

НАУЧНАЯ МЫСЛЬ

СЕРИЯ ОСНОВАНА В 2008 ГОДУ

**Е.П. ЗАРАМЕНСКИХ
И.Е. АРТЕМЬЕВ**

ИНТЕРНЕТ ВЕЩЕЙ

ИССЛЕДОВАНИЯ И ОБЛАСТЬ ПРИМЕНЕНИЯ

МОНОГРАФИЯ

Электронно-
Библиотечная
Система
znanium.com

Москва
ИНФРА-М
2023

УДК 004.72(075.4)
ББК 32.97
334

ФЗ
№ 436-ФЗ

Издание не подлежит маркировке
в соответствии с п. 1 ч. 2 ст. 1

Зараменских Е.П.

334 Интернет вещей. Исследования и область применения : монография / Е.П. Зараменских, И.Е. Артемьев. — Москва : ИНФРА-М, 2023. — 188 с. — (Научная мысль). — DOI 10.12737/13342.

ISBN 978-5-16-011476-7 (print)

ISBN 978-5-16-103731-7 (online)

Монография содержит исследование Интернета вещей как технической концепции, анализ возможных последствий ее развертывания и основных трендов, обзор существующих проектов и разработок, а также характеристику используемых на практике технологий из данной сферы.

УДК 004.72(075.4)
ББК 32.97

ISBN 978-5-16-011476-7 (print)
ISBN 978-5-16-103731-7 (online)

© Зараменских Е.П.,
Артемьев И.Е., 2015

Подписано в печать 29.06.2022.

Формат 60×90/16. Печать цифровая. Бумага офсетная.

Гарнитура *Newton*. Усл. печ. л. 11,75.

ППТ20. Заказ № 00000

ТК 455100-1896435-250915

ООО «Научно-издательский центр ИНФРА-М»

127214, Москва, ул. Полярная, д. 31В, стр. 1.

Тел.: (495) 280-15-96, 280-33-86. Факс: (495) 280-36-29.

E-mail: books@infra-m.ru

<http://www.infra-m.ru>

Отпечатано в типографии ООО «Научно-издательский центр ИНФРА-М»

127214, Москва, ул. Полярная, д. 31В, стр. 1

Тел.: (495) 280-15-96, 280-33-86. Факс: (495) 280-36-29

Оглавление

https://t.me/it_boooks/2

Список принятых сокращений	5
Введение	6
Глава 1. Концепция Интернета вещей	8
1.1. Развитие концепции.....	8
1.1.1. Радиочастотная идентификация (RFID) как предпосылка к возникновению концепции Интернета вещей	9
1.1.2. Возникновение понятия «Интернет вещей».....	10
1.2. Определение понятия	12
1.3. Получение информации об окружающем мире	15
1.4. Общая характеристика	18
1.5. Интернет вещей как основа Индустрии 4.0.....	23
1.6. Интернет вещей как источник угроз	26
1.7. Техническая безопасность	27
1.8. Социальные угрозы	29
1.9. Исследовательские центры и проекты	32
1.10. Тематические конференции	34
Глава 2. Технологии Интернета вещей.....	37
2.1. Средства виртуальной идентификации объектов внешней среды	38
2.1.1. Штрих-кодирование	39
2.1.2. Радиочастотная идентификация	44
2.1.3. Особенности технологий RFID и штрихового кодирования.....	56
2.2. Датчики и сенсоры Интернета вещей	58
2.2.1. Различия между датчиками и сенсорами.....	58
2.2.2. Функции и разновидности датчиков и сенсоров.....	60
2.2.3. Датчики и сенсоры в концепции «умного» дома.....	64
2.2.4. Сенсоры биометрических показателей человека.....	67
2.2.5. Датчики и сенсоры в сфере транспорта	70
2.2.6. Датчики параметров окружающей среды	79
2.3. Средства сбора, передачи, обработки, хранения и представления информации	84
2.3.1. Виды взаимодействия в Интернете вещей	85
2.3.2. Мобильные информационные терминалы для сбора и представления данных.....	86
2.3.3. Коммуникационные сети передачи данных	91
2.3.4. Обработка, хранение и представление данных	95
Глава 3. Практическое применение технологий Интернета вещей	102
3.1. Применение технологий электронного мониторинга.....	103
3.1.1. Применение штрих-кодирования	104
3.1.2. Применение радиочастотной идентификации	104
3.1.3. Мониторинг подвижных объектов и его составляющие	106
3.2. Контроль людей и животных.....	113

3.2.1. Мониторинг персонала.....	113
3.2.2. Мониторинг подконтрольных лиц	118
3.2.3. Контроль сотрудников спецподразделений	119
3.2.4. Мониторинг крупного рогатого скота	120
3.3. «Умный» дом.....	120
3.4. «Умный» город	123
3.4.1. Интернет вещей в сфере транспорта.....	127
3.4.2. «Умная» транспортная инфраструктура.....	134
3.4.3. Системы экстренного реагирования	137
3.4.4. Электронный мониторинг пассажирского транспорта.....	138
3.4.5. «Умные» автомобили	139
3.5. Интернет вещей в сфере грузоперевозок, логистики и торговли.....	143
3.5.1. Контроль грузов.....	143
3.5.2. Мониторинг почтовых отправок.....	144
3.5.3. Логистика и розничная торговля.....	147
3.6. Контроль вооружения и военной техники.....	150
3.6.1. Системы мониторинга огнестрельного оружия и снаряжения	151
3.6.2. Системы контроля баллистики в режиме реального времени	156
3.7. Интернет вещей в обеспечении здоровья человека	157
3.7.1. Мониторинг здоровья, диагностика и обеспечение ухода за пациентами.....	158
3.7.2. Поддержание здорового образа жизни	160
3.7.3. Возможности мобильных технологий в медицине	161
3.8. Мониторинг окружающей среды	162
3.8.1. Виды мониторинга окружающей среды	163
3.8.2. Контроль погоды.....	164
3.8.3. Сейсмический мониторинг	169
3.9. Системы безопасности и охранные комплексы	171
3.9.1. Безопасность и охрана жилища	171
3.9.2. Охрана территорий	173
3.9.3. Системы «интеллектуального» видеонаблюдения	173
3.10. Перспективы развития Интернета вещей	177
3.10.1. Развитие рынка Интернета вещей	177
3.10.2. Внедрение единых стандартов.....	180
Заключение.....	182
Используемая литература	183

Список принятых сокращений

EDGE (EGPRS – Enhanced Data rates for GSM Evolution) – цифровая технология беспроводной передачи данных для мобильной связи, которая функционирует как надстройка над 2G- и 2.5G- (GPRS) сетями.

GPRS (General Packet Radio Service – пакетная радиосвязь общего пользования) – надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных. GPRS позволяет пользователю сети сотовой связи производить обмен данными с другими устройствами в сети GSM и с внешними сетями, в том числе Интернет.

GPS (Global Positioning System) – спутниковая система навигации США.

GSM (Global System for Mobile Communications) – глобальный цифровой стандарт мобильной сотовой связи.

IP (Internet Protocol) – межсетевой протокол.

RFID (англ. Radio Frequency IDentification, радиочастотная идентификация) – метод автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках.

UPU (Universal Postal Union) – Всемирный почтовый союз.

VPN (Virtual Private Network – виртуальная частная сеть) – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

Wi-Fi – (Wireless Fidelity – беспроводная точность (передачи данных)) – торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11.

WMS (Warehouse Management System – система управления складом) – система управления, обеспечивающая автоматизацию и оптимизацию всех процессов складской работы профильного предприятия.

ГИС – географическая информационная система.

ГЛОНАСС (ГЛОбальная НАвигационная Спутниковая Система) – российская спутниковая система навигации.

ИС – интегральная схема.

ИТ – информационные технологии.

ЛВС – локальная вычислительная сеть.

МККР – Международный консультативный комитет по радио.

ПАК – программно-аппаратный комплекс.

ПО – программное обеспечение.

ПЗС – прибор с зарядовой связью (от английского CCD – Charge-Coupled Device).

СКУД – системы контроля и управления доступом.

СЭМПЛ – система электронного мониторинга подконтрольных лиц.

ТСД – терминал сбора данных.

ЭП – электронная пломба.

Введение

Информационное общество, существующее сегодня, активно использует информационные технологии если не во всех, то в большинстве сфер частной и общественной жизни. Основой возникновения информационного общества стали различные сети передачи данных, при помощи которых их пользователи могли обмениваться с минимальными издержками в максимально короткий срок. Сегодня самой масштабной из подобных сетей стал Интернет, который во многом определяет уклад жизни для 25% населения Земли, имеющих к нему доступ.

За несколько десятков лет с момента своего возникновения Интернет смог сформировать глобальную информационную среду. Возникло коммуникационное пространство, при помощи которого миллионы людей получили возможность создавать и обрабатывать информацию, а также обмениваться ей.

Тем не менее информационные технологии в целом и Интернет в частности всегда были оторваны от физической реальности. Можно сказать, что человек был и остается посредником, который связывает их с физическим миром. Действительно, современные сети и различные электронные устройства позволяют хранить и обрабатывать информацию. Но всю имеющуюся информацию они получают посредством человека, который самостоятельно создает ее. Такая информация зачастую несет в себе долю субъективности, поскольку ее получение напрямую связано с когнитивными особенностями каждого конкретного человека.

Но на рубеже XX и XXI веков ситуация стала меняться. Развитие технологий привело к возникновению сенсоров, способных воспринимать физический мир без непосредственного участия человека. А развитие технологий передачи данных позволило объединять различные датчики и сети, которые способны самостоятельно фиксировать информацию о реальности.

Совокупность устройств, способных фиксировать информацию о реальном мире и обрабатывать ее без непосредственного участия человека, получила название Интернета вещей. Говоря формальным языком, Интернет вещей (от англ. Internet of Things) – это концепция вычислительной сети физических объектов, оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой. Такая вычислительная сеть обладает специальными сенсорами для захвата данных об окружающем мире, средствами идентификации и передачи данных, а также различными средствами обработки полученной информации.

Сенсоры, датчики, а также узлы обработки и передачи информации, входящие в состав вычислительной сети, принято называть подключенными вещами (Connected Things). Подключенным устройством может быть как смартфон с доступом к Интернету, так и пожарный датчик, который способен оповестить диспетчера о задымлении. Подключенные вещи объединяет одно: они способны фиксировать объекты и

события реального мира, а затем передавать информацию внутри какой-либо сети или самостоятельно обрабатывать ее.

Интернет вещей – относительно новая технологическая концепция, которая активно изучается современной наукой и практиками из сферы бизнеса. Если посмотреть на количественную сторону вопроса, то «Интернет людей» уже превратился в «Интернет вещей». Сегодня Интернетом пользуется порядка 1,7 млрд жителей Земли, на которых приходится 35 млрд устройств. Однако количественная разница не может считаться определяющей. Важнейшей чертой Интернета вещей является не число подключенных устройств, а их способность самостоятельно или при минимальном участии человека идентифицировать реальный мир и собирать информацию о нем.

К технологиям Интернета вещей сегодня относится множество «умных» технологий самого разного направления. Однако многие приборы и устройства, без которых невозможно возникновение полноценного автономного Интернета вещей, по-прежнему не изобретены. Интернет вещей во многом остается технологической концепцией будущего. Вероятнее всего, недалекого, но оценить полномасштабное развертывание данных технологий в настоящее время все еще невозможно.

Тем не менее присутствие Интернета вещей в нашей жизни можно ощутить уже сейчас. Отдельные технологии Интернета вещей, начиная RFID-метками и заканчивая пилотными проектами «умной» инфраструктуры, существуют и активно развиваются.

Данное исследование нацелено на всесторонний анализ концепции Интернета вещей. Структура содержит в себе следующие главы:

первая глава посвящена детальному рассмотрению Интернета вещей как концепции, явления и совокупности технологий;

вторая глава рассматривает отдельные информационные технологии, относящиеся к сфере Интернета вещей;

в третьей главе приводится практическое применение технологий Интернета вещей.

Глава 1. Концепция Интернета вещей

1.1. Развитие концепции

Прежде чем говорить о техническом и концептуальном развитии Интернета вещей, необходимо обратить внимание на используемую терминологию. С технической точки зрения Интернет вещей – это объединяющий термин для совокупности технологий, которые обеспечивают захват разного рода данных из внешней среды и их дальнейшую обработку при минимальном участии человека. Использование непосредственно Интернета при этом не играет принципиальной роли. В широком понимании слово «Интернет» в контексте исследуемой концепции означает не только Интернет как таковой, но и любые другие средства передачи собранных данных об окружающем мире.

Сегодня все объекты, относящиеся к Интернету вещей, принято называть общим термином «подключенные вещи» (Connected Things). Однако на практике имеет смысл ввести дополнительное разделение объектов на «подключенные устройства» и «подключенные вещи». Под подключенным устройством будет пониматься узел в составе технологий Интернета вещей, способный самостоятельно воспринимать окружающую действительность. А термином «подключенная вещь» будет обозначаться объект, имеющий уникальную идентификацию в информационном пространстве, но не обладающий способностью захватывать данные из внешней среды. В случае, когда речь идет сразу об обеих группах, допустимо использование общей категории «подключенный объект».

Отдельно стоит добавить, что не все технологии, которые сегодня могут быть отнесены к сфере Интернета вещей, изначально задумывались как ее компоненты. Так, различные датчики разрабатывались не как подключенные устройства в составе Интернета вещей, а как самостоятельные технологические решения. Однако дальнейшее развитие технологий связи и идентификации позволило отнести некоторые из них к технологиям Интернета вещей. Иными словами, все технологии, о которых пойдет речь далее, можно условно разделить на две группы: созданные непосредственно для сферы Интернета вещей (например, «умная» дверь) и созданные для иных областей применения. Их объединяет тот факт, что и те, и другие сегодня имеют непосредственное отношение к исследуемой концепции.

Таким образом, в рамках обозначенной терминологии исторически первой технологией Интернета вещей является радиочастотная идентификация (RFID). Технологические решения, использующие радиочастотную идентификацию, зачастую могут функционировать и без использования Интернета. Тем не менее RFID вписывается в общее определение Интернета вещей, поскольку позволяет получить объективные данные об окружающем мире без непосредственного участия человека в случае, если сама идентификация дополняется различными информационными технологиями.

1.1.1. Радиочастотная идентификация (RFID) как предпосылка к возникновению концепции Интернета вещей

Самая отдаленная отсылка к возникновению радиочастотной идентификации относится к 1926 году. Тогда Никола Тесла в интервью для журнала *Collier's* сказал, что в будущем радио превратится в «большой мозг», вещи станут частью единого целого, а инструменты, благодаря которым это станет возможно, будут легко помещаться в кармане¹. Впрочем, сегодня данное высказывание имеет только культурно-историческую ценность, как пример футурологии прошлого.

В 1945 году Лев Сергеевич Термен (рис. 1) изобрел для Советского Союза устройство, которое позволило накладывать аудиоинформацию на случайные радиоволны.

Звук вызывал колебание диффузора, которое незначительно изменяло форму резонатора, модулируя отраженную радиочастотную волну. И хотя устройство представляло лишь пассивный передатчик, это изобретение причисляют к первым предшественникам RFID-технологии.

Технология, наиболее близкая к данной, – система распознавания «свой-чужой» IFF (Identification Friend or Foe), изобретенная Исследовательской лабораторией ВМС США в 1937 году. Она активно применялась союзниками во время Второй мировой войны, чтобы определить, своим или чужим является объект в небе. Подобные системы до сих пор используются как в военной, так и в гражданской авиации.

Еще одной вехой в использовании RFID-технологии является работа Гарри Стокмана (Harry Stockman) под названием «Коммуникации посредством отраженного сигнала» (англ. “Communication by Means of Reflected Power”). Стокман отмечает, что «...значительные работы по исследованию и разработке были сделаны до того, как были решены основные проблемы в связи посредством отраженного сигнала, а также до того, как были найдены области применения данной технологии».



Рис. 1. Лев Сергеевич Термен

¹ Интернет вещей – а что это? // НАБРАНАБР.RU : Информационный портал. 2012. URL: <http://habrahabr.ru/post/149593/> (дата обращения 25.02.2014).



Рис. 2. Чарльз Уолтон

Первая демонстрация современных RFID-чипов, как пассивных, так и активных, была проведена в Исследовательской лаборатории Лос-Аламоса (англ. Los Alamos Scientific Laboratory) в 1973 году. Портативная система работала на частоте 915 МГц и использовала 12-битные метки.

Первый патент, связанный собственно с названием RFID, был выдан Чарльзу Уолтону (Charles Walton) (рис. 2) в 1983 году.

1.1.2. Возникновение понятия «Интернет вещей»

Термин «Интернет вещей» был введен в употребление Кевином Эштоном в 1999 году на презентации RFID-меток для Procter&Gamble. Основатель исследовательского центра Auto-ID Кевин Эштон справедливо предполагал, что внедрение радиочастотной идентификации поможет облегчить работу логистических подразделений этой компании. Каждая метка хранит достаточно большой уникальный код, содержащий информацию о физическом объекте. Таким образом, RFID-чипы позволяют интегрировать данные об объектах внешней среды в информационное пространство.

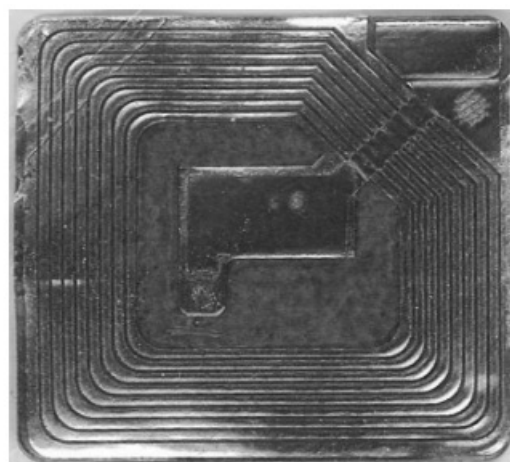
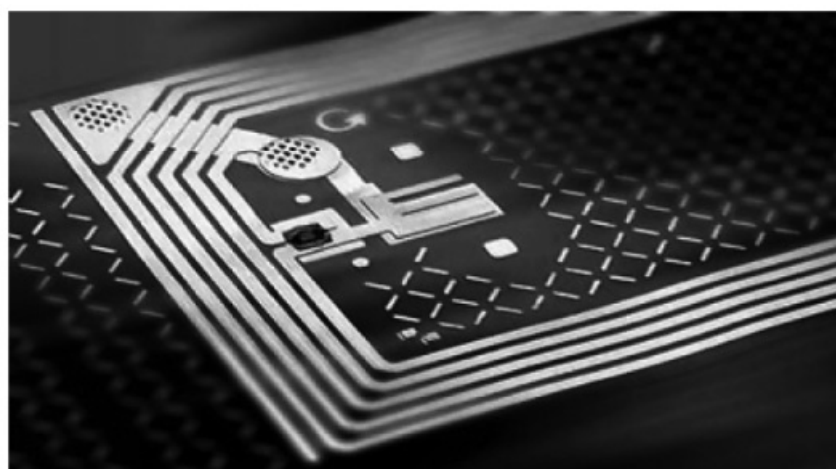


Рис. 3. Современные RFID-метки

Первое подключенное устройство (в сегодняшней терминологии) было создано еще до возникновения понятия «Интернет вещей». Им стал обыкновенный тостер, который выпускник МИТ Джон Ромки (один из «отцов» протокола TCP/IP) подключил к Интернету².

Примерно в то же время, в 1996 году, Марк Вейзер утверждал, что вычислительные мощности становятся более доступными, в результате чего уменьшается степень их наблюдаемости. Наиболее совершенными Марк Вейзер называет технологии, которые люди перестают замечать. Мобильные телефоны, терминалы и т.п. так сливаются с обыденной жизнью, что становятся ее неотъемлемыми частями. Далее эта идея развивалась в форме концепции «исчезающего (проникающего) компьютеринга» Норберта Стрейтца³.

Переломным моментом для концепции Интернета вещей стали 2008–2009 годы. В это время произошел переход от «Интернета людей» к «Интернету вещей». Изначально число людей, пользующихся Всемирной Сетью, было больше числа подключенных к ней устройств. Но в 2008–2009 годах эта ситуация изменилась. Консалтинговый отдел Cisco IBSG утверждает, что именно в это время Интернет вещей трансформировался из понятия в явление, поскольку число подключенных к Интернету устройств превысило число жителей Земли⁴.

Футуролог компании Cisco приводит интересную статистику соотношения пользователей Интернета и подключенных к нему устройств⁵. В 2003 году на планете было 6,3 млрд людей и 500 млн подключенных к Сети устройств (в среднем 0,08 устройства на жителя Земли). При таком распространении подключенных устройств Интернета вещей еще не существовало. Однако к 2010 году за счет распространения смартфонов и планшетов количество устройств выросло до 12,5 млрд, тогда как население Земли составило 6,8 млрд. В среднем на человека приходится 1,84 единицы устройства, но если брать только пользователей Интернета, то получается 6,25 единицы на человека. Планируется, что как минимум к 2015 году динамика сохранится.

В том же 2008 году вышел в свет отчет Национального разведывательного совета США, где Интернет вещей фигурировал в качестве одной из шести потенциально разрушительных технологий. Данная технология, по мнению американских аналитиков, несет прямую угрозу национальной информационной безопасности.

² Интернет вещей – а что это? // НАБРАНАБР.RU : Информационный портал. 2012. URL: <http://habrahabr.ru/post/149593/> (дата обращения 25.02.2014).

³ Чеклецов В.В. Чувство планеты: Интернет вещей и следующая технологическая революция. – М.: Российский исследовательский центр по Интернету вещей, 2013. – С. 14.

⁴ Про автомобили, голландских коров и уникальные свойства Интернета вещей // CISCO.COM: Новости. 2011. URL: <http://www.cisco.com/web/RU/news/releases/txt/2011/070711d.html> (дата обращения 25.02.2014).

⁵ Эванс Д. Интернет вещей: как изменится вся наша жизнь на очередном этапе развития Сети // CISCO.COM : Новости. 2012. URL: <http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html> (дата обращения 25.02.2014).

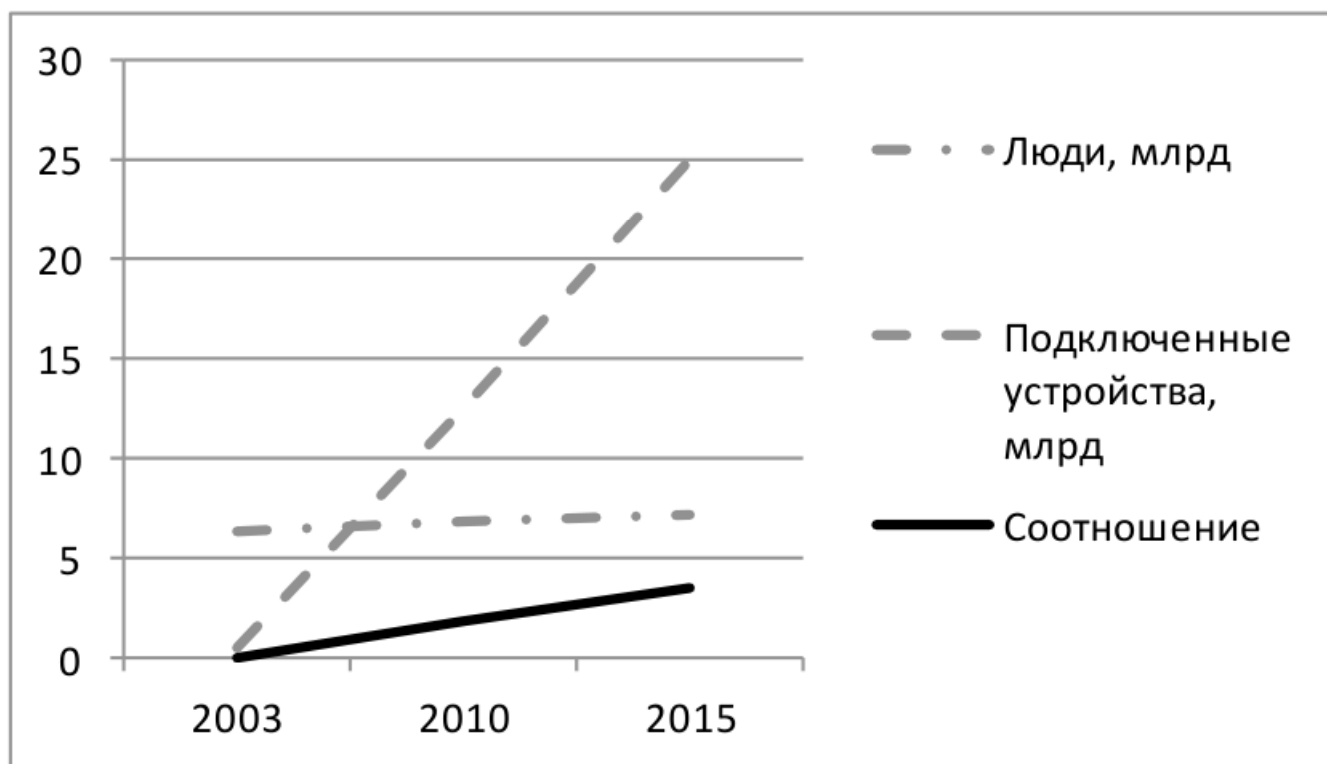


Рис. 4. Динамика числа жителей Земли и числа подключенных устройств

1.2. Определение понятия

Интернет вещей может пониматься как совокупность технологий, как концепция и как явление. Различное понимание обуславливает существование множества различных определений, каждое из которых делает акценты на соответствующих особенностях понятия.

Таблица 1

Определение понятия «Интернет вещей»

Интернет вещей – это...	Совокупность технологий	Концепция	Вектор технологического развития
Акценты	Составные технологии, относящиеся к сфере Интернета вещей	Интернет вещей как средство совмещения физического и информационного миров	Потенциальные возможности технологий Интернета вещей

Определение Интернета вещей как совокупности различных технологий приведено во введении. Интернет вещей – это концепция вычислительной сети физических объектов, оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой. Таким образом, Интернет вещей может быть представлен как совокупность технологий сбора информации об окружающем мире, технологий идентификации, технологий передачи данных, технологий хранения и обработки информации.

Интернет вещей в его техническом понимании должен удовлетворять целому ряду фундаментальных признаков, основные из которых выделены А.Е. Кучерявым⁶. К ним относятся:

1. *Связность*. Связность считается основной метрикой для самоорганизующихся сетей. Более того, в случае с Интернетом вещей связность влияет на длительность жизненного цикла его составных подсетей. Связность определяется как возможность любой вещи в составе сети быть связанной с глобальной коммуникационной инфраструктурой, а предпосылкой для связности выступает идентификация каждого подключенного устройства и каждой подключенной вещи.
2. *Гетерогенность*. Данный признак подразумевает, что устройства, подключенные к общей сети, могут быть произведены на различных программных и аппаратных платформах. Устройства Интернета вещей должны иметь возможность взаимодействовать друг с другом не только внутри экосистемы отдельно взятого производителя, но и в больших масштабах. Проблема фрагментированности современных сетей Интернета вещей рассмотрена далее.
3. *Динамичность*. Интернет вещей – самоорганизующаяся сеть, число узлов которой в любой момент времени является случайной величиной от 0 до N_{\max} . Все взаимосвязи внутри сети случайны во времени и создаются для достижения сетью какой-либо цели, включая просто передачу информации. Самоорганизующиеся сети состоят из сетей доступа (Ad Hoc, целевая сеть) и транзитной сети (mesh, ячеистая сеть). Целевые узлы не имеют маршрутизации и взаимодействуют только с ближайшими узлами, поэтому их часто называют дочерними. Однако у них нет строгой привязки к родительскому узлу, и при необходимости они сами могут выступать в роли родительских узлов. В свою очередь, ячеистые узлы обладают функцией маршрутизации и поддерживают соединение не только с ближайшими узлами.
4. *Множество подключенных объектов*. Интернет вещей в его классическом понимании подразумевает сеть с большим числом сенсоров, передатчиков, маршрутизаторов и иных объектов.

К определениям второй группы можно отнести дефиницию, предложенную CASAGRAS (Организация по координации и поддержке действий для мировой стандартизации в сфере RFID-идентификации)⁷.

Определение звучит следующим образом: **Интернет вещей** – глобальная сетевая инфраструктура, соединяющая физические и виртуальные объекты посредством использования захвата данных и коммуникационных возможностей.

⁶ Кучерявый А.Е. Интернет вещей : [Электронный документ] // ELSV.RU : Журнал «Электросвязь». Систем. требования: Adobe Reader. URL: <http://www.elsv.ru/files/actual/323.pdf> (дата обращения 25.02.2014).

⁷ RFID and the Inclusive Model for the Internet of Things: [Электронный документ] // GRIFS-PROJECT.EU : Информационный портал. Систем. требования: Adobe Reader. URL: <http://www.grifs-project.eu/data/File/CASAGRAS%20FinalReport%20%282%29.pdf> (дата обращения 25.02.2014).

Немецкая корпорация SAP AG приводит похожее определение. **Интернет вещей** – мир, где физические объекты плавно интегрированы в информационную среду и где физические объекты могут принимать участие в бизнес-процессах. Сервисам позволено взаимодействовать с умными объектами посредством интернета, делать запросы и изменять их состояние или информационные связи между ними с учетом безопасности и защиты личных данных⁸.

Для удобства в дальнейшем термин «технологии Интернета вещей» будет употребляться, когда речь идет о техническом понимании исследуемого понятия или технологий, относящихся к сфере Интернета вещей. А термин «концепция Интернета вещей» будет использоваться, когда Интернет вещей рассматривается как концепция в общем виде, без необходимости подробно останавливаться на ее составных частях.

К третьей группе можно отнести определения, которые на сегодняшний день остаются футурологическими. В них делается упор на потенциальные возможности Интернета вещей как в концептуальном, так и в техническом плане. Сюда относится определение Роба Ван Краненбурга, руководителя проекта развития Интернета вещей в рамках программы Европейского союза. Он считает, что Интернет вещей – концепция пространства, в котором аналоговый и цифровой миры могут быть совмещены. Это предопределяет наши отношения с объектами, а также свойства и суть самих объектов⁹. Таким образом, Интернет вещей в рамках данной дефиниции перестает быть множеством различных сенсоров и датчиков, объединенных между собой проводными и беспроводными каналами связи. Интернет вещей не является простой суммой технических устройств, которые входят в его состав. Исследователь отдельно отмечает, что теоретически «Интернет вещей позволяет абсолютно всем предметам коммуницировать друг с другом»¹⁰.

Представитель Cisco Дэйв Эванс акцентирует внимание на коммуникации Интернета вещей с окружающей средой. «Это новый этап развития Интернета, значительно расширяющий возможности сбора, анализа и распределения данных, которые человек может превратить в информацию, знания и, в конечном счете, мудрость», – считает исследователь¹¹.

Автор концепции Интернета вещей Кевин Эштон отмечает необходимость создания автономных устройств, которые могут получать данные из окружающего мира независимо от вмешательства человека.

⁸ Haller S. Internet of Things : An Integral Part of the Future Internet : [Электронный документ] // FUTURE-INTERNET.EU : European Future Internet Portal. 2009. Систем. требования: Adobe Reader. URL: http://services.future-internet.eu/images/1/16/A4_Things_Haller.pdf (дата обращения 25.02.2014).

⁹ Интернет вещей – а что это? // НАБРАНАБ.RU : Информационный портал. 2012. URL: <http://habrahabr.ru/post/149593/> (дата обращения 25.02.2014).

¹⁰ Internet of Things Роба Ван Краненбурга. Лекция в рамках Futurodesignlab // DESIGN-UNION.RU : Союз дизайнеров России. 2011. URL: <http://design-union.ru/authors/theory/1490-internet-of-things-futurodesignlab> (дата обращения 25.02.2014).

¹¹ Эванс Д. Интернет вещей: как изменится вся наша жизнь на очередном этапе развития Сети // CISCO.COM : Новости. URL: <http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html> (дата обращения 25.02.2014).

«Сегодня компьютеры – и, следовательно, Интернет – почти целиком зависят от человека в информации. Почти все из 50 петабайт данных, имеющихся в Интернете, были первоначально созданы людьми, – считает исследователь. – Если бы мы имели компьютеры, которые знают все о вещах, – используя данные, полученные без нашей помощи, – мы смогли бы проследить и просчитать все и значительно сократить пустые траты и потери».

Отдельного внимания заслуживает отличие Интернета вещей от традиционного Интернета. Согласно исследованию компании J'son & Partners Consulting¹², наиболее важные отличия можно сформулировать следующим образом:

- фокус на машинах, а не на человеке;
- существенное увеличение числа «подключенных устройств» и «подключенных вещей»;
- уменьшение размеров «подключенных устройств» и рост скорости передачи данных;
- фокус на получении информации и ее обработке, а не на коммуникации;
- возникновение новых стандартов и новой инфраструктуры.

1.3. Получение информации об окружающем мире

Интернет вещей как концепция и один из векторов развития современных информационных технологий имеет широкие перспективы. В определенном смысле, Интернет вещей – это одна из концепций получения информации об окружающем мире и ее дальнейшего использования. До ее возникновения существовали и другие концепции, каждая из которых имела свои отличительные особенности.

Одной из первых концепций получения информации об окружающем мире и ее дальнейшего использования была так называемая «галактика Гутенберга», сформировавшаяся вместе с изобретением книгопечатания. Информация об окружающем мире собиралась людьми и вручную фиксировалась в книгах или на аналогичных информационных носителях. Очевидно, что такая информация была статичной, недостаточной и ограниченной. О получении данных в реальном времени не было и речи: отсутствовали средства захвата информации, удобные информационные носители, быстрые и доступные средства передачи информации.

Технологии массовой коммуникации, получившие широкое распространение в XX веке, не внесли качественных изменений в «галактику Гутенберга». Общество всего лишь получило средства для обмена

¹² Интернет вещей и межмашинные коммуникации: современные технологии, тренды, дорожные карты. Обзор ситуации в России и в мире // APPS4ALL.RU : Разработчики и приложения для мобильных устройств. 2013. URL: <http://apps4all.ru/post/12-23-13-json-partners-consulting-predstavlyaet-issledovanie-quotinternet-veschej-i-mezhmashinnye-kommunikatsii-sovremennye-tehnologii-trendy-dorozhnye-karty-obzor-situatsii-v-rossii-i-mirequot> (дата обращения 25.02.2014).

информацией, которые могли использоваться только в вертикальной коммуникации сверху вниз – от одного отправителя к множеству реципиентов.

Концепция получения информации об окружающем мире стала качественно меняться только с изобретением Интернета. В 2001 году вышла книга «Галактика Интернет» за авторством Мануэля Кастельса, одного из выдающихся социологов современности из Университета Беркли. В книге констатировались фундаментальные изменения в современном обществе, вызванные Интернетом. Средства автоматизированного захвата данных из внешней среды по-прежнему отсутствовали, но информация перестала быть привязанной к своим физическим носителям и стала общедоступной. Возникли средства хранения и обработки больших объемов информации, а также быстрые и доступные каналы ее передачи. Это привело к дальнейшему развитию такого понятия, как «информационное общество». Информация об окружающем мире по-прежнему собиралась и фиксировалась непосредственно людьми, но на этом этапе стало проще ее обрабатывать, хранить и обмениваться ею.

Важно понимать, что возникновение и развитие информационного общества связано с двумя уровнями понимания Интернета. Условно Интернет включает в себя два уровня: физический и уровень веб-приложений. Физический уровень Интернета заложил фундамент для развития разнообразных веб-приложений, которые удовлетворяли индивидуальные информационные потребности большого числа людей. В некотором смысле, веб – это уровень приложений, работающих поверх Интернета в его физическом смысле. Его главной задачей было сделать так, чтобы люди могли получить какую-то практическую пользу от существования Всемирной Сети. Сюда относятся браузеры, социальные сети и прочие программные разработки. А история уровня веб-приложений включает в себя несколько этапов качественного развития, которые сегодня принято подразделять на Web 1.0 и Web 2.0.

Тем не менее Интернет в его физическом смысле с самого момента своего возникновения практически не изменялся качественно. Физический уровень Интернета представляет собой цепочку «маршрутизаторы – коммутаторы – оборудование». Цепочка долгое время оставалась практически неизменной, менялась лишь ее надстройка, представленная в форме веб-приложений. Технически сейчас Интернет работает как во времена протокола ARPANET, с той лишь разницей, что из протоколов сохранился только IP и стал общепризнанным (протоколы AppleTalk и Token Ring исчезли).

Между тем концепция Интернета вещей обещает стать первым качественным изменением физического уровня Интернета¹³. Качественное изменение такого масштаба обещает вызвать к жизни приложения, которые изменят человеческую жизнь. Уже сегодня существуют датчики температуры, вибрации, давления, освещения, влажности, физических

¹³ Эванс Д. Интернет вещей: как изменится вся наша жизнь на очередном этапе развития Сети // CISCO.COM : Новости. URL: <http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html> (дата обращения 25.02.2014).

нагрузок и пр. Если идентифицировать их в Сети и снабдить устройствами передачи данных, то они станут базовым уровнем архитектуры Интернета вещей. В дальнейшем, с появлением все более широких сенсорных сетей и «социальных вещей», многие экономические, бизнес- и политические процессы могут серьезно измениться, как когда-то изменились с развитием Интернета и веба.

Более того, качественные изменения произойдут и в концепции получения информации о внешней среде. Как на этапе «галактики Гутенберга», так и на этапе «галактики Интернета» человек самостоятельно собирал информацию об окружающем мире и фиксировал ее. Можно сказать, что человек был посредником между внешней средой и техникой, поскольку машины не могли собирать информацию самостоятельно. Упрощенно говоря, техника не знала ничего об окружающем мире – все ее знания были получены «со слов» людей.

Стоит подчеркнуть, что ни во времена «галактики Гутенберга», ни во времена «галактики Интернета» человек не имел возможности работать с данными, получаемыми в реальном времени. Когнитивные способности человека ограничены, и он физически не способен фиксировать большинство параметров реального мира для дальнейшей обработки с учетом их постоянных изменений. Поэтому, в некотором смысле, человек никогда не работал с информацией о настоящем времени – ему была доступна только информация о прошлом, пусть и об очень недавнем.

Таблица 2

Концепции получения информации об окружающем мире

Концепция	Получение информации	Обработка информации	Временная переменная
«Галактика Гутенберга»	Ручное	Ручная	Прошлое
«Галактика Интернет»	Ручное	Автоматическая	Прошлое
Интернет вещей	Автоматическое	Автоматическая	Настоящее

Таким образом, концепция Интернета вещей может интерпретироваться как новая концепция получения информации об окружающем мире с целью дальнейшего хранения, обработки и обмена.

Автор концепции Интернета вещей Кевин Эштон в 2009 году отдельно подчеркивал масштабы данного понятия. «Интернет вещей – это не «штрих-код на стероидах» и не способ сделать платные дороги более быстрыми. Мы не должны позволять нашему взгляду сузиться до такого масштаба. Интернет вещей обладает потенциалом изменить мир, так же

как ранее это сделал Интернет. А возможно, даже сильнее», – утверждает ученый¹⁴.

Возможность получения информации об окружающем мире в реальном времени постепенно изменит соотношение так называемых «реального» и «виртуального» миров. Изначально, когда монитор оставался единственным интерфейсом для взаимодействия «человек – компьютер», эти миры имели минимальное соприкосновение. Границы стали размываться с появлением ноутбуков, мобильных телефонов и планшетов, однако различия между двумя мирами до сих пор остаются более чем существенными¹⁵.

Концепция Интернета вещей на определенной точке своего развития создаст «гибридный», реально-виртуальный мир. В гибридном мире объекты реальности имеют свою идентификацию (или хотя бы отражение) в виртуальности, а объекты виртуальности накладывают свой отпечаток на реальность. Современные технологии геопозиционирования позволяют совместить и сопоставить события в реальном мире с виртуальной географией, а компьютерные технологии делают возможным вынесение виртуальных событий или объектов в реальность. Виртуальные пространства дополняют физический мир, причем пользователи активно участвуют в этом. В дальнейшем подобные технологии будут принимать все более широкий масштаб.

Одним из следствий становится концепция так называемой «дополненной реальности». Дополненная реальность существует уже сейчас. Примером может служить участие людей в сити-квестах и онлайн-новых играх на местности при помощи смартфонов. Так, в феврале 2014 года игра Ingress насчитывала более 1 млн игроков по всему миру, которые кооперировались и «захватывали» различные участки городов при помощи мобильных телефонов. В том же месяце тысячи игроков, которых разделяли сотни километров, смогли скоординироваться и «захватить» всю Норвегию на пару часов¹⁶.

1.4. Общая характеристика

В наиболее общем виде соотношение Интернета с техническим и прикладным проявлениями Интернета вещей можно представить в следующем виде.

¹⁴ Ashton K. That “Internet of Things” Thing // RFIDJOURNAL.COM : Technology News & Features. 2009. URL: <http://www.rfidjournal.com/articles/view?4986> (дата обращения 25.02.2014).

¹⁵ Чеклецов В.В. Чувство планеты: Интернет вещей и следующая технологическая революция. – М.: Российский исследовательский центр по Интернету вещей, 2013.

¹⁶ Норвегия стала первой страной, «захваченной» в популярной компьютерной игре Ingress // NORGE.RU : Новости из Норвегии. 2014. URL: <http://www.norge.ru/news/2014/02/09/23949.html> (дата обращения 25.02.2014).

**Соотношение Интернета с техническими
и прикладными проявлениями Интернета вещей**

	Совокупность технологий	Физический уровень	Уровень приложений
1-й этап	Интернет	Маршрутизаторы, коммутаторы, оборудование	Web-технологии (браузеры, сайты, социальные сети и т.п.)
2-й этап	Интернет вещей	«Подключенные вещи», «подключенные устройства», средства связи между ними, узлы хранения и обработки информации	«Умный дом», «умный город», «умные сети» и т.п.

Как уже говорилось ранее, сегодня человек чаще всего использует статичную информацию, поскольку возможности для сбора, анализа и интерпретации больших объемов данных в реальном времени отсутствуют. Технологии Интернета вещей, к которым относятся различные сенсоры, позволяют обществу, и в первую очередь экономике, работать с данными в реальном времени. Это уменьшит издержки экономики, позволит избежать множества техногенных катастроф и сделает общество гораздо более справедливым (например, за счет точного расчета налогов, тарифов ЖКХ и т.п.).

Фундаментальный уровень в исследованиях является достаточно хорошо проработанным, однако фрагментированное состояние существующих сетей Интернета вещей предполагает ряд условностей и допущений. Основными теоретиками можно считать Роба Ван Краненбурга, Кевина Эштона и Дэйва Эванса.

Огромное значение для исследования концепции Интернета вещей имеет статья Кевина Эштона “That “Internet of Things” Thing”¹⁷, опубликованная им в 2009 году. Кевин справедливо полагает, что в реальном времени вещи и явления гораздо важнее идей и информации. Тем не менее существующие сегодня информационные технологии получают входящие данные от людей, а не берут их самостоятельно из окружающего мира. Таким образом, можно утверждать, что наши компьютеры знают гораздо больше об идеях, нежели о вещах. И технологии Интернета вещей способны внести баланс в эту ситуацию.

¹⁷ Ashton K. That “Internet of Things” Thing // RFIDJOURNAL.COM : Technology News & Features. 2009. URL: <http://www.rfidjournal.com/articles/view?4986> (дата обращения 25.02.2014).

Кевин Эштон считает, что задача исследователей – улучшать компьютеры с той целью, чтобы они могли самостоятельно собирать информацию об окружающем мире. RFID-технологии, различные датчики, средства захвата данных и идентификации физических объектов научили компьютеры наблюдать, идентифицировать и понимать мир без ограничения на человеческое участие. Эти технологии нуждаются в дальнейшем развитии, однако уже сейчас концепция Интернета вещей обладает потенциалом, чтобы изменить все наше общество.

Другие исследователи согласны с тем, что концепция Интернета вещей вызовет далеко идущие последствия в масштабах всего общества. «Предметы смогут общаться друг с другом, управлять друг другом, передавать и принимать информацию. Последствия всего этого обещают быть огромными», – считает Роб Ван Краненбург¹⁸. Теоретик Интернета вещей трактует происходящие события как начало онтологического сдвига, который изменит саму суть вещей и их взаимоотношений.

Роб Ван Краненбург предложил довольно интересное видение архитектуры этого понятия. Исследователь интерпретирует концепцию Интернета вещей как «четырёхслойный пирог», уровни архитектуры которого можно сформулировать следующим образом:

Идентификация каждого объекта («умное устройство»). Так, компания Heineken ставит активные сенсоры на свою продукцию, что позволяет в реальном времени отслеживать передвижение каждого ящика пива. А в апреле 2013 года компания предложила концепцию «умных бутылок», которые могут взаимодействовать друг с другом¹⁹.

Сеть вещей, которые обслуживают потребности одного человека или небольшой группы лиц («умный дом»). Так, сегодня существует организация AllSeen Alliance во главе с Qualcomm, нацеленная на продвижение данной концепции на рынке.

Применение технологий в условиях городской жизни («умный город»). Одним из примеров может считаться проект Cisco по внедрению «умной» транспортной системы. Кроме того, российский теоретик Интернета вещей В.В. Чеклецов полагает, что в результате соединения проникающего компьютеринга, «зеленых» технологий, синтетической биологии и нанотехнологий может быть создан новый тип техноценозов.

Применение технологий на уровне всей планеты («сенсорная планета»). Существуют масштабные проекты с участием Cisco, HP, IBM и других крупных компаний.

¹⁸ Тэббитт С. Интернет вещей начинает жить собственной жизнью // CISCO.COM : Новости. URL: <http://www.cisco.com/web/RU/news/releases/txt/2012/112612b.html> (дата обращения 25.02.2014).

¹⁹ Heineken creates interactive bottle that responds to drinkers // IOTEVENT.EU : Internet of Things Event. 2013. URL: <http://iotevent.eu/heineken-creates-interactive-bottle-that-responds-to-drinkers/> (дата обращения 25.02.2014).

На основании приведенной выше архитектуры выделяются различные типы технических сетей, окружающих человека²⁰:

1) BAN (Body Area Network) – сети и приборы, действие которых направлено непосредственно на человека.

LAN (Local Area Network) – сети и приборы, расположенные на отдельно взятой небольшой местности.

WAN (Wide Area Network) – сети городского масштаба.

VWAN (Very Wide Area Network) – сети планетарного масштаба.

На сегодняшний день развертывание технологий Интернета вещей создает множество не связанных друг с другом сетей. Ситуация аналогична той, которая наблюдалась на заре становления Интернета. Вероятнее всего, в дальнейшем будет разработан единый протокол для всех «подключенных вещей» и «подключенных устройств».

На сегодняшний день существует ряд проблем, которые тормозят внедрение технологий Интернета вещей в социально-экономические процессы. Среди них можно выделить такие проблемы, как:

- Отсутствие стандартов на рынке. Существующие решения не поддаются интеграции, поскольку каждая крупная фирма стремится создать собственную среду. В результате возникает множество не связанных друг с другом сетей, причем предметы привязаны к своей сети и не могут использоваться в другой.
- Отсутствие необходимой автономности подключенных устройств. Сенсоры должны научиться получать энергию из окружающей среды. Кевин Эштон делал отдельный акцент на этой проблеме: *«Нам нужно улучшить компьютеры в том смысле, чтобы они смогли сами собирать информацию. Они должны научиться видеть, слышать и чувствовать мир для самих себя, и всю его случайную красоту»*. Данное направление подразумевает автономность устройств от человека²¹.
- Переход к стандарту IPv6. Свободные адреса IPv4 закончились 6 февраля 2010 года, отмечают представители Cisco²².

Интересной иллюстрацией к перспективам развития технологий Интернета вещей может послужить исследование компании J'son & Partners Consulting. Аналитики сформулировали сравнительную таблицу с драйверами и барьерами в развитии.

²⁰ Роб ванн Краненбург: Что такое IoT? // INTERNETOFTHINGS.RU : Российский исследовательский и консалтинговый центр. 2013. URL: <http://internetofthings.ru/78-blog/21-rob-van-kranenburg-chto-takoe-iot> (дата обращения 25.02.2014).

²¹ Ashton K. That 'Internet of Things' Thing // RFIDJOURNAL.COM : Technology News & Features. 2009. URL: <http://www.rfidjournal.com/articles/view?4986> (дата обращения 25.02.2014).

²² Эванс Д. Интернет вещей: как изменится вся наша жизнь на очередном этапе развития Сети // CISCO.COM : Новости. 2012. URL: <http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html> (дата обращения 25.02.2014).

Драйверы и барьеры в развитии технологий Интернета вещей

Драйверы	Барьеры
Быстрое развитие ИКТ-технологий	Отсутствие общих стандартов
Популярность смартфонов, планшетов и т.п.	Медленный переход к протоколу IPv6
Потребности логистики и управления поставками	Риск закрытости частных сетей
Потребности в повышении безопасности и удобства транспорта	Несовместимость ряда компонентов
Потребность в сохранении экологии и снижении затрат	Проблема защиты персональных данных и безопасности
Поддержка государств и действия инноваторов	Относительно высокая стоимость внедрения

С развитием технологий Интернета вещей связывается и развитие «туманных вычислений» (Fog Computing). Термин введен Cisco по аналогии с облачными вычислениями, но максимально приближенными к земле. «Туманные вычисления» производятся географически распределенными устройствами, которые собирают данные из окружающей среды в реальном времени и передают их в центры обработки и хранения данных.

Подключенные устройства являются составными частями Интернета вещей. Отдельный интерес представляет вопрос «Что считать подключенным устройством?». Для того чтобы объект можно было назвать таковым, он должен удовлетворять следующим требованиям²³:

- объект должен обладать уникальной идентификацией;
- объект должен быть способен воспринимать действительность;
- объект должен обладать функцией памяти;
- объект должен иметь возможность обрабатывать информацию;
- объект должен обладать свойством коммуникативности, т.е. иметь возможность связи с другими устройствами.

²³ Чеклецов В.В. Чувство планеты: Интернет вещей и следующая технологическая революция. – М.: Российский исследовательский центр по Интернету вещей, 2013. – С. 22.

«Подключенная вещь» должна удовлетворять критериям наличия личного уникального адреса, обладать функцией памяти и свойством коммуникативности.

Концепция Интернета вещей основана сразу на нескольких типах коммуникационного взаимодействия: M2M (Machine to Machine), M2E (Machine 2 Environment) и M2C (Machine 2 Consumer). На сегодняшний день наибольшее развитие получил первый тип коммуникации, к которому относится коммуникация V2V (Vehicle to Vehicle). К сфере автотранспорта также относится взаимодействие V2I (Vehicle 2 Infrastructure), продемонстрированное на Cisco Live-2013. Все перечисленные типы коммуникаций являют собой практические проявления концепции Интернета вещей. Стоит отметить, что наибольшее развитие получила сегодня M2M-коммуникация в сфере логистики и доставки грузов, основанная на использовании RFID-меток.

Коммуникация M2E существует на практике довольно давно, однако ее развитие обычно ограничивается либо отдельными приборами, либо вторым уровнем архитектуры Роба Ван Краненбурга (локальное пространство). Сюда относятся, прежде всего, «умные» датчики и технические средства, при помощи которых возможен автоматический мониторинг состояния окружающего мира. Китайские ученые предполагают, что в течение 30 лет технически возможно покрыть ключевые точки земного шара специальными сенсорами для мониторинга погоды и возможных катаклизмов.

Коммуникация по типу M2C на сегодняшний день практически не развита. До сих пор нет способов монетизации Интернета вещей. Исключение составляет так называемая «монетизация первого порядка» за счет продажи сенсоров и т.п. Крупные компании вроде Google сейчас акцентируют свое внимание на развитии технологий, с тем чтобы в дальнейшем придумать способы монетизации по обстоятельствам.

В целом же можно сказать, что технологии Интернета вещей создают интерактивную среду, которая ориентирована на человека. Для того чтобы приносить практическую пользу, этой среде необходимо научиться собирать и распознавать данные из окружающего мира без участия человека. Сегодня одной из самых перспективных и распространенных технологий Интернета вещей являются RFID-метки, но в будущем данная сфера пополнится и другими технологиями.

1.5. Интернет вещей как основа Индустрии 4.0

Развитие Интернета вещей и киберфизических систем, включающих в себя датчики, приводы, семантические M2M-коммуникации и активную память, встроенную в продукцию, легли в основу концепции «Индустрия 4.0». Основными целями Индустрии 4.0 являются смена способов производства: контроль производства в режиме реального времени, а также максимально тесная взаимосвязь технологических и бизнес-процессов.

Производство в рамках экономики знаний сегодня постепенно вступает в стадию Индустрии 4.0, инфраструктура и производственные

мощности которой самостоятельно способны понимать свое окружение и обмениваться данными по различным каналам коммуникации. Сегодня в процессе производства участвует огромное количество датчиков, которые регистрируют с высокой точностью различные параметры своего физического окружения. Отдельные элементы производственной системы уже сегодня могут принимать самостоятельные решения, касающиеся производства, за счет встроенных процессоров и программ аналитики.

Новая инфраструктура в промышленности может внедряться как «с нуля», так и на действующих предприятиях. Идея о множестве датчиков, которые собирают информацию об окружающем мире, обмениваются ей друг с другом и передают на специальные устройства для обработки и принятия решений, достаточно гибкая по своей природе. На текущий момент в индустрии уже наметились первые признаки постепенного перехода к использованию принципов концепции «Индустрия 4.0».

Индустрия 3.0, в рамках которой функционирует большинство современных предприятий, подразумевает наличие множества датчиков, которые собирают данные. Объем данных настолько велик, что человек уже не способен самостоятельно работать с ними, однако машины еще не научились обмениваться ими и эффективно применять в производственных нуждах. Очевидно, что многие процессы станут гораздо более эффективными и рентабельными, если небольшие радиодатчики смогут обмениваться данными друг с другом для их дальнейшего использования в производстве.

Концепция Индустрии 3.0 предполагает, что между виртуальным и физическим миром существует определенная граница. Более того, по факту они не пересекаются: физические датчики генерируют виртуальные данные, которые не используются для автоматического принятия решений. Технологии Индустрии 4.0 позволяют создать киберфизические системы, которые стирают эту достаточно условную границу между реальным и виртуальным.

Разумеется, системы поколения Индустрии 3.0 также собирали данные и обменивались ими. Но только концепция Индустрии 4.0 предполагает возможность того, что эти данные будут в реальном времени применяться производственными мощностями для самостоятельного выполнения определенных процессов и взаимодействия с окружением. Такие технологии могли бы обеспечить эффективный выпуск даже минимальной партии продуктов, поскольку позволили бы оперативно вносить изменения в производственные процессы.

Тот факт, что техника получит способность по-настоящему понимать окружающий мир, выведет на новый качественный уровень современное производство. Сегодня производственные установки программируются вручную людьми, когнитивные способности которых серьезно ограничены. Индустрия 4.0 предполагает, что техника сама сможет сконфигурироваться для выполнения производственных задач без участия человека.

В качестве аналогии для концепции Индустрии 4.0 можно привести обыкновенный муравейник. Каждый отдельно взятый муравей как таковой не слишком умен, но их совместное взаимодействие позволяет строить достаточно сложные муравейники, защищаться от хищников, выживать в опасных условиях и добывать пищу. Иными словами, муравейник – как и Индустрия 4.0 – не является простой суммой своих частей. Концепция Индустрии 4.0 основана на использовании синергетического эффекта от взаимодействия множества простых и дешевых устройств.

Однако мало собрать информацию и совершить информационный обмен. Для того чтобы производство стало интеллектуальным или самостоятельно сконфигурировалось, эту информацию требуется обработать при помощи «умных» аналитических программных средств. Данные об окружающем мире становятся информацией только после того, как получают некую интеллектуальную интерпретацию. Следовательно, Индустрия 4.0 будет характеризоваться высоким качеством взаимодействия, причем программы будут понимать контексты, в рамках которых была получена и обработана информация.

Профессор Вольфганг Вальстер – заведующий кафедрой на факультете информатики в Университете Саарбрюккена, главный исполнительный директор и директор по технической и научной работе в Немецком исследовательском центре искусственного интеллекта (DFKI) в Кайзерслаутерне, Саарбрюккене, Бремене и Берлине – один из ведущих в мире экспертов в области искусственного интеллекта года в интервью Корпоративному журналу Festo 1.2013 «Тенденции в автоматизации» сказал: «В мире Индустрии 4.0 производственное оборудование и продукты станут активными системными компонентами, управляющими своими производственными и логистическими процессами. Они будут включать в себя киберфизические системы, связывающие виртуальное пространство Интернета с реальным физическим миром. При этом они будут отличаться от существующих мехатронных систем наличием способности взаимодействовать со своим окружением, планировать и адаптировать свое собственное поведение согласно окружающим условиям, учиться новым моделям и линиям поведения и, соответственно, быть самооптимизирующимися. Они обеспечат эффективный выпуск даже минимальных партий при быстром внесении изменений в продукцию и большом количестве вариантов. Применение встроенных датчиков/исполнительных механизмов, обеспечение межмашинного обмена данными и использование активной семантической памяти приведет к появлению новых методов оптимизации, направленных на сохранение ресурсов в производственной среде. Это, в свою очередь, будет способствовать будущему созданию экологически безопасного и передового производства с приемлемыми расходами»²⁴.

По сути, Индустрия 4.0 – попытка применить на практике технологии, позволяющие создать более гибкое производство для лучшего удо-

²⁴ Корпоративный журнал Festo 1.2013 «Тенденции в автоматизации». URL: http://www.festo.com/net/SupportPortal/Files/299464/TIA_8_2013.pdf.

влетворения нужд заказчиков. Концепция «изготовление на заказ» (make-to-order) требует интерактивных коммуникаций со всеми сторонами, принимающими участие в разработке спецификаций и производстве, включая заказчиков, поставщиков, работников, а также – коммуникации с производственным оборудованием.

Концепция перемещения изготавливаемой продукции по автоматическим сборочным линиям с использованием электронных средств идентификации и внутренней памяти для добавления информации о производственном процессе изменяет режим производства с синхронного на асинхронный.

Например, автоматическая сборочная линия требует, чтобы любые изменения в спецификациях передавались линии синхронно с перемещением изготавливаемой продукции вдоль нее. Если хоть одна из единиц продукции «выпадает» из последовательности – начнется хаос. А в новом, асинхронном режиме производства каждое изделие по мере продвижения вдоль сборочной линии будет само инструктировать машину или станок о своих индивидуальных спецификациях.

Индустрия 4.0 – это шаг в будущее производства, настоящая промышленная революция, в основе которой лежат базовые технологии концепции Интернета вещей.

1.6. Интернет вещей как источник угроз

Любая технология, обладающая потенциалом изменить мир, может обернуться как против отдельных пользователей, так и против человеческого общества в целом. Технологии Интернета вещей открывают широкие возможности для индивидов, организаций и экономики. Однако даже сегодня, при отсутствии массового использования подключенных сенсоров и датчиков, существуют серьезные опасения по поводу перспектив их использования.

Как говорилось ранее, в 2008 году Национальный разведывательный совет США отнес Интернет вещей к списку из шести потенциально разрушительных технологий. Безусловно, деятельность разведки имеет свою специфику, и опасения местных аналитиков связаны, прежде всего, с вопросами информационной безопасности. Но не следует забывать, что новые технологии, получившие массовый характер, со временем меняют базовые принципы человеческого взаимодействия. Социальные нормы (как и модели социального поведения) изменяются с появлением определенных технологий. Телевидение и радио изменили вертикальную коммуникацию между государством и организациями с одной стороны и гражданами с другой. Мобильные телефоны изменили характер горизонтальной коммуникации между людьми, сделав ее более тесной. Web-технологии позволили людям оставаться на связи в режиме реального времени, а структура общественных связей стала все больше напоминать сеть, нежели вертикаль.

Тем не менее фактическая угроза от приведенных выше технологий несопоставима с угрозами, которые в перспективе таит в себе Интернет вещей. Телевидение, радио и Интернет изменили человеческую

жизнь, однако они всегда представляли и представляют собой своеобразную надстройку, пусть и прочно укоренившуюся в человеческой жизни. Тогда как технологии Интернета вещей потенциально способны изменить функционал вещей, которыми люди пользовались веками, а порой – тысячелетиями. Более того, изменение функционала идет рука об руку с возможностью (зачастую нелегальной) стороннего воздействия на таковые вещи. Хакеры, корпорации и отдельные государственные органы могут быть заинтересованы в этом с целью извлечения коммерческой выгоды или сбора данных. Вот почему вопрос безопасности технологий Интернета вещей имеет практическое значение сразу на нескольких уровнях.

1.7. Техническая безопасность

В начале 2014 года была официально зафиксирована первая кибератака, в которой приняли участие подключенные объекты²⁵. Исследователи из Proofpoint утверждают, что за период с 23 декабря по 6 января 100 000 подключенных устройств разослали более 750 000 спам-сообщений. Большая часть устройств (75%) представляла собой традиционные смартфоны и планшеты, однако среди оставшихся 25% были телевизоры, холодильники и аналогичная бытовая техника и электроника.

Отечественные аналитики из Лаборатории Касперского сходятся во мнении, что главной причиной стало незащищенное подключение устройств к Интернету и использование фабричных пар логинов и паролей²⁶. Можно прогнозировать, что прошедшая атака была не последней. В обозримом будущем можно ожидать DDoS-атаки с использованием подключенных объектов. Эксперты корпорации Symantec в целом разделяют подобные взгляды и утверждают, что в 2014 году Интернет вещей превратится в «интернет уязвимостей»²⁷. Современные устройства, подключенные к Сети, не обладают ни должной защитой, ни способностью проинформировать владельца об атаке.

В случае с технологиями Интернета вещей особую опасность представляют физические атаки. Под физической атакой подразумевается такая хакерская атака, которая наносит прямой материальный ущерб. Сегодня хакерские атаки способны навредить в первую очередь крупным компаниям, которые могут потерять внутренние данные или коммерческие клиентские базы, сформированные для ведения коммерческой деятельности.

²⁵ Впервые источником кибератаки стал интернет вещей // МК.RU : Московский Комсомолец. 2014. URL: <http://www.mk.ru/science/technology/article/2014/01/20/972642-ypervyie-istochnikom-kiberataki-stal-internet-veschey.html> (дата обращения 25.02.2014).

²⁶ «Интернет вещей»: уязвимость и безопасность // KASPERSKY.RU : Блог о бизнесе «Лаборатории Касперского». 2014. URL: <http://business.kaspersky.ru/internet-of-things-insecurity/> (дата обращения 25.02.2014).

²⁷ Эксперты: «интернет вещей» превратится в «интернет уязвимостей» // RIA.RU : РИА Новости. 2013. URL: <http://ria.ru/technology/20131217/984735839.html> (дата обращения 25.02.2014).

В отчете Cisco за 2013 год говорится, что киберпреступность перестала быть легким раздражающим фактором, который слегка увеличивает общие издержки бизнес-процесса. В скором времени экономика дойдет до поворотного момента, когда размер материального ущерба от кибератак будет превышать экономические преимущества, создаваемые информационными технологиями. А потому следует разрабатывать новые подходы, способные сократить ущерб от хакерских атак²⁸.

Развертывание технологий Интернета вещей только добавит проблем в сферу обеспечения безопасности. Проекты по внедрению технологий Интернета вещей в бизнесе, как правило, хорошо окупаются. Но каждый подключенный объект увеличивает число целей для хакерских атак и резко повышает значение конфиденциальной информации. К примеру, подключив к сети видеокамеры, владельцы магазинов смогут воспользоваться аналитикой для лучшего понимания поведения потребителей. Безусловно, коммерческая выгода от внедрения такой технологии очевидна. Но в отдельных случаях хакер может использовать камеру в магазине как точку входа в сеть компании, чтобы получить коммерчески важные данные. Вот почему при внедрении проектов из сферы Интернета вещей необходимо использовать объединенные решения физической и информационной безопасности.

Сегодня в отсутствие массового развертывания Интернета вещей уже существуют вирусы, нацеленные на физический вывод из строя инфраструктуры предприятий. Яркий пример подобного вируса – компьютерный червь Stuxnet, который может использоваться для шпионажа и диверсий на промышленных предприятиях²⁹.

На конференции BlackHat специалисты в сфере информационной безопасности продемонстрировали возможность реальной атаки на SCADA-системы нефтедобывающего предприятия³⁰. Последствия такой атаки могут стать катастрофическими не только для бизнеса, но и для экологии. Жизнь и здоровье людей также оказываются под угрозой.

Однако с развитием технологий Интернета вещей под удар попадут прежде всего рядовые пользователи подключенных вещей и устройств. Ценность таких технологий и их дальнейшая монетизация напрямую связаны с персонализированной информацией, которую способны собрать подключенные объекты. Защита собранных данных должна ставиться во главу угла, поскольку речь идет о неприкосновенности частной жизни.

Кроме того, атаки на подключенные объекты могут привести к достаточно неприятным «бытовым» последствиям. Продемонстрировать

²⁸ Эйбуд Дж. Интернет вещей: друг или враг? // CISCO.COM : Новости. 2013. URL: <http://www.cisco.com/web/RU/news/releases/txt/2013/08/081613a.html> (дата обращения 25.02.2014).

²⁹ Ильин Ю. Американско-израильское происхождение боевого трояна Stuxnet подтверждено // COMPUTERRA.RU : Журнал «Компьютерра». 2012. URL: <http://www.computerra.ru/31401/> (дата обращения 25.02.2014).

³⁰ Дайджест инцидентов в области информационной безопасности: 18 июля – 18 августа // KASPERSKY.RU : Блог о бизнесе «Лаборатории Касперского». 2013. URL: <http://business.kaspersky.ru/security-digest-jul18-aug18/> (дата обращения 25.02.2014).

это на практике можно, смоделировав следующую ситуацию. К примеру, не так давно Intel продемонстрировала концепт «умной двери», которая открывается и закрывается с использованием смартфона, на котором хранится электронный ключ. В случае успешной хакерской атаки на такую дверь ее владелец попросту не сможет вернуться домой или выйти из него³¹.

Другие технологии, предназначенные для «умного дома», могут быть выведены из строя хакерами с тем или иным уровнем материального ущерба для владельца. Так, взлом «умной лампы», способной мониторить положение людей и регулировать освещение, позволит хакерам менять яркость по собственному усмотрению. А атака на «умный стол», предназначенный для более точного позиционирования обитателей дома, позволит сбить с толку всю домашнюю сеть.

Не так давно журнал Forbes уже писал о приложении для домашней автоматизации, которое не имело должной защиты. В результате любой желающий, более-менее осведомленный в вопросах информационных технологий, мог управлять им из любой точки мира. Для управления оказались доступными телевидение, освещение и различные подключенные вещи и устройства³².

Нельзя забывать, что существует прямая зависимость между ценностью объекта и ущербом от того же объекта в случае, если он стал жертвой хакерской атаки. Причем ценность объекта вовсе не эквивалентна его рыночной стоимости. Так, дверь – относительно дешевый предмет, однако ее ценность определяется не рыночной стоимостью, а невероятно высоким субъективным значением функционала для каждого отдельно взятого индивида.

1.8. Социальные угрозы

Помимо экономического ущерба и физического вреда, технологии Интернета вещей, как и другие массовые технологии, грозят возникновением вполне осязаемых социальных угроз. Неприкосновенность частной жизни закреплена как на законодательном уровне, так и в сознании людей. Модели общественного поведения прямо демонстрируют это на практике. Так, каждый посетитель ресторана имеет возможность следить за другими гостями, однако никто этого не делает. Принцип вежливого невнимания и уважение к чужой частной жизни обуславливают значительную долю всех наших социальных интеракций. Тем не менее интеграция технологий Интернета вещей в социальные процессы может нанести серьезный ущерб личной жизни людей.

³¹ Intel поделилась своим видением интернета вещей // IXBT.COM : Информационный портал. 2014. URL: <http://www.ixbt.com/news/hard/index.shtml?17/67/77> (дата обращения 25.02.2014).

³² Hill K. When ‘Smart Home’ Get Hacked: I Haunted A Complete Stranger’s House Via The Internet // FORBES.COM : Information for the World’s Business Leaders. 2013. URL: <http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/> (дата обращения 25.02.2014).

Сегодня отдельные особенности каждого человека и его привычки известны только ему и его близкому окружению. На публике их принято скрывать. Технологии из мира Интернета вещей позволяют обучить внешнюю среду своим привычкам, сделать их публичными. Таким образом, окружающая среда может стать более удобной и комфортной. Но вместе с этим растет риск потери конфиденциальных, личных данных, не предназначенных для публичного просмотра.

В 1988 году вышла в свет книга Дэвида Брина «Прозрачное общество»³³. В своей аналитической книге писатель-фантаст утверждал, что понятие ривасу на Западе становится инструментом эксплуатации, и на практике раскрытие части информации увеличивает безопасность каждого отдельного человека, а не уменьшает ее. Тем не менее базовый уровень приватности не только нужно, но и можно сохранить даже с развитием информационных технологий³⁴.

Дэвид Брин считает, что частная жизнь останется неприкосновенной уже просто потому, что люди нуждаются в этом. Но одного только права на частную жизнь недостаточно, на практике люди и общество сталкиваются с трехуровневой схемой: право как абстрактная и юридическая норма, практическая возможность реализации права и способность определить нарушение права. Технологии Интернета вещей могут сузить пространство частной жизни, однако способны облегчить выявление правонарушений. Сенсоры и датчики, входящие в концепцию «умного города», позволяют выявлять нарушителей свобод и неприкосновенности частной жизни. Люди получают возможность привлечь к ответственности нарушителей, которые ранее оставались безнаказанными.

Приватность как таковая есть совокупность права знать что-либо о другом человеке и права говорить об этом. Потребность людей в частной жизни вкупе с ростом знания, вызванным информационными технологиями, неизбежно приведет к ограничениям. Оптимальным вариантом может стать так называемое «обратное наблюдение», при помощи которого граждане смогут наблюдать за наблюдателем. В результате удастся избежать неправомерного использования полученной информации, а также различных злоупотреблений со стороны корпораций и государственных органов.

В некотором смысле концепция Интернета вещей соотносится с идеями либерализма и рыночной экономики. Так, рыночная экономика предполагает отсутствие издержек на поиск информации о товаре. На практике эти издержки велики, и потребители совершают не оптимальный, а всего лишь удовлетворительный выбор. Технологии Интернета вещей сделают получение информации более простым, а потому можно говорить о некоей связи между классическими общественными концепциями и разворачивающейся новой эпохой Интернета.

³³ Brin D. The Transparent Society // WIRED.COM : Информационный портал. URL: <http://www.wired.com/wired/archive/4.12/fftransparent.html> (дата обращения 25.02.2014).

³⁴ Чеклецов В.В. Чувство планеты: Интернет вещей и следующая технологическая революция. – М.: Российский исследовательский центр по Интернету вещей, 2013.

Стоит сказать, что, несмотря на развитие технологий и возникновение массовых каналов трансляции информации, сегодняшний человек обладает гораздо большей приватностью, чем его предки. Телефонные переговоры когда-то несли аналогичную угрозу, однако принятие законов (к примеру, запрет на прослушивание без соответствующей санкции в США) и укоренение социальных норм привели к тому, что угрозы нивелировались, тогда как полезность для общества и человека не пострадала.

Можно также предположить, что часть людей не нуждается в том уровне приватности, который существует сегодня. Примером может служить распространение технологий трекинга. При помощи трекинг-технологий человек добровольно позволяет людям, вещам и организациям мониторить собственное положение в пространстве и перемещение. Сегодня по этому принципу работает FourSquare и в меньшей степени Twitter. Тем не менее в настоящий момент трекинг является свободным выбором конкретного человека, тогда как технологии Интернета вещей потенциально способны сделать его всеохватывающим. В этом случае вновь возникает дилемма между знанием и его использованием, его публичностью.

Впрочем, сценарий развития, близкий к антиутопиям в стиле «1984» Дж. Оруэлла, также возможен. В своей книге «Чувство планеты: Интернет вещей и следующая технологическая революция» В.В. Чеклецов рассказывает о китайском городе Шеньчжен, в котором расположено более 200 000 видеокамер для мониторинга поведения жителей. Кроме того, в городе используется система отслеживания движения жителей через специальные ID-карты на основе RFID-меток, использующихся для покупок.

Роб Ван Краненбург указывал условия, при которых внедрение Интернета вещей приведет к созданию открытого общества, а не к укреплению автократии:

- человек должен знать о степени своей прозрачности в той или иной ситуации;
- человек должен иметь обратную связь и контролировать органы наблюдения;
- человек должен иметь возможность подключаться к потокам данных в месте своего нахождения или обитания, а также к данным о всех процессах, важных для его жизни;
- человек должен иметь возможность стать «невидимым» хотя бы для тех устройств и систем, которые относятся непосредственно к его личным потребностям.

Однако на практике то русло, в котором будет развиваться Интернет вещей, зависит не от самой технологии, а от общественно-политических условий, в которых она будет существовать. При этом одни страны пойдут по пути создания открытого общества, тогда как другие будут использовать новые технологии для повышения контроля над гражданами.

1.9. Исследовательские центры и проекты

Основным исследовательским центром, фокусирующим свое внимание на Интернете вещей, остается **Auto-ID Labs** Кэвина Эштона. Auto-ID Labs – независимая сеть из семи лабораторий, которые исследуют и развивают новые технологии для революции в глобальной коммерции, обеспечивающая ранее несбыточные потребительские преимущества³⁵.

Семь университетов, входящих в состав Auto-ID Labs, расположены на четырех континентах. Исследователи утверждают, что новое поколение технологий Интернета вещей может произвести революцию в глобальной коммерции. Главный исследовательский партнер – GS1, некоммерческая организация, которая прославилась установлением стандартов в глобальной коммерции (введение штрих-кодов в индустрии продаж почти 40 лет назад). Цель лаборатории – добавить потребителя в B2B-ориентированную модель GS1, исследовать возможности нового программного обеспечения, оборудования, бизнес-процессов и приложений.

Исследования лаборатории делятся на три уровня: бизнес-процессы и прикладные исследования; Программное обеспечение и сеть; Оборудование³⁶.

На бизнес-уровне исследуются кейсы и практическое применение технологий, защита информации, фундаментально новые бизнес-процессы, а также индустрии платежей, лизинга, страхования, управления качеством, защиты товарных марок и производственного дизайна. На этом направлении фокусируются усилия MIT, Кембриджа, Университета Кейо (Япония) и Университета Цюриха.

На уровне программного обеспечения и сетей исследуется архитектура сетей будущего. На этом направлении фокусируются Университет Кейо и MIT.

И, наконец, в исследования сферы оборудования вовлечены Университет Фудань (Китай), ICU, MIT и Университет Аделаиды (Южная Австралия). Здесь исследуются чипы, память, батареи, сенсоры, возможности считывания информации из окружающего мира.

В Финляндии существует **национальный проект Интернета вещей**³⁷. Данное направление считается одним из стратегически важных исследовательских проектов в масштабах национальных интересов. Задачи проекта – создание исследовательского поля для изучения Интернета вещей и четкое определение центральных объектов исследования.

Сюда входят более 350 ученых и мировых экспертов. Проект включает в себя более 50 крупных компаний, организаций и университетов. Среди больших компаний: Ericsson, F-Secure, Finnpark, Intel,

³⁵ Auto-ID Labs. Официальный сайт. URL: <http://www.autoidlabs.org/> (дата обращения 25.02.2014).

³⁶ Auto-ID Labs: Research // AUTOIDLABS.COM. URL: <http://autoidlabs.org/research/page.html> (дата обращения 25.02.2014).

³⁷ DIGILE Internet of Things. Официальный сайт. URL: <http://www.internetofthings.fi/> (дата обращения 25.02.2014).

Nokia, Renesas Modile и 8 финских университетов. Из иностранных – университет Вухана в Китае.

На территории Европейского союза существует собственный **исследовательский кластер Интернета вещей**³⁸. Цель: исследовать огромный потенциал Интернета вещей для Европы и координировать сближение текущей научной активности. Создатели считают, что Интернет вещей имеет потенциал для увеличения европейской конкурентоспособности. Это важный драйвер для развития общества и экономики, базирующихся на информации.

С декабря 2013 года в России существует лаборатория «Интернета вещей» при факультете инфокоммуникационных сетей и систем СПбГУТ. Данный исследовательский центр занимается как концептуальными, так и технологическими исследованиями в сфере Интернета вещей. Ресурсы лаборатории делают возможным проектирование и прототипирование устройств, относящихся к сфере Интернета вещей³⁹. Исполнительным директором центра является Вадим Чеклецов, автор концептуального исследования «Чувство планеты: Интернет вещей и следующая технологическая революция».

Необходимо также рассмотреть проекты планетарного масштаба, первым из которых является **Planetary Skin Institute** при содействии Cisco. Декларируемая цель организации – улучшение жизни миллионов людей по всему миру за счет развития управления рисками и ресурсами. В исследованиях уделяется пристальное внимание сенсорам в составе Интернета вещей и технологиям Big Data⁴⁰.

IBM продолжает развивать свой проект **Smart Planet**, цель которого, как и следует из названия, – сделать многие аспекты нашего мира «умнее». Инициатива IBM нацелена на использование «умных» систем больших масштабов. Сюда относятся системы контроля городского трафика, «умные» дамбы, системы управления водными ресурсами, «зеленая» энергетика и строительство, а также разработки в сфере здравоохранения⁴¹.

Лаборатории компании HP запустили не менее амбициозный проект под названием **Central Nervous System for the Earth (CeNSE)**. Цель проекта – размещение большого числа различных сенсоров в разных частях планеты, а также их внедрение в человеческие зоны обитания. По замыслу ученых, такие сенсоры должны стать своеобразной искусственной нервной системой планеты. В целом подобная инициатива соотносится с прогнозами независимых экспертов о потенциальных масштабах концепции Интернета вещей.

³⁸ IERC European Research Cluster on the Internet of Things. Официальный сайт. URL: <http://www.internet-of-things-research.eu/index.html> (дата обращения 25.02.2014).

³⁹ Открытие лаборатории «Интернета вещей» // INTERNETOFTHINGS.RU. 2013. URL: <http://internetofthings.ru/sobytiya/69-otkrytie-laboratorii-interneta-veshchej> (дата обращения 25.02.2014).

⁴⁰ Planetary Skin Institute. Официальный сайт. URL: <http://www.planetaryskin.org/> (дата обращения 25.02.2014).

⁴¹ Smarter Planet. Официальный сайт. URL: http://www.ibm.com/smarterplanet/us/en/?ca=v_smarterplanet (дата обращения 25.02.2014).

1.10. Тематические конференции

1. MIT Internet of Things Conference 2014

8–14 октября 2014 г., Кембридж

Форум считается лучшим мероприятием, посвященным Интернету вещей. Приблизительные темы конференции⁴²:

- мобильный Интернет вещей: современное приложение смартфонов для создания и потребления данных;
- устройства для Интернета вещей или разработка схем. Современное оборудование, которое позволяет собирать данные, инновационные концепты для распространения повсюду сенсоров;
- архитектура и системный дизайн: надежность, устойчивость, масштабируемость, рентабельность и совместимость с экосистемой Интернета вещей;
- «облачные» вычисления и семантические веб-технологии: защита данных, хранение и доступ, коммуникационные протоколы, связанные данные и веб-семантика для совместимости с пользователями и устройствами;
- интерфейс и системы управления;
- аналитика в Интернете вещей: инновационные алгоритмы и технологии анализа данных для извлечения полезности из Интернета вещей.

2. IEEE Internet of Things World Forum⁴³

6–8 марта 2014 г., Сеул

Позиционируется как уникальное событие для лидеров индустрии, ученых и топовых чиновников. Мероприятие создано для рассмотрения ключевых критических инноваций в технологиях, которые изменят исследование и практическое применение пространства будущего.

Тема форума-2014: исследование того, как прогресс в технологиях и приложениях из сферы Интернета вещей может поощряться и культивироваться на благо всего общества. Цель форума – рассмотреть современное состояние в сфере Интернета вещей и практические исследования. Исследователи и практики из таких областей, как наука, стандартизация, производство и общественный сектор, попытаются презентовать свои исследования и нововведения, а также поделиться опытом.

3. Internet of Things Asia 2014⁴⁴

21–22 апреля 2014 г., Сингапур

Singex Group в партнерстве с Сингапурской ассоциацией автоматизации производства запускает новое мероприятие, Internet of Things

⁴² Call for Papers // IOT-CONFERENCE.ORG : Internet of Things 2014. URL: <http://www.iot-conference.org/iot2014/call-for-papers/> (дата обращения 25.02.2014).

⁴³ IEEE World Forum on Internet of Things. Официальный сайт. URL: <http://sites.ieee.org/wf-iot/> (дата обращения 25.02.2014).

⁴⁴ IOT Asia 2014. Официальный сайт. URL: <http://www.internetofthingsasia.com/> (дата обращения 25.02.2014).

Asia: выставка и конференция, фокусирующаяся на Интернете вещей и M2M. Это будет первое тематическое мероприятие в регионе, который фокусируется на связи технологий Интернета вещей с конечным бизнесом, государственным управлением и обществом.

4. Internet of Things Week 2014 London⁴⁵

16–20 июня 2014 г., Лондон

Данное мероприятие возникло в Европейском кластере исследования Интернета вещей с целью привлечения бизнесменов и ученых со всего мира. Задачи мероприятия:

- развитие возможностей Интернета вещей;
- соединение мирового бизнеса с научным сообществом для проведения инноваций;
- поддержка международного сотрудничества в сфере Интернета вещей;
- решение общественных и экономических вопросов.

5. ThingsCon⁴⁶

2–3 мая 2014 г., Берлин

Это двухдневная конференция о будущем компьютерного оборудования. Темы варьируются от Интернета вещей и подключенных устройств до 3D-печати и новых технологий производства. В переговорах, на семинарах и личных сессиях международные спикеры расскажут обо всем, что касается применения прототипов технологий в масштабах бизнеса.

Целевая аудитория: дизайнеры, инженеры, ученые, начинающие бизнесмены, маркетологи, пиарщики, производственники и изобретатели.

6. Internet of Things Festival⁴⁷

22 февраля 2014 г., Кембридж

Открытое мероприятие, посвященное творчеству, технологиям и Интернету. Доклады спикеров, демонстрации и практические сессии от MIT включают персональное, коммерческое и общественное применение Интернета вещей. Мероприятие стремится к совмещению реального и цифрового миров.

Некоторые темы: дроны и летающая техника; использование Интернета вещей от города до фермы; дизайн и производство в Интернете вещей; «железо», ПО, технологии и коммуникации в Интернете вещей; Интернет вещей глазами производителей микросхем; коммерциализация и бизнес-модели в Интернете вещей; «умные» и беспроводные контроллеры и др.

⁴⁵ IoT Week 2014. Официальный сайт. URL: <http://iot-forum.eu/iot-week-2014/> (дата обращения 25.02.2014).

⁴⁶ Things Con. Официальный сайт. URL: <http://thingscon.com/> (дата обращения 25.02.2014).

⁴⁷ The IoT Initiative. Официальный сайт. URL: <http://www.iotfestival.com/> (дата обращения 25.02.2014).

7. The 5th Annual Internet of Things Europe⁴⁸

3–4 марта 2014 г., Брюссель

На пятом саммите рассмотрен вопрос, как Интернет вещей может повлиять на развитие Европы в ближайшем будущем, а также политику ЕС относительно его развития. Участники рассмотрели текущую экосистему Интернета вещей в Европе и посмотрят на перспективы в ближайшем будущем.

Темы:

- Текущее состояние развертывания Интернета вещей в Европе: чего мы добились? Что нужно сделать?
- Понимание выгод от Интернета вещей и его влияния на общество: «умный город»; подключенный дом (The Connected Home).
- Финансирование Интернета вещей.
- Облачные вычисления, Большие данные и Интернет вещей.
- Интернет вещей на развивающихся рынках.
- Государственное управление и стандартизация.
- Управление и Интернет вещей.
- «Человеческая» сторона Интернета вещей.
- Безопасность и управление идентификацией.

⁴⁸ The 5th Annual Internet of Things European Summit. Официальный сайт. URL: http://www.eu-ems.com/summary.asp?event_id=210&page_id=1789 (дата обращения 25.02.2014).

Интернет вещей не является некоей единой технологией. К сфере Интернета вещей относится множество различных технологий, устройств и решений, совокупность которых позволяет передавать, хранить и обрабатывать объективные данные из внешней среды, полученные при минимальном участии человека. В упрощенном виде совокупность технологий, приводящих к возникновению концепции Интернета вещей, можно изобразить графически. Концепция Интернета вещей возникает на стыке трех своих компонентов:



Рис. 5. Совокупность технологий Интернета вещей

К данной триаде нередко добавляются программное обеспечение и технологии визуализации данных, однако работа технологий Интернета вещей может реализовываться на практике без непосредственного участия человека. В ряде случаев представление информации пользователю не является необходимым. К примеру, «умный» стол, основная функция которого – мониторинг положения людей для оптимизации работы сети подключенных устройств, никак не предоставляет пользователям получаемую информацию. Более того, концепция Интернета вещей предполагает, что работа с информацией происходит без участия людей или с их минимальным участием.

Приведенное выше сочетание технологий, образующих концепцию Интернета вещей, можно детализовать более подробно. Технологии, входящие в состав Интернета вещей, образуют цепочку, слаженная работа которой и обуславливает функциональные качества концепции Интернета вещей. Цепочка выглядит следующим образом:

- Технология идентификации объекта в окружающей среде.
- Технология автоматизированного получения данных об объекте.
- Технология идентификации сенсора, собравшего данные.
- Технология передачи данных с «подключенного» устройства на сервер.
- Технология хранения и обработки.
- Технология представления информации пользователям.

Средства идентификации подразделяются на средства идентификации объектов внешней среды и средства идентификации подключенных устройств. И если с решением последней задачи не возникает особых проблем (за исключением медленного перехода к стандарту IPv6), то «виртуализация» физических объектов вызывает серьезные проблемы.

Данная цепочка не заменяет, а уточняет приведенные выше концептуальные составляющие. Разное число составляющих обусловлено тем, что свойства подключенных устройств, к которым относятся сенсоры, включают в себя наличие технологий идентификации и средств передачи данных. А технология предоставления информации пользователям является дополнительной надстройкой, не относящейся к обязательным компонентам концепции Интернета вещей.

2.1. Средства виртуальной идентификации объектов внешней среды

Потребность в виртуальной идентификации объектов внешней среды обусловлена существованием двух типов подключенных устройств. К первой группе относятся подключенные устройства, способные воспринимать непосредственно окружающий мир. Их работа предполагает, что либо идентификация объекта или свойства внешней среды существует по умолчанию, либо они в состоянии самостоятельно произвести ее. Устройство температурного датчика таково, что среди всех свойств окружающего мира он распознает только одно – температуру.

Ко второй группе можно отнести подключенные устройства, которые могут взаимодействовать только с подключенными вещами. В используемой терминологии подключенная вещь – это объект физического мира, обладающий уникальной идентификацией в информационном пространстве, обладающий функцией памяти и соответствующий критерию коммуникативности. В случае, когда технологии Интернета вещей используют подключенные устройства второй группы, объекты окружающей среды нуждаются в дополнительной идентификации. Подобная ситуация возникает, когда, к примеру, сканер получает информацию от идентифицированной коробки с товаром, которая была трансформирована в подключенную вещь за счет использования RFID-метки. Если коробка не получит уникальную идентификацию, то она не станет подключенной вещью, а подключенное устройство (сканер) не сможет захватить информацию.

Таким образом, при развертывании технологий Интернета вещей нередко возникает задача виртуализации объектов реального мира. Технологии, позволяющие делать это, могут считаться основополагающими для возникновения и развития концепции Интернета вещей. Справиться с этой задачей позволяют различные технологии, среди которых наибольшее распространение получили штрих-кодирование и радиочастотная идентификация.

2.1.1. Штрих-кодирование

Штриховой код (штрих-код) – это последовательность черных и белых полос, представляющая некоторую информацию в удобном для считывания техническими средствами виде.

В 1948 году Бернард Сильвер, аспирант Института технологии Университета Дрекселя в Филадельфии, вместе с Норманом Джозефом Вудланду и Джордином Джохэнсоном начали исследовать различные системы маркировки. Их первая работающая система использовала ультрафиолетовые чернила, но они были довольно дороги, а кроме того, со временем исчезали.

Бернард Сильвер продолжил разработку меток, и его следующее вдохновение неожиданно дала азбука Морзе – он сформировал свой первый штриховой код из песка на берегу. Как он сам сказал: «Я только расширил точки и тире вниз и сделал из них узкие и широкие линии». Чтобы прочесть штрихи, он приспособил технологию саундтрек (звуковой дорожки), а именно оптический саундтрек, используемую для записи звука в кинофильмах. 20 октября 1949 года Вудланд и Сильвер подали заявку на изобретение. В результате ими был получен патент США № 2 612 994, изданный 7 октября 1952 года.

2.1.1.1. Способы штрих-кодирования информации

В настоящее время активно применяются два способа штрих-кодирования информации:

- линейный;
- двухмерный.

Линейный штрих-код

Линейными (обычными) называются штрих-коды, читаемые в одном направлении (по горизонтали). Наиболее распространенные линейные символика: EAN (EAN-8 состоит из 8 цифр, EAN-13 – из 13 цифр), UPC (UPC-A, UPC-E), Code56, Code128 (UPC/EAN-128), Codabar, Interleaved 2 of 5. Линейные символика позволяют кодировать небольшой объем информации (до 20–30 символов, обычно цифр).



Рис. 6. Пример линейного штрих-кода

Двухмерный штрих-код

Двухмерные символы были разработаны для кодирования большого объема информации. Расшифровка такого кода проводится в двух измерениях (по горизонтали и по вертикали).

Двухмерные коды подразделяются на многоуровневые (stacked) и матричные (matrix). Многоуровневые штрих-коды появились исторически ранее и представляют собой поставленные друг на друга несколько обычных линейных кодов. Матричные же коды более плотно упаковывают информационные элементы по вертикали.

В настоящее время разработано множество двухмерных штрих-кодов, применяемых с той или иной широтой распространения. Вот некоторые из них:

- Aztec Code;
- Data Matrix;
- MaxiCode;
- PDF417;
- QR код;
- Microsoft Tag.



Рис. 7. Пример двухмерного штрих-кода (QR-код)

Таблица 5

Примеры соотношения размеров символов двухмерного штрих-кода и емкости кода

Число слоев с данными	Размер символа	Байт
1	15 × 15	7
4	27 × 27	53
7	45 × 45	145
11	61 × 61	298
15	79 × 79	502
20	101 × 101	824
26	125 × 125	1314
32	151 × 151	1914

Логическая структура

Код EAN-13 с точки зрения кодировки товара условно можно разделить на 5 зон:

- префикс национальной организации GS1 (3 цифры);
- регистрационный номер производителя товара (4–6 цифр);
- код товара (3–5 цифр);
- контрольное число (1 цифра);
- дополнительное поле (необязательное штрих-кодовое поле, иногда там ставится знак «>», «индикатор свободной зоны»).

2.1.1.2. Преимущества штрих-кодирования

Поскольку штрих-код печатается и считывается машинами, его обработка занимает гораздо меньше времени, а также позволяет достичь более высокой точности, чем ввод данных вручную. Считывание штрих-кода занимает только 0,3 секунды. При этом нормой является менее одной ошибки в каждом 1 000 000 считанных кодов.

2.1.1.3. Аппаратные средства считывания штрих-кодов

Для обработки штрих-кодов используются специальные приборы – сканеры, которые позволяют преобразовать информацию со штрих-кода в электронный вид, пригодный для обработки. Сканер штрих-кода – это устройство, которые считывает штрих-код, нанесенный на упаковку товара, и передает эту информацию в компьютер, кассовые аппараты, POS-терминалы. Сканер может иметь различные интерфейсы для подключения к компьютеру, помимо стандартизированных RS232, PS/2, USB могут использоваться собственный разъем и интерфейс производителя. По отношению к компьютеру сканеры с интерфейсами PS/2 и USB обычно выглядят как обычная клавиатура. В силу этого с ними не должно возникать проблем при работе в Unix-подобных операционных системах.

Модели, обладающие расширенной функциональностью, можно настраивать, изменяя их поведение. Сканеры с подобной функциональностью обычно называются программируемыми.

Все существующие технологии сканирования штрих-кодов основываются на едином принципе – подсветке штрих-кода и сборе отраженного света, который затем обрабатывается процессором. Некоторые модели обладают улучшенными возможностями для считывания поврежденных штрих-кодов.

Сканеры штрихового кода классифицируются:

- по типу подсветки штрихового кода – светодиодные, лазерные (однолучевые и многолучевые, с одним сканирующим окном и с двумя (биооптические)) и не требующие подсветки;
- по дальности считывания (лазерные) – с головками long (дальность до 10 м) и standard (до 60 см) range;

- по типу светоприемника – на ПЗС-матрице (ССD-сканеры) (контактные и бесконтактные) или на фотодиоде;
- по типу исполнения – мини-сканеры, карманные, ручные (общего и промышленного применения), стационарные и комбинированные (стационарные/ручные);
- по защищенности – офисные и промышленные;
- по способу соединения с компьютером – проводные и беспроводные;
- по непрерывности действия – с триггером (кнопкой) и без триггера;
- по типам считываемых штрих-кодов – одномерные (1D), двухмерные (2D).

Светодиодный сканер (ССD)

Наиболее известный способ сканирования, при котором используются дающие размытый неяркий луч светодиода. При помощи стеклянного зеркала отраженный свет собирается и проецируется на матрицу ПЗС. Параметры считывания при наличии качественного и достаточно контрастного штрих-кода – на расстоянии 2–3 см от контакта. Трудности возникают, если приходится считывать штрих-код с неровной (криволинейной) поверхности. Данная технология в последнее время используется лишь в самых недорогих сканерах. Впрочем, если объемы для сканирования небольшие, то сканер ССD себя оправдывает.

Лазерный сканер

Этой технологии почти четыре десятка лет, и изменений она практически не претерпела: луч используемого для подсветки лазерного диода развертывается с помощью механического элемента – качающегося зеркала. Главным достоинством данной технологии является возможность считывать штрих-код с большого расстояния – от одного до нескольких метров. А основной недостаток – возникают проблемы со считыванием, если штрих-код недостаточно хорошо пропечатан даже на небольшом участке. Ведь узкая линия, вырезаемая тонким лазерным лучом для анализа, может оказаться именно тем испорченным участком. Кроме того, высока вероятность сбоев в работе и механических повреждений из-за большого количества подвижных деталей в конструкции лазерного сканера, а это влечет за собой дорогостоящий ремонт.

Линейный фотосканер

Одна из последних на данный момент технологий сканирования линейного штрих-кода возникла в 1999 году. Она объединила в себе два безусловных преимущества ранее известных технологий – в конструкции этого сканера нет подвижных элементов, а считывание штрих-кода возможно с достаточно большого расстояния.

Благодаря тому, что широкая подсветка четко сфокусирована и с механической стороны линейный фотосканер ничем не ограничен:

- захватывается более широкая полоса на штрих-коде;

- низкоконтрастные и поврежденные коды больше не являются проблемой;
- скорость считывания достаточно высока;
- конструкция сканера более прочна в сравнении с прежними технологиями.

Таким образом, становится понятно, почему линейным фотосканерам удастся успешно вытеснить лазерные и светодиодные сканеры из области наиболее широкого использования, где необходимо точное считывание штрих-кода на расстоянии до одного метра. Практическое отсутствие недостатков, универсальность и отличные характеристики считывания штрих-кодов – достаточно веские причины популярности линейных фотосканеров.

Матричный фотосканер

В основу положена новейшая технология. Штрих-код рассматривается как картинка, изображение, которое можно фотографировать, в то время как в лазерной технологии и в сканерах ССД штрих-код рассматривался как информация, закодированная в штрихах.

При матричной технологии сфотографированные мини-камерой изображения обрабатываются мощным процессором и самыми современными и совершенными алгоритмами распознавания и декодировки. Поэтому возможности этих фотосканеров намного шире, чем у лазерных и светодиодных, а соответствует цене хорошего лазерного сканера.



Рис. 8. Мини-сканер



Рис. 9. Портативный сканер



Рис. 10. Ручной сканер общего применения



Рис. 11. Ручной сканер промышленного применения



Рис. 12. Стационарный сканер

В целом можно констатировать, что штрих-кодирование соответствует первому звену технологической цепочки Интернета вещей. Штрих-код позволяет определить объект внешней среды, данные о котором необходимо считать и интегрировать в информационное пространство. Тем не менее технологии Интернета вещей предполагают автономную работу без непосредственного участия человека, а большинство сканеров, использующихся для считывания информации со штрих-кода, могут работать только за счет ручной обработки оператором. Безусловно, технология штрих-кодирования сокращает издержки на ввод и обработку информации, однако отнести ее к полноценным технологиям Интернета вещей в большинстве случаев нельзя. Ее следует интерпретировать как переходную технологию, которая в дальнейшем может быть заменена иными технологическими решениями.

2.1.2. Радиочастотная идентификация

Радиочастотный мониторинг в общем смысле предполагает персональную маркировку объектов специальными радиометками для их последующей дистанционной идентификации. В связи с этим радиочастотный мониторинг также относится к первому звену технологической цепочки Интернета вещей. Сегодня именно штрих-коды и RFID-метки связывают реальные объекты с информационными ресурсами. Эти технологии можно отнести к базовому уровню Интернета вещей. Будучи технологиями, работающими на первой ступени идентификации, RFID-метки и штрих-коды позволяют идентифицировать физический объект в информационном пространстве. В некотором смысле обе технологии представляют собой мост между реальным и виртуальным мирами. Однако, в отличие от штрих-кодирования, радиочастотная идентификация предполагает гораздо большую автономность от операторов.

Любой объект физического мира, маркированный RFID-меткой, может быть отнесен к категории подключенных вещей. В пункте 1.2 данного исследования приводились критерии определения подключенных вещей, среди которых выделяют наличие уникальной идентификации, функцию памяти и свойство коммуникативности. В случае с радиочастотным мониторингом выполняются все перечисленные пункты, поскольку:

- RFID-метка обеспечивает физическому объекту уникальную идентификацию в информационном пространстве;
- RFID-метка обладает функцией памяти и способна транслировать определенный код;
- RFID-метка обладает свойством коммуникативности, поскольку способна взаимодействовать с другими устройствами.

История RFID ведет начало не, как это принято считать на Западе, от радиотехнического патента Г. Маркони 1902 года, а от работ 1895–1896 годов российского инженера-электрика А.С. Попова. Ближайшим аналогом радиочастотной идентификации является технология радиолокационного опознавания – активных ответчиков (авиационных, морских и ракетных). Принято считать, что первые системы радиолокационного опознавания появились во время Второй мировой войны практически одновременно в Германии, Великобритании, США и СССР (Ленинградский физико-технический институт, радиолокационная станция «Редут») ⁴⁹.

Первая демонстрация современных RFID-чипов (на эффекте обратного рассеяния), как пассивных, так и активных, была проведена в Исследовательской лаборатории Лос-Аламоса (англ. Los Alamos Scientific Laboratory) в 1973 году. Портативная система работала на частоте 915 МГц и использовала 12-битные метки.

Первый патент, связанный собственно с названием RFID, был выдан Чарльзу Уолтону (Charles Walton) в 1983 году (патент США за № 4,384,288).

RFID (англ. Radio Frequency IDentification, радиочастотная идентификация) – метод автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках.

Любая RFID-система состоит из считывающего устройства (считыватель, ридер или интеррогатор) и транспондера (он же RFID-метка, иногда также применяется термин RFID-тег).

Контроль за перемещением промаркированного объекта заключается в чтении данных RFID-метки в контрольных точках, для чего метке достаточно попасть в электромагнитное поле, создаваемое антенной, подключенной к считывателю. Информация из считывателя передается в систему управления и далее в учетную систему.

Большинство RFID-меток состоит из двух частей. Первая – интегральная схема (ИС) для хранения и обработки информации, модулирования и демодулирования радиочастотного (RF) сигнала и некоторых других функций. Вторая – антенна для приема и передачи сигнала.

Транспондер может быть интегрирован в переносимый объект, например в этикетку с клеевым слоем или в пластиковую карту. На чипе, как правило, записывается числовой код, обеспечивающий однозначную идентификацию объекта. Так, на него может быть записан

⁴⁹ Российская Академия Естествознания «Современные наукоемкие технологии» № 8 2009 г.

электронный код продукта ЕРС (Elektronische Produktcode), который используется для идентификации потребительских товаров. Код ЕРС содержит информацию о производителе, продукте, его версии, серийном номере и об упаковке продукта.

2.1.2.1. Состав RFID-системы

Метки (tag) RFID – устройства, способные хранить и передавать данные. В памяти меток содержится их уникальный идентификационный код. Некоторые метки имеют перезаписываемую память.

Считыватели (reader) – приборы, которые читают информацию с меток и записывают в них данные. Эти устройства могут как быть постоянно подключенными к учетной системе, так и работать автономно.

Учетная система – программное обеспечение, которое накапливает и анализирует полученную с меток информацию и связывает все элементы в единую систему. Большинство современных учетных систем (программы семейства 1С, корпоративные информационные системы – MS Axapta, SAP R3 и др.) уже совместимы с RFID-технологией и не требуют специальной доработки.

2.1.2.2. Классификация RFID-меток

Технология RFID может быть реализована во многих областях. Для того чтобы системы, основанные на этой технологии, эффективно работали в любой среде, было разработано множество меток самого различного исполнения. Их условно можно разделить по следующим признакам:

- по рабочей частоте;
- по источнику питания;
- по типу памяти;
- по исполнению.

По рабочей частоте

Сегодня RFID-системы используют четыре частотных диапазона: 125–150 кГц, 13,56 МГц, 862–950 МГц и 2,4–5 ГГц. Выбор этих диапазонов частот обуславливается тем, что для большинства стран только в этих диапазонах разрешено вести коммерческие разработки. Для примера отметим, что диапазон 2,45 ГГц – это частоты, на которых работают беспроводные устройства стандарта Bluetooth и Wi-Fi.

Для каждого из упомянутых частотных диапазонов действуют свои стандарты со своей степенью проработки.

По рабочей частоте RFID-метки делятся на:

- метки диапазона LF (125–134 кГц);
- метки диапазона HF (13,56 МГц);
- метки диапазона UHF (860–960 МГц);
- UHF-метки ближнего поля.

Метки диапазона LF (125–134 кГц)

Для диапазона частот 125–134 кГц действуют стандарты: ISO 14223, ISO 11784/11785, ISO 18000-2. Пассивные системы данного диапазона имеют низкие цены и в связи с физическими характеристиками используются в качестве подкожных меток при чипировании животных, людей и рыб. Однако в связи с длиной волны существуют проблемы со считыванием на большие расстояния, а также проблемы, связанные с появлением коллизий при считывании.



Рис. 13. Метка диапазона LF (125 кГц)

RFID-метки этого диапазона применяются в системах контроля доступа, для идентификации животных, а также достаточно широко используются, например, в автомобильных иммобилайзерах.

Метки диапазона HF (13,56 МГц)

Для частоты 13,56 МГц действуют стандарты: ISO 14443, ISO 15693, ISO 10373, ISO 18000-3. Системы 13 МГц дешевы, не имеют экологических и лицензионных проблем, хорошо стандартизованы, имеют широкую линейку решений. Применяются в платежных системах, логистике, идентификации личности. Для частоты 13,56 МГц разработан стандарт ISO 14443 (виды A/B), в котором, в отличие от Mifare 1K, обеспечена система диверсификации ключей, что позволяет создавать открытые системы. Используются стандартизованные алгоритмы шифрования.

Как и для диапазона LF, в системах, построенных в HF-диапазоне, существуют проблемы со считыванием на большие расстояния, считыванием в условиях высокой влажности, наличия металла, а также проблемы, связанные с появлением коллизий при считывании.

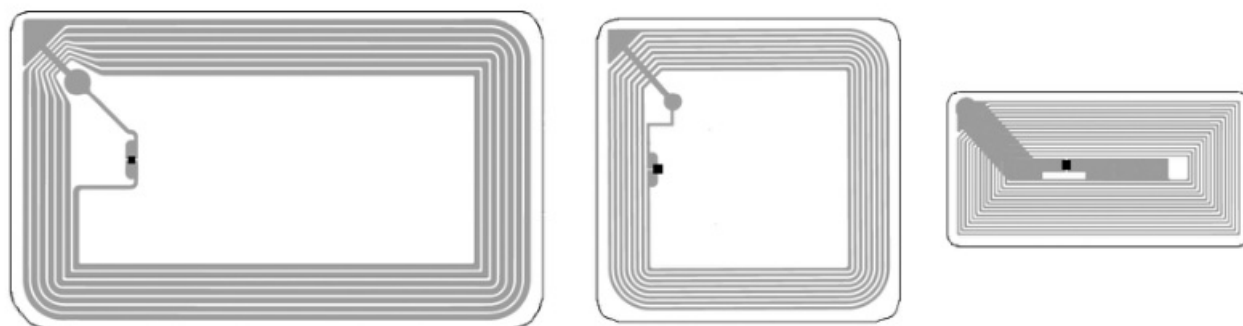


Рис. 14. Метки диапазона HF

Применяются в системах контроля доступа, платежных системах, а также для идентификации товаров в складских системах и книг в библиотечных системах.

Метки диапазона UHF (860–960 МГц, 2,4–5 ГГц)

Для диапазона частот 860–960 МГц и 2,4–5 ГГц действуют стандарты: U-CODE 18000-4, 18000-6. Метки сверхвысокочастотного диапазона обладают наибольшей дальностью регистрации, во многих стандартах данного диапазона присутствуют антиколлизсионные механизмы. В UHF RFID-системах по сравнению с LF и HF ниже стоимость меток, при этом выше стоимость прочего оборудования. В настоящее время частотный диапазон СВЧ открыт для свободного использования в Российской Федерации в так называемом «европейском» диапазоне – 863–868 МГц.

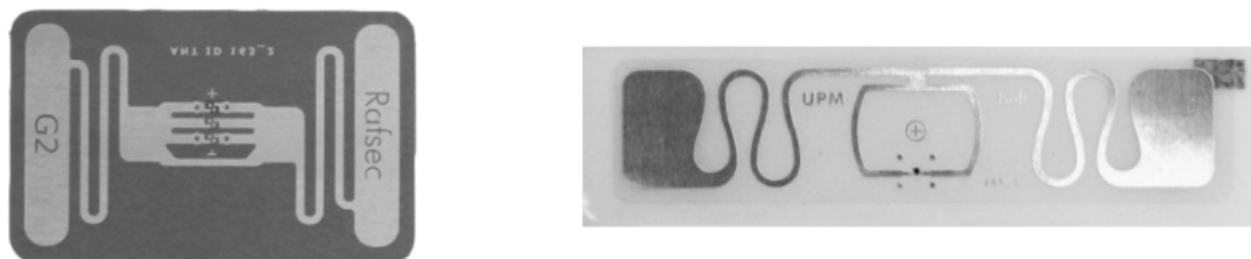


Рис. 15. Метки диапазона UHF

Областью применения являются системы логистики и учета движения транспорта. Отличительной особенностью является повышенная дальность и высокая скорость чтения.

Радиочастотные UHF-метки ближнего поля

Метки ближнего поля (англ. UHF Near-Field), не являясь непосредственно радиометками, а используя магнитное поле антенны, позволяют решить проблему считывания в условиях высокой влажности, в возможном присутствии воды и металла. С помощью данной технологии ожидается начало массового применения RFID-меток в розничной торговле фармацевтическими товарами (нуждающимися в контроле подлинности, учете, но при этом зачастую содержащими воду и металлические детали в упаковке).

По источнику питания

По типу источника питания RFID-метки делятся на:

- пассивные;
- активные;
- полупассивные.

Пассивные RFID-метки

Пассивные RFID-метки не имеют встроенного источника энергии. Электрический ток, индуцированный в антенне электромагнитным сигналом от считывателя, обеспечивает достаточную мощность для функ-

ционирования кремниевого CMOS-чипа, размещенного в метке, и передачи ответного сигнала.

В 2006 году компания Hitachi изготовила пассивное устройство, названное μ -Chip (мю-чип), размерами $0,15 \times 0,15$ мм (не включая антенну) и тоньше бумажного листа (7,5 мкм). Такого уровня интеграции позволяет достичь технология «кремний-на-изоляторе» (SOI). μ -Chip может передавать 128-битный уникальный идентификационный номер, записанный в микросхему на этапе производства. Данный номер не может быть изменен в дальнейшем, что гарантирует высокий уровень достоверности и означает, что этот номер будет жестко привязан (ассоциирован) с тем объектом, к которому присоединяется или в который встраивается этот чип. μ -Chip от Hitachi имеет типичный радиус считывания 30 см (1 фут). В феврале 2007 года Hitachi представила RFID-устройство, обладающее размерами $0,05 \times 0,05$ мм и толщиной, достаточной для встраивания в лист бумаги.

Компактность RFID-меток зависит от размеров внешних антенн, которые по размерам превосходят чип во много раз и, как правило, определяют габариты меток. Наименьшая стоимость RFID-меток составляет примерно 5 центов за метку фирмы SmartCode (при покупке от 100 млн штук). Эти метки стали стандартом для таких компаний, как Wal-Mart, Target, Tesco в Великобритании, Metro AG в Германии, и Министерства обороны США. К тому же из-за разброса размеров антенн метки имеют различные размеры – от почтовой марки до открытки. На практике максимальная дистанция считывания пассивных меток варьируется от 10 см (4 дюймов) (согласно стандарту ISO 14443) до нескольких метров (стандарты EPC и ISO 18000-6) в зависимости от выбранной частоты и размеров антенны. В некоторых случаях антенна может быть изготовлена печатным способом.

Производственные процессы от Alien Technology под названием Fluidic Self Assembly, от SmartCode – Flexible Area Synchronized Transfer (FAST) и от Symbol Technologies – PICA направлены на дальнейшее уменьшение стоимости меток за счет применения массового параллельного производства. Alien Technology в настоящее время использует процессы FSA и HiSam для изготовления меток, в то время как PICA – процесс от Symbol Technologies – находится еще на стадии разработки. Процесс FSA позволяет производить свыше 2 млн ИС пластин в час, а PICA процесс – более 70 млрд меток в год (если его доработают). В этих технических процессах ИС присоединяются к пластинам меток, которые в свою очередь присоединяются к антеннам, образуя законченный чип. Присоединение ИС к пластинам и в дальнейшем пластин к антеннам – самые пространственно чувствительные элементы процесса производства. Это значит, что при уменьшении размеров ИС монтаж станет самой дорогой операцией. Альтернативные методы производства, такие как FSA и HiSam, могут значительно уменьшить себестоимость меток. Стандартизация производства в конечном счете приведет к дальнейшему падению цен на метки при их широкомасштабном внедрении.

Некремниевые метки могут изготавливаться из полимерных полупроводников. В настоящее время их разработкой занимаются несколько компаний по всему миру. Метки, изготавливаемые в лабораторных условиях и работающие на частоте 13,56 МГц, были продемонстрированы в 2005 году компаниями PolyIC (Германия) и Philips (Голландия). В промышленных условиях полимерные метки будут изготавливаться методом прокатной печати (технология напоминает печать журналов и газет), в результате чего они будут дешевле, чем метки на основе ИС. В конечном счете это может закончиться тем, что для большинства сфер применения метки станут печатать так же просто, как и штрих-коды, и они станут такими же дешевыми.

Пассивные метки УВЧ- и СВЧ-диапазонов (860–960 МГц и 2,4–2,5 ГГц) передают сигнал методом модуляции отраженного сигнала несущей. Антенна считывателя излучает сигнал несущей частоты и принимает отраженный от метки модулированный сигнал. Пассивные метки ВЧ-диапазона передают сигнал методом модуляции нагрузки сигнала несущей частоты. Каждая метка имеет идентификационный номер. Пассивные метки могут содержать перезаписываемую энергонезависимую память EEPROM-типа.

Активные RFID-метки

Активные RFID-метки обладают собственным источником питания и не зависят от энергии считывателя, вследствие чего они читаются на дальнем расстоянии, имеют большие размеры и могут быть оснащены дополнительной электроникой. Однако такие метки наиболее дороги, а у батарей ограничено время работы.

Активные метки в большинстве случаев более надежны и обеспечивают самую высокую точность считывания на максимальном расстоянии. Активные метки, обладая собственным источником питания, также могут генерировать выходной сигнал большего уровня, чем пассивные, позволяя применять их в более агрессивных для радиочастотного сигнала средах: воде (включая людей и животных, которые в основном состоят из воды), металлах (корабельные контейнеры, автомобили), для больших расстояний на воздухе. Большинство активных меток позволяет передать сигнал на расстояния в сотни метров при жизни батареи питания до 10 лет. Некоторые RFID-метки имеют встроенные сенсоры, например для мониторинга температуры скоропортящихся товаров. Другие типы сенсоров в совокупности с активными метками могут применяться для измерения влажности, регистрации толчков/вибрации, света, радиации, температуры и газов в атмосфере (например, этилена).

Активные метки обычно имеют гораздо больший радиус считывания (до 300 м) и объем памяти, чем пассивные, и способны хранить большой объем информации для отправки приемопередатчиком. В настоящее время активные метки делают размерами не больше обычной пилюли и продают по цене в несколько долларов.



Рис. 16. Активные RFID-метки

Полупассивные RFID-метки

Полупассивные RFID-метки, также называемые полуактивными, очень похожи на пассивные метки, но оснащены батареей, которая обеспечивает чип энергопитанием. При этом дальность действия этих меток зависит не только от чувствительности приемника считывателя, и они могут функционировать на большем расстоянии и с лучшими характеристиками, чем пассивные метки.

По типу памяти

По типу используемой памяти RFID-метки делятся на:

- RO-rfid метки – только чтение (Read Only – RO). Метки с типом памяти Read Only записываются сразу при изготовлении, Такие метки пригодны только для идентификации. Никакую новую информацию в них записать нельзя, и их практически невозможно подделать.
- WORM-rfid метки – однократная запись и многократное чтение (Write Once Read Many – WORM). Метки с типом памяти Write Once Read Many помимо уникального идентификатора содержат блок однократно записываемой памяти, который потом можно многократно считывать.
- RW-rfid метки – чтение и перезапись (Read and Write). Метки с типом памяти Read and Write помимо уникального идентификатора содержат блок памяти для многократного чтения и перезаписи.

По исполнению

По исполнению RFID-метки делятся на:

- жесткие, в виде пластиковых карточек, бейджей, брелоков, колец или имеющие специальный корпус для особых условий эксплуатации;
- мягкие, в виде тонких пластиковых карточек, этикет-ленты, на которой можно наносить печатную информацию с помощью специальных принтеров (с клеевым слоем и без);
- в виде электронных радиочастотных пломб.

2.1.2.3. Считыватели RFID

Приборы для считывания данных с меток также бывают нескольких типов. По исполнению считыватели делятся на стационарные и переносные.

Стационарные считыватели

Стационарные считыватели крепятся неподвижно на стенах, порталах и в других подходящих местах. Они могут быть выполнены в виде ворот, вмонтированы в стол или закреплены рядом с конвейером на пути следования изделий.

По сравнению с переносными стационарные считыватели обычно обладают большей зоной чтения и мощностью и способны одновременно обрабатывать данные с нескольких десятков меток. Стационарные считыватели обычно напрямую подключены к компьютеру, на котором установлена программа контроля и учета. Задача таких считывателей – поэтапно фиксировать перемещение маркированных объектов в реальном времени.



Рис. 17. Стационарные считыватели на 8 антенн

Антенны

Антенна является важнейшим элементом RFID-системы.

Все выпускаемые антенны можно классифицировать:

- по дальности действия (короткого, среднего и дальнего радиуса);
- по исполнению (настольные, стационарные и порталные);
- по направлению поляризации (левосторонняя, правосторонняя, двухсторонняя);
- по скорости работы (обычные, быстродействующие).

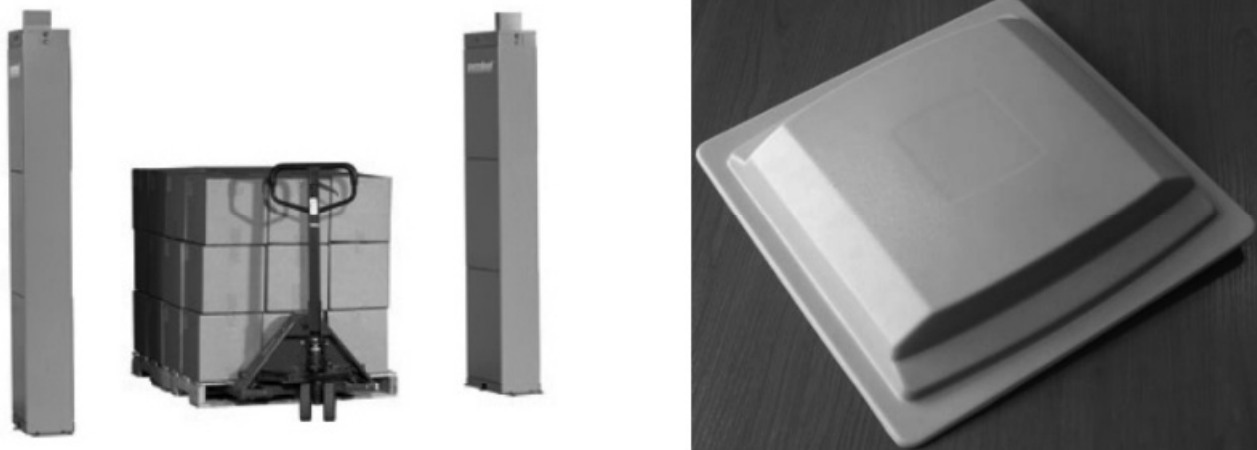


Рис. 18. Стационарные антенны

Переносные считыватели

Обладают сравнительно меньшей дальностью действия и зачастую не имеют постоянной связи с программой контроля и учета. Мобильные считыватели имеют внутреннюю память, в которую записываются данные с прочитанных меток (потом эту информацию можно загрузить в компьютер), и, так же как и стационарные считыватели, способны записывать данные на метку (например, информацию о произведенном контроле).

В зависимости от частотного диапазона метки дистанция устойчивого считывания и записи данных в них будет различна.

Переносные считыватели RFID-меток делятся на ручные и мобильные.

Ручные считыватели

Как правило, такие считыватели совмещены с терминалами сбора данных. Обладают меньшей дальностью действия (чтения и записи) поскольку ограничены мощностью источника питания. При наличии в терминале сбора данных беспроводной связи может быть постоянный обмен данными с учетной системой.



Рис. 19. Ручные считыватели

Ручные считыватели способны также записывать данные в метку (например, информацию о произведенной операции).

Мобильные считыватели

Поскольку такие считыватели имеют более мощный источник питания, то дальность и скорость чтения у них больше, чем у ручных. При этом они также могут быть оснащены беспроводной связью, обеспечивая работу в режиме реального времени.



Рис. 20. Мобильные считыватели

2.1.2.4. Преимущества радиочастотной идентификации

Возможность перезаписи. Данные RFID-метки могут перезаписываться и дополняться много раз, тогда как данные на штрих-коде не могут быть изменены – они записываются сразу при печати.

Отсутствие необходимости в прямой видимости. RFID-считывателю не требуется прямая видимость метки, чтобы считать ее данные. Взаимная ориентация метки и считывателя часто не играет роли. Метки могут читаться через упаковку, что делает возможным их скрытое размещение. Для чтения данных метке достаточно хотя бы ненадолго попасть в зону регистрации, перемещаясь, в том числе и на довольно большой скорости. Напротив, устройству считывания штрих-кода всегда необходима прямая видимость штрих-кода для его чтения.

Большее расстояние чтения. RFID-метка может считываться на значительно большем расстоянии, чем штрих-код. В зависимости от модели метки и считывателя радиус считывания может составлять до нескольких сотен метров. В то же время подобные расстояния требуются не всегда.

Большой объем хранения данных. RFID-метка может хранить значительно больше информации, чем штрих-код. На микросхеме площадью в 1 см^2 может храниться до 10 000 байт информации, в то время как штриховые коды могут вместить 100 байт (знаков) информации, для воспроизведения которых понадобится площадь размером с лист формата А4.

Поддержка чтения нескольких меток. Промышленные считыватели могут одновременно считывать множество (более тысячи) RFID-меток в секунду, используя так называемую антиколлизийную функцию. Устройство считывания штрих-кода может одновременно сканировать только один штрих-код.

Считывание данных метки при любом ее расположении. В целях обеспечения автоматического считывания штрихового кода комите-

ты по стандартам (в том числе EAN International) разработали правила размещения штрих-меток на товарной и транспортной упаковке. К радиочастотным меткам эти требования не относятся. Единственное условие – нахождение метки в зоне действия считывателя.

Устойчивость к воздействию окружающей среды. Существуют RFID-метки, обладающие повышенной прочностью и сопротивляемостью жестким условиям рабочей среды, а штрих-код легко повреждается (например, влагой или загрязнением). В тех сферах применения, где один и тот же объект может использоваться неограниченное количество раз (например, при идентификации контейнеров или возвратной тары), радиочастотная метка оказывается более приемлемым средством идентификации, так как ее не требуется размещать на внешней стороне упаковки. Пассивные RFID-метки имеют практически неограниченный срок эксплуатации.

Интеллектуальное поведение. RFID-метка может использоваться для выполнения других задач, помимо функции носителя данных. Штрих-код же непрограммируем и является лишь средством хранения данных.

Высокая степень безопасности. Уникальное неизменяемое число-идентификатор, присваиваемое метке при производстве, гарантирует высокую степень защиты меток от подделки. Также данные на метке могут быть зашифрованы. Радиочастотная метка обладает возможностью закрыть паролем операции записи и считывания данных, а также зашифровать их передачу. В одной метке можно одновременно хранить открытые и закрытые данные.

2.1.2.5. Недостатки радиочастотной идентификации

При работе с радиочастотной идентификацией необходимо учитывать некоторые недостатки и ограничения технологии. К ним относятся: относительно высокая стоимость; невозможность размещения под металлическими и экранирующими поверхностями; взаимные коллизии; подверженность помехам в виде электромагнитных полей.

Относительно высокая стоимость меток. Стоимость пассивной радиочастотной метки составляет от 0,15 доллара (при приобретении свыше 1 000 000 шт.) до 3 долларов (при приобретении 1 шт.). В случае с метками защищенного исполнения (или на металл) эта цена может достигать 7 и более долларов. Таким образом, стоимость RFID-меток превышает стоимость этикеток со штриховым кодом. Исходя из этого, использование радиочастотных меток целесообразно для защиты дорогих товаров от краж или для обеспечения сохранности изделий, переданных на гарантийное обслуживание. В сфере логистики и транспортировки грузов стоимость радиочастотной метки оказывается совершенно незначительной по сравнению со стоимостью содержимого контейнера, поэтому совершенно оправданно использование радиочастотных меток на упаковочных ящиках, паллетах и контейнерах.

Возможное экранирование при размещении на металлических поверхностях. Радиочастотные метки подвержены влиянию металла (это касается упаковок определенного вида – металлических контейнеров, иногда даже некоторых типов упаковки жидких пищевых продуктов, запечатанных фольгой). Это вовсе не исключает применение RFID, но приводит или к необходимости использования более дорогих меток, разработанных специально для установки на металлические поверхности, или к нестандартным способам закрепления меток на объекте.

Подверженность систем радиочастотной идентификации помехам в виде электромагнитных полей от включенного оборудования, излучающего радиопомехи в диапазоне частот, используемом для работы RFID-системой. Необходимо тщательно проанализировать условия, в которых система RFID будет эксплуатироваться. Для систем UHF диапазона 868–869 МГц это практически не актуально (в этом диапазоне никакие другие приборы не работают), но низкочастотные метки, работающие на частоте 125 кГц, подобному влиянию подвержены.

2.1.3. Особенности технологий RFID и штрихового кодирования

По функциональности RFID-метки как метод сбора информации очень близки к штрих-кодам, наиболее широко применяемым сегодня для маркировки товаров. Несмотря на удешевление стоимости RFID-метки, в обозримом будущем полное вытеснение штрих-кодов радиочастотной идентификацией вряд ли состоится по экономическим причинам (система не будет окупаться).

Технология штрихового кодирования появилась сравнительно давно по сравнению с RFID и получила широкое распространение по всему миру, в основном благодаря своей простоте и низкой стоимости. Однако для целого ряда областей эта технология оказывается нерезультативной, особенно там, где требуются контроль перемещения объектов в реальном времени, интеллектуальные решения автоматизации, способность работать в жестких условиях эксплуатации и нечто большее, чем бездумная маркировка объектов. Все это проблемы, которые RFID может решить гораздо эффективней.

В то же время и сама технология штрих-кодов продолжает развиваться. Новые разработки (например, двухмерный штрих-код Data Matrix) решают ряд проблем, ранее решавшихся лишь применением RFID. Технологии могут дополнять друг друга. Компоненты с неизменными потребительскими свойствами могут маркироваться неизменными данными на основе оптических технологий распознавания, несущими информацию об их дате выпуска и потребительских свойствах, а на RFID-метку можно записать информацию, подверженную изменению, такую как данные о конкретном получателе заказа на возвращаемой многоразовой упаковке.

**Сравнительная характеристика технологии
RFID и штрихового кодирования**

Характеристики технологии	RFID	Штрих-код
Необходимость в прямой видимости метки	Чтение даже скрытых меток	Чтение без прямой видимости невозможно
Объем памяти	От 10 до 10 000 байт	До 100 байт
Возможность перезаписи данных и многократного использования метки	Есть	Нет
Дальность регистрации	До 100 м	До 4 м
Одновременная идентификация нескольких объектов	До 200 меток в секунду	Невозможна
Устойчивость к воздействиям окружающей среды: механическому, температурному химическому, влаге	Повышенная прочность и сопротивляемость	Зависит от материала, на который наносится
Срок жизни метки	Более 10 лет	Зависит от способа печати и материала, из которого состоит отмечаемый объект, а также условий использования
Безопасность и защита от подделки	Подделка практически невозможна	Подделать легко
Работа при повреждении метки	Невозможна	Затруднена
Идентификация движущихся объектов	Да	Затруднена
Подверженность помехам в виде электромагнитных полей	Есть	Нет
Идентификация металлических объектов	Возможна	Возможна

Использование как стационарных, так и ручных терминалов для идентификации	Да	Да
Возможность введения в тело человека или животного	Возможно	Затруднено
Габаритные характеристики	Средние и малые	Малые
Стоимость	Средняя и высокая	Низкая

При выборе технологии для использования в каждом конкретном случае, необходимо учитывать, что:

- стоимость RFID выше стоимости системы учета, основанной на штрих-кодах;
- RFID-метки сложно самостоятельно изготовить, в то время как штрих-код можно напечатать на любом принтере.
- установленная техническая база для считывания штрих-кодов существенно превосходит по объему решения на основе RFID.

Таким образом, при построении сложных систем контроля и учета большого числа неоднородных объектов наиболее предпочтительным видится дифференцированный подход, предусматривающий комплексное использование технологий штрихового кодирования и радиочастотной идентификации.

2.2. Датчики и сенсоры Интернета вещей

По мере развития средств виртуальной идентификации физических объектов постепенно набирает актуальность вопрос создания точных сканеров и датчиков, способных работать в рамках концепции Интернета вещей. Аппаратная интерпретация исследуемой концепции подразумевает, что Интернет вещей – это совокупность устройств, способных фиксировать информацию о реальном мире и обрабатывать ее без непосредственного участия человека. Очевидно, что фиксирование информации и ее начальная обработка выполняются устройствами, известными каждому под названиями «датчики» и «сенсоры».

2.2.1. Различия между датчиками и сенсорами

Для более точного понимания различий между датчиками и сенсорами необходимо рассмотреть пирамиду превращения данных в «мудрость», предложенную компанией Cisco⁵⁰.

⁵⁰ Daly J. What Is the Internet of Things? // STATETECHMAGAZINE.COM : Technology Insights for Leaders in State & Local Government. 2013. URL: <http://www.statetechmagazine.com/article/2013/08/what-is-the-internet-of-things> (дата обращения 27.03.2014).



Рис. 21. Пирамида движения от данных к «мудрости»

Предполагается, что процесс познания окружающего мира начинается со сбора данных. Данные – это сырой материал, который необходимо обработать, прежде чем станет доступной информация. Человек, наблюдающий показания термометра, получает данные, а не информацию, поскольку эти показания не пригодны к дальнейшей обработке. Их необходимо зафиксировать и сохранить на физический носитель. Только после этого данные станут информацией, пригодной для передачи, хранения и дальнейшей обработки.

Кроме того, единичные данные не являются достаточно полезными. Для того чтобы извлечь из данных какую-либо пользу, нужно собрать достаточно большой объем данных. Сделать это без превращения данных в информацию зачастую невозможно. Действительно, сложно представить человека, который ежедневно смотрит термометр, не фиксируя при этом информацию, а затем получает знание о температурных циклах в данной местности.

Превращение информации в знание обусловлено тем, что для изучения объекта внешнего мира зачастую недостаточно информации о каком-то одном его параметре. Как правило, для этого требуется совокупность нескольких пластов информации. А «мудрость» в терминах Cisco возникает, когда знание об объекте сочетается с опытом его применения.

Ключевое различие между датчиками и сенсорами заключается в том, на каком из уровней пирамиды они работают. Датчик работает на уровне данных, поскольку его выходной «продукт» – сигнал о каком-либо свойстве объекта внешней среды. В свою очередь, сенсор работает на уровне информации, его выходной «продукт» – информация, возникшая путем трансформации собранных данных в удобную для хранения и обработки форму.

Интересным кажется и вопрос интерпретации подключенных датчиков в рамках концепции Интернета вещей. Можно сказать, что датчики представляют собой своеобразную переходную форму между подключенной вещью и подключенным устройством. Как и подключенная вещь, датчик внутри сети объектов Интернета вещей соответствует критериям наличия личного уникального адреса, функции памяти и свой-

ства коммуникативности. Однако, в отличие от подключенной вещи, датчик обладает способностью воспринимать информацию об окружающем мире. Тем не менее датчик не может называться полноценным подключенным устройством, поскольку он не способен проводить даже минимальную обработку полученных данных. Это обуславливает основное различие между датчиками и сенсорами. Датчики позволяют получить данные как таковые, которые еще не встроены в информационное пространство. А сенсор способен произвести непосредственно информацию, к которой далее могут быть применены какие-либо алгоритмы хранения, обработки и передачи.

С другой стороны, неспособность датчика самостоятельно обрабатывать входные данные компенсируется другими устройствами, которые входят в одну с ним сеть подключенных объектов. Обработку может взять на себя другой узел сети объектов Интернета вещей, тем самым сохраняя базовые принципы исследуемой концепции. Таким образом, датчики можно отнести к категории подключенных устройств, пусть и с некоторой натяжкой за счет компенсации последнего критерия иными устройствами.

Таблица 7

Сравнение датчиков и сенсоров

	Датчик	Сенсор
Выходной «продукт»	Данные	Информация
Категория в концепции Интернета вещей	Промежуточное состояние между подключенной вещью и подключенным устройством	Подключенное устройство

Сенсоры, относящиеся к сетям Интернета вещей, полностью соответствуют критериям определения подключенных устройств. Они обладают всеми вышеперечисленными функциями и способны преобразовывать входящие данные в информацию, пригодную для дальнейших действий с ней.

2.2.2. Функции и разновидности датчиков и сенсоров

Прежде всего необходимо внести разграничение между понятиями «сенсор» и «датчик». Под датчиком традиционно понимается устройство, способное преобразовать входное воздействие любой физической величины в сигнал, удобный для дальнейшего использования⁵¹. Сегодня существует ряд требований, предъявляемых к современным датчикам:

- Однозначная зависимость выходной величины от входной.
- Стабильные показания независимо от времени использования.
- Высокий показатель чувствительности.

⁵¹ Классификация датчиков, основные требования к ним // ELECTROLIBRARY.INFO : Избранные материалы рассылки. URL: http://www.electrolibrary.info/subscribe/sub_16_datchiki.htm (дата обращения 27.03.2014).

- Небольшие размеры и малая масса.
- Отсутствие воздействия датчика на контролируемый процесс.
- Возможность работы в различных условиях.
- Совместимость с другими устройствами.

Любой датчик включает в себя следующие элементы: чувствительный элемент и сигнализатор⁵². В ряде случаев могут добавляться усилитель и селектор сигналов, но зачастую потребность в них отсутствует. Составные части датчика обуславливают и принцип его дальнейшей работы. В тот момент, когда в объекте наблюдения происходят какие-либо изменения, их фиксирует чувствительный элемент. Сразу после этого изменения отображаются на сигнализаторе, данные которого объективны и информативны, но не могут быть обработаны автоматически.

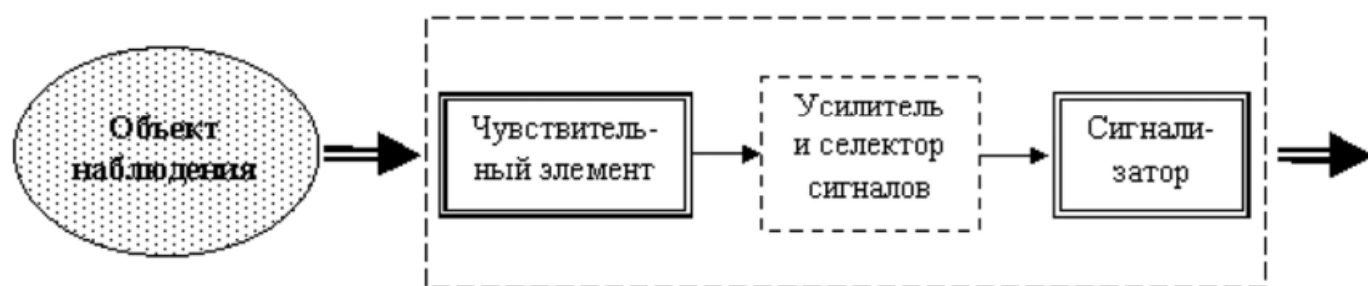


Рис. 22. Схема работы датчика

Примером простейшего датчика может служить ртутный термометр. В качестве чувствительного элемента используется ртуть, температурная шкала исполняет роль сигнализатора, а объектом наблюдения является температура. При этом важно понимать, что показания датчика представляют собой набор данных, а не информацию. Они не сохраняются во внешнюю или внутреннюю память и не пригодны для автоматизированной обработки, хранения и передачи.

Все датчики, использующиеся различными технологическими решениями из сферы Интернета вещей, можно разделить на несколько категорий. Основанием одной из самых удобных классификаций служит назначение устройств⁵³:

- датчики присутствия и движения;
- детекторы положения, перемещения и уровня;
- датчики скорости и ускорения;
- датчики силы и прикосновения;
- датчики давления;
- расходомеры;
- акустические датчики;
- датчики влажности;

⁵² Интеллектуальные сенсоры // INTUIT.RU. 2014. URL: <http://www.intuit.ru/studies/courses/590/446/info> (дата обращения 27.03.2014).

⁵³ Датчики и интеллектуальные сенсоры : [Электронный документ] // RFE.BY : Факультет радиофизики и компьютерных технологий БГУ, Минск. Сис. требования: Adobe Reader. URL: <http://www.rfe.by/media/kafedry/kaf5/publikation/kozlova/metrologia1/present13-14.pdf> (дата обращения 27.03.2014).

- детекторы световых излучений;
- датчики температуры;
- химические и биологические датчики.

Работа сенсоров серьезно отличается от работы датчиков. Прежде всего необходимо остановиться на определении понятия «сенсор». Под сенсором понимается устройство, способное преобразовать изменения, произошедшие в объекте наблюдения, в информационный сигнал, пригодный к дальнейшему хранению, обработке и передаче⁵⁴.

Схема работы сенсора близка к цепочке, характерной для датчика. В определенном смысле сенсор может трактоваться как улучшенный датчик, поскольку его структура может быть выражена в виде «составные элементы датчика» + «узел обработки информации». Функциональная схема сенсора выглядит следующим образом⁵⁵.

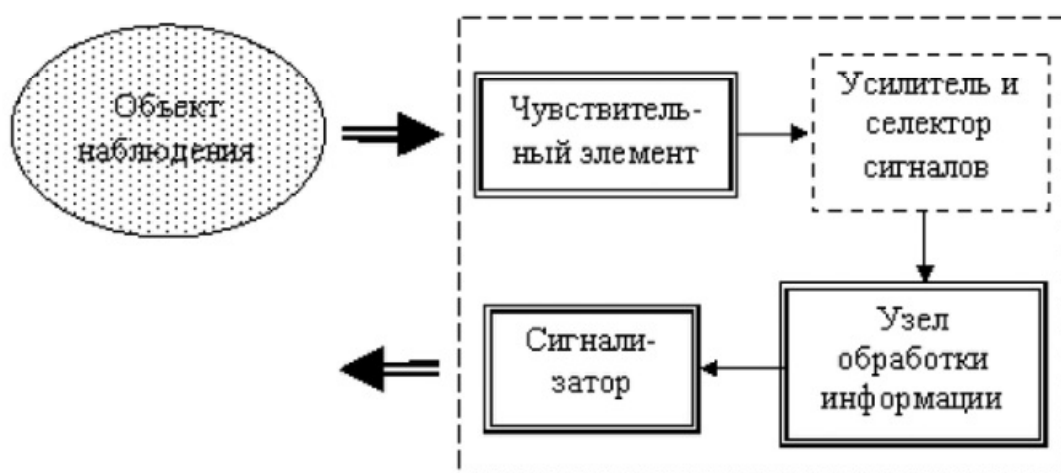


Рис. 23. Схема работы сенсора

При этом классификация сенсоров по назначению эквивалентна такой же классификации для датчиков. Нередко сенсоры и датчики могут измерять одну и ту же величину у одного и того же объекта, но датчики будут демонстрировать данные, а сенсоры – еще и преобразовывать их в информационный сигнал.

Кроме того, существует особый тип сенсоров, который имеет смысл рассмотреть для понимания концепции Интернета вещей. Это так называемые «умные» сенсоры, функциональная схема которых дополняется наличием алгоритмов для первичной обработки собранной информации. Таким образом, обычный сенсор способен обработать данные и предоставить их в виде информации, а «умный» сенсор способен производить какие-либо действия с самостоятельно захваченной информацией из внешней среды.

В будущем можно ожидать серьезного развития 3D-сенсоров, способных с высокой точностью сканировать окружающее пространство и строить его виртуальную модель⁵⁶. Так, в настоящий момент сенсор Capri 3D способен определять движения людей и их метрические харак-

⁵⁴ Там же.

⁵⁵ Интеллектуальные сенсоры // INTUIT.RU. 2014. URL: <http://www.intuit.ru/studies/courses/590/446/info> (дата обращения 27.03.2014).

⁵⁶ URL: <http://habrahabr.ru/post/179911/> (дата обращения 27.03.2014).

теристики. Кроме того, данный сенсор может отсканировать объект внешней среды и сохранить информацию в CAD-файле для дальнейшей отправки на печать на 3D-принтере.



Рис. 24. Сенсор Capri 3D, подключенный к Samsung Nexus 10

Особого внимания заслуживает развитие устройств, сочетающих в себе сразу несколько сенсоров разного типа. Как говорилось в пункте 2.2.1, для получения знания необходима информация о разных характеристиках объекта. А использование разных сенсоров позволяет получить необходимую информацию. В некотором смысле такие устройства действительно могут узнавать людей. Примером подобного устройства может служить беспроводной контроллер Kinect, использующийся в современных видеоиграх.

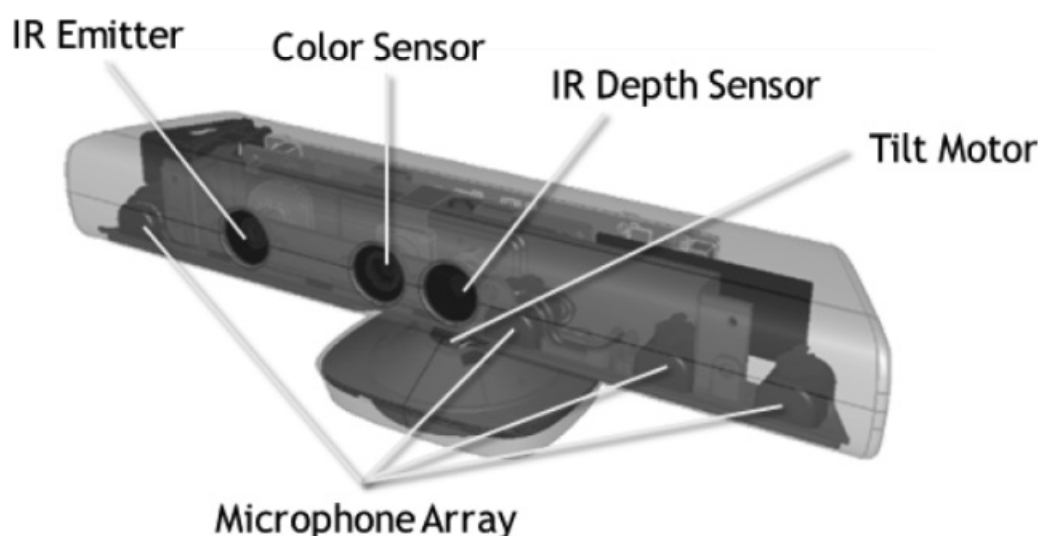


Рис. 25. Устройство беспроводного контроллера Kinect⁵⁷

Контроллер Kinect содержит в себе сразу несколько компонентов:

- инфракрасный излучатель;
- инфракрасный приемник;
- цветная камера;
- набор из 4 микрофонов и обработчика звукового сигнала;
- средство коррекции наклона.

⁵⁷ URL: <http://habrahabr.ru/post/150955/> (дата обращения 27.03.2014).

Принцип работы контроллера Kinect достаточно прост. Лучи, вышедшие из инфракрасного излучателя, отражаются и попадают в инфракрасный приемник. За счет этого удастся получить информацию о пространственном положении человека, который играет в видеоигру. Камера способна зафиксировать различные цветные данные, а микрофоны в состоянии улавливать голосовые команды игрока. В итоге контроллер оказывается в состоянии собрать достаточный объем информации о человеке, чтобы тот мог управлять игрой посредством движений или голосовых команд.

В определенном смысле контроллер Kinect относится к сфере технологий Интернета вещей. Он способен идентифицировать игрока, собрать информацию о нем и передать другим устройствам (игровой приставке). Но подобный набор сенсоров потенциально может использоваться и в других перспективных для концепции Интернета вещей областях, включая сферу развертывания технологий «умного» дома.

2.2.3. Датчики и сенсоры в концепции «умного» дома

Считается, что в будущем концепция «умного» дома станет одним из самых массовых проявлений Интернета вещей. «Умный» дом, соответствующий второму уровню архитектуры Интернета вещей, позволяет улучшить условия жизни людей и оптимизировать их затраты на воду, отопление и освещение, снизить потребление энергии, а также существенно повысить уровень безопасности. Подобный эффект достигается, в первую очередь, за счет массового использования разнообразных датчиков, сенсоров и контроллеров.

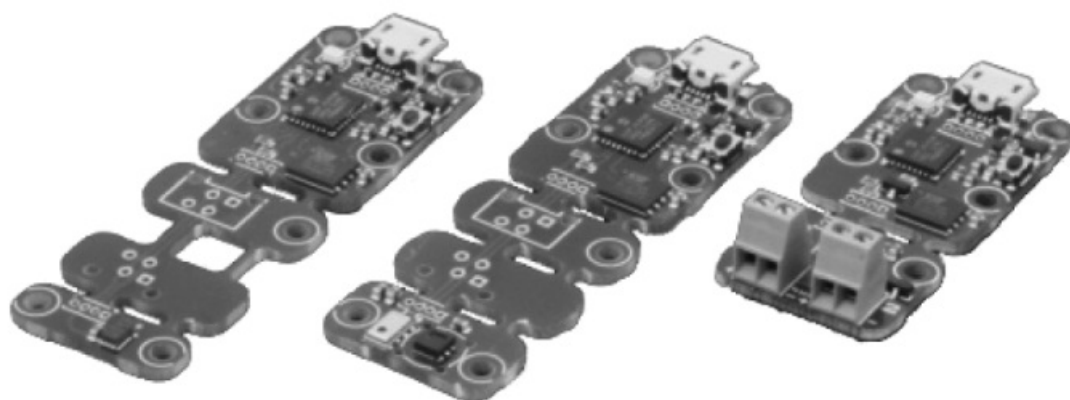


Рис. 26. Температурный сенсор Yoctopus для «умного» дома с возможностью USB-подключения

2.2.3.1. Датчики падения и запроса помощи

Одним из перспективных направлений развития датчиков и сенсоров, относящихся к сфере Интернета вещей, можно считать устройства, обеспечивающие безопасность пенсионеров и маломобильных групп населения. Ситуация такова, что для определенных групп населения падение в собственном доме может закончиться серьезной травмой. Кроме того, в некоторых случаях люди не в состоянии самостоятельно

вызвать помощь. В практике социальных работников нередко встречается случай, когда пенсионерам приходилось провести на полу всю ночь, поскольку они не могли ни подняться, ни оповестить родственников или экстренные службы о падении.

Одним из вариантов решения обозначенной проблемы может считаться автоматическое средство Safe@Home System⁵⁸. Принцип работы данной системы достаточно прост. В каждой комнате пожилого или маломобильного человека устанавливается система с несколькими сенсорами – оптическими и акустическими. Сенсоры способны воспринимать положение человека в комнате. Если система обнаруживает факт падения человека или фиксирует запрос о помощи, то включается внутренний таймер. Если в течение определенного времени человек не сможет встать самостоятельно, то сигнал будет передан на системный блок CareBox.

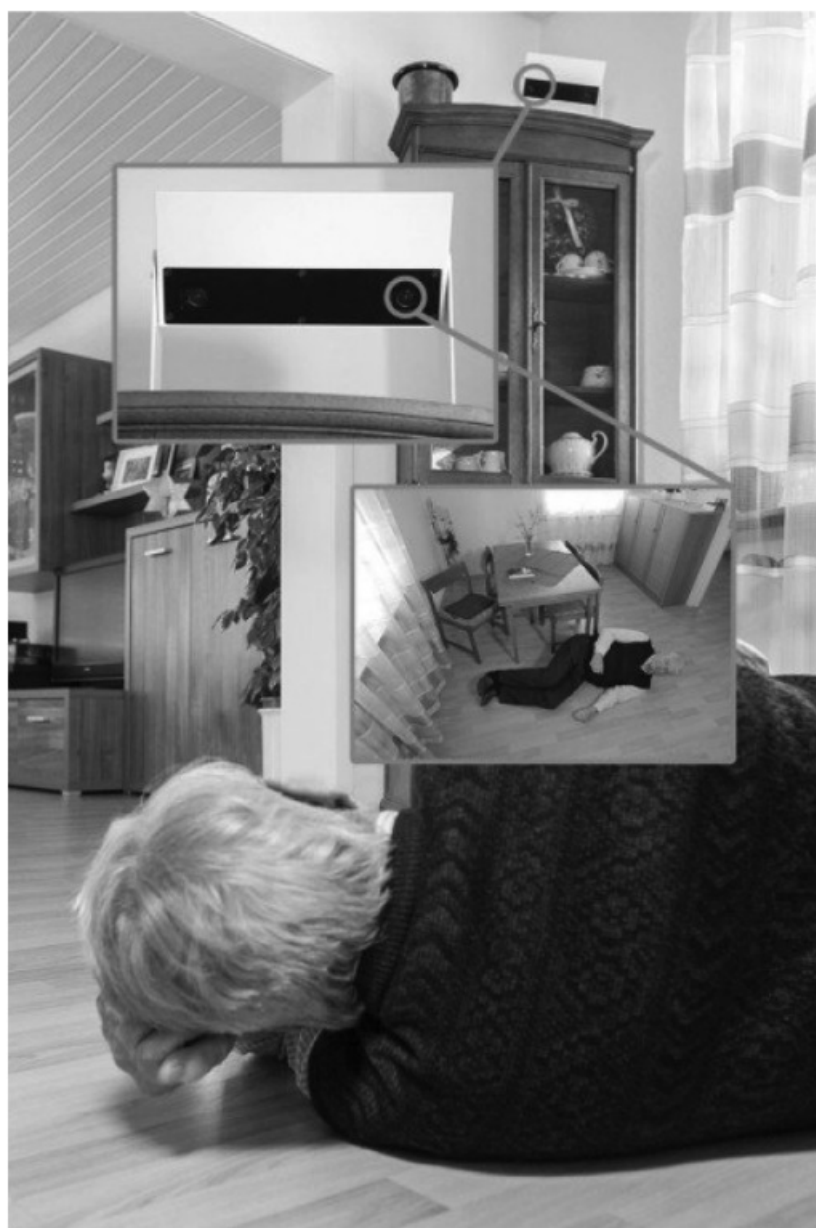


Рис. 27. Сенсоры системы Safe@Home

⁵⁸ Умные сенсоры помогут одиноким пожилым людям // HRONIKA.INFO : Хроники событий со всего мира. 2014. URL: <http://hronika.info/tehnologii/15291-umnye-sensory-pomogut-odinokim-pozhilym-lyudyam.html> (дата обращения 27.03.2014).

Прежде чем связываться с экстренными службами или родственниками, CareVox удостоверится в том, что помощь действительно необходима. Для этого система попытается вызвать человека к телефону. Если пенсионер или маломобильное лицо не ответят на звонок системы, то CareVox отправит сообщение в службы спасения, а также родственникам и/или друзьям.

При этом система обеспечивает достаточный уровень конфиденциальности, поскольку данные, собранные системой, не посылаются ни на какие удаленные сервера.

Система Safe@Home разработана Институтом машиностроения и автоматизации общества Фраунгофера, фондом Bruderhaus Diakonie и компаниями Silcom и Vitacom. Испытания системы, проведенные в 2012 году, показали ее высокую эффективность.

2.2.3.2. «Умное» напольное покрытие

Напольное сенсорное покрытие SensFloor, разработанное немецкими исследователями, решает ту же задачу, что и система Safe@Home. Тем не менее для этого используются принципиально иные сенсоры. Напольное покрытие состоит из тонкого (0,08 дюйма) полиэстерового текстиля. Текстиль используется в качестве ламинирующего слоя для небольших пластин, внешне напоминающих электронные платы. Одни из них работают как сенсоры давления, другие – как проводящие дорожки. Портативный контроллер в реальном времени собирает данные со всех сенсоров за счет установленных радиомодулей⁵⁹.

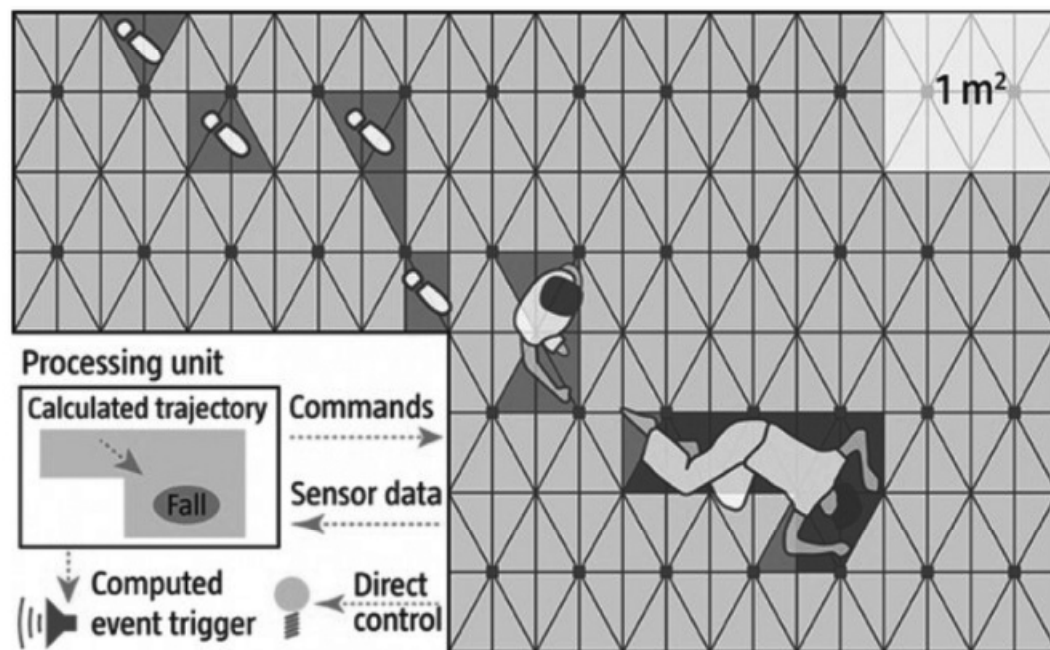


Рис. 28. Принцип работы системы SensFloor

Покрывие SensFloor измеряет емкостное сопротивление, которое зависит от передвижения человека по комнате. Количество активных

⁵⁹ Покрывия с электронными сенсорами превращают полы в гигантские сенсорные экраны // UMNYDOM : Умный дом. 2014. URL: <http://umnydom.com/pokrytiya-s-elektronnymi-sensorami-prevrashhayut-poly-v-gigantskie-sensornye-ekrany/1234/> (дата обращения 27.03.2014).

сенсоров позволяет определить, стоит человек или лежит на полу. В случае падения человека алгоритм работы системы близок к реализации, представленной в системе Safe@Home.

Полевые испытания системы проводились в домах престарелых в Европе. В Эльзасе подобным покрытием оснастили 1300 м² помещений. За год работы система смогла зафиксировать 28 падений, которые были бы несомненно замечены в обычных условиях.

2.2.4. Сенсоры биометрических показателей человека

Разнообразные сенсоры и датчики, входящие в сети подключенных устройств, представляют собой серьезный пласт технологий Интернета вещей. Именно они позволяют собрать данные и информацию об окружающем мире, а затем использовать ее для улучшения условий человеческой жизни, оптимизации бизнес-процессов, предотвращения техногенных катастроф и т.п. Сегодня существует множество сенсоров, которые соответствуют общим идеям концепции Интернета вещей. Тем не менее большинство технологий еще только предстоит изобрести.

2.2.4.1. Бесконтактные сенсоры электрических потенциалов

В настоящее время активно разрабатываются сенсоры электрических потенциалов (Electric Potential Sensors)⁶⁰. Ключевые разработки в этой области принадлежат специалистам из Университета Суссекса. Разработанные ими устройства способны записывать электрокардиограмму и электроэнцефалограмму на расстоянии метра от пациента, при этом физический контакт не требуется. Данный эффект достигается за счет того, что эти сенсоры способны улавливать биение сердца, а также электрическую активность мышц и нервных волокон на небольшом расстоянии от человека.

Технология находится на стадии развития, однако можно ожидать широкого распространения по мере появления все более совершенных сенсоров такого рода. При помощи подобных сенсоров можно ненавязчиво контролировать состояние пациентов в больницах, а также людей, относящихся к группам риска (пенсионеров, инвалидов, людей с «профильными» заболеваниями и т.п.).

Интерес к подобным технологиям выражала и компания PassivSystems, специализирующаяся на производстве технологий для «умного» дома. Сенсоры электрических потенциалов могут быть интегрированы в «умные» дома для повышения безопасности проживающих там людей. Кроме того, сенсоры позволяют мониторить передвижение человека по дому, тем самым оптимизируя энергозатраты на освещение, отопление и т.п.

⁶⁰ Бесконтактные сенсоры сердца встраивают в умные дома // NEWSLAND : Новости. 2010. URL: <http://newsland.com/news/detail/id/526079/> (дата обращения 27.03.2014).

Примером реализации технологии бесконтактного измерения электрических потенциалов на теле человека является серийно выпускаемый компанией Plessey Semiconductors датчик EPIC. Это датчик выполняет изменения в электрическом поле подобно тому, как магнитометр обнаруживает изменения в магнитном поле. Для него не требуется ни механического, ни резистивного контакта для проведения замеров. Достаточно расположить такой датчик около груди пациента, чтобы получить качественную электрокардиограмму (ЭКГ). EPIC – это сокращение английского термина Electric Potential Integrated Circuit – интегральная микросхема для измерения электрического потенциала.



Рис. 29. Датчик бесконтактного измерения электрических потенциалов

В медицине датчик может измерять потенциал на поверхности человеческого тела, что дает возможность использовать его в электрокардиографии (ЭКГ), электромиографии (ЭМГ), электроэнцефалографии (ЭЭГ) и электроокулографии (ЭОГ). В этих приложениях датчики демонстрируют лучшую разрешающую способность, чем традиционные способы.

Датчики способны следить за активностью глазных мышц – возможность управления прицеливанием или мышц руки для человеко-машинного взаимодействия.

2.2.4.2. Контактные линзы с анализатором уровня глюкозы

В начале 2014 года компания Google представила прототип сенсора, встроенного в контактные линзы⁶¹. Предполагается, что данным устройством будут пользоваться люди, страдающие диабетом. Заболевание диабетом предполагает, что человек должен постоянно мониторить уровень сахара в крови. Сегодня для этого чаще всего используются глюкометры, которые анализируют кровь, взятую из пальца. Это до-

⁶¹ Google разрабатывает «умные» контактные линзы для диабетиков // FERRA.RU. 2014. URL: <http://www.ferra.ru/ru/techlife/news/2014/01/17/Google-smart-contact-lens/> (дата обращения 27.03.2014).

статочно болезненная и неприятная процедура, поэтому многие люди до последнего откладывают ее и в итоге контролируют уровень сахара недостаточно интенсивно.

Важно понимать, что у лиц, страдающих сахарным диабетом, уровень глюкозы в крови изменяется достаточно часто. Он меняется после приема пищи, после тренировки, после физической нагрузки и т.п. Разумеется, использовать ручной глюкометр каждый раз – занятие достаточно затруднительное.

Тем не менее определить уровень глюкозы в крови можно посредством анализа слезной жидкости. Небольшой электрохимический сенсор, встроенный в контактную линзу, способен собирать нужную информацию.

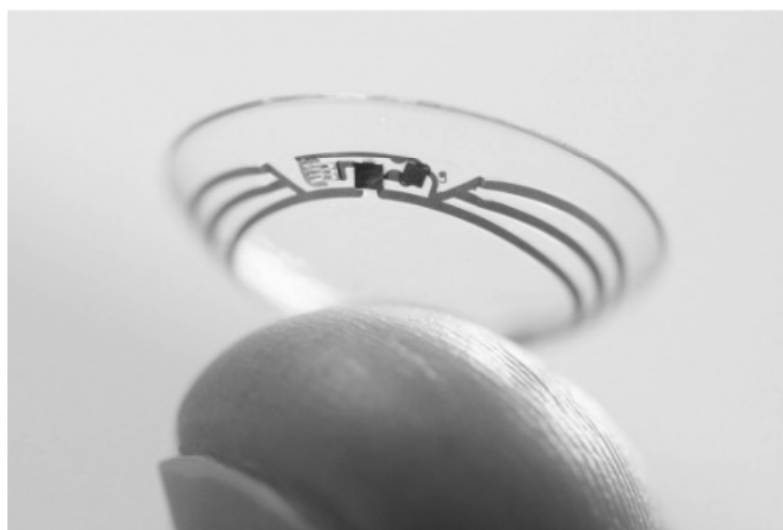


Рис. 30. Прототип «умной» контактной линзы от Google

Устройство контактной линзы для лиц, страдающих сахарным диабетом, достаточно простое. Чип и сенсор глюкозы размещаются между двумя слоями материала контактной линзы. В настоящий момент тестируются сенсоры, способные анализировать уровень глюкозы раз в секунду. Кроме того, в линзу планируется встроить светодиоды, которые будут информировать владельца об изменении уровня сахара в крови.

На сегодняшний день исследователи далеки от создания финальной версии своей технологии, но в обозримом будущем можно прогнозировать выход на рынок подобного продукта. Кроме того, он прекрасно иллюстрирует возможности современных сенсоров касательно развертывания концепции Интернета вещей в медицинской сфере.

2.2.4.3. Сенсоры, встраиваемые в одежду человека

В декабре 2014 года исследователи из Университета Лавала (Канада) подали заявку на патентование технологии вплетения в ткань из хлопка или шерсти датчиков и антенн беспроводной связи. В будущем одежда из такой «умной» ткани будет следить за ключевыми параметрами жизнедеятельности организма: уровнем глюкозы, сердечным ритмом, активностью головного мозга, положением тела и координатами GPS. Такая повседневная одежда сможет самостоятельно «позвонить» в

скорую помощь, порекомендовать диету или сообщить родственникам о состоянии близкого человека, который требует дополнительного ухода.

2.2.5. Датчики и сенсоры в сфере транспорта

Мониторинг в сфере транспорта предполагает автоматизированный контроль различных параметров транспортного средства, таких как:

- местоположение (координаты);
- параметры движения (направление и скорость);
- режимы работы двигателя;
- состояние и уровень заряда аккумуляторных батарей;
- наличие и расход топлива и других технологических жидкостей;
- режимы работы навесного оборудования;
- наличие и состояние груза;
- и др.

2.2.5.1. Приемники спутниковых навигационных сигналов

Приемник спутниковых сигналов – основной элемент любой системы транспортного мониторинга. Именно от него зависит достоверность получаемой информации⁶². Показания большинства сенсоров и датчиков не будут иметь смысловой нагрузки без точного позиционирования объектов в пространстве. Мобильный модуль, включающий в себя приемник-контроллер и модуль хранения и передачи данных, выполняет основные функции системы транспортного мониторинга:

- Вычисление географического положения транспортного средства, его скорости и вектора передвижения.
- Интеграция подключенных устройств, которыми оснащено транспортное средство. Датчики и сенсоры подключаются непосредственно к контроллеру.
- Хранение определенного объема данных в условиях отсутствия связи, с целью экономии трафика или в ожидании запроса из диспетчерского центра.
- Передача собранных данных в диспетчерский центр.

Существующие на рынке приемники спутниковых сигналов работают в стандартах NAVSTAR GPS или ГЛОНАСС. Первая система глобального позиционирования разработана и реализована Министерством обороны США, вторая – Министерством обороны СССР, позже – России.

⁶² Краткий анализ действующих на российском рынке систем дистанционного мониторинга транспорта, или как выбрать систему и потом долго не изумляться // SIRIUS.RU : Разработка диспетчерских систем. URL: <http://www.sirius.ru/article?n=1> (дата обращения 27.03.2014).

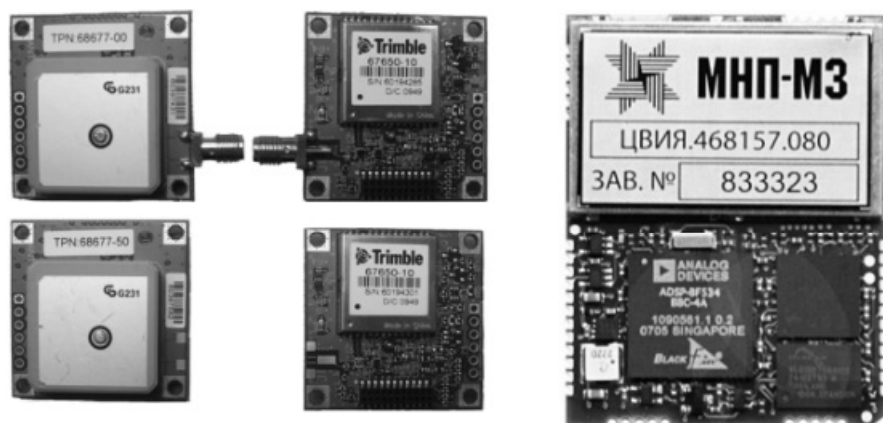


Рис. 31. Встраиваемые GPS-приемники на базе модуля CONDOR и навигационный приемник МНП-М3 для протоколов ГЛОНАСС

В отдельную категорию выделяются приемники, поддерживающие одновременно и протоколы ГЛОНАСС, и протоколы GPS⁶³.

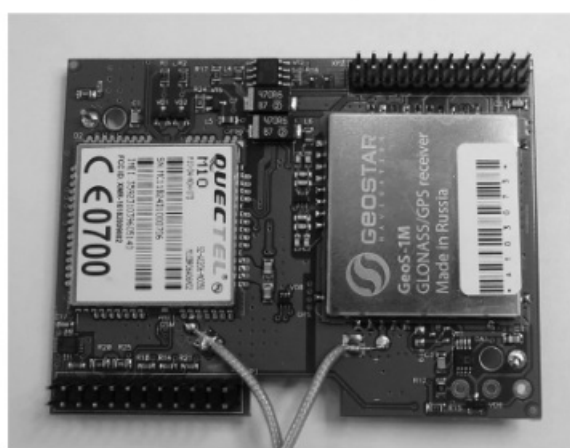


Рис. 32. Плата с ГЛОНАСС/GPS-приемником ГЕОС-1М

В ближайшем будущем можно ожидать выход на рынок устройств, которые будут поддерживать протоколы спутниковых навигационных систем COMPASS (Китай) и Galileo (Европейский союз). В настоящий момент вывод спутников данных систем на орбиту еще не закончен, поэтому полноценное использование протоколов в мониторинге транспорта невозможно. Ожидается, что они будут конкурировать с ГЛОНАСС за статус «второй» системы спутниковой навигации после GPS⁶⁴.

2.2.5.2. Датчики контроля состояния агрегатов и систем транспортного средства

Задачи, решаемые системой электронного транспортного мониторинга, зависят, прежде всего, от конкретных особенностей и потребностей. Отражение транспортных объектов на карте местности – единственная задача, свойственная для всех рассматриваемых систем. Специфические задачи разнятся в соответствии с потребностями конечного потребителя.

⁶³ URL: <http://habrahabr.ru/company/scout/blog/151385/>

⁶⁴ ГЛОНАСС нужен «эффект масштаба» // GLONASS-PORTAL.RU: Глонасс-портал. 2013. URL: http://www.glonass-portal.ru/articles/2012-10-24/gurko_glonass_perspektiva.avcms (дата обращения 27.03.2014).

Так, в сфере коммерческих пассажирских перевозок зачастую используется план по выручке для контроллеров. Автоматизированный подсчет числа пассажиров позволяет корректировать план с целью увеличения выручки компании-перевозчика и уменьшения возможных хищений. Обычно для этого используются инфракрасные датчики, устанавливаемые над дверным проемом. Их погрешность составляет не более 5–10% от реального пассажиропотока⁶⁵.



Рис. 33. Инфракрасный датчик контроля пассажиропотока МИД-485

В свою очередь, в случае грузовой перевозки скоропортящейся продукции может возникнуть вопрос соблюдения температурного режима. Составные части системы электронного транспортного мониторинга могут в реальном времени собирать данные о температуре в рефрижераторе. Для этого используются подключенные к терминалу аналоговые или цифровые датчики.



Рис. 34. Датчик температуры воздуха в рефрижераторе

К температурному контролю также относится и сбор сведений о температуре двигателя или температуре охлаждающей жидкости. В случае перегрева транспортное средство может выйти из строя. В дальнейшем ему потребуется дорогостоящий ремонт, а компания понесет ущерб из-за простоя транспорта или невозможности выполнить контрактные обязательства.

⁶⁵ Рушкевич А., Осадчий В. Мониторинг подвижных объектов: российские реалии и технические инновации: [Электронный документ] // WIRELESS-E.RU : Журнал «Беспроводные технологии». URL: http://www.wireless-e.ru/assets/files/pdf/2010_03_56.pdf (дата обращения 27.03.2014).



Рис. 35. Датчик температуры двигателя Starline и датчики температуры охлаждающей жидкости

Не меньший интерес представляет и контроль горюче-смазочных материалов. Существует два способа мониторинга расхода топлива. Первый способ – установка расходомера, который подсчитывает количество потребляемого топлива, второй – установка датчика уровня топлива непосредственно в бак. Второй вариант предпочтительнее, поскольку удобен в интеграции и обладает довольно низкой погрешностью в 1% от объема бака, что в несколько раз точнее резистивных штатных датчиков. Использование датчиков контроля топлива в совокупности с другими компонентами системы транспортного мониторинга позволяет снизить расходы топлива на 6–16%⁶⁶.



Рис. 36. Датчик уровня топлива Omnicomm LLS

В сфере автомобильного транспорта достаточно большое значение имеет возможность установки датчика состояния дверей. Открытая дверь создает угрозу для жизни водителя, пассажиров, а также ставит под угрозу сохранность груза. Для того чтобы контролировать факт открытия/закрытия двери, возможно использовать специальный датчик. Информация с датчика может либо поступать непосредственно водителю, либо транслироваться ему через диспетчерский центр, уведомленный о нарушении условий перевозки.

⁶⁶ Рушкевич А., Осадчий В. Мониторинг подвижных объектов: российские реалии и технические инновации : [Электронный документ] // WIRELESS-E.RU: Журнал «Беспроводные технологии». URL: http://www.wireless-e.ru/assets/files/pdf/2010_03_56.pdf (дата обращения 27.03.2014).



Рис. 37. Датчик контроля фактов открытия и закрытия дверей

В ряде случаев огромное значение имеет вопрос безопасности водителя, транспортного средства или перевозимого груза. Для обеспечения безопасности могут использоваться различные технологии и различные датчики и сенсоры. Так, в случае пассажирских перевозок прямое отношение к безопасности имеет контроль открытия и закрытия дверей. А в случае перевозки ценных грузов может возникнуть потребность в установке «тревожной кнопки» на случай атаки на транспортное средство. В ряде случаев необходимо проинформировать водителя о въезде в зону повышенной опасности. К примеру, подобные геограды можно интерактивно размещать возле территорий школ и детских садов⁶⁷. Также к сфере безопасности можно отнести информирование диспетчерского центра о нарушении скоростного режима или возникновении дорожно-транспортного происшествия.

В качестве источников информации о состоянии транспортного средства могут использоваться штатные бортовые датчики и сенсоры. Теоретически, любые датчики могут быть интегрированы со встроенной CAN-шиной, которая зачастую собирает информацию о пробеге, количестве потребляемого топлива, нагрузке на ось, состоянии агрегатов и т.п. CAN (Controller Area Network) – это система цифровой связи и управления электрическими устройствами автомобиля, позволяющая собирать данные от всех устройств, управлять ими и обмениваться информацией.

Тем не менее подключение сопряжено с рядом трудностей, главная из которых – возможность повредить предустановленную аппаратуру. В ряде случаев существуют готовые технологические решения данной проблемы. Так, для облегчения возможности интеграции CAN-шины с системами мониторинга европейские производители грузовиков приняли стандарт FMS, обеспечивающий безопасное подключение телематических устройств к CAN-шине через FMS-адаптер. При этом подключение терминала к шине без использования адаптера запрещено Европейской ассоциацией производителей автомобилей (ACEA) из-за возможности повредить бортовое оборудование⁶⁸.

⁶⁷ Мониторинг автотранспорта // ASTRON-GT.RU : Спутниковый мониторинг. 2008. URL: <http://www.astron-gt.ru/article/a-5.html> (дата обращения 27.03.2014).

⁶⁸ Рушкевич А., Осадчий В. Мониторинг подвижных объектов: российские реалии и технические инновации : [Электронный документ] // WIRELESS-E.RU: Журнал «Беспроводные технологии». URL: http://www.wireless-e.ru/assets/files/pdf/2010_03_56.pdf (дата обращения 27.03.2014).



Рис. 38. Пример схематичного размещения устройств, подключенных к CAN-шине автомобиля

В целом же можно констатировать, что сегодня на рынке существует множество готовых технологических решений, позволяющих контролировать большинство параметров различных транспортных средств.

2.2.5.3. Электронные радиочастотные пломбы

Автоматизированный контроль состояния и наличия грузов обеспечивается активным переходом к использованию электронных радиочастотных пломб (ЭП) – электронных устройств, применяемых для предотвращения случаев подделки запорно-пломбировочных устройств, несанкционированного вскрытия пломб и автоматизации учета грузов. Такие устройства, выполняя привычные функции обычных силовых пломб (запорно-пломбировочных устройств), являются частью электронной системы автоматического контроля сохранности грузов в процессе их транспортировки. Электронная радиочастотная пломба позволяет контролировать сохранность грузов дистанционным способом путем считывания внесенной в пломбу информации и определения ее целостности. Существует много разновидностей ЭП (рис. 39). Для работы ЭП используются несущие частоты 125 кГц, 13,56 МГц, 865 МГц, 315/433 МГц.

Таким образом, электронная пломба (ЭП) представляет собой запирающее и одновременно пломбирующее устройство, в корпус которого вставлен портативный электронный блок, который выполняет функции миниатюрного приемопередатчика радиосигналов. Обычно ЭП предоставляет для считывания следующую информацию: уникальный номер пломбы, номер автомобиля (контейнера), информацию о грузе, место назначения отправителя и получателя груза. Усовершенствованные модели таких устройств (обычно это активные или полуактивные RFID-метки) даже имеют часы для точного указания времени, когда пломба была вскрыта.



Рис. 39. Примеры конструктивного исполнения электронных пломб

Информация однократно вводится в RFID-метку пломбы в момент пломбирования контейнера или иного объекта. После этого изменения и дополнения записанной информации в процессе эксплуатации исключены. Электронная пломба устанавливается на транспортное средство точно таким же образом, как и обычная пломба. Номер пломбы и дополнительная информация посредством RFID-считывателя проверяется автоматизированной системой, вводится и сохраняется в базе данных отправителя. Затем данные передаются в компьютер центральной базы данных. Стационарные дистанционные считыватели информации для приема сигналов (информации), посылаемых ЭП по радиоканалу, устанавливаются в таможенных пунктах в портах, на автомобильных и железных дорогах. Используя автоматизированную систему, информация передается через компьютерную сеть в пункт доставки груза для его последующего контроля и очистки по прибытии. В конечном пункте доставки груза или в пункте перегрузки RFID-считыватель получит информацию, переданную ЭП. Если в процессе транспортировки пломба была вскрыта или нарушена, то считывание и получение информации становится невозможным, выдается сообщение о неисправности пломбы. Можно также сравнить и сопоставить информацию, полученную с ЭП, с информацией, ранее предоставленной отправителем. Определение фактов несрабатывания ЭП, несовпадения информации (фальсификации) служит основанием для выяснения причин и проведения необходимых процессуальных действий в отношении владельца груза и транспортного средства.

Необходимо отметить, что основные производители электронных пломб сосредоточены на производстве активных и полуактивных устройств, так как именно они наиболее востребованы перевозчиками морских контейнеров, контейнеров со скоропортящимися пищевыми продуктами и перевозчиками военных грузов. Информация о пассивных радиочастотных пломбах для целей внутреннего таможенного транзита или для контроля экспортных грузов практически отсутствует.

Активные электронные пломбы

Активная электронная пломба (рис. 40) предназначена для дистанционного, длительного (несколько лет) контроля и охраны грузов и контейнеров на транспорте, а также для контроля доступа и защиты стационарных объектов и помещений.



Рис. 40. Установка электронной пломбы IP-UHF-BiT Intermodal Seal на контейнере

При активации режима пломбы «Закрото» осуществляется мониторинг целостности запорного кабеля и других, критических для пломбы факторов (температура, напряжение питания). При этом в память пломбы заносятся дата и время всех действий, производимых с пломбой, а также тип этих действий.

Электронная пломба состоит из двух частей: запорного элемента и корпуса пломбы. Запорный элемент представляет собой металлический штырь или дужку из закаленной стали, запорного кабеля (запорный элемент зависит от конструкции пломбы), который вставляется в проушину запирающего элемента объекта (контейнера и т.д.). Затем запорный элемент фиксируется в корпусе пломбы. Запорный кабель может представлять собой оптоволокно, усиленное металлической оплеткой и покрытое термопластиковой оплеткой. Один конец кабеля может быть заранее закреплен в корпусе пломбы, а второй запирается механическим способом, исключая возможность вскрытия.

Перевод пломбы в рабочий режим производится после установки пломбы на объект с помощью считывающего устройства. Работа со считывателем осуществляется дистанционно. Для обмена данными необходимо присутствие электронной пломбы в поле считывателя.

По сравнению с обычной электронная пломба имеет ряд преимуществ. При закрывании такая пломба генерирует уникальный ключ,

сохраняющийся на карте памяти ридера. Открытие пломбы может быть осуществлено только при наличии данного ключа. Для открытия пломбы необходимо передать данный ключ в пункт назначения по выделенному каналу связи.

Получив команду от считывателя на переход в рабочий режим, пломба начинает осуществлять контроль за положением своего запорного элемента (установлен / не установлен) с одновременным отсчетом реального времени. При вскрытии пломбы информация о факте вскрытия и его времени заносится в базу данных пломбы. База данных пломбы способна хранить информацию о событиях, с ней происходивших.

По радиоканалу возможно получение всей служебной информации из памяти электронной пломбы: отображение состояния элементов питания электронной пломбы, информации о содержимом закрытого объема, дате и времени первоначального запираания, датах и времени всех открытий и запирааний, дате и времени несанкционированного отпираания и попыток взлома. Наличие температурного датчика позволяет зафиксировать попытки заморозить или нагреть пломбу.

Сменный источник питания пломбы рассчитан на несколько лет службы в рабочем режиме. При снижении напряжения источника питания ниже установленного в базу данных пломбы заносится соответствующая информация. При следующем обмене данными она будет передана в считывающее устройство.

Полуактивные электронные пломбы

Полуактивные (полупассивные) электронные пломбы (рис. 41) аналогичны пассивным пломбам, но имеют встроенную батарею. Батарея начинает использоваться после получения сигнала от считывателя. Благодаря этому удастся достичь большего расстояния считывания, поскольку используется энергия не только ридера, но и пломбы.



Рис. 41. Полуактивная электронная пломба

Пассивные электронные пломбы

Пассивные радиочастотные пломбы не имеют столько функциональных возможностей, как активные пломбы. Как правило, они не имеют в своем составе встроенного источника электроэнергии. Их основная функция – сообщить считывающему устройству свой уникальный номер (UID, EPC), если целостность пломбы не нарушена механи-

ческим или термическим образом. Основу пассивной пломбы составляет радиочастотный транспондер.

Пассивная пломба – это устройство одноразового использования. Стоимость такой пломбы составляет несколько долларов. Пассивная пломба с источником питания может стоить в два-три раза дороже по сравнению с пассивной.

2.2.6. Датчики параметров окружающей среды

Контроль параметров окружающей среды сегодня является актуальной задачей во многих сферах деятельности человека. Состояние окружающей среды является важнейшим фактором обеспечения существования растительного и животного мира, безопасного и комфортного проживания человека, возможности производства сельскохозяйственной и промышленной продукции. Отклонения показателей могут носить как естественный, так и техногенный характер и могут выходить за допустимые пределы, что должно приводить к принятию адекватных и своевременных мер для предотвращения негативных последствий.

Наибольшее внимание сегодня уделяется таким показателям, как:

- состояние атмосферы (температура, влажность, направление воздушных потоков, атмосферное давление и др.);
- состояние почвы;
- состояние Мирового океана и внутренних водоемов;
- состояние ледников;
- радиационная, химическая, бактериологическая и электромагнитная обстановка;
- сейсмическая и вулканическая активность;
- состояние магнитного поля Земли;
- солнечная активность;
- и др.

Зарубежные и отечественные наука и промышленность активно работают над созданием соответствующих измерителей и преобразователей физических величин, которые являются основой датчиков параметров окружающей среды.

2.2.6.1. Датчики климатических показателей

Выпускаемые сегодня промышленностью средства определения климатических показателей можно условно разделить на две группы: датчики показателей микроклимата, предназначенные для работы внутри помещений, и приборы, используемые в метеорологии.

Важнейшими микроклиматическими показателями являются температура, влажность, освещенность. Современные технологии позволяют осуществлять регулирование параметров теплового комфорта и показателей влажности для закрытых помещений. Однако изменение параметров среды невозможно без оценки существующих параметров, измерения влажности воздуха и величины изменения температуры. Специализированные приборы измерения влажности и температуры

широко применяются как в промышленном производстве, так и в частной жизни.

В качестве примера датчиков климатических показателей, применяемых в закрытых помещениях, могут быть представлены датчики температуры и влажности.

Мультифункциональный климатический датчик SB-CMS-THL производства китайской компании HDL сочетает в себе встроенные датчики:

- температуры воздуха в помещении;
- относительной влажности;
- уровня яркости света⁶⁹.



Рис. 42. Климатический датчик SB-CMS-THL

Temperature Sensor Ubiquiti mFi-THS разработан для мониторинга климатических данных (HVAC) и подобных применений. Измеряет температуру и влажность в помещениях с погрешностью не более $\pm 0,5^{\circ}\text{C}$ – температура, $\pm 3\%$ – влажность⁷⁰.



Рис. 43. Датчик температуры и влажности Ubiquiti mFi-THS

Примерами реализации функции измерения метеорологических показателей могут служить приборы производства одного из мировых лидеров в области промышленных измерений и измерений параметров окружающей среды финской компании Vaisala⁷¹.

Модули для измерения относительной влажности (RH), температуры (T) и точки росы (Td), обеспечивающие точность измерения климатических показателей воздуха: менее 1% – для влажности и 0,12% – для температуры.

⁶⁹ URL: http://domintellect.ru/shop/datchiki/datchik_temperaturi_vlagnosti_osveshennosti/ (дата обращения 27.03.2014).

⁷⁰ URL: <http://www.wmd.ru/products/mfi-ths.html#tab-accessories> (дата обращения 27.03.2014).

⁷¹ URL: <http://www.vaisala.ru/ru/weather/Pages/default.aspx> (дата обращения 27.03.2014).

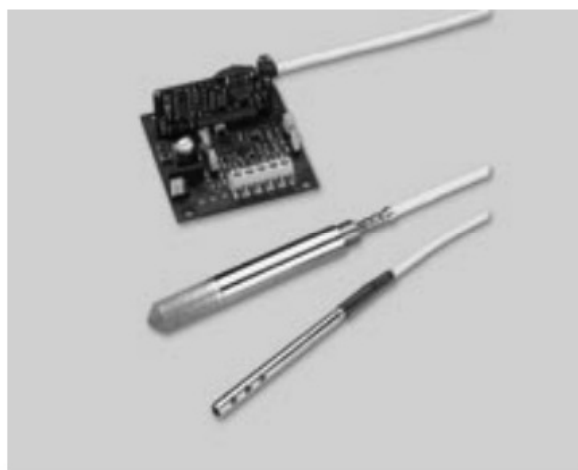


Рис. 44. Датчики измерения температуры и влажности

Датчики обнаружения молний объединяют в себе ОВЧ-интерферометрию с НЧ-технологией пеленгации по магнитному направлению и времени прихода электромагнитного импульса для возможностей определения картирования общих молний высшего уровня с калиброванными параметрами молний, а также для наибольшей эффективности обнаружения и максимально точного определения местоположения молний «облако-земля».



Рис. 45. Датчик обнаружения общих молний TLS200



Рис. 46. Датчик обнаружения молний «облако-земля» LS7002

Ультразвуковой датчик ветра WMT52 измеряет горизонтальную скорость и направление ветра. Конструкция прибора позволяет применять его в жестких климатических условиях.



Рис. 47. Ультразвуковой датчик ветра WMT52

Ультразвуковой датчик IRU-9400 предназначен для измерения уровня снега и воды, толщина наледи от 15 см до 1 м.



Рис. 48. Датчик уровня снега и воды IRU-9400

Среди отечественных разработчиков и изготовителей датчиков климатических показателей можно отметить компанию «АТАКОМ», производственно-коммерческую группу «ГРАНАТ», ЗАО «Эксимер», НПО «Эко-Интекс», ЗАО Научно-производственная фирма «ТИН» и др.

2.2.6.2. Автоматические метеорологические станции

Комплексное использование датчиков климатических показателей нашло применение при создании автоматических метеорологических станций.

Характерными примерами таких решений могут служить приборы производства американской компании Radiometrics.

Одним из примеров является профайлер ветра MP-3000A. Этот прибор предназначен для точного краткосрочного прогноза погоды. Микроволновой профайлер ветра измеряет метеорологические параметры (температуру, влажность, ветер, осадки) в реальном времени на высоте до 10 км. Полученные данные накладываются на трехмерную карту. Более того, в отличие от метеозондов микроволновые радиометры мобильны и работают в самых сложных погодных условиях.

Экстремальная погода (шквалы, молнии, ливни, град, гололед, туман) – самые сложные для прогнозирования метеорологические явления. Проблема в отсутствии своевременных данных о состоянии тропосферы (3–10 км), где формируется экстремальная погода. То есть радиозонды и самолеты ограничены во времени и радиусе действия, погодные радары не обнаруживают ранние стадии, а спутники недостаточно чувствительны в тропосфере. Поэтому радиометры Radiometrics незаменимы для мониторинга ключевой инфраструктуры и прогноза экстремальной погоды.



Рис. 49. Компактный гиперспектральный радиометр Radiometrics MP-3000A

Профайлер ветра Radiometrics MP-3000A обеспечивает:

- непрерывный мониторинг температуры, влажности и жидкой воды на высотах до 10 км;
- стабильную работу в любых погодных условиях;
- 35 каналов микроволновых частот;
- измерение температуры нижней границы облаков;
- точную привязку измеренных показателей к географическим координатам с использованием GPS;
- автоматическое создание прогноза погоды;
- инструментарий для предсказания важных изменений локальной погоды⁷².

Другим примером комплексного использования климатических датчиков является метеорологическая станция SIC-F01. Эта станция включает в себя ультразвуковые датчики, определяющие направление и скорость ветра, время выпадения дождя, а также датчики определения относительной влажности, температуры и атмосферного давления.

Высокая точность и высокое разрешение делают эту систему идеальной для точного прогноза погоды.

Данные SIC-F01 можно контролировать при помощи дисплея, а сама метеостанция обладает интерфейсом промышленной автоматизации, поддерживает Modbus / TCP.

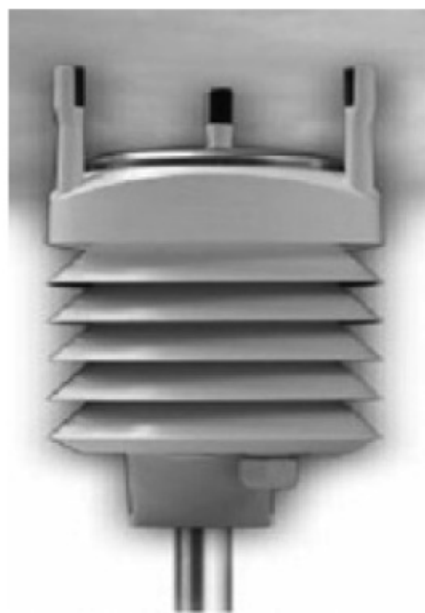


Рис. 50. Автоматизированная метеорологическая станции SIC-F01

Особенности метеорологической станции SIC-F01:

- высокая точность измерений;
- ультразвуковые датчики определения скорости ветра и количества выпадения осадков;
- отсутствие подвижных частей (экономия времени и денег на обслуживание);

⁷² URL: <http://www.sicenter.by/radiometrics.html> (дата обращения 27.03.2014).

- низкое энергопотребление повышает надежность и долговечность станции;
- удобство и простота использования;
- ЖК-дисплей с сенсорным экраном и мощный программный функционал⁷³.

2.2.6.3. Автономные регистраторы сейсмических сигналов

При построении сетей автоматизированного сейсмического для сейсмического мониторинга, а также при проведении наземных и мелководных геолого-геофизических работ активно применяются автономные регистраторы сейсмических сигналов АРСС.

Подобные регистраторы имеют встроенный трехкомпонентный сейсмометр, электронный модуль, встроенный накопитель, источник питания, а также интерфейс для передачи данных.

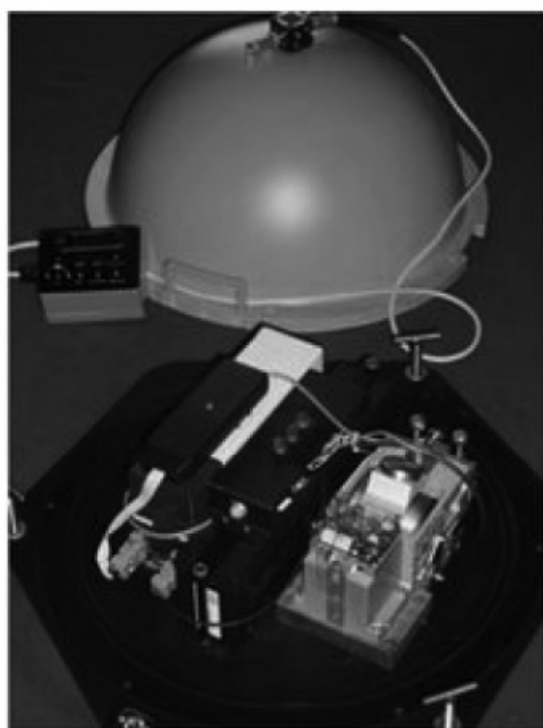


Рис. 51. Регистратор сейсмических сигналов

Регистраторы используются для изучения микросейсмического волнового фона при обследовании различных наземных и прибрежных районов и объектов, а также для регистрации и оперативной оценки характеристик сейсмических сигналов от различных источников в полевых и стационарных условиях.

2.3. Средства сбора, передачи, обработки, хранения и представления информации

Данные, создаваемые подключенными объектами Интернета вещей, являются значительным информационным ресурсом, предполагающим наличие возможностей их сбора, передачи, обработки, хранения

⁷³ URL: <http://www.sicenter.by/meteo-station-sic-f01.html> (дата обращения 27.03.2014).

и представления информации конечным потребителям. Подключенные устройства и вещи также нуждаются в управляющем воздействии, как со стороны других подключенных объектов и серверов соответствующих автоматизированных информационных систем, так и со стороны пользователей.

2.3.1. Виды взаимодействия в Интернете вещей

Интернет вещей представляет собой вычислительную сеть, имеющую:

- основные узлы – подключенные объекты;
- серверы управления подключенными объектами;
- пользовательские узлы – мобильные и персональные вычислительные устройства.

Здесь можно выделить три основных вида взаимодействий в Интернете вещей:

- 1) взаимодействие между подключенными объектами;
- 2) взаимодействие между пользователями и подключенными объектами;
- 3) взаимодействие между удаленными серверами и подключенными объектами.

Все эти виды взаимодействия с подключенными объектами Интернета вещей подразумевают доступ к этим объектам. В настоящий момент можно выделить три основных способа такого доступа:

- прямой доступ;
- доступ через шлюз;
- доступ через сервер.

Прямой доступ к подключенным объектам

В случае прямого доступа подключенные объекты должны иметь собственный IP-адрес или сетевой псевдоним, по которому к ним можно обратиться из любого клиентского приложения. Интерфейс с такими вещами обычно выполнен в виде web-ресурса с графическим интерфейсом для управления посредством web-браузера. Здесь также возможно использование специализированного программного обеспечения.

К недостаткам такого способа можно отнести:

- необходимость наличия у подключенного объекта фиксированного IP-адреса в сети, что зависит от провайдера услуги связи с Интернетом таких вещей. Другим выходом из ситуации является использование алиаса (сетевого псевдонима IP-адреса), что требует постоянного обращения подключенного объекта к специальному серверу с запросом об обновлении сетевого адреса по псевдониму;
- лимит подключений к подключенным объектам, обусловленный качеством связи с ними, а также их слабыми вычислительными ресурсами. Такая проблема решается путем включения в состав подключенных объектов высокопроизводительного оборудования и

подключения устройств к стабильному источнику связи с Интернетом. Это вызывает необходимость в большем потреблении энергии такими устройствами, что вынуждает делать их стационарными, питающимися от постоянных источников электроэнергии.

Доступ к подключенным объектам через шлюз

Доступ к подключенным объектам через шлюз является более рациональным способом организации взаимодействия и полностью вытесняет метод прямого доступа в случае необходимости организации связи обособленной сети подключенных объектов с глобальной сетью Интернет. Большинство стандартов беспроводных сенсорных сетей не поддерживают протокол IP, используя собственные протоколы взаимодействия. Такая особенность вызывает необходимость наличия устройства для ретрансляции сообщений из сенсорной сети в сеть Интернет для совместимости протоколов.

Недостатки такого подхода те же, что и в случае прямого доступа, но распространяются они на шлюз.

Доступ к подключенным объектам через сервер

Доступ к подключенным объектам через сервер подразумевает наличие посредника между этими объектами и пользователем. Таким посредником является сервер, в основные функции которого входят:

- прием сообщений от подключенных объектов и передача их пользователям;
- хранение принятой информации и ее обработка;
- обеспечение пользовательского интерфейса с возможностью двустороннего обмена между пользователем и подключенным объектом.

Такой способ доступа при решении ряда задач оказывается более рациональным, поскольку позволяет перенести нагрузку обработки запросов пользователей к подключенным объектам на централизованный сервер, тем самым разгружая слабые каналы связи с объектами, перенося нагрузку на проводные каналы связи между сервером и пользователями.

Доступ к подключенным объектам с помощью централизованного сервера также предоставляет надежные средства хранения и обработки информации, позволяет этим объектам взаимодействовать друг с другом и пользоваться дополнительными сервисами, такими как облачные и туманные вычисления.

2.3.2. Мобильные информационные терминалы для сбора и представления данных

В качестве универсальных средств сбора и представления данных получили широкое распространение мобильные терминалы сбора данных (ТСД). Эти устройства позволяют, с одной стороны, выполнить

сбор (считывание) данных с тех датчиков, которые не имеют собственных интерфейсов, а с другой стороны, предоставляют пользователю определенные возможности по получению доступа к результатам обработки таких данных информационной системой.

ТСД – это компактные мобильные переносные компьютеры, оснащенные дисплеем и разнообразными устройствами ввода данных: клавиатурой, сканером штрих-кодовых или RFID-меток, считывателем магнитных карт, GPS-приемником и т.д.

Исходя из названия, основное предназначение терминалов сбора данных – работа в различных системах автоматизации в качестве мобильных рабочих мест, которые перемещаются вместе с работником (например, кладовщиком на складе или товароведом в магазине) и через которые возможен оперативный ввод/получение данных в/из системы автоматизации в процессе приемки, отгрузки штрих-кодированной продукции, инвентаризации, выполнения других операций, результаты которых необходимо точно и максимально оперативно отобразить в учетной системе. Способов обмена данными между учетной системой и мобильным рабочим местом достаточно много: начиная от устаревших инфракрасных (IrDA) и RS232-интерфейсов и заканчивая современными USB и беспроводными Bluetooth, Wi-Fi. Если устройство предназначено для эксплуатации в отрыве от инфраструктуры компании, то к нему могут добавить мобильный модем GPRS/EDGE (как это бывает, к примеру, в курьерских службах ТНТ и DHL) – данные о доставке пакета сразу отправляются в центральный компьютер региона и немедленно становятся доступными на специальном веб-сайте, с помощью которого отправители отслеживают движение пакета или письма.

Изначально терминалы сбора данных представляли собой сканеры штрих-кодов со встроенной памятью данных и процессором. Сейчас они могут связываться с центральным компьютером компании по беспроводной сети, воспроизводить на своем дисплее сложные графические схемы, с помощью GPS-приемника точно указывать положение для того или иного груза, взаимодействовать с метками RFID для быстрой идентификации товара.

Обычно терминал имеет дизайн, облегчающий работу по сбору данных: чувствительный к нажатию экран, ограниченная клавиатура с клавишами больших размеров (чтобы можно было попадать на кнопки даже в перчатках), встроенный сканер штрих-кодов, специализированное программное обеспечение. Внешне он напоминает большой сотовый телефон или калькулятор средних размеров. Как правило, в явном виде обозначена цифровая клавиатура.

Обычно терминалы смонтированы в специальном защитном кожухе и способны выдерживать воздействие низких температур (до минус 30 градусов) и прочих внешних условий.



Рис. 52. Терминалы сбора данных

Заряда батареи обычно хватает на один рабочий день: 6–8 ч непрерывной работы, с батареей повышенной емкости – до 12 ч. При этом мобильный терминал всегда находится в режиме энергосбережения, и если его не использовать в течение трех минут, то он самостоятельно переходит в спящий режим.

2.3.2.1. Программное обеспечение ТСД

Для того чтобы организовать мобильное рабочее место, недостаточно наличия только самого терминала сбора данных. Необходимо соответствующее программное обеспечение, по своей функциональности отвечающее тем задачам, для которых будет использоваться устройство. Инструменты, применяемые для разработки такого программного обеспечения, зависят от типа платформы, используемой в ТСД. Выделяют два подхода:

- организация рабочего места на основе «тонкого» клиента;
- организация рабочего места на основе «толстого» клиента.

Организация рабочего места на основе «тонкого» клиента

Используется либо встроенный в платформу Remote Desktop Protocol, либо клиент Citrix Metaframe, позволяющие удаленно отображать содержимое рабочего стола персонального компьютера (сервера). Плюсы такого подхода очевидны: любой разработчик может написать программное обеспечение для такого мобильного рабочего места, используя знакомый ему инструмент. При этом экранные формы приложения будут в неизменном виде отображаться на экране терминала сбора данных.

Также для создания мобильного «тонкого» приложения применимы стандартные подходы, связанные с разработкой WEB-ориентированного приложения. Клиентом на ТСД в этом случае будет выступать любой поддерживаемый платформой WEB-explorer, например Microsoft Pocket IE.

Еще один подход – использование telnet. В этом случае консольное приложение, запущенное на telnet-сервере, отображается на экране ТСД посредством соответствующего Telnet-client. На текущее время данный подход является устаревшим в связи с общим устареванием фонда оборудования (мобильных терминалов под управлением DOS, Palm и проч.), для которого использование telnet было единственно возможным вариантом – в силу технических ограничений. Однако протокол telnet был (и в некоторых случаях остается) довольно популярным еще 5–10 лет назад, в основном в промышленных системах.

В любом случае, общим плюсом подхода является наличие непрерывного онлайн-обмена данными с host-системой, когда информация поступает в режиме реального времени, что отвечает концепции максимальной оперативности работы. Кроме того, подключение новых мобильных рабочих мест (и масштабирование системы) не вызывает особых затруднений: достаточно настроить на новом устройстве правила подключения к центральному серверу.

Минус подхода вытекает отсюда же: режим онлайн требует непрерывного нахождения терминала сбора данных в зоне покрытия беспроводной сети, что влечет дополнительные затраты на ее установку и поддержку.

Организация рабочего места на основе «толстого» клиента

«Толстый» клиент представляет собой приложение, разработанное для конкретной платформы мобильного терминала. Для операционных систем Microsoft Windows Mobile CE наиболее популярным инструментом в настоящий момент являются продукты семейства .NET, а также продукты других разработчиков. Кроме того, в случае оригинальной платформы (нестандартная операционная система) используются, как правило, средства разработки и библиотеки производителя мобильного устройства. «Толстое» приложение можно реализовать как в концепции онлайн-передачи данных, так и в офлайн (режим промежуточного накопления данных на терминале и передачи при следующем сеансе связи, Batch-режим).

Таким образом, для задач, не требующих оперативного обмена информацией с host-системой, или принципиальной невозможности организации такого обмена (например, работа экспедитора по доставке грузов с широкой географией) такой вариант будет более предпочтительным. И, конечно же, несомненный плюс – это снижение затрат на приобретение и установку беспроводного оборудования.

Минусы «толстого» клиента – жесткая привязка к платформе (операционной системе) ТСД, риски потери данных при несостоявшихся сеансах связи, зависимость от производительности мобильного устройства, необходимость организации промежуточной базы данных на терминале (усложнение разработки).

Прикладные программы для ТСД

Без сомнения, терминалы сбора данных не могут работать в отрыве от АСУ компании – для их сопряжения используется специальное ПО, контролирующее работоспособность конечных устройств и обеспечивающее получение от них информации в процессе работы. Обычно такая система гибко интегрируется в наиболее распространенные ERP-системы или системы электронного документооборота.

На сегодня имеется несколько прикладных пакетов, причем среди них примерно половина – самостоятельные разработки и половина – доделки популярных пакетов, таких как «1С: Предприятие».

«1С-Рарус: Терминал сбора данных» – распространенная разработка, используемая в качестве основы для различного рода надстроек. Предназначена для интеграции промышленных терминалов с программами семейства «1С: Предприятие». Представляет собой комплект конфигураций для разработчиков (набор метаданных, необходимых для считывания информации с терминалов), драйверов, программы для обмена данными с различными носимыми терминалами.

M-Trade помогает автоматизировать оптовую торговлю с автомобилями – в ПО предусмотрены средства учета движения товара вне офиса, создание и печать необходимых документов, синхронизация входных и выходных данных с информационной системой предприятия.

Пакет Stock Control предназначен для проведения инвентарного учета товаров на складе с помощью портативных терминалов (правда, только Psion). Программа выделяется среди конкурентов системой поиска товаров по штрих-коду.

Примерно схожими возможностями обладает ПО «Инвентаризация», правда, его функционал расширен – инвентарный учет можно проводить не только на складе или в магазине, но и в офисе, а максимальный объем БД составляет 60 тыс. наименований.

2.3.2.2. Режимы работы ТСД

Существует три основных режима работы ТСД.

Первый (так называемый batch-режим) позволяет загружать в терминал предварительно подготовленный заказ и накладные, чтобы в дальнейшем вести учет независимо от учетной системы, сверяясь с данными загруженного документа. Удобство данного режима полностью зависит от того, какое программное обеспечение используется с терминалом.

При втором режиме (online) данные заносятся напрямую в учетную систему, что делает терминал проводником между объектом учета и системой управления предприятием. Соответственно, работа в online-режиме более оперативная, но не факт, что надежная – все зависит от четкой «видимости» ближайшего хотспота и качества работы сети. К слову, для внедрения такого режима помимо терминала с поддержкой Wi-Fi необходимо другое оборудование (точки доступа, повторители и т.д.), что значительно удорожает это решение.

Третий режим – комбинированный, когда в терминал загружаются заказы и накладные, а сброс данных в систему осуществляется через каждые два-три часа по беспроводной сети – работник подходит к явно обозначенному хотспоту и «выстреливает» данные для обновления. Такой вариант является наиболее распространенным.

2.3.3. Коммуникационные сети передачи данных

2.3.3.1. Персональные вычислительные сети ZigBee

ZigBee представляет собой спецификацию сетевых протоколов и описывает беспроводные персональные вычислительные сети. Эта технология ориентирована на приложения, которые требуют гарантированной надежной передачи данных при низких скоростях и длительной работе от автономных источников питания. При малом потреблении энергии ZigBee поддерживает не только простые соединения, но и самоорганизующуюся и самовосстанавливающуюся ячеистую топологию с ретрансляцией и маршрутизацией сообщений.

Основная особенность технологии ZigBee заключается в том, что она при малом энергопотреблении поддерживает не только простые топологии сети («точка-точка», «дерево» и «звезда»), но и самоорганизующуюся и самовосстанавливающуюся ячеистую (mesh) топологию с ретрансляцией и маршрутизацией сообщений. Кроме того, спецификация ZigBee содержит возможность выбора алгоритма маршрутизации в зависимости от требований приложения и состояния сети, механизм стандартизации приложений – профили приложений, библиотека стандартных кластеров, конечные точки, привязки, гибкий механизм безопасности, а также обеспечивает простоту развертывания, обслуживания и модернизации. Применение сетей ZigBee в Российской Федерации в частотном диапазоне 2,405–2,485 ГГц не требует получения частотных разрешений и дополнительных согласований.

ZigBee – стандарт для набора высокоуровневых протоколов связи, использующих небольшие, маломощные цифровые трансиверы, основанный на стандарте IEEE 802.15.4–2006 для беспроводных персональных сетей, таких как, например, беспроводные наушники, соединенные с мобильными телефонами посредством радиоволн коротковолнового диапазона. Технология определяется спецификацией ZigBee, разработанной с намерением быть проще и дешевле, чем остальные персональные сети, такие как Bluetooth. ZigBee предназначен для радиочастотных устройств, где необходима длительная работа от батареек и безопасность передачи данных по сети⁷⁴.

2.3.3.2. Беспроводные сети NFC

NFC (Near Field Communication) представляет собой технологию высокочастотной беспроводной связи на малом расстоянии взаимодей-

⁷⁴ URL: <https://ru.wikipedia.org/wiki/ZigBee> (дата обращения 27.03.2014).

ствия. NFC реализует возможность для устройств в малом радиусе действия (10 сантиметров) обмениваться данными.

Эта технология – простое расширение стандарта бесконтактных карт (ISO 14443), которая объединяет интерфейс смарт-карты и считывателя в единое устройство. Устройство NFC может поддерживать связь и с существующими смарт-картами, и со считывателями стандарта ISO 14443, и с другими устройствами NFC, и таким образом – совместимо с существующей инфраструктурой бесконтактных карт, уже используемой в общественном транспорте и платежных системах. NFC нацелена прежде всего на использование в цифровых мобильных устройствах.

Технология NFC в настоящее время главным образом нацеливается на использование в мобильных телефонах и планшетах. Существуют три основных области применения NFC:

- эмуляция карт: устройство NFC ведет себя как существующая бесконтактная карта;
- режим считывания: устройство NFC является активным и считывает пассивную RFID-метку, например для интерактивной рекламы;
- режим P2P: два устройства NFC вместе связываются и обмениваются информацией.

Возможно множество применений, таких как:

- мобильная покупка в общественном транспорте – расширение существующей бесконтактной инфраструктуры;
- мобильные платежи – устройство действует как платежная карта;
- электронная доска – мобильный телефон используется для чтения RFID-меток с уличных досок для объявлений, чтобы на ходу получать информацию;
- спаривание Bluetooth – для соединения устройств Bluetooth 2.1 и выше, поддерживающих NFC, достаточно сблизить их и принять соединение. Процесс активации Bluetooth с обеих сторон, поиска, ожидания, соединения и авторизации заменен простым «прикосновением» мобильных телефонов.

Другие применения в будущем могут включать:

- электронную покупку билетов (авиабилеты, билеты на концерт и другие);
- электронные деньги;
- карты путешественника;
- удостоверения личности;
- мобильную торговлю;
- электронные ключи – ключи от машины, ключи от дома/офиса, ключи от гостиничного номера и т.д.

Для конфигурирования и инициализации других беспроводных соединений, таких как Bluetooth, Wi-Fi или Ultra-wideband.

Программа лицензирования патента для NFC в настоящее время разрабатывается в Via Licensing Corporation – независимом филиале Dolby Laboratories.

NFC была одобрена как стандарт ISO/IEC 8 декабря 2003 года и позже как стандарт Ecma International.

NFC – технология с открытой платформой, стандартизированная в ECMA-340 и ISO/IEC 18092. Эти стандарты определяют схемы модуляции, кодирование, скорости передачи и радиочастотную структуру интерфейса устройств NFC, а также схемы инициализации и условия, требуемые для контроля за конфликтными ситуациями во время инициализации – и для пассивных, и для активных режимов NFC. Кроме того, они также определяют протокол передачи, включая протокол активации и способ обмена данными.

Сейчас оплата наличными уже кажется нам прошлым веком, но и обычные банковские карты тоже стали привычным средством оплаты, так что многих интересует, а что дальше? В будущем нас повсеместно ждут удобные мобильные платежи с помощью технологии NFC, в которых никто, кроме вас, не касается банковской карты, да и существует она только в вашем смартфоне. Приятно, что на наших глазах это будущее уже наступает.

Все больше торговых предприятий внедряет этот современный способ оплаты, и чем крупнее город, тем больше таких компаний: сети супермаркетов и гипермаркетов, продуктовые магазины, сети заправок, сети ресторанов Starbucks, Burger King, Subway и другие заведения общественного питания, аптеки и другие торговые предприятия⁷⁵.

2.3.3.3. Защищенные GPRS/EDGE/3G-сети

Виртуальная защищенная IP-сеть – VPN (Virtual Private Network) федерального масштаба, замкнутая на локальную (в том числе распределенную по всей территории Российской Федерации) вычислительную сеть (ЛВС) корпоративного клиента. Данная сеть исключает выход пакетного трафика за ее пределы и проникновение в эту сеть извне. Она основана на использовании технологии пакетной передачи данных – GPRS/EDGE/3G и действует в зоне покрытия сети оператора мобильной связи.

Техническое решение обеспечивает защищенную коммуникацию с удаленными объектами корпоративного клиента на всей территории Российской Федерации через технологическую мультисервисную IP-сеть оператора связи для систематической передачи данных, файлов, электронной почты, команд управления удаленными объектами, сбора от них различной телеметрической информации, в том числе об их местоположении.

⁷⁵ URL: https://ru.wikipedia.org/wiki/Near_Field_Communication (дата обращения 27.03.2014).

VPN корпоративного клиента изолируется в объединенной GPRS/EDGE/3G-сети и IP-сети оператора мобильной связи с использованием для каждой VPN своих виртуальных маршрутизаторов, персональной таблицы маршрутизации, а также туннелирования и шифрования. Кроме того, в VPN реализуется требуемая политика разграничения доступа.

Подключение локальной вычислительной сети корпоративного клиента к оборудованию сотовой связи с выходом на IP-сеть оператора мобильной связи может производиться как с использованием ресурсов Интернет, так и с использованием арендованных выделенных каналов связи. В обоих случаях применяется технология туннелирования (GRE, IPSec, L2TP) и обеспечивается шифрование трафика.

Корпоративному клиенту предоставляется точка подключения выделенного канала, логический адрес APN (Access Point Name), определяющий настройки виртуальной подсети клиента и пул IP-адресов. Для выделенной APN на GGSN прописывается персональный набор правил,

Абонентам корпоративного клиента присваиваются свои статические IP-адреса или организуется динамическое присвоение IP-адресов из согласованного диапазона. В случае статического выделения адресов присвоенные IP-адреса однозначно прописываются для каждой SIM-карты (абонентского номера сети сотовой связи корпоративного клиента) в HLR.

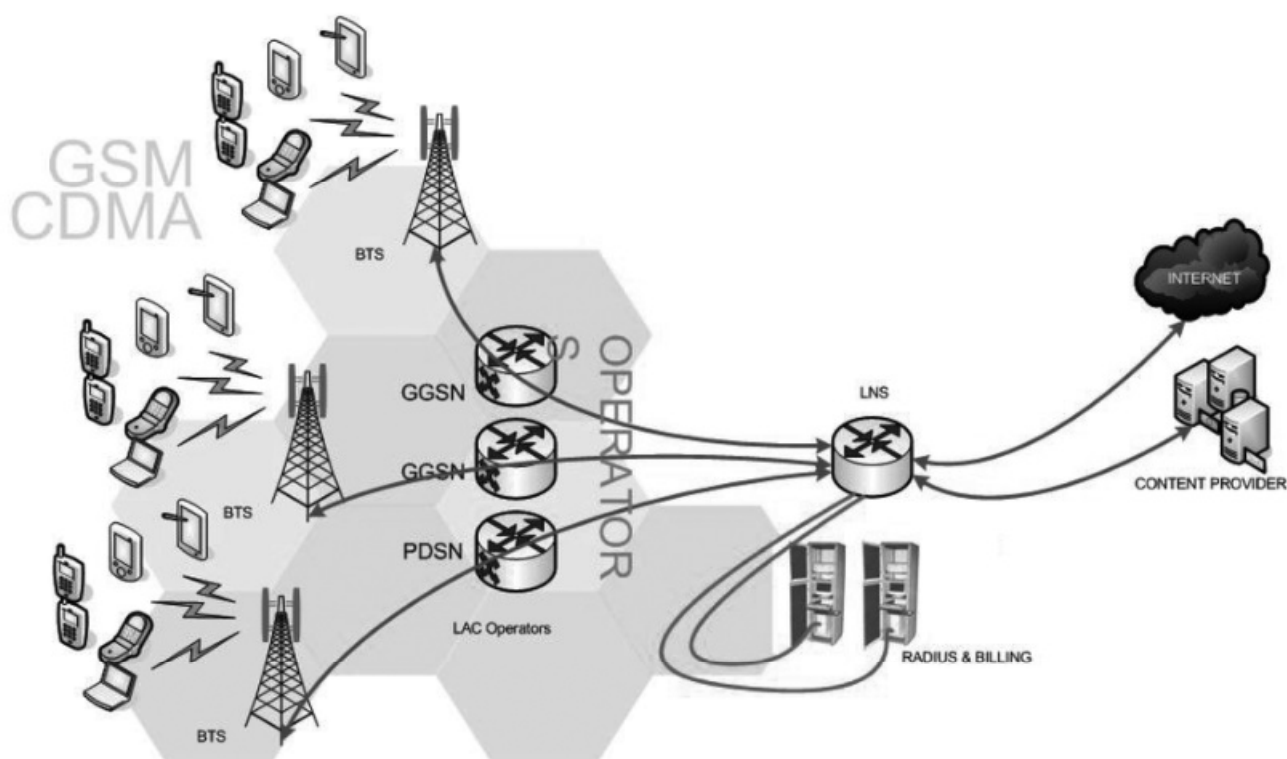


Рис. 53. Схема организации виртуальной защищенной IP-сети

При подключении ЛВС корпоративного клиента по выделенным каналам связи с использованием протоколов L2TP или GRE абонентским номерам возможно присвоение собственных внешних IP-адресов корпоративного клиента.

Кроме того, корпоративному клиенту может предоставляться приоритетное обслуживание (QoS и CoS) при передаче информации как в IP-сети оператора мобильной связи, так и в радиоэфире.

2.3.4. Обработка, хранение и представление данных

Технологии Интернета вещей обуславливают формирование новых требований к способам обработки и хранения информации, возникающей в процессе их применения.

После того, как датчики и сенсоры собрали данные о транспортном средстве, а мобильный модуль передал их в диспетчерский центр, в работу системы вступает программное обеспечение серверов и диспетчерских терминалов. В определенном смысле именно программное обеспечение определяет главные различия между существующими на рынке системами. От него же во многом зависят фактический функционал системы и ее практическая полезность.

2.3.4.1. Автоматизированные системы сбора, обработки и отображения данных

Одной из основных технологий для сбора, обработки и отображения данных об объекте управления или наблюдения в режиме реального времени является технология SCADA, реализуемая на базе программно-аппаратного комплекса.

SCADA-система (Supervisory Control And Data Acquisition) – программно-аппаратный комплекс сбора данных и диспетчерского контроля. Смысл, вкладываемый в термин SCADA, изменялся вместе с развитием технологий автоматизации и управления технологическими процессами. В 80-е годы под SCADA-системами чаще понимали программно-аппаратные комплексы сбора данных реального времени. С 90-х годов термин SCADA больше используется для обозначения только программной части интерфейса АСУ ТП (автоматической системы управления технологическими процессами)⁷⁶.

Основное назначение SCADA-систем: сбор информации автоматизированного процесса, вывод ее пользователю в удобном виде, сохранение сообщений в базу данных и дистанционное управление любым элементом автоматизированного комплекса.

Любая SCADA-система включает три основных структурных компонента: удаленный терминал (RTU – Remote Terminal Unit), диспетчерский пункт управления (MTU – Master Terminal Unit) и коммуникационную систему (CS – Communication System).

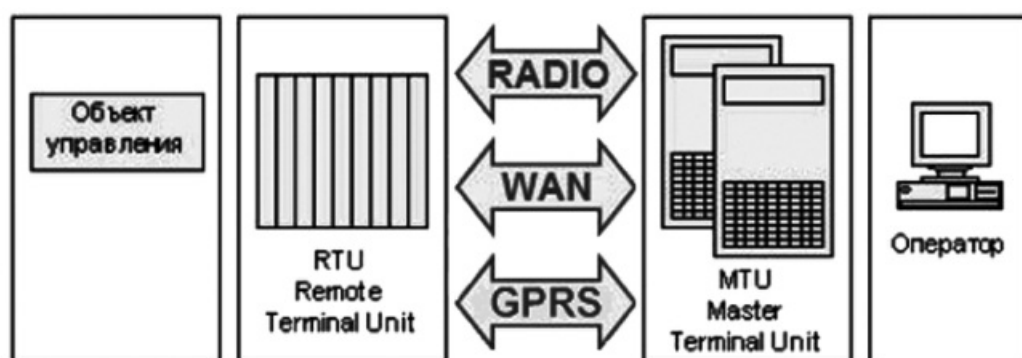


Рис. 54. Обобщенная структура SCADA-систем

⁷⁶ URL: <http://www.tadviser.ru/index.php/SCADA> (дата обращения 27.03.2014).

Remote Terminal Unit (RTU). Удаленный терминал подключается непосредственно к контролируемому объекту и осуществляет управление в режиме реального времени. Таким терминалом может служить как примитивный датчик, осуществляющий съем информации с объекта, так и специализированный многопроцессорный отказоустойчивый вычислительный комплекс, осуществляющий обработку информации и управление в режиме реального времени.

Master Terminal Unit (MTU), Master Station (MS). Диспетчерский пункт управления осуществляет обработку данных и управление высокого уровня, как правило, в режиме квазиреального времени. Он обеспечивает человеко-машинный интерфейс. MTU может быть как единственным компьютером с дополнительными устройствами подключения к каналам связи, так и большой вычислительной системой или локальной сетью рабочих станций и серверов.

Communication System (CS). Коммуникационная система необходима для передачи данных с RTU на MTU и обратно. В качестве коммуникационной системы могут использоваться следующие каналы передачи данных: выделенные линии, радиосети, аналоговые телефонные линии, ISDN-сети, сотовые сети GSM (GPRS). Зачастую устройства подключаются к нескольким сетям для обеспечения надежности передачи данных⁷⁷.

SCADA-система обычно содержит следующие подсистемы:

- Драйверы или серверы ввода-вывода – программы, обеспечивающие связь SCADA с промышленными контроллерами, счетчиками, АЦП и другими устройствами ввода-вывода информации.
- Подсистема реального времени – программа, обеспечивающая обработку данных в пределах заданного временного цикла с учетом приоритетов.
- Человеко-машинный интерфейс (HMI, англ. Human Machine Interface) – инструмент, который представляет данные о ходе процесса человеку-оператору, что позволяет оператору контролировать процесс и управлять им. Программа-редактор для разработки человеко-машинного интерфейса.
- Подсистема логического управления – программа, обеспечивающая исполнение пользовательских программ (скриптов) логического управления в SCADA-системе. Набор редакторов для их разработки.
- База данных реального времени – программа, обеспечивающая сохранение истории процесса в режиме реального времени.
- Подсистема управления тревогами – программа, обеспечивающая автоматический контроль технологических событий, отнесение их к категории нормальных, предупреждающих или аварийных, а также обработку событий оператором или компьютером.

⁷⁷ URL: <http://www.tadviser.ru/index.php/SCADA> (дата обращения 27.03.2014).

- Генератор отчетов – программа, обеспечивающая создание пользовательских отчетов о технологических событиях. Набор редакторов для их разработки.
- Внешние интерфейсы – стандартные интерфейсы обмена данными между SCADA и другими приложениями. Обычно OPC, DDE, ODBC, DLL и т.д.

На программном уровне SCADA-система состоит из двух основных функциональных подсистем:

- подсистема получения данных;
- подсистема обработки и отображения данных.

Программные продукты класса SCADA широко (более 50 предложений) представлены на мировом и российском рынках. Это несколько десятков SCADA-систем, к наиболее популярным из которых можно отнести:

- InTouch (Wonderware) – США;
- Citect (CI Technology) – Австралия;
- FIX (Intellution) – США;
- Genesis (Iconics Co) – США;
- Factory Link (United States Data Co) – США;
- RealFlex (BJ Software Systems) – США;
- Sitex (Jade Software) – Великобритания;
- TraceMode (AdAstrA) – Россия;
- Simplicity (GE Fanuc) – США;
- САРГОН (НВТ-Автоматика) – Россия⁷⁸.

2.3.4.2. Обработка и хранение Больших данных

Большие данные продолжают расширяться и увеличиваться в объеме. Количество обрабатываемой и хранимой информации увеличивается взрывными темпами. Одним из основных генераторов Больших данных сегодня является Интернет вещей, а в будущем его вклад в создание данных будет только возрастать.

Сегодня стремительно увеличивается количество устройств и гаджетов, подключенных к Сети. Все эти устройства, включая фитнес-трекеры, камеры телефонов и даже умные кофеварки, генерируют данные, которые требуется где-то хранить. С увеличением количества данных в мире увеличивается и потребность в увеличении вычислительных мощностей и свободном объеме для хранения информации.

⁷⁸ URL: <http://www.moodle.ipm.kstu.ru/mod/wiki/view.php?id=6964#toc-5> (дата обращения 27.03.2014).

Большие данные (англ. Big Data) – серия подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объемов и значительного многообразия для получения воспринимаемых человеком результатов, эффективных в условиях непрерывного прироста, распределения по многочисленным узлам вычислительной сети, сформировавшихся в конце 2000-х годов, альтернативных традиционным системам управления базами данных⁷⁹.

С другой стороны, обработка больших объемов информации – это только часть «айсберга». Как правило, когда говорят о термине *Big Data*, то используют наиболее популярное определение трех V, что означает Volume – объем данных, Velocity – необходимость обрабатывать информацию с большой скоростью и Variety – многообразие и часто недостаточную структурированность данных. Например, время операции по проверке баланса на карте при снятии наличных исчисляется в миллисекундах. Именно такие требования диктует рынок. Третья сторона вопроса – это разнообразие и неструктурированность информации. Все чаще и чаще приходится оперировать медиаконтентом, записями в блогах, слабо структурированными документами и т.д.⁸⁰

Big Data обычно хранятся и организуются в распределенных файловых системах. В общих чертах, информация хранится на нескольких (иногда тысячах) жестких дисках, на стандартных компьютерах. Так называемая «карта» (map) отслеживает, где (на каком компьютере и/или диске) хранится конкретная часть информации. Для обеспечения отказоустойчивости и надежности каждую часть информации обычно сохраняют несколько раз, например трижды. Так, например, предположим, что вы собрали индивидуальные транзакции в большой розничной сети магазинов. Подробная информация о каждой транзакции будет храниться на разных серверах и жестких дисках, а «карта» (map) индексирует, где именно хранятся сведения о соответствующей сделке. С помощью стандартного оборудования и открытых программных средств для управления этой распределенной файловой системой (например, Hadoop), сравнительно легко можно реализовать надежные хранилища данных в масштабе петабайт⁸¹.

Методы и техника анализа Больших данных

К основным методам и техникам анализа, применимым сегодня к Большим данным, можно отнести:

- методы класса Data Mining: обучение ассоциативным правилам (англ. association rule learning), классификация (методы категоризации новых данных на основе принципов, ранее примененных к уже

⁷⁹ URL: https://ru.wikipedia.org/wiki/Большие_данные (дата обращения 27.03.2014).

⁸⁰ URL: http://dis-group.ru/solutions/data_management/big_data/ (дата обращения 27.03.2014).

⁸¹ URL: <http://www.statsoft.ru/products/Enterprise/big-data.php> (дата обращения 27.03.2014).

наличествуемым данным), кластерный анализ, регрессионный анализ;

- краудсорсинг – категоризация и обогащение данных силами широкого, неопределенного круга лиц, привлеченных на основании публичной оферты, без вступления в трудовые отношения;
- смешение и интеграция данных (англ. data fusion and integration) – набор техник, позволяющих интегрировать разнородные данные из разнообразных источников для возможности глубинного анализа, в качестве примеров таких техник, составляющих этот класс методов, приводятся цифровая обработка сигналов и обработка естественного языка (включая тональный анализ);
- машинное обучение, включая обучение с учителем и без учителя, а также Ensemble learning (англ.) – использование моделей, построенных на базе статистического анализа или машинного обучения для получения комплексных прогнозов на основе базовых моделей (англ. constituent models, ср. со статистическим ансамблем в статистической механике);
- искусственные нейронные сети, сетевой анализ, оптимизация, в том числе генетические алгоритмы;
- распознавание образов;
- прогнозная аналитика;
- имитационное моделирование;
- пространственный анализ (англ. Spatial analysis) – класс методов, использующих топологическую, геометрическую и географическую информацию в данных;
- статистический анализ, в качестве примеров методов приводятся A/B-тестирование и анализ временных рядов;
- визуализация аналитических данных – представление информации в виде рисунков, диаграмм, с использованием интерактивных возможностей и анимации, как для получения результатов, так и для использования в качестве исходных данных для дальнейшего анализа.

Здесь необходимо отметить, что объем создаваемых Интернетом вещей и подлежащих хранению данных может быть значительно уменьшен за счет разумного подхода к проектированию алгоритмов обработки этих данных, при котором храниться должны только обработанные данные, представляющие реальную практическую ценность.

2.3.4.3. Представление данных

Диспетчерское программное обеспечение может быть построено на основании нескольких типов систем. Сегодня на рынке выделяют системы транспортного мониторинга, использующие один из трех типов диспетчерского программного обеспечения:

- программное обеспечение полного цикла, включающее в себя инструменты визуализации, устройства хранения данных и алгоритмы их обработки;
- клиентское программное обеспечение, которое устанавливается на рабочие компьютеры диспетчеров. В этом случае хранение и обработка данных производятся сервером;
- программное обеспечение с веб-интерфейсом.



Рис. 55. Визуализация данных системой транспортного мониторинга «РЕКОД-МТ» с клиентским программным обеспечением для диспетчеров

Программное обеспечение, используемое системами транспортного мониторинга, решает ряд специфических задач.

Основными из них можно считать:

- сбор телеметрической информации от абонентских терминалов;
- обработку принятых данных;
- архивирование и хранение данных;
- визуализацию данных;
- составление аналитических отчетов;
- автоматизацию контроля расхода топлива и передвижения транспортных средств;
- уведомление диспетчеров о возникновении критических событий;
- и др.

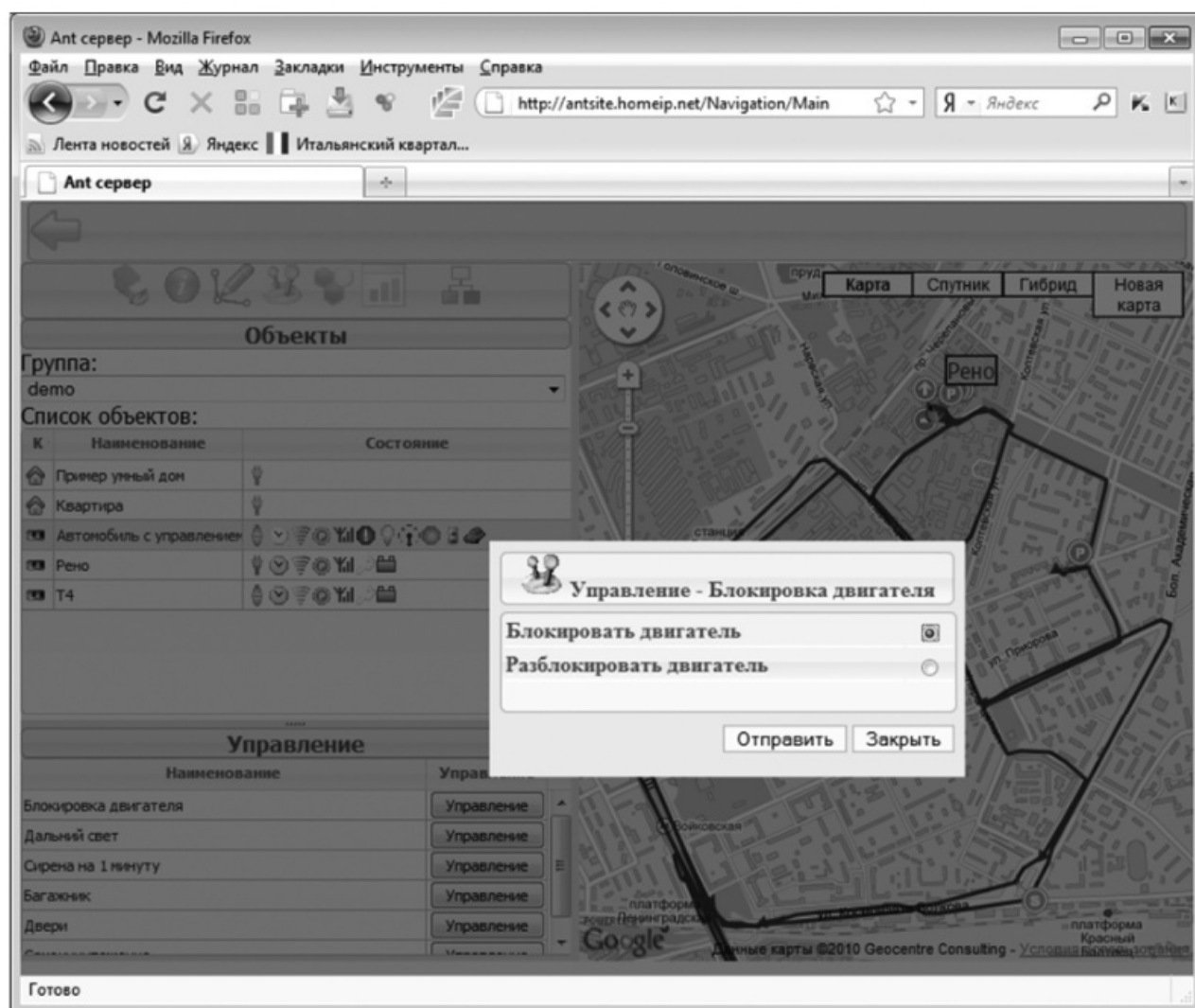


Рис. 56. Визуализация данных системой транспортного мониторинга М2Б с веб-интерфейсом

В целом же можно констатировать, что фундаментальная задача диспетчерского программного обеспечения – добавить элемент человеческого участия в М2М-коммуникацию между бортовыми сенсорами и датчиками, средствами передачи данных, алгоритмами обработки информации и обратной связи диспетчерского центра с транспортным средством.

Глава 3. Практическое применение технологий Интернета вещей

Информационные технологии, рассмотренные во второй главе, являются одним из технических воплощений концепции Интернета вещей. Системы электронного мониторинга уже сейчас включают в себя компоненты, соответствующие всем звеньям технологической цепочки Интернета вещей. А отдельные части этой системы, такие как радиочастотная идентификация, могут использоваться в других решениях в качестве своеобразного моста между физической реальностью и информационным пространством.

Системы электронного мониторинга в целом и их начальный уровень идентификации, представленный RFID и штрих-кодированием, обладают большим потенциалом для внедрения в различные сферы бизнеса и экономики. Эти технологии позволяют идентифицировать реальный объект в виртуальности, создавая его информационный образ. А наличие информации, представленной в унифицированном формате, позволяет применять различные технологии хранения, обработки и передачи информации, сокращая тем самым издержки человеческой деятельности.

Считается, что добавочная стоимость за счет использования технологий Интернета вещей в мировой бизнес-практике составит 1,9 трлн долларов к 2020 году. Лидирующими сферами по использованию Интернета вещей станут производство (15%), здравоохранение (15%) и страхование (11%)⁸². Можно прогнозировать, что значительная часть применяемых технологий Интернета вещей придется на системы электронного мониторинга и радиочастотную идентификацию.

Сейчас можно выделить несколько сфер экономики, использование систем и компонентов электронного мониторинга в которых является коммерчески выгодным. К ним относят логистику, сельское хозяйство, маркетинг, транспорт, туризм, безопасность и здравоохранение.

Мировая практика показывает, что внедрение технологий Интернета вещей, представленных системами электронного мониторинга и электронной идентификации, действительно уменьшает издержки компаний и открывает широкое пространство для дальнейшего развития. Отдельные примеры подобного использования имеет смысл рассмотреть подробнее.

⁸² Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020 // GARTNER.COM : Technology Research. 2013. URL: <http://www.gartner.com/newsroom/id/2636073> (дата обращения 25.02.2014).

**Системы и компоненты электронного мониторинга
в различных областях экономики**

Область экономики	Применение систем и компонентов электронного мониторинга
Логистика	Внедрение автоматизированной идентификации на всех звеньях логистической цепочки
Сельское хозяйство	Мониторинг передвижения крупного рогатого скота
Маркетинг	Применение технологий штрих-кодирования, которые могут быть распознаны смартфонами
Транспорт	Создание автоматизированных транспортных систем, мониторинг передвижения транспортных средств
Туризм	Применение технологий штрих-кодирования для представления информации о памятниках, достопримечательностях и др.
Безопасность	Контроль за оборотом оружия и его применением
Здравоохранение	Контроль за распространением лекарств
Производство	Точная идентификация производственной цепочки

3.1. Применение технологий электронного мониторинга

Технологии электронного мониторинга, ставшие когда-то импульсом к возникновению концепции Интернета вещей, сегодня продолжают оставаться его основой. Главная идея Интернета вещей – дать возможность обществу и экономике получать информацию о событиях и явлениях в реальном времени. Технологии и системы электронного мониторинга успешно выполняют эту задачу, сокращая затраты компаний на ведение бизнеса, облегчая человеческий труд и уменьшая лишние траты.

Электронный мониторинг включает в себя совокупность технологий, которые позволяют получать и обрабатывать информацию о контролируемых субъектах и объектах. Системы мониторинга могут использоваться для ведения учета: материальных потоков, людских потоков, транспортных средств, товаров и т.д.

Технологии электронного мониторинга продолжают совершенствоваться, но и существующие уже на данный момент системы предлагают широкий функционал. Одной из основных задач, решаемой с помощью электронного мониторинга, является информационное обеспечение компании данными о местоположении и состоянии контролируемого субъекта или объекта.

В основе технологий электронного мониторинга лежат технологии обеспечения идентификации объектов: штрих-кодирование, использование радиочастотных идентификационных (RFID) меток и радиочастотных пломб, терминалов сбора данных, а так же технология позиционирования по спутниковым навигационным сигналам.

3.1.1. Применение штрих-кодирования

Свыше 900 000 компаний более чем в 120 странах мира применяют штриховое кодирование кодом EAN-13 для своих товаров.

Переливание крови было одним из первых приложений штрихового кодирования в медицине. В 1972 году Codabar был принят в качестве стандарта для американской службы крови. Codabar был избран, так как в то время это была единственная система, обеспечивающая методы проверки правильности прочтения, что было обязательным условием безошибочного отслеживания крови и идентификации пациента.

Несмотря на то, что существует более 300 стандартов, самыми популярными являются UPC-A и Code 39. UPC-A/UPC-E используется практически на всех товарах, продаваемых в розничных сетях США, а Code 39 используется для автоматизации при идентификации. Им можно закодировать числа и буквы, он может быть напечатан любой длины и его можно прочесть любым сканером штрих-кода. Он широко используется в управлении и на производстве.

Применение QR-кодов в сфере розничной торговли продемонстрировал международный поставщик алкоголя Diageo, который совместно с компанией Evrything внедрил технологии идентификации для некоторых сортов подарочного алкоголя. Каждая единица продукции получила персональную идентификацию. Так, при покупке бутылки виски в подарок человеку предлагают создать персональное онлайн-видеосообщение. Для его активации получателю достаточно привести смартфон на код, который нанесен на бутылку. Объем продаж существенно вырос. В планах компании Evrything – снабжение персональными идентификаторами лекарств и бытовой техники.

3.1.2. Применение радиочастотной идентификации

В настоящее время технологии RFID наиболее широко распространены в ряде отраслей.

1. **Системы контроля и управления доступом (СКУД).** Обеспечение и разграничение доступа персонала на объекты, контроль входов/выходов, контроль рабочего времени, ведение баз данных сотрудников, обеспечение и разграничение доступа транспорта на объекты, мониторинг транспорта, отслеживание маршрутов обхода объекта сотрудниками охранных служб.

2. **Промышленная идентификация.** Идентификация сборочных единиц или транспортных систем конвейера, решение задач контроля

прохождения по производственному циклу, маршрутизация изделий по вариантам исполнения, ведение баз данных изделий и комплектующих. Оборудование способно работать в условиях загрязненности, большого разброса температур. В ряде случаев используются специальные радиометки, способные выдерживать действия промышленных жидкостей (кислоты, щелочи, масла), работающие при температурах до +300 °С.

3. Учет и контроль объектов на складе, в хранилищах и т.п. Существует отдельный класс радиометок, позволяющих групповую регистрацию десятков и сотен меток, одновременно работающих на дистанциях в несколько метров и даже десятков метров. Специальные виды радиометок выдерживают многократные химические отмычки тары, работают на металле стеллажей, имеют вид одноразовых бумажных наклеек.

4. Промышленная автоматика, дистанционные программируемые выключатели света, дистанционные радиоизвещатели (тревожные кнопки), герконовые извещатели открытия/закрытия окон и дверей с радиоканалом, электронные пломбы с памятью событий, измерители температуры, давления с низким потреблением энергии, большой набор электронных замков (дверные, мебельные, витринные, висячие и т.д.), датчики учета расхода энергоносителей и др.

RFID-метки в цепочке «производитель-потребитель»

Радиочастотная идентификация активно используется для повышения эффективности всех этапов жизненного цикла любого конечного продукта. Технологии RFID присутствуют в каждом звене цепочки «производитель-потребитель»:

- идентификация каждой единицы конечного продукта (уровень производства);
- идентификация продукции при комплектации заказа, транспортировке и инвентаризации, а также идентификация местоположения на складе (уровень логистики);
- идентификация местоположения товаров в розничном магазине и идентификация стоимости товаров при совершении кассовых операций (уровень розничной торговли);
- идентификация данных о продукте, таких как срок годности, состав, условия хранения и т.п. (уровень конечного потребителя).

Внедрение радиочастотной идентификации на всех звеньях цепочки производства и редиистрибуции способствует снижению различных издержек, вызванных необходимостью вручную соотносить физические объекты с информационным пространством. Иными словами, участие людей в оптимизированной цепочке минимизируется, и за счет автоматизации издержки становятся меньше.

Технически внедрение технологий радиочастотной идентификации не обязательно должно начинаться с уровня производства. Теоретически, RFID может быть внедрен как на уровне логистики, так и на уровне розничной торговли. Однако в этом случае снижение издержек будет гораздо менее заметным.

3.1.3. Мониторинг подвижных объектов и его составляющие

Сбор и обработка информации об окружающем мире – основа концепции Интернета вещей. Для ее практического осуществления необходимо соединить воедино три составляющие концепции: средства связи между подключенными устройствами, средства идентификации объектов внешней среды и сенсоры, способные воспринимать информацию об окружающем мире.

Среди информационных технологий, решающих данные задачи, одно из ключевых мест занимают системы электронного мониторинга. Под мониторингом понимается систематический сбор и обработка информации, которая может быть использована для улучшения процесса принятия решения, а также, косвенно, для информирования общественности или прямо как инструмент обратной связи в целях осуществления проектов, оценки программ или выработки политики. Наиболее близкий русский эквивалент слова «мониторинг» – отслеживание. Термины «контроль», «надзор», «присмотр», которые иногда указывают в качестве синонимов, имеют несколько иное значение.

В свою очередь, электронный мониторинг – это исполнение функций мониторинга электронными средствами. Электронный мониторинг как одна из технологий Интернета вещей включает в себя все звенья рассмотренной выше цепочки.

Системы электронного мониторинга содержат в себе три составляющие: навигационную, геоинформационную и транспортную. Каждая из них имеет прямое соотношение со звеньями технологической цепочки Интернета вещей.

Навигационная составляющая выполняет задачу идентификации физического объекта во внешней среде, сбор информации, идентификацию сенсоров в сети. Транспортная составляющая представляет собой звенья, при помощи которых собранные данные передаются для дальнейшей обработки. Геоинформационная составляющая выступает в качестве заключительных звеньев, где обеспечивается хранение информации и ее обработка, а также может осуществляться представление ее конечным пользователям.

Таблица 9

Соотношение составных частей системы электронного мониторинга с технологической цепочкой Интернета вещей

Технологическая цепочка Интернета вещей	Составляющие системы электронного мониторинга
Идентификация объекта	Навигационная
Получение данных	Навигационная
Идентификация сенсора	Навигационная
Передача данных	Транспортная
Хранение и обработка	Геоинформационная
Представление информации	Геоинформационная

3.1.3.1. Навигационная составляющая

Решение задачи осуществления электронного мониторинга связано с необходимостью автоматизации определения местонахождения подвижных объектов и субъектов, в том числе с использованием навигационного оборудования. Иными словами, возникает потребность в идентификации объекта в окружающей среде и дальнейшем определении его координат в автоматическом режиме.

Классификация систем и способов автоматизированного местоопределения

В основу классификации систем и способов автоматизированного местоопределения подвижных объектов положен подход, рекомендованный Международным консультативным комитетом по радио (МККР) Международного союза электросвязи в Отчете 904-1 XVI Пленарной ассамблеи (Дубровник, 1986).

В зависимости от размера географическая зона, на которой действует система автоматизированного местоопределения подвижных объектов, может быть:

глобальной, если зона действия составляет территории нескольких государств, материк, территорию всего земного шара;

зональной, ограниченной, как правило, границами некоторого региона;

локальной, рассчитанной на малый радиус действия, что характерно в основном для систем дистанционного сопровождения.

Методы определения местоположения, используемые в системах автоматизированного местоопределения подвижных объектов, по классификации МККР можно разбить на две основные категории:

- методы приближения (зональные системы);
- методы определения местоположения по радиочастоте.

Системы на базе методов приближения

С помощью достаточно большого количества базовых станций операторов мобильной сотовой связи, точное местоположение которых известно, создается сеть контрольных зон. Местоположение контролируемого подвижного объекта определяется по мере прохождения им контрольных зон. Информация от базовых станций передается на сервер мониторинга.

Для зональных систем точность местоопределения и периодичность обновления данных напрямую зависят от плотности расположения базовых станций по территории действия системы. Методы приближения требуют развитой инфраструктуры связи для организации подсистемы передачи данных с большого числа базовых станций в системе мониторинга и поэтому являются весьма дорогими при построении систем, охватывающих большие территории.

Радиочастотные методы местоопределения

Данную группу методов можно условно разбить на две подгруппы:

- методы радиопеленгации, когда абсолютное или относительное местоположение подвижного объекта определяется при приеме излучаемого им радиосигнала сетью стационарных или мобильных приемных пунктов;
- методы, реализующие вычисление координат по результатам приема специальных радиосигналов в приемном устройстве (методы прямой или инверсной радионавигации).

Методы радиопеленгации

Принцип работы системы, основанной на методах радиопеленгации, – прием сигнала, излучаемого малогабаритным радиомаяком на контролируемом объекте, сетью стационарных радиоприемных центров и вычисление области неопределенности положения подконтрольного лица методом триангуляции. Применение широкополосных сигналов обеспечивает высокую частоту обновления информации в системе при высокой помехозащищенности. Точность местоопределения зависит от плотности размещения стационарной радиоприемной сети на территории и может составлять единицы метров в режиме непрерывного слежения и корректировки данных по электронной карте.

Таким образом, радиомаяк выступает в качестве устройства, при помощи которого информация о физическом положении объекта во внешней среде транслируется на радиоприемные центры, которые выступают в качестве звена, обрабатывающего информацию. В результате данные о реальном мире переводятся в информационное пространство в автоматизированном режиме.

Системы, основанные на методах радиопеленгации, хорошо зарекомендовали себя при использовании их на открытой местности. Однако в условиях плотной городской застройки система имеет большие погрешности. Кроме того, стоимость инфраструктуры, необходимой для охвата значительной площади, весьма велика.

Методы радионавигации

Реализуются на основе импульсно-фазовых наземных и спутниковых навигационных систем. Наилучшие точностные и эксплуатационные характеристики в настоящее время имеют спутниковые навигационные системы, в которых достигается точность местоопределения в стандартном режиме не менее 50–100 м, а с применением специальных методов обработки информационных сигналов в режиме фазовых определений или дифференциальной навигации – до единиц метров.

Достоинство этих методов – глобальность местоопределения, что позволяет применять их практически на любых территориях и трассах любой протяженности. Космическая радионавигация воплотила в себе новейшие достижения компьютерных и телекоммуникационных технологий. Симбиоз спутниковой системы позиционирования, современной радиосвязи и электронной картографии позволяет определять местопо-

ложение контролируемого объекта или субъекта, вычислять расстояния, задавать маршруты и отслеживать их соблюдение, получать справки о картографических объектах.

Внедрение спутниковой навигации снижает эксплуатационные затраты за счет эффективного использования имеющихся ресурсов.

Спутниковые системы навигации

Принцип работы спутниковых систем навигации основан на измерении расстояния от антенны на объекте (координаты которого необходимо получить) до спутников, положение которых известно с большой точностью. Таблица положений всех спутников называется альманахом, которым должен располагать любой спутниковый приемник до начала измерений. Каждый спутник передает в своем сигнале навигационное сообщение, содержащее весь альманах. Таким образом, исходя из расстояний до нескольких спутников системы, с помощью обычных геометрических построений на основе альманаха спутниковый приемник вычисляет положение объекта в пространстве (рис. 57).

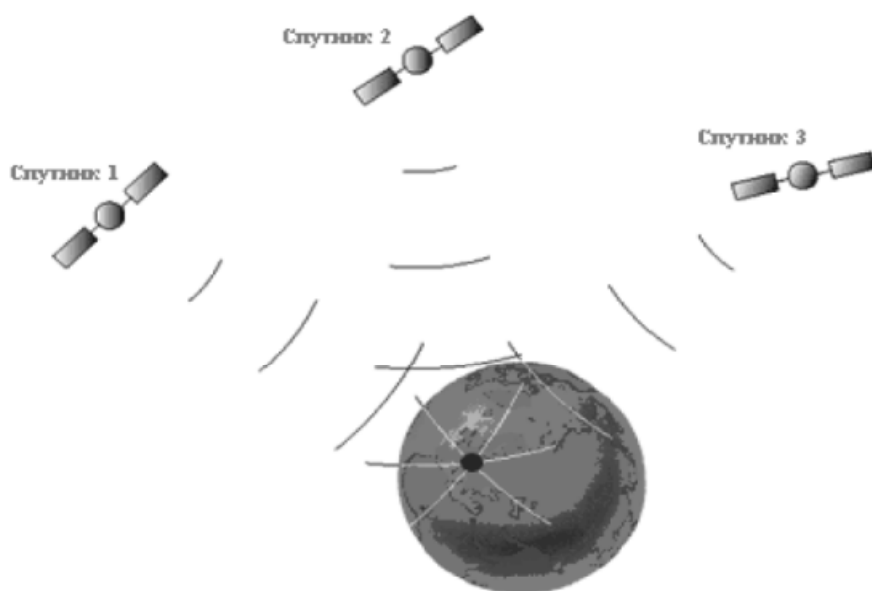


Рис. 57. Группа спутников навигационной системы

Метод измерения расстояния от спутника до антенны приемника основан на постоянстве скорости распространения радиоволн. Для осуществления возможности измерения времени распространения радиосигнала каждый спутник навигационной системы излучает сигналы точного времени в составе своего сигнала, используя точно синхронизированные с системным временем атомные часы. При работе спутникового приемника его часы синхронизируются с системным временем, и при дальнейшем приеме сигналов вычисляется задержка между временем излучения, содержащимся в самом сигнале, и временем приема сигнала. Располагая этой информацией, навигационный приемник вычисляет координаты антенны.

При решении задач местоопределения с использованием спутниковых навигационных систем возникает ряд проблем, требующих специальных технических приемов по их решению:

- отсутствие атомных часов в большинстве навигационных приемников. Этот недостаток обычно устраняется требованием получения информации не менее чем с трех (2-мерная навигация при известной высоте) или четырех (3-мерная навигация) спутников;
- неоднородность гравитационного поля Земли, влияющая на орбиты спутников;
- неоднородность атмосферы, из-за которой скорость и направление распространения радиоволн могут меняться в определенных пределах;
- отражения сигналов от наземных объектов, что особенно заметно в городе;
- невозможность разместить на спутниках передатчики большой мощности, из-за чего прием их сигналов возможен только в прямой видимости на открытом пространстве.

На сегодняшний день известны следующие системы спутниковой навигации.

ГЛОНАСС – в нее входят 24 спутника, движущиеся над поверхностью Земли в трех орбитальных плоскостях. Начало работ по созданию ГЛОНАСС было положено в декабре 1976 г. Находится в промышленной эксплуатации с сентября 1993 г. Полная группировка, позволяющая непрерывно пользоваться средствами отечественной спутниковой навигации по всей территории планеты, в соответствии с Федеральной целевой программой «Глобальная навигационная система», должна состоять из 27 активных спутников, при этом система ГЛОНАСС обеспечит точность местоопределения наземного объекта на местности в пределах 1,5 м. Для обеспечения функционирования наземного сегмента системы Федеральное агентство по геодезии и картографии готовит отечественные цифровые карты необходимых масштабов.

NAVSTAR (GPS) – принадлежит министерству обороны США, что является ее главным недостатком. Находится в промышленной эксплуатации с 1995 г.

Бэйдоу («Большая Медведица») – разворачиваемая Китаем с 2007 г. подсистема GNSS, предназначенная для использования только в этой стране. Особенность – небольшое количество спутников, находящихся на геостационарной орбите. Планируется ввод в эксплуатацию к 2015 г.

Galileo – общеевропейская навигационная система, находящаяся на этапе создания спутниковой группировки. Ее создание планируется завершить в 2016 г.

IRNSS – индийская навигационная спутниковая система, находящаяся в состоянии разработки. Предполагается для использования только в этой стране. Первый спутник орбитальной группировки был запущен в 2008 г.

Из перечисленных навигационных систем в эксплуатации находятся только NAVSTAR (GPS) и ГЛОНАСС. Комбинированное использование обеих систем позволяет более точно определять координаты и повышает надежность функционирования системы местоопределения.

Для развития системы ГЛОНАСС в России в рамках государственно-частного партнерства в ноябре 2007 г. Роскосмосом при участии ОАО АФК «Система» зарегистрирована компания ОАО «Навигационно-информационные системы» (НИС). В ноябре 2008 г. на заседании Межведомственной рабочей группы с участием представителей Роскосмоса, Минкомсвязи и Министерства экономического развития предложено объединить разрозненных операторов спутниковой навигации на базе системы ГЛОНАСС в единую сеть на базе НИС.

Во исполнение постановления Правительства РФ от 12 сентября 2008 г. № 680 приказом Федерального космического агентства от 24 декабря 2008 г. № 187 ОАО «Навигационно-информационные системы» определено федеральным сетевым оператором по оказанию навигационных услуг в Российской Федерации. На базе НИС создается единый навигационно-информационный центр, который отвечает за распространение информационно-картографического обеспечения, а также создание единой технологической базы для всех операторов, работающих в сфере спутниковой навигации. ОАО «Навигационно-информационные системы» также уполномочено участвовать в разработке нормативных документов и стандартов лицензирования ГЛОНАСС.

3.1.3.2. Геоинформационная составляющая

Геоинформационная составляющая включает в себя хранение и обработку информации, а также представляет собой последнее звено в цепочке технологий Интернета вещей, определенное как технологии представления информации конечным пользователям.

Отображение данных о местоположении транспортных средств и других объектов осуществляется с использованием специализированных географических информационных (геоинформационных) систем.

Геоинформационные системы (ГИС) – это интегрированные в единой информационной среде электронные пространственно-ориентированные изображения (карты, схемы, планы и т.п.) и базы данных. Такая интеграция значительно расширяет возможности системы и позволяет упростить аналитические работы с пространственно-географической информацией.

ГИС характеризуются следующими отличительными особенностями:

- наглядностью представления семантической информации за счет отображения взаимного пространственного расположения данных на электронной карте;
- улучшением структурированности информации и, как следствие, повышением эффективности ее анализа и обработки.

Традиционный набор функций ГИС при работе с картой включает:

- показ карты в различных масштабах;
- размещение объектов обстановки и контролируемых объектов на различных информационных слоях электронной карты;
- выбор набора информационных слоев карты для отображения информации;

- зависимость внешнего вида отображаемых объектов от их семантических характеристик;
- оперативное получение информации об объекте при выделении его курсором мыши на отображаемой карте;
- возможность распечатки любых фрагментов карты.

Названные задачи определяют функциональное предназначение картографической основы:

- получение пространственной информации об интересующих пользователя ГИС объектах или событиях;
- отображение на карте анализируемых событий и явлений, информация о которых поступает из различных источников;
- получение адресной информации и привязка на ее основе внешних баз данных;
- анализ территории, объектов и событий с последующей визуализацией результатов в виде цветных тематических карт;
- задание маршрутов движения контролируемых объектов, расчет длины и временного графика передвижения по заданной территории.

Основа успешного создания и функционирования ГИС – наличие базовых электронных карт в необходимом масштабе.

Исходным картографическим материалом при построении ГИС служат карты и планы на бумажной основе, спутниковые и аэрофотоснимки, в результате специальной компьютерной обработки (оцифровки) которых создаются их растровые изображения, при последующей обработке (трассировке) которых получают многослойные векторные карты. Навигационные векторные карты обогащаются дополнительными атрибутами элементов карты и объектами, необходимыми для эффективной работы навигационной системы.

В Российской Федерации функции создания и ведения федерального картографо-геодезического фонда возложены на Федеральное агентство геодезии и картографии (Роскартография).

Пользование материалами Федерального картографо-геодезического фонда осуществляется согласно установленным требованиям: регистрация работ в территориальных управлениях геодезии и картографии, получение разрешения на использование материалов фонда, заключение договоров на предоставление неисключительных прав на использование и др.

3.1.3.3. Транспортная составляющая

Говоря терминами технологической цепочки Интернета вещей, транспортная составляющая относится к технологиям передачи данных. Для функционирования системы электронного мониторинга необходимо наличие системы передачи данных по каналам связи, отвечающей требованиям по пропускной способности, надежности и защищенности.

По своему типу эти каналы можно разделить на:

- проводные – по выделенным и коммутируемым внутризональным и местным каналам связи;
- мобильные – по каналам сотовой GSM-связи, объединенным в закрытые виртуальные GPRS/EDGE/3G-сети, для передачи GPRS-трафика, SMS-сообщений и голоса.

3.2. Контроль людей и животных

В настоящее время активно развиваются и получают широкое распространение системы, осуществляющие контроль людей и животных.

Системы мониторинга людей применяются в таких сферах, как:

- контроль местоположения сотрудников компаний;
- мониторинг состояния и местонахождения военнослужащих и сотрудников спецподразделений;
- мониторинг лиц, отбывающих уголовные наказания в виде ограничения свободы, или находящихся под домашним арестом;
- контроль нахождения и состояния детей и людей с ограниченными возможностями.

Современные системы мониторинга позволяют осуществлять эффективный контроль за:

- домашними питомцами;
- крупным рогатым скотом в сельском хозяйстве;
- дикими животными в научных целях.

3.2.1. Мониторинг персонала

Для мониторинга персонала могут использоваться два вида технологий:

- контроль перемещения;
- контроль присутствия.

Эти технологии различаются как используемым оборудованием, так и целями, для которых они внедряются. Системы контроля перемещения позволяют получить данные о местоположении сотрудника в любой момент времени в любой точке. Системы контроля присутствия в основном применяются для учета и контроля лиц на ограниченной территории (например, в пределах здания, предприятия).

3.2.1.1. Контроль перемещения

Технологии контроля перемещения предполагают наличие устройства (трекера), обеспечивающего определение координат субъекта по сигналам спутниковых навигационных систем или базовым станциям операторов сотовой связи. Использование спутникового навигационного сигнала обеспечивает определение местоположения субъекта с высокой точностью (менее 10 м). В мировой практике широкое распростра-

нение получили устройства, использующие сигнал GPS, что обусловлено тем, что навигационные приемники на базе GPS производятся более 10 лет и технология хорошо отработана, они имеют низкое энергопотребление и небольшую стоимость. Применение устройств, использующих сигнал ГЛОНАСС, до недавнего времени было ограничено их высокой стоимостью и большим энергопотреблением. Однако сегодня эта ситуация активно изменяется в свете активного участия отечественных и зарубежных компаний в разработке и производстве мультисистемных чипов ГЛОНАСС/GPS.

Использование навигационного поля, формируемого базовыми станциями сотовых операторов, ограничивается низкой точностью определения координат (более 100 м) и высокой стоимостью услуг оператора.

Трекеры, как правило, оснащаются модулем, обеспечивающим возможность передачи полученных навигационным приемником координат на сервер мониторинга по каналам мобильной сотовой связи.

Для обеспечения гарантированной идентификации контролируемого субъекта может применяться RFID-метка, которая закрепляется за конкретным сотрудником.

Координаты субъекта определяются с установленной периодичностью и пересылаются на сервер мониторинга, где происходит их накопление и последующая обработка.

Системы контроля перемещения позволяют отслеживать местонахождение и перемещения человека, а также автоматически контролировать посещение им установленных разрешенных и запрещенных зон. Данная информация может представляться в удобном для оператора виде с использованием электронных карт местности.



Рис. 58. Персональный трекер



Рис. 59. Мобильное контрольное устройство

3.2.1.2. Контроль присутствия

Технологии контроля присутствия предполагают наличие устройств (считывателей), контролирующих RFID-метки, закрепленные за субъектами контроля. Считыватели устанавливаются на входах/выходах контролируемых территорий, внутри помещений, а также в транспортных средствах и иных объектах. Данные от них по каналам

связи поступают на сервер мониторинга, где происходит их накопление и последующая обработка.

Технологии радиочастотной идентификации нашли применение не только в системах контроля товаров, оружия, но и в системах учета и контроля персонала.

Одной из наиболее часто встречающихся технологий является система ограничения доступа. Эта технология основана на использовании специальных карт, в которые встроены RFID-метки, и устройств пропускного режима, содержащих ридер. При поднесении карты к считывающему устройству оно получает данные о личности, сверяется с базой и определяет его права доступа. Такая технология позволяет помимо ограничения доступа осуществлять также контроль рабочего времени, но она не может быть использована для мониторинга сотрудников из-за малого радиуса считывания ридеров.

Однако современные технологии позволяют преодолеть эту проблему. Решение задачи мониторинга перемещения персонала заключается в использовании систем идентификации, позволяющих осуществлять распознавание объектов на расстоянии до 100 м без участия человека. Использование такого оборудования позволяет контролировать нахождение сотрудников в различных помещениях или различных подразделениях компании, при этом система не потребует дополнительных действий со стороны сотрудников. Идентификаторы могут быть выполнены в виде простых бейджей, браслетов (возможно оповещение при попытке снятия) или брелоков.

Список задач, которые позволяют решать системы, построенные на современном оборудовании радиочастотной идентификации (RFID):

- контроль рабочего времени персонала;
- контроль местоположения сотрудников;
- контроль нахождения сотрудников на рабочем месте;
- решение задач по обеспечению безопасности на объекте;
- управление доступом в помещения на предприятии.



Рис. 60. Турникет



Рис. 61. Стационарное контрольное устройство

3.2.1.3. Позиционирование с помощью радиомаяков

Новым уровнем развитием протоколов беспроводной передачи данных для мобильных устройств стал протокол Bluetooth Low Energy (BLE), который представляет собой технологию беспроводной персональной сети и используется для передачи данных на короткие расстояния. Как следует из названия, он использует минимальную энергию, сохраняя при этом дальность связи, такую же, как и стандартный Bluetooth.

В чем отличия BLE и обычного Bluetooth?

- Потребляемая мощность: Bluetooth LE потребляет очень мало энергии для своей работы. Устройство может работать до 3 лет от одной батарейки размером с монету.
- Стоимость: устройства BLE на 60–80% дешевле, чем традиционные Bluetooth.
- Применение: BLE идеально подходит для простых приложений, требующих небольшие периодические передачи данных.

BLE лег в основу технологии новой технологии iBeacon, представленной Apple в конце 2013 года. Технология позволяет мобильным приложениям (на устройствах iOS и Android) слушать сигналы радиомаяков из реального мира и каким-либо образом реагировать на них.



Рис. 62. Устройства iBeacon

В сущности технология iBeacon позволяет использовать микролокацию как внутри зданий, так и на открытой местности. Это открывает новые возможности по созданию навигационных систем на базе методов триангуляции, обеспечивающих точность позиционирования менее одного метра в местах, где невозможен прием спутникового навигационного сигнала.

Радиомаяки или датчики iBeacon – это устройства небольшого размера, которые можно устанавливать на стены и другие элементы конструкции помещений, излучающие в пространство радиосигнал по стандарту Bluetooth 4.0. Излучаемый на частоте 2,4 ГГц через регуляр-

ные промежутки времени радиосигнал содержит небольшой пакет (или пакеты) данных. Чаще всего это односторонняя передача такого сообщения. Маячки являются открытыми устройствами и транслируют свое сообщение всем устройствам. Такими устройствами являются смартфоны, которые периодически сканируют BLE и используют полученную информацию для взаимодействия с пользователем. Например, push-уведомления, подсказки или действия.



Рис. 63. Радиомаяки iBeacon

Как правило, датчики iBeacon работают от батареи. Срок работы датчика от одной батареи в среднем от одного до двух лет. Период вещания iBeacon составляет 100 мс. Высокая частота вещания сокращает срок службы батарейки, но позволяет смартфонам быстрее откликаться на сообщения. Здесь стоит заметить, что смартфон тоже охраняет свою батарею и сканирует BLE не постоянно, а по своим правилам. По стандарту BLE маячки могут вещать сигнал на расстояние до 100 м, на практике удалось добиться оптимального соотношения расстояние/мощность в 20 м и предполагаемого срока службы батареи 1 год.

Для позиционирования объекта с использованием iBeacon устройства BLE измеряют расстояния до радиомаяков, находящихся в зоне приема, и с помощью мобильного приложения, получающего по каналам беспроводной связи (GSM, WiFi) данные о месторасположении этих радиомаяков, рассчитывает собственные координаты или определяет свое относительное месторасположение в окружающем пространстве.

К возможным направлениям применения iBeacon уже в ближайшее время можно отнести:

- Музеи и выставки – разместив маяки около экспонатов, получаем возможность сделать интерактивный тур. Посетитель, подходя к экспонату, получает дополнительную информацию. Таким образом, значительно упростив задачи экскурсовода и даже полностью заменив их в будущем.
- Позиционирование в городе – расширив предыдущий пример до размера города и установив маяки в исторических местах и около памятников, получаем целый город-музей.
- Скидки и акции в магазинах – проходя мимо прилавков, получаем оповещения о скидках и новых предложениях.

- Помощь людям с нарушением зрения – смартфоны уже оснащаются возможностями, помогающими слабовидящим общаться со своим устройством, такие как преобразование текста в речь, распознавание голоса. При обнаружении маячка можно проигрывать голосовое сообщение о том, где пользователь находится и куда можно двигаться дальше.
- Кофейни, бары, рестораны – виртуальное меню с дополнительной информацией о блюде и рекомендациях по выбору.
- Учебные учреждения – вся необходимая информация для учащихся от расписания занятий до меню в столовой на сегодня.



Рис. 64. Варианты применения iBeacon

3.2.2. Мониторинг подконтрольных лиц

Мировой опыт электронного мониторинга подконтрольных лиц берет свое начало в последней четверти XX века. Впервые электронные средства стали применяться для контроля осужденных.

В конце 1983 г. Верховный суд штата Нью-Мексико разрешил использование электронных систем слежения и уполномочил судей штата приговаривать лиц, впервые совершивших преступление, к домашнему аресту с обязательным ношением ножных электронных браслетов.

После вынесения приговора в доме осужденного ставился радиоконтроллер, подключаемый к обычной телефонной сети. Браслет с радиомаяком надевался осужденному на ногу, и, если он отдалялся от контроллера на достаточно большое расстояние, в полицию поступал тревожный сигнал.

Система дистанционного контроля над осужденными получила распространение во многих странах. В США такая практика используется в 49 штатах из 50. В Европе система электронного контроля для усиления надзора за осужденными начинает использоваться все большим числом систем уголовного судопроизводства. Так, в Великобритании экспериментальная работа по электронному мониторингу началась в 1989 году.

В последующем функции электронного мониторинга стали расширяться до обеспечения режима слежения за перемещением осужденных с использованием сигналов GPS. В Великобритании слежение за осужденными практикуется с 2004 года.

Мониторинг подконтрольных лиц в России

В России мониторинг подконтрольных лиц в ближайшее время начнет активно применять Федеральная служба исполнения наказаний (ФСИН России) для контроля лиц, приговоренных к наказанию в виде ограничения свободы. Начиная с 2015 года планируется использование до 150 тыс. электронных браслетов с системами спутникового позиционирования. Из них примерно треть будут использовать отечественную систему ГЛОНАСС.

Данный вид надзора и контроля предусматривает для осужденных запрет посещения детских учреждений, таких как школы и детские сады; массовых мероприятий, таких как концертные залы, клубы; запрет на выезд за пределы определенного территориального образования, а также запрет на смену места работы, учебы и жительства без оповещения надзорного органа.

3.2.3. Контроль сотрудников спецподразделений

Датчик BulletVest (компания 3Arc) позволяет в автоматическом режиме осуществлять мониторинг (позиция по GPS, время, скорость движения) и может быть встроен в бронежилет для немедленного информирования о воздействии на него и быстрого реагирования.



Рис. 65. Датчик BulletVest (3Arc)

Информация может обрабатываться удаленно в режиме реального времени. В случае ранения человека, носящего жилет, автоматически создается и высылается отчет с детальной информацией о точке воздействия на жилет и траектории движения пули, нанесшей это воздействие. Эти сведения помогают контролирующим сотрудникам анализировать нападающего и предлагать правильные решения для сохранения жизни носителя жилета с минимальной задержкой.

Существуют две версии датчиков, которые позволяют либо использовать их в качестве самостоятельных устройств, либо совместно с датчиками огнестрельного оружия, используя радиоканал.

Кнопка самодиагностики позволяет запускать процесс проверки системы принудительно и также может быть использована в качестве тревожной кнопки для вызова помощи в чрезвычайной ситуации. Настройки системы могут быть изменены через компьютер или «по воздуху».

3.2.4. Мониторинг крупного рогатого скота

Технологии Интернета вещей активно применяются в сельском хозяйстве в Европе. Системы электронного мониторинга используются для контроля за перемещением крупного рогатого скота. Кроме того, система собирает информацию о физиологическом состоянии животных и передает ее фермерам.

Французская Medria Technologies и немецкая Deutsche Telekom разработали систему, которая информирует фермеров об отеле скота и готовности к спариванию. В стойлах и в поле устанавливаются устройства для связи по типу M2M (machine to machine), снабженные сим-картами. К животным крепятся датчики, собирающие информацию и передающие ее на устройства сбора данных. Устройство передает фермеру информацию посредством SMS. В 2012 году данной технологией пользовались 4000 европейских ферм⁸³.

В Голландии в уши коров вживляют радиочастотные датчики, которые позволяют следить за состоянием животных. Датчики имплантируются в ушную раковину животных. Технология представлена компанией Sparked⁸⁴.

3.3. «Умный» дом

«Умный» дом – это современный автоматизированный жилой дом, в котором используются системы датчиков, сенсоров и контроллеров для повышения удобства проживающих там людей⁸⁵. «Умный» дом в состоянии распознавать конкретные ситуации, которые происходят в пределах охватываемой сенсорами и датчиками территории, и соответствующе на них реагировать. К примеру, такой дом может самостоятельно выключить освещение в комнате, когда человек покинет ее. Или включить чайник, когда утром прозвенит будильник и жильцы начнут собираться на работу.

⁸³ Тэббитт С. Интернет вещей начинает жить собственной жизнью // CISCO.COM : Новости. URL: <http://www.cisco.com/web/RU/news/releases/txt/2012/112612b.html> (дата обращения 25.02.2014).

⁸⁴ Про автомобили, голландских коров и уникальные свойства Интернета вещей // CISCO.COM : Новости. 2011. URL: <http://www.cisco.com/web/RU/news/releases/txt/2011/070711d.html> (дата обращения 25.02.2014).

⁸⁵ URL: <http://habrahabr.ru/post/129743/>

Зарубежная статистика утверждает, что использование технологий «умного» дома более чем оправданно с экономической точки зрения. Так, эксплуатационные затраты сокращаются на 30%, затраты на электроэнергию – на 30%, затраты на воду – на 41%, затраты на отопление – на 50%. Кроме того, выбросы углекислого газа сокращаются в целом на 30%⁸⁶.

Технические решения, совокупность которых и составляет концепцию умного дома, не заменяют предметы обихода. Напротив, большинство сенсоров, датчиков и контроллеров встраиваются в привычные вещи. Это утверждение можно проиллюстрировать несколькими примерами. Так, «умная» дверь выполняет функционал, заложенный и в обычную дверь: защищает дом от посторонних. Разница лишь в форме его реализации и уровне автоматизации. Если обычную дверь необходимо открывать вручную ключом, то «умная» дверь может быть открыта при помощи смартфона владельца.

В случае с «умным» столом можно говорить о расширении функционала. При помощи инфракрасных датчиков он способен отслеживать положение людей в помещении для точного позиционирования. Далее эта информация будет использоваться системой, которая отрегулирует освещение в доме: выключит его в пустых помещениях и включит лампы в комнатах с людьми. Разумеется, «умный» стол можно использовать и по прямому назначению: обедать за ним, класть какие-либо предметы и т.п.

Поскольку технологии «умного» дома встраиваются в обычные предметы, в качестве критерия классификации можно использовать функциональное назначение оборудования, которое они дополняют. Сенсоры, датчики и контроллеры «умного» дома образуют несколько функциональных систем⁸⁷:

- система освещения;
- система электропитания;
- система климата;
- система связи;
- система безопасности и мониторинга.

Каждая из перечисленных систем способна работать автономно, но наилучший результат достигается при совместном использовании всех пяти систем. Как правило, в «умном» доме имеется единый центр контроля за работой всех пяти систем. Обычно доступ к нему можно получить через различные мобильные устройства.

⁸⁶ Перспективы рынка систем «умный дом» // 220HELP.RU : Инженерные системы для дома. URL: <http://www.220help.ru/uslugi/umnyj-dom/perspektivy-gynka> (дата обращения 27.03.2014).

⁸⁷ Концепция системы «Умный Дом» // ASCENTIS.RU : Инженерный центр. URL: <http://www.ascentis.ru/smart/smtheory/39-smtheorycon> (дата обращения 27.03.2014).



Рис. 66. Устройство «умного» дома

Каждая из систем включает в себя различные устройства и подсистемы, целесообразные ставящимся перед системой задачам, а потому имеет смысл более подробно остановиться на каждой из них. Так, система освещения включает в себя датчики, реагирующие на присутствие человека. В ином случае система освещения может брать информацию о присутствии от других систем «умного» дома. Тем не менее возможность определить присутствие человека является одной из базовых, поскольку она позволяет включать свет только тогда, когда в помещении кто-то находится.

Вторым обязательным компонентом системы освещения выступают автоматические устройства, позволяющие включать и выключать свет в соответствии с заданными алгоритмами. Сюда же относятся устройства, при помощи которых система освещения может закрывать шторы, ставни и т.п.

Подсистема электропитания в составе системы «умного» дома. Она поддерживает непрерывную работу электротехнических устройств и распределяет нагрузку. Сюда же относится контроль за генератором электрического тока, если речь идет о частном доме. Кроме того, система способна составлять аналитические отчеты о потреблении электроэнергии, тем самым способствуя снижению затрат на оплату коммунальных услуг. Детальная настройка системы позволяет настроить автоматическое отключение от сети электропитания устройств, которые владельцы домов по какой-то причине забыли выключить сами.

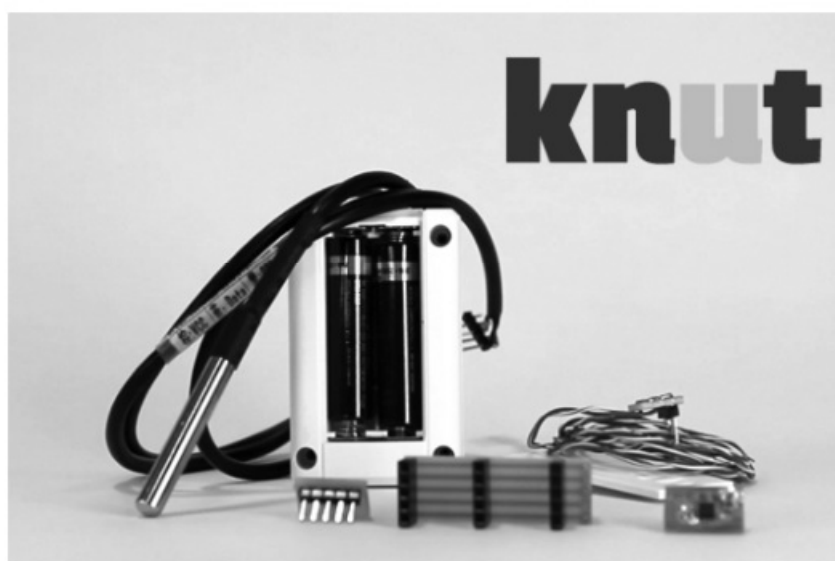


Рис. 67. Модульная система Knut для контроля влажности воздуха, температуры (в том числе воды) и статуса «открыт/закрыт» для дверей

Климат-система включает в себя вентиляцию, кондиционирование и отопление. Наибольшее значение для ее адекватного функционирования имеют температурные датчики, датчики влажности и сенсоры передвижения жителей дома. Система позволяет поддерживать в доме оптимальную температуру, поскольку может в реальном времени мониторить температурные показания. Это сокращает затраты электроэнергии – так, система может отключать кондиционер с наступлением темного времени суток, когда заданная температура может поддерживаться без принудительного охлаждения воздуха. Также климат-система может быть оборудована автоматикой для открытия/закрытия окон с целью вентиляции или охлаждения помещения.

Система связи включает в себя не только интернет и телефонию, но также локальную сеть, в рамках которой работают все подсистемы «умного» дома. А система безопасности и мониторинга может состоять из датчиков огня, датчиков задымления, средств видеонаблюдения, средств контроля доступа в помещение, средства удаленного информирования о происшествиях в доме владельцев и экстренных служб.

3.4. «Умный» город

Идея проникновения технологий в нашу жизнь непрерывно развивается для использования в интересах миллионов человек. Использование сетевых технологий и в том числе Интернета становится всеобъемлющим. Интернет вещей распространяется от «умного» дома до «умного» города – комплексных систем со множеством тесно взаимосвязанных подсистем. Смарт-инфраструктуру можно развернуть на улицах городов даже в масштабах целых стран и регионов. Так, в концепции «умного» города (smart city) представляется возможным снизить нагрузку на городские службы и инфраструктуры посредством повсеместного внедрения различных датчиков и анализаторов (загрязнения воды и окружающей среды, шума, энергоэффективности, линий коммуникаций).

Транспортная сфера становится одним из основных двигателей развития интеллектуальных систем. Так, в России сегодня реализуется пилотный федеральный проект «Инновационные дороги». Помимо использования современных материалов, транспортная инфраструктура инновационных дорог будет оснащаться множеством сенсоров и датчиков, которые помогут оптимизировать освещение трасс, продублируют светодиодами дорожную разметку, определяют требуемые объемы реагентов во время гололеда, адаптируют скоростной режим под текущую загруженность трассы. Предусмотрены и «умные» дорожные знаки, «общающиеся» с автомобилем посредством специальных датчиков.

К примеру, ультразвуковые датчики, установленные на дорогах, способны собирать информацию о плотности транспортного потока. В связке с «умными» камерами наблюдения, которые распознают аварии и заторы, они собирают информацию о загрузке дорог и передают ее в специальный центр. По такому принципу работает, к примеру, Центр управления транспортом в Токио. Среди прочих смарт-технологий там активно используются инфракрасные датчики, которые посылают информацию об оптимальных маршрутах водителям проезжающих мимо автомобилей. За счет работы этого центра, в котором трудится всего 30–40 человек, пробкой в Токио считается движение со скоростью ниже 40–60 км/ч. К этой же сфере относится введение беспилотных поездов, которые движутся без машинистов. Примеры автоматизированных поездов уже сейчас можно встретить на некоторых ветках в Париже, Дубае, Копенгагене, Нюрнберге и т.п.

Еще одним из примеров элементов инновационных дорог являются так называемые лазерные «виртуальные пешеходы». Пришедшая из Южной Кореи и адаптированная рядом европейских городов концепция предполагает установку датчиков приближения пешехода к дороге, которые проецируют лазерное изображение пешеходов/световую завесу, предупреждающие водителей о пешеходном переходе⁸⁸.



Рис. 68. «Виртуальные пешеходы»

⁸⁸ URL: http://vik95.ru/poleznoe/stroitelstvo_dorog_budushhego_ne_za_gorami.html (дата обращения 27.03.2014).

Но, разумеется, применение интеллектуальных систем не ограничивается одним лишь транспортом. Такие системы могут оптимизировать работу больниц и прочих институтов здравоохранения; качественно распределять производственные мощности на предприятиях; оптимально использовать топливо, электроэнергию и расходные материалы и т.п. В целом в корпоративной среде интеллектуальные системы, взаимодействующие с объектами управления и внешней средой в реальном времени, способны оптимизировать бизнес-процессы, удерживать бизнес на пике конкурентоспособности и увеличивать прибыль.

Особенно преуспела в развитии «умного города» компания IBM, реализовавшая на практике уже многие элементы городских smart-технологий⁸⁹:

- единая транспортная карта (Лондон);
- «умные» LED-светофоры;
- «умные» перекрестки (Сингапур);
- системы мониторинга трафика и чрезвычайных ситуаций в реальном времени (Рио-де-Жанейро);
- технология Smart Grid в энергетике (Амстердам, Чаттануга, Дублин, Малага и Масдар);
- электрические транспортные средства (Амстердам и Малага);
- инструменты поддержки и подготовки в области ИКТ (Кейптаун);
- командный центр комплексной безопасности (Лаваса).

При этом как в масштабах IBM, так и в концепциях развития smart city других компаний в число основных секторов, где используются «умные» решения, входят в первую очередь энергетика, здравоохранение, транспорт, инфраструктура.

К примеру, «умная» энергетика предполагает, что интеллектуальная энергетическая система города поможет горожанам и энергетикам сделать осознанный выбор среди многочисленных возможностей покупки, продажи и потребления энергии. Так, компания Center Point Energy (Хьюстон, США) установила в городе более 2 млн «умных» счетчиков энергии, благодаря которым жители получили возможность работать с информацией по энергообеспечению через Интернет⁹⁰. На практике это означает, что они могут сравнивать свое энергопотребление с другими квартирами, домами или даже городами, получать персональные рекомендации (например, по запуску определенного объема белья в стирку в определенное время), регулировать работу бытовой техники, получать уведомления о превышении своего лимита энергопотребления.

⁸⁹ URL: <http://www.infocity.az/?p=19509#!prettyPhoto> (дата обращения 27.03.2014).

⁹⁰ URL: <http://sciencesation.ru/assets/files/lectures/2013/sokovnin.pdf> (дата обращения 27.03.2014).



Рис. 69. Портал IBM Smart City

На данном уровне смарт-архитектуры постепенно внедряются системы экстренного реагирования. Российский проект ЭРА-ГЛОНАСС предполагает оснащение транспортных средств специальными устройствами, которые определяют географическое положение автомобиля и информируют полицию и медицинскую службу или МЧС в случае аварии. Похожие системы существуют и в других регионах мира: SIMRAW в Бразилии, OnStar в США, eCall в Европе и др.

К примеру, реализованный в Рио-де-Жанейро проект Rio Operations Center представляет собой систему оповещения городских властей и аварийных служб об изменении погодных условий. Данные более чем 30 ведомств (по метеосводкам, состоянию почв, ситуациям на дорогах) были интегрированы для своевременной генерации оповещений по приближающимся ливням и природным катаклизмам. Городские службы в итоге получают информацию, на какие участки нужно послать максимальное количество спасателей, где нужно быстро организовать эвакуацию людей, какие дороги оптимальны для использования.

Как и в случае с «умным» домом, существуют и комплексные решения для «умных» городов. В 2014 году компания Intel заявила, что готова превратить город-миллионер Сан-Хосе (штат Калифорния) в первый в мире «умный» город, где компьютеры с многочисленными сенсорами и датчиками возьмут на себя управление всей инфраструктурой. Такая система сможет в реальном времени отслеживать мельчайшие изменения в городской жизни, включая пробки, шумовое загрязне-

ние, чрезвычайные происшествия и т.п., а также координировать работу городских служб и полиции. При этом в Intel полагают, что киберпреступность не представляет угрозы, поскольку пилотный проект использует сложную защиту на основе облачных технологий⁹¹.

За счет массового распространения Интернета и подключенных к нему объектов популярность приобрели интеллектуальные технологии различных уровней применения – от «оптимизации» жизни одного отдельно взятого человека до управления и оптимизации деятельности городов и стран. Однако существует множество барьеров, замедляющих темпы развертывания этих технологий. Так, компания IBM оценила требования к аппаратным ресурсам «умных городов»: приблизительно 1 млрд транзисторов в микросхемах встроенных устройств на одного жителя⁹². А с точки зрения программных ресурсов быстрому развитию подобных ИКТ-технологий препятствуют отсутствие общих стандартов и возможная несовместимость компонентов технологий различных производителей. К тому же применение Интернета вещей в сфере бизнеса (например, логистики и поставок компаний) частично затрудняется фактом закрытости и изолированности корпоративных/частных сетей, обеспокоенностью вопросом защиты персональных данных.

3.4.1. Интернет вещей в сфере транспорта

Одним из перспективных и активно исследуемых направлений развития технологий Интернета вещей является сфера транспорта. Технологии Интернета вещей, применяющиеся сегодня в этой области, позволяют в значительной степени оптимизировать движение транспортных средств любой категории.

В настоящий момент наибольшее распространение получили технологии мониторинга транспортных средств, при помощи которых диспетчерский центр может в реальном времени получать данные о географическом положении транспортного средства, а также информацию с многочисленных подключенных устройств, установленных на борту. Последнее становится возможным за счет идентификации транспортного средства, которая превращает его в подключенную вещь.

Одним из векторов развития технологий Интернета вещей является разработка «умных» автомобилей и «умной» инфраструктуры, способных поддерживать коммуникацию V2V и V2I без непосредственного участия человека. В данных масштабах автомобили с установленными сенсорами и датчиками интерпретируются как составная подсеть глобальной сети подключенных вещей, способных без участия человека осуществлять сбор информации об окружающей среде, состоянии и перемещении транспортного средства в реальном времени. В конечном

⁹¹ URL: <http://www.unian.net/science/928470-intel-sozdast-v-kalifornii-umnyiy-gorod-kotoryim-budut-upravlyat-kompyuteryi-smi.html> (дата обращения 27.03.2014).

⁹² URL: <http://www.infocity.az/?p=19509> (дата обращения 27.03.2014).

счете это приведет к образованию «умной» транспортной среды, объекты которой смогут самостоятельно взаимодействовать друг с другом и решать задачи, которые сегодня выполняет человек.

3.4.1.1. Получение данных о транспортных средствах

В рамках концепции Интернета вещей транспортное средство с установленными сенсорами может восприниматься как подключенная вещь, а бортовые сенсоры и датчики – как подключенные устройства. Идентификацию транспортного средства обеспечивает мобильный модуль со встроенным контроллером, а идентификация сенсоров во внутренней сети транспортного средства производится либо им же, либо CAN-шиной.

Технологии Интернета вещей, которые могут быть использованы в сфере получения данных о транспортных средствах, включают в себя множество разнообразных решений. Однако на сегодняшний день наибольшее развитие получили системы электронного мониторинга транспорта.

Системы электронного мониторинга транспорта относятся к области мониторинга подвижных объектов. Подобные системы включают в себя устройства для обеспечения спутниковой навигации, оборудование и технологии сотовой и/или радиосвязи, а также различную вычислительную технику. В качестве синонима к выражению «мониторинг транспорта» нередко используется словосочетание «трекинг транспорта». В целом можно констатировать, что оба определения равнозначны и смысловой разницей не обладают.

В наиболее общем виде системы электронного мониторинга включают в себя множество транспортных средств и диспетчерский центр. На транспортные средства устанавливаются различные регистраторы, а в диспетчерский центр ставится компьютер или несколько серверов, обеспечивающих получение, хранение, обработку и визуализацию информации. Сегодняшние системы транспортного мониторинга предполагают возможность двусторонней связи между диспетчерским центром и транспортными средствами⁹³.

Электронный транспортный мониторинг можно разделить на пассивный (офлайновый) и активный (онлайновый). Офлайновые системы подразумевают, что информация о координатах и иных параметрах транспортного средства считывается на диспетчерском пункте или во время остановки по беспроводным каналам связи или при помощи проводного подключения.

⁹³ Соловьев М. Телематические аспекты в системах мониторинга подвижных и стационарных объектов : [Электронный документ] // GWE.RU : Компания «Геликс». Сис. требования: Adobe Reader. URL: http://www.gwe.ru/download/BT_03_35-37.pdf (дата обращения 27.03.2014).



Рис. 70. Общая схема работы систем транспортного мониторинга

К плюсам офлайновых систем относятся простота в использовании и установке, низкая стоимость, отсутствие абонентской платы за передачу трафика по беспроводным сетям. Тем не менее данные системы не могут быть отнесены к сфере технологий Интернета вещей, поскольку они не позволяют получать данные о транспортных средствах в реальном времени и обеспечивают лишь послерейсовый контроль. А с увеличением охвата сотовых операторов распространенность подобных систем существенно снизилась и сегодня практически не имеет ценности для коммерческих и государственных структур.

Куда больший интерес представляют онлайн-системы транспортного мониторинга. В случае их использования на транспортное средство устанавливается мобильный модуль, включающий в себя приемник спутниковых сигналов (также называемый «контроллер» или «трекер») и модуль хранения и передачи координат. Программное обеспечение, вшитое в мобильный модуль, получает координаты от спутников, сохраняет их в энергонезависимой памяти и отправляет в диспетчерский центр посредством модуля передачи. Сервер получает данные с транспортного средства, которые обрабатываются при помощи специального программного обеспечения и выдаются диспетчеру.

Таким образом, техническая составляющая онлайн-систем транспортного мониторинга включает в себя:

- Транспортное средство с контроллером, использующим протоколы GPS и/или ГЛОНАСС.
- Встроенные и установленные датчики состояния транспортного средства и его отдельных устройств, а также различные сенсоры.
- Средства для GSM, CDMA, УКВ или спутниковой беспроводной связи.
- Сервера с программным обеспечением для приема, хранения и обработки информации.
- Компьютер диспетчера или пользовательские веб-приложения.

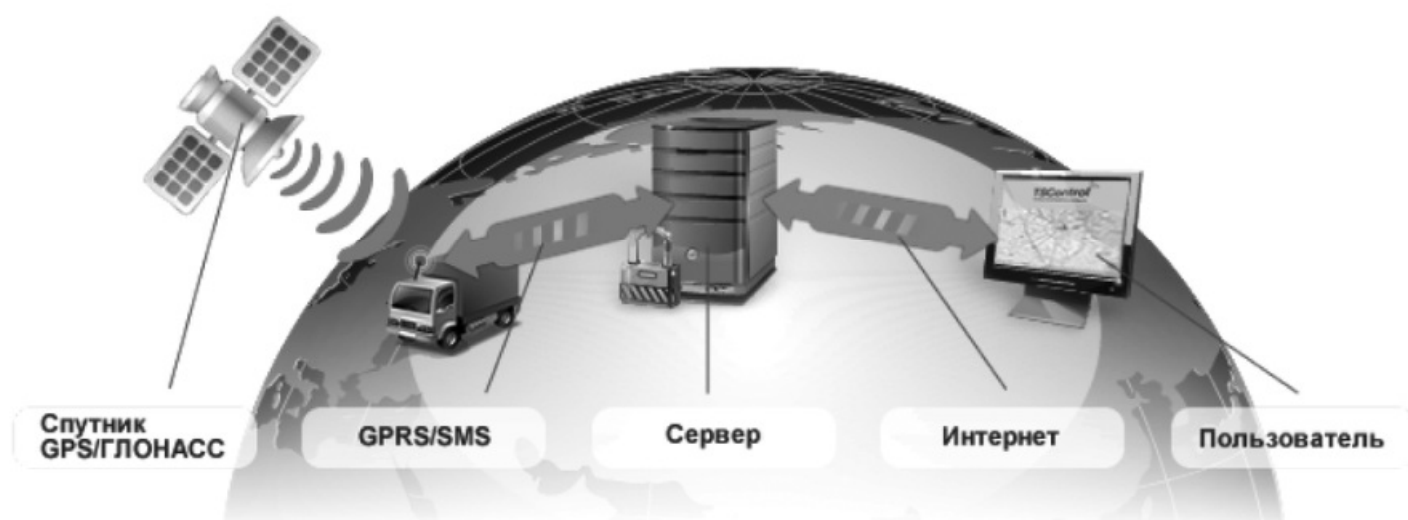


Рис. 71. Схема работы онлайн-систем транспортного мониторинга

Представленная выше цепочка позволяет работать с данными о транспортном средстве, поступающими в реальном времени. Тем не менее непрерывный поток данных создает определенную нагрузку на сервера и увеличивает объем трафика, а соответственно и издержки на использование системы транспортного мониторинга. В связи с этим, онлайн-системы транспортного мониторинга обычно обладают несколькими режимами передачи данных:

- непрерывная передача данных;
- периодическая передача данных;
- передача данных по событию;
- передача данных по запросу диспетчеров.

В качестве отдельной категории можно выделить так называемый «интеллектуальный трекинг», который позволяет определить частоту записи географических координат транспортного средства и необходимость их отправки в диспетчерский центр. Как правило, интеллектуальный трекинг учитывает такие параметры транспортного средства, как скорость, направление и время. Существует информация, что использование интеллектуального трекинга позволяет уменьшить количество передаваемого трафика на 80–90%, при этом сохранив детализацию маршрута транспортного средства.

Разумеется, систему электронного мониторинга транспорта можно рассматривать в категориях технологической цепочки Интернета вещей, сформулированной ранее. Соответствие компонентов систем электронного мониторинга транспорта звеньям данной цепочки можно проиллюстрировать следующим образом (табл. 10).

**Технологическая цепочка Интернета вещей
в электронном мониторинге транспорта**

Звено технологической цепочки Интернета вещей	Компонент системы электронного мониторинга транспорта
Идентификация объекта в окружающей среде	Методы идентификации транспортного средства (например, по VIN-коду автомобиля)
Автоматизированное получение данных об объекте	Контроллер, встроенные и установленные датчики и сенсоры
Идентификация сенсоров и датчиков	Подключение к контроллеру, обладающему уникальной идентификацией; идентификация сенсоров и датчиков внутри сети
Передача данных с подключенных устройств на сервер	Средства для GSM, CDMA, УКВ или спутниковой беспроводной связи
Технологии хранения и обработки	Внутренняя (как правило, энергонезависимая) память; внутреннее и серверное программное обеспечение
Технология представления информации пользователям	Программное обеспечение диспетчерских компьютеров или веб-приложения для доступа к полученной и обработанной серверами информации

Здесь стоит сделать одно важное дополнение. Системы транспортного мониторинга относятся к классу систем мониторинга подвижных объектов, поэтому идентификация объекта внешней среды (которым в данном случае выступает транспортное средство) как такового – недостаточное условие для полноценного применения на практике концепции Интернета вещей. В случае с транспортным мониторингом особое значение получают контроль присутствия и контроль перемещения.

Контроль присутствия позволяет подтвердить, что транспортное средство движется по определенному маршруту. Непрерывное получение данных о транспортном средстве в реальном времени не является обязательным условием для подобного контроля. Так, транспортное средство с радиочастотными метками может двигаться по заданному маршруту, в определенных точках которого стоят автоматические считыватели информации. В результате удастся обеспечить контроль пере-

мещения транспортного средства. А при наличии в контрольной точке средств беспроводной связи бортовая система сможет передать в диспетчерский центр и другие показания датчиков.

В свою очередь, контроль перемещения предполагает более детальный контроль местоположения транспортного средства в пространстве. Наличие средств беспроводной связи является обязательным условием такого контроля. А наличие беспроводной связи позволяет передавать в диспетчерский центр и другие параметры подконтрольного транспортного средства.

В контексте технологий Интернета вещей транспортное средство является подключенной вещью, поскольку установленное на него оборудование обеспечивает соответствие критериям наличия личного уникального адреса, функции памяти и обладает свойством коммуникативности. Сенсоры и датчики, входящие в состав бортового оборудования, являются подключенными устройствами, поскольку они соответствуют перечисленным выше критериям, а также способны воспринимать объективные свойства внешней среды.

3.4.1.2. Задачи, решаемые системой транспортного мониторинга

В наиболее общем смысле задача системы транспортного мониторинга – собрать определенный объем информации о входящих в нее транспортных средствах. Детализируя, перечень задач подобных систем можно сформулировать следующим образом:

- определение местоположения транспортного средства, его скоростных показателей и дополнительных параметров;
- контроль графика движения транспортных средств и учет их передвижения;
- сбор статистики с целью дальнейшей оптимизации;
- обеспечение безопасности пассажиров, водителей, транспортных средств и перевозимых грузов.

Задачи, решаемые системами транспортного мониторинга, можно подразделить на базовые и специфические. К базовым задачам относится отслеживание пространственно-временных показателей транспортного средства, определяющих его географическое положение. Возможность отслеживания данных показателей формирует первичный объем данных о транспортном средстве, без которого сбор дополнительных данных чаще всего не имеет смысла.

К специфическим задачам можно отнести сбор дополнительной информации о транспортном средстве в соответствии с его технико-функциональными особенностями.

**Специфические задачи систем электронного
транспортного мониторинга**

Основание классификации	Тип транспортного средства	Пример специфической задачи
По среде передвижения транспортных средств	Наземное колесное	Оптимизация стиля вождения
	Наземное железнодорожное	Оповещение о приближении к платформам
	Морское	Уровень ватерлинии
	Речное	Автоматическое сравнение высоты транспортного средства с высотой мостов
	Воздушное	Контроль герметичности салона
По функциям и решаемым задачам транспортных средств	Личный транспорт	Информирование о попытке угона и дальнейшая блокировка двигателя
	Общественный транспорт	Учет числа пассажиров
	Перевозка грузов	Анализ уровня загруженности транспортного средства
	Перевозка опасных грузов и грузов со специфическими условиями хранения и транспортировки	Контроль соблюдения условий перевозки
	Перевозка особо ценных грузов	Контроль безопасности груза и водителя
Службы экстренного реагирования	Определение ближайшего к месту происшествия транспортного средства	

Возможность решения тех или иных задач напрямую зависит от оборудования, датчиков и сенсоров, установленных на транспортное средство. Теоретически число параметров, информацию о которых можно получить за счет использования таких систем, практически не ограничено. Однако специфика работы каждой организации предполагает упор на сбор определенной, наиболее важной информации о транспортном средстве.

3.4.2. «Умная» транспортная инфраструктура

«Умная» транспортная среда – это совокупность транспортных средств, их бортовых сенсоров и объектов инфраструктуры, которые могут взаимодействовать друг с другом с целью обеспечения различных форм транспортировки без непосредственного участия человека.



Рис. 72. Составные части «умной» транспортной среды

Первым этапом создания «умной» транспортной среды стала возможность захвата данных об отдельном транспортном средстве. Технологии, используемые для такого сбора данных, сегодня относятся к системам электронного мониторинга транспорта и используются частными и государственными организациями, деятельность которых так или иначе связана с обеспечением транспортировки грузов или пассажиров.

Возможность получать информацию о различных параметрах транспортного средства в реальном времени имеет принципиальное значение для создания «умной» транспортной среды. Фактически, она позволяет автоматизировать задачи, которые ранее мог выполнить только водитель-человек. Контроль открытия дверей, контроль топлива, контроль давления в шинах, контроль нагрузки на ось, контроль температуры – все эти и многие другие задачи сейчас возможно решить автоматически, либо без участия человека, либо с его минимальным участием.

В некотором смысле, роль человека как оператора транспортного средства неуклонно снижается. Сегодня можно добиться полной или практически полной автоматизации контроля состояния транспортного средства. А по мере развития технологий «умного» автомобиля и «умной» инфраструктуры появится возможность управлять транспортным средством без непосредственного участия водителя-оператора.

**Возможности автоматизации задач оператора
транспортного средства за счет технологий Интернета вещей**

Задачи	Технологии Интернета вещей
Контроль состояния транспортного средства	Системы мониторинга транспортного средства
Управление транспортным средством	Технологии «умных» автомобилей-беспилотников
Взаимодействие транспортного средства с инфраструктурой	Технологии «умной» инфраструктуры

Возникновение автоматизированной коммуникации между транспортными средствами и объектами инфраструктуры должно стать третьим, завершающим этапом формирования «умной» транспортной среды. Автономная инфраструктура не может существовать без «умных» автомобилей, поскольку ее главная задача – обслуживать работу транспортных средств-беспилотников без участия людей-операторов.

Сегодня уже существуют объекты транспортной инфраструктуры, способные работать без участия человека. В качестве примера можно привести автоматическую безоператорную АЗС, разработанную компанией ООО «ИНИТ». Однако важно понимать, что она сейчас она не является звеном V2I-коммуникации, поскольку заправку автомобиля производит его водитель. Таким образом, взаимодействие объекта инфраструктуры с транспортным средством опосредовано человеком.

3.4.2.1. «Инновационные дороги» в России

Сегодня в России реализуется пилотный федеральный проект под названием «Инновационные дороги»⁹⁴. Проект реализуется Федеральным дорожным агентством, Министерством экономического развития, Роснано и правительствами Москвы, Рязанской области и Татарстана. Планируется, что затраты на первый этап проекта составят 100 млрд рублей, а первые результаты будут достигнуты уже в 2015 году.

Инновационные трассы будут существенно отличаться от обыкновенных российских дорог. На этапе прогнозирования можно сказать, что они позволят снизить аварийность и смертность, уменьшат затраты на свое обслуживание и будут служить гораздо дольше.

Первые изменения коснутся государственных стандартов, на основании которых укладывается дорожное покрытие. Большинство стандартов устарело и не готово к тому, что по дорогам будут двигаться современные 40-тонные грузовые транспортные средства. Для строительства дорог будут использоваться современные пластичные и прочные материалы: фибробетон, базальтопластиковая арматура, покрытие против скольжения и т.п.

⁹⁴ В России построят самые умные в мире дороги // ZR.RU : За Рулем.пф. 2013. URL: http://www.zr.ru/content/news/509946-v_rossii_postrojat_samyje_umnyje_v_mire_dorogi/ (дата обращения 27.03.2014).

Инновационные дороги будут использовать и технологии, относящиеся к сфере Интернета вещей. Датчики и сенсоры помогут оптимизировать освещение трасс, а также помогут определиться с объемами выброса противогололедных реагентов. Помимо этого, при помощи сенсоров удастся внедрить адаптивный скоростной режим, который учитывает текущую загрузку трассы, а также интерактивную систему работы светофоров.

В перспективе проект инновационных дорог может быть скомбинирован с проектом ЭРА-ГЛОНАСС. На дороге будут установлены различные системы оповещения, информацию с которых потенциально может принять любой автомобиль, оснащенный необходимым бортовым оборудованием. Система будет предупреждать водителей о крутых поворотах, дорожно-транспортных происшествиях, внезапном ухудшении погоды и т.п.

Изменения коснутся и системы управления дорожным трафиком. Теоретически, система будет способна передавать на информационное табло водителей варианты оптимальных маршрутов, за счет чего удастся избежать возникновения пробок и снизить среднее время, проведенное в пути.

Интерактивные системы видеонаблюдения будут активно использоваться в работе правоохранительных органов. Их функционал позволит обнаруживать угнанные автомобили, а также фиксировать нарушение разметки или скоростного режима.

3.4.2.2. Зарубежный опыт развития транспортной инфраструктуры

Датчики парковки в Лондоне

В начале 2014 года в Вестминстере стали устанавливать «умные» датчики парковки⁹⁵. Водители, пользующиеся специальным приложением, смогут быстрее найти парковочное место за счет установки подобных датчиков. Статистика утверждает, что сегодня в столице Великобритании водители тратят порядка 15 минут на поиски парковочного места. Внедрение «умных» датчиков парковки обещает исправить эту статистику в лучшую сторону.

В случае успешного опыта аналогичная система будет развернута по всему Лондону. В полевых испытаниях еще до тестирования в Вестминстере использовалось 189 датчиков, которые в целом были признаны эффективными.

Управление транспортом в Токио

Токио традиционно считался городом с сильными транспортными заторами. Порядка 20–25 лет назад средняя скорость транспорта в час

⁹⁵ «Умные» датчики помогут водителям Лондона быстро находить свободное место для парковки // PULSE-UK.ORG.UK : Еженедельная русская газета в Лондоне. 2014. URL: <http://pulse-uk.org.uk/novosti/umnyie-datchiki-pomogut-voditelyam-londona-byistro-nahodit-svobodnoe-mesto-dlya-parkovki/> (дата обращения 27.03.2014).

пик падала до очень низкого уровня. Но в 1995 году в Токио открылся Центр управления транспортом, главная задача которого – оптимизация движения колесного наземного транспорта⁹⁶.

Центр управления транспортом собирает данные с различных датчиков. На токийских дорогах находится множество ультразвуковых датчиков, которые определяют плотность транспортного потока и передают данные в Центр. Не менее важным источником информации являются камеры видеонаблюдения, установленные на скоростных автомагистралях. Кроме того, дорожная полиция также оперативно информирует центр о ситуации на дорогах.



Рис. 73. Центр управления транспортом в Токио

В городе установлено около 17 тыс. инфракрасных детекторов, сигналы с которых поступают на проезжающие мимо автомобили. За счет этих сигналов водители могут выбрать оптимальный маршрут движения, огибающий большинство пробок. Помимо контроля над прокладкой оптимальных маршрутов, Центр управления может дистанционно регулировать интервалы работы всех 15 тыс. светофоров, расположенных в Токио.

Во многом именно за счет работы Центра управления транспортом Токио удалось добиться достаточно хороших показателей скорости на дорогах. Так, на скоростной трассе считается затором движение со скоростью менее 60 км/ч, а на обычной дороге – менее 40 км/ч.

3.4.3. Системы экстренного реагирования

В настоящее время многими странами реализуются системы оперативного реагирования на дорожно-транспортные происшествия. В России статус такой системы имеет проект ЭРА-ГЛОНАСС. Проект предполагает оснащение колесных транспортных средств навигационно-

⁹⁶ Выбить пробки. Как японцы приручили большой город // RG.RU : Российская газета. 2012. URL: <http://www.rg.ru/2012/07/05/japan-poln.html> (дата обращения 27.03.2014).

коммуникационными устройствами для определения его географического положения. М2М-модули системы способны определить факт попадания транспортного средства в дорожно-транспортное происшествие и передать информацию в экстренные службы по беспроводным каналам связи. Планируется, что время прибытия скорой помощи сократится на 30%⁹⁷.

Система задумывалась и реализовывалась как совместная с европейским проектом eCall. Тем не менее между проектами существует серьезная разница. ЭРА-ГЛОНАСС предполагает подключение всех колесных транспортных средств, тогда как eCall рассчитана на легковые автомобили и грузовики массой до 3,5 тонн. Кроме того, отечественный проект работает на протоколах ГЛОНАСС, а eCall использует протоколы GPS.

Похожая система существует в Бразилии и называется SIMRAW. Ее функционал аналогичен ЭРА-ГЛОНАСС и eCall, но изначально она создавалась для предотвращения угонов автомобилей. Потребность вызвана тем, что в Бразилии ежегодно угоняют 400 тыс. легковых автомобилей общей стоимостью 4 млрд долларов, еще на 1 млрд долларов угоняют грузовой и спецтранспорт.

В США функционирует проект OnStar, который успешно работает более 15 лет. За прошедшее время система отреагировала на 170 тыс. дорожно-транспортных происшествий. На конец 2011 года система насчитывала более 6 млн абонентов в США, Канаде, Мексике, Китае и Латинской Америке. Функционал системы аналогичен проекту ЭРА-ГЛОНАСС. Кроме того, есть GPS-навигация, возможность удаленно заглушить двигатель, помощь в дороге, прогноз погоды и т.п.

3.4.4. Электронный мониторинг пассажирского транспорта

Один из пилотных проектов в сфере электронного мониторинга на общественном транспорте был представлен компанией Cisco на ежегодной конференции в 2013 году. Так, на Cisco Live-2013 к сети были подключены 34 автобуса, которые перевозили по улицам города 20 тыс. участников конференции. Использовалась технология Cisco Connected Fleet Management для управления подключенным транспортом.

В конгресс-центре была интерактивная карта, на которой можно было увидеть расположение автобуса. Туда выводилась информация о скорости движения, давлении в шинах, температуре двигателя и эффективности использования топлива. Все данные поступали в реальном времени с бортовых систем. Территории возле школ были помечены как зоны особого внимания. Бортовая система посылая водителю особый сигнал при их пересечении. Система мгновенно передавала информацию о ДТП и нарушении скоростного режима.

⁹⁷ Мальцев С. Международные аспекты развития проекта «ЭРА-ГЛОНАСС» // VESTNIK-GLONASS.RU : Межотраслевой журнал навигационных технологий. 2013. URL: http://vestnik-glonass.ru/stati/mezhdunarodnye_aspekty_razvitiya_proekta_era_glonass/ (дата обращения 27.03.2014).

Кроме того, автобусы имели беспроводную связь, причем доступ к ней у пассажиров был по тем же паролям и идентификаторам Cisco Live SSID. В салонах находились цифровые рекламно-информационные панели, информация на которых менялась в зависимости от положения автобуса⁹⁸.

3.4.5. «Умные» автомобили

Создание беспилотных автомобилей обещает стать вторым этапом формирования «умной» транспортной среды. Для того чтобы транспортное средство могло перемещаться без прямого контроля оператора, необходимо использование программно-аппаратного комплекса, включающего в себя множество сенсоров и датчиков.

Совокупность подключенных устройств должна предоставлять системе следующую информацию:

- положение транспортного средства в каждый момент времени;
- скорость и направление движения транспортного средства;
- расстояние до неподвижных объектов (инфраструктура, различные препятствия, остановившиеся транспортные средства);
- расстояние до подвижных объектов (транспортные средства, пешеходы, различные подвижные препятствия);
- траектория движения подвижных объектов.

Помимо сенсоров и датчиков, необходимых для получения перечисленной информации, «умный» автомобиль должен обладать средствами удаленного контроля двигателя, зажигания и управления, а также средствами двусторонней беспроводной передачи данных. Последний пункт имеет принципиальное значение, поскольку способствует обеспечению безопасности за счет возможности удаленного «выключения» автомобиля в случае подозрения на неисправность. Программная часть данного комплекса должна обеспечивать автономное движение «умного» автомобиля на основании получаемых данных.

Существующие сегодня пилотные проекты «умных» автомобилей используют следующую совокупность подключенных устройств для обеспечения автономного движения:

- бортовые видеокамеры;
- лазерный датчик LIDAR;
- датчики позиционирования;
- датчики контроля скорости;
- радары для определения дистанции;
- коммуникационная антенна;
- GPS-приемник;
- контроллер трансмиссии;
- контроллер двигателя;
- акселерометр;
- датчики положения руля.

⁹⁸ Интернет вещей в действии был продемонстрирован участниками конференции Cisco Live // CISCO.COM : Новости. 2013. URL: <http://www.cisco.com/web/RU/news/releases/txt/2013/07/070813f.html> (дата обращения 25.02.2014).

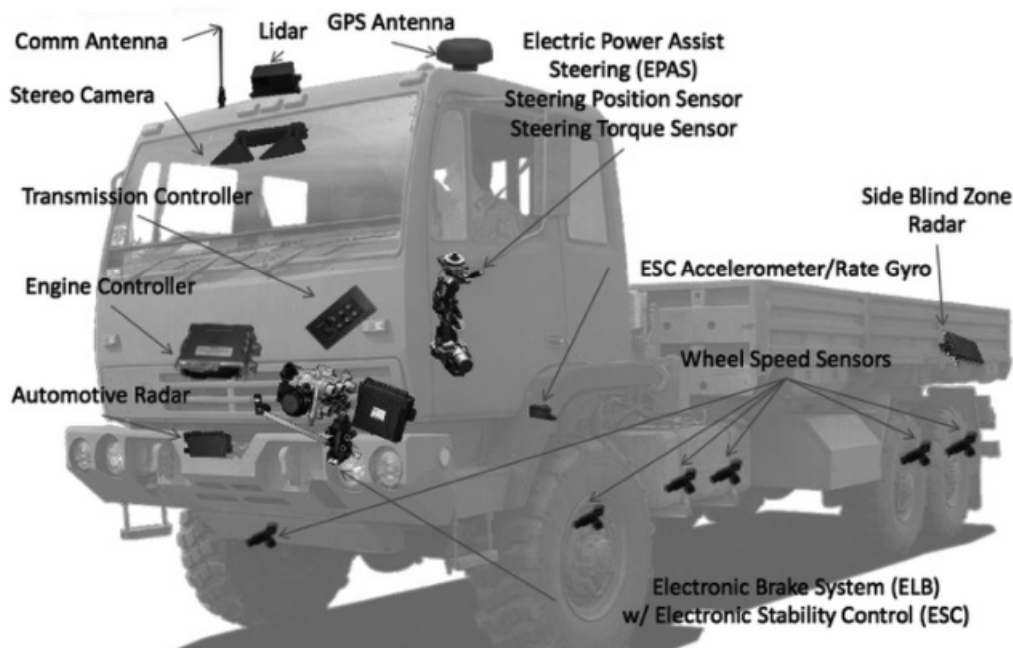


Рис. 74. Составные элементы системы AMAS, использующейся для превращения автомобиля в беспилотник

3.4.5.1. Зарубежный опыт создания беспилотных автомобилей

Сегодня пристальное внимание уделяется беспилотным наземным транспортным средствам, которые в дальнейшем могут стать компонентами автоматизированной транспортной сети. Правовая база для использования таких автомобилей уже начинает формироваться в некоторых странах. Так, в 2012 году Невада и Калифорния выдали разрешение на использование беспилотников на своих улицах.

Одним из лидеров в разработке беспилотных автомобилей является лаборатория Google X. Для превращения автомобиля в беспилотник используются информация сервиса Google Street View, видеокамеры, лазерный датчик LIDAR на крыше, радары в передней части автомобиля и датчик на заднем колесе для более точного позиционирования. Суммарная стоимость оборудования составляет \$150 тыс., причем \$70 тыс. приходится на LIDAR⁹⁹.

При помощи установленного оборудования система строит в реальном времени 3D-карту окружающей местности, которая в дальнейшем сравнивается с информацией из Google Street View. По состоянию на март 2013 года такие автомобили не могли передвигаться при плохой погоде, поскольку сопоставить карту с данными сервиса не представлялось возможным. Однако за время проведения испытаний автомобиль попал в аварию всего один раз, когда стоял на светофоре и в него случайно въехали¹⁰⁰.

⁹⁹ Priddle A, Woodyard C. Google discloses costs of its driverless car tests // USATODAY.COM : Информационный портал. 2012. URL: <http://content.usatoday.com/communities/driveon/post/2012/06/google-discloses-costs-of-its-driverless-car-tests/1#.UwyyyoWUMdX> (дата обращения 25.02.2014).

¹⁰⁰ Muller J. With Driverless Cars, Once Again It Is California Leading The Way // FORBES.COM : Information for the World's Business Leaders. 2012. URL: <http://www.forbes.com/sites/joannmuller/2012/09/26/with-driverless-cars-once-again-it-is-california-leading-the-way/> (дата обращения 25.02.2014).

Интерес Google к Интернету вещей не ограничивается беспилотными автомобилями. На Шоу потребителей электроники в Лас-Вегасе стало известно, что Google собирается купить портфель компании Nest, которая делает умные термостаты и детекторы дыма, за 3,2 млрд долларов. Можно предположить, что Google намерен развивать концепцию «умного дома»¹⁰¹.

В 2008 году прошла информация, что General Motors собираются начать собственное тестирование беспилотных автомобилей в 2015 году. Тем не менее подтверждения информации отсутствуют¹⁰².

Американские военные компании также разрабатывают технологии, при помощи которых можно автоматизировать передвижение наземного транспорта. В январе 2014 года компания Lockheed Martin провела испытания технологии Autonomous Mobility Applique System (AMAS), благодаря которой любой армейский грузовик может быть превращен в беспилотный автомобиль. После установки системы грузовик может автономно перемещаться по дорогам, объезжать препятствия, реагировать на появление пешеходов и других машин¹⁰³.

Сегодня в американской армии уже успешно работает Squad Mission Support System. Этот беспилотник предназначен для перевозки амуниции и боеприпасов. Доступно управление через спутник. Прошел полевые испытания в Афганистане¹⁰⁴. Существуют прогнозы, согласно которым к 2023 году в армии США на одного военнослужащего будет приходиться 10 роботов¹⁰⁵. Использование летающих дронов и так называемых «атакующих роев» считается одним из перспективных направлений Интернет вещей для армии и полиции.

3.4.5.2. Отечественные разработки «умных» автомобилей

ОАО «КАМАЗ» и Cognitive Technologies разрабатывают беспилотный автомобиль. Работающий образец транспортного средства планируется создать уже в июне этого года.

Ожидается, что беспилотный грузовик будет использовать информацию от видеокамер для анализа дорожной обстановки. Система сможет распознавать дорожные знаки, сигналы светофора, другие автомобили и пешеходов. Время реакции системы – не более 0,3 секунды.

¹⁰¹ Cohen S. Year of the Internet of Things // FORBES.COM : Information for the World's Business Leaders. 2014. URL: <http://www.forbes.com/sites/sarahcohen/2014/01/14/year-of-the-internet-of-things/> (дата обращения 25.02.2014).

¹⁰² Squatriglia C. Gm Says Driverless Cars Could Be on the Road by 2018 // WIRED.COM : Информационный портал. 2008. URL: <http://www.wired.com/autopia/2008/01/gm-says-driverl/> (дата обращения 25.02.2014).

¹⁰³ Autonomous Mobility Applique System (AMAS) // LOCKHEEDMARTIN.COM : Lockheed Martin. URL: <http://www.lockheedmartin.com/us/products/amas1.html> (дата обращения 25.02.2014).

¹⁰⁴ SMSS // LOCKHEEDMARTIN.COM : Lockheed Martin. URL: <http://www.lockheedmartin.com/us/products/smss.html> (дата обращения 25.02.2014).

¹⁰⁵ Gaudin S. U.S. Military may have 10 robots per soldier by 2023 // COMPUTER-WORLD.COM : IT news, features, blogs, tech review, career advice. 2013. URL: http://www.computerworld.com/s/article/9244060/U.S._military_may_have_10_robots_per_soldier_by_2023 (дата обращения 25.02.2014).

«Важной особенностью проекта является возможность реальной работы в российских условиях. В отличие от зарубежных разработчиков, больше ориентирующихся на идеальные условия дорожного движения: качественную разметку, благоприятные погодные условия и т.д., – наш подход к созданию системы машинного зрения позволяет распознавать дорожную сцену (в том числе границы дороги, ширину полос движения и т.д.) в отсутствие какой-либо разметки. Задача состоит в создании системы более совершенной, чем за границей», – пояснил руководитель проекта по созданию систем машинного зрения Олег Славин.

Cognitive Technologies занимается разработкой модуля, позволяющего обеспечить беспилотное управление транспортным средством, в том числе в сложных погодных условиях и при отсутствии надлежащей дорожной разметки.

«Сейчас подобные разработки ведут все ключевые мировые производители грузовых автомобилей, что говорит о том, что в будущем ожидается активное развитие данного сегмента рынка», – сказал Афанасьев. Для запуска «беспилотников» на базе КАМАЗа в промышленную эксплуатацию необходимо внесение изменений в законодательство, говорит Ускова. В 2017 году планируется запустить пилотный проект в Татарстане на дорогах общего пользования, а также начать процедуру внесения поправок в законы.

В 2012 году по заданию Минпромторга ФГУП «НАМИ» выполнил НИР по созданию интеллектуальных самоуправляемых «беспилотных» грузопассажирских АТС гражданского назначения. В рамках проекта разработан макетный образец «беспилотного» АТС на базе автомобиля «Лада-Калина», с новейшей 7 ступенчатой АКПП без гидротрансформатора российской компанией «КАТЕ», системы управления движением и технического зрения, приводы управления автомобиля.

На макетном образце автомобиля «Лада-Калина» обеспечена работоспособность приводов педали тормоза, дроссельной заслонки, рулевого управления и селектора переключения режимов работы АКПП, управляемых с помощью электронных пультов системы управления движением. «Создание интеллектуальных самоуправляемых «беспилотных» грузопассажирских АТС гражданского назначения» Основные элементы системы управления Рулевого управления Дроссельной заслонкой Тормозной системой Трансмиссией Зажиганием Светотехникой Основные алгоритмы управления движением в условиях моделирования организованной и неорганизованной дорожных сетей:

- включения и выключения двигателя;
- режимов прямолинейного движения автомобиля;
- режимов поворота автомобиля;
- распознавания препятствий;
- определения дорожных знаков;
- определения дорожной разметки;
- определения местоположения автомобиля;

- поддержания заданного расстояния за впереди идущим автомобилем;
- поддержания скорости движения;
- подачи сетевой сигнализации;
- подачи звуковой сигнализации.

В состав технического зрения входит набор видеокамер, радаров дальнего и ближнего действия, лазеры и GPS/ГЛОНАСС-приемники. С помощью системы технического зрения «беспилотный» автомобиль анализирует обстановку вокруг себя на расстоянии до 200 м, распознает дорожную разметку, дорожные знаки, светофоры и определяет движущиеся и не движущиеся объекты. С помощью системы GPS/ГЛОНАСС автомобиль может передвигаться из точки А в точку Б без участия водителя, прокладывая траекторию движения и анализируя дорожную ситуацию. Система технического зрения параллельно позволяет решать дополнительные важные задачи повышения безопасности транспортного средства. Например, разрабатываются системы обнаружения препятствий на дороге (машина, человек, животное и т.д.) и автоматической остановки автомобиля.

3.5. Интернет вещей в сфере грузоперевозок, логистики и торговли

3.5.1. Контроль грузов

В настоящее время все большее внимание уделяется обеспечению сохранности и безопасности грузов при их транспортировке и/или хранении. В мире разработано много эффективных устройств, каждое из которых может применяться в зависимости от требований конкретного случая. Это и запорно-пломбировочные устройства, и контрольные пломбы, и идентификационные наклейки, и индикаторы внешних воздействий (например: на удар, переверот, воздействие температуры, влажности), и другие устройства и изделия. Подавляющее большинство современных средств идентификации и контроля, поставляемых на рынок основными мировыми производителями таких товаров, достаточно надежны. Их соответствие подтверждено ведущими сертификационными и контрольными органами всего мира. Однако если нет тотального контроля целостности пломбы или иного контрольного устройства со стороны представителей отправителя или получателя, то значимость пломбирующих устройств заметно снижается. На эффективность защиты влияет общеизвестный «человеческий фактор». В большинстве случаев контрольные изделия (пломбы) проверяются вручную.

Сегодняшние стандарты для контейнерных перевозок и трейлеров предлагают ограниченную защиту от неавторизованного доступа и еще более ограниченную доступность информации о том, кто, когда и зачем имел контакты с вашим грузом или контейнером.

Транспортные компании подвергаются дополнительным рискам неизвестности – риску воровства, подделки, загрязнения, угрозам терроризма, контрабанды и наркотрафика.

Примером современного решения в области контроля грузоперевозок может служить представленное европейской компанией EcoTelematics Group в 2014 году новое решение NaviFleet для контроля сохранности грузов при перевозке в трейлерах.

Новая система позволяет осуществлять контроль за грузами, используя комбинацию радиочастотной идентификации (RFID) и GPRS-коммуникации. Система автоматически определяет местоположение трейлера и контейнера, оптимизирует использование транспорта.

Каждое устройство Secureseal, используя GSM/GPRS/GPS устройства телематики NaviFleet, посылает на сервер системы исчерпывающую информацию о нахождении груза и сохранности пломбы. Все действия с грузом и электронными пломбами фиксируются в системе с точной позицией произошедшего события и временем.

Приложения NaviFleet предоставляют пользователям различные варианты доступа к данным системы мониторинга, в том числе с использованием web-интерфейсов и мобильных устройств.

3.5.2. Мониторинг почтовых отправлений

В последнее время активно ведутся работы по внедрению RFID-технологий в производственные процессы почтовых и курьерских служб в Северной Америке, Европе, на Ближнем Востоке и в Восточной Азии.

В прошлом году почтовая RFID-система успешно прошла испытания в Корее. Система полностью автоматизирует весь процесс доставки почты от принятия конверта до классификации и диспетчеризации его.

Активно ведет работы в этом направлении шведская почта. Используемые здесь системы включают различные инновации, в том числе и RFID-системы для контроля доступа почтовых транспортных средств, и RFID-системы для оборудования сортировки писем.

Почта Катара внедрила технологию RFID от Motorola. Корпорация Qatar Post объявила о внедрении технологии RFID компании Motorola как составной части инициативы по определению качества работы почтовых служб на Ближнем Востоке. Почтовая служба Qatar Post, входящая в руководящий комитет проектной группы по качеству услуг Всемирного почтового союза (UPU), недавно завершила испытания в арабском регионе, в ходе которых тестировались пассивные и полупассивные системы RFID.

После завершения проекта результаты будут представлены для всех 22 стран арабского региона, что произведет революцию в сфере почтовых услуг. В доказательство эффективности системы Всемирный почтовый союз рекомендует определить штрафы для почтовых служб за перебои в доставке почты.

Австралийская почта использует RFID. Более чем 12 000 RFID-меток каждый месяц используется австралийской почтовой службой для отслеживания перемещения почтовых сообщений. Ручная сортировка писем полностью заменена использованием технологии RFID. Это поз-

воляет более эффективно контролировать перемещение почтовых отправлений и анализировать проблемы, связанные с пересылкой писем.

Почта Таиланда взяла на вооружение почтовые метки DogBone производства UPM Raflatac. В сочетании с RFID-считывателями, закрепленными на дверях промежуточных почтовых пунктов, метки позволили значительно ускорить процесс обработки почты.

Технологию радиочастотной маркировки и идентификации используют также Saudi Post, Deutsche Post/DHL Europe, курьерская служба UPS. Всемирный почтовый союз пользуется инновационной технологией радиочастотной идентификации RFID для оценки скорости передачи почтовых сообщений между странами.

В тестирование системы, в основе которой лежат разработки компании Reva Systems, принимают участие два десятка стран, включая Индию, Южную Корею, Швейцарию и Того. В список испытателей также попали несколько государств, уже использующих альтернативные RFID-решения (Мексика, Норвегия и Саудовская Аравия). Руководство Всемирного почтового союза полагает, что к 2012 году система будет развернута в 100 странах. А в обозримом будущем предлагаемым решением сможет воспользоваться каждая из 191 стран, входящих в состав союза.

Компания Savi Technology (Lockheed Martin), поставщик технологий для логистических компаний, получила одобрение от Радиокomiteeта Китая на тестирование прибора радиоиdентификатора технологии Radio Frequency Identification (RFID) на территории страны. Идентификатор получил все необходимые сертификаты, его установка на контейнеры позволит отслеживать их в режиме реального времени на всем пути следования, от места загрузки в Китае до конечного места назначения.

Всего же в мире ежегодно отправляется и принимается около 650 млрд почтовых отправлений, большая часть из которых в будущем будет промаркирована радиочастотными метками.

Самым большим на сегодня почтовым RFID-проектом считается испанский почтовый проект Correos.

3.5.2.1. Мониторинг почтовых отправлений в России

На сегодняшний день в Российской Федерации существует множество компаний, которые осуществляют доставку корреспонденции и грузов для юридических и частных лиц, как по территории России, так и за ее пределами. Часть компаний, такие как ФГУП «Почта России», ООО «СПСР-Экспресс», ООО «ЕМС Гарантпост», ООО «Экспресс Точка Ру» и др., для этих целей активно используют возможности мониторинга для предоставления клиентам информации о состоянии выполнения доставки их отправлений.

Одним из самых крупных отечественных перевозчиков отправлений является ФГУП «Почта России», которое активно использует современные технологии мониторинга.

Данная технология подразумевает присвоение регистрируемым почтовым отправлениям (заказным или с объявленной ценностью) уникального почтового идентификатора. На каждом этапе пересылки информация почтового идентификатора заносится в единую систему учета и контроля, благодаря чему возможно отследить прохождение почтового отправления через web-витрину на сайте компании.

В нашей стране направление радиочастного мониторинга только начинает свое развитие. По имеющейся информации, ФГУП «Почта России» имеет планы по внедрению технологии RFID. В реализации проекта будет задействована Госкорпорация РОСНАНОТЕХ. По сведениям из прессы, в рамках пилотного проекта RFID-метки начнут наносить на все отправления экспресс-подразделения – «Почта России» EMS.

В ближайшее время RFID-метки появятся на всех почтовых емкостях – от коробок и мешков до контейнеров, а также на регистрируемых письмах и бандеролях. Уже с 2014 года RFID-метками планируется маркировать все почтовые отправления EMS.

3.5.2.2. Система учета почтовых отправлений в Испании

Sociedad Estatal Correos y Telégrafos, S.A., обычно называемая просто Correos (в переводе Почта), является государственным почтовым оператором Испании. Компания входит в группу Correos, единственным владельцем которой является правительство Испании. Компания занимается доставкой отправлений уже более 300 лет. Сегодня компания имеет более 10 000 офисов и представительств, в которых работают около 62 000 сотрудников, и осуществляет доставку примерно 4,4 млн отправлений в год.

В 2004 году Correos начала проект по внедрению RFID-меток. Для проекта была выбрана система пассивных меток и закуплено оборудование в количестве:

- метки – 50 000;
- ридеры – 609;
- антенны – 3580;
- серверы – 371.

Были выбраны UHF-метки со следующими характеристиками:

- рабочая частота: UHF-860 до 960 Mzh (ультравысокая частота);
- протокол: EPC GEN-2, Class 1 / ISO 18000;
- выполняемые функции: считывание/запись;
- память: только идентификатор (96 бит);
- расстояние для считывания: 5 м;
- расстояние для записи: 2 м;
- температура: от –25 до +50 °С.

На данный момент служба имеет:

- 45 000 передвижных контейнеров, снабженных высокочастотными RFID-метками;
- 20 000 стандартных контейнеров, снабженных системой RFID.



Рис. 75. Передвижные контейнеры с RFID-метками



Рис. 76. Стандартные контейнеры с RFID-метками

Благодаря проекту внедрения RFID-меток почтовая служба Correos смогла добиться:

- повышения эффективности работы в целом (на 22%);
- повышения эффективности считывания данных об отправлениях (на 12%);
- сокращения отклонений в норме затрат;
- повышения конкурентоспособности компании.

3.5.3. Логистика и розничная торговля

3.5.3.1. Применение штрих-кодирования

Сегодня применение штрих-кодов в сфере логистики и торговли стало фактически повсеместным.

В качестве примера применения штрих-кодирования можно привести систему управления запасами (WMS) «БУХта: Складской комплекс».

WMS «БУХта: Складской комплекс» – это технология управления складом в режиме реального времени.

Система используется такими компаниями, как: Логистический оператор «Ниеншанц Логистик» (Холдинг Адамант); Сеть гипермаркетов бытовой электроники «Техношок»; Розничная аптечная сеть «Фармакор»; Дистрибьюторская компания «Инструмент-Гарант»; Торговая компания «РБД»; Логистический оператор «ОКСЭТ» (складской комплекс Невский); Производственная компания «ЕвроСтройСтандарт» (холдинг Адамант); Производственная компания «Птицефабрика РОС-КАР».

Компания БУХта предлагает своим заказчикам целый комплекс услуг, необходимых для того, чтобы успешно внедрить и использовать современные информационные технологии для управления. Вся техника, которая участвует в системе управления БУХта, может тестироваться и настраиваться как сотрудниками компании БУХта, так и самостоятельно заказчиком.

Решение WMS «БУХта: Складской комплекс» может быть применено в различных отраслях, в частности:

- ЗРІ-операторами;
- дистрибьюторскими и торговыми компаниями;
- производственными организациями;
- фармацевтическими компаниями.

Одной из особенностей решения является возможность работы с любыми типами паллет и грузов¹⁰⁶.

3.5.3.2. Применение RFID-меток

Новым перспективным направлением развития средств автоматизации в логистике и розничной торговле становится активное использование RFID-меток

Компании X5 Retail Group, Sitronics и Роснано работают над внедрением технологии RFID в сфере розничной торговли и сопутствующих логистических операциях. Предполагается, что производитель будет маркировать каждую единицу своей продукции RFID-метками. Это позволит автоматически идентифицировать продукцию на всех этапах комплектования и доставки. Сама метка будет содержать в себе различную информацию, включая срок годности, режимы хранения и перевозки.

Непосредственно в магазинах потребителям не придется стоять в кассовых очередях. Для оплаты покупок достаточно будет пройти через специальную рамку, которая автоматически идентифицирует товары из тележки и сформирует чек. Ожидается, что снижение издержек всего цикла производства и дистрибуции составит до 20%. А к косвенным эффектам от внедрения новой технологии относится контроль за произ-

¹⁰⁶ URL: <http://www.autoid-rrc.ru/katalog-reshenijj-sklad/wms-bukhta-skladskojj-kompleks> (дата обращения 27.03.2014).

водством, контроль за торговлей алкоголем и табаком, борьба с фальсификацией и контрафактом.

Таким образом, автоматический учет и контроль распространялся бы на весь жизненный цикл товара, начиная с момента его производства и заканчивая продажей потребителю. Стоит отметить, что в розничную сеть X5 Retail Group входит более 4000 магазинов, что позволит снизить стоимость одной RFID-метки в случае массового внедрения данной технологии.

Сегодня технология находится на стадии практического тестирования компанией «Магазин будущего», являющейся совместным предприятием X5 Retail Group, Роснано и компании АТИ. Пропускная способность касс тестового магазина увеличилась более чем в три раза. Стоимость метки составляет 4 рубля, однако массовое внедрение существенно снизило бы ее стоимость.

Помимо идентификации каждого продукта, в «умном» магазине используются специальные тележки со средствами навигации. Тележка выводит на экран свое местоположение и позволяет работать с каталогом всех товаров, находящихся в магазине. После того как нужный товар найден по названию, можно посмотреть его местоположение на карте.

3.5.3.3. Использование мобильных средств ввода данных

Развитие технологий в области создания мобильных средств ввода и передачи данных позволяет широко применять подобные устройства в сфере контроля большого количества объектов учета, таких как товары на складах и полках магазинов, грузы на терминалах и в транспортных средствах, почтовые отправления и др.

Терминалы сбора данных благодаря большому выбору и возможности их оперативной инсталляции гармонично вписываются в любую систему, где нужно проводить быстрый, точный и надежный учет, максимально устраняя человеческий фактор.

Наибольшее распространение ТСД получили при работе на различного рода складах, от логистических до почтовых и пищевых, – при постоянно увеличивающихся номенклатуре и количестве единиц хранения становится очень сложно вручную управлять товародвижением, даже при наличии механизированных погрузчиков и квалифицированного рабочего персонала.

В данном случае ТСД могут применяться в двух направлениях. Во-первых, как устройства, которые автоматически фиксируют происходящие на складе события (приемка товара, перемещение, подбор заказа, отгрузка определенных партий и т.д.). В таком случае они играют роль считывателей и обработчиков информации о промаркированном штрих-кодом или RFID-меткой товаре. При этом беспроводные терминалы передают информацию о происходящих бизнес-процессах в учетную систему склада в режиме реального времени, что позволяет встраивать такие решения в различные циклы непрерывного производства или доставки товаров в режиме реального времени.

Во-вторых, как исполнительные устройства программного обеспечения (WMS), управляющего товародвижением на складе. Указания о необходимости выполнять те или иные действия с товарами кладовщики и грузчики в данном случае получают непосредственно с экрана терминалов. Кроме того, посредством сканирования маркированного товара и точек его размещения кладовщики подтверждают все свои действия, что позволяет избавиться от ошибок в работе, – с помощью графической схемы склада всегда можно точно сказать, где находится та или иная группа товаров, в каком количестве, какие условия хранения для нее определены.

Чуть менее распространенный вариант – ТСД в торговле. В данном случае ТСД применяются для приемки и возврата товара и проведения инвентаризации, а в сочетании с мобильным носимым принтером – для переоценки товаров прямо в торговом зале. Определенная экономия средств при этом складывается благодаря отсутствию необходимости монтажа дорогостоящей кабельной инфраструктуры, быстрой и простой установке беспроводного сетевого оборудования, мгновенному подключению новых сотрудников (в том числе оперативному расширению мобильных рабочих мест для временного персонала), использованию беспроводных устройств не только для передачи данных, но и для оперативной голосовой связи по IP-сети (VoIP), а также мониторингу и печати полочных ценников непосредственно в торговом зале.

За последнее время были автоматизированы склады таких компаний, как Yamaha Motor (склад площадью 1200 м²: пять стационарных и три ТСД), «Еврокнига» (1200 м²: три стационарных и два ТСД), Synergenta (7000 м²: шесть стационарных и пятнадцать ТСД), «Гема» (15 000 м²: восемь стационарных и шестнадцать ТСД) и многие другие.

Чуть менее распространенный вариант – ТСД в торговле. Здесь можно отметить проекты торговых сетей Metro Cash & Carry, Real, Spar, «Седьмой Континент», «Азбука Вкуса», «Патэрсон», «Перекресток», «Рамстор», «Эльдорадо», «Утконос». В магазинах «Ашан» помимо обычных ТСД с целью уменьшения очередей внедряются специальные мобильные точки, где консультанты подсчитывают стоимость товаров, находящихся в корзине пользователя, и упаковывают их в герметичные пакеты. В кассе достаточно только оплатить общий счет без повторного сканирования всех покупок.

3.6. Контроль вооружения и военной техники

RFID-маркировка наиболее эффективна для проведения быстрой инвентаризации оружия, боеприпасов и имущества на больших складах, так как позволяет быстро обнаруживать факты неучтенной выдачи или хищения таковых. Кроме того, RFID-метки могут использоваться для учета транспортных средств и личного состава.



Рис. 77. RFID-метка на БТР

RFID-считыватель



RFID-жетоны



Рис. 78. RFID-жетон

Внедрение технологии RFID позволяет:

- мгновенно идентифицировать оружие (боеприпасы) с его местом хранения или с определенным солдатом;
- быстро и эффективно проводить инвентаризацию в оружейных комнатах и на складах боеприпасов;
- ускорить и автоматизировать существующую медленную и неэффективную систему распределения, исключить неучтенные выдачи;
- исключить доступ неавторизованных лиц к оружию и боеприпасам и тем самым снизить риск хищения.

3.6.1. Системы мониторинга огнестрельного оружия и снаряжения

Системы мониторинга огнестрельного оружия (компания 3Arc) позволяют осуществлять автоматический контроль (положение по GPS и случаи стрельбы) с помощью устройства, которое крепится непосредственно к оружию. Такие устройства прочны, водонепроницаемы, имеют встроенные антенны и батареи.



Рис. 79. Датчик контроля оружия (3Arc)

Система позволяет отслеживать в режиме реального времени, когда оружие было впервые использовано, сколько выстрелов сделано, близость противника, траекторию движения входящих и исходящих пуль и т.д.

Такая информация позволяет в реальном времени мгновенно получать сведения о происходящей ситуации и впоследствии строить более точную картину произошедшего.

Используя энергосберегающий датчик движения и GPS, система мониторинга огнестрельного оружия поможет найти пропавшее оружие и немедленно просигнализирует в случае отдаления оружия от бронежилета (3Arc BulletVest), с которым оно синхронизировано, далее, чем на установленное расстояние. Настройки системы могут быть изменены через компьютер или «по воздуху».

Характеристики:

- чувствительный датчик Sirf III GPS с встроенными часами;
- поддержка мировых стандартов GSM: 850/900/1800/1900 МГц;
- возможность хранения до 6000 отчетов о событиях в случае отсутствия соединения с сервером;
- зашифрованные отчеты для обеспечения максимальной безопасности:
 - общие отчеты об оружии;
 - отчеты о предупредительных выстрелах;
 - отчеты о выстрелах;
 - отчеты о попытках вскрытия датчика;
 - отчеты о пересечении «зон безопасности» (до 5 зон);
 - отчеты о низком заряде батареи;
- встроенная 3,6 В 1600 мАч литиевая батарея обеспечивает до 12 ч работы;
- низкое энергопотребление и использование 3D-датчика положения (с настраиваемой чувствительностью) для переключения устройства между режимами: «спящий», «энергосберегающий» и «обычный».

3.6.1.1. Автоматизация учета оружия в Бюро дипломатической безопасности при Госдепартаменте США

Одним из самых крупных проектов по контролю движения оружия внутри склада является проект бюро дипломатической безопасности при Госдепартаменте США. В Соединенных Штатах агенты этого бюро осуществляют охрану Госсекретаря США и Посла США при ООН, а также высокопоставленных иностранных гостей ниже рангом, чем главы государств, во время их визитов в США.

На одном из оружейных складов Бюро в штате Вирджиния, где находятся сотни единиц огнестрельного оружия, оно маркируется видимыми или невидимыми метками RFID EPC для автоматического от-

слеживания их использования агентами. Это позволяет Департаменту вести электронный учет того, кто из сотрудников взял или вернул те или иные единицы оружия в автоматическом режиме. Система RFID также может подавать сигналы тревоги в случае несанкционированных действий. Эта система, известная под названием EasyArms, была установлена компанией ODIN, разрабатывающей решения в области RFID и специализирующейся на системной интеграции.



Рис. 80. Использование RFID-меток на оружейном складе

Новая система также включает пассивные RFID-метки EPC Gen 2, которыми оснащено оружие, получаемое агентами. На воротах на входе в хранилище установлены RFID-ридеры. Управление системой и обработка информации осуществляются с помощью программного обеспечения EasyEdge компании ODIN (на ридере) и программного обеспечения EasyArms (на сервере). Как только будет проверено, что система функционирует правильно и считывает 100% всех меток, Бюро планирует рассмотреть возможность установки этой системы на других оружейных складах.

Раньше операции по получению оружия проходили в ручном режиме. Каждый агент, используя идентификационную карту с высокочастотной бесконтактной меткой RFID, которую он носит на шнурке на шее, открывает единственную дверь хранилища. В этом помещении оружие хранится в запирающихся шкафах с кодовыми замками. При регистрации вручную агент выбирает необходимое оружие и заполняет бланк, указывая имя и идентификационный номер, а также серийный номер пистолета, его марку и модель.

По мнению специалистов компании ODIN, проблема с операциями в ручном режиме состоит в том, что они могут занимать слишком много времени и не отличаются точностью. Агент должен внести всю необходимую информацию в то время, как другие ждут своей очереди на эту процедуру. Более того, существует опасность, что агент может не внести необходимую информацию при регистрации оружия. В ODIN утверждают, что на полицейских оружейных складах точность отслеживания оружия составляет не более 50 %.

С помощью RFID Департамент надеется повысить точность отслеживания и тем самым добиться того, чтобы оружие хранилось в положенном месте, а процедура его получения или сдачи стала более эффективной.

По прибытии на склад агент должен предъявить свое удостоверение с бесконтактной высокочастотной меткой для того, чтобы открыть дверь хранилища. Когда он входит в помещение, ридер Sirit считывает уникальный идентификационный номер, закодированный на RFID-метке EPC Gen 2, прикрепленной к шнуру. Программное обеспечение EasyEdge, установленное на ридере, контролирует его, фильтруя считанную с меток информацию и посылая полученные данные на компьютер, где по идентификационному номеру устанавливается имя агента и прочая информация. Затем эта информация передается в систему, отвечающую за управление активами Бюро. На видеомониторе агент видит свое имя и перечень маркированного метками оружия, которое он носит в данный момент, а также оружия, которое он взял во время своего предыдущего посещения склада. Таким образом, сразу же можно выявить несоответствие.

Затем агент возвращает взятое прежде оружие в соответствующий шкаф или же берет оружие, которое он планирует использовать в этот день. Выходя со склада, агент видит другой монитор, на котором указывается его имя, а также обозначение каждого маркированного метками оружия, считанное ридером. Если он обнаруживает, что метку не удалось считать, он может оповестить об этом руководство.

Для того чтобы система RFID считывала метки всех единиц оружия, которые носит агент, и при этом не считывала метки на оружии других сотрудников, находящихся поблизости, все сотрудники должны входить в дверь по одному. Если несколько агентов попытаются войти в помещение или выйти из него одновременно, программное обеспечение EasyEdge обнаружит несколько личных RFID-меток, просигнализирует об этом, включая уведомление на мониторе, и проинструктирует сотрудников вернуться и пройти портал снова по одному.

Если агент попытается покинуть оружейный склад с оружием, на ношение которого он не имеет права, или же кто-либо попытается унести оружие, и система не обнаружит у него RFID-метки Gen 2, подтверждающей, что он является сотрудником Бюро, EasyEdge передаст эту информацию в систему Maximo, которая направит руководству соответствующее электронное сообщение. На экране, установленном на выходе из оружейного склада, появится предупреждение с указанием имени

данного лица, а также информации о том, какое оружие было вынесено или возвращено с нарушением установленных правил.

Самая сложная задача в этом проекте заключалась в обеспечении того, чтобы RFID-метки были прикреплены к различным видам огнестрельного оружия без опасности его повреждения или смещения деталей и без ущерба для его функционирования. Пистолеты и другое ручное огнестрельное оружие маркируются меткой Confidex размерами $1 \times 0,5 \times 0,0625$ дюйма, которая прикрепляется внутри оружия таким образом, чтобы ее не было заметно и было невозможно удалить.



Рис. 81. Пример RFID-метки для оружия

Что касается автоматических винтовок, определенные проблемы представляет тепло, выделяемое при их использовании, поэтому для них были выбраны метки Titan, которые могут выдерживать высокие температуры. Для оружия из углеродных материалов специалисты ODIN выбрали метку, разработанную Omni-ID для маркировки неметаллических и металлических поверхностей.

Несмотря на то, что система была установлена недавно, в ODIN уверены, что она будет функционировать с почти 100-процентной точностью. Дополнительным преимуществом внедрения системы будет сокращение времени, необходимого для того, чтобы взять и сдать оружие, особенно когда одновременно регистрируются четыре или более единиц.

3.6.1.2. Использование RFID-меток для учета оружия и бронежилетов в Департаменте полиции города Гамбурга

Аналогичный проект был предпринят в Департаменте полиции города Гамбурга. Они используют RFID-технологии для быстрой идентификации огнестрельного оружия и бронежилетов, используемых офицерами, во время проверок и во время несения дежурства. В режиме реального времени можно получать информацию о том, имеет ли сотрудник право на ношение конкретного оружия и возвратил ли он его на склад во время ухода со службы. Кроме того, отделения полиции имеют бронежилеты, оборудованные таким же образом, позволяющим быстро определять принадлежность каждого жилета к определенному офицеру, а также надежно идентифицировать должностное лицо в случае трагедии.

Интегрированные в рукоятку пистолета, эти надежные RFID-метки обеспечивают точность работы, даже в окружении металла, и выдерживают воздействие нагрузок, в том числе во время стрельбы. А также позволяют избежать ошибок, которые могут произойти, если серийные номера вводятся в систему вручную. Это делает управление выдачи и контроля оружия и жилетов более эффективным и экономит время.

3.6.1.3. Внедрение RFID-меток итальянскими производителями оружия

Другим примером использования RFID-меток для контроля и учета оружия является итальянский производитель пистолетов Chiappa Firearms. RFID-чип будет устанавливаться в рукоятку и будет иметь идентификационную информацию, такую как проверка сертификации, в соответствии с требованиями правительства Италии для всех видов огнестрельного оружия, сделанного в Италии. Чип будет также нести другую соответствующую информацию, включая имя производителя, серийный номер и ссылку в информационной базе данных. Считывание метки будет доступно на расстоянии не больше дюйма, поэтому RFID-метки будут использоваться только для учета оружия, но не для слежения за ним. До внедрения RFID итальянским инспекторам приходилось проверять каждый ящик с оружием вручную, путем открытия и визуального осмотра оружия. После завершения процедуры осмотра они должны были закрыть ящик и отштамповать его.

3.6.1.4. Использование RFID-меток для контроля оружия в России

По заказу Минобороны РФ в течение последних лет проводился ряд НИОКР по разработке средств радиочастотной идентификации вооружения и боеприпасов (UHF-считывателей).

3.6.2. Системы контроля баллистики в режиме реального времени

Система контроля баллистики в режиме реального времени (компания 3Arc) включает устройства, которые могут работать независимо или как единое целое для обеспечения уверенного контроля, для правоохранительных органов, военных и охранных организаций.

Преимущества системы включают:

- обнаружение случаев использования оружия или разряжения;
- построение отчетов о количестве выстрелов и траектории каждой пули;
- определение, являются ли выстрелы исходящими или входящими;
- определение, находится ли противник в непосредственной близости;
- определение воздействия травматических пуль на бронежилет офицера (при использовании 3Arc BulletVest).

Эта информация транслируется постоянно с помощью GPRS (в аварийном случае – через SMS) по каналам сотовой связи в систему слежения 3Ags в центре мониторинга для немедленного реагирования, отчета или анализа. Информация о местоположении устройств обновляется через установленные промежутки времени, что позволяет проводить трассировку маршрута движения на карте, и находится на web-сервере 3Ags. Индивидуальные значения длительности интервалов обновления, параметров отчетов и реагирования на экстренные случаи могут меняться через стандартный web-браузер.

3.7. Интернет вещей в обеспечении здоровья человека

Интернет вещей в сфере обеспечения здоровья человека оказывает все более заметное влияние на повседневную жизнь, открывая громадные преимущества во всем спектре предоставления услуг, от лечения в условиях стационара до медобслуживания и социального обслуживания на местах и ухода за собой.

Интернет вещей (IoT) станет значительной частью новой волны IT в здравоохранении, и технологии Третьей платформы – облако, Большие данные, мобильные решения и социальные сети – будут играть центральную роль в этой трансформации.

Интернет вещей является основополагающим для будущего развития здравоохранения. Сенсоры вкупе с аналитикой данных, облаком и мобильными устройствами и приложениями дают возможность радикально изменить наш подход к диагностике болезней, лечению и предупреждению заболеваний, делая реальностью профилактический подход, в центре которого стоит сам пациент.

Большое развитие получают технологии носимых устройств с использованием сенсоров, особенно в направлении профилактики заболеваний. Согласно опубликованному в 2014 году отчету исследовательской компании IDC Health Insights, персональные устройства, предназначенные для профилактики, будут одним из первых применений IoT в секторе здравоохранения в Центральной и Восточной Европе (CEE).

Ведущий аналитик исследования IDC Health Insights (CEMA) Нино Гигуашвили отмечает: «Находясь на скрещении охраны здоровья, фитнеса и моды, IoT персональной профилактики будет одним из самых быстро растущих рынков в здравоохранении в CEE. Растущая доступность продаваемых без рецепта недорогих носимых устройств поддержания здоровья и профилактики будет также расширять спектр сторон, участвующих в профилактическом обслуживании, предоставляя достаточно возможностей всем игрокам и расширяя саму экосистему».

Этот рынок откроет также большие возможности помимо самих носимых устройств, так как включает аналитику, облако и бесконечное разнообразие мобильных приложений медицинского назначения. IDC прогнозирует, что оборот рынка персональных устройств профилактики и поддержания здоровья более чем удвоится к концу 2018 года, демонстрируя среднегодовой темп роста (CAGR) 16,5%¹⁰⁷.

¹⁰⁷ URL: <http://d-russia.ru/idc-prognoziruuet-povyshenie-rol-i-interneta-veshhej-v-razviti-i-zdravooxraneniya.html> (дата обращения 27.03.2014).

Здравоохранение во всем мире постепенно подходит к тому этапу, за которым последует переход к ориентированной на пациента инструментальной модели здравоохранения. Такой переход уже понемногу осуществляется, в том числе и в нашей стране, и связано это с так называемым электронным здравоохранением (общепринятый термин – eHealth). Сюда относятся такие сервисы, как телемедицина, электронные медицинские карты, дистанционная запись к врачу и др. Но все это только малая часть того, что может быть использовано в здравоохранении.

Одно из относительно новых направлений электронного здравоохранения носит название «мобильное здравоохранение» (mHealth).

Мобильное здравоохранение – это термин, обозначающий использование мобильных устройств и беспроводных технологий в целях медицинской помощи, а также обеспечения здорового образа жизни человека. Наиболее известным примером технологий mHealth являются программы для мобильных телефонов и планшетов, связанные с контролем физического состояния (например, веса) или фитнесом. Когда же я размышляю о mHealth, я чаще всего все-таки думаю о ее функциональности с двух точек зрения: использование мобильных технологий медицинскими организациями для улучшения оказания медицинской помощи и использование этих технологий пациентами для контроля собственного здоровья.

Сегодня mHealth – это два крупных направления, которые развиваются параллельно, с разной скоростью, оказывая при этом взаимное влияние друг на друга. Первое – это технологии, устройства, приложения и услуги для лечения и ухода за пациентами, второе – это системы и устройства, предназначенные для контроля за соблюдением здорового образа жизни (wellness) и фитнеса (fitness). В настоящее время в mHealth постепенно идет сближение или, скорее, слияние этих направлений. Поэтому будет правильнее говорить не о здравоохранении или медицине, а об обеспечении здоровья человека во всех смыслах с использованием мобильных и не только технологий.

3.7.1. Мониторинг здоровья, диагностика и обеспечение ухода за пациентами

Этот сектор развивается не так бурно, как сектор систем для фитнеса. Но тем не менее рынок мобильного мониторинга и диагностики уже в 2012 году, согласно отчету исследовательской компании Transparency Market Research, равнялся 650 млн USD, будет расти со скоростью 43,3% в год до 2020 года и составит 8 млрд USD в 2019 году.

В эту категорию mHealth входят:

- системы мониторинга: работы сердца, давления, глюкозы, работы мозга, сна и т.п.;
- многопараметрические системы мониторинга;
- системы удаленного взаимодействия с врачом;
- носимые, имплантируемые и проглатываемые сенсоры различных жизненных показателей;

- диагностические системы и системы быстрого анализа (крови, слюны, мочи, дыхания и т.п.);
- системы для ухода за пожилыми людьми, хронически больными и детьми;
- приложения для контроля здоровья, контроля употребления лекарств, планирования лечения, обучающие системы и др.

Датчики носимой электроники могут существенно повысить качество лечения и жизни пациентов на этапе диагностики, лечения и реабилитации. На фоне постоянно возрастающих бюджетов системы здравоохранения использование датчиков носимой электроники может сэкономить немало денег, а значит, многие виды лечения могут стать доступнее.



Рис. 82. Система мониторинга работы сердечно-сосудистой системы

Именно в этом направлении заложен будущий успех mHealth, именно с ним аналитики связывают переформатирование отрасли медицины и здравоохранения, а также гигантский рост доходов участников рынка.

Вот только несколько конкретных примеров, которые уже реально работают.

- В Швеции успешно работает система, позволяющая дистанционно снимать показания стимуляторов сердца пациентов. Система Soarian Clinical позволяет издалека осуществлять мониторинг состояния как самого пациента, так и его кардиостимулятора, избавляя его (это, как правило, очень пожилые люди) от необходимости каждые полгода приезжать на прием для проверки состояния. Эта технология не только надежная, но и очень чувствительная – система мониторинга реагирует на такие изменения здоровья пациента или проблемы стимулятора, которые сам пациент часто просто не замечает или не обращает внимания.
- Система удаленной поддержки хронических заболеваний Care Innovations (совместный продукт Intel и GE), позволяющая людям, страдающим хроническими заболеваниями, получать медицинскую информацию о собственном здоровье и необходимую медицинскую поддержку в любом месте, где бы они ни находились.
- Visi Mobile – носимая на теле система из небольших датчиков, позволяющая вовремя фиксировать ухудшение здоровья владельца и

соединять его со своим врачом, вне зависимости от того, где пациент находится в данный момент.

- Существуют также решения, основанные на использовании специализированных миниатюрных систем, контролирующих отдельные показатели здоровья человека. Например, компания Glucovation разработала систему постоянного мониторинга сахара в крови SugarSenz, которая может использоваться как диабетиками, так и здоровыми людьми. Устройство прикрепляется (приклеивается) к коже и периодически проникает сквозь кожу для получения образца крови для измерения. Или решение компании HealthWatch в виде маек hWear со встроенными датчиками ЭКГ, что позволяет этой одежде использоваться как ЭКГ-измеритель.
- В Японии, где коммуникации и здравоохранение развиты очень сильно, обыденностью становятся «умные» унитазы (и это не шутка), которые регулярно берут анализы у членов семьи и ведут записи в карте пациента. Благодаря этому многие болезни можно предотвратить или купировать в самом начале.

3.7.2. Поддержание здорового образа жизни

Рынок устройств и приложений для фитнеса и поддержания здорового образа жизни сегодня развивается заметно быстрее, чем первое направление mHealth. Это связано не в последнюю очередь с тем, что отрасль здравоохранения очень консервативна – новые продукты и услуги появляются в ней только после многочисленных испытаний, клинических исследований и согласований с различными ведомствами. Для фитнес-устройств этого не требуется, и они быстрее находят путь к потребителю. По данным опроса, который провела компания Accenture, во всем мире 43% потребителей хотят купить устройство контроля физической активности и физического состояния.



Рис. 83. Фитнес-браслет

Список товаров этой категории включает:

- трекеры физической активности разного рода (браслеты, «умная» одежда, наушники, очки, и др.);
- спортивные часы;
- носимые сенсоры, пульсометры;

- приложения для указанных устройств и самостоятельные приложения для контроля и управления собственным физическим состоянием.

Этот рынок очень подвижен, все время появляются новые устройства, явных лидеров пока нет, хотя и слышна тяжелая поступь гигантов электронной отрасли, которые один за другим начали выпускать продукты в этой категории. Отметим, что индустрия носимых устройств может переориентироваться с браслетных трекеров, которые были популярны в 2014 году, на датчики здоровья, которые будут полностью встраиваться в или на человеческое тело в 2018 году, говорится в отчете PSFK Labs и в журнале iQ, которые курирует Intel. В 2015 году, согласно их прогнозу, функции носимых устройств расширятся и передача информации для медицинских целей и изменения поведения будет свойственна одежде, а браслеты будут использоваться для коммуникаций, верификации паролей и показывать данные о состоянии здоровья с помощью «эмоционального зеркала». В конечном счете функции коммуникации и контроля перейдут к очкам, утверждает в отчете, а в 2018 году почти все функции будут имплантированными¹⁰⁸.

В качестве примера можно привести разработки Российской компании HealBe, которая в 2015 г. выводит на международный рынок фитнес-трекер GoBe, который по изменению электропроводимости различных живых тканей способен измерять уровень глюкозы в крови, пульс, стресс, жидкости в организме, а также стресс, пройденное расстояние и качество сна. Все эти параметры по Bluetooth передаются на смартфон. GoBe – это первое носимое устройство, которое автоматически и безболезненно может контролировать количество калорий, которые поступили в организм с пищей, говорят его создатели. Прибор может пригодиться и диабетикам – для непрерывного мониторинга уровня глюкозы.

В ближайшее десятилетие подобные устройства будут использоваться в медицине все чаще, говорят эксперты. Причем отправлять данные они научатся не только на смартфон владельца, но и на сервер больницы, и на личные терминалы врачей¹⁰⁹.

3.7.3. Возможности мобильных технологий в медицине

Возможности, которые сегодня доступны в мобильной медицине, быстро растут с появлением новых устройств, датчиков, приложений. Телемедицина и удаленный мониторинг, передача данных пациентов, электронные карты, электронные рецепты, контроль сна и беременности и т.п. Эта отрасль очень быстро развивается во всем мире, даже в слабо развитых странах, где она может стать «палочкой-выручалочкой» для людей, не имеющих доступа к врачебной помощи. Повышение коэффициента использования времени врачей и их продуктивности, повышение

¹⁰⁸ URL: <http://habrahabr.ru/company/medgadgets/blog/227159/> (дата обращения 27.03.2014).

¹⁰⁹ URL: <http://www.russianelectronics.ru/leader-r/review/doc/71689/> (дата обращения 27.03.2014).

качества обслуживания, упрощение доступа и возвращение справедливости в здравоохранение (отношение к старикам, неравный доступ к услугам и т.п.), большее участие самих пациентов, потенциально снижение затрат или как минимум намного большая польза от инвестиций.

mHealth – это не только новые технологии, это совершенно новый путь взаимодействия пациента с врачом и ухода за больными. Это облегчение такого взаимодействия с обеих сторон: для пациента упрощается процесс получения медицинской помощи, для врача – уменьшается нагрузка от рутинных операций, позволяя тем самым больше времени уделять собственно диагностике и лечению. Мобильный доступ к информации облегчает получение данных и ускоряет принятие решений, а также уменьшает расстояние между пациентом и врачом. Врачи и медсестры могут общаться более эффективно и оперативно. Больницы и клиники постоянно стремятся переосмыслить модели и процессы ухода за больными для улучшения помощи пациентам и обеспечения их безопасности.

3.8. Мониторинг окружающей среды

Состояние окружающей среды, соответственно и среды обитания, непрерывно изменяется. Эти изменения различны по характеру, направленности, величине, неравномерно распределены в пространстве и во времени. Естественные, природные, изменения состояния среды имеют весьма важную особенность – они, как правило, происходят около некоторого среднего относительно постоянного уровня. Их средние значения могут существенно изменяться лишь в течение длительных интервалов времени.

Совсем другой особенностью обладают техногенные изменения состояния среды обитания, которые стали особенно значительными в последние десятилетия. Техногенные изменения в отдельных случаях приводят к резкому, быстрому изменению среднего состояния природной среды в регионе.

Для изучения и оценки негативных последствий техногенного воздействия возникла необходимость организации специальной системы контроля (наблюдения) и анализа состояния окружающей среды, в первую очередь из-за загрязнений и эффектов, вызванных ими в среде. Такую систему называют системой мониторинга состояния окружающей среды, которая является частью универсальной системы контроля состояния окружающей среды.

Под мониторингом окружающей среды (англ. monitoring от лат. Monitor – предостерегающий) понимается определенная система наблюдения (а также оценки и прогноза) состояния и развития природных процессов и явлений. Термин «мониторинг» в теории и практике защиты окружающей среды получил распространение после Стокгольмской конференции ООН по окружающей среде (1972 г.).

Основными задачами мониторинга являются:

- систематические наблюдения за состоянием среды и источниками, воздействующими на окружающую среду;

- оценка фактического состояния природной среды;
- прогноз состояния окружающей среды и оценка прогнозируемого состояния последней.

Мониторинг – это система наблюдений, оценки и прогноза состояния среды обитания.

Мониторинг является многоцелевой информационной системой¹¹⁰.

3.8.1. Виды мониторинга окружающей среды

Существует большое число видов мониторинга, различающихся по учитываемым источникам и факторам антропогенных воздействий, откликам компонентов биосферы на эти воздействия, методам наблюдений и т.п. На рис. 84 приведена классификация видов мониторинга по следующим признакам: по месту относительно окружающей среды, наблюдаемым негативным факторам, целевым функциям, базированию.

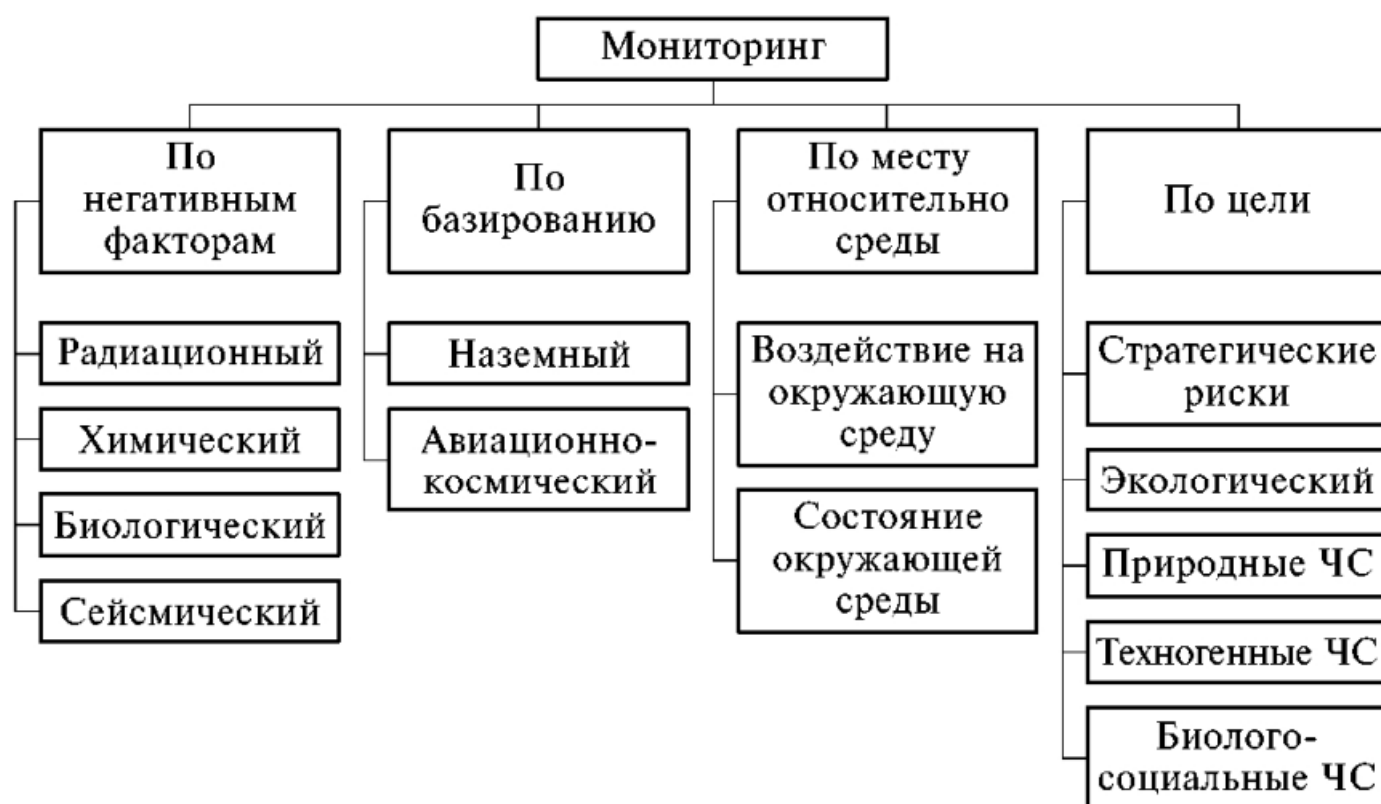


Рис. 84. Виды мониторинга окружающей среды

По месту относительно окружающей среды различают:

- мониторинг воздействия на окружающую среду;
- мониторинг состояния окружающей среды.

Мониторинг воздействия на окружающую среду – это многоцелевая информационная система, в задачи которой входят наблюдение, оценка и прогноз изменений окружающей среды под влиянием антропогенных воздействий (включая источники воздействия на окружающую среду и отходы).

Мониторинг по видам факторов воздействия делится на радиационный, химический, биологический, сейсмический и др.

¹¹⁰ URL: <http://ohrana-bgd.narod.ru/pravo5.html> (дата обращения 27.03.2014).

Мониторинг чрезвычайных ситуаций по своим целевым функциям, степени охвата контролируемой территории, техническим особенностям включает в себя мониторинг природных, техногенных, биолого-социальных чрезвычайных ситуаций, экологический мониторинг.

Наиболее информативной и представительной по числу и видам принимаемых во внимание объектов окружающей среды является система экологического мониторинга, которая охватывает геофизические и биологические аспекты. Экологическим мониторингом предусматриваются наблюдение, оценка и прогноз антропогенных изменений состояния абиотической составляющей биосферы, в том числе изменений уровней загрязнения природных сред вредными химическими, биологическими и радиоактивными веществами и ответной реакции экосистем на эти изменения. Иными словами, экологический мониторинг включает мониторинг антропогенных изменений природной среды и мониторинг вызываемых ими эффектов. Кроме того, составным элементом экологического мониторинга является мониторинг источников и факторов антропогенного воздействия. Экологический мониторинг учитывает все основные изменения, вызываемые антропогенными воздействиями на фоне естественной изменчивости.

Система экологического мониторинга позволяет решить значительную часть задач мониторинга техногенных воздействий, осуществляемого в интересах управления безопасностью и риском, которые касаются наблюдения, оценки и прогноза техногенных воздействий при нормативных (безаварийных) условиях функционирования потенциально опасных объектов. К числу этих задач следует отнести:

- наблюдение за источниками и факторами техногенного воздействия на окружающую среду и состоянием этой среды;
- оценку уровней физических полей (радиационного, акустического, теплового и др.), полей концентраций вредных веществ в различных средах в сравнении с предельно допустимыми уровнями, а также состояния окружающей природной среды, откликов и реакций абиотической и биотической составляющих биосферы на техногенные воздействия;
- прогноз техногенных воздействий, состояния окружающей среды и оценку этих прогнозных данных.

По используемым средствам (**базированию**) мониторинг делится на наземный и авиационно-космический (путем дистанционного зондирования Земли)¹¹¹.

3.8.2. Контроль погоды

В сфере мониторинга окружающей среды контроль и прогноз погоды занимают особое место. Результатами работы метеорологических служб на бытовом уровне мы интересуемся ежедневно, корректируем наши планы. Промышленность и сельское хозяйство, государственные

¹¹¹ URL: www.mchs.gov.ru/upload/site1/library/tXNOeJyL5A.pdf

службы охраны окружающей среды и безопасности в различных сферах, муниципальные службы ЖКХ и многие другие согласуют свою деятельность в соответствии с анализом и прогнозом состояния погоды.

Ведущие мировые производители оборудования и программного обеспечения принимают активное участие в развитии такой важной сферы, как контроль погоды.

Так, крупнейшая в мире IT-компания IBM анонсировала запуск в 2015 году открытой облачной технологии, которая позволит партнерам компании в разработке ПО для Интернета вещей.

В IBM говорят, что IT-сервисы, которые будут базироваться на облаке компании, помогут бизнесу использовать новые источники данных (многочисленные датчики автоматизации зданий, смартфоны и бытовая техника) и улучшить собственные продукты.

Одним из первых крупных партнеров «голубого гиганта» в этой области выбрана компания Weather Co., которой принадлежит телеканал о погоде Weather Channel. Ее подразделение WSI поможет перенести сервис с метеорологическими сводками в облако IBM, где анализом займется суперкомпьютер Watson. Комплекс мер позволит клиентам использовать данные о погоде вместе с аналитическими инструментами компании.

«Партнерство Weather Company и IBM может сделать еще умнее работу критически важных бизнес-систем», – заявил старший вице-президент подразделения IBM Analytics Боб Пиччиано. По его словам, с помощью Интернета вещей обе компании будут собирать данные о погоде с сенсоров по всей планете, хранить их в облаке, обрабатывать и предоставлять компаниям во всем мире.

«То переломный момент для компаний, которые всегда зависели от погоды, но у них раньше не было доступа к разнообразным данным или сложной аналитике», – заявил гендиректор The Weather Company Дэвид Кенни.

Weather Company сейчас выдает пользователям около 700 тыс. прогнозов в секунду. Более точные прогнозы позволят автоводителям сэкономить на ремонте машин: по данным IBM, ежегодно страховщики выплачивают миллиард долларов только водителям, машины которых пострадали от града¹¹².

Ведущим поставщиком автоматизированных систем поддержки принятия погодных решений является Weather Decision Technologies, Inc. (WDT) – американская компания, основанная в 1999 году. WDT имеет патенты на лучшие технологии для автоматического анализа данных с радаров, спутников и наземных станций, точных измерений и прогнозов осадков, предсказания опасных погодных явлений с запасом времени до 4 ч. Компания разрабатывает, интегрирует и подключает метеорологические комплексы ПО/оборудование по всему миру (гирометео, авиа, чрезвычайные погодные ситуации, мезомасштабные и локальные прогнозы). Компания также предоставляет услуги по информи-

¹¹² URL: <http://lenta.ru/news/2015/03/31/ibmiot/> (дата обращения 27.03.2014).

рованию о погоде, созданию программ и приложений, подтверждению информации о погоде, онлайн-сервисы iWatch и iMap.

Уникальные системы Weather Decision Support Systems (WDSS) используют надежные аналитические алгоритмы, авторизованные и лицензированные ведущими мировыми центрами, такими как Национальная лаборатория по изучению ураганов (NSSL), Университет Оклахомы, Университет МакГилл, MIT (Lincoln Labs). WDT – признанный лидер в системах Численного Прогноза Погоды (NWP), использующих самую совершенную модель комплексной обработки метеорологической информации WRF (Weather Research and Forecast). WDT предоставляет клиентам индивидуальные системы WDSS для решения задач гидрологии и управления водными ресурсами, метеорологии, авиации, а также различных отраслей промышленности, например для морских буровых платформ.

WDT отличают ряд важных возможностей:

- высоко интегрированная и простая в использовании система поддержки погодных решений для метеорологических служб и авиадиспетчеров;
- позволяет агрегировать информацию из различных метеоисточников: метеолокаторы, спутниковые данные, грозопеленгаторы, термодинамические радиометры и т.д.;
- позволяет строить различные типы прогнозов: турбулентность в авиации, вероятность туманности, тип осадков, краткосрочный и долгосрочный прогноз погоды;
- интеллектуальный алгоритм высокой точности для обнаружения фронта бури, прогнозирование бури, система раннего оповещения, алгоритм предсказания гроз¹¹³.

Ключевыми элементами системы анализа погодных условий и предупреждения о чрезвычайной метеорологической обстановке являются метеорологические радиолокаторы и система грозопеленгации и грозового оповещения, которые позволяют прогнозировать и своевременно предупредить пользователей о приближении экстремальной погоды и возможности подтопления или града. Все имеющиеся муниципальные системы водоотвода рассчитаны на определенный уровень осадков и при экстремальных ливнях не могут предотвратить подтопление городов.

Решить данную проблему в крупных городах практически невозможно, так как при сильных ливнях кратковременно выпадает большой объем осадков, с которым не могут справиться городские коллекторы. Задача правительственных и муниципальных органов в таких случаях своевременно предупреждать население о приближении экстремальных погодных условий, что позволит свести к минимуму возможный ущерб от подтопления, града, шквального порывистого ветра и других экстремальных погодных явлений. Система предупреждения о чрезвычайных погодных условиях на основе системы грозопеленгации и дополнитель-

¹¹³ URL: <http://www.sicenter.by/Weather-Decision-Technologies.html> (дата обращения 27.03.2014).

ного метеорологического оборудования способна отображать метеорологическую информацию в режиме реального времени, своевременно предупреждать о приближении опасных погодных явлений и прогнозировать и визуализировать четкие границы участка страны, области или города, которые находятся под угрозой подтопления, града или шквального ветра.

В качестве примера системы анализа погодных условий и предупреждения о чрезвычайной метеорологической обстановке можно привести комплексные решения американской компании Earth Networks. Компания была основана в 1993 году и в настоящее время является вторым по популярности сервисом, предоставляющим информацию о погоде в Интернете. Компания Earth Networks владеет брендом WeatherBug, существующим с 2000 года, когда впервые было запущено десктопное приложение WeatherBug.

Сегодня портфель решений компании Earth Networks включает в себя не только разработку и поставку «под ключ» систем грозопеленгации и грозового оповещения, но и предоставляет заказчикам компании ряд готовых комплексных решений для решения задач, связанных со своевременным прогнозом опасных погодных явлений во всех отраслях промышленности и общественной деятельности.



Рис. 85. Сеть автоматизированных метеорологических станций

Среди решений компании Earth Networks следует выделить:

- систему грозооповещения Dangerous Thunderstorm Alerts;
- систему раннего оповещения для национальных гидрометеослужб;
- «точечный» краткосрочный прогноз погоды для указанной геопозиции Encast;
- «метеомонитор» – пакет программ для визуализации прогноза погоды и отображения метеоинформации в режиме реального времени;
- систему предотвращения поражения молнией;
- сеть автоматических метеостанций Mesonet;
- консалтинг и поддержку национальных метеорологических агентств;
- онлайн-метеопрогноз;
- автономную автоматическую систему предупреждения о приближении грозы;
- систему поддержки метеорологических прогнозов PulseRad;
- систему поддержки принятия решений для ситуационных и диспетчерских центров StreamerRT;

- мировую сеть грозового оповещения Earth Networks Total Lightning Network (включает в себя на сегодняшний день более 700 датчиков в 40 странах мира);
- погодные камеры;
- автоматические метеорологические станции;
- WeatherBug Home – систему оптимизации энергообеспечения «умного» дома;
- систему визуализации погоды для телевизионных компаний.

На сегодняшний день основными заказчиками системы грозопеленгации и грозового оповещения являются:

- аэронавигация;
- национальные метеорологические службы;
- министерства по чрезвычайным ситуациям;
- энерготранспортные и компании в сфере энергетики и добычи природных ресурсов;
- ситуационные центры областей и городов;
- спортивные объекты;
- образовательные учреждения¹¹⁴.

В качестве примера поставщика оборудования и услуг в области контроля погоды на российском рынке можно привести белорусскую компанию «Центр системных интеграций». Эта компания работает как авторизованный поставщик и системный интегратор по установке, установке и настройке систем грозопеленгации и грозового оповещения, а также дополнительных продуктов и услуг, созданных на основании системы грозопеленгации:

- система обнаружения внутриоблачных грозовых разрядов и наземных молний, как основной индикатор приближающейся экстремальной погоды;
- системы раннего предупреждения о чрезвычайных погодных условиях для национальных гидрометеорологических служб;
- один из основных инструментов анализа ситуации и создания краткосрочного прогноза погоды в системах поддержки принятия решений;
- отображение погоды в режиме реального времени, востребованное в различных сферах – от рядовых пользователей до телевизионных агентств и отраслевых решений в различных сферах промышленности;
- пакет готовых приложений для отображения грозовых разрядов в режиме реального времени и отображения в различных приложениях – от корпоративных систем прогноза погоды до отображения погодных условий в пользовательских приложениях для смартфонов и планшетов;
- Научные исследования изменения климата¹¹⁵.

¹¹⁴ URL: <http://www.sicenter.by/weatherbug.html> (дата обращения 27.03.2014).

¹¹⁵ URL: <http://www.sicenter.by/weatherbug.html> (дата обращения 27.03.2014).

3.8.3. Сейсмический мониторинг

Сейсмический мониторинг относится к технологиям уменьшения риска опасных природных явлений. Он базируется на организации сети непрерывных долговременных наблюдений на исследуемой территории. В современной трактовке мониторинг включает не только регистрацию, но и дальнейшую оперативную обработку и интерпретацию сейсмологических данных с выходом на прогнозные оценки. В зависимости от размеров охватываемой мониторингом территории он может подразделяться на уровни: мировой, региональный, локальный.

Сейсмический мониторинг является неотъемлемой частью жизнеобеспечения населения регионов с выраженной сейсмической активностью. Он позволяет автоматически детектировать, определять местоположение и наносить на карту даже очень слабые сейсмические события, что способствует изучению динамики тектонических разломов.

Сейсмический мониторинг является также неотъемлемой частью систем обеспечения безопасности ответственных сооружений (в частности, атомных электростанций, скважин, шахт, мостов и др.). Соединенные со средствами коммуникаций, системы мониторинга позволяют осуществлять уведомление населения и официальных лиц о происходящих землетрясениях или других сейсмических событиях.

В настоящее время сейсмический мониторинг осуществляется практически во всех странах Европейского континента и во многих странах мира, при этом не обязательно расположенных в сейсмически активных поясах Земли.

В связи с развитием промышленности, особенно энергетической сферы, возникла необходимость сейсмического контроля тех участков земной коры, на которых расположены объекты энергетики.

Обычно для *сейсмического мониторинга* используется сеть сейсмических станций, равномерно распределенная на площади исследований или охватывающая исследуемый участок. Кроме отдельных сейсмических станций, в некоторых странах Европы используются также сейсмические группы (*seismic array*), которые можно назвать сейсмическими «антеннами». Сейсмические группы есть в некоторых странах Скандинавии и северной Европы – в Норвегии, Швеции, Финляндии, Германии, России.

Прикладными задачами сейсмического мониторинга являются изучение региональной или локальной сейсмической активности данной территории или локального участка (например района АЭС, ГЭС, рудников, шахт, открытых карьеров и т.д.).

В результате локации сейсмических источников и определения их параметров (времени в очаге, координат эпицентра, глубины гипоцентра – в случае землетрясения и магнитуды) появляются новые, инструментальные данные о современных землетрясениях. Эти данные, совместно с данными об исторических землетрясениях, используются для сейсмического районирования. На основе пространственного распределения гипоцентров землетрясений, оценки их параметров (сейсмической активности, максимальной магнитуды землетрясения) оконтуривают сейсмогенные зоны и оценивают сейсмический риск территории.

С 2010 года в странах Евросоюза внедряются новые стандарты по оценке сейсмических условий *Eurocode-08*.

Другая практическая цель использования сейсмического мониторинга – создание системы сигнализации и предупреждения о сейсмической опасности от тектонических землетрясений вокруг крупных инженерно-технических и экологически опасных объектов, таких как атомные гидроэлектростанции и речные дамбы. Игналинская система сигнализации и предупреждения о сейсмической опасности в Литве является примером решения такой задачи.

Результаты сейсмического мониторинга используются и в научных целях – для изучения внутреннего строения Земли, физических свойств вещества недр и т.д.

Системы мониторинга, совмещенные с мобильными сейсмическими группами, эффективно используются для различного рода научных и прикладных исследований, включая картирование магматических тел, геотермальных ресурсов и залежей гидрокарбонатов.

Автоматический сейсмический мониторинг реального времени является не только важнейшей, но и одновременно сложнейшей задачей сейсмологической практики. Его важность определяется такими потребностями, как:

1. Оперативная корректировка карт тектонической активности региона, карт балльности и сотрясаемости.
2. Необходимость принятия экстренных мер и исполнения оперативных мероприятий в зависимости от текущей сейсмической обстановки на основе автоматических уведомлений, обеспечиваемых системой мониторинга.
3. Автоматическое формирование баз сейсмологических данных, включая их наполнение непрерывными волновыми формами наблюдаемых процессов, бюллетенями сейсмическими событиями и прочей сопроводительной информацией.
4. Обмен информацией с другими сейсмологическими центрами и сетями сбора данных.
5. Автоматическое использование непрерывных данных реального времени от других сейсмических сетей с целью улучшения локации сейсмических событий и оценки их параметров.

Для реализации эффективной системы сейсмического мониторинга реального времени требуется высокоразвитое аппаратное и математическое программное обеспечение, отвечающее современным требованиям.

Одним из примеров проведения сейсмического мониторинга является построение в 2006 г. в районе эпицентра Урэг-Нурского землетрясения локальной сети временных сейсмологических станций. Целью проведения работ было получение информации об особенностях фоновой сейсмичности в этом районе Алтая. Важно было получить первые сведения о глубинах землетрясений в этом районе, уточнить информацию о пространственной приуроченности землетрясений к тем или иным тектоническим структурам, изучить механизмы очагов землетрясений. Пример сети станций приведен на рисунке.

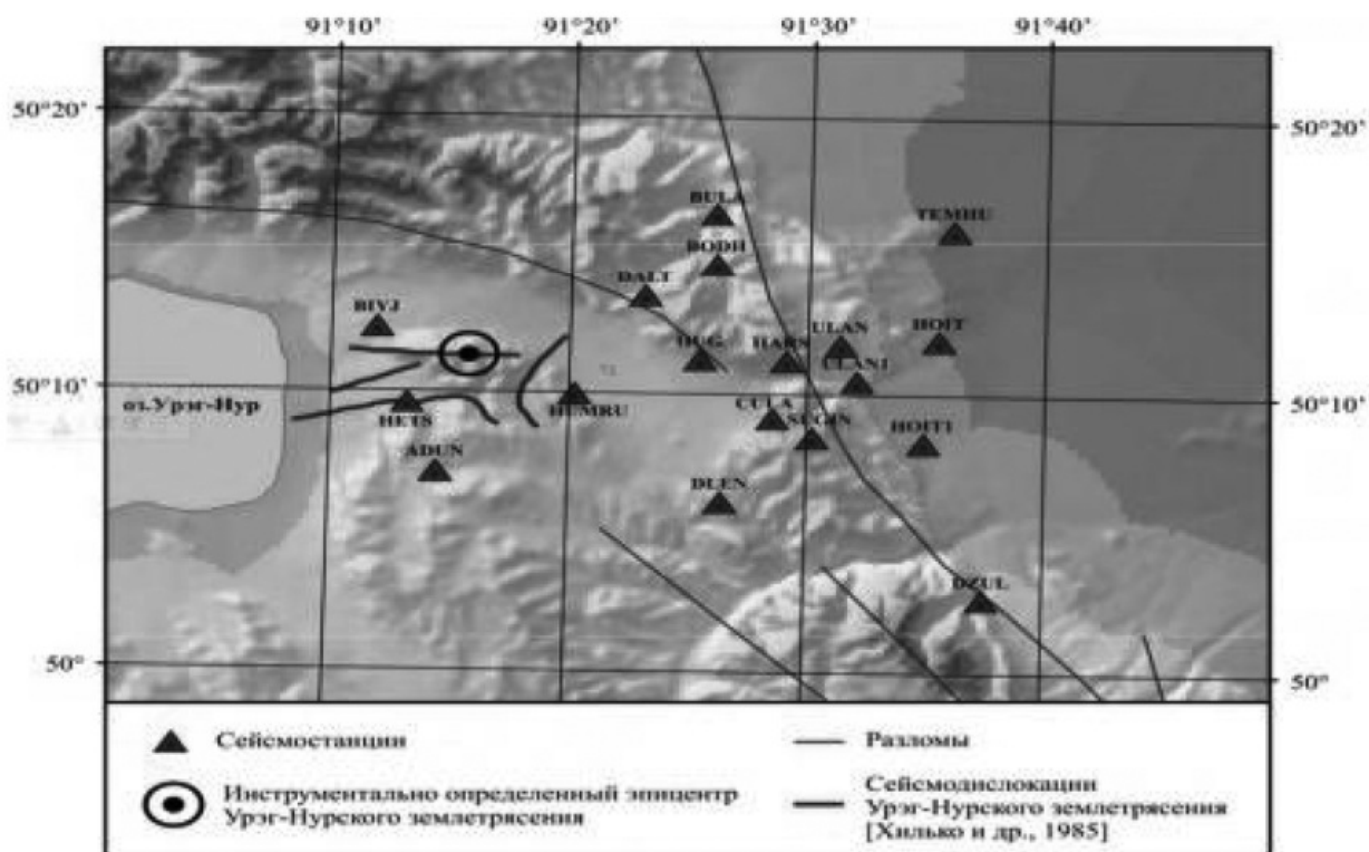


Рис. 86. Пример сети сейсмологических станций

3.9. Системы безопасности и охранные комплексы

Конечно же, Интернет входит и в отрасль безопасности. RFID-технология активно применяется в системах контроля и управления доступом (СКУД) для целей идентификации объектов доступа (людей, автомобилей). При этом используются различные стандарты и физические форматы RFID-меток.

Для идентификации людей наиболее популярным является формат бесконтактной пластиковой карточки, по размеру совпадающей с банковской, карточку для запроса доступа, как правило, нужно осознано подносить к считывающему устройству на расстояние порядка 10 см.

В ключи зажигания автомобилей также иногда встраиваются метки для повышения защиты от угона. Считыватель находится в замке зажигания и подключен к иммобилайзеру или бортовому компьютеру.

3.9.1. Безопасность и охрана жилища

В 2013 году компания August анонсировала умный замок, который может открываться ключом или через Bluetooth при поднесении смартфона. Кроме того, разработчики пошли еще дальше и добавили возможность рассылать приглашения-ключи другим людям, они смогут также открыть дверь. Да еще и оставить свои комментарии – приложение на телефоне является клиентом к профильной социальной сети¹¹⁶.

¹¹⁶ URL: <http://apptractor.ru/internet-veshhey> (дата обращения 27.03.2014).



Рис. 87. «Умный» дверной замок

«Умные» дверные замки – идея не новая, однако многие из них не всегда удобны и даже требуют ежемесячной платы за обслуживание. Компания August разработала новое устройство, которое легко монтируется и позволяет слать ключи доступа на смартфоны iPhone 5 и 4S, при этом не требуя дополнительных расходов.

Для установки замка достаточно заменить лишь часть секретного механизма существующего. Замок можно открывать и закрывать как с помощью iPhone через Bluetooth, так и обычным ключом. Электронные ключи доступа (приглашения) рассылаются через отдельное приложение и либо имеют срок действия (например, если вы пригласили гостей), либо работают на постоянной основе. Замок распознает хозяина и открывается автоматически без необходимости дополнительных действий с его стороны.

Более того, приложение для замка – это маленькая приватная социальная сеть. Устройство фиксирует, кто и когда заходил и выходил, а приложение позволяет оставлять заметки и фотографии. August Smart Lock не требует подключения к Wi-Fi-сети, он также не зависит и от электросети, поскольку работает от 4 батареек, которые «продержатся» от 6 месяцев до года. Приложение показывает уровень заряда, поэтому отключение устройства не застанет врасплох¹¹⁷.

Компания Honeywell, известный производитель термостатов, в конце 2014 года продемонстрировала разработку под названием Lyric. Речь идет не об одноименном термостате, а о новой линейке устройств, призванной защитить дом от вторжения. В нее входят центральный модуль с тачскрином, две различных панели управления, детектор дыма, сирена, брелок для взаимодействия с системой, а также датчики открытия, движения и разбития стекла.

¹¹⁷ URL: <http://onegadget.ru/cat/home/page/5> (дата обращения 27.03.2014).



Рис. 88. Линейка устройств Lyrig для защиты дома от вторжения

Из любопытного отметим возможность управления с помощью голосовых команд, интеграцию с термостатом Lyrig и поддержку мобильного приложения для iOS/Android¹¹⁸.

3.9.2. Охрана территорий

В первой половине 2014 года было заявлено, что Томский университет систем управления и радиоэлектроники (ТУСУР) и ЗАО «НПФ Микран» приступили к разработке радаров миллиметрового диапазона и созданию на их основе комплексных систем мониторинга для выделенных пространств¹¹⁹. Изначально предполагалось, что затраты на проект составят порядка 360 млн рублей.

Основным элементом системы будет высокоточная радиолокационная станция. Система сможет обнаружить подвижные цели на подконтрольной территории и отследить их перемещение. Для повышения эффективности системы к ней будут подключены видеокамеры и другие охранные датчики. В перспективе можно ожидать, что это повысит безопасность охраняемых объектов и снизит риск для жизни и здоровья работающих там охранников.

3.9.3. Системы «интеллектуального» видеонаблюдения

Системы видеонаблюдения играют важную роль в обеспечении безопасности граждан, производственных и бизнес-процессов организаций, инфраструктурных, транспортных, гражданских и специальных объектов. Особенно эффективны системы видеонаблюдения в случае их объединения с программно-аппаратными комплексами анализа видеопотоков реального времени. Это позволяет снизить зависимость уровня безопасности граждан, бизнес-процессов и объектов от ошибок операторов (человеческого фактора), максимально быстро выявлять угрожающие ситуации и привлекать к ним внимание соответствующих служб.

¹¹⁸ URL: http://www.ferra.ru/ru/digihome/review/SmartHome-January2015/#Honeywell_готовится_к_покорению_рынка_систем_безопасности (дата обращения 27.03.2014).

¹¹⁹ «Умные» сенсоры для охранных комплексов разработают в Томске // RIA.RU : РИА Новости. 2013. URL: <http://ria.ru/science/20130412/932302042.html> (дата обращения 27.03.2014).

Системы «интеллектуального» видеонаблюдения активно внедряются сегодня во многих сферах, в том числе на транспорте и в ЖКХ.

В настоящее время Московская городская телефонная сеть (МГТС) проводит в нескольких округах Москвы тестирование системы «интеллектуального» видеонаблюдения. В тестовых зонах МГТС установила 300 видеокамер наблюдения. В настоящее время с их помощью проверяется возможность автоматического мониторинга качества работы организаций ЖКХ.

В ближайшее время МГТС планирует создать еще пять опытных зон, в которых протестирует возможности проектов видеоаналитики как для бизнес-пользователей, так и для индивидуальных потребителей. Кроме того, компания уже создала Центр интеллектуального видеонаблюдения, на базе которого будет построена система по сбору, анализу и использованию видеоданных в Москве. Инвестиции в ситуационный центр и пилотные зоны составят 30 млн рублей.

Информацию с камер и результаты ее «интеллектуальной» обработки МГТС будет передавать по высокоскоростной оптоволоконной сети на базе технологии GPON в ситуационный центр заказчика для анализа и дальнейшей обработки. Все видеоданные будут храниться от месяца и более в одном из центров обработки данных группы компаний МТС, в которую входит оператор МГТС.

Система будет иметь различные возможности по масштабированию (от локального решения в одной квартире или доме до проектов для всего города) и осуществлению любых видов видеоанализа (от обнаружения и отслеживания движения различных объектов, их классификации и идентификации до распознавания и автоматического реагирования на заданные в программе анализа ситуации).

Первичный анализ информации, обнаружения и сопровождения подозрительных ситуаций автоматически позволяет уменьшить нагрузку на каналы связи и систему архивирования за счет фильтрации ненужных видеоданных (более 99% первичного видео не представляет интереса для аналитики) и снизить нагрузку на операторов, сократив их количество.

Каждая тысяча видеокамер генерирует более 16 ч видео в минуту, на обработку которого в ручном режиме необходимо 100 человек. После внедрения системы видеоаналитики, по расчетам МГТС, для анализа этого же объема информации потребуется не более пяти-десяти человек.

Осенью 2014 года протестированные решения и созданные в рамках пилотных зон продукты начали вводиться в коммерческую эксплуатацию для корпоративных и государственных заказчиков. Для этого МГТС намерена дополнительно установить восемь тысяч видеокамер; в дальнейшем количество камер будет увеличено под конкретные проекты. Вывод системы на массовый рынок запланирован в 2015 году.

Действующая сейчас госпрограмма «Безопасный город» предусматривает инвестиции в размере 192,7 млрд рублей в московские системы безопасности. Как ожидается, до 2016 года в столице должны

полностью оснастить системами безопасности транспорт, объекты городского хозяйства, социальной сферы и спорта.

В настоящее время МГТС обслуживает более 47 тыс. камер, расположенных в парках, школах, придомовых территориях и местах массового скопления людей в трех округах Москвы. По оценке компании, для полного покрытия Москвы видеонаблюдением необходимы не менее 300 тыс. камер, для оценки данных с которых без применения автоматизированных систем видеонализа необходимо около восьми тысяч сотрудников.

Система видеонаблюдения за ЖКХ позволяет, например, не только увидеть, убран снег во дворах или нет, выходила ли уборочная техника, но и контролировать ход таких работ. С помощью информации, полученной со средств видеофиксации, удалось обнаружить несколько нарушений, за которые подрядные организации по итогам 2013 года были оштрафованы на 1,2 млрд руб.¹²⁰

В конце прошлого года состоялся конкурс на разработку проектной документации на оснащение системой интеллектуального видеонаблюдения (ИСВН) объектов Московского метрополитена. Сумма контракта составила более 387 млн рублей. И это лишь 10% от общей суммы, составляющей приблизительно 4 млрд рублей, выделенной из федерального и городского бюджета на внедрение в Московском метрополитене современной системы интеллектуального видеонаблюдения.

В 1998 году Московский метрополитен обзавелся первыми системами видеонаблюдения с записью видео. Сегодня камеры установлены на всех станциях и во всех переходах, а также во всех вагонах Кольцевой линии. Начиная с середины 2012 года на многих станциях Московского метрополитена проводились пилотные внедрения интеллектуального видеонаблюдения.



Рис. 89. Автоматическая идентификация «бесхозного» предмета

¹²⁰ URL: <http://texnomaniya.ru/technology/v-moskve-postroyat-sistemu-intellektualnogo-videonablyudeniya.html> (дата обращения 27.03.2014).

Сопоставление информации, полученной от обзорного видеонаблюдения, биометрической и ситуационной видеоаналитики, позволит в автоматическом режиме выявлять противоправные действия, фиксировать нарушителей и проверять их по базам розыска. А также прогнозировать маршрут их перемещения для осуществления задержания службой охраны.

Для выполнения этих задач будут использоваться камеры двух типов: для обзорного и ситуационного видеонаблюдения – IP-камеры, а для биометрического видеонаблюдения – камеры машинного зрения.

Информационно-аналитическая подсистема также играет важную роль, ведь ежедневно столичное метро пропускает более 8 млн пассажиров. Получение статистических данных о распределении пассажиропотоков позволит скорректировать работу эскалаторов, интервалы между поездами, работу касс и обслуживающего персонала.

Московский метрополитен настолько многолюден, что неизбежно ежедневное выявление видеоаналитикой огромного количества событий. Некоторые из них не требуют молниеносной реакции персонала метрополитена и внешних служб, но есть и другая категория событий, например, падение человека на рельсы или обнаружение опасного преступника. Для того чтобы реагировать на наиболее важные, не терпящие отлагательств, события в первую очередь, в системе интеллектуального видеонаблюдения будет предусмотрена система приоритетов (ранжирования событий). Приоритет события может зависеть от различных признаков: типа события, зоны наблюдения, точности распознавания, дальности объекта и других, а также от комбинации этих факторов. Причем для разных категорий пользователей приоритеты будут разными, так как у каждой службы своя зона ответственности.



Рис. 90. Автоматическая идентификация человека

Для оперативного получения информации о тревожных событиях патрульные службы, осуществляющие контроль за порядком на территории метрополитена, а также другие сотрудники метрополитена будут оснащены мобильными терминалами. На них будут поступать опера-

тивные уведомления о тревожных событиях, требующих быстрого реагирования, в том числе о появлении лиц, представляющих интерес для патруля. При обнаружении такого лица система интеллектуального видеонаблюдения будет определять возможную траекторию его следования и отправлять уведомление на мобильные терминалы нарядов, находящихся в непосредственной близости от этой траектории. В уведомлении будет отображаться фотография зафиксированного лица, время и место его обнаружения, а также причина привлечения внимания патруля и инструкция по действиям. Время доставки тревожного события на мобильное устройство составит не более 10 с, а передача информации будет осуществляется при помощи беспроводных Wi-Fi точек доступа и с использованием сетей GSM 2G\3G¹²¹.

3.10. Перспективы развития Интернета вещей

Концепция Интернета вещей может быть воплощена на практике с использованием различных наборов технологий, и электронный мониторинг – лишь один из них. Сегодня существуют технические разработки, которые способны расширить пространство применения технологий Интернета вещей в обозримом будущем.

3.10.1. Развитие рынка Интернета вещей

Согласно исследованиям аналитической фирмы IDC, рост мирового рынка Интернета вещей (Internet of Things, IoT) создает широкие возможности для производителей всех вертикальных рынков, которые включают в свою продукцию эту категорию товаров. По прогнозу компании, к 2017 году рынок IoT-продуктов может вырасти почти в два раза.

Согласно оценкам IDC, доходы от технологий и сервисов для поддержки IoT (включая компоненты, процессы и ИТ-поддержку) увеличатся с 4,8 трлн долл., зафиксированных в 2012 г., до 7,3 трлн к 2017 г. Среднегодовые темпы роста на этом рынке за период 2012–2017 г. составят 8,8%.

Аналитики обследовали 18 вертикальных рынков, чтобы оценить на ближайшие несколько лет их возможности, связанные с адаптацией технологии IoT. Очевидно, что в настоящее время существуют глобальные возможности для рынка IoT, это и подключенные к Сети дома и автомобили, и «умные» измерения, и «умные» устройства, производящие контроль и отображающие показатели состояния здоровья организма. Все эти уже существующие продукты, по мнению IDC, стимулируют производство на вертикальных рынках.

В IDC полагают, что рынок Интернета вещей следует рассматривать в приложении к вертикальным рынкам, так как ценность IoT-продукта базируется на его конкретном использовании на каждом из этих рынков. Усилия маркетологов и успех продаж будут находиться в прямой зависимости от того, насколько доходным является тот или иной вертикальный рынок на его потенциале для данного продукта. Аналитики подчеркивают, что развитие вертикальных рынков, исполь-

¹²¹ URL: <http://habrahabr.ru/company/synesis/blog/212119/> (дата обращения 27.03.2014).

зующих IoT, должно соответствовать специфическим для отрасли бизнес-процессам. На начальном этапе внедрения IoT наибольшие возможности получают вертикальные рынки, выпускающие предметы потребления, дискретное производство и государственные предприятия. Пока же далеко не все отрасли понимают ценность IoT-продукта.

Первым шагом на пути монетизации IoT-продуктов становится экосистема IoT/M2M. ИТ-компании, сфокусированные на горизонтальных рынках, в ближайшие 5 лет будут создавать IoT-решения (в том числе приложения M2M) как для промышленных приложений, так и для потребительского рынка¹²².

3.10.1.1. Мировой рынок Интернета вещей

Один из ключевых факторов, обуславливающий рост мирового рынка Интернета вещей, – это растущее число подключаемых устройств. По оценкам Cisco, в 2008 году количество устройств в Интернете превысило население Земли, и сейчас на каждого жителя планеты приходится более 3 подключаемых к Интернету устройств.

Определение размера рынка Интернета вещей представляет некоторую сложность, так как существует множество определений Интернета вещей, каждое из которых претендует на большую системность и полноту. В рамках исследования, проведенного компанией J'son & Partners Consulting, под рынком Интернета вещей понимается совокупность рынков следующего оборудования, технологий и услуг, обеспечивающих межмашинные коммуникации:

RFID	Облачные сервисы	SCADA
Датчики	NFC	Zigbee
Шлюзы	СЕР	IDS

С учетом этого и для целей прогнозирования мирового рынка эксперты J'son & Partners Consulting использовали консенсус-оценки, проведенные на основе прогнозов ряда агентств, таких как GSMA, Harbor Research, ABI Research и т.д. Данные были проанализированы и преобразованы в наиболее вероятный прогноз.



Рис. 91. Прогноз развития мирового рынка ИВ, 2010–2020 гг.

¹²² URL: <http://www.itbestsellers.ru/news/detail.php?ID=29079> (дата обращения 27.03.2014).

По данным J'son & Partners Consulting, в 2013 году размер мирового рынка Интернета вещей составил 98 млрд долл. и 14,3 млрд устройств. В перспективе до 2020 года объем рынка вырастет до 359 млрд долл. и 34,2 млрд устройств.

Основную долю в объеме мирового рынка ИВ занимают технологии RFID, датчики и NFC-модули.

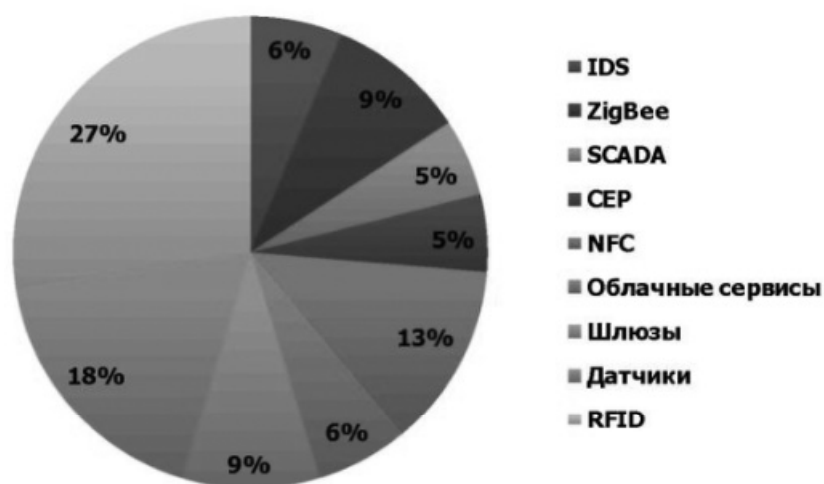


Рис. 92. Консенсус-оценки структуры мирового рынка ИВ в 2010–2013 годах

ИВ находит применение во множестве отраслей экономики, специализированных процессах, повседневной жизни. Сегментация по сферам применения включает:

- городскую среду и общественную безопасность («умные» города, подключенные здания, «умные» счетчики для ЖКХ, «умный» транспорт, технологии геолокации и др.);
- розничную торговлю и банковские услуги (RFID, электронные платежные устройства и системы);
- электроэнергетику («умные» электросети, энергосберегающие технологии);
- здравоохранение (удаленная поддержка пациентов и пожилых людей);
- частную жизнь («умный» дом, «умные» автомобили, потребительская телематика) и др.¹²³

3.10.1.2. Российский рынок Интернета вещей

Участники рынка достаточно сдержанно оценивают современное состояние и развитие российского рынка ИВ в сравнении с тенденциями в передовых странах. Тем не менее на протяжении последних лет национальный рынок начал формироваться путем реализации ряда «пионерских» проектов по применению технологии RFID, работ по использованию предустановленного оборудования GPRS/ГЛОНАСС на транспорт-

¹²³ Аналитический обзор «Интернет вещей и межмашинные коммуникации». URL: http://www.json.ru/poleznye_materialy/free_market_watches/analytics/internet_vewej_i_mezhmashinnye_kommunikacii_obzor_situacii_v_rossii_i_mire/ (дата обращения 27.03.2014).

ных средствах, строительства умных парковок, пилотных проектов NFC в московском метро и платежных терминалах, запуска M2M-услуг на базе специальных SIM-карт и устройств типа GPS-трекеров для разных целевых групп потребителей.



Рис. 93. Прогноз развития российского рынка ИВ, 2010–2020 гг.

В соответствии с прогнозом J’son & Partners Consulting, российский рынок ИВ в 2015 году вырастет до 527 млн долл., а в перспективе до 2020 года – до 980 млн долл. Основными драйверами будут, как и в мире, технология RFID, сенсорные сети и NFC¹²⁴.

3.10.2. Внедрение единых стандартов

Отсутствие единых стандартов является одним из главных препятствий в развитии ряда технологий Интернета вещей, включая сугубо бытовые. В связи с этим компания Qualcomm совместно с Linux Foundation стала организатором альянса, цель которого – преодоление отсутствия стандартов и продвижение концепции «умного дома» на рынке. Был учрежден AllSeen Alliance для создания и развития открытой структуры, позволяющей устройствам различных производителей взаимодействовать друг с другом. В альянс входят такие компании, как Qualcomm, LG, Panasonic, Haier, Silicon Image, TP-Link и др. Среди членов значатся Cisco, Sears, Wilocity и Linux Foundation¹²⁵.

Изначально Qualcomm пыталась продвигать свой стандарт AllJoyn для взаимодействия подключенных вещей, но добиться успеха не удалось. В итоге технология была передана созданному альянсу для дальнейшего развития. «Мы находимся на этапе, когда компании пытаются реализовать концепцию Интернета вещей исключительно собственными силами, потому что не видят другого решения, а создание альянса при-

¹²⁴ Аналитический обзор «Интернет вещей и межмашинные коммуникации». URL: http://www.json.ru/poleznye_materialy/free_market_watches/analytics/internet_vewej_i_mezhmashinnye_kommunikacii_obzor_situacii_v_rossii_i_mire/ (дата обращения 27.03.2014).

¹²⁵ Abuot Allseen // ALLSEENALLIANCE.ORG: AllSeen Alliance. URL: <https://allseenalliance.org/allseen> (дата обращения 25.02.2014).

звано показать, что есть работающая и достаточно развитая технология, которой Qualcomm хочет поделиться», – утверждает вице-президент компании Роб Чандхок.

Отдельно подчеркивается и озвученный ранее факт слабого развития Интернета вещей на практике. Поначалу мы начнем с малого, вроде управления замками и лампочками, – считает Роб Чандхок, – а постепенно технология будет становиться все более всеобъемлющей»¹²⁶.

Проблема аппаратной совместимости может быть разрешена при помощи разработок компании Intel. Intel анонсировала процессор Quark, который позиционируется как процессор для Интернета вещей. На сегодня это один из самых маленьких процессоров (1/5 от Intel Atom), однако его энергопотребление меньше в 10 раз. На Intel Developer Forum CEO Брайан Кржанич объяснил, что компания планирует поставлять процессор и платы на его основе производителям бытовой техники и электроники¹²⁷. Intel намеревается стимулировать другие компании к использованию их технологии.

При этом в Intel создано специальное подразделение Internet of Things Solution Group¹²⁸. В задачи данного подразделения входит развитие процессоров Atom и Quark и их продвижение на рынке. Программное обеспечение разрабатывают дочерние компании Wind River и McAfee.

А стандартной операционной системой для Интернета вещей может стать Android¹²⁹. Технологический директор недавно созданного облачного сервиса Xively Филипп ДесАустельс утверждает, что «С Android вы получаете энергоэффективную систему, для которой легко разработать сенсорный интерфейс, в нее легко загружать данные и выгружать их обратно. За ней просто стоит самое большое сообщество». Пример использования данной ОС в концепции Интернета вещей – система орошения сельскохозяйственных полей, в которой сеть крохотных водостойких компьютеров управляет водяными клапанами.

Важно отметить, что доля устройств под управлением Android на рынке перевалила за 80% уже в ноябре 2013 года¹³⁰. Учитывая, что смартфоны и планшеты являются одними из основных подключенных устройств, нельзя недооценивать перспективы этой системы.

¹²⁶ Ходаковский К. Альянс AllSeen ускорит внедрение концепции «Интернета вещей» // 3DNESW.RU : Daily Digital Digest. 2013. URL: <http://www.3dnews.ru/786664> (дата обращения 25.02.2014).

¹²⁷ Intel анонсировала Quark, процессор для «Интернета вещей» // HABRAHABR.RU : Информационный портал. 2013. URL: <http://habrahabr.ru/post/193382/> (дата обращения 25.02.2014).

¹²⁸ Merritt R. Intel Creates Internet of Things Group // EETIMES.COM : Connecting the Global Electronics Community. 2013. URL: http://www.eetimes.com/document.asp?doc_id=1320001 (дата обращения 25.02.2014).

¹²⁹ За «Интернетом вещей» стоит Android – и он везде // HABRAHABR.RU : Информационный портал. 2013. URL: <http://habrahabr.ru/post/182674/> (дата обращения 25.02.2014).

¹³⁰ Доля Android на рынке мобильных ОС впервые перевалила за 80% // IXBT.COM : Информационный портал. 2013. URL: <http://www.ixbt.com/news/hard/index.shtml?17/36/41> (дата обращения 25.02.2014).

Заключение

Быстрое развитие информационных технологий постепенно приводит к возникновению информационного пространства нового формата, которое будет способно захватывать данные о физических объектах в реальном времени. По мере развития технологий техника становится автономной, уменьшая издержки человеческой деятельности.

Концепция Интернета вещей, призванная описать новый этап развития информационного пространства в целом и Интернета в частности, привлекает пристальное внимание ведущих мировых компаний, исследовательских центров и ученых. Отдельные аналитики считают, что 2014 год станет годом Интернета вещей¹³¹.

При этом практическое развертывание технологий Интернета вещей в различных областях бизнеса можно считать достаточно низким. На сегодняшний день наибольшее развитие получили системы электронного мониторинга, а также их основная составляющая часть – технологии идентификации.

Подобную логику развития можно считать более чем закономерной. Технологии идентификации позволяют перекинуть мост между двумя мирами – физическим и информационным. Для того чтобы машины смогли получать данные непосредственно из внешней среды, им необходимо научиться распознавать и идентифицировать среду. А технологии идентификации, к которым относятся RFID и штрихкодирование, дают возможность создать подобие информационного двойника для физического объекта.

Вероятно, в дальнейшем получат развитие и другие технологии, относящиеся к сфере Интернета вещей. Прежде всего, в обозримом будущем можно ожидать широкого распространения «умной» инфраструктуры, которая будет запоминать и анализировать потребности людей, чтобы сделать внешнюю среду безопаснее, удобнее, комфортнее. Сегодня развитие таких технологий тормозится отсутствием единых форматов и мощных, но при этом миниатюрных источников питания. Однако шаги в обоих направлениях уже предпринимаются.

Подводя итог, можно сказать, что Интернет вещей действительно обладает потенциалом изменить мир. И первые изменения коснутся различных бизнес-процессов, оптимизация или переработка которых станет следствием развития технологий Интернета вещей.

¹³¹ Cohen S. Year of The Internet of Things. 2014. URL: <http://www.forbes.com/sites/sarahcohen/2014/01/14/year-of-the-internet-of-things/> (дата обращения 25.02.2014).

Используемая литература

1. *Акимов В.А., Лесных В.В., Радаев Н.Н.* Основы анализа и управления риском в природной и техногенной сферах: Учеб. пособие // «Деловой экспресс». М., 2004. С. 41–44. URL: www.mchs.gov.ru/upload/site1/library/tXNOeJyL5A.pdf (дата обращения 27.03.2014).
2. Бесконтактные сенсоры сердца встроит в умные дома // NEWSLAND: Новости. 2010. URL: <http://newsland.com/news/detail/id/526079/> (дата обращения 27.03.2014).
3. Впервые источником кибератаки стал интернет вещей // МК.RU: Московский Комсомолец. 2014. URL: <http://www.mk.ru/science/technology/article/2014/01/20/972642-vpervyie-istochnikom-kiberataki-stal-internet-veschey.html> (дата обращения 25.02.2014).
4. В России построят самые умные в мире дороги // ZR.RU: За Рулем.рф. 2013. URL: http://www.zr.ru/content/news/509946-v_rossii_postrojat_samyje_umnyje_v_mire_dorogi/ (дата обращения 27.03.2014).
5. Выбить пробки. Как японцы приручили большой город // RG.RU: Российская газета. 2012. URL: <http://www.rg.ru/2012/07/05/japan-poln.html> (дата обращения 27.03.2014).
6. ГЛОНАСС нужен «эффект масштаба» // GLONASS-PORTAL.RU: Глонасс портал. 2013. URL: http://www.glonass-portal.ru/articles/2012-10-24/gurko_glonass_perspektiva.avcms (дата обращения 27.03.2014).
7. Дайджест инцидентов в области информационной безопасности: 18 июля – 18 августа // KASPERSKY.RU : Блог о бизнесе «Лаборатории Касперского». 2013. URL: <http://business.kaspersky.ru/security-digest-jul18-aug18/> (дата обращения 25.02.2014).
8. Датчики и интеллектуальные сенсоры: [Электронный документ] // RFE.BY : Факультет радиофизики и компьютерных технологий БГУ, Минск. Сис. требования: Adobe Reader. URL: <http://www.rfe.by/media/kafedry/kaf5/publikation/kozlova/metrologia1/present13-14.pdf> (дата обращения 27.03.2014).
9. Доля Android на рынке мобильных ОС впервые перевалила за 80% // IXBT.COM: Информационный портал. 2013. URL: <http://www.ixbt.com/news/hard/index.shtml?17/36/41> (дата обращения 25.02.2014).
10. «Интернет вещей и межмашинные коммуникации. Обзор ситуации в России и мире» // Исследование компании J'son & Partners Consulting 2013. URL: http://www.json.ru/files/news/2013-06-25_IOT_MW_RU.pdf (дата обращения 25.02.2014).
11. За «Интернетом вещей» стоит Android – и он везде // НАВРАНАБР.RU: Информационный портал. 2013. URL: <http://habrahabr.ru/post/182674/> (дата обращения 25.02.2014).
12. *Ильин Ю.* Американо-израильское происхождение боевого трояна Stuxnet подтверждено // COMPUTERRA.RU : Журнал «Компьютерра». 2012. URL: <http://www.computerra.ru/31401/> (дата обращения 25.02.2014).
13. Интеллектуальные сенсоры // INTUIT.RU. 2014. URL: <http://www.intuit.ru/studies/courses/590/446/info> (дата обращения 27.03.2014).
14. Интернет вещей – а что это? // НАВРАНАБР.RU : Информационный портал. 2012. URL: <http://habrahabr.ru/post/149593/> (дата обращения 25.02.2014).

15. Интернет вещей в действии был продемонстрирован участниками конференции Cisco Live // CISCO.COM: Новости. 2013. URL: <http://www.cisco.com/web/RU/news/releases/txt/2013/07/070813f.html> (дата обращения 25.02.2014).
16. Интернет вещей и межмашинные коммуникации: современные технологии, тренды, дорожные карты. Обзор ситуации в России и в мире // APPS4ALL.RU : Разработчики и приложения для мобильных устройств. 2013. URL: <http://apps4all.ru/post/12-23-13-json-partners-consulting-predstavlyaet-issledovanie-quotinternet-veschej-i-mezhmashinnye-kommunikatsii-sovremennye-tehnologii-trendy-dorozhnye-karty-obzor-situatsii-v-rossii-i-mirequot> (дата обращения 25.02.2014).
17. Интернет вещей: уязвимость и безопасность // KASPERSKY.RU : Блог о бизнесе «Лаборатории Касперского». 2014. URL: <http://business.kaspersky.ru/internet-of-things-insecurity/> (дата обращения 25.02.2014).
18. Карасев С. ARM намерена закрепиться на рынке «Интернета вещей» // 3DNESW.RU: Daily Digital Digest. 2013. URL: <http://www.3dnews.ru/775743> (дата обращения 25.02.2014).
19. Классификация датчиков, основные требования к ним // ELECTROLIBRARY.INFO: Избранные материалы рассылки. URL: http://www.electrolibrary.info/subscribe/sub_16_datchiki.htm (дата обращения 27.03.2014).
20. Концепция системы «Умный Дом» // ASCENTIS.RU : Инженерный центр. URL: <http://www.ascentis.ru/smart/smtheory/39-smtheorycon> (дата обращения 27.03.2014).
21. Концепция федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов. Одобрена Распоряжением Правительства РФ от 27.08.2005 № 1314-р. Собрание законодательства Российской Федерации от 29.08.2005 г. № 35.
22. Краткий анализ действующих на российском рынке систем дистанционного мониторинга транспорта, или как выбрать систему и потом долго не изумляться // SIRIUS.RU: Разработка диспетчерских систем. URL: <http://www.sirius.ru/article?n=1> (дата обращения 27.03.2014).
23. Кучерявый А.Е. Интернет вещей: [Электронный документ] // ELSV.RU: Журнал «Электросвязь». 2013. Сис. требования: Adobe Reader. URL: <http://www.elsv.ru/files/actual/323.pdf> (дата обращения 25.02.2014).
24. Мальцев С. Международные аспекты развития проекта «ЭРА-ГЛОНАСС» // VESTNIK-GLONASS.RU: Межотраслевой журнал навигационных технологий. 2013. URL: http://vestnik-glonass.ru/stati/mezhdunarodnye_aspekty_razvitiya_proekta_era_glonass/ (дата обращения 27.03.2014).
25. Мониторинг автотранспорта // ASTRON-GT.RU: Спутниковый мониторинг. 2008. URL: <http://www.astron-gt.ru/article/a-5.html> (дата обращения 27.03.2014).
26. Норвегия стала первой страной, «захваченной» в популярной компьютерной игре Ingress // NORGE.RU: Новости из Норвегии. 2014. URL: <http://www.norge.ru/news/2014/02/09/23949.html> (дата обращения 25.02.2014).
27. Перспективы рынка систем «умный дом» // 220HELP.RU : Инженерные системы для дома. URL: <http://www.220help.ru/uslugi/umnyj-dom/perspektivy-gynka> (дата обращения 27.03.2014).
28. Постановление Правительства РФ от 31.03.2010 г. № 198 «Об утверждении перечня аудиовизуальных, электронных и иных технических средств надзора и контроля, используемых уголовно-

- исполнительными инспекциями федеральной службы исполнения наказаний для обеспечения надзора за осужденными к наказанию в виде ограничения свободы».
29. Покрытия с электронными сенсорами превращают полы в гигантские сенсорные экраны // UMNYDOM: Умный дом. 2014. URL: <http://umnydom.com/pokrytiya-s-elektronnymi-sensorami-prevrashhayut-poly-v-gigantskie-sensornye-ekrany/1234/> (дата обращения 27.03.2014).
 30. Про автомобили, голландских коров и уникальные свойства Интернета вещей // CISCO.COM: Новости. 2011. URL: <http://www.cisco.com/web/RU/news/releases/txt/2011/070711d.html> (дата обращения 25.02.2014).
 31. Роб ван Краненбург: Что такое IoT? // INTERNETOFTHINGS.RU : Российский исследовательский и консалтинговый центр. 2013. URL: <http://internetofthings.ru/78-blog/21-rob-van-kranenburg-chno-takoe-iot> (дата обращения 25.02.2014).
 32. *Рушкевич А., Осадчий В.* Мониторинг подвижных объектов: российские реалии и технические инновации: [Электронный документ] // WIRELESS-E.RU : Журнал Беспроводные технологии. URL: http://www.wireless-e.ru/assets/files/pdf/2010_03_56.pdf (дата обращения 27.03.2014).
 33. *Соловьев М.* Телематические аспекты в системах мониторинга подвижных и стационарных объектов : [Электронный документ] // GWE.RU: Компания «Геликс». Сис. требования: Adobe Reader. URL: http://www.gwe.ru/download/BT_03_35-37.pdf (дата обращения 27.03.2014).
 34. *Тэббитт С.* Интернет вещей начинает жить собственной жизнью // CISCO.COM: Новости. URL: <http://www.cisco.com/web/RU/news/releases/txt/2012/112612b.html> (дата обращения 25.02.2014).
 35. «Умные» датчики помогут водителям Лондона быстро находить свободное место для парковки // PULSE-UK.ORG.UK : Ежедневная русская газета в Лондоне. 2014. URL: <http://pulse-uk.org.uk/novosti/umnyie-datchiki-pomogut-voditelyam-londona-byistro-nahodit-svobodnoe-mesto-dlya-parkovki/> (дата обращения 27.03.2014).
 36. «Умные» сенсоры для охранных комплексов разработают в Томске // RIA.RU: РИА Новости. 2013. URL: <http://ria.ru/science/20130412/932302042.html> (дата обращения 27.03.2014).
 37. Умные сенсоры помогут одиноким пожилым людям // HRONIKA.INFO: Хроники событий со всего мира. 2014. URL: <http://hronika.info/tehnologii/15291-umnye-sensory-pomogut-odinokim-rozhilyum-lyudyam.html> (дата обращения 27.03.2014).
 38. *Ходаковский К.* Альянс AllSeen ускорит внедрение концепции «Интернета вещей» // 3DNESW.RU: Daily Digital Digest. 2013. URL: <http://www.3dnews.ru/786664> (дата обращения 25.02.2014).
 39. *Чеклецов В.В.* Чувство планеты: Интернет вещей и следующая технологическая революция. – М.: Российский исследовательский центр по Интернету вещей, 2013. – С. 15.
 40. *Черняк Л.* Платформа Интернета вещей // OSP.RU: Открытые системы. 2012. URL: <http://www.osp.ru/os/2012/07/13017643/> (дата обращения 25.02.2014).
 41. *Эванс Д.* Интернет вещей: как изменится вся наша жизнь на очередном этапе развития Сети // CISCO.COM: Новости. 2012. URL: <http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html> (дата обращения 25.02.2014).

42. Эванс Д. Интернет вещей: как изменится вся наша жизнь на очередном этапе развития Сети // CISCO.COM: Новости. URL: <http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html> (дата обращения 25.02.2014).
43. Эйбуд Дж. Интернет вещей: друг или враг? // CISCO.COM: Новости. 2013. URL: <http://www.cisco.com/web/RU/news/releases/txt/2013/08/081613a.html> (дата обращения 25.02.2014).
44. Эксперты: «интернет вещей» превратится в «интернет уязвимостей» // RIA.RU: РИА Новости. 2013. URL: <http://ria.ru/technology/20131217/984735839.html> (дата обращения 25.02.2014).
45. Abuot Allseen // ALLSEENALLIANCE.ORG: AllSeen Alliance. URL: <https://allseenalliance.org/allseen> (дата обращения 25.02.2014).
46. Ashton K. That 'Internet of Things' Thing // RFIDJOURNAL.COM: Technology News & Features. 2009. URL: <http://www.rfidjournal.com/articles/view?4986> (дата обращения 25.02.2014).
47. Auto-ID Labs. Официальный сайт. URL: <http://www.autoidlabs.org/> (дата обращения 25.02.2014).
48. Auto-ID Labs: Research // AUTOIDLABS.COM. URL: <http://autoidlabs.org/research/page.html> (дата обращения 25.02.2014).
49. Autonomous Mobility Applique System (AMAS) // LOCKHEEDMARTIN.COM: Lockheed Martin. URL: <http://www.lockheedmartin.com/us/products/amas1.html> (дата обращения 25.02.2014).
50. Brin D. The Transparent Society // WIRED.COM : Информационный портал. URL: <http://www.wired.com/wired/archive/4.12/fftransparent.html> (дата обращения 25.02.2014).
51. Call for Papers // IOT-CONFERENCE.ORG : Internet of Things 2014. URL: <http://www.iot-conference.org/iot2014/call-for-papers/> (дата обращения 25.02.2014).
52. Cohen S. Year of the Internet of Things // FORBES.COM : Information for the World's Business Leaders. 2014. URL: <http://www.forbes.com/sites/sarahcohen/2014/01/14/year-of-the-internet-of-things/> (дата обращения 25.02.2014).
53. DIGILE Internet of Things. Официальный сайт. URL: <http://www.internetofthings.fi/> (дата обращения 25.02.2014).
54. Daly J. What Is the Internet of Things? // STATETECHMAGAZINE.COM : Technology Insights for Leaders in State & Local Government. 2013. URL: <http://www.statetechmagazine.com/article/2013/08/what-is-the-internet-of-things> (дата обращения 27.03.2014).
55. Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020 // GARTNER.COM : Technology Research. 2013. URL: <http://www.gartner.com/newsroom/id/2636073> (дата обращения 25.02.2014).
56. Gaudin S. U.S. Military may have 10 robots per soldier by 2023 // COMPUTERWORLD.COM : IT news, features, blogs, tech review, career advice. 2013. URL: http://www.computerworld.com/s/article/9244060/U.S._military_may_have_10_robots_per_soldier_by_2023 (дата обращения 25.02.2014).
57. Google разрабатывает «умные» контактные линзы для диабетиков // FERRA.RU. 2014. URL: <http://www.ferra.ru/ru/techlife/news/2014/01/17/Google-smart-contact-lens/> (дата обращения 27.03.2014).

58. Hall E. Diageo Personalizes Whiskeys With Videos From Gift-Givers // ADAGE.COM : Advertising Age. 2012. URL: <http://adage.com/article/global-news/diageo-personalizes-whiskeys-videos-gift-givers/238015/> (дата обращения 25.02.2014).
59. Haller S. Internet of Things: An Integral Part of the Future Internet : [Электронный документ] // FUTURE-INTERNET.EU : European Future Internet Portal. 2009. Сис. требования: Adobe Reader. URL: http://services.future-internet.eu/images/1/16/A4_Things_Haller.pdf (дата обращения 25.02.2014).
60. Heineken creates interactive bottle that responds to drinkers // IOTEVENT.EU : Internet of Things Event. 2013. URL: <http://iotevent.eu/heineken-creates-interactive-bottle-that-responds-to-drinkers/> (дата обращения 25.02.2014).
61. Hill K. When 'Smart Home' Get Hacked: I Haunted A Complete Stranger's House Via The Internet // FORBES.COM: Information for the World's Business Leaders. 2013. URL: <http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/> (дата обращения 25.02.2014).
62. IEEE World Forum on Internet of Things. Официальный сайт. URL: <http://sites.ieee.org/wf-iot/> (дата обращения 25.02.2014).
63. IERC European Research Cluster on the Internet of Things. Официальный сайт. URL: <http://www.internet-of-things-research.eu/index.html> (дата обращения 25.02.2014).
64. Intel анонсировала Quark, процессор для «Интернета вещей» // НАБРАНАБ.RU: Информационный портал. 2013. URL: <http://habrahabr.ru/post/193382/> (дата обращения 25.02.2014).
65. Intel поделилась своим видением интернета вещей // IXBT.COM: Информационный портал. 2014. URL: <http://www.ixbt.com/news/hard/index.shtml?17/67/77> (дата обращения 25.02.2014).
66. Internet of Things Роба Ван Краненбурга. Лекция в рамках Futurodesignlab // DESIGN-UNION.RU: Союз дизайнеров России. 2011. URL: <http://design-union.ru/authors/theory/1490-internet-of-things-futurodesignlab> (дата обращения 25.02.2014).
67. IOT Asia 2014. Официальный сайт. URL: <http://www.internetofthingsasia.com/> (дата обращения 25.02.2014).
68. IoT Week 2014. Официальный сайт. URL: <http://iot-forum.eu/iot-week-2014/> (дата обращения 25.02.2014).
69. Merritt R. Intel Creates Internet of Things Group // EETIMES.COM: Connecting the Global Electronics Community. 2013. URL: http://www.eetimes.com/document.asp?doc_id=1320001 (дата обращения 25.02.2014).
70. Muller J. With Driverless Cars, Once Again It Is California Leading The Way // FORBES.COM: Information for the World's Business Leaders. 2012. URL: <http://www.forbes.com/sites/joannmuller/2012/09/26/with-driverless-cars-once-again-it-is-california-leading-the-way/> (дата обращения 25.02.2014).
71. Nayak M. 6 Technology Trends to Keep an Eye on This Year // TECH.CO: Tech Cocktail. 2014. URL: <http://tech.co/upcoming-technologies-watch-2014-2014-02> (дата обращения 25.02.2014).
72. Planetary Skin Institute. Официальный сайт. URL: <http://www.planetaryskin.org/> (дата обращения 25.02.2014).
73. Priddle A, Woodyard C. Google discloses costs of its driverless car tests // USATODAY.COM: Информационный портал. 2012. URL: <http://content.usatoday.com/communities/driveon/post/2012/06/google->

- discloses-costs-of-its-driverless-car-tests/1#.UwyuyoWUMdX (дата обращения 25.02.2014).
74. RFID and the Inclusive Model for the Internet of Things: [Электронный документ] // GRIFS-PROJECT.EU: Информационный портал. Систем. требования: Adobe Reader. URL: <http://www.grifs-project.eu/data/File/CASAGRAS%20FinalReport%20%282%29.pdf> (дата обращения 25.02.2014).
 75. Smarter Planet. Официальный сайт. URL: http://www.ibm.com/smarterplanet/us/en/?ca=v_smarterplanet (дата обращения 25.02.2014).
 76. SMSS // LOCKHEEDMARTIN.COM: Lockheed Martin. URL: <http://www.lockheedmartin.com/us/products/smss.html> (дата обращения 25.02.2014).
 77. Squatriglia C. Gm Says Driverless Cars Could Be on the Road by 2018 // WIRED.COM: Информационный портал. 2008. URL: <http://www.wired.com/autopia/2008/01/gm-says-driverl/> (дата обращения 25.02.2014).
 78. The 5th Annual Internet of Things European Summit. Официальный сайт. URL: http://www.eu-ems.com/summary.asp?event_id=210&page_id=1789 (дата обращения 25.02.2014).
 79. The IoT Initiative. Официальный сайт. URL: <http://www.iotfestival.com/> (дата обращения 25.02.2014).
 80. Things Con. Официальный сайт. URL: <http://thingscon.com/> (дата обращения 25.02.2014).
 81. Cohen S. Year of The Internet of Things. 2014. URL: <http://www.forbes.com/sites/sarahcohen/2014/01/14/year-of-the-internet-of-things/> (дата обращения 25.02.2014).
 82. URL: <http://pl-e.ru/w/RFID>.
 83. URL: <http://kritikalsolutions.com/images/stories/ADAS.png>.
 84. URL: <http://oxozle.com/2014/07/15/chto-takoe-ibeacon>.
 85. URL: <http://www.3arc.com/eu/PersonalTrackers/WeaponsIntelligence/tabid/67/language/en-GB/Default.aspx> (дата обращения 27.03.2014).
 86. URL: http://www.ua.all.biz/img/ua/service_catalog/427316.jpeg (дата обращения 27.03.2014).
 87. URL: http://gadgetsin.com/uploads/2012/06/knut_an_app_powered_monitor_for_your_home_3.jpg (дата обращения 27.03.2014).
 88. URL: <http://www.tecmovia.com/wp-content/uploads/2014/02/posts/us-army-autonomous-030214-01.png> (дата обращения 27.03.2014).
 89. URL: <http://www.3arc.com/eu/PersonalTrackers/WeaponsIntelligence/tabid/67/language/en-GB/Default.aspx> (дата обращения 27.03.2014).
 90. URL: http://pl-e.ru/w/RFID_помогает_контролировать_движение_табельного_оружия (дата обращения 27.03.2014).
 91. URL: <http://habrahabr.ru/company/medgadgets/blog/227159/> (дата обращения 27.03.2014).