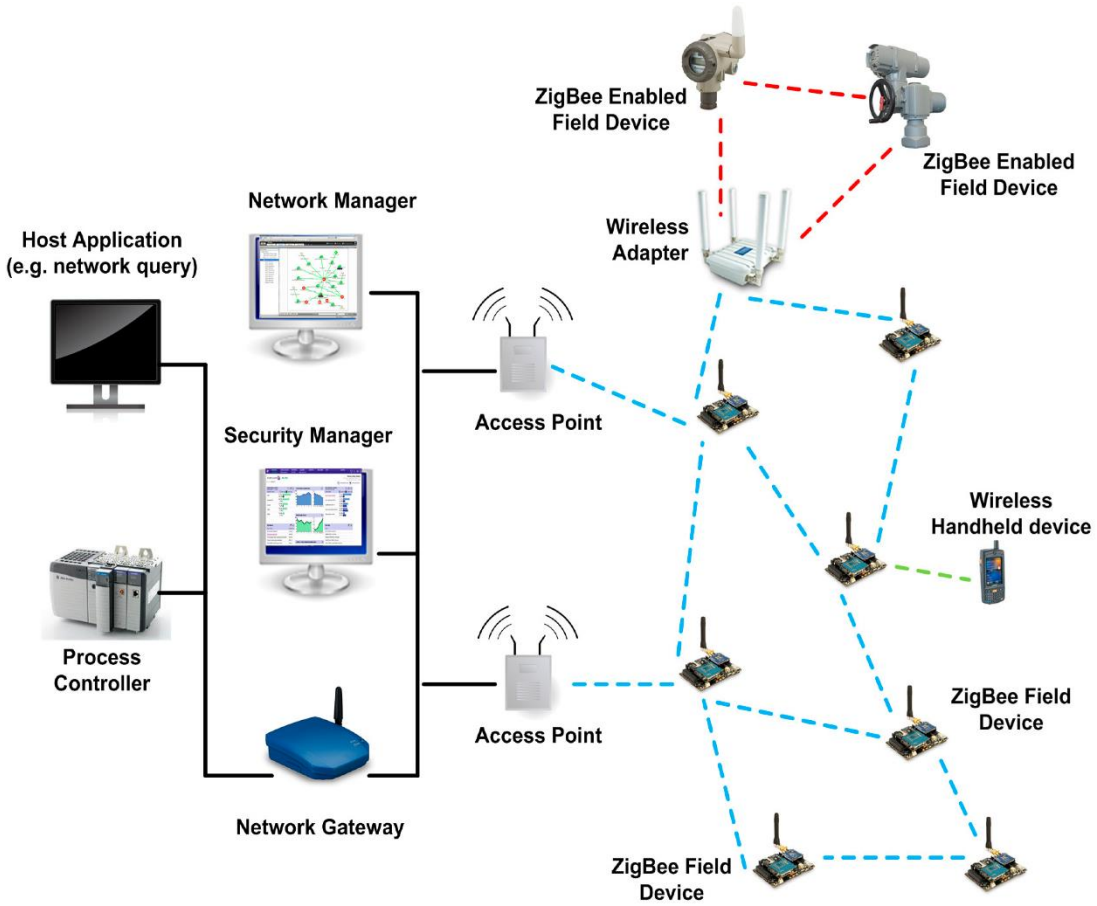


Рис. 24 – LPWAN на базе инкапсуляции в себе сети ZigBee

Типовые средства идентификации, передачи (равно как измерения данных) в LPWAN лучше всего описывают LoRa-модули (Родственная к LPWAN технология)

Каждый комплект может служить строительным блоком для развития сети, где разработчики могут рассчитывать на расстояние до 10 км и 10 лет автономной работы от двух батарей AAA. Технология LoRa использует модуль с расширенным спектром, который обеспечивает отличную устойчивость данных в шумовой среде и работает через физические препятствия.

Рис. 25 – Базовый комплект LoRa модулей

На рисунке 25 представлена базовая конфигурация для LPWAN сети: не хватает лишь оконечных устройств (сенсоров, датчиков и т.д). Здесь два модема (полнофункциональные устройства) и одно управляющее устройство, выполняющее роль координатора, в некоторой степени и программатора и средства ввода/вывода информации (ЖК-модуль, тактовые кнопки, интерфейсы). Вот так выглядят сети будущего. Никакой избыточности. Аскетизм предельной степени.

III. Окружающий интеллект: платформа, технология, применение.

Окружающий интеллект (англ. Ambient intelligence, AmI) — термин для обозначения окружающей среды, насыщенной электронными устройствами, которые реагируют на присутствие людей. В русскоязычных источниках термин «окружающий интеллект» упоминается, но пока не является устоявшимся эквивалентом английского Ambient intelligence. В англоязычных источниках парадигма окружающего интеллекта основывается на технологиях распределённых вычислений, построении персональных профилей контекстной ориентированности, клиенто-ориентированного дизайна человеко-компьютерного взаимодействия и характеризуется наличием следующих особенностей:

встроенность: многие сетевые устройства интегрированы в окружающую среду;

контекстная ориентированность: эти устройства могут распознавать пользователя и связанный с ним ситуационный контекст;

кастомизация: они могут быть приспособлены к потребностям конкретного пользователя;

адаптивность: они могут изменяться в ответ на реакцию пользователя;

упреждение: они могут предвидеть желания пользователя без каких-либо особых действий со стороны последнего.

По оценкам Консультативной группы Еврокомиссии по вопросам информационного общества и технологий (ISTAG), окружающий интеллект получает общественное признание благодаря созданию им следующих возможностей:

- облегчение контактов между людьми;
- ориентация на сотрудничество и культурное развитие;
- распространение знаний и навыков, повышение качества работы и выбора потребителей;
- формирование доверия и уверенности в себе;
- содействие устойчивому развитию личности, общества и окружающей среды в долгосрочной перспективе;
- простота и лёгкость контроля со стороны рядовых пользователей.

Ярким представлением окружающего интеллекта является платформа **Интернета вещей.**

Internet of Things, IoT — концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.

Концепция сформулирована в 1999 году как осмысление перспектив широкого применения средств радиочастотной идентификации для взаимодействия физических предметов между собой и с внешним окружением. Наполнение концепции многообразным технологическим содержанием и внедрение практических решений для её реализации начиная с 2010-х годов считается устойчивой тенденцией в информационных технологиях, прежде всего, благодаря повсеместному распространению беспроводных сетей, появлению облачных вычислений, развитию технологий межмашинного взаимодействия, началу активного перехода на IPv6 и освоению программно-определяемых сетей. Современное решение из класса "Интернета вещей" содержит, в том или ином виде, порознь или комбинированно, следующие компоненты:

Исполнительные элементы (иногда называемые "актуаторами"). С вышестоящими контроллерами они связываются, как правило, по некоторому узкоспециализированному протоколу. Это могут быть унаследованные проводные протоколы (RS–232/485, 1–Wire, USB, CAN), беспроводные протоколы малой дальности (Bluetooth, ZigBee и т.п.) или современные протоколы сетей LP-WAN (Low-power Wide-area Network) с низким энергопотреблением и большой дальностью. Именно технологии LPWAN стали одной из важнейших компонент, определяющих облик современного IoT.

Использование IP на этом уровне также не исключается (поверх Ethernet, сотовых сетей или Wi-Fi), но датчики на базе специализированных локальных протоколов, как правило, получаются проще, функциональнее и дешевле, чем полноценные IP-хосты — а цена имеет в данном случае первостепенное значение. С другой стороны, по мере расширения выпуска готовых встраиваемых компьютеров в формате System-on-Chip (SoC) и System-on-Module (SoM) и снижения их стоимости доля "чистых" IP-решений может увеличиться. (В частности, NSG предлагает в данном классе вычислительное ядро NSG UltraLite для построения разнообразных систем автоматизации, в т.ч. IoT.)

Контроллеры исполнительных механизмов. В общем случае, они терминируют соединения с датчиками на физическом уровне, а протокол канального уровня либо также терминируют и преобразовывают данные в какой-либо из стандартных протоколов IP-стека (как правило, UDP, но теоретически не исключён и, например, TCP).

Сервер IoT непосредственно работает с датчиками: регистрирует их в системе, аутентифицирует (при необходимости), опрашивает, принимает показания, отсылает команды исполнительным элементам. Дальнейший обмен с прикладным сервером также идёт по сети IP. При этом могут использоваться разнообразные прикладные протоколы поверх TCP или UDP — например, SNMP или Zabbix. Современная тенденция состоит в использовании для этой цели механизма **MQTT (Message Queue Telemetry Transport**), как наиболее подходящего для поставленной задачи. Именно он строит общую крышу, под которую ныне становится возможным подвести самые разнородные решения и их компоненты. Это вторая ключевая компонента, отличающая IoT от разрозненных систем предыдущих поколений.

Прикладной сервер работает уже не с датчиками, а исключительно с данными, полученными от них: накапливает, хранит, обсчитывает какую-то статистику и аналитику, генерирует отчёты в разных формах… Наконец, сервер замыкает контур управления между датчиками и исполнительными элементами, если на нём задан какой-либо детерминированный алгоритм, по принципу "щёлкни кобылу по носу — она махнёт хвостом". Если же такой алгоритм не задан, то контур управления остаётся открытым и замыкается уже на пользовательском устройстве или вручную самим пользователем: получил данные — подумал головой — отправил команду.

Клиентские устройства и приложения позволяют пользователю видеть информацию от сервера и отдавать команды серверу (а через него — исполнительным элементам). Как частный случай, алгоритм для автоматического управления может быть задан на клиентах, а не на сервере.
Клиенты IoT могут быть наиболее разнообразными: стационарные компьютеры, мобильные устройства, специализированные пульты, со стандартными или специализированными приложениями. С прикладным сервером они могут взаимодействовать посредством HTTP, MQTT, электронной почты, сервисов мгновенного обмена сообщениями, консольных команд и многого другого, что можно придумать для этой цели сейчас или в будущем. Плюс средства, выходящие за рамки стека IP: SMS, USSD, голосовой телефонный интерфейс.

Ещё раз подчеркнём, что описанная выше архитектура IoT — пока ещё очень предварительная и не устоявшаяся. И вероятней всего она будет гибкой, атипичной к уже классическим системам. В частности, любые два или несколько смежных элементов могут быть объединены в одном устройстве. Или же, наоборот, они могут быть рассредоточены в территориально-распределённую инфраструктуру с несколькими серверами IoT, многими контроллерами IoT при каждом сервере, и множеством датчиков на каждом контроллере.

Например, как уже сказано выше, датчик IoT может объединяться с контроллером в "интеллектуальный датчик" с встроенной поддержкой IP-стека; контроллер в этом случае если и сохраняется, то вырождается в обычный коммутатор Ethernet или маршрутизатор IP, безо всякой специфики IoT. Контроллер может объёдиняться с сервером IoT, а сервер — с прикладным сервером. С другой стороны, функции прикладного сервера могут быть частично или полностью переданы клиентам. Серверы MQTT могут располагаться и на сервере IoT, и на прикладном сервере, и на отдельном хосте. И так далее. Именно такая гибкость позволяет, с одной стороны, модифицировать архитектуру в соответствии с практическими требованиями, а с другой стороны — рассматривать её как универсальный шаблон, пригодный для самых разных задач.

Как крайний случай, интеллектуальный датчик может содержать в себе все вышестоящие звенья, вплоть до прикладного сервера (**рис.26**); вне его остаётся только клиентское устройство. Противоположный вариант — все промежуточные сервисы располагаются где-то в облаке поставщика услуг, а у клиента остаются только датчики (например, с протоколом NB-IoT) на площадке и мобильное устройство в руках.

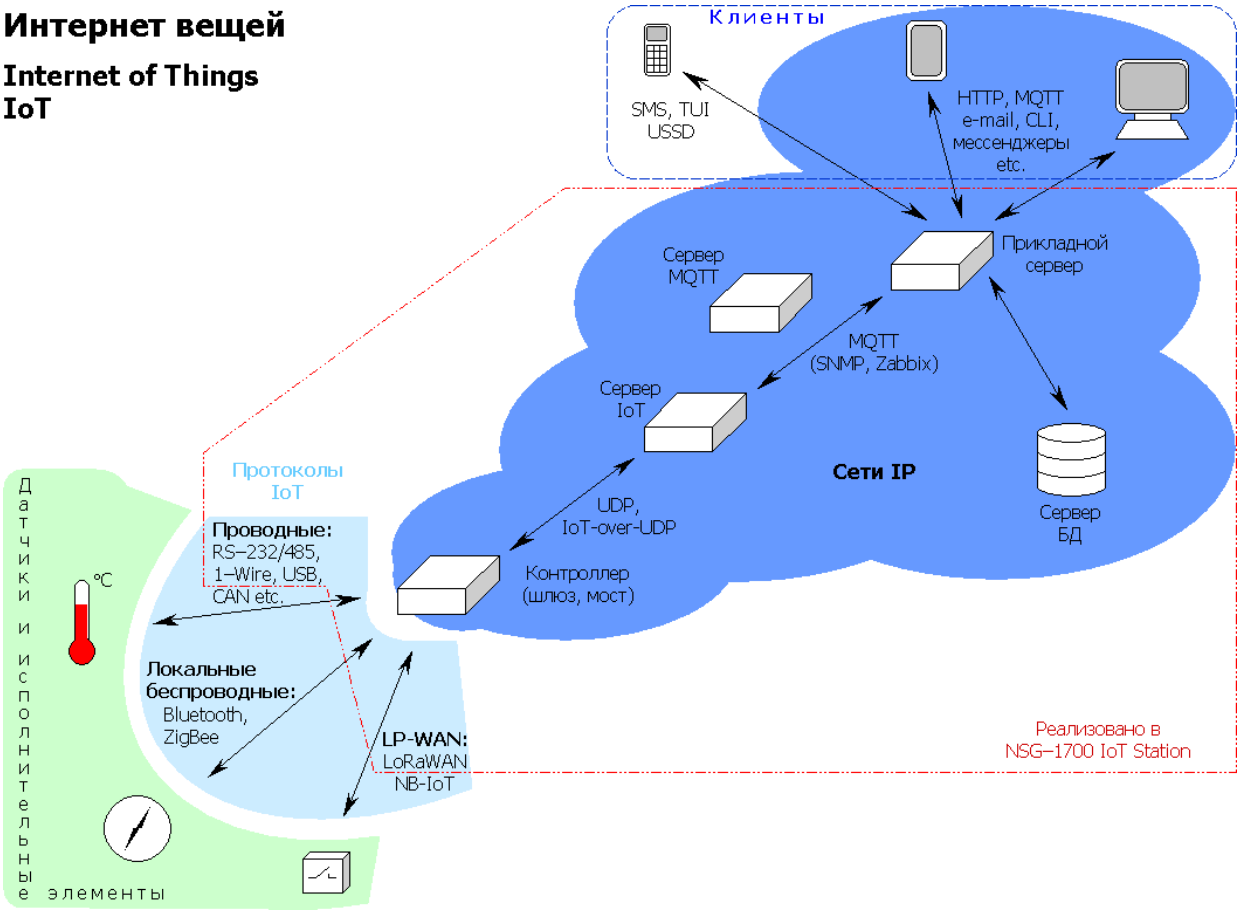


Рисунок 26 – IoT-платформа

Таким образом, результируя, концепция IoT позволяет выделить три **набора технологий**, описывающих средства измерения, передачи данных и идентификации – три столба данной системы. Опишем их:

Средства идентификации

Задействование в «интернете вещей» предметов физического мира, не обязательно оснащённых средствами подключения к сетям передачи данных, требует применения технологий идентификации этих предметов («вещей»). Хотя толчком для появления концепции стала технология RFID, но в качестве таких технологий могут использоваться все средства, применяемые для автоматической идентификации: оптически распознаваемые идентификаторы (штрихкоды, Data Matrix, QR-коды), средства определения местонахождения в режиме реального времени. При всеобъемлющем распространении «интернета вещей» принципиально обеспечить уникальность идентификаторов объектов, что, в свою очередь, требует стандартизации.

Для объектов, непосредственно подключённых к интернет-сетям, традиционный идентификатор — MAC-адрес сетевого адаптера, позволяющий идентифицировать устройство на канальном уровне, при этом диапазон доступных адресов практически неисчерпаем (248 адресов в пространстве MAC-48), а использование идентификатора канального уровня не слишком удобно для приложений. Более широкие возможности по идентификации для таких устройств даёт протокол IPv6, обеспечивающий уникальными адресами сетевого уровня не менее 300 млн устройств на одного жителя Земли.

Рис. 27 – Принципы обеспечения безопасности в IoT

Средства измерения

Особую роль в интернете вещей играют средства измерения, обеспечивающие преобразование сведений о внешней среде в машиночитаемые данные, и тем самым наполняющие вычислительную среду значимой информацией. Используется широкий класс средств измерения, от элементарных датчиков (например, температуры, давления, освещённости), приборов учёта потребления (таких, как интеллектуальные счётчики) до сложных интегрированных измерительных систем. В рамках концепции «интернета вещей» принципиально объединение средств измерения в сети (такие, как беспроводные датчиковые сети, измерительные комплексы), за счёт чего возможно построение систем межмашинного взаимодействия.

Как особая практическая проблема внедрения «интернета вещей» отмечается необходимость обеспечения максимальной автономности средств измерения, прежде всего, проблема энергоснабжения датчиков. Нахождение эффективных решений, обеспечивающих автономное питание сенсоров (использование фотоэлементов, преобразование энергии вибрации, воздушных потоков, использование беспроводной передачи электричества), позволяет масштабировать сенсорные сети без повышения затрат на обслуживание (в виде смены батареек или подзарядки аккумуляторов датчиков).

Средства передачи данных

Спектр возможных технологий передачи данных охватывает все возможные средства беспроводных и проводных сетей.

Для беспроводной передачи данных особо важную роль в построении «интернета вещей» играют такие качества, как эффективность в условиях низких скоростей, отказоустойчивость, адаптивность, возможность самоорганизации. Основной интерес в этом качестве представляет стандарт IEEE 802.15.4, определяющий физический слой и управление доступом для организации энергоэффективных персональных сетей, и являющийся основой для таких протоколов, как ZigBee, WirelessHart, MiWi, 6LoWPAN, LPWAN.

Среди проводных технологий важную роль в проникновении «интернета вещей» играют решения **PLC** — технологии построения сетей передачи данных по линиям электропередачи, так как во многих приложениях присутствует доступ к электросетям (например, торговые автоматы, банкоматы, интеллектуальные счётчики, контроллеры освещения изначально подключены к сети электроснабжения). 6LoWPAN, реализующий слой IPv6 как над IEEE 802.15.4, так и над PLC, будучи открытым протоколом, стандартизуемым IETF, отмечается как особо важный для развития «интернета вещей

IV. Актуаторы, айтрекеры – элементы сетей завтрашнего дня.

Данная глава предназначена для приобретения на вооружение двух лексических единиц, активно встречающихся в литературе, на практике, на производстве. Эти термины в русскоязычном сегменте в самое ближайшее время станут такими же привычными, как и понятия коммутации, маршрутизации. Более того, вы скорей всего знаете эти термины. **Актуаторы** уже упоминались чуть ранее в этом пособии, а айтрекеры уже давно на слуху в интернет-издания. Безусловно, я бы мог поместить «расшифровку» и этимологию этих понятий в самый конец книги, но… Это будет не совсем правильно. А вот на вопрос: почему так? Вы сможете получить ответ сейчас.

Перейдем к развернутому определению термина «актуатор» и «айтрекер», используя и смежные понятия:

Актуатор (исполнительный элемент, **актуатор**) — функциональный элемент системы автоматического управления, который воздействует на объект, изменяя поток энергии или материалов, которые поступают на объект. Большинство исполнительных устройств имеет механический или электрический выход.

Состоит из двух функциональных блоков: исполнительного устройства (если исполнительное устройство механическое, то его часто называют исполнительный механизм) и регулирующего органа, например, регулирующего клапана, и может оснащаться дополнительными блоками.

В теории автоматического управления под исполнительным устройством понимают устройство, передающее воздействие с управляющего устройства на объект управления. Иногда рассматривается как составная часть объекта управления. Управляющим устройством может быть любая динамическая система. Входные и выходные сигналы исполнительных устройств, а также их методы воздействия на объект управления могут иметь различную физическую природу.

Виртуальные приборы (англ. Virtual Instrumentation) — концепция, в соответствии с которой организуются программно-управляемые системы сбора данных и управления техническими объектами и технологическими процессами, при которой система организуется в виде программной модели некоторого реально существующего или гипотетического прибора.

Причём программно реализуются не только средства управления (рукоятки, кнопки, лампочки и т. п.), но и логика работы прибора.

Связь программы с техническими объектами осуществляется через интерфейсные узлы, представляющие собой драйверы внешних устройств — АЦП, ЦАП, контроллеров промышленных интерфейсов и т. п. Предшественницей концепции виртуальных приборов служила концепция слепых приборов, предусматривающая организацию системы в виде физического устройства («ящика», реализующего логику работы прибора, но не имеющего пользовательского интерфейса), и программно-реализуемых средств управления (представляющих собой HMI в чистом виде). Виртуальные приборы (англ. Virtual Instrumentation) — концепция, в соответствии с которой организуются программно-управляемые системы сбора данных и управления техническими объектами и технологическими процессами, при которой система организуется в виде программной модели некоторого реально существующего или гипотетического прибора, причём программно реализуются не только средства управления (рукоятки, кнопки, лампочки и т. п.), но и логика работы прибора. Связь программы с техническими объектами осуществляется через интерфейсные узлы, представляющие собой драйверы внешних устройств — АЦП, ЦАП, контроллеров промышленных интерфейсов и т. п.

Предшественницей концепции виртуальных приборов служила концепция слепых приборов, предусматривающая организацию системы в виде физического устройства («ящика», реализующего логику работы прибора, но не имеющего пользовательского интерфейса), и программно-реализуемых средств управления (представляющих собой HMI в чистом виде).

Концепция виртуальных приборов применяется в качестве базовой в таких продуктах, как:

1. LabVIEW фирмы National Instruments (США) (http://www.natinst.com),
2. реализуется на программной архитектуре VISA;
3. DASYLab фирмы DATALOG GmbH (Германия) (http://www.dasylab.com);
4. DIAdem фирмы GfS mbH (Германия);
5. ZETLab фирмы "ЭТМС" (Россия);

В вычислительной технике актуаторы представляют собой преобразователи, превращающие входной сигнал (электрический, оптический, механический, пневматический и др.) в выходной сигнал (обычно в движение, но не всегда), воздействующий на объект управления.

Устройства такого типа включают: электрические двигатели, электрические, пневматические или гидравлические приводы, релейные устройства, электростатические двигатели (англ. Comb drive), DMD-зеркала и электроактивные полимеры, хватающие механизмы роботов, приводы их движущихся частей, включая соленоидные приводы и приводы типа «звуковая катушка» (англ. Voice coil), а также многие другие.

Виртуальные (программные) приборы используют исполнительные устройства и датчики для взаимодействия с объектами реального мира. С помощью датчиков сигнал передаётся в виртуальный прибор, обрабатывается и выдаётся в реальный мир с помощью различного вида исполнительных устройств (рис.28).

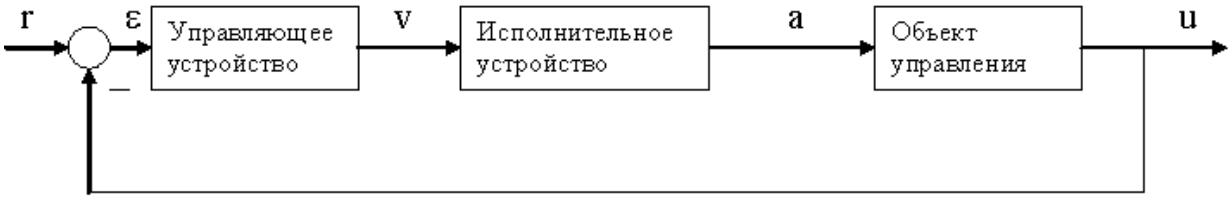


Рис. 28 – Компоненты простого актуаторы

Окулография (отслеживание глаз, трекинг глаз; айтрекинг) — определение координат взора («точки пересечения оптической оси глазного яблока и плоскости наблюдаемого объекта или экрана, на котором предъявляется некоторый зрительный раздражитель»).

Отслеживатель глаз (**айтрекер**) — устройство (рис.29), используемое для определения ориентации оптической оси глазного яблока в пространстве (то есть для отслеживания глаз).

Отслеживатели глаз используются в исследованиях зрительной системы, психологии, когнитивной лингвистике, промышленном управлении. Для отслеживания глаз используется несколько методов. Самый популярный — покадровый анализ видеосъёмки глаза, также используются контактные методы, такие как электроокулография.

Рис. 29 – Айтрекер

Применения систем айтрекинга включают в себя веб-юзабилити (удобство чтения веб-страниц конечным потребителем), рекламу, оптимизацию внешнего дизайна продукции и автоматизацию разработки. В общем коммерческое использование отслеживания глаз в большинстве сводится к тому, что группе потребителей предъявляется один и тот же визуальный стимул, в то время как отслеживаются движения глаз. Примерами конечных стимулов могут быть веб-сайты, телевизионные программы, трансляции спортивных состязаний, фильмы, рекламные ролики, страницы журналов, страницы газет, упаковки некоторых продуктов и прилавки магазинов, также банкоматы и пользовательские интерфейсы программного обеспечения.

Результирующие данные могут быть статистически анализированы и графически отражены для того, чтобы показать справедливость сделанных выводов. Путём исследования фиксаций, изменения размера зрачка, морганий и ряда других параметров исследователи в значительной степени могут определить эффективность созданного информационного ресурса или продукта. Пока некоторые компании пытаются решить подобные задачи внутренними ресурсами, другие привлекают фирмы, предлагающие услуги отслеживания глаз. Наиболее многообещающее поле использования коммерческого отслеживания глаз это веб-юзабилити. Несмотря на то, что традиционные техники юзабилити дают достаточно адекватные данные путём анализа кликов мышкой и прокручивания, айтрекинг даёт возможность анализировать связь между поведением пользователя и кликами мышкой.

Это даёт значительное улучшение оценки того, какие фрагменты веб-сайта являются наиболее привлекательными для пользователя, какие фрагменты веб-сайта вызывают трудности у конечного пользователя и какие пользователем не замечаются. Айтрекинг также может быть использован для оценки эффективности поиска, правильности концепции бренда, онлайн-исследования, юзабилити перехода между страницами, эффективности общего дизайна и многих других аспектов веб-дизайна. В процессе исследования может быть проведено сравнение двух сайтов-конкурентов.

Отслеживание глаз традиционно используется для оценки эффективности рекламы на различных медиаресурсах. Телевизионные видеоролики, рекламные буклеты, реклама на интернет-сайтах, показ эмблемы спонсоров в телепрограммах, все это открывает обширное поле деятельности для коммерческого отслеживания глаз. Анализируются заметность упаковки с продуктом или некоторого логотипа на витрине магазина, газеты, веб-сайта и телепрограммы. Это позволяет исследователям с высокой детализацией оценивать то, как потребители замечают или не замечают логотип конечного продукта, упаковку, POS. Таким образом, специалист по рекламе может оценить эффективность рекламной компании благодаря реальному визуальному восприятию.

Отслеживание глаз позволяет разработчикам упаковки продукта оценить её эффективность. Таким образом могут быть оценены заметность, привлекательность и соответствие современным трендам исследуемой упаковки с целью оптимального выбора. Отслеживание глаз часто используется, пока коммерческий продукт ещё находится на стадии прототипа. Прототипы часто тестируются парами для выявления наиболее эффективного своего дизайна, а также сравнение с решениями конкурентов.

Одно из наиболее многообещающих применений отслеживания глаз это оптимизация дизайна уличных терминалов. В настоящее время исследователи дошли до того, что предлагают интегрировать айтрекеры в серийно производимые уличные терминалы/банкоматы. Основной задачей этого является уменьшения времени взаимодействия между человеком и устройством.

Отслеживатели глаз могут также использоваться для оптимизации системы автофокуса цифровой фотокамеры (резкость наводится туда, куда смотрит пользователь).

The National Highway Traffic Safety Administration (NHTSA) утверждает, что интеграция отслеживателей глаз в автомобиле может сократить количество ДТП на 100 тысяч в год. В соответствие с их исследованиями до 80 % ДТП происходят в результате неправильных действий водителя в течение 3-х секунд перед аварией. Экипировка автомобилей айтрекерами позволит значительно увеличить класс безопасности этих автомобилей. «Лексус» обещает оснастить модель LS460 встроенным отслеживателем глаз, подающим предупреждающий сигнал в случае, если водитель отвлекается от дороги.

С 2006 года система айтрекинга используется в коммуникационном оборудовании для полностью парализованных людей. Они позволяют набирать текстовые сообщения, отправлять электронную почту, работать в интернете, используя исключительно их глаза. Отслеживание глаз позволяет достичь положительных результатов даже в случае церебрального паралича, при котором пациент совершает непроизвольные движения.

Понятно, что современный айтрекинг **не может обойтись** без интеграции **в мир сетевого окружения**. И работы в этом направлении уже ведутся. Рекомендую ознакомится с статьей на портале Хабрахабр «Айтрекинг в UX-исследованиях (QR-код с ссылкой указан на текущей страницей). Рекомендовал бы также найти небольшую статью «Управление компьютером при помощи глаз — практическая реализация» на том же портале.

Айтрекинг в UX-исследованиях

Конечным этапом или сущностной ценностью данного издания является закрепление понимания функционирования сетей в концепции Internet of Things (IoT), построенных в рамках LPWAN/BAN/PAN. Для это необходимо воспользоваться инструментом моделирования сети, содержащей в себе актуаторы (датчики), средства контроля (управляющие компоненты, полнофункциональные устройства).

Таким образом, необходимо было решить три **задачи** практического характера:

1. Исследование реально существующей интеллектуальной домашней сети.
2. Добавление проводных устройств ввода-вывода в интеллектуальную домашнюю сеть
3. Добавление беспроводных устройств ввода-вывода в интеллектуальную домашнюю сеть.

Для этих целей была разработана комплексная лабораторная работа. Для выполнения данной работы необходимо **следующее оборудование и программное обеспечение**: Персональный компьютер с 64х битной операционной системой Windows 7, 8, 8.1, 10 (рекомендуемо) или Ubuntu Linux 16.04 LTS (и выше) с установленным программным обеспечением: симулятором сети передачи данных Cisco Packet Tracer версии не ниже 7.1 (рекомендуется 7.2 и новее).

Напомним, что умный дом — единая система управления в доме, офисе, квартире или здании, включающая в себя датчики, управляющие элементы и исполнительные устройства.

Исследуем конечные устройства IoT в программе Cisco Packet Tracer 7.2:

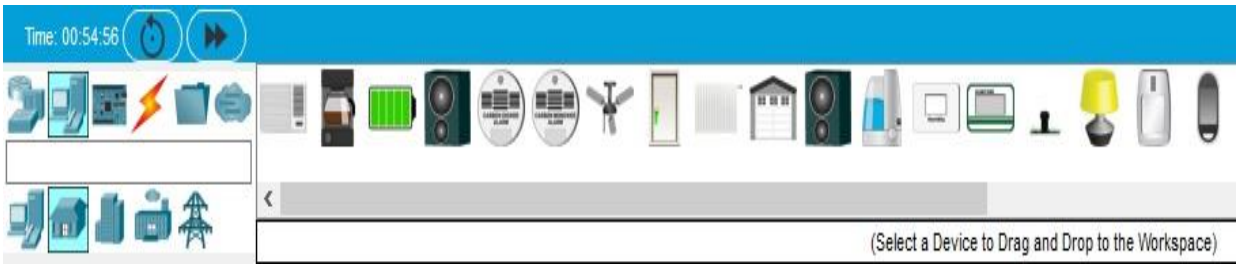


Рис.30 - Конечные устройства IoT в программе Cisco Packet Tracer.

В нижнем меню программы Cisco Packet Tracer во вкладке End Devices (рис.30) –> Home находятся различные элементы Smart Home IoT для умного дома.

Наведя мышкой на устройство, откроется окно основного перечня свойств данного элемента:

Рис.31 - Информационное окно с основной сетевой информацией об устройстве.

С интерфейсом на первоначальном этапе мы разобрались. Теперь мы должны открыть (рис.32) готовый проект сети (файл: **Packet Tracer - Adding IoT Devices to a Smart Home.pkt)**

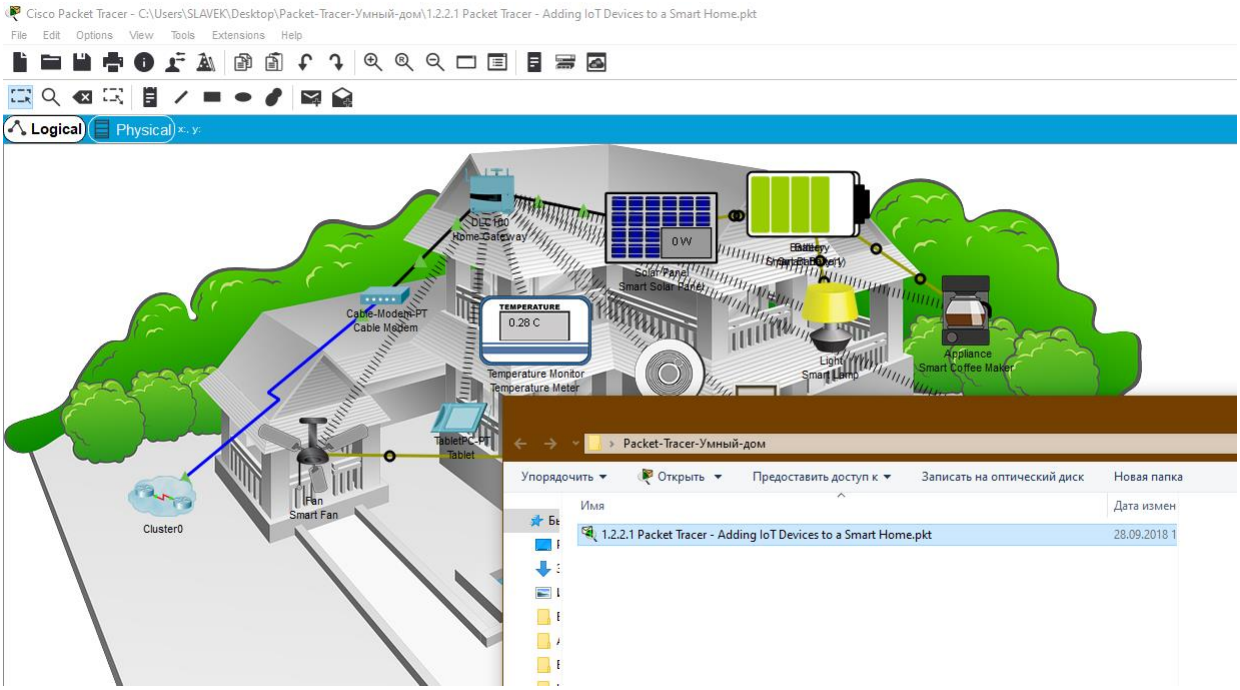


Рис. 32 – Проект сети

Давайте рассмотрим ее более детально. Интеллектуальная домашняя сеть, представленная на рисунке 32, состоит из инфраструктурных устройств, таких как «домашний» шлюз – управляющее устройство (устройство координатор по классификации PAN/LPWAN сетей).

Щелкнем значок Home Gateway, чтобы открыть окно устройства Home Gateway.

Перейдем на вкладку Config для просмотра настроек (рис.32):

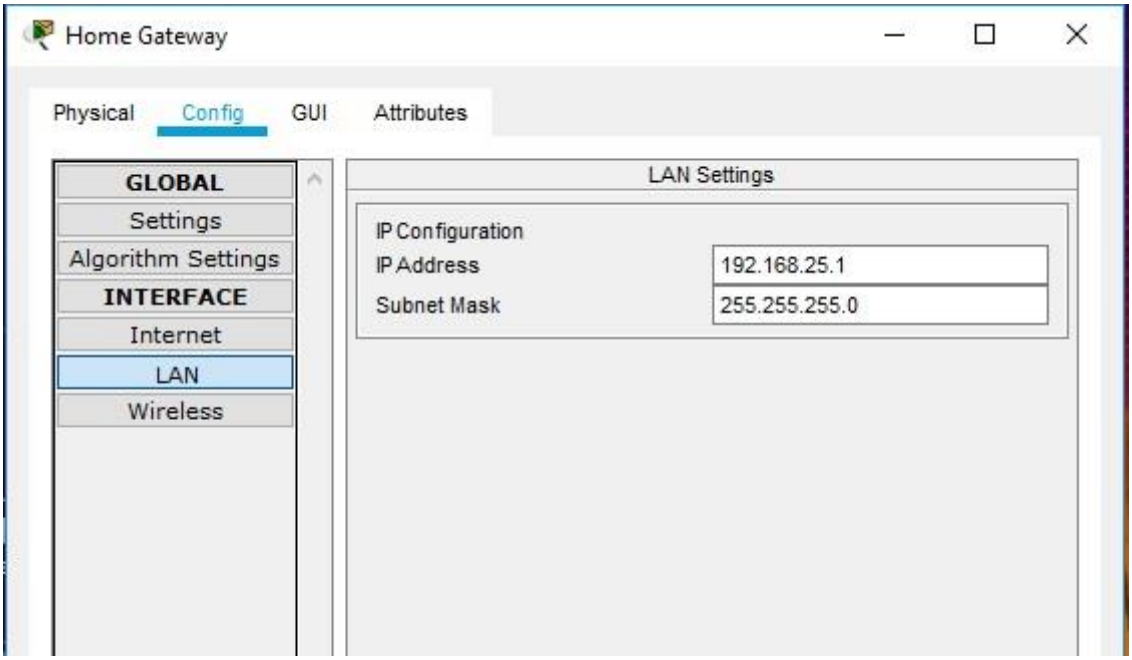


Рис. 32 – Окно настроек LAN главного шлюза.

Тут мы видим IP адрес сети. Нажмём на Wireless и увидим настройки беспроводной сети. Затем перейдите на вкладку «Конфигурация», а затем в левой панели щелкните «ЛВС», чтобы просмотреть настройки локальной сети главного шлюза. Запишите IP-адрес домашней сети для дальнейшего использования. Нажмите «Беспроводная связь» (Wireless) в левой панели, чтобы просмотреть настройки беспроводной сети домашнего шлюза.

Запишите SSID домашней сети и WPA2-PSK пароль для дальнейшего использования. Закройте окно Home Gateway.

Затем щелкните значок устройства планшета (**Tablet PC**), чтобы открыть окно планшета. В окне «Планшет» (**рис.33**) выберите вкладку «Рабочий стол», а затем щелкните значок «Веб-браузер». В окне веб-браузера введите IP-адрес Home Gateway **192.168.25.1** в поле URL и нажмите «Перейти». На экране входа в Home Gateway введите admin для имени пользователя и пароля и нажмите «Отправить».

В окне веб-браузера (**рис. 34**) введите IP-адрес Home Gateway 192.168.25.1 (адрес панели администрирования Home Gateway по умолчанию) в поле URL и нажмите «Перейти». На экране входа в Home Gateway введите admin для имени пользователя и пароля и нажмите «Отправить».

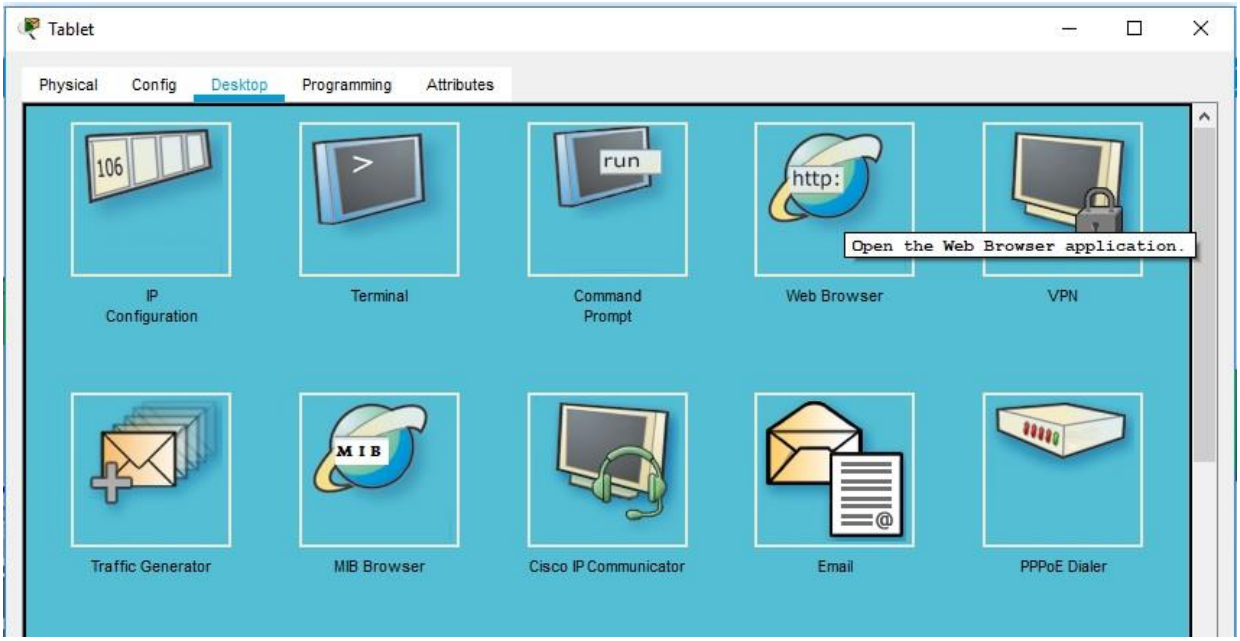


Рис. 33 – вкладка Desktop

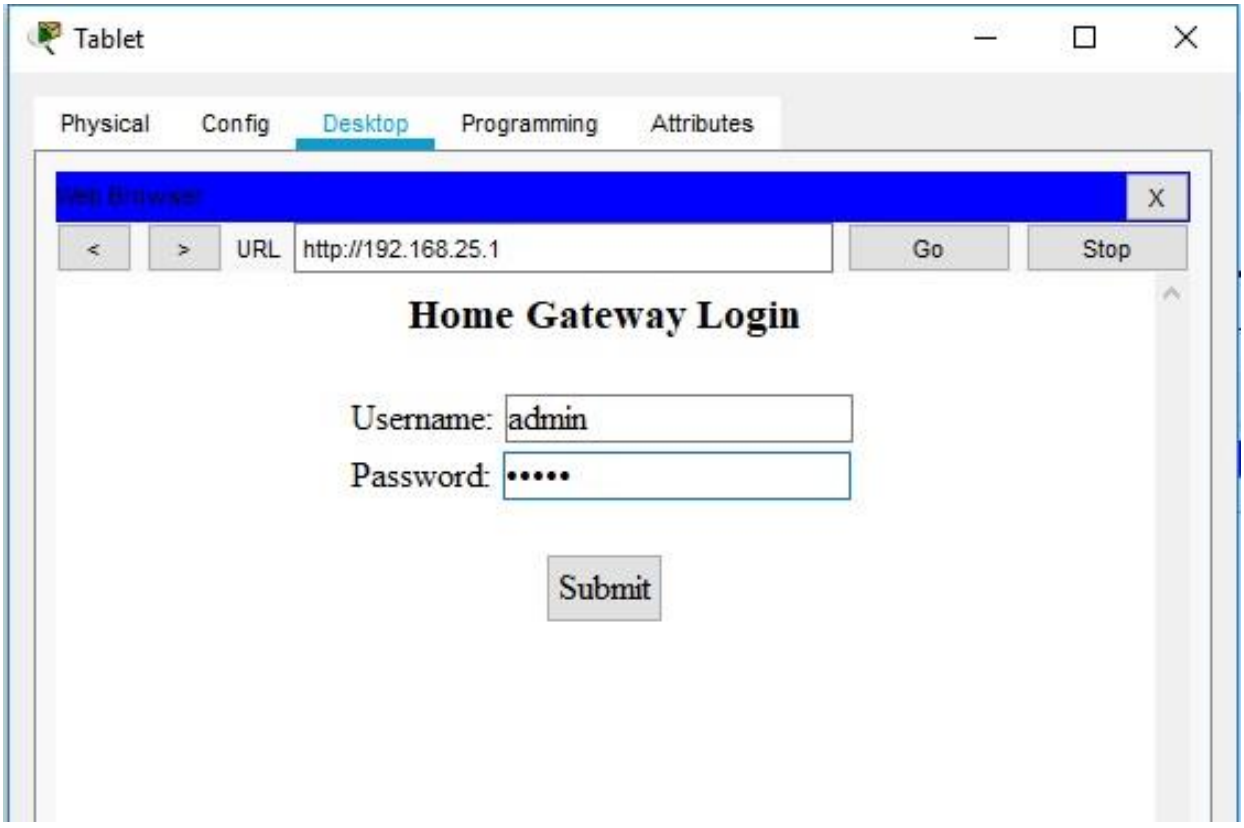


Рис. 34 – Панель сетевого администрирования Home Gateway

После того, как вы подключились к веб-интерфейсу Home Gateway, появится список всех подключенных устройств IoT. Когда вы нажимаете на устройство в списке, отображается состояние и настройки этого устройства.

В своем отчете отразите все подключенные устройства, отразив их тип, PTT (серийный номер).

Добавление проводных устройств ввода-вывода в интеллектуальную домашнюю сеть.

Подключение устройства в сеть с помощью кабеля.

а. В поле «Выбор устройства» выберите значок «Газонный разбрызгиватель»(Lawn Sprinkler), а затем щелкните в рабочей области, где вы хотите разместить разбрызгиватель.

б. Присоединение газонного разбрызгивателя к домашнему шлюзу.

В поле «Выбор типа устройства» щелкните значок [Подключения] (это выглядит как молния). Щелкните значок типа соединителя Copper Straight Through в поле «Выбор устройства». Затем нажмите значок «Разбрызгиватель» и подключите один конец кабеля к интерфейсу FastEthernet0 Sprinkler. Затем щелкните значок Home Gateway и подключите другой конец кабеля к доступному интерфейсу Ethernet.

Настройка разбрызгивателя для сетевого подключения

а. Нажмите значок устройства разбрызгивателя в рабочей области, чтобы открыть окно устройства. Обратите внимание: прямо сейчас имя разбрызгиватель для газона является общим IoT0.

Окно устройства откроется на вкладке «Спецификация» (рис.35), которая дает информацию об устройстве, которое может быть отредактировано.

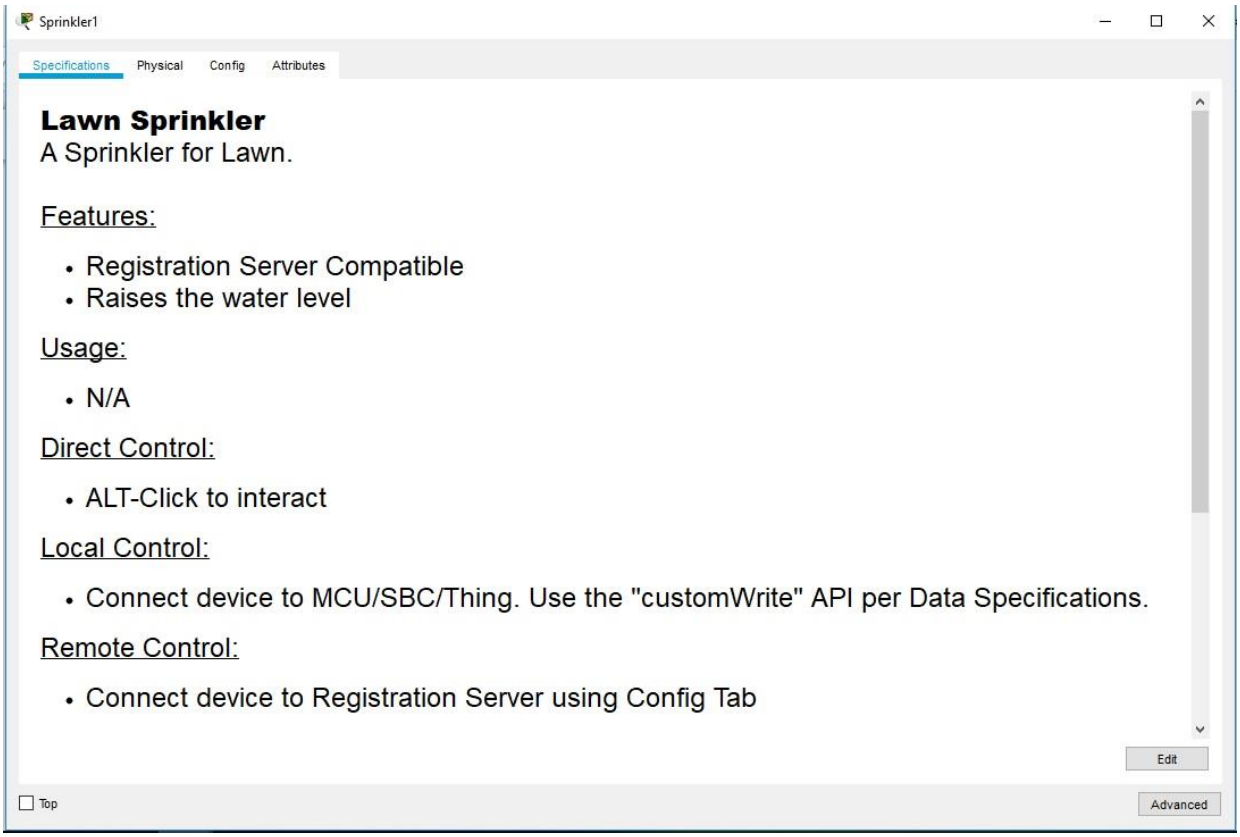


Рис. 35 – Окно спецификаций

6. Перейдите на вкладку «Конфигурация», чтобы изменить настройки конфигурации устройства. На вкладке «Конфигурация» (рис. 36) внесите следующие изменения в «Настройки»:

— Установите отображаемое имя в Sprinkler1 (обратите внимание, что имя окна изменяется на Sprinkler1).

— Установите сервер IoT на домашний шлюз.

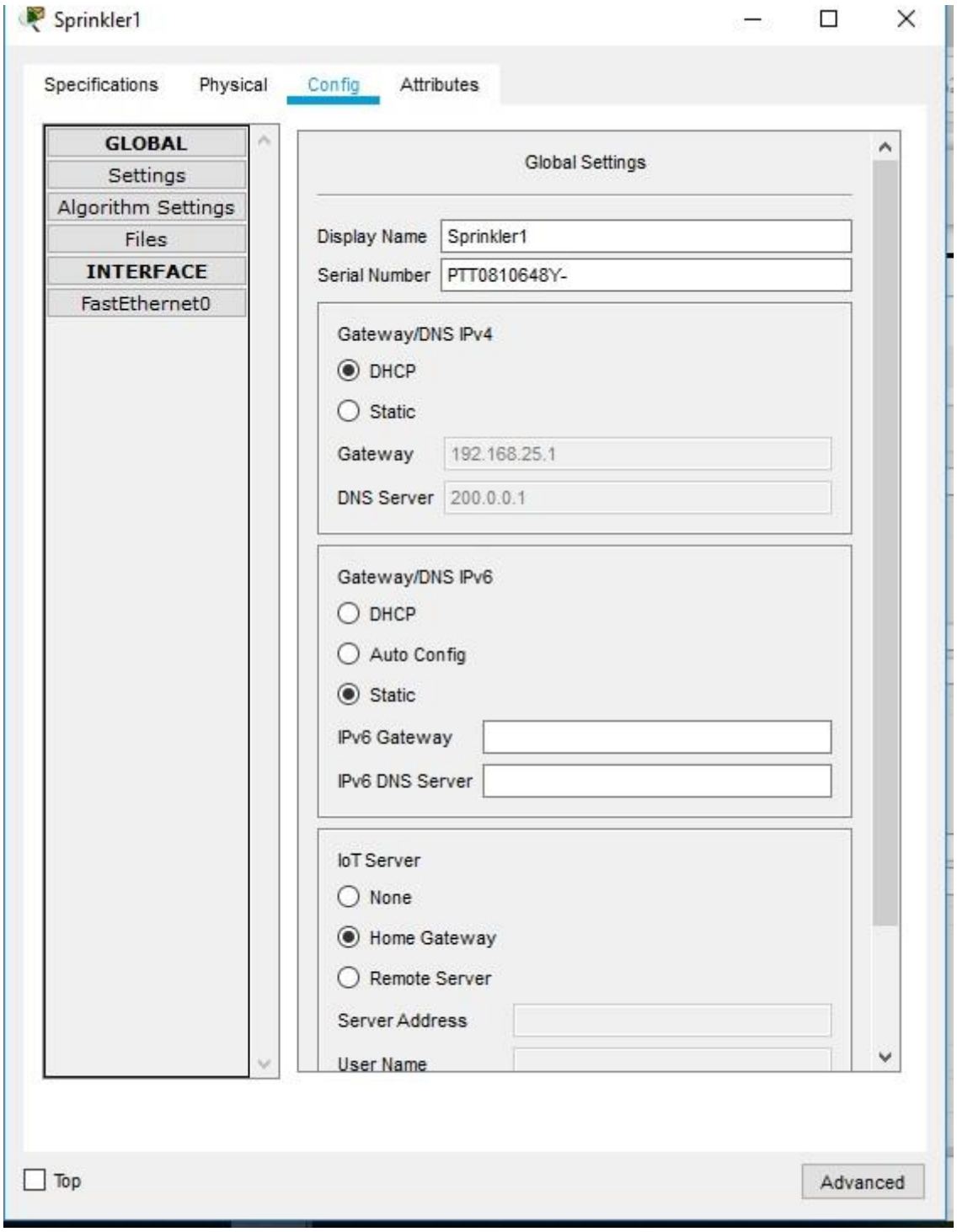


Рис. 36 – Вкладка конфигурации IoT-устройства

Нажмите FastEthernet0 и измените IP-конфигурацию на DHCP. Закройте окно разбрызгивателя.

c. Убедитесь, что разбрызгиватель находится в сети. Войдите в Home Gateway из планшета. Устройство Sprinkler 1 теперь должно появиться в списке IoT Server — Devices.

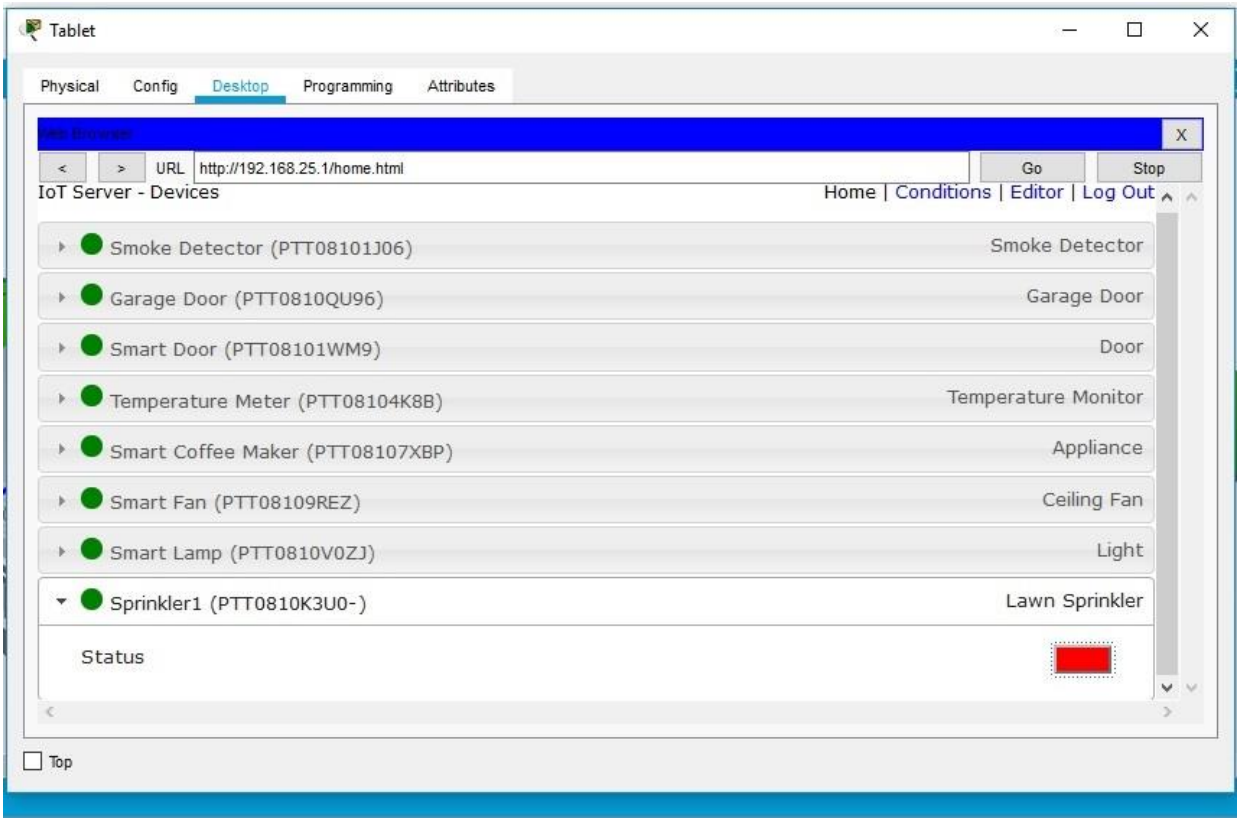


Рис. 37 – Status Sprinkler

Измените статус разбрызгивателя на включен. Для этого щёлкните по красной кнопке.

У кнопки должен поменяться цвет на зелёный. Закройте окно планшета. Экспериментируйте, добавив другие типы IoT-устройств в интеллектуальную домашнюю сеть.

Рис. 38 – Включенный IoT-разбрызгиватель воды

Добавление беспроводных устройств ввода-вывода в интеллектуальную домашнюю сеть

Добавление беспроводного устройства в сеть.

В поле «Выбор конкретного устройства» щелкните значок «Детектор ветра», а затем щелкните в рабочей области, где вы хотите разместить детектор ветра (Wind Detector).

Добавьте беспроводной модуль в детектор ветра.

Нажмите значок Wind Detector в рабочей области, чтобы открыть окно устройства IoT. В правом нижнем углу окна устройства IoT нажмите кнопку «Дополнительно». Обратите внимание, что в верхней части окна видны больше вкладок. Перейдите на вкладку «Конфигурация ввода-вывода» (рис.39).

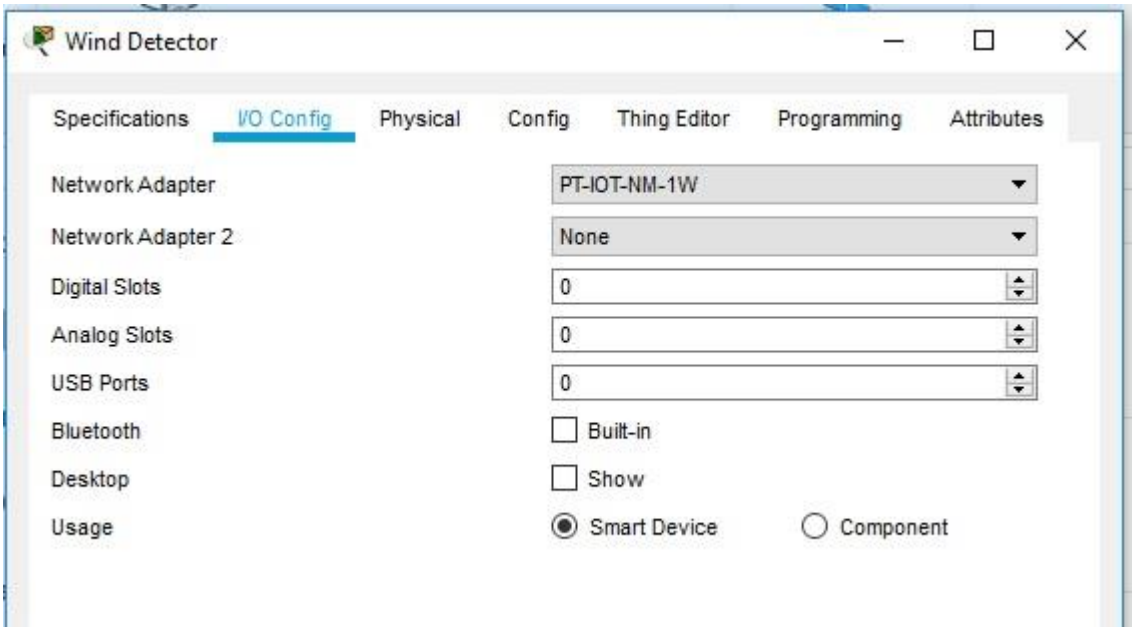


Рис. 38 – Вкладка «Конфигурация ввода-вывода»

Измените выпадающий список Network Adapter на PT-IOT-NM-1W, который является беспроводным адаптером.

Настройте детектор ветра для беспроводной сети.

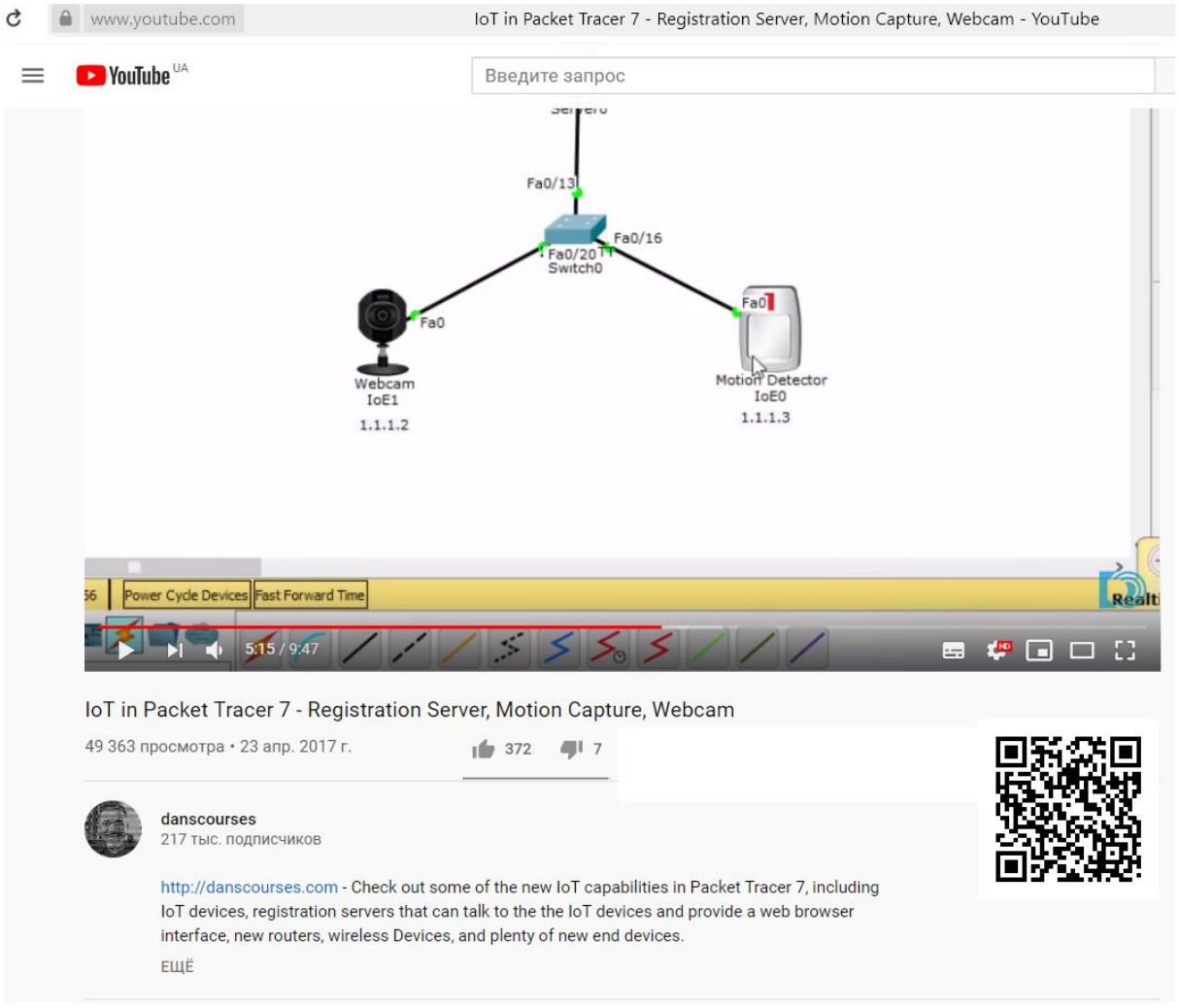
Перейдите на вкладку Конфигурация. Измените отображаемое имя на Wind_Detector и измените IoT-сервер на Home Gateway. Затем щелкните Wireless0 в левой панели. Измените тип аутентификации на WPA2-PSK и в поле PSC Pass Phrase введите mySecretKey. Это настройки беспроводной сети домашнего шлюза (Home Gateway), которые вы записали ранее.

Между детектором ветра и Домашним шлюзом должно быть установлено беспроводное соединение (полосы-волны между устройствами в общей схеме). Убедитесь, что детектор ветра находится в сети (проверьте через админ.панель)

Войдите в Home Gateway с помощью планшета. Устройство Wind Detector теперь должно появиться в списке IoT Server — Devices.

Экспериментируйте, добавив другие типы устройств IoT в интеллектуальную домашнюю беспроводную сеть. Можно так же согласовать работу двух устрой. Посмотрите в **видео** (**QR-на текущей странице - IoT in Packet Tracer 7 - Registration Server, Motion Capture, Webcam**), как можно согласовать работу датчика движения и вебкамеры.

В отчете вы должны приложить скриншот таблицы маршрутизации Home Gateway, описать его технические характеристики (количество портов LAN/WAN), приложить сетевые настройки для всех подключенных устройств. Также вам необходимо будет подключить Home Gateway проводным образом к любой локальной проводной (не IoT сети), **сделанной ранее вами**.



§ VIII. Модель межмашинного взаимодействия(M2M).

Представьте себе обширное предприятие, оснащенное «умным» оборудованием и технологиями, основанными на радиометках, — все машины соединены друг с другом и общаются в рамках производственного процесса с помощью датчиков и исполнительных механизмов. Операторы пользуются планшетами, связываясь с производственными системами для диагностики и управления. Данные о загруженности и работоспособности оборудования, а также диагностика накапливаются в корпоративных системах планирования ресурсов и оптимизации производства. Взамен оборудование получает команды подстройки производственного цикла, оптимизирующие соотношение затрат и качества. Машины также «общаются» со своими производителями, по мере необходимости заказывая ремонт и запчасти, чтобы избежать простоев. Системы, основанные на агентских модулях, распределяют нагрузку между производственными линиями, действующими в разных регионах мира, помогая оптимизировать затраты на цепочку поставок. Все это уже реальность — так называемые умные фабрики, а фабрики будущего смогут адаптироваться к новым требованиям гораздо быстрее, чем нынешние решения для гибкого производства. Умная фабрика соединяет машины, логистику и людей, обеспечивая оперативную повсеместную координацию.

Межмашинное взаимодействие (машинно-машинное взаимодействие, англ. Machine-to-Machine, M2M) — это как раз и есть общее название технологий, которые позволяют машинам обмениваться информацией друг с другом, или же передавать её в одностороннем порядке. Это могут быть проводные и беспроводные системы мониторинга датчиков или каких-либо параметров устройств (температура, уровень запасов, местоположение и т. д.). К примеру, банкоматы или платёжные терминалы могут автоматически передавать информацию по GSM-сетям, а также если у них закончилась чековая бумага или наличность, или же наоборот, что наличности слишком много и требуется приезд инкассаторов.

M2M также активно используется в системах безопасности и охраны, вендинге, системах здравоохранения, промышленных телеметрических системах (производство, энергетика, ЖКХ и др.) и системах позиционирования подвижных объектов на основе систем ГЛОНАСС/GPS. Одним из подклассов M2M является межмашинное взаимодействие с использованием мобильных решений, для него также может использоваться аббревиатура M2M (англ. Mobile-to-Mobile). Принципы, по которым различные полевые устройства соединяются с ИТ-системами предприятия, применимы не только к автоматизации и производственной отрасли.

Основное различие между IoT и M2M заключается в том, что IoT (Интернет вещей) использует беспроводную связь, в то время как M2M (межмашинное взаимодействие) может использовать как проводную, так и беспроводную связь. IoT подключает интеллектуальные устройства к сети для сбора данных, анализа и принятия разумных решений, а M2M позволяет устройствам связываться и выполнять необходимые действия без участия человека.

IoT — это Интернет вещей, а M2M — межмашинное взаимодействие. IoT подключает интеллектуальные устройства к сети для сбора данных, анализа и принятия разумных решений. С другой стороны, M2M позволяет устройствам связываться и выполнять необходимые действия без участия человека. IoT использует беспроводную связь, тогда как M2M может использовать проводную или беспроводную связь.

IoT требует активного подключения к Интернету, в то время как у M2M оно может отсутствовать. Требование к интернет-соединению у M2M зависит от работающего приложения, IoT сильно зависит от интернет-соединения и наличия «облака», тогда как M2M в часто полагается на проводную сеть.

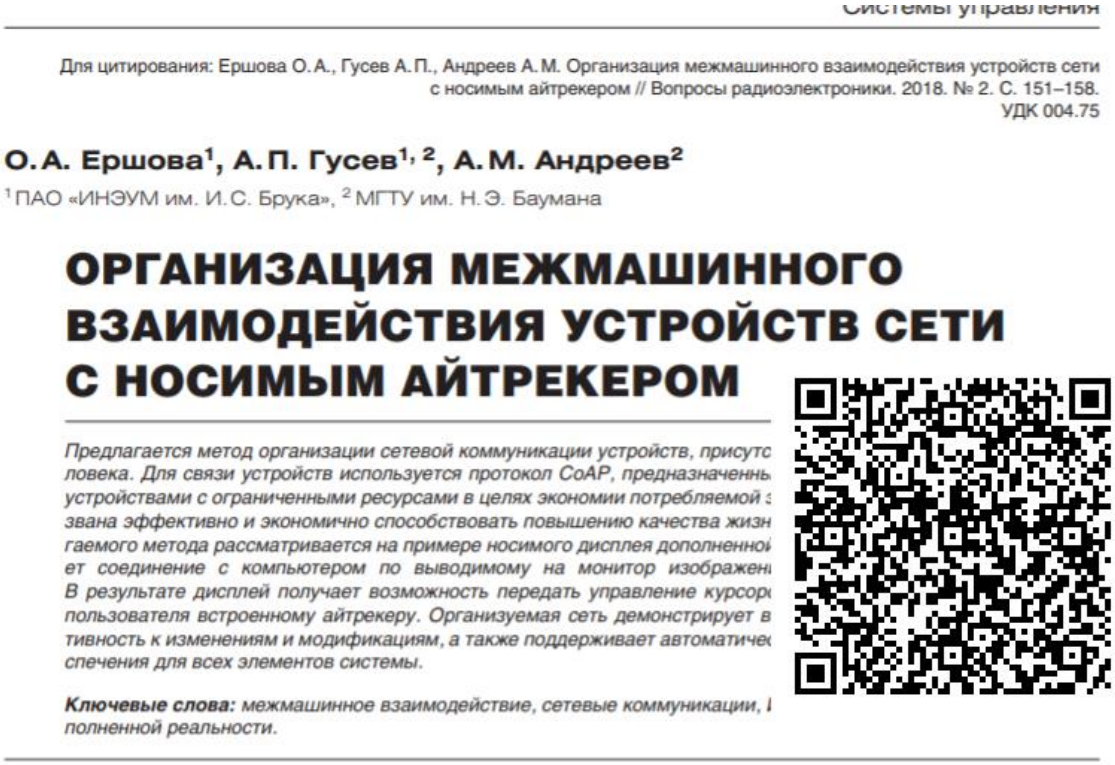
Сегодня мир более связан, чем когда-либо. Развитие технологий объединяет не только людей, но и устройства и машины по всему миру. IoT и M2M — это две технологии, которые помогают повысить производительность, эффективность, точность и улучшить общее качество жизни. M2M и IoT очень являются очень близкими технологиями, но IoT является более новой из них. M2M является основой для IoT. Системы на базе IoT и M2M автоматически контролируют себя, реагируют на изменения и выполняют задачи без вмешательства человека. В частности, межмашинное взаимодействие (Machine-to-Machine, M2M) уже осуществляется в транспортной индустрии для диагностики автомобилей и их соединения с информационными системами. Средства M2M применяются в имплантируемых медицинских устройствах и глобальных логистических компаниях.

§ IX. Организация межмашинного взаимодействия устройств сети с носимым айтрекером*

В статье-обзоре, которую я предлагаю к прочтению, предлагается метод организации сетевой коммуникации устройств, присутствующих в повседневной жизни человека. Для связи устройств используется описываемый протокол CoAP, предназначенный для обмена сообщениями между устройствами с ограниченными ресурсами в целях экономии потребляемой электроэнергии.

По заявлению авторов: подобная сеть призвана эффективно и экономично способствовать повышению качества жизни людей. Механизм работы предлагаемого метода рассматривается на примере носимого дисплея дополненной реальности, который устанавливает соединение с компьютером по выводимому на монитор изображению идентификационного QR-кода. В результате дисплей получает возможность передать управление курсором мыши на мониторе компьютера пользователя встроенному айтрекеру.

Организуемая сеть демонстрирует высокую производительность, адаптивность к изменениям и модификациям, а также поддерживает автоматическое обновление программного обеспечения для всех элементов системы.



Системы управления

Для цитирования: Ершова О.А., Гусев А.П., Андреев А.М. Организация межмашинного взаимодействия устройств сети с носимым айтрекером // Вопросы радиоэлектроники. 2018. № 2. С. 151–158.
УДК 004.75

О.А. Ершова[1], А.П. Гусев[1, 2], А.М. Андреев[2]

[1] ПАО «ИНЭУМ им. И.С. Брука», [2] МГТУ им. Н.Э. Баумана

ОРГАНИЗАЦИЯ МЕЖМАШИННОГО ВЗАИМОДЕЙСТВИЯ УСТРОЙСТВ СЕТИ С НОСИМЫМ АЙТРЕКЕРОМ

Предлагается метод организации сетевой коммуникации устройств, присутс ловека. Для связи устройств используется протокол CoAP, предназначенны устройствами с ограниченными ресурсами в целях экономии потребляемой звана эффективно и экономично способствовать повышению качества жизн гаемого метода рассматривается на примере носимого дисплея дополненно ет соединение с компьютером по выводимому на монитор изображени В результате дисплей получает возможность передать управление курсор пользователя встроенному айтрекеру. Организуемая сеть демонстрирует в тивность к изменениям и модификациям, а также поддерживает автоматичес спечения для всех элементов системы.

Ключевые слова: *межмашинное взаимодействие, сетевые коммуникации, полненной реальности.*

Список использованных источников.

1. Одом У. Компьютерные сети. Первый шаг. Computer Networking: First-step / Пер. В. Гусев. — СПб.: «Вильямс», 2006. — 432 с. — (Первый шаг). — 3 000 экз. — ISBN 5-8459-0881-7. Таненбаум Э, Уэзеролл Д. Компьютерные сети. — Питер, 2012. — 960 с.
2. Малиновский Б.Н. История вычислительной техники в лицах. - К.: фирма "КИТ", ПТОО "А.С.К.", 1995. - 384 с.
3. Орлов С.А. Технологии разработки программного обеспечения. Разработка сложных программных систем: Учебное пособие для вузов / Сергей Александрович Орлов. - СПб.: Питер, 2002. - 464 с.: ил. - (Учебник для вузов).
4. Кирсанов, Э.А. Обработка информации в пространственно-распределенных системах радиомониторинга: статистический и нейросетевой подходы [Электронный ресурс]: учебное пособие / Э.А. Кирсанов, А.А. Сирота. — Электрон. дан. — Москва : Физматлит, 2012. — 344 с.
5. Сборник методических указаний для выполнения практических заданий и лабораторных работ курса "IoT Академия Samsung" [Электронный ресурс]: — Режим доступа: http://timp.keva.su/samsungIoT.7z (дата обращения: 19.11.2019).
6. Леонид Черняк. Платформа Интернета вещей. Открытые системы. СУБД, №7, 2012. Открытые системы (26 сентября 2012).
7. Росляков А.В., Ваняшин С.В., Гребешков А.Ю. Интернет вещей. Учебное пособие. — Самара: ПГУТИ, 2015. — 200 с.
8. Кенин, Александр Практическое руководство системного администратора / Александр Кенин. - М.: БХВ-Петербург, 2013. - 766 с.
9. Тихвинский В., Коваль В., Бочечка Г. Перспективы стандартизации интернета вещей в международных организациях связи//Первая миля. 2017. № 2 (63). С. 26 -32.
10. Алексеев В. Технологии «Интернета вещей» для сетей ISM не лицензируемого диапазона частот//Беспроводные технологии. 2017. Т. 1. № 46. С. 44 -50.
11. Шешалевич В.В. LPWAN - низкопотребляющие сети большого радиуса действия. Связь для интернета вещей//Безопасность информационных технологий. 2017. № 3. С. 6 -16.

12. Motlagh N. H., Taleb T., Arouk O. Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives//IEEE Internet of Things Journal. New Jersey, US: IEEE, 2016, pp. 899 -922.
13. Терентьев М.Н. Обзор публикаций, посвящённых самоорганизации беспроводных сенсорных сетей//Труды МАИ. 2017. № 94. URL: http://trudy.mai.ru/published.php?ID=81149
14. Трифонова С.В., Холодов Я.А. Исследование и оптимизация работы беспроводной сенсорной сети на основе протокола ZigBee//Компьютерные исследования и моделирование. 2012. Т. 4. № 4. С. 855 -869.
15. Бородин В.В., Петраков А.М., Шевцов В.А. Анализ алгоритмов маршрутизации в сети связи группировки беспилотных летательных аппаратов//Труды МАИ. 2016. № 87. URL: http://trudymai.ru/published.php?ID=69735
16. Шешалевич В.В. LPWAN -низкопотребляющие сети большого радиуса действия. Связь для интернета вещей//Безопасность информационных технологий. 2017. № 3. С. 6 -16.
17. Беспроводные сенсорные сети: обзор. Акулдиз И.Ф. - Перевод с английского: Левжинский А.С. [Электронный ресурс]: — Режим доступа: http://masters.donntu.org/2011/fknt/levzhinsky/library/translate.htm (дата обращения: 9.01.2020).

BAN, PAN, LAN, CAN WSN: Zigbee, IoT, M2M

Данное издание предназначено для восполнения недостающих теоретических знаний по дисциплинам, междисциплинарным курсам, связанных с принципами организации межсетевого взаимодействия, архитектуры информационных систем: («Организация, принципы построения и функционирования компьютерных систем», «Математический аппарат для построения компьютерных систем», «Дизайн архитектуры распределенных сетей», «Инфокоммуникационные системы и сети», «Информационные технологии», «Внедрение и поддержка программного обеспечения компьютерных систем», «Компьютерные и телекоммуникационные сети») студентов, осваивающих программы среднего и высшего профессионального обучения.

Получение недостающих знаний – серьезный инструмент общего процесса актуализации: поддержания практических и теоретических знаний индивидуума в актуальном состоянии, т.е. приведение их в соответствие с состоянием отображаемых объектов предметной области будущего специалиста в сфере информационных технологий и вычислительной техники. Я отождествляю вкладываемый смысловой контекст данной книги с понятиями необходимого и достаточного условий — известных вам по изучаемым математическим дисциплинам.

Учебное издание «Компьютерные сети. IoT и межмашинное взаимодействие» и выступает в роли достаточного условия процесса снятия информационной энтропии, касающегося профессионального ориентирования студентов вышеперечисленного профиля подготовки.

Издание содержит в себе ряд перспективных т.н. «Рабочих предложений» (RFC) от IETF, IEEE, и иных организаций, занимающихся сертификацией технологий в рассматриваемой области человеческой деятельности, а также статей с верифицированных иностранных и отечественных научных и публицистических изданий. Часть информации подана в явном компрессированном виде, и неявном – полноценном. Все это достигается за счет внедрения на страницы издания печатных QR-кодов с ссылками на те или иные интернет-ресурсы. Таким образом, книга получает куда более расширенное функционально-интерактивное предназначение.

Надеюсь, что тщательно подобранные, переработанное и адаптированные к чтению, материалы данного учебного курса (вместе с планируемым дополнением, выраженным в виде курса лабораторных работ в сетевом эмуляторе Cisco Packet Tracer) станут путеводной звездой для поколения новых инженеров – архитекторов Интернета завтрашнего дня.

В.Д. Мунистер

2020